R G B WH GR BL Grey Scale #13 C M Y K
DANES-PICTA.COM
A 1 2 3 4 5 6 M 8 9 10 11 12 13 14 15 B 17 18 19

22

AKADEMIA OBRONY NARODOWEJ

mgr Krzysztof LIEDEL

ZARZĄDZANIE ZASOBAMI INFORMACYJNYMI W WARUNKACH ZAGROŻEŃ TERRORYSTYCZNYCH DLA BEZPIECZEŃSTWA PAŃSTWA

Rozprawa doktorska

Biblioteka Główna
Akademii Obrony Narodowej
S/7595
05-007595-001-0

Warszaw

75500

Colour Chart #13
Blue Cyan Green Yellow Red Magenta White 3/Color Black
Inches Centimetres
DANES-PICTA.COM

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ BEZPIECZEŃSTWA NARODOWEGO

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 45500
Akademii Obrony Narodowej

mgr Krzysztof LIEDEL

ZARZĄDZANIE ZASOBAMI INFORMACYJNYMI W WARUNKACH ZAGROŻEŃ TERRORYSTYCZNYCH DLA BEZPIECZEŃSTWA PAŃSTWA

Rozprawa doktorska

Rozprawa pod kierunkiem naukowym:
płk. w st. spocz. prof. zw. dr hab. inż. Piotra Sienkiewicza

WARSZAWA **2009**

Spis treści

WSTĘP **7**

1 Metodologiczne podstawy badań nad zarządzaniem zasobami informacyjnymi **13**

1.1 Przedmiot badań 13

1.2 Cel główny i cele szczegółowe pracy 16

1.3 Problemy badawcze i hipotezy robocze 16

1.4 Metody i techniki badawcze 22

1.5 Ocena piśmiennictwa 27

1.6 Obszar i organizacja badań 28

2 Terroryzm – charakterystyka zjawiska i jego zwalczania **33**

2.1 Charakterystyka zjawiska terroryzmu 33

2.1.1 Geneza terroryzmu 34

2.1.2 Definiowanie i klasyfikacje terroryzmu 37

2.1.3 Metody ataków terrorystycznych 43

2.2 Systemy przeciwdziałania terroryzmowi – aspekty informacyjne 49

2.2.1 Rozpoznanie zagrożeń terrorystycznych 50

2.2.2 Profilaktyka 52

2.2.3 Zwalczanie terroryzmu 58

2.2.4 Minimalizacja i likwidacja skutków ataków terrorystycznych 66

2.3 Wnioski 69

3 Rola zasobów informacyjnych w systemie przeciwdziałania **71**

3.1 Informacja jako zasób strategiczny 71

3.1.1 Społeczeństwo informacyjne 71

3.1.2 Informacja jako kategoria 79

3.2 Klasyfikacja zasobów informacyjnych 83

3.3 Wartość i użyteczność informacji 87

3.3.1 Jakość informacji 88

3.3.2 Użyteczność informacji 89

3.3.3 Wartość informacji 91

3.4 Informacyjny zasób strategiczny w systemie bezpieczeństwa państwa 93

2.3 Informacyjny zasób strategiczny w systemie przeciwdziałania terroryzmowi – podejście reaktywne i proaktywne w przeciwdziałaniu terroryzmowi 99

2.3 Wnioski 101

4 Zarządzanie zasobami informacyjnymi w systemie przeciwdziałania terroryzmowi 103

4.1 Zarządzanie zasobami informacyjnymi 103

4.2 Zbieranie (pozyskiwanie) informacji 105

4.3 Przetwarzanie informacji 109

4.3.1 Pojęcie cyklu analitycznego 109

4.3.2 Struktura dokumentu analitycznego 111

4.3.3 Techniki analityczne (techniki twórczego myślenia) 112

4.3.4 Analiza ryzyka jako kluczowy element w planowaniu antyterrorystycznym 114

4.4 Przechowywanie (bazy danych) 118

4.5 Udostępnianie informacji 123

4.6 Media masowe a terroryzm – wykorzystanie mediów w przeciwdziałaniu terroryzmowi 126

4.7 Bezpieczeństwo informacyjne 139

4.7.1 Bezpieczeństwo i ochrona informacji niejawnych 139

4.7.2 Ujęcie proceduralno – organizacyjne 141

4.7.3 Bezpieczeństwo personalne 142

4.7.4 Bezpieczeństwo fizyczne 143

4.7.5 Bezpieczeństwo techniczne 144

4.7.6 Ochrona informacji niejawnych w NATO i Unii Europejskiej 145

4.8 Wnioski 151

5 Systemy informacji w przeciwdziałaniu terroryzmowi – wybrane rozwiązania 153

5.1 System amerykański – Narodowe Centrum Kontr-Terrorystyczne 153

5.1.1 Analiza 158

5.1.2 Wsparcie operacyjne 160

5.1.3 Zarządzanie misjami 162

5.2 System niemiecki – Wspólne Centrum Walki z Terroryzmem (GTAZ) 162

5.3 System francuski – Jednostka ds. Koordynacji Zwalczania Terroryzmu (UCLAT) 170

5.4 System brytyjski – Wspólne Centrum Analiz Terroryzmu (Joint Terrorism Analysis Centre – JTAC) oraz system zarządzania kryzysowego 177

5.4.1 Wspólne Centrum Analiz Terroryzmu (JTAC) 177

5.4.2 Koordynacja reagowania w sytuacjach kryzysowych 178

5.5 Inne rozwiązania 179

5.5.1 Centrum Antyterrorystyczne polskiej Agencji Bezpieczeństwa Wewnętrznego 179

5.5.2 Prace Centrum Badań nad Terroryzmem Collegium Civitas 183

5.5.3 Prace RAND Corporation 186

5.5.4 Wspólna Polsko-Amerykańska Grupa Robocza ds. Zwalczania Terroryzmu 190
5.6 Wnioski 193
6 Model zarządzania zasobami informacyjnymi w systemie przeciwdziałania terroryzmowi..... 201
6.1 Podstawowe funkcje zarządzania 201
6.2 Koordynacja w systemie przeciwdziałania terroryzmowi 204
6.3 Rozpoznanie sytuacji zagrożeń 210
6.4 Analiza informacji w systemie przeciwdziałania terroryzmowi 213
6.5 Przechowywanie – bazy danych 215
6.6 Komunikacja ze społeczeństwem i media w systemie przeciwdziałania terroryzmowi 220
6.7 Warunki realizacji modelu 223
Zakończenie 225
Literatura 227
ZAŁĄCZNIK 1 239
ZAŁĄCZNIK 2 241
ZAŁĄCZNIK 3 245
ZAŁĄCZNIK 4 246

WSTĘP

Nie ma czegoś takiego, jak izolowany człowiek lub sytuacja. Istnieje tylko relacja między człowiekiem i środowiskiem. Relacja, której sens oddaje wyraz „zagrożenie".

A. Magnusson

Każda epoka ma własny, niepowtarzalny nakaz chwili. I pierwszym wymogiem chwili obecnej jest stworzenie skutecznego systemu bezpieczeństwa. W XXI wieku rodzi się nowy globalny system bezpieczeństwa, który mógłby stwarzać nadzieję na minimalizację ryzyka wojen i wystąpienia zagrożeń dla pokoju, zakłócających bądź utrudniających trwały i zrównoważony rozwój cywilizacyjny. Obecnie istnieje świadomość, że kres bipolarnego systemu globalnego bezpieczeństwa nie przyniósł żadnego „końca historii", natomiast cieniem na myśleniu o „wieczystym pokoju" kładą się nowe zagrożenia z terroryzmem na czele.[1]

Obrona przez terroryzmem międzynarodowym to jedno z najważniejszych wyzwań współczesności. Terroryzm ze względu na swój charakter, tj. niezwykłą różnorodność form i dynamikę, zdolność ewoluowania i szybkiego dostosowywania się do środków bezpieczeństwa stosowanych przez państwa jest zagrożeniem szczególnie trudnym w zwalczaniu. Terroryzm międzynarodowy jest ponadto zjawiskiem, które rozpatrywać należy w dwóch podstawowych aspektach:

- w aspekcie bezpośrednich skutków, czyli strat ludzkich oraz strat materialnych,
- w aspekcie konsekwencji o charakterze politycznym.

Nie wymaga szczegółowego omawiania pierwszy aspekt skutków ataków terrorystycznych. Należy jednak poświęcić więcej uwagi wymiarowi drugiemu. Z punktu widzenia państwa jest on szczególnie istotny, bowiem zaburza relacje społeczne, a zwłaszcza relacje pomiędzy rządem i społeczeństwem. Niezależnie od zmian roli państwa we współczesnych społeczeństwach, jednym z podstawowych zobowiązań rządów jest zapewnienie bezpieczeństwa i przestrzegania porządku publicznego na terytorium kraju.

---

[1] Sienkiewicz P., Świeboda H., *Perspektywy badań systemowych nad bezpieczeństwem, AKAFM, Kraków 2009.*

W sytuacji, w której rząd i podległe mu służby odpowiedzialne za bezpieczeństwo, nie są w stanie zabezpieczyć przed atakiem terrorystycznym, podważone zostaje zaufanie społeczne do rządzących elit w najbardziej podstawowej kwestii, jaką jest gwarancja bezpieczeństwa. Dlatego też, dla zachowania stabilności politycznej państwa oraz ze względu na konieczność zapewnienia pożądanej ochrony obywateli, państwa muszą tworzyć efektywne systemy bezpieczeństwa, w tym przeciwdziałania terroryzmowi. Jeden z najbardziej uznanych współczesnych badaczy terroryzmu, Bruce Hoffman, pisze:

> *Najpierw denerwujesz się wsiadając do autobusu. Później zastanawiasz się nad tym, czy pójść do supermarketu. Następnie dwa razy rozważasz, czy posiedzieć dłużej w swojej ulubionej kawiami. Wreszcie żadne miejsce nie wydaje się bezpieczne. Grupy terrorystyczne mają strategię – skurczyć do niebytu obszary, w których ludzie poruszają się swobodnie [...].*[2]

Odrębną refleksję warto poświęcić kwestii terytorialnego zasięgu zagrożenia terrorystycznego. W zglobalizowanym świecie zagrożenie takie, jak terroryzm, utraciło już wyłącznie lokalny wymiar. Terroryzm jest zjawiskiem, które w niezwykle elastyczny sposób dostosowuje się do zmieniających się wymogów otaczającej rzeczywistości.

Zdolność ewolucji, przy jednoczesnej możliwości realizowania transgranicznych, międzynarodowych, a nawet globalnych celów, jest jednym z czynników, które wpływają na wagę zagrożenia terroryzmem. Wpływają na to także: szeroki zasięg i wielorakość zagrożeń terrorystycznych, ich zmienność i dynamika. Jest to wyzwanie dla demokratycznych państw oraz ich trwałego i zrównoważonego rozwoju. Stawić czoła temu wyzwaniu muszą instytucje i służby odpowiedzialne za bezpieczeństwo współczesnych państw. Rośnie przy tym znaczenie ekspertyz i raportów opracowywanych przez ośrodki badawcze i akademickie[3].

Potrzeba badań nad zjawiskiem terroryzmu i zagrożeniami terrorystycznymi dla bezpieczeństwa współczesnych państw wynika nie tylko z potrzeb poznawczych, ale

---

[2] Hoffman B., *The Logic of Suicide Terrorism* [in:] Howard Russell D., Sawyer Reid L. (ed.), *Terrorism and Counterterrorism. Understanding the New Security Environment*, The McGrawHill Companies, Guilford 2005, s. 260.

[3] Patrz: Nardulli B., *The Global War on Terrorism. An early look at Implications for the Army,* RAND Corporation, Santa Monica 2003.

także z potrzeby czysto utylitarnej, wspomagania budowy systemu bezpieczeństwa państwa w zakresie ochrony przed zagrożeniami terrorystycznymi.

W pracy dokonano przeglądu istotnych elementów systemu przeciwdziałania terroryzmowi w najważniejszym wymiarze tego systemu, tj. organizowania, koordynowania i synchronizacji działań wszystkich podmiotów zaangażowanych w przeciwdziałanie terroryzmowi.

Skuteczne przeciwdziałanie zagrożeniom terrorystycznym wymaga efektywnego systemu informacyjnego, zapewniającego realizację następujących procesów informacyjnych:

- pozyskiwanie informacji o źródłach i obiektach zagrożeń, metodach i technikach działań terrorystycznych, strukturach i lokalizacji organizacji terrorystycznych, itp. pochodzących z różnych, także niestandardowych źródeł,
- przesyłanie informacji w pożądanej formie, terminie i wymaganej wiarygodności,
- przechowywanie informacji o zagrożeniach terrorystycznych – tworzenie specjalistycznych baz danych,
- przetwarzanie informacji dla celów prognozowania i planowania działań antyterrorystycznych,
- dystrybucja informacji dla właściwych odbiorców, w pożądanym czasie i formie,
- kształtowanie pożądanych relacji z mediami (systemem masowego komunikowania).

Realizacja powyższych procesów informacyjnych wymaga organizacji i funkcjonowania systemu zarządzania informacjami oraz efektywnego wykorzystania technologii teleinformatycznych: Internetu, systemów rozpoznania (także kosmicznego), itp., a także współczesnych systemów zarządzania wiedzą.

Należy uwzględniać również efekt korzystania z technologii teleinformatycznych przez organizacje terrorystyczne. Przyniosło to nowy typ terroryzmu – cyberterroryzm[4].

[4] Jemioło T., Kisielnicki J., Rajchel K. (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, WSPol, Warszawa 2009; Świeboda H., *Zagrożenia informacyjne bezpieczeństwa RP.* Rozprawa doktorska;

Określono pożądany model funkcjonowania sytemu zarządzania zasobami informacyjnymi w sytuacji zagrożenia terrorystycznego dla bezpieczeństwa instytucji państwowych i społeczeństwa. Proces realizacji tego zadania w innych państwach poddany został szczegółowej analizie, której celem było określenie pożądanych cech systemowych: strukturalnych i funkcjonalnych.

W pierwszej części rozprawy zaprezentowano podstawowe kwestie dotyczące zjawiska terroryzmu oraz zagrożeń terrorystycznych dla współczesnych państw. Zdefiniowano zjawiska oraz ich wpływ na rozwój bezpiecznego państwa i funkcjonowanie społeczności międzynarodowej.

Drugą część pracy poświęcono zasobom informacyjnym i ich znaczeniu w organizacji przeciwdziałania terroryzmowi. Przedstawiono najważniejsze kwestie metodologiczne i terminologiczne dotyczące zasobów informacyjnych i ich roli w systemie bezpieczeństwa państwa ze szczególnym uwzględnieniem organizacji przeciwdziałania terroryzmowi.

W trzeciej części zaprezentowano procesy zarządzania zasobami informacyjnymi właściwe dla efektywnego wykorzystywania zasobów informacyjnych w systemie przeciwdziałania terroryzmowi. Przedstawione zgodnie z cyklem zarządzania zasobami informacyjnymi (gromadzenie – przetwarzanie – przechowywanie – dystrybucja), funkcje zarządzania ujęto w aspekcie maksymalizacji ich efektywności w sytuacji przeciwdziałania zagrożeniom terrorystycznym dla bezpieczeństwa.

Czwarta część rozprawy została poświęcona prezentacji wyników badań nad systemami zarządzania zasobami informacyjnymi w systemie przeciwdziałania terroryzmowi w czterech państwach, prowadzących intensywne działania w zakresie zwalczania terroryzmu, tj. w USA, Wielkiej Brytanii, Francji i Niemczech.

W piątej części pracy zaprezentowano rekomendowane modelowe rozwiązanie w zakresie zarządzania zasobami informacyjnymi w systemie przeciwdziałania terroryzmowi. Model ten obejmuje wszystkie etapy zarządzania informacją w specyficznym kontekście przeciwdziałania terroryzmowi, tj. rozpoznanie, przetwarzanie informacji, przechowywanie informacji (bazy danych), dystrybucja informacji oraz koordy-

---

Lichocki E., *Model systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informacyjnego Sił Zbrojnych Rzeczypospolitej Polskiej*. Rozprawa doktorska, AON, 2009.

nację działań antyterrorystycznych, a także zagadnienia związane z komunikacją ze społeczeństwem i mediami w systemie przeciwdziałania terroryzmowi.

Podjęcie tematu zarządzania zasobami informacyjnymi na potrzeby systemu przeciwdziałania terroryzmowi wynika nie tylko z zainteresowań naukowych autora, ale także z wieloletnich doświadczeń praktycznych w obszarze bezpieczeństwa państwa. Doświadczenia te, związane są zarówno ze służbą w Policji, jak i z pracą w Ministerstwie Spraw Wewnętrznych i Administracji na stanowisku naczelnika wydziału ds. przeciwdziałania zagrożeniom terrorystycznym oraz kierowaniem zespołami zadaniowymi Międzyresortowego Centrum ds. Zwalczania Przestępczości Zorganizowanej i Międzynarodowego Terroryzmu:

- zespołem zadaniowym do stworzenia podstaw prawnych działania Krajowego Koordynatora do Spraw Przeciwdziałania Terroryzmowi,
- zespołem zadaniowym do spraw koordynacji współpracy w przeciwdziałaniu terroryzmowi.

Istotnym motywem do podjęcia takich badań były także liczne wizyty studyjne oraz staże odbyte w RAND Corporation. Zainteresowanie terroryzmem, jako potencjalnym wyzwaniem dla krajowych i globalnych systemów bezpieczeństwa datuje się zresztą od czasu wczesnej refleksji autora nad przeciwdziałaniem terroryzmowi lotniczemu[5].

Na podjęcie tematu rozprawy i przeprowadzenie niezbędnych badań uwieńczonych pracą doktorską złożyły się następujące motywy:

- praktyczne, wyrażające się chęcią wniesienia wkładu do kształtującego się w Polsce systemu przeciwdziałania terroryzmowi;
- wieloletnie zainteresowania zawodowe i badawcze tematyką bezpieczeństwa;
- związane z udziałem w badaniach nad informacją w systemie przeciwdziałania terroryzmowi[6].

[5] Patrz: Liedel K., *Zwalczanie terroryzmu lotniczego – aspekty prawnomiędzynarodowe*, Warszawa 2003.

[6] Na przykład udział autora w pracach projektu badawczego: „Model wykorzystania środków masowego przekazu w przeciwdziałaniu i walce z terroryzmem w warunkach RP".

Należy podkreślić, że przedmiotem rozprawy nie są problemy wyboru sił i środków, których należy użyć w określonych akcjach antyterrorystycznych, lecz organizacja procesów informacyjnych rozpatrywanych z punktu widzenia potrzeb systemu zarządzania informacjami „o terroryzmie".

Autor wyraża wdzięczność Komendzie Akademii Obrony Narodowej i Wydziału Bezpieczeństwa Narodowego Akademii Obrony Narodowej za umożliwienie otwarcia przewodu doktorskiego oraz przełożonym, przyjaciołom i współpracownikom z Collegium Civitas.

Pragnę serdecznie podziękować Panu Profesorowi Piotrowi Sienkiewiczowi za wsparcie i przewodnictwo intelektualne oraz nieustającą mobilizację do tego, aby przedsięwzięcie w postaci badań stanowiących podstawę stworzenia niniejszej pracy ukończyć i zaprezentować w formie rozprawy doktorskiej.

Rozdział 1

Metodologiczne podstawy badań nad zarządzaniem zasobami informacyjnymi

Współczesny paradygmat wojny, w którym wojny prowadzone przez państwa ze względu na narodowe interesy za pomocą formalnych środków walki zbrojnej, zastępowany jest przez podejście postmodernistyczne. [...] Podczas gdy wojna pomiędzy państwami zostaje po jednaj stronie obrotowych drzwi historii, konflikty niskiej intensywności pomiędzy różnymi organizacjami nadchodzą z drogiej strony. Suwerenności narodowe podważane są przez organizacje (podmioty niepaństwowe) które odmawiają uznania państwowego monopolu w zakresie zbrojnej przemocy.

Martin van Creveld, 1991 (*Transformation of War*)

1.1 Przedmiot badań

Przedmiotem badań, których rezultaty uwieńczone zostały powstaniem niniejszej rozprawy, zatytułowanej *Zarządzanie zasobami informacyjnymi w warunkach zagrożeń terrorystycznych dla bezpieczeństwa państw,* jest zastosowanie szeroko pojętych **metod zarządzania zasobami informacyjnymi jako zasobami strategicznymi w systemie bezpieczeństwa antyterrorystycznego państwa.** Na wybór tematu rozprawy i p[przedmiotu badań wpłynęła przede wszystkim jego wyjątkowa ranga w kontekście współczesnych wyzwań cywilizacyjnych i zagrożeń dla bezpieczeństwa państwa oraz aktualność zarówno w wymiarze globalnym, jak i lokalnym, w szczególności dla Polski jako kraju, który stoi przed potrzebą zbudowania efektywnego systemu przeciwdziałania terroryzmowi.

Przedmiotem badań były te zagadnienia, które bezpośrednio dotyczą jednej z podstawowych potrzeb państwa, tj. zapewnienia funkcjonalności działań instytucji odpowiedzialnych za bezpieczeństwo państwa. Funkcjonalność i racjonalność takich działań wymagają przede wszystkim skutecznej koordynacji, która umożliwia wzajemne wspieranie wielu przedsięwzięć, ich synchronizację w czasie i przestrzeni.

W kontekście działań związanych z bezpieczeństwem państwa skuteczna koordynacja wymaga przede wszystkim efektywnego zarządzania informacjami w celu tworzenia wspólnego obrazu sytuacji („świadomości sytuacyjnej") dla wszystkich podmiotów odpowiedzialnych za bezpieczeństwo wewnętrzne i zewnętrzne państwa.

Rosnący wpływ poza-militarnych zagrożeń wymaga analizowania i prognozowania zmian w bliższym i dalszym otoczeniu państwa, co wiąże się z optymalizacją procesów informacyjnych w aspekcie potrzeb systemu przeciwdziałania terroryzmowi.

Całość problematyki terroryzmu oraz metod jego zwalczania w kontekście potrzeb i wymagań zarządzania informacjami w procesie zapewniania bezpieczeństwa państwa wymaga dokładnej, kompleksowej i wielopłaszczyznowej analizy systemowej. Pomimo istnienia już bogatej literatury, pozostaje jeszcze bardzo wiele kwestii poznawczych i praktycznych, które zmuszają do podejmowania badań multi- i interdyscyplinarnych.

Sformułowanie tematu określa zakres i zasięg podjętych badań nad systemem zarządzania zasobami informacyjnymi istotnymi dla bezpieczeństwa państwa w aspekcie instytucjonalnym (z uwzględnieniem głównych podmiotów zaangażowanych w przeciwdziałanie terroryzmowi).

Skłonił także do zaprezentowania istoty informacji jako zasobu strategicznego we współczesnych systemach bezpieczeństwa, pozwalając na szczegółową analizę:

- informacji jako zasobu strategicznego państwa,
- informacji jako zasobu strategicznego w systemie bezpieczeństwa,
- informacji jako zasobu strategicznego w systemie przeciwdziałania terroryzmowi.

Przyjęte założenia podjętej analizy pozwoliły na przedstawienie szerokiego spektrum zagadnień, tj. wszystkich poziomów funkcjonowania instytucji państwowych i zarządzania zasobami informacyjnymi państwa w sytuacji zagrożenia dla bezpieczeństwa państwa generowanego przez zjawisko terroryzmu.

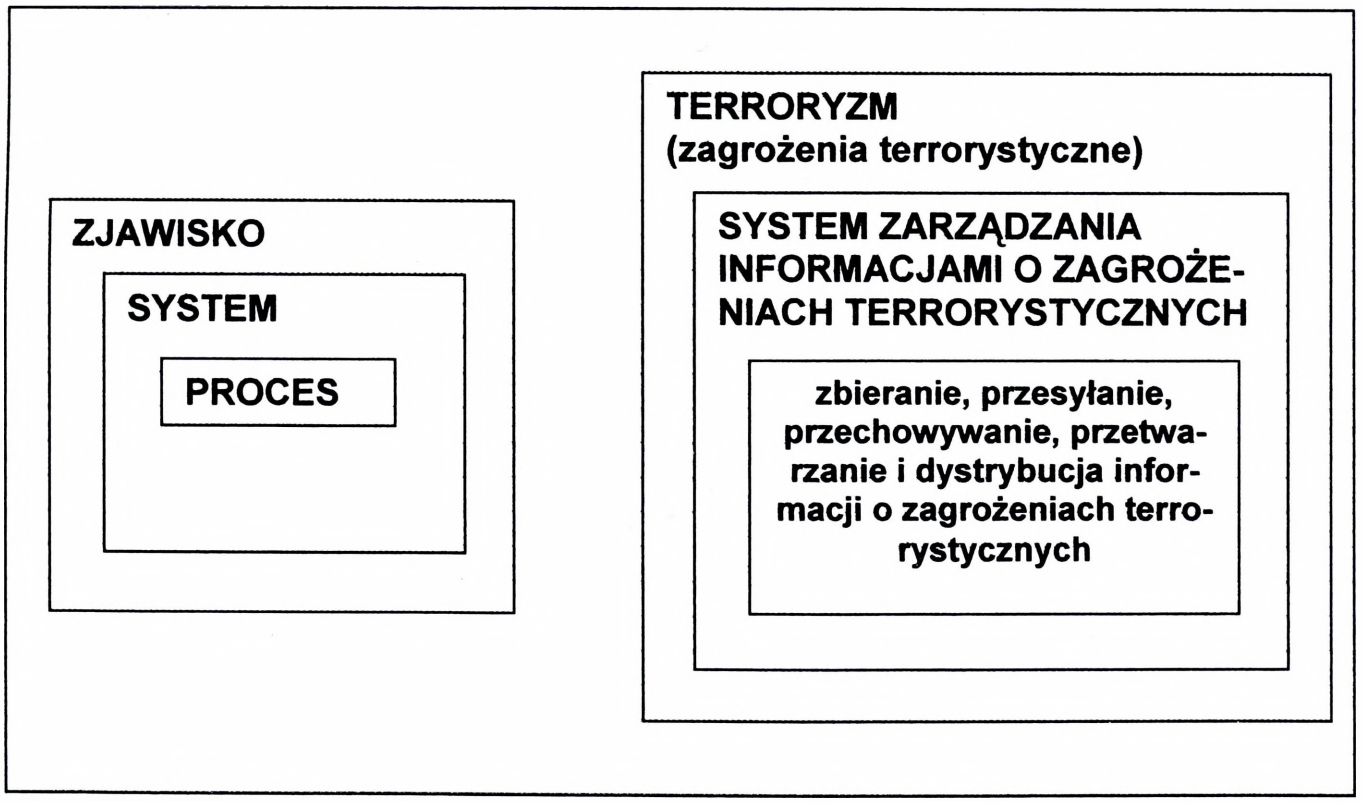
W celu określenia przedmiotu badań przyjęto swoistą hierarchię kategorii poznania:

- zjawisko (byt, wyróżniony fragment rzeczywistości będący przedmiotem poznania),
- system (złożony obiekt, traktowany jako całość, w którym zjawisko realizuje się lub jest siłą mającą wpływ na zjawisko),

- procesy (realizowany w systemie ciąg zdarzeń będących przyczyną lub skutkiem zmian zjawiska)[7].

W związku z powyższym przedmiot badań w niniejszej rozprawie zyskał następującą konkretyzację (rys. 1):

- **zjawisko:** TERRORYZM jako zagrożenia dla bezpieczeństwa narodowego i międzynarodowego,
- **system:** SYSTEM ZARZĄDZANIA INFORMACJAMI O ZAGROŻENIACH TERRORYSTYCZNYCH BEZPIECZEŃSTWA RP,
- **procesy:** zarządzanie informacjami o zagrożeniach terrorystycznych, czyli organizacja i koordynacja procesów pozyskiwania, przesyłania, przetwarzania, przechowywania i dystrybucji informacji zgodnie z potrzebami i wymaganiami sytemu przeciwdziałania terroryzmowi (w systemie bezpieczeństwa narodowego RP).



Rys. 1: Ogólny model przedmiotu (obiektu) badań i jego konkretyzacja
Źródło: opracowanie własne.

[7] W trakcie seminarium doktoranckiego prof. P. Sienkiewicza przyjęto jako ogólne kategorie opisu przedmiotu badań: zjawiska, procesy, zdarzenia, rzeczy.

1.2 Cel główny i cele szczegółowe pracy

Niniejsza rozprawa doktorska, zgodnie z przyjętymi zasadami prowadzenia przedsięwzięć badawczych, posiada dwa podstawowe cele badawcze:

- cel poznawczy: analiza systemu zarządzania informacjami jako elementu systemu bezpieczeństwa państwa w kontekście przyjętych założeń teoretycznych dla procesów zarządzania oraz w kontekście systemów zarządzania informacjami istniejących w wybranych państwach;
- cel utylitarny: opracowanie modelu zarządzania informacjami w procesie rozpoznania zagrożeń dla bezpieczeństwa państwa przez terroryzm na potrzeby systemu przeciwdziałania terroryzmowi, z uwzględnieniem rozwiązań, których zastosowanie byłoby możliwe w Polsce (w istniejących warunkach organizacyjno – prawnych).

Do celów szczegółowych pracy należy natomiast zaliczyć:

1. Określenie wpływu zasobów informacyjnych na kształtowanie strategii państwa w przeciwdziałaniu terroryzmowi;
2. Określenie elementów, procedur i relacji stanowiących części składowe systemu zarządzania informacją w odniesieniu do instytucji i służb odpowiedzialnych za przeciwdziałanie terroryzmowi w państwie;
3. Dokonanie analizy rozwiązań stosowanych w innych, wybranych państwach w celu stworzenia modelu „optymalnego" systemu przeciwdziałania terroryzmowi.

Określone w ten sposób cele główne i szczegółowe pracy stanowią podstawę, która pozwoliła na sformułowanie problemów badawczych, wyznaczających obszar badań empirycznych.

1.3 Problemy badawcze i hipotezy robocze

Dynamika i złożoność zjawiska terroryzmu jako wyzwania i zagrożenia stojącego przed współczesnymi państwami wymaga stworzenia nowych rozwiązań organizacyjnych i systemowych w celu przeciwdziałania temu zagrożeniu.

Ze względu na charakter zagrożenia terrorystycznego, dużą liczbę powodowanych ofiar i wysokie straty materialne, racjonalną strategią przeciwdziałania terroryzmowi jest strategia zapobiegania (prewencji). Zdolności zapobiegania zagrożeniom terrorystycznym stanowią główny czynnik efektywności rozwiązań organizacyjnych I systemowych. Dla skutecznego zapobiegania terroryzmowi najistotniejszym środkiem jest posiadanie informacji zaspokajających potrzeby i spełniających wymagania podmiotów odpowiedzialnych za podjęcie działań zapobiegawczych na etapie przygotowywania ataku terrorystycznego.

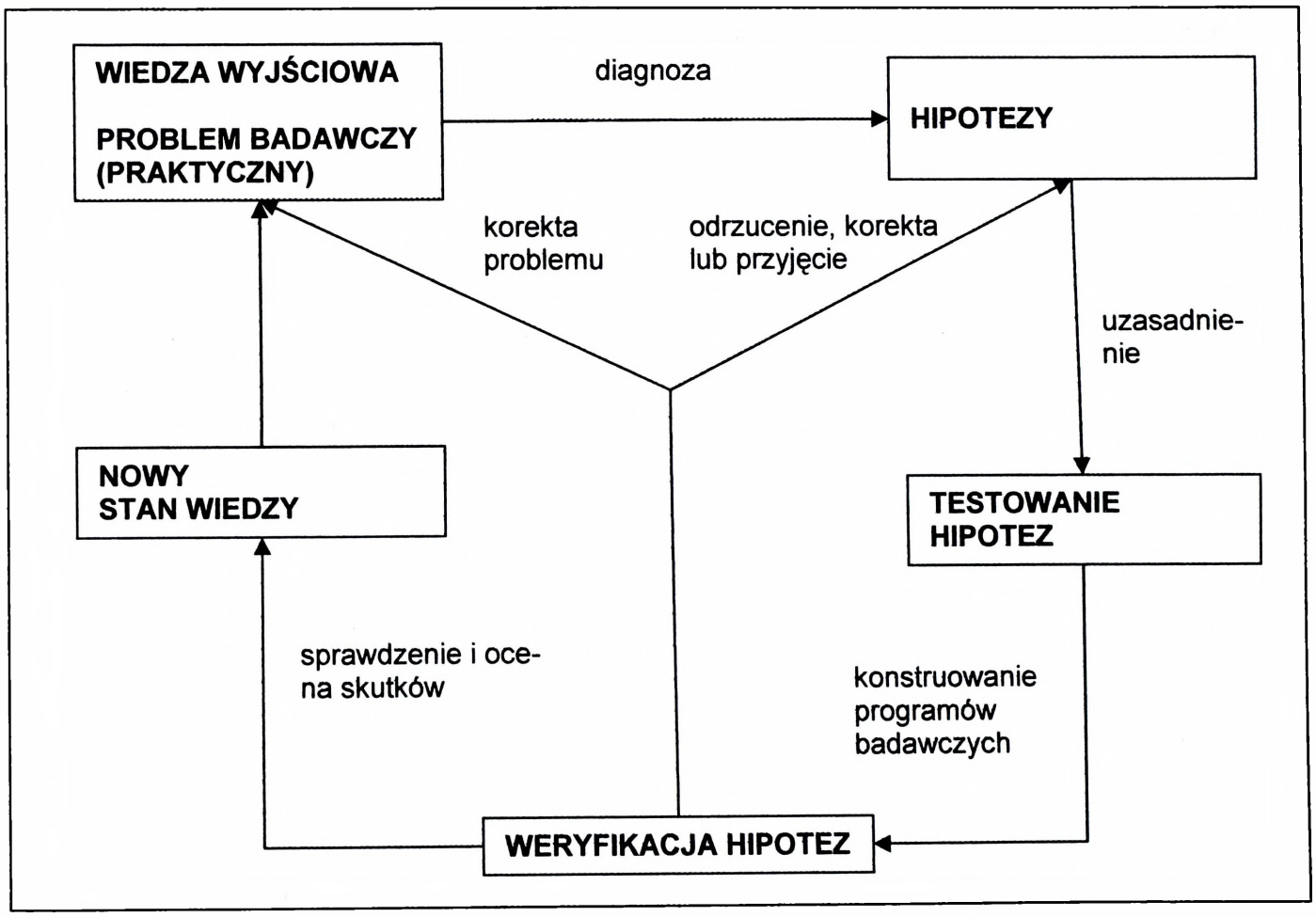
Z powyższych powodów konieczne jest stworzenie takiego systemu, który umożliwi efektywne zapobieganie zagrożeniom terrorystycznym poprzez sprawne zarządzanie systemem obiegu informacji oraz sprawne funkcjonowanie wszystkich jego elementów, a zatem:

- rozpoznania,
- przetwarzania informacji,
- przechowywania informacji,
- dystrybucji / rozpowszechniania informacji,
- koordynacji w systemie przeciwdziałania terroryzmowi,
- komunikacji ze społeczeństwem i mediami w systemie przeciwdziałania terroryzmowi.

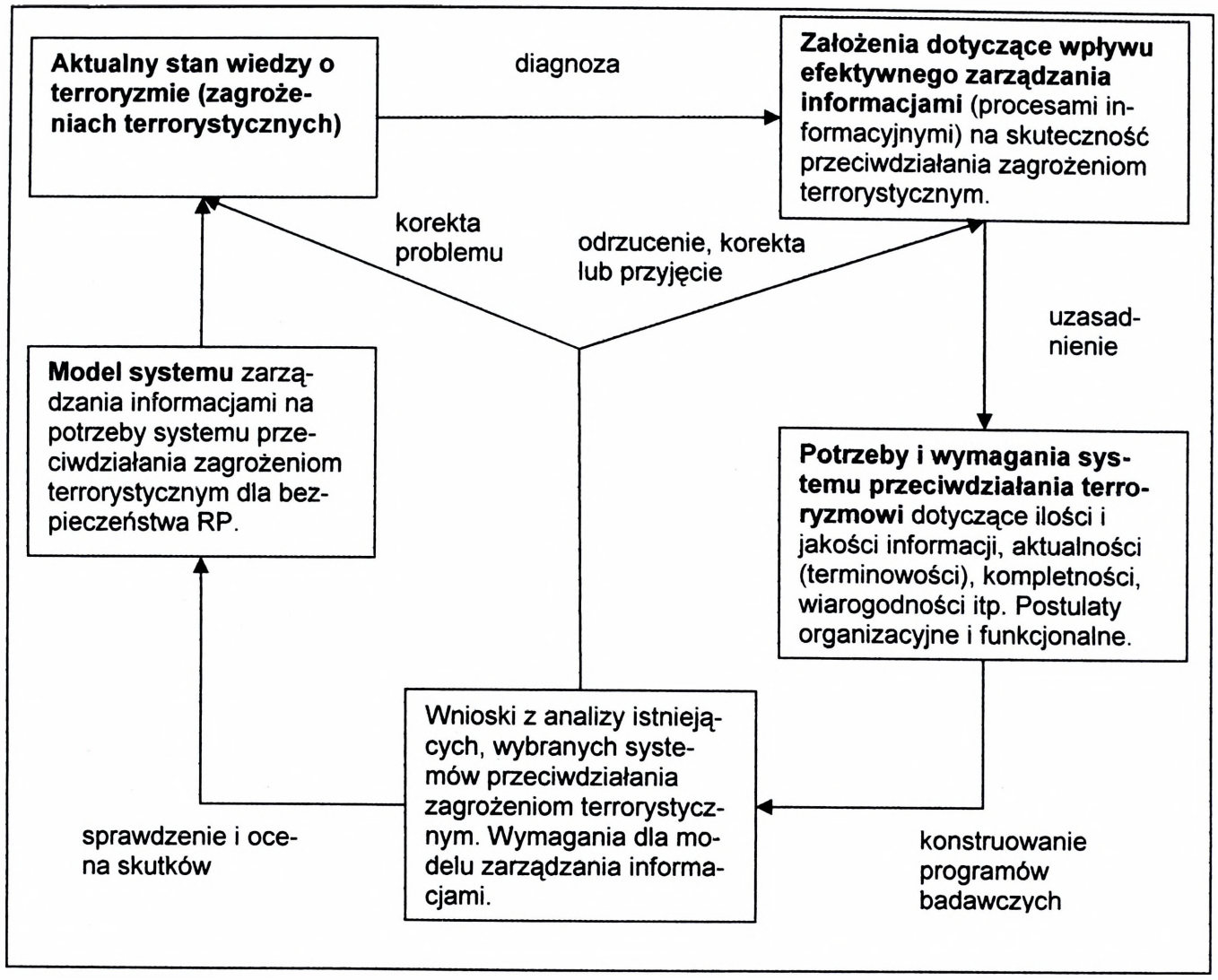
Model systemu zarządzania informacjami umożliwi przyjęcie niezbędnych dla efektywnej koordynacji procedur i mechanizmów współdziałania podmiotów odpowiedzialnych za przeciwdziałanie terroryzmowi. Model powinien umożliwić wybór procedury sterowania przepływami informacji, niezbędnych dla określenia zadań realizowanych przez uczestników systemu Opis centralnego elementu systemu, tj. centrum koordynacji i zarządzania informacjami, umożliwi stworzenie optymalnego podsystemu koordynacji i wymiany informacji w systemie przeciwdziałania terroryzmowi.

Z przyjętych celów głównych i szczegółowych pracy wynikają problemy badawcze, które spełnią warunki *sine qua non* właściwie sformułowanych problemów badawczych, tj. określających efektywność poszukiwanych działań, empirycznie rozstrzygalnych oraz posiadających wartość praktyczną. W pracy podjęto następujący główny problem badawczy:

wykazanie potrzeby istnienia w ramach systemu bezpieczeństwa państwa, szczególnie w kontekście przeciwdziałania zagrożeniom terrorystycznym, efektywnego systemu zarządzania zasobami informacyjnymi jako zasobami strategicznymi z punktu widzenia tego systemu oraz wskazanie kierunku jego rozwoju oraz możliwości stworzenia takiego systemu w Polsce dzięki opracowaniu modelu spełniającego warunki I ograniczenia właściwe dla Polski.



Rys. 2: Ogólny model badań naukowych
Źródło: Sienkiewicz P., *Metodologia badań systemowych*, Warszawa 2008.



Rys. 3: Ogólny model badań naukowych nad zarządzaniem informacjami o zagrożeniach terrorystycznych dla bezpieczeństwa RP
Źródło: opracowanie własne

Dla rozwiązania przedstawionego powyżej problemu badawczego konieczne jest przeprowadzenie wieloetapowych badań, które pozwolą rozwiązanie następujących szczegółowych problemów badawczych:

1. Wykazanie wpływu zasobów informacyjnych państwa w obszarze przeciwdziałania terroryzmowi na wybór strategii przeciwdziałania temu zagrożeniu:
   - wykazanie wpływu zasobów informacyjnych na procesy tworzenia racjonalnego systemu bezpieczeństwa oraz polityki bezpieczeństwa państwa;
   - wykazanie wpływu zasobów informacyjnych na działania realizowane w ramach systemu przeciwdziałania terroryzmowi na wszystkich płaszczyznach jego funkcjonowania;

2. Określenie zasad funkcjonowania systemu zarządzania zasobami informacyjnymi posiadanymi przez podmioty odpowiedzialne za bezpieczeństwo państwa w warunkach zagrożenia państwa przez terroryzm:
   - określenie teoretycznych zasad zarządzania informacjami w systemie przeciwdziałania terroryzmowi, stanowiących podstawę budowy modelu systemu zarządzania informacjami o zagrożeniach;
   - przeprowadzenie badań nad istniejącymi systemami zarządzania informacjami w ramach systemu bezpieczeństwa antyterrorystycznego;
3. Określenie struktury modelu systemu zarządzania informacjami w państwie, umożliwiającego określenie, procedur i mechanizmów dystrybucji informacji (a tym samym koordynacji działań) mających istotne znaczenie dla efektywnego przeciwdziałania terroryzmowi:
   - wskazanie elementów systemu oraz procesów i relacji (stosunków i sprzężeń) wewnątrz systemu, które warunkują jego prawidłowe funkcjonowanie;
   - wskazanie relacji i uwarunkowań zewnętrznych systemu, takich jak ramy prawno – organizacyjne, niezbędnych dla prawidłowego funkcjonowania systemu.

Dla rozwiązania przedstawionych problemów badawczych, uwzględniając analizę krytyczną literatury przedmiotu oraz wstępną analizę porównawczą istniejących na świecie systemów zarządzania zasobami informacyjnymi w ramach systemów bezpieczeństwa antyterrorystycznego oraz własne doświadczenia zawodowe w obszarze przeciwdziałania terroryzmowi w warunkach RP, autor przyjął następujące hipotezy robocze:

I. Terroryzm stanowi jedno z najpoważniejszych zagrożeń asymetrycznych dla współczesnych państwa oraz dla ładu międzynarodowego;

II. Zwalczanie terroryzmu, w związku z dynamiką tego zjawiska, jest zadaniem szczególnie złożonym i trudnym, w jego realizacja uzależniona jest od stworzenia efektywnych, elastycznych i posiadających zdolności adaptacyjne, systemów przeciwdziałania temu zjawisku;

III. Współczesne systemy bezpieczeństwa, podobnie jak inne sfery życia społecznego i politycznego, nacechowane są silną zależnością od zdobywanych i przetwarzanych zasobów informacyjnych, a zatem stworzenie efektywnego systemu zdobywania, przetwarzania, przechowywania i dystrybucji informacji w ramach działań mających na celu przeciwdziałanie terroryzmowi, zwiększy bezpieczeństwo państwa, jego interesów i obywateli;

IV. W Polsce kształtuje się system przeciwdziałania terroryzmowi, jednak w chwili obecnej jego założenia nie uwzględniają w dostatecznym stopniu potrzeby i wymagania stworzenia efektywnie funkcjonującego systemu zarządzania zasobami informacyjnymi, spełniającego wymagania systemu przeciwdziałania terroryzmowi;

V. W ramach istniejącego systemu prawno – organizacyjnego możliwe jest dokonanie takich zmian, które umożliwią stworzenie i funkcjonowanie systemu zarządzania zasobami informacyjnymi;

VI. Możliwe jest określenie obszarów odpowiedzialności poszczególnych uczestników systemu przeciwdziałania terroryzmowi oraz dokonanie takiego podziału obszarów odpowiedzialności, który wyczerpie zadania, których wykonanie konieczne jest dla zapewnienia bezpieczeństwa i stabilności społecznej oraz politycznej państwa;

VII. Istniejące w innych państwach systemy zarządzania zasobami informacyjnymi zostały sprawdzone w podczas dotychczasowego funkcjonowania, zaś elementy ich struktury można uznać za efektywne;

VIII. Istnieje możliwość implementowania w systemie zarządzania zasobami informacyjnymi, odpowiedniego do polskich warunków prawno – organizacyjnych, elementów systemu zarządzania zasobami informacyjnymi, wykorzystywanych w innych państwach.

1.4 Metody i techniki badawcze

Współczesne społeczne badania systemowe aczkolwiek wywodzą się z cybernetyki i teorii systemów, to wchłonęły wiele obszarów tradycyjnej socjologii i politologii. Kluczową kategorią jest kategoria **systemu,** czyli takiego obiektu, który rozpatrywany jest jako **całość,** tworzoną przez zbiór **elementów** i **relacji** między nimi. Istotnym postulatem badań systemowych jest **holizm,** zakładający, że rzeczywistość postrzegana jest w sposób całościowy i że badanie całości ma sens. Nie oznacza to rezygnacji z ujęć tradycyjnych (tab. 1)[8].

Tab. 1: Różnice między ujęciem systemowym a ujęciem tradycyjnym

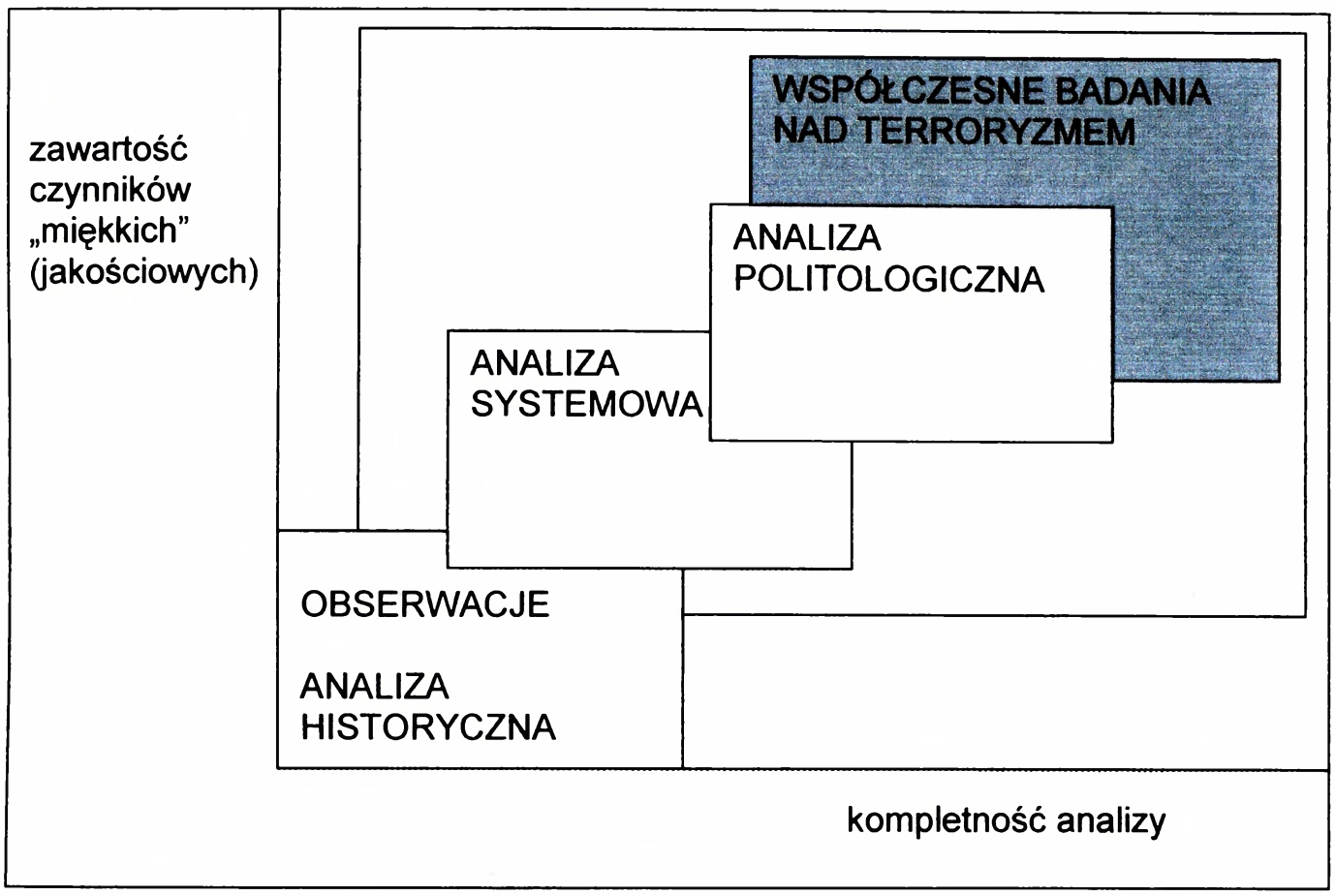
UJĘCIE ANALITYCZNE (REDUKCJONISTYCZNE)	UJĘCIE SYSTEMOWE
1. Wyodrębnienia: koncentruje się na elementach.	1. Łączy: koncentruje się na relacjach między elementami.
2. Bada charakter relacji.	2. Bada efekty relacji.
3. Opiera się na danych szczegółowych.	3. Opiera się na ogólnym modelu.
4. Modyfikuje precyzyjne i szczegółowe, ale trudne do zastosowania parametry.	4. Modyfikuje grupy parametrów.
5. Uwzględnia oddziaływania liniowe i słabe.	5. Modele ogólne, ale dające się wykorzystywać przy podejmowaniu decyzji.
6. Znajomość szczegółów, cele słabo określone.	6. Uwzględnia oddziaływania nieliniowe i silne.
7. Prowadzi do działania „zalgorytmizowanego".	7. Znajomość celów, szczegóły płynne.
8. Prowadzi do nauczania „monodyscyplinarnego".	8. Prowadzi do działania celowego.
	9. Prowadzi do nauczania „multi- i interdyscyplinarnego".

Źródło: Sienkiewicz P., Świeboda H., *Metodologia badań nad bezpieczeństwem*, AON, Warszawa 2008.

Badanie sytuacji zagrożeń terrorystycznych charakteryzujących się niepewnością i ryzykiem, a w szczególności wywołanych przez nie sytuacji kryzysowych i konfliktowych odbywało się w ostatnim półwieczu na różnych poziomach ogólności

[8] Sienkiewicz P., Świeboda H., *Perspektywy badań systemowych nad bezpieczeństwem*. Międzynarodowa Konferencja naukowa nt. Bezpieczeństwo. Wymiar współczesny oraz perspektywy badań. Kraków 2008.

(i konkretności). Dominowały analizy historyczne, socjologiczne, psychologiczne, politologiczne itp., lecz brakowało jednolitej platformy metodologicznej. Nadzieje wiązane są z metodologią badań systemowych, a w szczególności z analizą systemową (w ujęciu RAND Corporation).



Rys. 4: Metody badań nad terroryzmem
Źródło: na podstawie Sienkiewicz P., *Metodologia badań nad bezpieczeństwem* [w:] *Wybrane metody badań nad obronnością,* AON, Warszawa 2008, s. 36.

Grupa problemów związanych z terroryzmem i przeciwdziałaniem zagrożeniom terrorystycznym jest bezpośrednio warunkowana wzrastającą złożonością, swoistym splątaniem różnych podmiotów dążących do często bardzo różnych celów. Analiza politologiczna, której przedmiotem jest bezpieczeństwo narodowe (międzynarodowe), korzysta na przykład z modeli gier i symulacji komputerowej, metod analizy ryzyka, techniki scenariuszy itp. – twórczo rozwijanych w ramach badań operacyjnych i analizy systemowej. Podobne zależności i wpływy bez trudu można dostrzec anali-

zując współczesne badania nas bezpieczeństwem ekonomicznym, biznesowym, ekologicznym itp.[9]

Założenia i ograniczenia:

Podstawę metodologiczną badań systemowych stanowią następujące zasady:[10]

1. Badane są pewne zorganizowane całości, dobrze wyodrębnione ze środowiska (otoczenia). Całości te określane są jako systemy.
2. System może być podzielony na części (podsystemy) i ich relacje na wiele różnych sposobów; nie ma podziału uniwersalnego.
3. Każdy podział systemu na części daje pewien jego obraz. Podział zależy więc od tego, które cechy systemu lub jego elementy stanowią przedmiot badań.
4. Własności składników systemu nie mogą być badane niezależnie od systemu, w którym występują. Nie ma własności niezależnych od środowiska (otoczenia). Nie ma stałego i niezależnego od kryterium analizy podziału na system i otoczenie.

Stosowanie zasad metodologicznych pozwala na wyodrębnienie systemu według założeń:

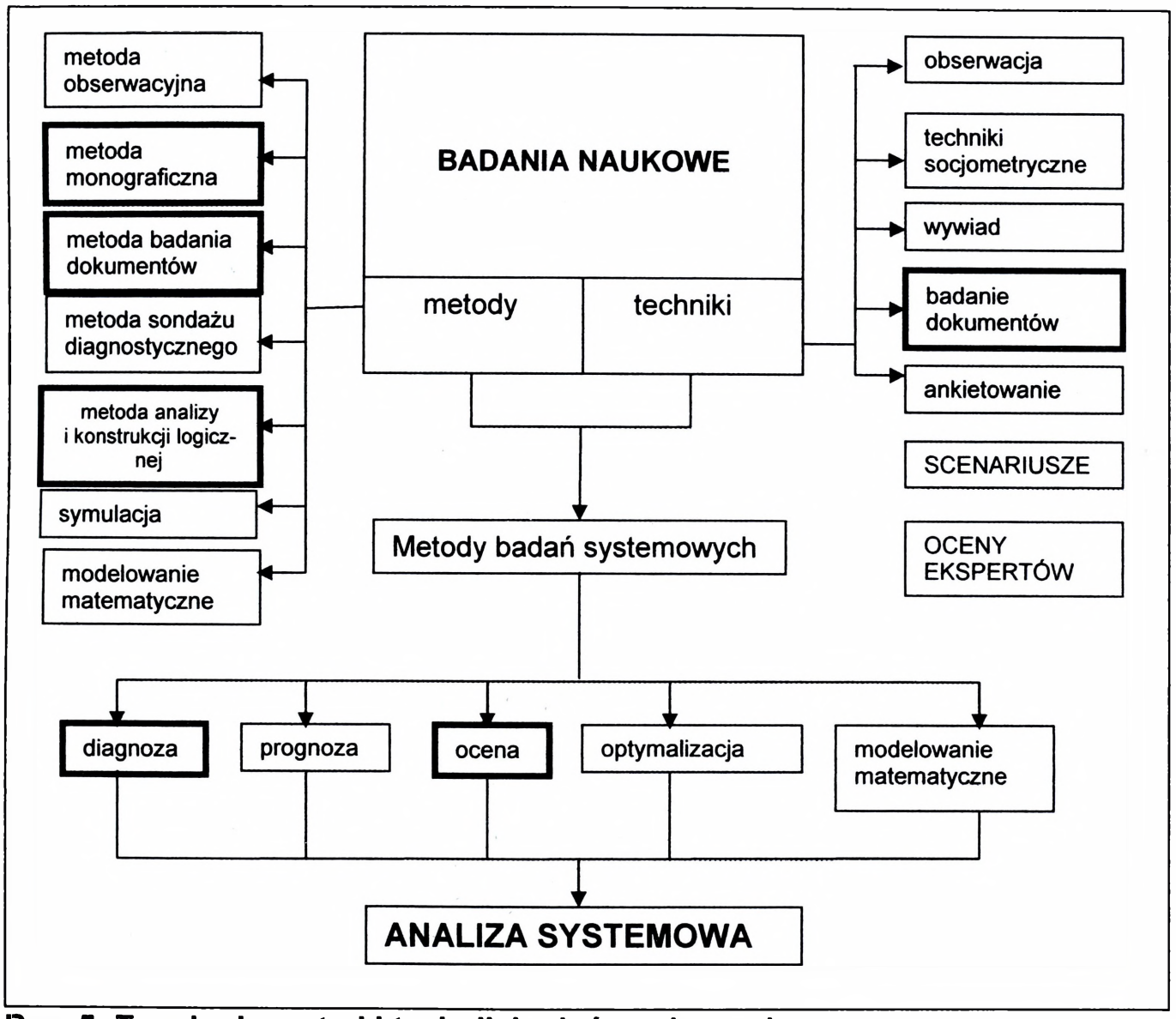
1. Zasada ścisłości określania granic systemu i jego otoczenia;
2. zasada niezmienności dokonanego rozróżnienia między systemem a jego otoczeniem w trakcie badań;
3. zasada zupełności podziału systemu (na podsystemy);
4. zasada rozłączności rozpatrywanych systemów (i ich podsystemów);
5. zasad funkcjonalności, czyli podziału systemu na podsystemy ze względu na rodzaj spełnianych przez nie funkcji w całości.

Zaletą zastosowania analizy systemowej jest wprowadzenie znacznej dozy obiektywizmu do badania procesu bezpieczeństwa informacyjnego, który jest w znacznej mierze subiektywny, uwzględnianie szerszego kontekstu badań, a także uwzględnienie czynnika niepewności i ryzyka. Ponadto analiza systemowa pozwala skoncentrować uwagę na skutkach działania, co może sprzyjać ujawnieniu nieprzewidzianych następstw analizowanego zagrożenia.

---

[9] Sienkiewicz P., Świeboda H., *Wybrane metody badań naukowych nad bezpieczeństwem i obronnością*, AON Warszawa 2008, s. 37.
[10] Sienkiewicz P., *Analiza systemowa*, Bellona, Warszawa 1995, s. 22.

Złożoność i obszerność badań wymagała zastosowania analizy systemowej jako „meta-metody" spinającej poszczególne etapy badań. Przyjęto, że analiza systemowa jest zbiorem metod i technik analitycznych, ocenowych i decyzyjnych, służących racjonalnemu rozwiązywaniu sytuacji decyzyjnych, przede wszystkim w warunkach niepewności i ryzyka. Dlatego, dla zrealizowania głównego celu badawczego, przyjęto następujący schemat postępowania:



Rys. 5: Typologia metod i technik badań naukowych
Źródło: Sienkiewicz P. (red.), *Metodologia badań systemowych nad bezpieczeństwem i obronnością*, AON Warszawa 2009 (w przygotowaniu).

Wśród metod i technik badawczych zastosowanych podczas rozwiązywania problemów badawczych znalazły się przede wszystkim następujące:

1. **analiza** – wykorzystana w części pierwszej, drugiej i trzeciej zasadniczej, odpowiednio w celu:

- w celu analitycznego przedstawienia prawnych podstaw funkcjonowania współczesnych systemów przeciwdziałania terroryzmowi na przykładzie systemu prawnego USA,
- podczas prezentowania szczególnych rozwiązań narodowych w odniesieniu do systemów przeciwdziałania terroryzmowi, dla zobrazowania całości mechanizmów systemów przeciwdziałania terroryzmowi oraz wykorzystywanych w nich i tworzonych przez nie współzależności i metod współpracy,
- ukierunkowana na przedstawienie procesów decyzyjnych niezbędnych w systemie przeciwdziałania terroryzmowi, dla których niezbędne jest sprawne funkcjonowanie systemu zarządzania zasobami informacyjnymi w systemie przeciwdziałania terroryzmowi;

2. **metoda porównawcza (analogii)** – zastosowana przede wszystkim w czwartej części pracy, w celu przedstawienia funkcjonujących na świecie systemów obiegu informacji w systemach przeciwdziałania terroryzmowi (na przykładzie czterech państw);
3. **analiza i krytyka piśmiennictwa oraz opracowań naukowych dotyczących zakresu badań** – przede wszystkim w pierwszej i drugiej części pracy, dotyczących kwestii definiowania terroryzmu oraz roli zasobów informacyjnych w systemie przeciwdziałania terroryzmowi ze względu na konieczność zaprezentowania dotychczasowego dorobku nauki w zakresie badań nad informacją, społeczeństwem informacyjnym oraz szeroko pojętymi systemami przeciwdziałania terroryzmowi;
4. **modelowanie systemowe** – w części trzeciej zasadniczej, wykorzystane w procesie tworzenia modelu zarządzania zasobami informacyjnymi w systemie przeciwdziałania terroryzmowi;
5. **obserwacja uczestnicząca** – wykorzystana głównie dla celów części drugiej zasadniczej podczas badań nad systemami obiegu informacji w systemach przeciwdziałania terroryzmowi na świecie;
6. **wywiady** – wykorzystane głównie dla celów części drugiej zasadniczej podczas pogłębionych badań nad systemami obiegu informacji w systemach przeciwdziałania terroryzmowi na świecie.

1.5 Ocena piśmiennictwa

Literatura, poruszająca zagadnienia związane z przedmiotem rozprawy jest bardzo szeroka. Wśród dotychczas opublikowanych opracowań znaleźć można wiele cennych pozycji w obszarach, których dotyczą tematyki niniejszej pracy. Warto przy tym jednak zauważyć, iż brak jest opracowań zwartych bezpośrednio dotyczących tematu niniejszej rozprawy.

Poszczególne obszary badań zostały przedstawione w licznych pozycjach, które na potrzeby rozprawy podzielić można na kilka grup:

I. prace dotyczące zagadnień z zakresu badań systemowych, w szczególności analizy systemowej zarówno Polsce, jak i na świecie, wśród których odnotować warto prace. Piotra Sienkiewicza, E.S. Quade'a, Hermana Kahna, Irwina Manna i Wayne'a I. Bouchera[11],

II. prace dotyczące bezpieczeństwa narodowego i międzynarodowego, wśród których na szczególną uwagę zasługują prace Stanisława Kozieja, Ryszarda Zięby, Marka Madeja, Jarosława Gryza, Tadeusza Jemioło, Kazimierza Malaka, Józefa Flisa, Ryszarda Jakubczaka, Jacka Pawłowskiego[12],

III. prace dotyczące terroryzmu i jego zwalczania, wśród których wymienić należy przede wszystkim takich autorów, jak: Kuba Jałoszyński, Bartosz Bolechów, Robert Borkowski, Bruce Hoffman, Katarzyna Maniszewska[13];

---

[11] Sienkiewicz Piotr, *10 wykładów*, AON, Warszawa 2005; Sienkiewicz Piotr, *Analiza systemowa,* Warszawa 1995; *Techniques of Systems Analysis*, Herman Kahn, Irwin Mann, Rand 1956; *Systems Analysis and Policy Planning. Applications in Defense*, E. S. Quade and Wayne I. Boucher (ed.), Rand 1968; *Some Problems Associated with Systems Analysis*, E. S. Quade, Rand 2003.

[12] Koziej Stanisław, *Bezpieczeństwo narodowe i obronność Rzeczypospolitej Polskiej*, Wyd. Adam Marszałek, Toruń 1996; Koziej Stanisław, *Między piekłem a rajem: szare bezpieczeństwo na progu XXI wieku*, Wydaw. Adam Marszałek, Toruń 2006; Zięba Ryszard, *Instytucjonalizacja bezpieczeństwa europejskiego*, Wydawnictwo Naukowe Scholar; Warszawa 2004; Madej Marek, *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Polski Instytut Spraw Międzynarodowych, Warszawa 2007; Gryz Jarosław, *System zarządzania kryzysowego*, Wyd. Adam Marszałek, Toruń 2007; Jemioło Tadeusz, Malak Kazimierz, *Bezpieczeństwo zewnętrzne Rzeczypospolitej Polskiej*, AON Warszawa 2002; Jakubczak Ryszard, Flis Józef, *Bezpieczeństwo narodowe Polski w XXI wieku*, Bellona, Warszawa 2006; Pawłowski Jacek, *Strategiczne problemy i dylematy we współczesnym świecie*, Wyd. Adam Marszałek, Toruń 2004.

[13] Jałoszyński Kuba, *Współczesny wymiar antyterroryzmu*, Wydawnicwto TRIO, Warszawa 2008; Jałoszyński Kuba, *Koncepcja współczesnych działań antyterrorystycznych*, Akademia Obrony Narodowej, Warszawa 2003; Bolechów Bartosz, *Terroryzm w świecie podwubiegunowym*, Wydawnictwo Adam Marszałek; Toruń 2004; Borkowski Robert, *Terroryzm ponowoczesny. Studium z antropologii polityki*, Wydawnictwo Adam Marszałek; Toruń 2006; Hoffman Bruce, *Oblicza terroryzmu*, Politeja, Warszawa 1999; Maniszewska Katarzyna, *Terroryzm a media*, ATUT, Wrocław 2006.

IV. prace z zakresu badań nad społeczeństwem informacyjnym i rolą informacji we współczesnym świecie Piotra Sienkiewicza, Tomasza Goban-Klasa, Kazimierza Krzysztofka, Lecha Zachera, Lesława Habera[14],

V. prace poruszające zagadnienia związane z bezpieczeństwem informacyjnym i walką informacyjną autorstwa Andrzeja Białasa, Józefa Janczaka, Grzegorza Świdzikowskiego, Romana Kwećki, Anne Aldis[15].

Szczególnie istotne w kontekście omawiania wcześniejszego piśmiennictwa nadmienienie, iż bogate zasoby informacji nt. terroryzmu, systemów przeciwdziałania mu, baz danych dotyczących ataków terrorystycznych oraz ich konsekwencji odnaleźć można w zasobach Internetu.

1.6 Obszar i organizacja badań

Badania, których prowadzenie konieczne było ze względu na cel pracy oraz sformułowane problemy badawcze, przeprowadzone zostały z uwzględnieniem istniejących podstaw teorii informacji, zarządzania zasobami informacyjnymi oraz teorii zagrożeń terrorystycznych.

Wymienione obszary badawcze poddane zostały badaniom w formie zintegrowanej w momencie prowadzenia badań empirycznych nad istniejącymi systemami zarządzania informacjami w systemach przeciwdziałania terroryzmowi w USA, Francji, Wielkiej Brytanii oraz w Niemczech.

---

[14] Goban-Klas Tomasz, Sienkiewicz Piotr, *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999; Sienkiewicz Piotr, Wieleba Ryszard, Wocial Janusz, Kuca Marceli, Skoczylas Magdalena, *Wartość informacji w dowodzeniu i zarządzaniu. Metodologia analizy potrzeb informacyjnych*, AON, Warszawa 2002; Sienkiewicz Piotr, *Systemy kierowania*, Wiedza Powszechna, Warszawa 1989; Zacher Lech, *Transformacje społeczeństw od informacji do wiedzy*. C.H. Beck, Warszawa, 2007; *Społeczeństwo sieci*. Wyd. Naukowe PWN, Warszawa, 2007; McLuhan Marshall, *Zrozumieć media*. WNT, Warszawa, 2004; *Zagrożenia asymetryczne bezpieczeństwa państwa obszaru transatlantyckiego*. Wyd. PISM, Warszawa, 2007; Haber Lesław *Społeczeństwo informacyjne. Wizja czy rzeczywistość?* (red), wyd. Uczelniane Wydawnictwa Naukowo–Dydaktyczne, Kraków, 2004; Haber L., *Od robotnika do internauty – w kierunku społeczeństwa informacyjnego*. AGH, Kraków, 2008; Goban-Klas T., *Media i komunikowanie masowe – teoria i analizy prasy, radia, telewizji i Internetu*. Warszawa, 2004.

[15] Kwećka Roman, *Informacja w walce zbrojnej*, AON, Warszawa 2001; Białas Andrzej, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wyd. Naukowo-Techniczne, Warszawa 2006; Aldiss Anne, Herd Greame P. (ed.), *The Ideological War on Terror. Worldwide strategies for counter-terrorism*, Routledge, London and New York 2007; Białas Andrzej, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wyd. Naukowo-Techniczne, Warszawa 2006; Janczak Józef, Świdzikowski Grzegorz, *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*, AON - Warszawa 2004.

Badania dotyczące poszczególnych problemów badawczych przeprowadzone zostały w kilku etapach:

- **etap badań wstępnych:** poświęcony weryfikacji problemów badawczych oraz metod i technik badawczych;
- **etap badań podstawowych**: poświęcony przeprowadzeniu analizy krytycznej dotychczasowego piśmiennictwa, zarówno w zakresie teorii zarządzania zasobami informacyjnymi, jak i badań nad terroryzmem i implikacjami, jakie wynikają z tego zagrożenia dla poszczególnych państw oraz społeczności międzynarodowej;
- **etap badań empirycznych:** poświęcony dokładnemu zbadaniu istniejących systemów zarządzania zasobami informacyjnymi w 4 wybranych państwach;
- **etap konstruowania modelu systemu zarządzania zasobami informacyjnymi**: podczas którego wytworzona została propozycja takiego modelu, dostosowana do warunków Polskich.

Konsekwencją przedstawionych ustaleń, założeń i ograniczeń jest ostateczna procedura badawcza, przedstawiona w postaci modelu procesu badań (tab. 2).

Tab. 2: Etapy realizacji badań

I etap badań: „diagnoza wstępna"

(1) ANALIZA AKTÓW PRAWNYCH
dotyczących zagrożeń terrorystycznych

(2) ANALIZA DZIAŁALNOŚCI ORGANIZACJI
zajmujących się przeciwdziałaniem terroryzmowi

(3) ANALIZA DOSTĘPNYCH DANYCH STATYSTYCZNYCH
dotyczących zagrożeń terrorystycznych

(4) ANALIZA DOROBKU NAUKOWEGO Z ZAKRESU BEZPIECZEŃSTWA NARODOWEGO
dotyczącego metod analizy i przewidywania zagrożeń terrorystycznych

↓

II etap badań: „analiza terroryzmu"

(5) Charakterystyka zjawiska
definiowanie i klasyfikacje terroryzmu, systemy przeciwdziałania – aspekty informacyjne

↓

III etap badań: „analiza istniejących systemów zarządzania informacjami"

(6) analiza cech strukturalnych i funkcjonalnych

(7) wnioski i założenia dla modelu systemu

↓

IV etap badań: „weryfikacja badań"

(8) opracowanie modelu systemu zarządzania informacjami o zagrożeniach terrorystycznych na potrzeby systemu przeciwdziałania terroryzmowi RP

↓

V etap badań: „prezentacja wyników badań"

(9) UPOWSZECHNIENIE WYNIKÓW I WNIOSKÓW
z wszystkich etapów analiz i badań przez: (1) konferencje, (2) publikacje obejmujące: identyfikację zagrożeń terrorystycznych, zarządzania bezpieczeństwem narodowym, przeciwdziałania terroryzmowi, zarządzania informacjami

(10) OPRACOWANIE DYSERTACJI WRAZ Z REKOMENDACJAMI
dla projektów systemu zarządzania informacjami o zagrożeniach terrorystycznych

Źródło: opracowanie własne.

Badania empiryczne prowadzone były:

- podczas pracy autora w sektorach administracji publicznej, właściwych ds. bezpieczeństwa, szczególnie w okresie kierowania wydziałem ds. przeciwdziałania zagrożeniom terrorystycznych w Ministerstwie Spraw Wewnętrznych i Administracji oraz kierowania zespołami zadaniowymi Międzyresortowego Centrum ds. Zwalczania Przestępczości Zorganizowanej i Międzynarodowego Terroryzmu:
    - zespołem zadaniowym do stworzenia podstaw prawnych działania Krajowego Koordynatora do Spraw Przeciwdziałania Terroryzmowi,
    - zespołem zadaniowym do spraw koordynacji współpracy w przeciwdziałaniu terroryzmowi;
- w toku wizyt studyjnych poza granicami kraju w instytucjach właściwych do przeciwdziałania terroryzmowi (w tym w Centrum Badań nad Terroryzmem RAND Corporation w Santa Monica);
- podczas kierowania Studiami Podyplomowymi w Zakresie Analizy Bezpieczeństwa i Zagrożeń Terrorystycznych w Collegium Civitas oraz wykładów na Studiach Podyplomowych w zakresie bezpieczeństwa informacyjnego w Akademii Obrony Narodowej.

Zakłada się, że w rezultacie prezentowanych badań wykazana została potrzeba stworzenia systemu zarządzania zasobami informacyjnymi w systemie bezpieczeństwa antyterrorystycznego państwa oraz nakreślony został kształt modelu takiego systemu. Wyniki badań, zarówno teoretycznych, jak i empirycznych, odzwierciedlone są w kolejnych częściach pracy.

Rozdział 2

Terroryzm – charakterystyka zjawiska i jego zwalczania

2.1 Charakterystyka zjawiska terroryzmu

Po zakończeniu zimnej wojny jednym z najważniejszych zadań, jakie stały przed polskimi władzami było wyrwanie państwa z szarej strefy bezpieczeństwa i zakotwiczenie jego polityki bezpieczeństwa w strukturach systemu zachodnich sojuszy i organizacji międzynarodowych. Wraz z wstąpieniem Polski do NATO w roku 1999, zabezpieczone zostało międzynarodowe wsparcie dla Polski na wypadek konfliktu o charakterze militarnym. Wydawać by się mogło, że zakończenie zimnej wojny i udział, jaki w tym miała ekonomiczna porażka bloku wschodniego, pozwoli na względnie spokojne funkcjonowanie społeczności międzynarodowej przez co najmniej kilka dekad. Jak się jednak okazało, wyeliminowanie konfliktów międzypaństwowych to za mało, aby zagwarantować międzynarodowy pokój i bezpieczeństwo.

Najpoważniejszą kategorią zagrożeń, które pojawiły się po zakończeniu zimnej wojny, są zagrożenia asymetryczne. Ta kategoria zagrożeń jest definiowana jako zagrożenia, których celem jest neutralizacja lub likwidacja przewagi przeciwnika przez stosowanie taktyki i dostępnej broni w niekonwencjonalny sposób, pozwalający na wykorzystanie zarówno słabych punktów przeciwnika, jak i własnej przewagi w jakimś elemencie prowadzonej operacji: *na skutek dysproporcji potencjałów militarnych i innego rodzaju zasobów oraz (albo) odmienności kulturowych między przeciwnikami decyduje się na wybór asymetrycznych strategii i metod prowadzenia konfliktu. [...] Strategie asymetryczne (sposoby prowadzenia konfliktu) pojmuje się zaś zazwyczaj jako polegające na wykorzystywaniu w działaniach istniejących między stronami odmienności poprzez stosowanie metod, środków i taktyk niekonwencjonalnych z punktu widzenia przeciwnika, przy czym pojęcie „asymetryczność" odnosi się do aktywności słabszej strony układu.*[16]

Jest to taktyka działania, która umożliwia realne uderzenie skierowane przez słabych przeciwko silnym, przez podmioty pozapaństwowe w państwa. Dlatego właśnie historia nie skończyła się – i nieprędko się skończy. W momencie, w którym zni-

[16] Madej M., *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Warszawa 2007, przypis 74 na stronie 44.

ka jedno zagrożenie, pojawia się inne, wypełniające próżnię. Zagrożenia asymetryczne są nowym zjawiskiem, które zajęło miejsce potencjalnego konfliktu międzypaństwowego.

2.1.1 Geneza terroryzmu

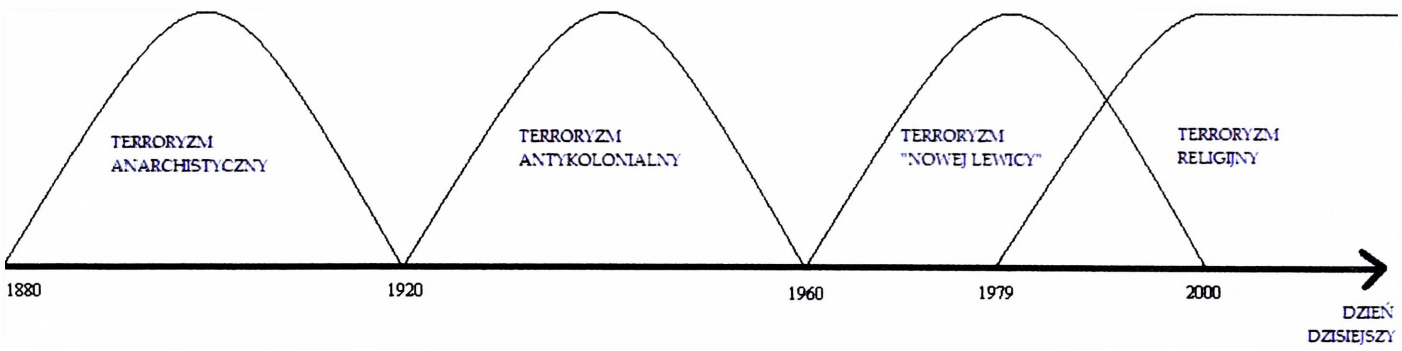
Wśród najpoważniejszych zagrożeń asymetrycznych, jak wskazują wydarzenia ostatnich lat (m.in.: atak na World Trade Center 11 września 2001 r., ataki na pociągi podmiejskie w Madrycie 11 marca 2004 r., ataki na londyńskie metro i transport naziemny 7 i 11 lipca 2005 r. oraz udaremnione zamachy, których celem miały być transatlantyckie loty z Wielkiej Brytanii do USA, ujawnione w sierpniu 2006 r.), wokół którego wciąż toczą się debaty medialne, polityczne, społeczne i etyczne, jest terroryzm.

Zjawisko to, którego nazwa pochodzi od łac. *terror*, czyli strach, ma bardzo długą historię i korzenie sięgające głęboko w przeszłość. Odróżnić przy tym należy dwie kwestie: pierwsza z nich to istota terroryzmu, jako zjawiska politycznego, obecnego w politycznej i społeczne rzeczywistości większości współczesnych państw. Druga z nich, to istota terroryzmu, jako metody działania opartej na zastraszaniu, która jest uniwersalnym narzędziem wszystkich, którzy dążą do osiągnięcia swoich celów w drodze wymuszania na innych podmiotach określonych zachowań. Ten drugi rodzaj terroru towarzyszy ludzkości od zawsze: groźba silniejszego oparta na posiadanych przez niego narzędziach pozostaje narzędziem wpływu, któremu poddają się jednostki, grupy społeczne i całe narody. Skuteczność tej metody zrodziła terroryzm polityczny takim, jakim znamy go dzisiaj – poprzez wszystkie etapy jego powstawania i kolejne fale terroryzmu, który z powodzeniem stosowali rosyjscy anarchiści w XIX w., skrajna lewica, skrajna prawica, a który dziś stosują ekstremiści religijni.

David C. Rapoport proponuje wskazanie 4 fal terroryzmu.[17] Pierwszą z nich był terroryzm anarchistów rosyjskich, przez nich samych określany mianem „propagandy czynu", który rozwinął się w XIX w. Kolejna fala terroryzmu, terroryzm antykolonialny, wiązał się z demokratyzacją stosunków międzynarodowych i dążeniem kolonii do uniezależnienia się od metropolii. Terroryzm lewacki, określany angielskim mianem

[17] Rapoport, David C., *The Four Waves of Modern Terrorism* [w:] Cronin, Audrey Kurth, Ludes James M. (red.), *Attacking Terrorism. Elements of a GRAND Strategy,* Georgetown UP., Washington, D.C. 2004, s. 46-73.

„new left terrorism", czyli terroryzm nowej lewicy był już wyrazem dążeń o charakterze społecznym, a nie narodowościowym. Fala terroryzmu, z którą mamy do czynienia obecnie, to fala terroryzmu religijnego. Podstawowym dążeniem tej generacji ugrupowań terrorystycznych jest doprowadzenie do zaistnienia – jako celu ostatecznego – globalnego kalifatu, państwa bożego na ziemi, które rządzić się będzie prawem opartym na zasadach religii jako podstawie współżycia społecznego.



Rys. 6: Model 4 fal terroryzmu
Źródło: David C. Rapoport, *The Four Waves of Modern Terrorism,* Washington, D.C. 2004.

Kolejne fale terroryzmu miały jedną wspólną cechę: stosowanie przemocy lub groźby użycia przemocy dla realizacji założonych celów politycznych. Różniły je jednak zarówno cele polityczne, jakie zakładały, stosowane metody ataków, a także wybór tych celów.

Tab. 3: 4 fale terroryzmu według Davida C. Rapoporta

Fala terroryzmu	Ideologia	Cele ataków	Metody ataków
Terroryzm anarchistyczny	Wyeliminowanie rządów, przebudzenie mas, doprowadzenie do demokratyzacji życia społecznego i politycznego	Wybrane jednostki, przedstawiciele władzy	Zamachy z użyciem broni palnej, podkładanie ładunków wybuchowych
Terroryzm antykolonialny	Uzyskanie prawa narodów do samostanowienia, bunt przeciwko metropoliom	Przedstawiciele administracji (policja, sądownictwo, administracja) w celu sprawienia, że koszt utrzymywania kolonii będzie wyższy niż zyski	Zamachy z użyciem broni palnej, podkładanie ładunków wybuchowych
Terroryzm „nowe lewicy"	Demokratyzacja życia społecznego i politycznego, ideologia napędzana wojną w Wietnamie i skuteczny opór Wietkongu	Przedstawiciele władzy i establishmentu, ograniczone ataki na osoby postronne	Branie zakładników, podkładanie ładunków wybuchowych, porwania samolotów, zamachy na przedstawicieli władzy i establishmentu
Terroryzm religijny	Utworzenie światowego kalifatu (w wypadku terroryzmu islamistycznego, dominującego współcześnie zagrożenia), wprowadzenie na świecie rządów szari'atu	Wszyscy członkowie atakowanych społeczeństw, zgodnie z przekonaniem, że winą jest bycie częścią grzesznego kręgu kulturowo – społecznego: dążenie do powodowania ofiar masowych	Zamachy na cele miękkie (podkładanie ładunków wybuchowych itp.), superterroryzm (w założeniu: użycie broni chemicznej, atomowej, radiologicznej i biologicznej), cyberterroryzm

Źródło: opracowanie własne.

Jako metoda działania, dostosować się terroryzm może do potrzeb każdej niemal ideologii, którą jej zwolennicy postanowią promować z użyciem takich metod, jak metody terrorystyczne. Wyraźnie widać to na przykładzie zjawiska, które badacze określają mianem terroryzmu „jednej sprawy", a więc na przykład ekoterroryzmu. Nietrudno wyobrazić sobie, jakie zagrożenie przyniesie ze sobą popularyzacja terroryzmu jako metody walki – nie brak we współczesnych państwa i współczesnych stosunkach międzynarodowych radykalnych grup, które mogą okazać się skłonne do stosowania przemocy w imię wyznawanych przez siebie zasad i stawianych sobie celów. Wiele wielkich ideologii, szczególnie tych, które stawiały sobie za cel zmianę

obowiązującego porządku społecznego w imię tak zwanego „wyższego dobra", okazywało się aż nadto skłonnymi do uznawania, że cel uświęca środki[18].

Stąd zresztą pochodzi najważniejsze zagrożenie, jakie stanowi terroryzm – jeśli państwa szybko nie zdołają wypracować mechanizmów skutecznego przeciwdziałania temu zjawisku, będzie ono rozprzestrzeniać się coraz bardziej, stając się narzędziem w rękach kolejnych zradykalizowanych grup nacisku, które do realizacji swoich celów nie wahają się użyć przemocy. Terroryzm, jako narzędzie realizacji celów politycznych charakteryzuje się przede wszystkim zdolnością do dostosowywania się do nowych warunków oraz omijania nowych systemów bezpieczeństwa, tworzonych przez państwa.

Jest zatem przeciwdziałanie terroryzmowi nie tylko działaniem o charakterze doraźnym – bez budowania skutecznych mechanizmów i systemów przeciwdziałania terroryzmowi żadne z współczesnych państw nie będzie mogło być pewne, że nie znajdzie się nowe ugrupowanie, frakcja bądź organizacja, które uzna, że narzędzie skuteczne – bo takim będzie terroryzm, o ile nie zostaną zbudowane skuteczne strategie przeciwdziałania mu – jest najlepszym i najbardziej wydajnym sposobem osiągnięcia celu.

2.1.2 Definiowanie i klasyfikacje terroryzmu

Organizacje terrorystyczne i ich członkowie poprzez stosowane przez nich narzędzia tego, co uważane jest przez nich za walkę polityczną, pozostają na marginesie współczesnych społeczeństw. Czyny o charakterze terrorystycznym to, po odjęciu od nich motywacji ideologicznej, politycznej czy religijnej, poważane przestępstwa, a nawet zbrodnie. Zabójstwa, podkładanie ładunków wybuchowych, czerpanie środków finansowych z działalności takiej, jak handel narkotykami, bronią lub handel ludźmi, które są integralnymi częściami działalności większości organizacji terrorystycznych, to czyny, które potępiane i karane są w niemal wszystkich porządkach prawnych. Terroryści nie przestrzegają w swojej walce żadnych zasad – nawet tych, które dotyczą prowadzenia walki zbrojnej. Ich ofiarami przecież w przeważającej większości nie są przedstawiciele – oficjalni – państw, przeciwko którym występują, nie atakują oni

[18] Patrz także: Posłuszna E., *Terroryzm w obronie praw zwierząt – źródła inspiracji* [w:] Liedel K., (red.), *Terroryzm – anatomia zjawiska*, Warszawa 2006, s. 146 i dalsze.

jedynie funkcjonariuszy służb, wojskowych czy choćby urzędników. Uderzają przede wszystkim w cywili, niewinne ofiary walki, która ich bezpośrednio nie dotyczy.

Terroryzm jest zjawiskiem, którego jedną z najważniejszych cech są dalekosiężne skutki psychologiczne. Jak pisze jeden z najważniejszych badaczy terroryzmu współczesności, Brian Michael Jenkins, terroryzm do teatr – skierowany nie jest do jego bezpośrednich ofiar, a do tych, którzy patrzą.[19] Ten aspekt terroryzmu jest niezmiernie istotny w kontekście założeń i badań prowadzonych na potrzeby niniejszej pracy – terroryzm bez informacji i jej rozprzestrzeniania jest metodą walki, która zasadniczo jest nieefektywna.

Od lipca 1968 r. kiedy to grupa terrorystów związana z ugrupowaniem Baader-Meinhoff porwała samolot linii El-Al lecący z Rzymu do Tel-Avivu, żądając w zamien za uwolnienie zakładników uwolnienia terrorystów powiązanych z Organizacją wyzwolenia Palestyny oraz członków grupy Baader-Meinhoff, terroryzm stał się zjawiskiem integralnie powiązanym z globalnym obiegiem informacji. 22 lipca 1968 r. jest datą, która dała początek nowej rozgrywce, jeśli chodzi o metodologię terroryzmu: zglobalizowała obszar działań terrorystów. Okazało się, że w dobie globalnych mediów globalny może stać się również szantaż ugrupowań terrorystycznych: można porwać samolot na jednym końcu świata, aby szantażować rząd państwa znajdującego się na drugim końcu świata. Media zapewnią bowiem nie tylko przekazanie rządów terrorystów właściwemu odbiorcy, ale także przekażą społeczeństwu komunikat na temat tego, że terroryści postawili rządowi takie, a nie inne warunki – i jakie mają argumenty, aby domagać się ich wypełnienia.

John Horgan w swojej pracy *Psychologia terroryzmu* pisze, iż terroryzm może zostać zdefiniowany jako odrębna forma wojny psychologicznej[20]. Posługuje się przy tym argumentem związanym z tą częścią definicji terroryzmu, która mówi, że celem sprawców jest wywołanie lęku i dalekosiężnych skutków psychologicznych. Argumentuje zatem, iż „przemożny lęk" jest terminem klinicznym, definiowanym jako stan ciągłego przerażenia lub odczuwania lęku, związanego z bardzo wysokim poziomem pobudzenia psychofizjologicznego. Zauważa przy tym, że wywołanie w społeczeństwie takiego właśnie stanu ma kluczowe znaczenie dla celów, które chcą osiągnąć

[19] Jenkins B.M., *International Terrorism: A New Mode of Conflict* [w:] Carlton D., Schaerf C. (red.), *International Terrorism and World Security*, London 1976, cyt. za.: Hoffman B., *Oblicza terroryzmu*, Warszawa 1999, s. 126.
[20] Horgan J., *Psychologia terroryzmu*, PWN, Warszawa 2008, s. 34.

terroryści. Wywołanie przerażenia w dużych grupach społecznych ma w dalszej perspektywie służyć stworzeniu odpowiednich warunków do wywołania zmian politycznych, które są bezpośrednim celem terrorystów. Horgan podkreśla również, że stan ten może być zwiększony przez uwagę, jaką zagrożeniu bądź konkretnemu zajściu poświęcają media[21].

Czym zatem jest terroryzm, który zagraża współczesnym państwom? Otóż przede wszystkim, jest metodą działania. Narzędziem, które stosowane konsekwentnie i efektywnie, pozwala jednostkom i grupom nadawać określony charakter przebiegowi wydarzeń w stosunkach międzynarodowych. Terroryzmem jest, według najbardziej ogólnej jego definicji, każde działanie, które polega na użyciu siły bądź groźby użycia siły (w stosunku do osób lub obiektów cywilnych) dla wymuszenia jakiegoś działania bądź zaniechania działania w celu politycznym. Nie posiada zatem własnej tożsamości – niczego, z wyjątkiem skłonności do stosowania przemocy w imię realizacji politycznych celów. Potrafi przystosować się dla każdej sprawy, mogą wykorzystać go zwolennicy każdej ideologii i zwolennicy każdego poglądu – o ile tylko zdecydują się na promowanie swojej prawdy na drodze przemocy i groźby użycia przemocy.

Dlatego warto, zamiast poświęcać uwagę poszczególnym definicjom terroryzmu, których sformułowano już setki, zrozumieć jego istotę. Metoda takiego definiowania terroryzmu oprzeć się może na dwóch – zasadniczo – podstawach. Pierwsza z nich, to metoda wymieniania elementów składowych, które pojawiają się statystycznie najczęściej w definicjach terroryzmu. Badania nad częstotliwością pojawiania się takich zjawisk, traktowanych jako przynależne przejawom terroryzmu, prowadzone były przez wielu badaczy. Wśród nich wymienić można szczególnie Alexa Schmidta[22]. Wymienia on takie zidentyfikowane zjawiska powiązane z terroryzmem, jak:

- stosowanie przemocy, siły lub groźby ich użycia,
- polityczna motywacja sprawców,
- działanie w celu wywołania strachu,
- chęć wywołania psychologicznych skutków i reakcji,
- rozróżnienie celu zamachu i bezpośredniej ofiary,

[21] Ibidem, s. 34.
[22] Patrz: Schmidt A. i in., *Political terrorism: a New guide to actors, authors, concepts, data bases, theories and literature*, New York 1988, s. 47.

- celowość i planowanie działań,
- metoda walki,
- konflikt z obowiązującymi regułami zachowań społecznych,
- wymuszenia,
- wykorzystywanie mediów w celu poszukiwania rozgłosu,
- zbrodnia ślepa (przypadkowy dobór ofiar),
- wykorzystywanie symboliki,
- nieobliczalność działań sprawców,
- ukryty charakter organizacji stosującej metody terrorystyczne.

Do kryteriów, wskazywanych jako pozwalające na zakwalifikowanie danego zjawiska jako mającego charakter terrorystyczny, należą także[23]:

- terroryzm jest strategią użycia przemocy zaplanowaną dla osiągnięcia wyznaczonego celu poprzez zasianie strachu i poczucia niepewności,
- opiera swoje działania na bezprawnym użyciu siły bądź groźby użycia siły w drodze ciągłej kampanii bądź incydentalnych ataków,
- terroryści używają przemocy w stosunku do cywili i celów nie-militarnych,
- zdobycie władzy, manipulowanie nią i stosowanie jej do wywoływania zmian jest nieodłącznym czynnikiem pozostającym u źródeł terroryzmu,
- obszar działania (państwo, region bądź grupa społeczna) szybko staje się transnarodowy w wypadku zaistnienia jakichkolwiek powiązań na skalę międzynarodową.

Bruce Hoffman, w wyniku analizy dorobku naukowego w zakresie badań nad terroryzmem sformułował podsumowanie tego zjawiska, mówiące, że terroryzm[24]:

- jest nieodłącznie polityczny w obszarze celów i motywacji,
- jest zaplanowany tak, aby powodować długofalowe reperkusje psychologiczne dalej, niż tylko bezpośrednia ofiara czy cel,

[23] Whittaker D. J., *Terrorists and terrorism in the contemporary world*, London and New York 2004, s.2.
[24] Hoffman B., *Oblicza terroryzmu*, Warszawa 1999, s. 41.

- stosują go organizacje, w których istnieje hierarchia przywódcza oraz konspiracyjna struktura komórek (ich członkowie nie noszą mundurów ani innych elementów identyfikacyjnych),
- jest dokonywany przez ugrupowanie subnarodowe lub podmiot niepaństwowy,
- stosuje przemoc, lub – co równie istotne – grozi jej zastosowaniem.

Kolejną metodą, która może pozwolić na stwierdzenie, że dane wydarzenie było rzeczywiście przejawem stosowania metod terrorystycznych, to definiowanie poprzez odróżnienie. Należy bowiem ustanowić jasną granicę pomiędzy terroryzmem, a co najmniej trzema innymi zjawiskami, które w przejawach swoich zdają się być do niego podobne.

Pierwszym z tych zjawisk jest terror kryminalny[25]. Jest to metoda stosowana przez grupy przestępcze, najczęściej takie, których działania mają charakter zorganizowany. W drodze do maksymalizowania swoich zysków, pochodzących z działalności przestępczej stosują one takie same metody jak ugrupowania terrorystyczne, wśród których znaleźć można zabójstwa, podkładanie ładunków wybuchowych czy branie zakładników. Jednak są to czyny popełniane z myślą o zysku w wymiarze finansowym, a nie politycznym, a tym samym nie spełniają one jednego z podstawowych warunków zaistnienia aktu terrorystycznego: prowadzą do zdobycia pieniędzy, a nie władzy.

Kolejne zjawisko, które w wielu swoich przejawach podobne może się wydawać do terroryzmu, to partyzantka, bądź też – według innych określeń – guerilla[26]. Zachowany w tym wypadku jest warunek politycznego celu działania, bowiem działania ugrupowań partyzanckich bardzo często związane są z dążeniem do uzyskania autonomii jakiegoś regionu, bądź ustanowienia prawa do samostanowienia jakiejś grupy etnicznej. Jednak w wypadku partyzantki – o ile nie posługuje się ona nielegalnymi metodami terrorystycznymi – istnieje jedna poważna różnica: celem działań ugrupowań partyzanckich nie powinny być osoby nie związane z konfliktem, osoby cywilne. Działania ugrupowania, które dąży do prawno międzynarodowego uznania swoich dążeń stosować się muszą do międzynarodowych regulacji dotyczących konflik-

[25] Ibidem, s. 39 – 40.
[26] Ibidem, s. 39.

tów zbrojnych, a zatem do prawa wojennego, stanowionego przez międzynarodowe konwencje i traktaty.

Ostatnia kategoria zjawisk często mylnie identyfikowanych jako zjawiska o charakterze terrorystycznym, to zjawiska związane z przejawami przemocy o podłożu psychopatologicznym[27]. W wypadku osób, które stosują przemoc – z wykorzystaniem tych samych narzędzi, jakie stosują ugrupowania terrorystyczne – nie można mówić o akcie terrorystycznym, ze względu na brak realnych motywów politycznych.

Aby przedstawić w pełni różnorodność definicji terroryzmu, spotykanych we współczesnym piśmiennictwie, warto przytoczyć kilka z tych definicji. Robert Borkowski w swojej książce *Terroryzm ponowoczesny* pisze, że terroryzm to akty przemocy lub ich groźba ich dokonania, których celem jest zaszantażowanie władzy i opinii publicznej. Definiuje zatem terroryzm jako metodę walki o osiąganie określonych celów politycznych, której narzędziem jest zbrodnia, a celem wzbudzenie strachu.[28]

Jednocześnie przytacza się listę istotnych cech charakterystycznych zjawiska terroryzmu, wśród których znalazły się[29]:

- uznawanie przemocy zbrojnej za wyłącznie skuteczną metodę walki politycznej, co skutkuje fetyszyzacją przemocy,
- okrucieństwo i nihilizm moralny w podejmowanych akcjach, co pokazać ma z jednej strony siłę i determinację terrorystów, a z drugiej strony ma wzbudzać i utrzymywać strach przed terrorystami,
- wzbudzenie silnego i powszechnego poczucia zagrożenia poprzez zastraszenie nie tylko elit politycznych, ale i całego społeczeństwa,
- uzyskanie rozgłosu i obecność w mass mediach, bowiem bez masowego audytorium terrorysta jest nikim,
- polityczny szantaż i wymuszenie określonych zmian politycznych,
- akty przemocy i zbrodni nie zawsze mają doprowadzić do obalenia władzy i przejęcia steru rządów, w wielu przypadkach mają jednak na celu przygotowanie sytuacji rewolucyjnej, a więc doprowadzenie do anarchizacji życia publicznego, zastraszenie i zdemoralizowanie funkcjonariuszy pań-

---

[27] Ibidem, s. 40.
[28] Borkowski R., *Terroryzm ponowoczesny. Studium z antropologii polityki*, Toruń 2006, s. 45.
[29] Cesarz Z., Stadtmuller E., *Problemy polityczne współczesnego świata,* Wrocław 1996 [cyt. za:] Borkowski R., *Terroryzm ponowoczesny,* op.cit., s. 45 – 46.

stwowych, zademonstrowanie siły terrorystów, sprowokowanie represji i ograniczania swobód obywateli przez państwo celem wykreowania buntowniczych nastrojów.

W innej definicji terroryzmu akcentuje się natomiast takie cechy tego zjawiska[30]:

[...] istotą terroryzmu jest ostentacyjne i maksymalistyczne (masowe, totalne, nieograniczone), celowe (tj. świadomie zamierzone) atakowanie niewinnych, postronnych (cywilnych) osób i dóbr publicznych (otoczenia) dla pośredniego (asymetrycznego, poprzez opinię publiczną) oddziaływania na rzeczywistego przeciwnika politycznego bądź ideologicznego.

Współczesny terroryzm jest zjawiskiem międzynarodowym. Globalizacja terroryzmu nie jest pustym pojęciem. W dobie terroryzmu religijnego, a właściwie religijno – ideologicznego, którego dążenia również mają globalny charakter – bowiem dążenia do stworzenia światowego państwa rządzonego według zapisów szari'atu, czyli prawa religijnego, nie można określić inaczej, niż tylko globalnym celem – nie można dłużej opierać strategii zwalczania terroryzmu na działaniach indywidualnych państw. Wraz z globalizacją i jej procesami dotykającymi niemalże wszystkich przejawów życia społecznego, politycznego i gospodarczego, pojawiła się także globalizacja zjawiska przemocy. Globalizacja środków komunikacji i telekomunikacji pociągnęła za sobą globalizację celów. Cele te stały się widoczne – jeśli nie w bezpośrednim doświadczeniu, to poprzez rzeczywistość wirtualną, telewizję i możliwość bezpośredniego przekazu audio i wideo na skalę globalną.

Współczesne organizacje terrorystyczne wyzbyły się już zasadniczo charakteru organizacji o charakterze hierarchicznym. Ich nowa, sieciowa postać umożliwia im mobilność i elastyczność w obliczu działań organów ścigania pojedynczych państw.

2.1.3 Metody ataków terrorystycznych

Terroryzm – w jego obecnej postaci – to zagrożenie na tyle nowe, że ani społeczność międzynarodowa, ani poszczególne państwa nie znalazły sposobu na ujęcie walki z nim w ramy prawne czy też strategiczno – taktyczne, które wiązałyby obie strony konfliktu.

---

[30] Koziej S., *Między piekłem a rajem: szare bezpieczeństwo na progu XXI w.*, Toruń 2006, s. 31.

Warto się zatrzymać przez chwile przy tym, co stanowi o przekonaniu ugrupowań terrorystycznych o sensowności stosowania takiej metody, jak terroryzm. W dobie zaawansowanych narzędzi technicznych i technologicznych, jakimi posługują się państwa w przeciwdziałaniu temu zagrożeniu, coraz skuteczniejszych systemów bezpieczeństwa – co stanowi o atrakcyjności tej metody?

Tab. 4: Rodzaje ataków terrorystycznych według celu ataku

Rodzaj celu ataku	Potencjalne konsekwencje	Wady celu	Zalety celu
Element infrastruktury krytycznej państwa	Poważane zakłócenie funkcjonowania państwa i jego struktur, duży wpływ na życie ludności na dużym terenie, potencjalnie na całym terytorium państwa.	Ścisła ochrona celu, monitoring celu i jego okolic, duże prawdopodobieństwo przerwania ataku nawet w trakcie jego przeprowadzania.	Ze względu na poważne konsekwencje, terroryści i ich atak obecni są w życiu społecznym i politycznym państwa aż do całkowitego usunięcia szkód.
Element infrastruktury gospodarczej państwa (np. giełda papierów wartościowych)	Poważane zakłócenie funkcjonowania państwa i jego struktur, długofalowe zakłócenia życia gospodarczego i społecznego nawet po usunięciu bezpośrednich skutków ataku.	Cel może być dobrze zabezpieczony. Obywatele mogą w większości nie odczuwać bezpośredniego związku z celem ataku, tym samym strach powodowany przez taki atak może być ograniczony.	Długofalowe skutki ataku, możliwość wpływu na życie społeczne i gospodarcze państwa w długiej perspektywie, a tym samym kształtowanie zmian na scenie politycznej.
Symbol narodowy	Silne uderzenie w tożsamość danej społeczności.	Może nie spowodować daleko idących konsekwencji ekonomicznych. Cel może być stosunkowo dobrze chroniony, co utrudnia przeprowadzenie ataku.	Wykazanie zdolności do uderzenia w obiekty, które cieszą się największym społecznym sentymentem – wokół których koncentruje się tożsamość państwa.
Cel miękki (na przykład centrum handlowe, środek transportu publicznego, miejsce kultu religijnego)	Poważne straty w postaci ofiar śmiertelnych i rannych. Panika wśród społeczeństwa. Poważne szkody materialne.	Atak na cel nie spowoduje poważnych, długotrwałych zakłóceń w funkcjonowaniu struktur państwowych ani struktur zarządzania kryzysowego.	Cel może być słabo zabezpieczony. Całe społeczeństwo może identyfikować się z jego ofiarami, co potęguje panikę.

Źródło: opracowanie własne.

Badacze i analitycy działań ugrupowań terrorystycznych, pracujący dla korporacji RAND – jednego z największych na świecie ośrodków naukowo – badawczych zajmujących się taką problematyką – sformułowali cztery teorie mówiące o tym, dlaczego największy ze współczesnych przeciwników wśród organizacji terrorystycznych, czyli Al-Qaida, konsekwentnie stosuje taką metodę działania[31].

Pierwsza z tych hipotez to hipoteza przymusu (ang. *coersion hypothesis*)[32]. Opiera się ona na założeniu, iż istotnym czynnikiem skłaniającym Al-Qaidę do dokonywania ataków terrorystycznych jest ten, który wchodzi w skład definicji terroryzmu – a zatem użycie siły, aby zmusić państwa do wycofania się z jej terenu, czy też raczej terenów, na który chce mieć ona ostateczny wpływ, a zatem świata muzułmańskiego.

Kolejna hipoteza, hipoteza zniszczeń (ang. *damage hypothesis*), mówi, iż działania o charakterze terrorystycznym mają na celu głównie dokonanie maksymalnych szkód, zarówno w wymiarze materialnym, jak i politycznym – szkód, które zmniejszą zdolność państw do podejmowania działań, które prowadzone są przez organizacje terrorystyczne na ich własnym terenie, a przynajmniej na terenie, które za własny one uważają.[33]

Hipoteza integracji (zgromadzenia, ang. *rally hypothesis*) opiera się na założeniu, które mówi, że wielkie zamachy terrorystyczne stanowią dowód siły organizacji terrorystycznych, dowód, który pozwala na integrowanie wokół nich coraz większej liczy zwolenników, a zatem zwiększanie nie tylko ich zdolności operacyjnych i powiększanie środków, jakimi dysponują, ale także zwiększają poprawcie, które może zostać w przyszłości wykorzystane w celu realizacji ostatecznych dążeń, to jest zdobycia władzy i utrzymania jej[34].

Hipoteza franszyzy (ang. *franchise hypothesis*) natomiast odwołuje się do poglądu, który związany jest z dotychczasowymi dokonaniami społeczności międzynarodowej w zakresie przeciwdziałania terroryzmowi, tj. z osłabieniem Al-Qaidy[35]. Mówi ona o tym, iż mimo, że organizacja ta mogła utracić zdolności do podejmowania własnych działań operacyjnych, to nadal posiada zdolność inspirowania innych organi-

---

[31] Libicki M. C., Chalk P., Sisson M. W., *Exploring Terrorist Targeting Preferences*, RAND 2007, s. 8.
[32] Ibidem, s. 9.
[33] Ibidem, s. 11.
[34] Ibidem, s. 12.
[35] Ibidem, s.14.

zacji i wykorzystywania ich zdolności do przeprowadzania ataków – sama nie ponosząc przy tym dalszych strat. W sytuacji zaniku, bądź też minimalizowania wagi celów, które można określić mianem „lokalnych", zwiększa się zagrożenie integracją poszczególnych ugrupowań terrorystycznych. Warto zresztą zastanawiając się nad tym brać pod uwagę jeden istotny fakt: sieci takie, jak Al-Qaida, działające na poziomie globalnym mają lokalnym organizacjom terrorystycznym do zaoferowania coś niezwykle istotnego, a mianowicie możliwość bezpośredniego udziału w światowym dżihadzie, a więc globalizację wymiaru ich działań. Pamiętać jednak należy, iż jednocześnie uzyskują one coś niemal równie cennego – to jest lokalny wymiar zdolności operacyjnych, pozwalający na uzyskanie ludzi oraz logistyki na poziomie, na jaki pozwala jedynie znajomość terenu, ze znajomością całej jego specyfiki, sposobów działania lokalnych organów ścigania, nastrojów ludzi i politycznego nastawienia władz lokalnych i regionalnych.

Dokonawszy analizy teoretycznej motywacji ugrupowań terrorystycznych, warto podjąć analogiczny wysiłek w odniesieniu do metod stosowanych przez organizacje terrorystyczne.

Tab. 5: Rodzaje ataków terrorystycznych według zastosowanej metody ataku

Rodzaj / typ ataku	Obiekt ataku	Potencjalny cel / skutki
ZABÓJSTWA	Przedstawiciele administracji, sił policyjnych lub zbrojnych państwa, które jest przedmiotem ataku.	Służą przede wszystkim wykazaniu słabości i bezradności danego rządu w oczach obywateli i odebraniu mu wiarygodności.
ZAMACHY BOMBOWE	Miejsca publiczne, takie jak kina, centra handlowe, węzły komunikacyjne i inne miejsca, w których gromadzą się znaczne grupy ludzi.	zamach bombowy nie musi zostać doprowadzony do momentu eksplozji złożonego urządzenia wybuchowego – sama informacja o podłożeniu ładunku powoduje panikę, wymaga przeprowadzenia ewakuacji zagrożonego budynku i powoduje zakłócenia w normalnym funkcjonowaniu instytucji
PORWANIA OSÓB	Osoby porwane mają wysoki status społeczny lub polityczny (przetrzymywane są w nieznanym służbom bezpieczeństwa miejscu).	W celu wymuszenia wypłaty okupu lub osiągnięcia innego celu, jak na przykład uwolnienie zatrzymanych przez państwo terrorystów lub ich stronników.

UPROWADZENIA ŚRODKÓW TRANSPORTU	samolotów, autobusów, pociągów	Charakterystyczne zwłaszcza dla fali terroryzmu „nowej lewicy", służą wykazaniu słabości i bezradności danego rządu w oczach obywateli i odebraniu mu wiarygodności oraz wymuszeni podjęcia działań wskazanych przez terrorystów.
BRANIE ZAKŁADNIKÓW	Zakładnikami mogą być osoby przypadkowe (lub ich grupa), przetrzymywani są zaś w miejscu znanym służbom bezpieczeństwa, często wzięcie zakładników powiązane jest z wymienionym wcześniej uprowadzeniem środka transportu (np. samolotu).	Służą wykazaniu słabości i bezradności danego rządu w oczach obywateli i odebraniu mu wiarygodności oraz wymuszeni podjęcia działań wskazanych przez terrorystów.
NAPADY RABUNKOWE	----------	Służą zazwyczaj zdobyciu środków finansowych przeznaczonych na finansowanie działalności organizacji terrorystycznej (podobnym celom służyć mogą inne aspekty działań organizacji terrorystycznych, na przykład udział w handlu bronią, narkotykami lub ludźmi).

Źródło: opracowanie własne na podstawie: Jałoszyński K., *Współczesny wymiar antyterroryzmu*, Warszawa 2008, s. 44 i dalsze.

Odrębna kategoria metod terrorystycznych należy do prognozowanej dopiero ery tzw. super-terroryzmu, posługującego się środkami takimi jak broń chemiczna, biologiczna, nuklearna, radiologiczna. Do chwili obecnej ataki z użyciem takich środków walki są rzadkie, ze względu na znaczne trudności towarzyszące zdobyciu i wykorzystaniu środków niezbędnych do przeprowadzenia takiego ataku.

Ostatnią kategorią terroryzmu, szczególnie istotną w kontekście omawiania roli zasobów informacyjnych w systemie bezpieczeństwa państwa, jest cyberterroryzm. Według Departamentu Sprawiedliwości USA aktem terroryzmu sieciowego (cyberterroryzmu) jest użycie technologii informatycznej zarówno do rozpowszechniania programów, ataków na sieci, systemy komputerowe, infrastrukturę telekomunikacyjną,

jak i dla wymiany informacji czy przesyłania gróźb do szantażowanych podmiotów lub instytucji.

Cyberterroryzm można podzielić na:

- aktywizm – niedestrukcyjna działalność, w ramach której Internet służy wsparciu prowadzonej kampanii,
- haktywizm – kombinacja aktywizmu i działań przestępczych; wykorzystuje on metody hakerskie przeciwko określonym celom w Sieci, by zakłócić funkcjonowanie Internetu, nie powodując przy tym poważnych strat; działalność ta ma na celu nie tyle zniszczenie zasobów przeciwnika, ale przede wszystkim zwrócenie uwagi na dany problem,
- cyberterroryzm – politycznie motywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów w szerszym rozumieniu tego słowa; jest to także użycie Internetu do komunikowania się, propagandy i dezinformacji przez organizacje terrorystyczne.

Jedną z przyczyn zagrożeń wiążących się z cyberterroryzmem w kontekście bezpieczeństwa informacyjnego kraju, jest fakt, iż sieć komputerowa jest w dzisiejszej epoce siecią nerwową kraju. W krajach wysoko rozwiniętych niezakłócone działanie cyberprzestrzeni jest podstawą nie tylko prawidłowego funkcjonowania gospodarki, ale także bezpieczeństwa kraju.[36]

W obrębie cyberterroryzmu szczególnie poważnym zagrożeniem jest metoda ataku polegająca na spiętrzeniu i nałożeniu na siebie ataków przeciwko infrastrukturze krytycznej państwa prowadzonych w cyberprzestrzeni oraz fizycznie, przeciwko jej materialnym elementom[37]. W wypadku ataku w cyberprzestrzeni zakłóceniu ulec może działanie materialnych elementów infrastruktury krytycznej państwa – w wypadku ataku na budynek mieszczący istotny węzeł internetowy i zespół routerów spowoduje załamanie komunikacji internetowej odczuwalne w skali regionu bądź nawet kraju.

---

[36] Verton D., *Black Ice: niewidzialna groźba cyberterroryzmu*, Helion, Warszawa 2004, s. 76.
[37] Szerzej na ten temat: Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa państwa*, Warszawa 2004, s. 38.

Tym samym cyberterroryzm może być zarówno aktem podłożenia bomby w strategicznym miejscu, zakłóceniem poprzez atak hackerski działania komunikacji opartej na łączach internetowych, a nawet przekazywaniem treści zagrażających lub prowadzących do powstania zagrożenia bezpieczeństwa państwa. Przejęcie przez hackerów kontroli nad podsystemami infrastruktury krytycznej państwa może zagrozić zarówno systemom łączności, zapewniania dopływu energii czy wody. Trzeba wciąż brać pod uwagę, że im wyżej rozwinięte państwo, tym większa część jego zasobów i instytucji jest kontrolowana lub posługuje się zinformatyzowanymi systemami łączności i zarządzania.

Dodatkowym aspektem zagrożenia cyberterroryzmem jest jego aspekt propagandowy. Przekaz ideologii terrorystycznej, wspierany przekazem dotyczącym przemocy i zagrożenia, jakie stanowi on dla społeczeństw i stabilności państw, jest wyrazem walki o „rząd dusz" oraz o zdobycie dominacji w sferze informacji i wpływu na szerokie grupy społeczne.

2.2 Systemy przeciwdziałania terroryzmowi – aspekty informacyjne

Terroryzm w swojej współczesnej postaci jest zjawiskiem zglobalizowanym, taka też więc musi być walka z nim. Przeciwdziałanie terroryzmowi pozostaje istotnym zagadnieniem uwzględnianym w polityce wewnętrznej i zewnętrznej wielu państw, poświęcają mu także wiele uwagi organizacje międzynarodowe.

Poszczególne państwa budują skomplikowane w swej istocie systemy przeciwdziałania temu zjawisku. Zaangażowane siły i środki, które stanowią elementy tych systemów obejmują zarówno służby i instytucje, jak też mechanizmy prawne, które stanowią integralną część systemów politycznych, społecznych i bezpieczeństwa tych państw. Ze względu na naturę zagrożenia, jego zwalczanie pozostaje dla ogromniej większości państw tym obszarem, który kojarzony jest z wyłączną ich kompetencję, co tym bardziej komplikuje ustanawianie międzynarodowych mechanizmów współpracy w tym zakresie.

System przeciwdziałania terroryzmowi zdefiniować zatem należałoby jako zespół sił i środków, funkcjonujących w ramach i na podstawie określonych rozwiązań prawnych, organizacyjnych i funkcjonalnych, których zadaniem jest rozpoznanie za-

grożeń terrorystyczne, zapobieganie im i zwalczanie oraz minimalizacja i likwidacja ich skutków.

Wśród podmiotów, które stanowią elementy systemu przeciwdziałania terroryzmowi, wymienić należy wszystkie organy, służby i instytucje, które realizują zadania w zakresie przeciwdziałania terroryzmowi. Wśród nich znajdują się:

- służby specjalne (wywiad i kontrwywiad),
- służby o charakterze policyjnym (policja, straż graniczna, służby celne, służby imigracyjne, policje skarbowe),
- służby finansowe (wywiad finansowy, resort finansów, służby nadzoru bankowego),
- służby dyplomatyczne,
- instytucje edukacyjne,
- służby zarządzania kryzysowego.

W systemie przeciwdziałania terroryzmowi na poziomie realizowanych zadań wyróżnia się kilka podstawowym elementów. Należą do nich[38]:

- rozpoznanie,
- profilaktyka,
- zwalczanie terroryzmu,
- minimalizacja i likwidacja skutków ataków terrorystycznych.

Każdy z tych elementów zawiera, dla pełnej skuteczności danego składnika systemu i przedsiębranych w związku z nim działań, substrat związany z posiadaniem i stosownym wykorzystaniem informacji. Niniejszy rozdział będzie stanowił próbę prezentacji wymienionych elementów współczesnego systemu przeciwdziałania terroryzmowi w kontekście wspomnianego substratu informacyjnego.

2.2.1 Rozpoznanie zagrożeń terrorystycznych

Rozpoznanie jest narzędziem, które umożliwia zbadanie otoczenia w celu ujawnienia i ustalenia potencjalnych aktywności terrorystycznych - uderzających w bezpieczeństwo publiczne. Pozwala na określenie własnych słabości i potencjalnych celów dla terrorystów. Proces planowania działań antyterrorystycznych wyznacza nam

[38] Patrz także: Jałoszyński K., *Współczesny wymiar antyterroryzmu,* Warszawa 2008, s. 98.

również punkt startowy w określaniu problemów, z jakimi mierzą się służby odpowiedzialne za bezpieczeństwo państwa[39]. Mimo wszystko, wiele razy zdarza się, iż to co uznawane jest za problem, w rzeczywistości jest tylko symptomem prawdziwego problemu, nie jest więc też przyczyną zaistniałej sytuacji. Istotne jest zatem zbieranie wszelkich informacji, potencjalnie związanych z problemem i poprawne ich analizowanie, aż do momentu, w którym można uzyskać pewność, jaka jest dokładnie natura zagrożenia i jaką może przybrać ono formę.

Do przedsięwzięć zaliczanych do grupy rozpoznania w zakresie przeciwdziałania terroryzmowi należą między innymi działania rozpoznania policyjnego. Znajdują się wśród nich[40]:

- rozpoznanie operacyjne dotyczące obywateli danego państwa oraz cudzoziemców zamieszkałych na stałe lub przebywających czasowo, co do których zachodzi podejrzenie działalności o charakterze terrorystycznym, uczestniczenia w grupach, organizacjach, lub związkach podejrzewanych o działalność terrorystyczną lub jej wspieranie,
- rozpoznanie operacyjne grup, organizacji i związków, co do których istnieje podejrzenie o działalność terrorystyczną oraz finansowania takiej działalności w kraju lub poza jego granicami,
- pozyskiwanie poufnych osobowych źródeł informacji wywodzących się z wcześniej wymienionych struktur przestępczych lub umożliwiających bezpośrednie dotarcie do środowisk posiadających wiedzę o nich,
- współpraca w zakresie wymiany informacji o przekraczaniu granic i migracji przez osoby podejrzewane o działalność terrorystyczną, z właściwymi placówkami służby granicznej danego kraju,
- rozpoznanie operacyjne środowisk wywodzących się z państw wysokiego ryzyka.

Powyższe działania określa się zbiorczo mianem czynności operacyjno – rozpoznawczych. Należą do nich czynności, których „głównym celem jest zapobieganie, rozpoznawanie i wykrywanie sprawców przestępstw". Można przy tym wskazać, że

---

[39] Prońko J., *Bezpieczeństwo państwa. Zarys teorii problemu i zadań administracji publicznej,* Bielsko-Biała 2007, s. 39.
[40] Jałoszyński K., *Współczesny wymiar antyterroryzmu*, op. cit., s. 114.

„czynności takie nie mają charakteru procesowego, stanowią natomiast pozaprocesowe, techniczno – taktyczne czynności praktyki organów (...) mające na celu zapobieganie i zwalczanie przestępczości". [41]

Czynności operacyjno – rozpoznawcze podejmowane są w celu rozpoznawania, zapobiegania i wykrywania przestępstw oraz ścigania ich sprawców. Czynności te realizowane są wraz z czynnościami analityczno – informacyjnymi w celu uzyskiwania i przetwarzania informacji istotnych dla ochrony bezpieczeństwa państwa i jego porządku konstytucyjnego.[42]

Najważniejszą funkcją rozpoznania w kontekście przeciwdziałania terroryzmowi jest funkcja infromacyjna. Funkcja ta zapewnia dopływ informacji, przetworzonych do postaci umożliwiającej wykorzystanie ich w procesach decyzyjnych polityki bezpieczeństwa narodowego i międzynarodowego. Istotą tej funkcji jest pozyskiwanie przez właściwe instytucje i służby, analizowanie i przekazywanie właściwym organom decyzyjnym informacji o zagrożeniach dla bezpieczeństwa państwa.

W tym kontekście informacja określana jest jako termin stosowany w odniesieniu do *wszystkich rodzajów nie poddanego ocenie materiału informacyjnego, o równych stopniach wiarygodności, pochodzącego z jakichkolwiek źródeł, a posiadającego potencjalną wartość wywiadowczą.*[43]

Informacje pozyskiwane w procesie rozpoznania można ogólnie podzielić na informacje uzyskiwane z dwóch podstawowych źródeł: od człowieka – jako źródła informacji o nim samym i otaczającej go rzeczywistości oraz za pomocą środków technicznych.

2.2.2 Profilaktyka

Obecnie wzrastające niemal we wszystkich państwach zagrożenie terroryzmem wysuwa na plan pierwszy potrzebę stosowania wielu metod profilaktycznych opartych na różnorodnych dyscyplinach naukowych i udziale społeczeństwa. Ważną rolę odgrywa tutaj zaktywizowanie i zilustrowanie działań społeczeństwa na rzecz poprawy własnego bezpieczeństwa. Rolą służb odpowiedzialnych za przeciwdziałanie ter-

---

[41] Hoc A., *Zagadnienia odpowiedzialności karnej za szpiegostwo*, Warszawa 1985 [cyt. za: Zalewski S., *Służby Specjalne w państwie demokratycznym*, Warszawa 2002, str. 58].
[42] Zalewski S., *Służby Specjalne w państwie demokratycznym*, Warszawa 2002, str. 59.
[43] *Encyklopedia szpiegostwa*, Warszawa 1995, str. 114-115.

roryzmowi jest osiągnięcie takiego wpływu na organizację życia by nie stwarzało ono możliwości dla terrorystów.

Strategia służb antyterrorystycznych w kwestiach profilaktyki obejmować powinna:

- znajomość technik sytuacyjnego i społecznego zapobiegania zamachom terrorystycznym,
- metody zjednywania sobie społeczeństwa w walce z terroryzmem,
- system analizowania zamachów terrorystycznych pod kątem czasu, miejsca, metody, taktyki tak aby jak najlepiej wykorzystać istniejące środki do ich zwalczania,
- wykorzystanie wiedzy wykwalifikowanych ekspertów do pomocy i porad w sprawie specjalistycznych środków zapobiegania zamachom terrorystycznym – na zasadzie współpracy w określaniu metod postępowania przy tworzeniu instrukcji, algorytmów działania, badaniu systemów alarmowych, analizowaniu zachowań itp.
- wypracowanie metod oceniających podejmowane inicjatywy w przeciwdziałaniu terroryzmowi w celu określenia ich skuteczności,
- dysponowanie środkami do rozpowszechniania inicjatyw profilaktycznych,
- zaangażowanie grup specjalistów, pracowników środków masowego przekazu mogących propagować walkę z terroryzmem.

Profilaktyka to zespół metod i środków mających na celu uniemożliwienie albo utrudnienie dokonania zamachu terrorystycznego. Profilaktyka antyterrorystyczna obejmuje wcześniejsze studia nad genezą i etiologią zamachów terrorystycznych, przy czym operuje ona przede wszystkim metodami z zakresu psychologii i pedagogiki społecznej. Jej celem jest pozytywne ukierunkowanie aktywności ludzkiej, usuwanie zagrożeń oraz wywarcie wpływu na zmianę ujemnych postaw i tolerancji[44].

Warunki skuteczności zapobiegania zamachom terrorystycznym można sprowadzić do trzech zasad:

a) zasady indywidualizacji, polegającej na dostosowaniu metod profilaktyki do rodzaju i okoliczności działalności terrorystycznej, motywu i sposobu działania przestępczego,

[44] Hołyst B., *Kryminalistyka*, Warszawa 2000, s. 97.

b) zasady systematyczności stanowiącej zaprzeczenie doraźnych akcji profilaktycznych,
c) zasady kompleksowości, sprowadzającej się do wielostronnego stosowania metod profilaktyki[45].

Opracowanie metod profilaktyki antyterrorystycznej musi być poprzedzone dokładnymi badaniami z zakresu struktury i dynamiki zagrożenia terrorystycznego, a także metod i motywów działalności terrorystycznej. Wszelkie diagnozy, prognozy czy zalecenia nie oparte na wynikach badań empirycznych zbyt często okazują się chybione i bezwartościowe.

Ze względu na treść i zakres funkcji profilaktycznych można wyróżnić trzy podstawowe kierunki działań w systemie przeciwdziałania terroryzmowi:

a) operatywny,
b) badawczy,
c) instruktażowy[46].

Najszersze zastosowanie znajdują funkcje operatywne. Wymienić tu należy różne formy pracy obserwacyjno-wywiadowczej i informacyjno-rozpoznawczej. Dla działalności profilaktycznej ważne jest prowadzenie skutecznego rozpoznania środowisk zagrożonych działalnością terrorystyczną.

Dla programowania działalności profilaktycznej duże znaczenie mają tzw. atlasy zagrożenia terrorystycznego, stale aktualizowane[47]. Poszczególne mapy stają się z jednej strony źródłem hipotez wyjaśniających, jak dalece charakter danego regionu, jego historia, wewnętrzna sytuacja, polityczna, problemy społeczno-gospodarcze, perspektywy rozwojowe oraz wzajemne związki wpływają na strukturę i dynamikę zagrożenia terrorystycznego. Z drugiej zaś strony mapy te mają znaczenie informacyjne dla administracji rządowych w prowadzeniu długotrwałej polityki zwalczania i przeciwdziałania terroryzmowi.

Rozważając kwestie związane z funkcjami badawczymi, warto podkreślić, że od dłuższego czasu organy przeciwdziałania terroryzmowi podejmują lub inicjują różnorodne badania naukowe w dziedzinie profilaktyki. Celem działalności instruktażowej w systemie przeciwdziałania terroryzmowi jest oddziaływanie na obywateli w tym kierunku aby postępowali oni w sposób utrudniający terrorystom ich działal-

[45] Hołyst B., op. cit., s. 99.
[46] Hanausek T., *Kryminalistyka. Zarys wykładu*, Kraków 2005, s. 105.
[47] Zobacz także: Siemaszko A., *Atlas przestępczości w Polsce*, Warszawa 2009.

ność oraz zachowywali się w przypadku zaistnienia zamachu terrorystycznego w taki sposób aby ograniczyć lub zminimalizować skutki.

W większości państw zagrożonych zamachami terrorystycznymi istnieją specjalne komórki, których zadania sprowadzają się do udzielania porad w zakresie profilaktyki oraz ostrzeżeń przed skutkami lekkomyślnej postawy wobec zjawiska terroryzmu. W ramach działalności instruktażowej służby antyterrorystyczne na całym świecie wykorzystują środki masowego przekazu (radio, prasa, telewizja) dla upowszechniania informacji o metodach działania terrorystów i możliwościach uniknięcia skutków zamachu terrorystycznego[48].

Bardzo ważną rolę w działalności profilaktycznej służb antyterrorystycznych odgrywa współdziałanie ze społeczeństwem. Efektywność działania tych organów w przeciwdziałaniu terroryzmowi zależy w poważnym stopniu właśnie od pomocy społeczeństwa. Profilaktyka mająca na celu przygotowanie społeczeństwa do potencjalnego ataku, a więc kształtowanie świadomości społecznej, uczenie społeczeństwa sposobów reagowania na potencjalne zagrożenie, mechanizmów zachowań w sytuacjach kryzysowych – te elementy profilaktyki społecznej stają się niezbędnym elementem systemu przeciwdziałania terroryzmowi[49].

Zarówno badacze, teoretycy, jak i praktycy zwalczania terroryzmu kładą od dawna duży nacisk na współpracę w zwalczaniu terroryzmu oraz na koordynację tej współpracy. Jest to warunek, którego spełnienie jest tak samo niezbędne, jak trudne do spełnienia. Zapewnienie efektywnej współpracy nawet pomiędzy służbami, których wspólnym zadaniem jest zapewnienie bezpieczeństwa państwa jest niezwykle trudne ze względu na odrębne kultury pracy, inne modele rozwiązywanie problemów oraz poczucie wyłącznej kompetencji. Tym trudniejsza jest współpraca służb z podmiotami, które nie realizują zadań związanych ze zwalczaniem terroryzmu na co dzień, współpracę z instytucjami i ludźmi, których punkt skupienia jest zupełnie inny. A jednak i bez takiej współpracy żadne państwo nie będzie w pełni bezpieczne od terroryzmu.

Operacje terrorystyczne, tak jak każde działanie, które ma być przeprowadzone na obcym dla działającego terenie, działanie jak najbardziej dyskretne i niedo-

[48] Piasecka P., *Jak przygotować społeczeństwo na zagrożenie terrorystyczne podczas wielkich imprez sportowych* [w:] Liedel K., *EURO 2012: Mistrzostwa Europy w cieniu terroryzmu*, Warszawa 2007, s. 52.
[49] Ibidem, s. 52.

strzegalne dla postronnych, działanie, które musi przynieść sukces przy pierwszej próbie – wymaga starannych przygotowań i logistycznego zabezpieczenia, a także wcześniejszego rozpoznania terenu. Ten etap przygotowania ataku i rozpoznania celów – a także etap przygotowania narzędzi ataku, to etap, na którym służby odpowiedzialne za bezpieczeństwo państwa potrzebują wsparcia swojego najważniejszego partnera – społeczeństwa, które mają chronić.

Kształtowanie świadomości społecznej i przekazywanie do publicznej wiadomości informacji na temat właściwych algorytmów zachowań na wypadek zaistnienia ataku terrorystycznego jest niezmiernie ważnym elementem prewencji zagrożeń. Stanowi ono cenny wkład w przygotowanie do reagowania na sytuacje kryzysowe i pozwala na zapoznanie społeczeństwa ze standardami zachowań w sytuacji zagrożenia.[50]

Ze względu na to należy kształtować społeczną świadomość dotyczącą na przykład tego, na co powinno się zwracać uwagę na co dzień[51]:

Przygotowanie ataku i narzędzi ataku

1. *zwracaj uwagę na obcokrajowców, którzy wynajmują mieszkania na krótki okres; poświęć również uwagę nagłemu zwiększeniu aktywności w takich miejscach, zwiększonej liczbie odwiedzin obcokrajowców, szczególnie zachowujących się nietypowo i nerwowo,*
2. *zwróć uwagę na osoby, które zakupują lub przewożą znaczne ilości materiałów chemicznych i składują je w mieszkaniach lub innych miejscach nie związanych z legalną produkcją przemysłową.*

Rozpoznanie celów

1. *zwróć uwagę na osoby, które filmują lub fotografują obiekty przemysłowe, węzły komunikacyjne, obiekty rozrywkowe, centra handlowe, wieżowce i miejsca kultu religijnego;*
2. *zwróć uwagę szczególnie na osoby, które długo przebywają w jakimś miejscu użyteczności publicznej (centra handlowe i rozrywkowe), które nie za-*

---

[50] Ibidem, s. 55.
[51] Spis zasad, będący częścią poradnika opublikowanego przez Ministerstwo Spraw Wewnętrznych i Administracji we współpracy z dziennikiem, opublikowany w *Terroryzm – co robić w sytuacji zagrożenia?*, dodatek do dziennika „Rzeczpospolita" z dnia 25 lutego 2005 r.

chowują się zgodnie przeznaczeniem obiektów, w których się znajdują, a jedynie prowadzą obserwację otoczenia.

Przeprowadzenie ataku

1. *zwróć uwagę na nerwowo się zachowujące, odbiegające sposobem zachowania od innych osoby;*
2. *zwracaj uwagę na pozostawiony bez opieki bagaż, torby, plecaki, pakunki,*
3. *zwracaj uwagę na osoby ubrane nieodpowiednio do pogody, np. noszące grube, maskujące okrycie mimo upału);*
4. *zwracaj uwagę na nieodpowiednio zaparkowane pojazdy, np. w pobliżu wejść do centrów handlowych, tuż pod kościołem itp. oraz na ich kierowców.*

Realizowane przez poszczególne państwa kampanie społeczne przyjmują także postać kampanii informacyjnych polegających na informowaniu obywateli o możliwościach i sposobach kontaktowania się z władzami w wypadku podejrzeń co do potencjalnego zagrożenia. Przywołać można tu brytyjską kampanię „są dwa sposoby na sprawdzenie, czy niebezpieczeństwo istnieje: jedna to kontakt w policją – druga to milczące pozwolenie na popełnienie zbrodni" realizowana jest głównie w postaci licznych plakatów. Obrazowały one sytuacje, na które należy reagować: znalezienie podejrzanej paczki, natknięcie się na niewłaściwie zaparkowany samochód, dostrzeżenia podejrzanie zachowujących się osób.

W dziedzinie przygotowania kraju na potencjalne zagrożenie terrorystyczne jednym z najistotniejszych elementów jest prowadzenie ćwiczeń i szkoleń, z udziałem nie tylko osób, służb i instytucji odpowiedzialnych za bezpieczeństwo państwa, ale także z udziałem społeczeństwa. Prowadzenie ćwiczeń powinno mieć trzy podstawowe cele: testowanie koordynacji działań kontr-terrorystycznych, testowanie strategicznego decydowania oraz testowanie mechanizmu dowodzenia i kontroli.

W ćwiczeniach w dziedzinie zwalczania terroryzmu powinny znaleźć się elementy, które mają wnosić realny wkład w zwiększanie zdolności reagowania na atak terrorystyczny. W ćwiczeniach brać udział powinny różne siły policyjne w połączeniu z właściwymi do zwalczania terroryzmu instytucjami poza-policyjnymi. Do kluczowych elementów ćwiczeń należą: operacyjne reagowanie, rządowe narzędzia kryzysowe, komunikacja publiczna i kontakty z mediami, zarządzanie kryzysowe oraz wyciągnię-

te wnioski. Celem ćwiczeń nie jest ich bezbłędne przeprowadzenie, a wyłapanie luk i niedoskonałości reagowania w sytuacji realnego zagrożenia.

Jak wspomniano wyżej, oprócz ćwiczeń testujących właściwy system przeciwdziałania terroryzmowi, organizować powinno państwo również ćwiczenia z udziałem społeczeństwa. Kształtowanie właściwych mechanizmów zachowania i reagowania w sytuacji zagrożenia jest najbardziej efektywne właśnie w procesie ćwiczeń, które unaoczniają ich uczestnikom również scenariusze potencjalnego rozwoju wydarzeń. W państwach realizujących takie działania na bazie dotychczasowych doświadczeń w dziedzinie przeciwdziałania terroryzmowi, ćwiczenia takie przyjmują często postać ćwiczeń związanych z ewakuacją dużych zbiorowisk ludzi. Osoby, które mają okazję uczestniczyć w takich ćwiczeniach zyskują kilka bardzo ważnych umiejętności i istotnych informacji. Dowiadują się wiele o algorytmach działania służb, o możliwym czasie oczekiwania na akcję ratunkową, o pożądanych mechanizmach zachowań własnych[52].

Dzięki temu, w sytuacji realnego zagrożenia nie tylko spokojniej reagują, unikając paniki, która jest przecież reakcją wynikającą głównie z lęku przed nieznanym i braku umiejętności odniesienia się do tego nieznanego zagrożenia.

2.2.3 Zwalczanie terroryzmu

Zwalczanie terroryzmu międzynarodowego to jeden z najbardziej znanych i najszerzej omawianych aspektów przeciwdziałania terroryzmowi. Niemniej jednak pamiętać należy, że powszechność pojęcia nie oznacza powszechności właściwego rozumienia tego pojęcia. Dlatego właśnie omawiając zwalczanie terroryzmu w kontekście systemu przeciwdziałania terroryzmowi należy zwrócić uwagę na wielopłaszczyznowość działań, jakie konieczne są dla efektywności działań podmiotów odpowiedzialnych za bezpieczeństwo państwa w tym obszarze.

[52] Informacje z wizyty studyjnej w Londynie (Home Office) po zamachach 7 i 21 lipca 2005 r.

Fizyczne zwalczanie terroryzmu

Pierwszą – i konieczną – reakcją na atak przeprowadzony przez ugrupowanie terrorystyczne jest dążenie do wyeliminowania bezpośredniego zagrożenia stwarzanego przez to ugrupowanie. Możliwe sposoby zrealizowania takiego zamierzenia sprowadzają się przede wszystkim do działań o charakterze siłowym, do fizycznego ujęcia bądź wyeliminowania sprawców ataku. Działanie takie będzie skuteczne w stosunku do danej grupy terrorystycznej, której członkowie zostaną wykluczeni z gry operacyjnej toczącej się pomiędzy organami wdrażania prawa a przedstawicielami ugrupowań terrorystycznych.

Jednostki (pododdziały) antyterrorystyczne policji są bliższe strukturom wojskowym niż policyjnym. Przy tworzeniu policyjnych pododdziałów antyterrorystycznych na świecie (w latach 70.) czerpano inspirację z wojskowych jednostek specjalnych, zwłaszcza w zakresie szkolenia[53].

Ponadto taktyka walki bezpośredniej pododdziałów antyterrorystycznych oparta jest na metodach walki piechoty, obejmującej podejście do celu (obiektu) oraz bezpośrednie rażenie przeciwnika ogniem. Sposobem działania jest atak (stanowiący formę natarcia – podstawowego rodzaju działań zaczepnych[54]) zmierzający do likwidacji lub unieszkodliwienia wroga, w tym wypadku terrorystów. Zasady taktyki działania pododdziałów antyterrorystycznych są oparte na zasadach taktyki wojsk lądowych (piechoty). Jego istotą jest neutralizacja zagrożenia, uratowanie przetrzymywanych zakładników z minimalnym zagrożeniem dla ratowanych ludzi, osób postronnych oraz samych członków pododdziału antyterrorystycznego[55].

Pododdział antyterrorystyczny, aby w sposób efektywny realizować swoje zadania, musi mieć przede wszystkim odpowiednią strukturę organizacyjną, składającą się z dwóch podstawowych pionów (komórek): bojowego i wsparcia. Taki układ strukturalny daje gwarancję prawidłowego funkcjonowania pododdziału, jego samodzielność organizacyjną. Jest to niezbędny warunek realizacji operacji antyterrorystycznych. Czynności związane z procesem szkolenia, pracą sztabową i kancelaryjną,

---

[53] Jałoszyński K., *EURO 2012 – budowa jednostki kontrterrorystycznej policji równie ważna jak budowa stadionów* [w:] Liedel K., *EURO 2012: Mistrzostwa Europy w cieniu terroryzmu*, Warszawa 2007, s. 67.

[54] Kaczmarek W., *Natarcie związku taktycznego*, rozprawa habilitacyjna, „Zeszyty Naukowe AON" 1997, nr 4(29), dodatek do nr 4, s. 27.

[55] Jałoszyński K., *EURO 2012 – budowa jednostki kontrterrorystycznej policji równie ważna jak budowa stadionów,* op. cit., s. 63.

zabezpieczeniem magazynowym, rusznikarskim, obsługą środków transportu, itp. realizowane są przez pion wsparcia.

Proces i zakres szkolenia podporządkowany powinien być konkretnie zdefiniowanym zadaniom, a także weryfikacji predyspozycji psychofizycznych służących w nim policjantów (np. skoki spadochronowe).

Dla pełnej efektywności realizowanych zadań jednostka antyterrorystyczna powinna być wyposażona w silny pion analityczny i planowania operacyjnego. Ponadto w skład jednostki powinny wchodzić komórki szkoleniowo – taktyczne i rozpoznawcze, a także logistyczne.

Jak łatwo zauważyć, współczesna jednostka antyterrorystyczna, poza pionem bojowym, zajmującym się fizycznym zaangażowaniem w zwalczanie terroryzmu, swoje działania opiera w znacznym stopniu na zasobach informacyjnych:

- rozpoznaniu sytuacji przed przeprowadzeniem akcji bojowej,
- zasobach wiedzy na temat taktyki terrorystów i stosowanych przez nich metod walki,
- zasobach wiedzy na temat współczesnych taktyk i technik bojowych formacji antyterrorystycznych,
- wiedzy na temat metod szkolenia.

Piony: analityczny i planowania operacyjnego nie miałyby racji bytu bez posiadania dostępu do stosownych informacji.

Dla podsumowania omówienia płaszczyzny fizycznego zwalczania terroryzmu warto podkreślić jeden jej istotny aspekt: nie ma ona wymiaru prewencyjnego w swojej istocie. Jest zawsze działaniem *post factum*. Dlatego nigdy nie będzie miała waloru prewencji i wyprzedzenia, które są najważniejszymi cechami działań uznawanych za najbardziej skuteczne we współczesnych systemach przeciwdziałania terroryzmowi.

Dla skutecznej realizacji powierzonych sobie zadań, zarówno policyjne, jak i wojskowe jednostki specjalne muszą funkcjonować w oparciu o spójny system prawny. Podstawą podejmowania działań mających na celu zwalczanie zjawisk o charakterze przestępczym, w tym stanowiących zagrożenie dla bezpieczeństwa

narodowego, takich jak terroryzm międzynarodowy, stanowi właściwe kształtowanie norm prawnych stanowiących podstawę funkcjonowania systemu ścigania.

Od początków kampanii antyterrorystycznej dyskutuje się nad rozwiązaniami prawnymi stosownymi do prowadzenia działalności kontr-terrorystycznej. Najbardziej zaawansowane prawodawstwo kontr-terrorystyczne w dziedzinie przeciwdziałania terroryzmowi poprzez efektywne gromadzenie i wymianę informacji posiadają Stany Zjednoczone w postaci *Patriot Act*. Najważniejsze grupy postanowień tego aktu prawnego posłużą zatem jako przykład rozwiązań prawnych służących zwalczaniu terroryzmu.

Prawna płaszczyzna zwalczania terroryzmu na przykładzie amerykańskiej ustawy *Patriot Act* i innych amerykańskich regulacji prawnych w tym obszarze[56]

W sekcji 201 ustawy *Patriot Act* znalazł się zapis, który zezwala na zakładanie podsłuchów, jeżeli służby federalne prowadzą dochodzenie w związku z atakami na obywateli USA poza terytorium USA, użyciem broni masowego rażenia, działaniami terrorystycznymi poza granicami krajowymi, transakcjami pieniężnymi z rządem, który sponsoruje terroryzm, zapewnianiem wsparcia materialnego terrorystom i dostarczaniem broni do określonych organizacji terrorystycznych jak również przestępstwa związane z użyciem broni chemicznej.

Sekcja 202, jak sekcja 201, uzupełnia listę ciężkich przestępstw wobec, których może być wykorzystywany podsłuch. Zezwala na zakładanie podsłuchów w dochodzeniu związanym z przestępstwem komputerowym i nadużyciem (zwanym piractwem komputerowym).

W sekcji 203 *Patriot Act* upoważnia do wymiany informacji o „zagranicznych służbach wywiadowczych" zgromadzonych podczas dochodzeń kryminalnych z niektórymi funkcjonariuszami federalnymi. Wprowadza zmianę do federalnego prawa dotyczącego podsłuchów w celu zezwolenia funkcjonariuszom organów porządku publicznego na ujawnianie nagrań z podsłuchiwania innym „funkcjonariuszom federalnych organów porządku publicznego, wywiadu, ochrony, ds. imigracji, obrony na-

[56] USA *Patriot Act*, tekst ustawy dostępny na stronie Kongresu USA o adresie [http://www.locke.gov].

rodowej lub bezpieczeństwa narodowego" w zakresie, w jakim informacje dotyczą „zagranicznych służb wywiadu", „kontrwywiadu" lub w zakresie „informacji o wywiadzie zagranicznym" oraz będzie pomagać funkcjonariuszom w wykonywaniu swoich obowiązków. *Patriot Act* zawiera bardziej ogólne prawo do wymiany informacji tego samego rodzaju otrzymanych z dochodzeń kryminalnych z tymi samymi funkcjonariuszami w tych samych okolicznościach. Upoważnia ona również do ujawnienia informacji o zagrożeniach zgromadzonych podczas prowadzenia dochodzenia kryminalnego odpowiednim funkcjonariuszom rządu federalnego, stanowego, lokalnego lub zagranicznego w celu przeciwdziałania tej groźbie. Informacja o zagrożeniu może zawierać informacje o zagrożeniu atakiem, innych „poważnych wrogich aktach", sabotażu, terroryzmie, bądź potajemnych działaniach ze strony wywiadu. Sekcja 203 *Patriot Act* została stworzona po to, by zająć się problemami związanymi z barierami w wymianie informacji pomiędzy funkcjonariuszami służb wymiaru sprawiedliwości a funkcjonariuszami służby bezpieczeństwa narodowego. Sekcja 203 zapożycza swoją definicję „wywiadu zagranicznego" oraz „kontrwywiadu" z Ustawy o Bezpieczeństwie Narodowym z 1947 roku. Termin „informacje wywiadu zagranicznego" jest nowy. Dotyczy on informacji nt. osób ważnych dla państwa informacji, które związane są z możliwościami Stanów Zjednoczonych w zakresie ochrony przed rzeczywistymi bądź potencjalnymi atakami, działaniami sabotażowymi, terroryzmem lub tajnymi działaniami wywiadowczymi obcych państw lub w odniesieniu do obcego państwa, dotyczą „krajowej obrony lub bezpieczeństwa Stanów Zjednoczonych" lub „prowadzenia spraw zagranicznych Stanów Zjednoczonych".

Sekcja 206 *Patriot Act* usprawnia procedury wydawania nakazów dotyczących inwigilacji „wielomiejscowej" lub wielopunktowej. Sąd może wydać nakaz inwigilacji skoncentrowanej raczej na obiekcie, niż na urządzeniu, które obiekt wykorzystuje, kiedy „działania przedmiotu, którego wniosek dotyczy mogą skutkować udaremnieniem identyfikacji" określonego urządzenia. Ten nowy nakaz nie określa osoby wyznaczonej do pomocy; rząd może wydać ogólny nakaz dotyczący identyfikowanych osób lub nośników. *Patriot Act* modernizuje prawo do zakładania podsłuchów i zbliża je do przepisów prawa karnego dotyczących zakładania podsłuchów. *Patriot Act* wymaga, aby nakaz określał „tożsamość, jeśli jest znana, lub opis celu inwigilacji elektronicznej".

Patriot Act zapisami sekcji 209 modernizuje przepisy dotyczące przejmowania poczty głosowej przechowywanej u dostawcy usług eliminując wymóg posiadania nakazu założenia podsłuchu telefonicznego.

Prawo stanowiące o prywatności komunikacji elektronicznej zabrania usługodawcom dobrowolnego ujawniania, nawet rządowi, większości połączeń klientów lub zapisów. *Patriot Act* stworzyła w sekcji 212 wyjątek od tej zasady – zarówno dla połączeń jak i zapisów. Zezwala usługodawcom na ujawnianie materiału, jeżeli „mają podstawy by wierzyć", że istnieje „sytuacja nadzwyczajna zagrażająca życiu lub uszkodzenia ciała jakiejkolwiek osoby". Co więcej, zapisami sekcji 225 przyznał standardowy ustawodawczy immunitet (zwolnienie od spraw sądowych) spółkom telefonicznym, ISP, dzierżawcom i innym, którzy pomagają wprowadzić nakazy na mocy FISA, działając w dobrej wierze.

Sekcja 223 nakłada odpowiedzialność na urzędników rządowych za bezprawne ujawnienia informacji uzyskanych z podsłuchów i potwierdza prawo agencji rządowych do ukarania pracowników za dobrowolne i celowe naruszenie federalnego prawa dotyczącego podsłuchu lub gromadzenia informacji. Sekcja 223 nakłada również odpowiedzialność cywilną na Stany Zjednoczone za umyślne naruszenie federalnego prawa dotyczącego podsłuchu, prawa związanego z przechowywanymi połączeniami oraz prawa FISA w odniesieniu do inwigilacji, rewizji osobistych lub wykorzystaniem czy zainstalowaniem urządzenia *„pen register"* lub *„trap and trace"*.

Patriot Act w sekcji 215 łagodzi wymogi konieczne do spełnienia w celu otrzymania nakazu zajęcia akt biznesowych. Poprzednio konieczne było zaprezentowanie „konkretnych faktów dających podstawę, by wierzyć", że obiekt śledztwa pochodził „z mocarstw zagranicznych lub był agentem mocarstw zagranicznych". Po powstaniu sekcji 215, rząd ma tylko obowiązek stwierdzić, że dane lub przedmioty poszukiwane są dla celów śledztwa prowadzonego przez wywiad zagraniczny lub w celu zapewnienia ochrony przed międzynarodowym terroryzmem lub też dla tajnych działań wywiadu, chociaż śledztwo w sprawie obywatela Stanów Zjednoczonych może nie być „prowadzone całkowicie na podstawie działań chronionych Pierwszą Poprawką do Konstytucji". Nie istnieje żaden wymóg dowodowego lub faktycznego wykazywania, a sędzia ma bardzo małą swobodę w interpretacji wniosku o zajęcie akt. Jeżeli sędzia zdecyduje, że „aplikacja spełnia wymogi" sekcji, musi wydać nakaz. Sekcja 215 eliminuje wszelkie ograniczenia dotyczące rodzajów działalności lub jednostek, któ-

rych dane mogą być zajęte. Ponadto, sekcja rozszerza zakres przedmiotów, które FBI może uzyskać korzystając z prawa wynikającego z zasady „od danych" do „wszelkich rzeczy materialnych (w tym książki, dane, dokumenty i wiele innych)". Odbiorca nakazu może nie ujawniać faktu, że FBI poszukiwała określonych danych lub że je uzyskała dane.

Patriot Act wprowadza podobne zmiany do procedur w celu uzyskania nakazów udzielających prawo do korzystania z urządzeń typu pen register (rejestruje numery wychodzące z aparatu) lub „*trap and trace*" (rejestruje numery przychodzące). Urządzenia „*pen register*" oraz „*trap and trace*" nagrywają informacje odpowiednio o odbiorcy i źródle połączenia. Poprzednio wymagane było przedstawienie informacji o przyczynie, na podstawie której uznano, że monitorowana przez jedno z tych urządzeń linia mogła być używana przez jednostkę lub obce mocarstwo zaangażowane w międzynarodowe działania terrorystyczne lub szpiegostwo, które jest pogwałceniem prawa karnego Stanów Zjednoczonych. Po powstaniu sekcji 214, nie ma już takiego wymogu. Nowe wymogi w zakresie sporządzania wniosku są podobne do opisanych powyżej dla akt biznesowych.

Sekcja 216 zmienia definicje „*pen register*" i „*trap and trace*", w celu wyjaśnienia, że odnoszą się do poczty elektronicznej i Internetu, tak samo jak do połączeń telefonicznych.

Patriot Act poprawia ustawę o zabezpieczeniu kontrwywiadowczym poprzez zmienienie wymogu poświadczania, kiedy rząd ubiega się o nakaz nadzoru lub nakaz rewizji. Poprzednio, rząd miał obowiązek poświadczyć, że „celem" aplikacji było uzyskanie informacji o wywiadzie zagranicznym. Po stworzeniu sekcji 218, rząd ma obowiązek zaświadczenia, że uzyskanie informacji o wywiadzie zagranicznym jest „istotnym celem" wniosku. Zmiana ta miała na celu promowanie wymiany informacji między wywiadem a funkcjonariuszami wymiaru sprawiedliwości oraz eliminowania tego co otrzymało nazwę „ściany", która oddzieliła dochodzenia wymiaru sprawiedliwości i agencji wywiadu.

Sekcja 6001 Ustawy o Reformie Służb Wywiadowczych i Zapobieganiu Terroryzmowi (*Intelligence Reform and Terrorism Prevention Act*) z 2004 roku, znana jako poprawka „*lone wolf*" zezwala na inwigilację nowej kategorii jednostek. Postanowienie to poprawia definicję „agenta obcego mocarstwa" wynikającą z ustawy o zabez-

pieczeniu kontrwywiadowczym (*Foreign Intelligence Surveillance Act*) w taki sposób, aby obejmowała każdą osobę nie będącą obywatelem USA, która „angażuje się w terroryzm międzynarodowy lub działania związane z jego przygotowaniem". Poprzednio, definicja ta wymagała ogniwa łączącego z obcym mocarstwem lub jednostką, taką jak rząd zagraniczny czy międzynarodowa organizacja terrorystyczna[57]. Rozwinięta definicja pozwala rządowi na wykorzystanie FISA w dochodzeniu prowadzonym w przypadku osoby nie będącej obywatelem USA, o której nie wiadomo, że posiada powiązania z grupą lub jednostką. Kongres przyjął to postanowienie zwane „lone wolf", ponieważ istniała obawa, że poprzednia definicja nie obejmowała jednostek niestowarzyszonych – lub tych, dla których nie można ustalić żadnego związku – którzy niemniej jednak angażują się lub przygotowują się do zaangażowania w terroryzm międzynarodowy.

Sekcja 213 *Patriot Act*, znana jako postanowienie o „*sneak and peek*", daje prawo do opóźnionego powiadomienia o wykonywaniu nakazów rewizji w dochodzeniach kryminalnych. Poprzednio, prawo nie pozwalało na przeprowadzanie tajnych rewizji na terenie prywatnych posesji w dochodzeniach kryminalnych, chociaż FISA pozwalała na takie rewizje dla celów bezpieczeństwa narodowego. Jednakże, sądy pozwalały na rewizje z opóźnionym powiadomieniem w wielu sprawach karnych na początku lat 80-tych. W większości tych spraw dokonywano jedynie tajnego zajęcia dowodów niematerialnych (np., informacje lub zdjęcia), a nie majątku trwałego. Sekcja 213 wprowadza zmianę do artykułu 18 Kodeksu Stanów Zjednoczonych, sekcja 3103a, która dotyczy nakazów rewizji i zajęcia dowodów w przestępstwach federalnych, pozwalając na rewizje „*sneak and peek*". To nowe prawo nie jest ograniczone do terroryzmu; pozwala na dokonywanie rewizji z opóźnionym powiadomieniem dla wszelkich dochodzeń federalnych związanych z przestępstwami.

Sekcja 805 *Patriot Act* zmodyfikowała przepisy dotyczące udzielania pomocy materialnej terrorystom. Pierwotna definicja „pomocy materialnej lub środków" w innych ustawach zawierała dostarczanie pomocy rzeczowej, takiej jak pieniądze, towary i materiały, ale również mniej konkretną pomoc, taką jak „personel" i „szkolenie"[58]. Sekcja 805 rozszerzyła definicję włączając „fachową poradę lub pomoc".

---

[57] Baker S., Kavanagh J. (ed.), *Patriot Debates. Experts Debate the USA Patriot Act*, Chicago 2005, s. 47.

[58] Baker S., Kavanagh J. (ed.), *Patriot Debates. Experts Debate the USA Patriot Act,* op. cit., s. 68.

Ostatnim elementem *Patriot Act*, który warto omówić, jest prawo do zatrzymania prewencyjnego. W *Patriot Act* Kongres zmienił Ustawę o Imigracji i Narodowości, nakazując Prokuratorowi Generalnemu lub osobie przez niego wyznaczonej poświadczenie, że cudzoziemiec był zamieszany w działalność zagrażającą bezpieczeństwu Stanów Zjednoczonych w celu zatrzymania takiego cudzoziemca na siedem dni przed przedstawieniem zarzutów o przestępstwo imigracyjne lub karne. Rząd federalny uzyskał tym samym prawo do zatrzymywania cudzoziemców bez postawienia zarzutów na o wiele dłuższe okresy po prostu przez uwięzienie ich w sposób tajny i odmowę prawa do przesłuchań lub adwokata.

2.2.4 Minimalizacja i likwidacja skutków ataków terrorystycznych

W każdym systemie konieczne jest istnienie odpowiednich mechanizmów i procedur nie tylko na wypadek stanu normalnego państwa bądź organizacji, ale także specyficznych rozwiązań, które pełnią swoją rolę w sytuacji zaistnienia warunków szczególnych, które określić można mianem sytuacji kryzysowych.

Pojęcie to odnieść można do stanu narastającej destabilizacji, niepewności i napięcia społecznego, stwarzającego zagrożenie w dla integralności terytorialnej państwa, jego stabilności społecznej, politycznej i ekonomicznej oraz życia, zdrowia, mienia, środowiska lub infrastruktury krytycznej, w tym spowodowanego zdarzeniem o charakterze terrorystycznym, które charakteryzuje się możliwością utraty kontroli nad przebiegiem zdarzeń albo eskalacji zagrożenia[59].

Regulacje w zakresie zarządzania kryzysowego ujęte są w ustawach regulujących postępowanie specjalistycznych służb w zakresie zwalczania konkretnych zagrożeń. Konieczne jest jednak również stworzenie mechanizmu zarządzania kryzysowego funkcjonującego na szczeblu centralnym, zapewniającego kierowanie i koordynowanie działań antykryzysowych w przypadku różnych zagrożeń występujących zarówno na całym terytorium państwa, jak i jego części.

---

[59] Szlachcic B., *Bezpieczeństwo wewnętrzne państwa. Administracja rządowa i samorządowa w zarządzaniu reagowaniem kryzysowym* [w:] Liedel K., Prońko J., Wiśniewski B., (red. nauk.), *Administracja publiczna w systemie przeciwdziałania nadzwyczajnym zagrożeniom dla ludzi i środowiska*, Bielsko-Biała – Warszawa 2007, s. 28.

System zarządzania kryzysowego powinien obejmować organy administracji rządowej i samorządowej, siły zbrojne oraz niektóre podmioty sektora prywatnego (właścicieli i posiadaczy elementów infrastruktury krytycznej)[60]. Utrzymywanie w gotowości do działania struktur zarządzania kryzysowego pozwala na odpowiednio wczesne eliminowanie źródeł sytuacji kryzysowych, współdziałanie ich eliminowaniu zaistniałych sytuacji oraz szybkie usuwanie skutków takich zdarzeń. Odpowiednie regulacje prawne w tym zakresie powinny zatem określać rolę i zadania poszczególnych podmiotów, które wymienione zostały wyżej.

Dla stworzenia sprawnego systemu zarządzania kryzysowego przydatne jest powołanie na każdym szczeblu administracji publicznej (centralnym, administracji rządowej w terenie, samorządowym) centrów zarządzania kryzysowego. Do zadań centrów zarządzania kryzysowego na poszczególnych szczeblach należeć powinno m.in. pełnienie całodobowego dyżuru w celu zapewnienia przepływu informacji na potrzeby zarządzania kryzysowego, współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej oraz współdziałanie z podmiotami prowadzącymi akcje ratownicze i humanitarne[61].

Krajowe systemy zarządzania kryzysowego powinny stanowić jednocześnie odniesienie do międzynarodowych mechanizmów i regulacji w tym obszarze, na przykład do Systemu Reagowania Kryzysowego Organizacji Traktatu Północno-Atlantyckiego.

Dla celów zapewnienia koordynacji zarządzania kryzysowego na poziomie narodowym w systemie zarządzania kryzysowego funkcjonować może centralny organ / podmiot koordynacyjny. Najważniejsze zadania realizowane przez taki podmiot obejmować powinny[62]:

- realizacja spraw z zakresu planowania cywilnego,
- monitorowanie potencjalnych zagrożeń,
- uruchamianie, w przypadku zaistnienia zagrożeń, procedur związanych z zarządzaniem kryzysowym,

---

[60] Ibidem, s.54.
[61] Prońko J., *Bezpieczeństwo państwa. Zarys teorii problemu i zadań administracji publicznej,* op. cit., s. 77.
[62] Ibidem, s. 78.

- współpraca ze strukturami zarządzania kryzysowego organizacji międzynarodowych, do których należy dane państwo,
- zapewnienie obiegu informacji między krajowymi i zagranicznymi organami i strukturami zarządzania kryzysowego.

Przy omawianiu kwestii zarządzania kryzysowego konieczne wydaje się odniesienie się do dwóch istotnych kwestii: planowania cywilnego i infrastruktury krytycznej. Instrumentem służącym osiągnięciu przez organy administracji publicznej właściwego poziomu przygotowania do działań w sytuacjach kryzysowych jest całokształt przedsięwzięć planistycznych zdefiniowanych jako „planowanie cywilne". Planowanie cywilne stanowi zatem całokształt przedsięwzięć planistycznych, stanowiący element zarządzania kryzysowego, w szczególności polegających na opracowywaniu planów i programów mających na celu optymalne wykorzystanie dostępnych zasobów w sytuacjach zagrożeń oraz w czasie stanów nadzwyczajnych i w czasie wojny - w zakresie zapobiegania powstawaniu i rozprzestrzenianiu się zagrożenia oraz w zakresie przygotowania do zwalczania zagrożenia, a także reagowania w sytuacji zagrożenia i usuwania jego skutków[63].

Planowanie cywilne oznacza również planowanie w zakresie wspierania sił zbrojnych państwa w razie ich użycia oraz planowanie wykorzystania sił zbrojnych do realizacji zadań z zakresu zarządzania kryzysowego.

Jeżeli w sytuacji kryzysowej użycie innych sił i środków jest niemożliwe lub może okazać się niewystarczające oddziały sił zbrojnych państwa powinny mieć możliwość wykonywania zadań z zakresu zarządzania kryzysowego. Koordynowanie udziału oddziałów sił zbrojnych w realizacji zadań z zakresu zarządzania kryzysowego, w zależności od obszaru występowania zagrożeń, zapewniać powinny organy administracji publicznej odpowiedniego szczebla. Do zadań realizowanych w sytuacji kryzysowej przez siły zbrojne należeć może[64]:

- współudział w monitorowaniu zagrożeń;
- wykonywanie zadań związanych z oceną skutków zjawisk zaistniałych na obszarze występowania zagrożeń;
- wykonywanie zadań poszukiwawczo-ratowniczych;
- ewakuowanie poszkodowanej ludności i mienia;

[63] Szlachcic B., *Bezpieczeństwo wewnętrzne państwa.*, op. cit, s. 30.
[64] Ibidem, s. 32.

- wykonywanie zadań mających na celu przygotowanie warunków do czasowego przebywania ewakuowanej ludności w wyznaczonych miejscach;
- współudział w ochronie mienia pozostawionego na obszarze występowania zagrożeń;
- izolowanie obszaru występowania zagrożeń lub miejsca prowadzenia akcji ratowniczej;
- wykonywanie prac zabezpieczających, ratowniczych i ewakuacyjnych przy zagrożonych zabytkach;
- prowadzenie prac wymagających użycia specjalistycznego sprzętu technicznego lub materiałów wybuchowych będących w zasobach sił zbrojnych;
- usuwanie materiałów niebezpiecznych i ich unieszkodliwianie, z wykorzystaniem sił i środków będących na wyposażeniu sił zbrojnych;
- likwidowanie skażeń i zakażeń biologicznych;
- usuwanie skażeń promieniotwórczych;
- wykonywanie zadań związanych z naprawą i odbudową infrastruktury technicznej;
- współudział w zapewnieniu przejezdności szlaków komunikacyjnych;
- udzielanie pomocy medycznej i wykonywanie zadań sanitarno-higienicznych i przeciwepidemicznych.

2.3 Wnioski

Terroryzm jako nowa postać zagrożeń dla bezpieczeństwa państwa jest jednym z najgroźniejszych przeciwników, z którymi mierzyć się muszą współczesne podmioty stosunków międzynarodowych.

Ze względu na dynamikę tego zjawiska oraz szybkość, z jaką dostosowuje się ono do nowych rozwiązań w zakresie organizacji i technologii systemów bezpieczeństwa, w celu ochrony przed terroryzmem konieczne jest tworzenie systemów przeciwdziałania terroryzmowi, których cechą jest zdolność do ewoluowania co najmniej równa tej, jaką posiadają organizacje terrorystyczne.

Ze względu na trudności, jakich nastręcza definiowanie terroryzmu, związane z wielowymiarowością tego zjawiska, zarówno w sensie politycznych, jak i w sensie wielości przejawów, rodzajów zagrożeń, metodologii ataków oraz wspierających je ideologii, przeciwdziałanie temu zjawisku musi mieć charakter wieloaspektowy, takiej więc zasadzie wieloaspektowości podporządkowane być powinny również systemu przeciwdziałania terroryzmowi.

Warto podkreślić, że budowa takiego systemu jest więc skomplikowana z co najmniej dwóch przyczyn:

- musi on posiadać niezwykłe zdolności adaptacyjne, które pozwolą mu co najmniej nadążać za dynamiką zjawiska, jaki jest terroryzm,
- muszą charakteryzować się budowa pozwalającą na wieloaspektowe przeciwdziałanie zagrożeniu, a zatem uwzględniać maksymalną ilość podmiotów realizujących zadania w zakresie przeciwdziałania terroryzmowi, aby umożliwić prowadzanie działania na wszystkich płaszczyznach.

Złożoność zjawiska i niezwykle wymagające warunki, jakie stawia ono podmiotom, których zadaniem jest przeciwdziałanie mu sprawiają, że terroryzm jest jednym z najpoważniejszych zagrożeń we współczesnym świecie.

Rozdział 3

Rola zasobów informacyjnych w systemie przeciwdziałania terroryzmowi

3.1 Informacja jako zasób strategiczny

3.1.1 Społeczeństwo informacyjne

Ewolucja funkcji informacyjnej i warunków funkcjonowania instytucji oraz zmiany, jakie dokonały się w ciągu ostatnich kilkunastu lat dzięki zdobyczom nowoczesnej techniki i technologii informatycznej, dzięki rozwojowi procesów zarządzania, przyspieszeniu procesu wymiany towarowej, poprawie konkurencyjności we wszystkich sektorach gospodarki sprawiły, że zasoby informacyjne oraz ich pozyskiwanie i właściwe wykorzystanie stają się kluczowym czynnikiem sukcesu nie tylko każdej instytucji czy organizacji, a wręcz całych społeczeństw.

Analiza przeobrażeń społeczno-ekonomicznych na skutek wzrastającej roli informacji oraz wpływu technologii informacyjnej doprowadziła do koncepcji społeczeństwa informacyjnego. Powszechnie uznaje się, że żyjemy w wieku informacji. Na wyjaśnienie tego pojęcia uczeni proponowali wiele różnorodnych terminów. Aby określić złożone i szybko zmieniające się społeczeństwo, którego rozwój zależy od niezwykle zaawansowanych technologii, a także od postmaterialistycznego systemu wartości A. Toffler zaproponował termin „superuprzemysłowione społeczeństwo"[65]. Jeszcze do niedawna termin ten wyrażano także zwrotem „szok przyszłości", a obecnie preferowane jest określenie „społeczeństwo trzeciej fali". Wymienione terminy powszechnie zastępowane są przez „społeczeństwo informacyjne". Sam termin pochodzi z Japonii, a jako pierwszy użył go w 1963 r. Tadao Umesamo w artykule na temat ewolucyjnej teorii społeczeństwa opartego na „przemysłach informacyjnych". Prawdopodobnie spopularyzowane pojęcie to zostało przez Japończyka Kenichi Koyama w 1968 roku[66].

---

[65] Dziuba D. T., *Gospodarki nasycone informacją i wiedzą*, Warszawa 2000, str. 11
[66] Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Kraków 1999, str. 33

Istota koncepcji społeczeństwa informacyjnego dotyczy transformacji od społeczeństwa produkującego towary do społeczeństwa wytwarzającego usługi.

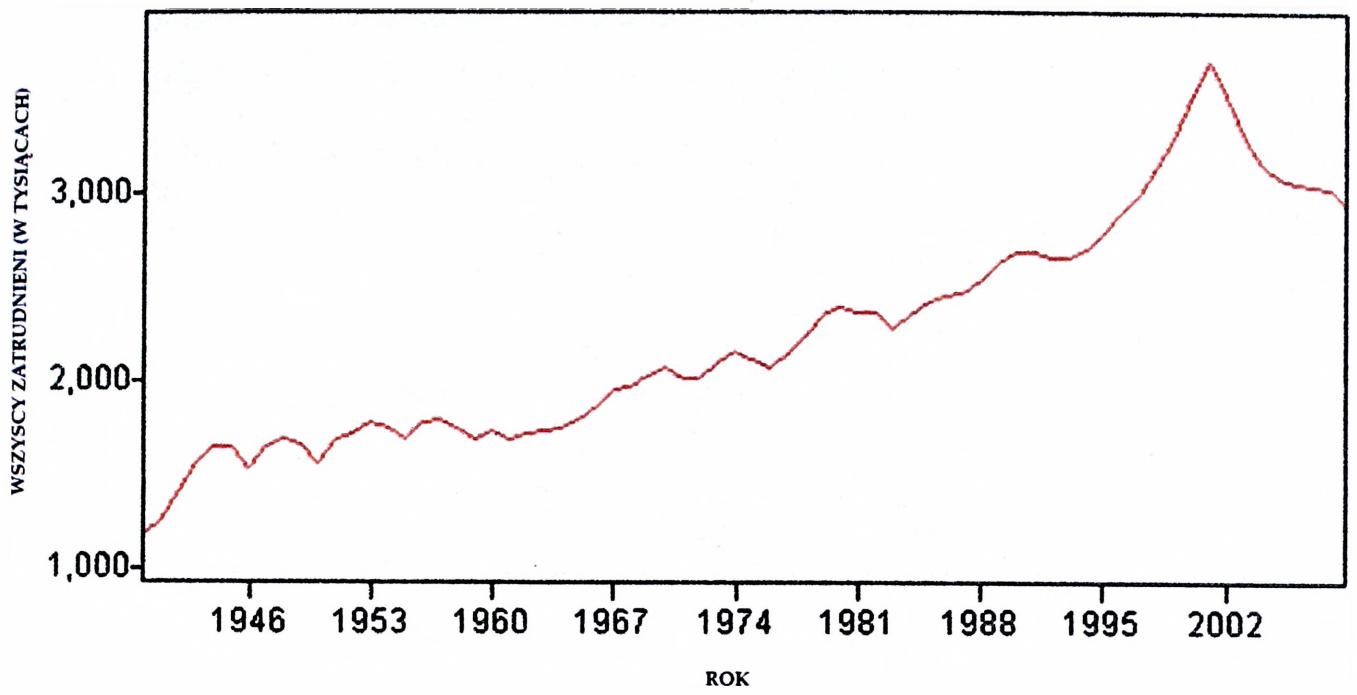
Analiza danych statystycznych przedstawionych w tabeli nr 1 wskazuje, że w ciągu 120 lat systematycznie wzrastała wielkość zatrudnienia w sektorze informacyjnym w USA. Zatrudnienie w sektorze informacyjnym w USA ulegało dalszym zmianom (tab. 6, rys. 7).

Tab. 6: Czterosektorowa agregacja zatrudnienia w gospodarce USA (udział procentowy) w latach 1860–1980

Lata	Sektor informacyjny	Sektor rolnictwa	Sektor przemysłu	Sektor usług	Łącznie
1860	5,8	40,6	37,0	16,6	100
1870	4,8	47,0	32,0	16,2	100
1880	6,5	43,7	25,2	24,6	100
1890	12,4	37,2	28,1	22,3	100
1900	12,8	35,3	26,8	25,1	100
1910	14,9	31,1	36,3	17,7	100
1920	17,7	32,5	32,0	17,8	100
1930	24,5	20,4	35,3	19,8	100
1940	24,9	15,4	37,2	22,5	100
1950	30,8	11,9	38,3	19,0	100
1960	42,0	6,0	34,8	17,2	100
1970	46,4	3,1	28,6	21,9	100
1980*	46,6	2,1	22,5	28,8	100

* szacunki Bureau of Labour Statistics (BLS)

Źródło: D. T. Dziuba, *Gospodarki nasycone informacją i wiedzą*, str. 18.



Rys. 7: Zatrudnienie w sektorze informacyjnym w USA w latach 1939 – 2008
Źródło: opracowanie własne na podstawie danych Bureau of Labour Statistics, USA.

Społeczeństwo amerykańskie przechodziło ewolucyjne zmiany od społeczeństwa produkującego towary do społeczeństwa wytwarzającego usługi oraz wzrost roli sektora informacyjnego w gospodarce, co powodowało jednocześnie znaczny wzrost zatrudnienia w sektorze informacyjnym (tab. 4).

Tab. 7: Zatrudnienie w sektorze informacyjnym w USA w latach 1939 – 2008

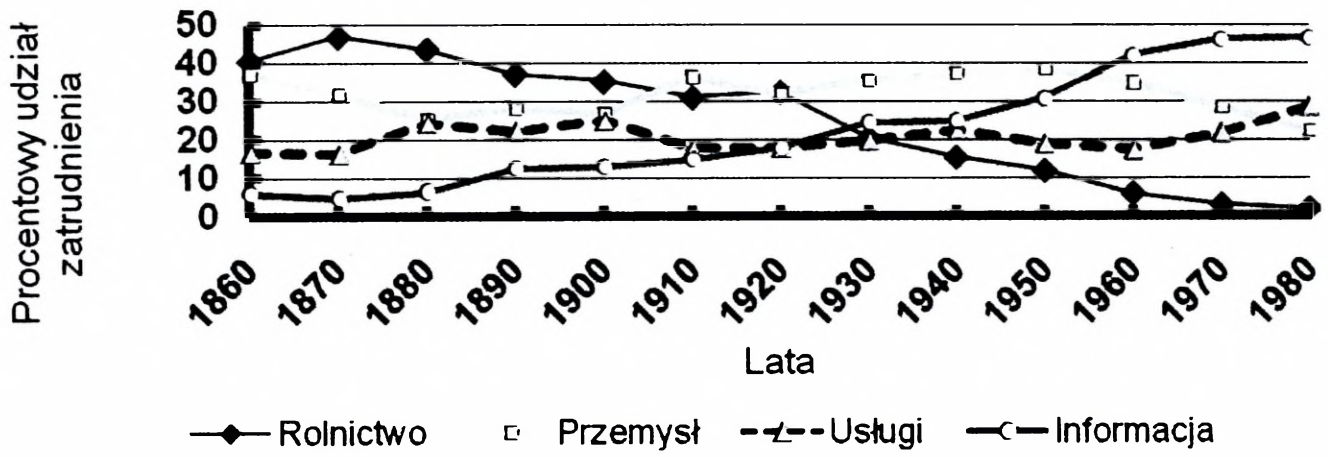
Rok	Zatrudnienie w sektorze informacyjnym
1940	1 241 000
1950	1 689 000
1960	1 691 000
1970	2 008 000
1980	2 364 000
1990	2 691 000
2000	3 705 000
2008	2 940 000

Źródło: opracowanie własne na podstawie danych Bureau of Labour Statistics, USA.

Przyjmując za kryterium wielkość zatrudnienia w poszczególnych sferach gospodarki, można określić graniczne daty stadiów rozwojowych społeczeństwa USA. Okres 1860-1980 można umownie podzielić na trzy etapy, wyznaczające momenty

przechodzenia od społeczeństwa rolniczego przez przemysłowe do „społeczeństwa informacyjnego". W etapie I (1860-1906) największą grupę zatrudnionych obejmowało rolnictwo. Na przełomie wieków zatrudnienie w przemyśle zaczęło dynamicznie wzrastać i stało się dominujące na etapie II (1906-1954). Tak więc w 1906 r. „zakończyło się" w USA społeczeństwo rolnicze, a „zaczęło" przemysłowe. Od 1954 roku (etap III) zaczęło dominować zatrudnienie w sektorze informacyjnym, a społeczeństwo amerykańskie weszło w stadium „społeczeństwa informacyjnego" (rys. 2).[67]

Schemat . 1: Zmiany struktury zatrudnienia w sektorach gospodarki USA (1860-1980)



Źródło: opracowanie własne.

W roku 2009 według szacunku Bureau of Labour Statistics stan zatrudnienia w USA osiągnął odpowiednio:

- ok. 60 % - usługi,
- ok. 1% - rolnictwo,
- ok. 20 % - przemysł,
- ok. 20 % - usługi.

Prawidłowości zaobserwowane w społeczeństwie USA występują w społeczeństwach innych wysoko rozwiniętych krajów, jak na to wskazują dane o strukturze zatrudnienia w USA, Wielkiej Brytanii, RFN i Australii w latach 1900 – 1980 (patrz tab. 5).

[67] Dziuba D. T., *Gospodarki nasycone informacją i wiedzą*, op.cit., str. 19

Tab. 8: Struktura zatrudnienia w krajach wysoko rozwiniętych (1990-1980)

	1900	1910	1920	1930	1940	1950	1960	1970	1980
SEKTOR INFORMACYJNY									
USA	12,8	14,9	17,7	24,5	24,9	30,8	42,0	46,4	46,6
Wielka Brytania	12,4	13,5	19,8	20,9	24,4	27,8	33,1	36,6	38,0
RFN	–	–	–	–	–	18,3	24,6	30,7	33,2
Australia	–	8,5	11,5	15,6	16,3	17,0	22,5	27,5	30,2
SEKTOR USŁUG									
USA	25,1	17,7	17,8	19,8	22,5	19,0	17,2	21,9	28,8
Wielka Brytania	34,0	35,7	29,7	27,5	27,3	27,1	26,9	26,7	26,9
RFN	–	–	–	–	–	20,9	–	–	25,9
Australia	–	33,5	34,0	30,3	32,7	35,0	32,5	32,2	35,6
SEKTOR PRZETWÓRCZY									
USA	26,8	36,3	32,0	35,3	37,2	38,3	34,8	28,6	22,5
Wielka Brytania	45,4	43,4	43,2	45,2	42,6	39,9	36,1	33,7	31,5
RFN	–	–	–	–	–	38,3	–	–	35,1
Australia	–	27,0	27,5	30,9	32,0	33,0	33,0	31,2	26,7
SEKTOR PIERWOTNY									
USA	35,3	31,1	32,5	20,4	15,4	11,9	6,0	3,1	2,1
Wielka Brytania	8,2	7,6	7,3	6,4	5,8	5,2	3,9	3,0	2,0
RFN	–	–	–	–	–	22,5	–	–	5,8
Australia	–	31,0	27,0	23,2	19,9	16,5	12,0	9,1	7,4

Źródło: D. T., Dziuba, Gospodarki nasycone informacją i wiedzą, str. 79.

Analiza danych dotyczących sektora informacyjnego w czterech państwach (USA, Wielkiej Brytanii, RFN i Australii – tab. 5) wskazuje stały wzrost sektora informacyjnego w ogólnej liczbie zatrudnionych oraz spadek udziału sektorów rolnictwa i przemysłu[68]. W analizowanym okresie sektor usług cechowała tendencja wzrostowa, lecz z pewnymi wahaniami. Na podstawie zebranych danych w literaturze przedmiotu wyodrębniono trzy modele społeczeństwa:

1) rolnicze, zwane przedprzemysłowym (przedindustrialnym),
2) przemysłowe (industrialne),
3) informacyjne (poprzemysłowe, postindustrialne)[69].

Wiedzę i technologię uznano za wyznaczniki rozwoju społecznego i ekonomicznego. Informacja i wiedza stały się tak istotne w produkcji jak kapitał, praca i ziemia.

[68] Ibidem, s.12.
[69] Ibidem, str. 14.

Gałęzie produkcji związane z przemysłem wytwórczym lub wydobywczym przekształciły się w gałęzie uzależnione w znacznym stopniu od informacji.

Prognozy uczonych wskazują, że społeczeństwo informacyjne będzie kształtowane przez rozwój przemysłów informatycznych. Rozwój komputerów i technologii przekazywania danych obniży w znaczny sposób koszt przetwarzania danych i ich upowszechniania, ułatwiając zastosowanie technologii do szerokiego spektrum działalności gospodarczej[70].

W społeczeństwie agrarnym czynnikiem ograniczającym rozwój gospodarczy była ziemia, w społeczeństwie przemysłowym – kapitał, natomiast czynnikiem warunkującym rozwój gospodarczy społeczeństwa informacyjnego jest dostęp do zgromadzonej informacji i w odpowiedni sposób przetworzonej w wiedzę.

W procesie transformacji do społeczeństwa informacyjnego można wyróżnić kilka współzależnych elementów:

1. Informacja staje się podstawowym i strategicznym zasobem, od którego zależy organizacja gospodarki światowej.
2. Rozwój technologii informacyjnej dostarcza niezbędnej infrastruktury do przetwarzania i rozpowszechniania informacji, umożliwiając np. handel w czasie rzeczywistym, monitorowanie relacji ekonomicznych, społecznych i politycznych.
3. Rynki jako miejsce transformują w kierunku rynków elektronicznych – przestrzeni rynkowej. Rynek staje się wszechobecny, a informacja i wiedza stają się obiektami kupna-sprzedaży.
4. Nikną tradycyjne granice organizacji.
5. Rozwój mediów i usług wyszukiwania informacji „przebudował" światowy system finansowy.
6. Informatyzacja integruje gospodarki lokalne ze światową. Globalizacja i rozwój technologii wpływają na różne sfery gospodarki. Proces globalizacji zmienia sposoby działalności gospodarczej, przyspiesza dystrybucję *know-how* i innowacji.

---

[70] Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, op. cit., str. 48.

7. Obecnie zauważa się tendencję do zacierania granic między sferą rozrywki a informacyjną[71].

W społeczeństwie informacyjnym różnice między poszczególnymi mediami i usługami informacyjnymi stają się mniej widoczne. Media integrowane są jakby we wszechobecny kanał informacyjny. Ten segment rynku staje się w dużej mierze zorientowany na rozrywkę[72]. Rynek rozrywki stanowi najszybciej rosnącą gałąź produkcji i sprzedaży w wysoko rozwiniętych państwach. Wyrazem zacierania się różnic pomiędzy rozrywką a informacją jest też m.in. mnogość fuzji przedsiębiorstw w sektorze elektroniki użytkowej, produkcji medialnej, sieci kablowych, wydawnictw, produkcji sprzętu komputerowego i oprogramowania oraz telekomunikacji.

Odpowiedź na pytanie o to, kiedy społeczeństwo można uznać za społeczeństwo informacyjne, nie jest jednoznaczna, gdyż w literaturze napotyka się wiele różnych definicji społeczeństwa informacyjnego. Jednak dla określenia społeczeństwa informacyjnego można się posłużyć następującymi kryteriami:

- technologicznym,
- przestrzennym,
- kulturowym,
- ekonomicznym i fachowo-zawodowym[73].

Kryterium technologiczne podkreśla zmiany techniczne, którym podlega funkcjonowanie społeczeństwa. Wyznacznikiem zmian społecznych jest proces wytworzenia nowej jakości technologii informacyjnej, szybkie rozpowszechnianie się komputerów, spadek ich cen oraz wzrost możliwości obliczeniowych.

Kryterium przestrzenne rozpatruje strategiczną rolę informacji, światowe tendencje integracyjne, przełamywanie barier między społecznościami oraz wdrażanie w życie idei globalnej wioski na skutek dystrybucji technologii informacyjnej w przestrzeni. Przenikanie technologii informacyjnych do wszystkich dziedzin życia i wynikające z tego faktu fundamentalne zmiany społeczeństw i jednostek charakteryzuje kryterium kulturowe. Badaniem gospodarki informacyjnej, oceną stopnia zinformatyzowania społeczeństwa na podstawie mobilności zawodowej oraz stopnia udziału

[71] Dziuba D. T., *Gospodarki nasycone informacją i wiedzą* , op. cit., str. 13
[72] Jabłoński W., *Kreowanie informacji. Media relations*, Warszawa 2006, PWN, s. 43.
[73] Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, op. cit., s. 66.

sektora informacyjnego w grupie osób aktywnych zawodowo zajmuje się kryterium ekonomiczne i fachowo-zawodowe. Na podstawie przyjętych kryteriów za społeczeństwo informacyjne uważa się społeczeństwo przemysłowe, skoncentrowane na produkcji, dystrybucji i użytkowaniu informacji. Czynnikami determinującymi istnienie społeczeństwa informacyjnego i gospodarki informacyjnej są:

1) traktowanie informacji jako dobra ekonomicznego, podstawowego zasobu i podstawowej kategorii ekonomicznej,
2) upowszechniony dostęp do technologii informacyjnych, tworzących obecnie różne kanały dystrybucji,
3) swobodna cyrkulacja różnorodnych kategorii informacji w społeczeństwie, implikująca nowe formy demokratyzacji,
4) około 50 % zatrudnionych w sektorze informacyjnym,
5) udział sektora informacyjnego w PNB (PKB) ok. 50 %,
6) dominacja sektora informacyjnego w gospodarce,
7) warunkowanie przez sektor informacyjny sprawnego funkcjonowania innych sektorów i działów gospodarki,
8) specjalny status nauki i edukacji.

Szczególną rolę przypisuje się uczelniom wyższym. Uczelnie, gdzie wiedza teoretyczna jest tworzona i kodyfikowana, stają się podstawowymi instytucjami społecznymi. Społeczeństwo wiedzy nie może sobie pozwolić na utratę jej potencjału. Nowego znaczenia nabierają też np. postulaty upowszechniania edukacji na poziomie wyższym i średnim. Bardzo ważne staje się określenie roli państwa w promowaniu rozwoju takiego społeczeństwa i gospodarki[74].

W literaturze pojawiają się również wskazania dotyczące istnienia wyznaczników aksjologicznych społeczeństwa informacyjnego jako epoki rozwoju ludzkości[75]:

- przechodzenie od mechanistycznej do systemowej wizji świata, w której nawet niewielkie zmiany warunków początkowych, a więc działania indywidualne, mogą niekiedy w zasadniczy sposób wpłynąć na bieg historii,

---

[74] Dziuba D. T., *Gospodarki nasycone informacją i wiedzą*, op.cit., str. 20
[75] Wierzbołowski J., *Aksjologiczne i społeczne skutki przekształcenia informacji w zasób*, Warszawa, 1997 [cyt. za: Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, op. cit., str. 46]

- odchodzenie od wielu paradygmatów oświeceniowych, w tym utożsamiania rozwoju z postępem,
- ewolucja systemu wartości, prowadzącej do zwiększenia adaptacyjności zarówno jednostek, jak i całych społeczeństw do narastającej zmienności otoczenia jako *conditio humana* początku XXI w.

Pamiętać jednak należy o tym, że w literaturze, pośród wielości formułowanych definicji społeczeństwa informacyjnego napotkać można takie, które w zwięzłej formie oddają jego najważniejsze cechy, tj. powiązanie komputerów ze środkami łączności, co zwiększa produktywność pracy. Taką definicję proponują Piotr Sienkiewicz i Tomasz Goban Klas[76]:

Społeczeństwo informacyjne to społeczeństwo, które nie tylko posiada rozwinięte środki przetwarzania informacji i komunikowania, lecz przetwarzanie informacji jest podstawą tworzenia dochodu narodowego i dostarcza źródła utrzymania większości społeczeństwa.

3.1.2 Informacja jako kategoria

Termin „informacja" pochodzi od łacińskiego wyrażenia *informatio* i oznacza wyobrażenie, wyjaśnienie, zawiadomienie. W mowie potocznej wyraża zaś jakąkolwiek wiadomość. Terminem tym posługiwano się w nielicznych, wyraźnie dających się odróżnić sytuacjach i dlatego wydawał się powszechnie zrozumiały. Od czasów sformułowania podstaw teorii informacji przez C. E Shannona (nazywanej też teorią Shannona lub matematyczną teorią informacji)[77] powstało szereg różnych określeń tego pojęcia.

Wśród najważniejszych znanych definicji pojęcia informacji wymienia się:

- *informacja to zbiór faktów, zdarzeń, cech itp. określonych obiektów (rzeczy, procesów, systemów) zawarty w wiadomości (komunikacie), tak ujęty i podany w takiej postaci (formie), że pozwala odbiorcy ustosunkować*

[76] Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, op. cit., str. 43
[77] Sienkiewicz P., *10 wykładów*, Warszawa 2005, str. 60

się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne [Piotr Sienkiewicz (1983)];[78]

- *informacja jest transformacja jednego komunikatu asocjacji informacyjnej w drugi komunikat tej asocjacji oraz informowanie jest to transformowanie informacji zawartych w łańcuchu oryginałów w informacje zawarte w łańcuchu obrazów* [Marian Mazur (1970)];[79]
- *informacja jest to wiedza przekazywana przez innych ludzi bądź uzyskiwana przez studia, obserwacje, badania* [A. Webster];[80]
- *informacja jest to czynnik sterujący strumieniami zasileń, wykorzystywany w organizmach żywych lub maszynach do bardziej sprawnego, efektywnego i celowego działania* [E. Kowalczyk];[81]
- *informacja – bodziec oddziałujący na układ recepcyjny człowieka, powodujący wytwarzanie w jego wyobraźni przedmiotu myślowego, odzwierciedlającego obraz rzeczy materialnej lub abstrakcyjnej, [...] który w jego przekonaniu (świadomości) kojarzy się z jakoś z tym bodźcem. Oznacza to, że informacje to tylko te doznania, które inspirują umysł ludzki do pewnej wyobraźni. Jej istnienie jest relatywnie związane z istnieniem człowieka i jego umysłem* [L. Ciborowski].[82]

Informacja może być rozumiana zarówno w szerokim, jak i w wąskim znaczeniu. Szerokie ujęcie informacji przedstawia określenie N. Wienera, dla którego *informacją jest nie tylko wiadomość o czymś, ale także każda decyzja, sugestia czy polecenie*. W tym ujęciu informacja może być przekazywana nie tylko w układzie człowiek – człowiek, ale także w innych układach, w których rolę nadawcy i odbiorcy mogą pełnić oprócz istot żywych też maszyny i inne obiekty. Natomiast H. Greniewski prezentuje wąskie ujęcie informacji. Jest nią *wiadomość uzyskiwana przez człowieka poprzez obserwację lub czynność umysłową, podlegająca przekazowi w układzie nadawca (człowiek) – odbiorca (człowiek)*[83].

---

[78] Ibidem, str. 62
[79] Sienkiewicz P., *10 wykładów*, op.cit., str. 62
[80] Strzoda M., *Zarządzanie informacjami w organizacji*, Warszawa 2004, str. 16
[81] Ibidem, str. 16
[82] Kwećka R., *Informacja w walce zbrojnej*, Warszawa 2001, str. 24
[83] Czekaj J., *Metody zarządzania informacją w przedsiębiorstwie*, Kraków 2000, str. 17.

Pojęcie informacji w czterech znaczeniach: jako rzecz, wielkość mierzalną, potencjał i jako zmianę rozpatrzył C. Berman[84]. Informacja jako rzecz jest, według niego, produktem określonego procesu, mającym wykonawcę (źródło informacji) i użytkownika (odbiorcę), i jako taka może być poddawana operacjom takim jak: wytwarzanie, magazynowanie, przesyłanie, przetwarzanie, wymiana, kupno, sprzedaż itp. Informacji można przypisać szereg różnych właściwości: treść, formę, wielkość, wartość, użyteczność i wiele innych. Informacja ma naturę znakową – jest czymś, ma własną postać i strukturę fizyczną. Nie ma znaczenia, jakie tworzywo i jakie procesy zostały wykorzystane do jej wytworzenia – papier, płyta kompaktowa, czy sekwencja drgań powietrza wzbudzanych strunami głosowymi. Podstawą równoważności różnych postaci fizycznych informacji jest zbiór określonych stanów, ich liczba oraz zachodzące między nimi związki. Tworzywo jest jednak niezbędne, by nadać informacji postać zdolną do oddziaływania na adresata, umożliwiającą jej identyfikację i odpowiednia interpretację. Informacja ma swoje odniesienie do określonego stanu rzeczy, tj. przedmiotów, faktów, zdarzeń, zjawisk, związków pomiędzy nimi, a także stanów ciała i psychiki oraz ma odbiorcę (rzeczywistego lub potencjalnego, indywidualnego lub zbiorowego).

Badanie informacji jako wielkości mierzalnej wynika z potrzeby ilościowej charakterystyki wiadomości, niezbędnej w ocenie skuteczności procesu komunikacji. Istnieją bowiem sytuacje i konteksty, w których przekazana wiadomość zawiera za mało lub za dużo informacji (zagadnienie optimum informacji w procesie informowania i komunikowania stanowi jeden z problemów podejmowanych na gruncie ilościowej teorii informacji)[85].

Z ilościowym aspektem informacji koresponduje ujęcie informacji jako potencjału, czyli zdolności informacji do określonej zmiany stanu rzeczy na skutek zmniejszenia lub eliminacji niepewności odbiorcy w odniesieniu do rozważanych przez niego stanów, wybranych ze zbioru stanów możliwych. To ujęcie informacji odgrywa szczególną rolę w procesie podejmowania decyzji.

Znaczenie informacji jako zmiany odnosi się szczególnie do jej roli w kształtowaniu postaw i zachowań, czyli jako czynnika zmniejszającego nieokreśloność, wpływającego na zachowanie się systemu oraz realizację różnych jego funkcji.

---

[84] Berman C., *Informacja i aspekty komunikacji*, „Zagadnienia Naukoznawstwa", nr 3-4, 1991.
[85] Ibidem.

Zmiana stanu odbiorcy przez informację dokonuje się w różny sposób: bezpośrednio, przez jej odniesienie do zamierzonej zmiany, w postaci zalecenia, instrukcji, ostrzeżenia itp. lub pośrednio – przez jej odniesienie do stanu rzeczy będącego przedmiotem poznawania czy opisu, co wiąże się z podnoszeniem poziomu wiedzy i tworzeniem podstaw do racjonalnego działania.

Podstawowym źródłem występujących różnic w określaniu informacji jest fakt, że informacje rozpatruje się przynajmniej w dwóch znaczeniach. W pierwszym znaczeniu informacja traktowana jest jako odbicie tego, co istnieje w sensie materialnym (tzw. relacja odbicia) np. odwzorowanie własności rzeczy, formy związków lub zależności obiektów, zjawisk bądź procesów myślowych. W drugim znaczeniu traktuje się ją jako czynnik określający w pewnym stopniu formę (postać) przyszłych rzeczy i zjawisk (tzw. relacja realizacji). Tak rozumiana informacja służy identyfikacji lub antycypacji i można ją traktować jako miarę zmniejszania stopnia nieokreśloności lub miarę stopnia zorganizowania systemów[86].

Liczne próby zdefiniowania informacji nie przyniosły zadawalającego wyniku. Wszystkie definicje prezentowane w literaturze omawiają jedynie wybrane aspekty informacji. Większość autorów zgodna jest co do tego, że pełne wyjaśnienie istoty informacji może być dokonane na gruncie teorii informacji i winno uwzględniać jej podstawowe aspekty: semantyczny, ilościowy, jakościowy i pragmatyczny. Jednak w wyniku prowadzonych działań badawczych opisano szereg własności informacji. Podsumowując dotychczasowe rozważania przedstawić należy wybrane własności informacji[87].

1. Informacja może istnieć obiektywnie, niezależnie od woli i świadomości ludzi.
2. Informacja może występować w systemie jako „czynnik sprawczy", odnosząc się do zjawisk, które nie występują w chwili obecnej, ani nie występowały w przeszłości, ale pojawią się w przyszłości.
3. Informacja może dotyczyć procesów i zjawisk nierealnych, które w danym systemie nigdy nie zaistniały i nie zaistnieją w przyszłości.
4. Informacja może być doświadczana, choć nie jest posiadana.
5. Zbiór informacji jest „zbiorem" niewyczerpalnym. Informacja, w przeciwieństwie do innych zasobów, nie zużywa się w procesach jej wykorzystania.

---

[86] Czekaj J., *Metody zarządzania informacją w przedsiębiorstwie*, op.cit., str. 16.
[87] Dziuba D. T., *Gospodarki nasycone informacją i wiedzą*, op.cit., str. 26.

6. Informacja może być przetwarzana, powielana i transportowana w czasie i przestrzeni szczególnie za pomocą technik informacyjno-telekomunikacyjnych.
7. Specyficzną cechą informacji jest konieczność jej aktualizacji.
8. Cechą informacji jest jej różnorodność.
9. Informacje mogą podlegać deformacji, zniekształceniom czy też fałszowaniu na skutek świadomego działania człowieka lub zdarzeń przypadkowych.
10. Informację traktujemy jako jedną z podstawowych kategorii ekonomicznych.
11. Informacja musi być wyrażona wiadomością (komunikatem) za pośrednictwem materialnych nośników informacji.

Pełne zrozumienie pojęcia informacji możliwe jest w kontekście zrozumienia jej szczególnych funkcji we współczesnej rzeczywistości. Należą do nich[88]:

- funkcja modelowania (opisywanie) – może być obrazem rzeczywistości, miarą złożoności i różnorodności badanego wycinka rzeczywistości,
- funkcja decyzyjna – może motywować do działania, a więc osiągania pewnych celów,
- funkcja sterująca – buduje się systemy informatyczne (bazy wiedzy i bazy danych) stanowiące podstawę planowania i podejmowania optymalnych lub racjonalnych decyzji,
- funkcja rozwoju wiedzy (cywilizacji) – „dane → informacja → wiedza → mądrość",
- funkcja kapitałotwórcza – obok ziemi, kapitału i pracy,
- informacja jest towarem,
- funkcja kulturotwórcza.

3.2 Klasyfikacja zasobów informacyjnych

Zasoby informacji przechowywane, przetwarzane i dystrybuowana w systemie informacyjnym państwa sklasyfikować można według kilku wskaźników. Pierwszym z nich są źródła informacji – źródła operacyjne lub otwarte. Warto także zauważyć, że zasobem informacyjnym są nie tylko zatomizowane informacje, pochodzące z różnych źródeł rozpoznania, ale także informacje wytwarzane w systemie informacyjnym

[88] Praca zbiorowa, *Zagrożenia dla bezpieczeństwa informacyjnego państwa. Identyfikacja, analiza zagrożeń i ryzyka. Tom I – Raport z badań*, AON, Warszawa 2004, str. 162.

państwa. Informacje przechowywane w systemie pochodzą bowiem nie tylko ze źródeł operacyjnych lub z działań analitycznych skierowanych na źródła otwarte. Przetworzone informacje, analizy i raporty, a także opracowywane na ich podstawie strategie, decyzje i plany stanowią równie cenne zasoby informacyjne systemu.

Można więc zauważyć, że według źródeł, w systemie informacyjnym państwa, zidentyfikować można cztery rodzaje zasobów informacyjnych:

- informacje pochodzące ze źródeł operacyjnych,
- informacje pochodzące ze źródeł otwartych (prasa, radio, telewizja, Internet, opracowania i raporty naukowo-badawcze itp.),
- informacje wygenerowane wewnątrz systemu:
  - analizy,
  - raporty,
  - strategie,
  - plany,
  - decyzje,
- informacje pochodzące od partnerów (współpracujących służb specjalnych i policyjnych innych państw, rządów i ich administracji).

Kolejna klasyfikacja, którą należy wskazać, to klasyfikacja dotycząca stopnia niejawności informacji, które wchodzą w skład danego zasobu informacyjnego. Klasyfikacje takie opisywane są w aktach prawnych, stanowiących ramy i podstawy systemu ochrony informacji niejawnych, jednak, aby zrozumieć sposób funkcjonowania takiej klasyfikacji, skuteczniejsze będzie przedstawi cienie jej w formie opisu poszczególnych kategorii informacji[89]:

- informacja jawna (publiczna) – informacje, do której wszyscy mogą uzyskać dostęp; informacja ta może nie być stale dostępna (na przykład w powszechnie dostępnych zbiorach, sieciach informacyjnych, lecz zostanie udostępniona na żądanie każdego, kto takie żądanie sformułuje;

[89] *Information Management. Information Security Classification, Government of Alberta*, Alberta 2005, tekst dostępny na stronie o adresie [http://www.im.gov.ab.ca/publications/pdf/InfoSecurityClassification.pdf].

- informacje przeznaczone do użytku wewnętrznego: informacja, która mogłaby spowodować szkody, jeśli ujawniona zostałaby poza obrębem systemu informacyjnego właściciela informacji; dostępna jest dla osób zatrudnionych (członków organizacji) oraz upoważnionych osób spoza organizacji na podstawie zasady *need-to-know* (potrzeby informacji);
- informacje o poufne: informacja, której ujawnienie mogłoby spowodować poważne szkody dla organizacji i jej funkcjonowania; dostęp do niej ściśle przypisany jest do osób, funkcji lub ról i zadań realizowanych w organizacji;
- informacje tajne: informacje, których ujawnienie mogłoby spowodować katastrofalne szkody lub sprowadzić zagrożenie dla bezpieczeństwa oraz życia i zdrowia osób; dostęp do nich ograniczony jest do wąskiej grupy osób oraz do konkretnych stanowisk w organizacji.

Kolejny sposób klasyfikowania zasobów informacyjnych, to klasyfikacja pod względem krytyczności zasobów. Odnosi się ona do stopnia, w jakim utrata informacji zagrozi realizacji zadań przez posiadacza lub dysponenta zasobu[90]:

- zasoby pochodne: zasoby, które zaczerpnięte zostały z informacji przechowywanych w innych systemach i na ich podstawie mogą zostać odtworzone; ich utrata jest zatem kłopotliwa, ale nie wpływa na prowadzone działania;
- zasoby nie-krytyczne: zasoby, które mogą zostać odtworzone na podstawie informacji krytycznych; inaczej, niż w wypadku informacji pochodnych ich jedyna wersja, to wersja danego systemu informacyjnego, ale mogą zostać ponownie wytworzone na podstawie informacji krytycznych; ich utrata może spowodować zakłócenie działania systemu;
- zasoby krytyczne: zasoby, których dostępność bezpośrednio wpływa na funkcjonowanie systemu, a ich utrata może spowodować brak jego funkcjonalności lub co najmniej utratę zaufania partnerów;
- zasoby wpływające na życie / zdrowie: w niektórych systemach przechowywane są zasoby, których naruszenie lub zakłócenie dostępności

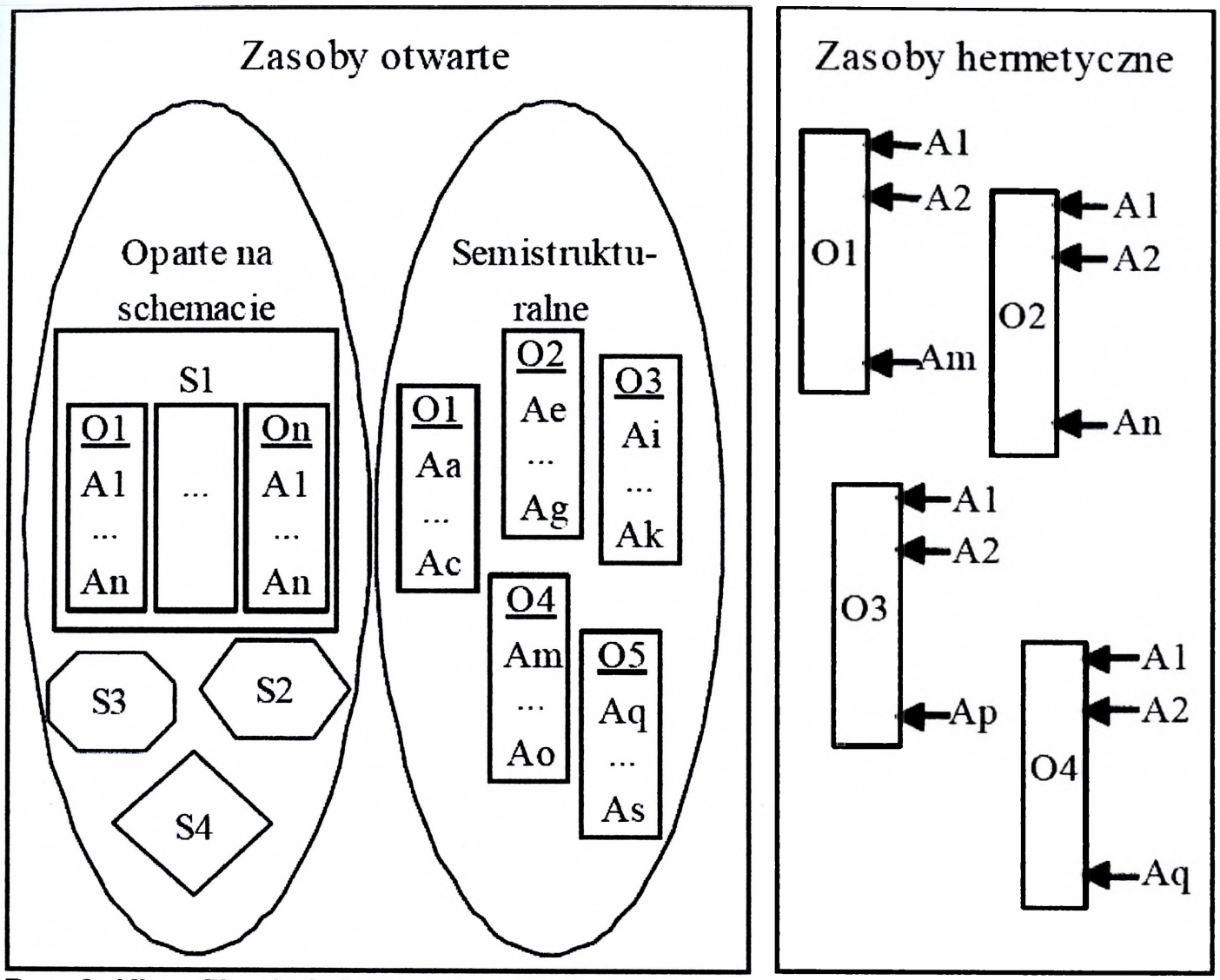
[90] *University of Colorado Boulder (campus) Guidance on Information Asset Classification*, tekst dostępny na stronie o adresie: [http://www.colorado.edu/its/security/assetinventory/UCB%20Guidance%20on%20Information%20Asset%20Classification.pdf].

może spowodować bezpośrednie zagrożenia dla życia lub zdrowia osób (należeć do nich mogą na przykład procesy teleinformatyczne, od których zależy prawidłowe funkcjonowanie kanałów komunikacji lub systemów ochrony i kontroli dostępu).

Kolejna postać klasyfikacji zasobów informacyjnych, to klasyfikacja dotycząca formy uporządkowania i struktury systemu informatycznego, w którym przechowywane są zasoby informacyjne sposobu udostępniania zawartych w nich danych. Według tej klasyfikacji zasoby dzielą się na[91]:

- zasoby otwarte, których wewnętrzna struktura przeszukiwana jest podczas wyszukiwania informacji w systemie; w procesie tworzenia zapytań mogą być używane tylko niektóre atrybuty takich zasobów; dane i informacje będące przedmiotem wyszukiwania w zasobach otwartych można podzielić m.in. na:
  - dane atomowe dotyczące pojedynczej wartości danego obiektu,
  - pojedyncze wartości dotyczące zbioru obiektów,
  - wiele wartości dotyczących jednego obiektu,
  - zbiory wartości atomowych dotyczące zbioru obiektów,
  - dane porównawcze, wybierające obiekty na podstawie podobieństwa lub różnic w stosunku do wskazanego obiektu;
- zasoby hermetyczne, które stanowią zamkniętą całość; w wyniku zapytania użytkownikowi dostarczany jest cały zasób, bez przeszukiwania jego wewnętrznej struktury; w wypadku takich zasobów ich atrybuty używane są do generowania zapytania, ale nie stanowią jego przedmiotu; atrybutem zasobu hermetycznego może być rodzaj zasobu (tekst, obraz, zdjęcie, multimedia), nazwisko lub nazwa autora, data utworzenia itp.

[91] Put D., *Integracja zasobów informacyjnych w systemach heterogenicznych* [w:] *Bazy Danych: Rozwój metod i technologii,* Kozielski S., Małysiak B., Kasprowski P., Mrozek D. (red.), WKŁ 2008, tekst dostępny na stronie o adresie [http://zti.inf.polsl.pl/BDAS/2008/BDAS%6008%20-%20Integracja%20zasob%C3%B3w%20informacyjnych%20w%C2%A0systemach%C2%A0heterogenicznych.pdf?Id=523&val=1].



Rys. 8: Klasyfikacja informacji rozproszonej
(S – system, O – Obiekt, A – atrybut)
Źródło: Put D., *Integracja zasobów informacyjnych w systemach heterogenicznych*, op. cit.

3.3 Wartość i użyteczność informacji

Informacja, jak starano się wykazać powyżej, pełni istotną funkcję w wielu obszarach funkcjonowania współczesnej cywilizacji – w tym w obszarze zapewniania bezpieczeństwa współczesnego państwa. Niemniej jednak, aby stwierdzenie to zachowywało swoją prawdziwość, nie można zapomnieć o tym, że jak każdy inny zasób, musi informacja posiadać pewne cechy, które zapewnią możliwość jej optymalnego wykorzystania.

3.3.1 Jakość informacji

Istnieją zestawy cech, charakteryzujących informację, pozwalających określać jej jakość. Należą do nich między innymi[92]:

- agregacja (poziom syntezy informacji),
- aktualność (zgodność informacji ze stanem rzeczywistym),
- celowość (zdolność do wyznaczania norm sterujących w procesie sterowania),
- wartość (spowodowanie zmiany wartości sytuacji decyzyjnej),
- decyzyjność (stopień wpływu na przebieg procesu decyzyjnego),
- dokładność (stopień uwzględnienie szczegółów w treści informacji),
- jednoznaczność (stosowanie jednoznacznego języka oraz precyzyjnie określonych pojęć),
- komunikatywność (ilość pracy niezbędnej dla nadania jej przez odbiorcę formy umożliwiającej wnioskowanie i podjęcie decyzji),
- pełność (stopień likwidacji niepewności decydenta w procesie zarządzania),
- porównywalność (możliwość porównania informacji z innymi informacjami),
- prawdziwość (zgodność treści informacji z rzeczywistym przebiegiem opisywanego przez nią zdarzenia),
- precyzyjność (stopień jednoznaczności terminologii użytej przez informację),
- prospektywność (stopień antycypacji przebiegu planowanych zdarzeń),
- rzetelność (brak zniekształceń intencjonalnych w treści informacji),
- wiarygodność (brak deformacji informacji),
- wierność (informacja o zbiorze oryginałów jest taka sama, jak w zbiorze obrazów),
- źródłowość (pochodzenie informacji z bezpośredniej lub pośredniej obserwacji).

---

[92] Niedźwiedziński M., *Cechy informacji – próba systematyzacji*, „Systemy informatyczne", 1987, nr 1 [cyt. za: Praca zbiorowa, *Zagrożenia dla bezpieczeństwa informacyjnego państwa,* op.cit,. str. 164].

Podsumowując, mianem jakości informacji określić można cechę informacji wyrażającą stopień spełnienia wymagań stawianych przez system decyzyjny w zakresie aktualności, pełności i niezawodności.[93] W tym kontekście jako aktualność (terminowość) informacji rozumiemy cechę informacji wyrażającą fakt otrzymania przez decydenta informacji w pożądanym (wymaganym) czasie. Poprzez pełność (kompletność) informacji rozumiemy cechę informacji wyrażającą zawartość rzeczywistych informacji o stanie rzeczy w danej wiadomości. Ostatnia z wymaganych cech, niezawodność (prawidłowość) wyrażą stopień wpływu zniekształceń i zakłóceń na informacje dostarczane przez system informacyjny ich odbiorcom (decydentom).

Z bogactwa podanych powyżej cech określających jakość informacji, a także wziąwszy pod uwagę fakt, że nie jest to jedyne zestawienie cech informacji napotykane w literaturze[94], trzeba stwierdzić, że poprawne określenie ilościowych miar wartości informacji jest raczej niemożliwe[95].

Niemniej jednak należy poświęcić odpowiednią uwagę temu, aby informacje, na których opierać ma się planowanie najważniejszych przedsięwzięć realizowanych w ramach systemu, a także zarządzanie systemem i alokacja jego zasobów, były informacjami zapewniającymi optymalizację powyższych działań. Dlatego właśnie należy upewnić się, że informacje, które stanowią zasób w danym systemie bezpieczeństwa są: wartościowe, użyteczne i mają wysoką jakość.

3.3.2 Użyteczność informacji

Użytecznością informacji nazywa się właściwość wyrażającą wpływ informacji na trafność podejmowanych decyzji (skuteczność zarządzania)[96]. Cecha ta związana jest z procesem podejmowania decyzji. Osoba podejmująca decyzję, może podejmować ją w sytuacji dysponowania określonymi informacjami, lub też w sytuacji braku tych informacji. Przyjmuje się, że każda informacja, która zmniejsza niewiedzę w obszarze dotyczącym podejmowanej decyzji, jest informacją użyteczną, zaś ta jej użyteczność zależy od konkretnego problemu decyzyjnego. Jako bardziej użyteczną

---

[93] *Zagrożenia dla bezpieczeństwa informacyjnego państwa*... , op. cit. str. 173.
[94] Patrz: Kisielnicki J., *Kryteria jakości systemów informatycznych funkcjonujących w gospodarce narodowej*, „Systemy informatyczne", 1987, nr 1 [cyt. za: *Zagrożenia dla bezpieczeństwa informacyjnego*..., op.cit, str. 166].
[95] *Zagrożenia dla bezpieczeństwa informacyjnego państwa*... , op. cit. str. 167.
[96] Ibidem, str. 168

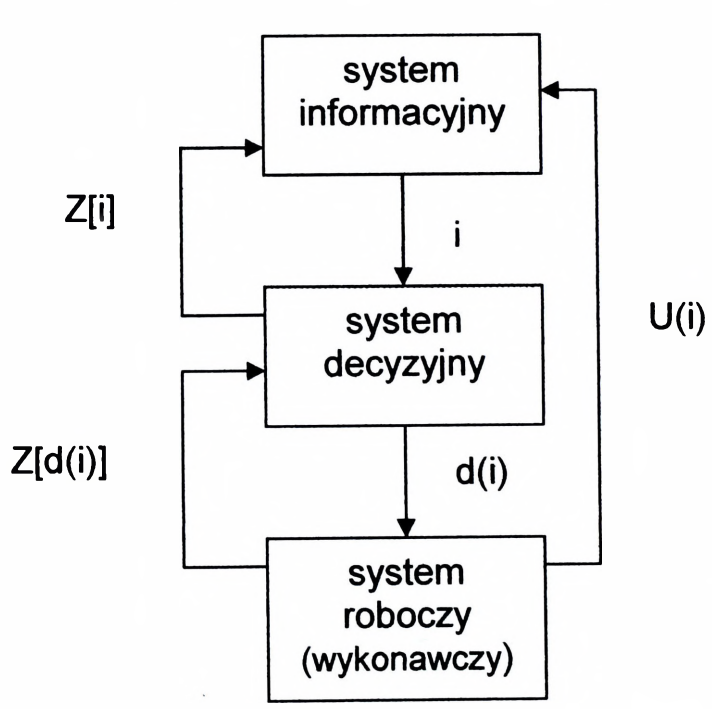
można określić informację, gdy przy różnym stanie rzeczy opisywanej przez nią, skutki działania są bardzo zróżnicowane.

Użyteczność informacji wyrazić można również poprzez efektywność systemu (rys. 9)[97]. Jeżeli przyjmiemy, że:

- **d** – decyzja,
- **i** – informacja,
- **d(i)** – decyzja podjęta na podstawie informacji,
- **E** – efektywność systemu,
- **E(d)** – efektywność systemu w wypadku podjęcia decyzji w wypadku braku informacji,
- **E[d(i)]** - efektywność systemu w wypadku podjęcia decyzji w wypadku posiadania informacji,

to użyteczność informacji „i" wyniesie:

$$E_i = E[d(i)] - E(d)$$



Rys. 9: Ilustracja korelacji pomiędzy użytecznością informacji i efektywnością systemu informacyjnego
Źródło: *Zagrożenia dla bezpieczeństwa informacyjnego państwa*, op. cit. str. 172.

Przyjmuje się także, że system informacyjny uzyskuje pewien zysk po udostępnieniu informacji „i":

[97] Ibidem, str. 170

- **Z[i]** – zysk po udostępnieniu informacji **i**,
- **Z_0[i]** – zysk bez udostępnienia informacji **i**

zatem użyteczność „brutto" informacji „i" wyniesie:

$$Z_i = Z[i] - Z_0[i].$$

Użyteczność informacji ustala się zatem ze względu na problem decyzji oraz kryterium decyzji. Wyraża ta cecha pragmatyczny aspekt informacji. Ocena użyteczności decyzji ze względu na kryterium decyzji oznacza, że w zależności od kryterium podejmowania decyzji lub oceny szansy realizacji poszczególnych stanów rzeczy decyzja informacja może mieć równą użyteczność.

Jednocześnie, wziąwszy pod uwagę fakt, że samo podejmowanie decyzji wymaga pewnej dozy arbitralności, arbitralne staje się także wartościowanie informacji ze względu na jej przydatność.[98]

3.3.3 Wartość informacji

Mianem wartości informacji określa się cechę kompleksową, wyrażającą związki między użytecznością i jakością rozpatrywane z punktu widzenia wpływu informacji na efektywność działania.

Rys. 10: Wpływ jakości i użyteczności informacji na jej wartość
Źródło: *Zagrożenia dla bezpieczeństwa informacyjnego państwa*, op. cit., str. 172.

Jest to zarazem taka własność informacji, która wyrażą stopień spełnienia potrzeb i wymagań użytkowników informacji w procesie działania[99]. Wartość informacji powinna określać bezwzględną wartość uzyskaną przez informacje w procesie działania, a więc jej wartość społeczną. Należy przy tym podkreślić względną niezależność ilości informacji zawartej w określonej wiadomości i jej wartości. Może bowiem

[98] *Zagrożenia dla bezpieczeństwa informacyjnego państwa*, op. cit. str. 172.
[99] *Zagrożenia dla bezpieczeństwa informacyjnego państwa*, op. cit. str. 180.

wystąpić sytuacja, w której wartość wzrasta w zależności od wzrostu ilości informacji do pewnego maksimum, po czym może zacząć wykazywać tendencję malejącą. Zjawisko to wynika z ograniczonych możliwości użytkownika co do wykorzystania zbyt dużej ilości informacji dostarczonych w danej jednostce czasu. Z tego względu – dla uniknięcia zjawiska szumu informacyjnego – zadaniem systemu informacyjnego może niekiedy stać się selekcja informacji, która zwiększy wartość informacji i stopień ich wykorzystania.

Zauważyć należy także, że wartość informacji może być wyrażona, jak się uważa, jedynie w sposób względny. Przy założeniu, że system decyzyjny dysponuje danym zbiorem informacji, który podzielić można na semantycznie niezależne podzbiory, w celu określenia wartości informacji zawartych w poszczególnych podzbiorach przeprowadzić można działanie, które pozwoli na określenie reguł, które dla dowolnej decyzji i dla dowolnych wydzielonych podzbiorów informacji pozwalają jednocześnie stwierdzić zachodzenie jednej i tylko jednej zależności, określającej wartość informacji zawartych w poszczególnych podzbiorach z punktu widzenia danej decyzji. W ten sposób rodzina podzbiorów zostaje częściowo uporządkowana ze względu na ich wartość dla podjęcia określonej decyzji.

Wartość informacji może być – jak się uważa – wyrażona tylko w sposób względny. Z punktu widzenia procesu decyzyjnego istotny jest taki komunikat, który wskazuje na istnienie problemu lub prawdopodobieństwo jego wystąpienia, a także możliwości jego potencjalnego rozwiązania przez decydenta.

Aby określony komunikat był użyteczny dla decydenta, powinien zawierać dane dotyczące następujących kwestii:

- istoty problemu (analiza merytoryczna),
- lokalizacji przestrzennej problemu,
- lokalizacji problemu w czasie,
- najistotniejszych przyczyn powstania problemu,
- aktualnych i potencjalnych skutków problemu,
- stopień powtarzalności (zrutynizowania problemu)[100].

Jeśli potrzeby informacyjne decydenta przedstawione zostanę w zaprezentowany wyżej sposób, to można zauważyć, że są one wszechstronne, wynikają bowiem

[100] *Zagrożenia dla bezpieczeństwa informacyjnego państwa…* , op. cit. str. 184.

z racjonalnych przesłanek decyzyjnych. Jednocześnie podkreślić trzeba, że stanowić one powinny punkt odniesienia do badania wartości informacji w każdej konkretnej sytuacji decyzyjnej dla określonego decydenta przy określonym problemie decyzyjnym, poprzez zawartość informacyjną komunikatów.

3.4 Informacyjny zasób strategiczny w systemie bezpieczeństwa państwa

Angielska klasyczna ekonomia polityczna uwzględnia trzy podstawowe zasoby: ziemię, kapitał i pracę. Wraz z rozwojem społeczeństw określanych mianem „społeczeństw informacyjnych" oraz gospodarek nasyconych wiedzą, wyróżniono kolejną kategorię ekonomiczną, czyli informację[101]. Według teoretyków należy traktować ją jako zasób podobny do innych zasobów, tak jak pieniądz. Mają one wartość i wymagają ponoszenia określonych kosztów podczas ich wykorzystywania.

Aby zapewnić możliwość posługiwania się – swobodnego – informacją w systemie bezpieczeństwa państwa, konieczne jest zapewnienie mu bezpieczeństwa informacyjnego właśnie. Aby w pełni zrozumieć znaczenie tego pojęcia, odnieść się należy przede wszystkim do pierwotnego w stosunku do niego pojęcia bezpieczeństwa narodowego.

Bezpieczeństwo narodowe, nazywane również bezpieczeństwem państwa, najczęściej rozumiane jest jako jedna z podstawowych funkcji każdego państwa.[102] Obejmuje ona problematykę przeciwstawienia się wszelkim zagrożeniom zewnętrznym oraz wewnętrznym dla istnienia oraz rozwoju narodu i państwa. Państwo w trosce o własne bezpieczeństwo narodowe ustala zbiór wartości wewnętrznych, które jego zdaniem powinny być chronione przed zagrożeniami. Należą do nich:

a) przetrwanie (biologiczne przeżycie ludności, narodu jako grupy etnicznej oraz państwa jako niezależnej jednostki politycznej),
b) integralność terytorialna,
c) niezależność polityczną (w sensie ustrojowym, samowładności i swobody afiliacji),

---

[101] Dziuba D. T., *Gospodarki nasycone informacją i wiedzą*, op. cit., str. 13.
[102] Kuźniar R., *Niebezpieczeństwa nowego paradygmatu bezpieczeństwa* [w:] Kuźniar R., Lachowski Z. (red.), *Bezpieczeństwo międzynarodowe czasu przemian. Zagrożenia – koncepcje – instytucje*, Warszawa 2003, PISM, s. 210.

d) jakość życia, na którą składają się: standard życia, szczebel rozwoju społeczno – gospodarczego, zakres praw i swobód obywatelskich, system kulturalny, stan środowiska naturalnego, możliwości i perspektywy dalszego rozwoju[103].

Współcześnie coraz wyraźniej występuje tendencja do poszerzania przez państwa treści pojęcia bezpieczeństwa, zarówno jeśli chodzi o wartości wewnętrzne podlegające ochronie, jak i środki ochrony stosowane przez jego narodową politykę bezpieczeństwa. Tendencja ta jest skutkiem rewolucji naukowo-technicznej, dokonujących się procesów internacjonalizacji różnych dziedzin życia społecznego i wzrostu współzależności pomiędzy podmiotami na forum międzynarodowym.

Na przełomie XX i XXI wieku obserwujemy wzrost wagi kolejnej, informacyjnej płaszczyzny bezpieczeństwa narodowego – bezpieczeństwa informacyjnego, które razem z bezpieczeństwem ekonomicznym staje się priorytetowym aspektem bezpieczeństwa[104]. Dokonujące się za sprawą cyfrowej rewolucji przemiany techniczne i organizacyjne będą powodowały nowe zróżnicowanie między państwami i narodami, wynikające ze stopnia wprowadzenia nowych rozwiązań do praktyki gospodarczej i do procesów funkcjonowania każdego społeczeństwa. Tempo przemian jest silnie uwarunkowane ekonomicznie i społecznie, a ważnymi atutami w „grze o jutro" jest aktualny potencjał gospodarczy, posiadana infrastruktura informacyjna, wielkość i dynamika rynku, innowacyjność i otwartość na zmiany oraz społeczne zdolności adaptacyjne, a wreszcie poziom i jakość wykształcenia, struktura wiekowa społeczeństwa oraz świadomość i determinacja działania elit. Przepływ i wymiana informacji według prognoz, staną się podstawą dla sprawnego funkcjonowania firm, administracji wszystkich szczebli oraz życia jednostek. Staną się, jak utrzymuje Alvin Toffler, „naczelnym czynnikiem wytwórczości i władzy człowieka" w społeczeństwie informacyjnym[105]. Powstanie takiego społeczeństwa stanowi wyzwanie dla bezpieczeństwa narodowego, a nowa technika to nowe pole potencjalnego rozpoznania, walki interesów, a nawet otwartego konfliktu, zmuszające do posiadania skutecznego systemu bezpieczeństwa informacyjnego.

---

[103] Szerzej patrz także: Stemplowski R., *Horyzont poznawczy i polityczny pojęcia „bezpieczeństwo państwa"* [w:] Kuźniar R., Lachowski Z. (red.), *Bezpieczeństwo międzynarodowe czasu przemian. Zagrożenia – koncepcje – instytucje*, Warszawa 2003, PISM, s. 255.
[104] Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Warszawa 2006, Wyd. Naukowo – Techniczne, s. 27.
[105] Toffler A., *Budowa nowej cywilizacji. Polityka trzeciej fali*, Poznań 1996, Zysk i S-ka, s. 78.

Przez praktyków, bardzo często bezpieczeństwo informacyjne rozumiane jest jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania. Środki bezpieczeństwa podejmowane są w celu zapewnienia poufności, integralności i dostępności informacji. Ich celem jest wyeliminowanie zagrożenia dla informacji. Wskazuje to, że przytoczona wyżej definicja bezpieczeństwa informacyjnego sformułowana została w ujęciu negatywnym.

W miarę intelektualnego rozwoju i politechnizacji życia informacje zaczęły nabierać coraz większych wartości[106]. Ich posiadanie stało się warunkiem lepszej i bezpieczniejszej egzystencji. Na tym też tle pojawiła się konkurencja. Informacje zaczęto coraz bardziej chronić jako dobro materialne. Chęć stworzenia sobie podobnych do innych lub lepszych warunków życia stworzyła potrzebę zdobywania informacji. Zrodził się zatem swoisty rodzaj walki — jedni, możliwymi dla siebie sposobami, dążą do zdobycia informacji, a drudzy — z podobnym zaangażowaniem — starają się im to udaremnić. W postępowaniu takim występuje sprzeczność celów i działań, czyli najbardziej dystynktywnych cech, które kojarzą się z desygnatem pojęcia ,,walka". Można by powiedzieć, że przedmiotem tej walki stała się informacja, a narzędziami — wszelkie środki dostosowane do jej zdobywania, zakłócania i obrony. Walka taka nazywana jest walką informacyjną[107].

Wobec wzrostu znaczenia informacji ujęcie negatywne bezpieczeństwa informacyjnego jest niewystarczające dla zapewnienia bezpieczeństwa narodowego. Każda płaszczyzna bezpieczeństwa narodowego staje się coraz bardziej zależna od swobodnego przepływu informacji i od zachowania systemów bazujących na informacjach. Wojsko, gospodarka, energetyka, media, systemy finansowe i transportowe są szczególnie uzależnione od systemów informatycznych. Już dziś stanowią one kluczowe elementy procesu podejmowania decyzji w wielu organizacjach cywilnych i wojskowych. Ich dotychczasowy rozwój i zakresy wdrożeń pozwalają prognozować, że obszary zastosowań informatycznych będą obejmować coraz większe przestrzenie funkcjonalne. Teoretycznie został stworzony niemalże nieograniczony dostęp do ogromnych zbiorów informacji, a w tym: finansowych, przemysłowych, marketingo-

---

[106] Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, op.cit., str. 33.
[107] *Zagrożenia dla bezpieczeństwa informacyjnego państwa*, op. cit., s. 64.

wych, technologicznych, wojskowych i innych. Niezbędne dla bezpieczeństwa państwa staje się wprowadzenie polityki bezpieczeństwa informacyjnego zapewniającej ochronę istniejących systemów, ale również gwarantującej państwu i podmiotom, które chroni, posiadanie, przetrwanie i swobodę rozwoju „społeczeństwa informacyjnego". Takie ujęcie bezpieczeństwa informacyjnego ma charakter pozytywny.

Środki polityki bezpieczeństwa informacyjnego budowane w oparciu o ujęcie pozytywne muszą uwzględniać, że:

- informacja stanowi zasób strategiczny państw i organizacji XXI wieku,
- informacja i wynikająca z niej wiedza oraz technologie informatyczne staną się podstawowym czynnikiem wytwórczym,
- większość dochodu państwa zostanie uzyskana z szeroko rozumianego sektora informacyjnego,
- procesy decyzyjne w innych sektorach gospodarki i życia społecznego uzależnione będą od systemów przetwarzania i przesyłania informacji,
- zakłócenie prawidłowości działania systemów informacyjno – sterujących nie wymaga wysokich nakładów materialnych,
- rywalizacja pomiędzy przeciwnikami przeniesie się na płaszczyznę walki informacyjnej[108].

Potrzebę wypracowania skutecznych środków polityki bezpieczeństwa informacyjnego wymusza wzrastająca informatyzacja sił zbrojnych, zwiększające się ciągle możliwości systemów łączności, ze wzrastającym nasyceniem wojsk nowymi technikami walki – w tym szczególnie bronią precyzyjnego rażenia[109]. Jak widać, zarówno na Zachodzie jak i Wschodzie współczesna walka informacyjna najbardziej łączona jest z walką zbrojną. Wyrażane są nawet poglądy – z czym trzeba się zgodzić – że w przyszłości ta forma zmagań stać się może ekwiwalentem innych rodzajów walk, w tym i walki zbrojnej. Można więc przewidywać, że obserwowany w tym zakresie wyścig może doprowadzić w przyszłości do tego, że walka informacyjna stanie się nawet substytutem wojny. Umiejętnie prowadzona jest z pewnością w stanie naru-

---

[108] *Zagrożenia dla bezpieczeństwa informacyjnego państwa*..., op. cit, s. 6.
[109] Strasburger D., *Walka informacyjna w wojnie asymetrycznej* [w:] Nowacki G. (red.), *Informacja w walce zbrojnej, Materiały z sympozjum naukowego*, Warszawa 2002, AON, s. 162 i dalsze.

szać szeroko rozumiane proporcje strategiczne i kształtować sceny polityczne, tak w aspekcie międzynarodowym, jak i wewnętrznym[110].

Współczesność wchłonęła też w sferę walki informacyjnej media, które w sposób dla siebie nieświadomy mogą być wykorzystywane przez przeciwnika jako narzędzia skutecznego zakłócania informacyjnego[111]. Szczególnie dogodne do tego warunki istnieją w państwach demokratycznych, gdzie wolna prasa, goniąc za sensacjami dnia codziennego, jest niezwykle podatna na dezinformowanie i błyskawiczne rozprzestrzenianie wszelkich informacji, które mogą przynosić korzyści określonemu przeciwnikowi. Z tych samych powodów może stać się niepostrzeżenie źródłem upływności informacyjnej. Współczesne środki walki informacyjnej są dostosowane do zdobywania informacji przeróżnymi metodami i technikami. Nawet wśród zaprzyjaźnionych państw trwa w tym zakresie ciągła konkurencja i sądzić należy, że nigdy nie zostanie zaniechana. Uzyskana w tym zakresie przewaga spełniać może nie tylko funkcje wspomagające walkę zbrojną, ale może również spełniać funkcje odstraszania przez unaocznianie przeciwnikowi braku realnych perspektyw do osiągnięcia łatwych korzyści. Już dziś bardzo skutecznymi środkami walki informacyjnej stać się mogą wszystkie te, które dostosowane są do zdalnego wprowadzania wirusów komputerowych do sieci informacyjnych, dostosowanych programowo do samopowielania się i szybkiego rozprzestrzeniania. Ogromne znaczenie mogą mieć również tak zwane bomby logiczne, które jako odpowiednio opracowane aplikacje programowe, będą dostosowane do uaktywniania się na określone wcześniej sygnały lub według zaprogramowanych reżimów czasowych. Skutecznym przedsięwzięciem może być także blokowanie wymiany informacji i szerzenie dezinformacji w torach transmisyjnych za nieświadomym pośrednictwem środków masowego przekazu. Współczesne narzędzia walki informacyjnej stwarzają możliwości podejmowania skutecznej działalności ukierunkowanej na sterowanie procesami decyzyjnymi przeciwnika, nawet w skali państwowej[112]. Wprowadzenie do publicznego i utajonego systemu informacyjnego danego państwa złożonych zbiorów precyzyjnie dobranych prawdziwych i sfałszowanych danych może tworzyć z góry zaplanowane nastroje społeczne i klimat polityczny, które w efekcie spowodują podejmowanie decyzji zgodnych z oczekiwaniami sprawcy tych manipulacji. Współczesne środki walki informa-

[110] Ibidem, s. 163.
[111] Jabłoński W., *Kreowanie informacji. Media relations*, op. cit., s. 67.
[112] *Zagrożenia dla bezpieczeństwa informacyjnego państwa…*, op. cit., s. 116.

cyjnej wskazują, jak nigdy dotąd, na konieczność uwzględniania tego problemu nie tylko w programach reformowania sił zbrojnych, ale również i w funkcjonowaniu państwa. Potrzeba taka wynika chociażby z tego, że ich użycie jest możliwe nie tylko w okresie zagrożenia i wojny. Już w okresie pokoju mogą być podejmowane w tym zakresie dobrze zamaskowane wysiłki ukierunkowane nie tylko na zdobywanie informacji, ale również na powodowanie niepokojów, zamieszek i kryzysów rządowych, co w atmosferze ciągle trwającej globalnej konkurencji wydaje się być bardzo realne. Nie można też wykluczyć, że w ramach tego mogą być stosowane różnego rodzaju akty terrorystyczne sterowane przez jakieś państwo. Ta forma przemocy może być prowadzona chociażby siłami służb specjalnych, o których wiadomo, że są stale na całym świecie doskonalone i rozwijane. Może to nawet stanowić ekwiwalent otwartych agresji, co z coraz większą intensywnością daje się obserwować już teraz.[113]

Wysiłki walki informacyjnej mogą być ukierunkowane na podrywanie autorytetu zaatakowanego państwa na arenie międzynarodowej, czy też podrywanie jego zaufania sojuszniczego. W szerokim zakresie może być włączana do tego dyplomacja, handel zagraniczny i media. Na oddziaływanie takie szczególnie jest podatna sfera ekonomiczna, polityczna i społeczna. W działaniach tych mogą być również prowokowane incydenty międzypaństwowe, powodujące napięcia społeczne w stosunkach dobrosąsiedzkich. Każdy ma jakieś sekrety, skrzętnie ukrywane przed otoczeniem, i każdy też chciałby posiąść informacje o warunkach najlepszej egzystencji w określonym otoczeniu. Przy większych strukturach organizacyjnych zbiory tajemnic i zapotrzebowań na informacje rozrastają się. W przypadku państwa czy koalicji liczba elementarnych postaci tajemnic i zapotrzebowań na informacje jest przeogromna i znaczeniowo niezmiernie złożona. Z tego też względu dbałość o bezpieczne warunki egzystencji państwa wiąże się nierozerwalnie z potrzebą ciągłego rozpoznawania otoczenia i bronienia dostępu do własnych tajemnic.

[113] Herman M., *Potęga wywiadu*, Warszawa 2002, Bellona, s. 302.

2.3 Informacyjny zasób strategiczny w systemie przeciwdziałania terroryzmowi – podejście reaktywne i proaktywne w przeciwdziałaniu terroryzmowi

Terroryzm jest przede wszystkim metodą działania, która służy osiąganiu celów politycznych. Jest ona skonstruowana w taki sposób, aby nieść dalekosiężne skutki, do których należeć mają reperkusje psychologiczne[114]. Podstawowym narzędziem, którym posługuje się terroryzm jest przemoc lub też groźba użycia przemocy. Trzeba przy tym pamiętać, że właściwym celem ataku terrorystycznego nie są nigdy tylko osoby pokrzywdzone podczas samego ataku terrorystycznego. Celem są także ludzie, którzy ten atak obserwują. Osoby te, obywatele poszczególnych państwa, to jednocześnie wyborcy – wyborcy, którzy na mocy umowy społecznej oddali swój głos na rządzących, oczekując w zamian zaspokajania pewnych podstawowych potrzeb, spośród których najbardziej prominentną jest potrzeba bezpieczeństwa i wolności od strachu.

Zwalczanie terroryzmu, a zwłaszcza skuteczne jego zwalczanie wymaga wzięcia pod uwagę konieczności budowy systemu bezpieczeństwa. System ten musi spełniać jeden, podstawowy warunek, który stanowi o jego skuteczności. Musi być na tyle szczelny, żeby do minimum ograniczyć prawdopodobieństwo potencjalnego ataku terrorystycznego.

Istnieją dwa podstawowe podejścia w zwalczaniu terroryzmu - reaktywne i proaktywne[115]. Zgodnie z reaktywnym podejściem oczekuje się na zamach terrorystyczny i liczy się na to, iż będzie się w stanie, w miarę rozwoju wydarzeń, ograniczyć straty w ludziach i rozmiarze zniszczeń własności publicznej oraz prywatnej. Wadą tego podejścia jest to, iż działa się już po skutku, gdy poniesiono straty. Inna opcją jest podejście proaktywne. Według niego można przewidywać nadchodzące zamachy terrorystyczne i przygotowywać się na nie. Działanie proaktywne zwiększa prawdopodobieństwo zapobiegania atakom terrorystycznym i umożliwia uniknięcie jakichkolwiek strat w ludziach jak szkód dotyczących mienia.

---

[114] Borkowski R., *Terroryzm ponowoczesny. Studium z antropologii polityki*, Wydawnictwo Adam Marszałek; Toruń 2006, s. 38.
[115] Liedel K., *Działania proaktywne w zwalczaniu terroryzmu*, „Terroryzm: zagrożenia – prewencja – przeciwdziałanie", nr 1/2008, s. 34.

Dotychczasowe doświadczenia wskazują, że proaktywne podejście do terroryzmu jest najlepszą z opcji. Zapewnia najskuteczniejszy sposób prewencji zamachów terrorystycznych. Dzięki temu możemy zminimalizować możliwe poniesione straty.

Zbieranie informacji jest zagadnieniem kluczowym dla proaktywnego podejścia do zwalczania terroryzmu. Nie mając świadomości tego, jakie zagrożenie stanowią dla państwa poszczególne grupy i organizacje terrorystyczne, a także nie wiedząc jakie potencjalne działania mają w planach, nie jesteśmy w stanie przedsięwziąć żadnych kroków dla zapobieżenia zagrożeniom. Z tego powodu gromadzenie informacji oraz ich analiza ma kluczowe znaczenie dla skuteczności zwalczania działalności terrorystycznej. Działania takie bowiem mają na celu rozpoznawanie przygotowań do zamachu i niedopuszczenie do jego wykonania.

Stąd, z punktu widzenia społeczeństwa, gromadzenie i właściwe zarządzanie informacją w ramach proaktywnego podejścia do przeciwdziałania terroryzmowi są najlepszą metodą zwalczania zjawisk o charakterze terrorystycznym. Jednak, aby działania prowadzone w tej płaszczyźnie były skuteczne, współczesne państwo musi zapewnić rozwiązania prawno-organizacyjne niezbędne do prawidłowego i skutecznego prowadzenia działań o charakterze wywiadowczym i rozpoznawczym. Muszą istnieć:

1) instrumenty prawne umożliwiające służbom specjalnym prowadzenie działań w obszarach chronionych prawami i wolnościami człowieka,
2) jednostki organizacyjne zajmujące się badaniem i analizowaniem uzyskiwanych informacji oraz przygotowywaniem materiałów do opracowywania polityki, strategii programów zwalczania terroryzmu,
3) koordynacja obiegu informacji pomiędzy instytucjami zajmującymi się zwalczaniem terroryzmu[116].

Działania służb specjalnych, aby mogły być skuteczne, muszą częściowo odbywać się w obszarze, który chroniony jest w demokratycznych społeczeństwach przed ingerencją państwową. Stąd istotne jest, aby wszystkie podejmowane przez te służby działania były regulowane właściwym aktami prawnymi przez organy ustawodawcze państw oraz ujęte we właściwe, zapewniające skuteczne i zgodne z prawem ramy organizacyjne. W obliczu rosnącego zagrożenia terroryzmem pojawia się coraz wię-

[116] Ibidem, s. 35.

cej takich rozwiązań prawnych i instytucji, które umożliwiają państwom w sposób proaktywny coraz skuteczniejszą walkę z terrorystami.

2.3 Wnioski

Współczesne społeczeństwo nie bez powodu określane jest mianem społeczeństwa informacyjnego. Informacja i systemy informacyjne stanowią nie tylko o dobrobycie obywateli współczesnych państw, komforcie ich życia czy dostępnie do wiedzy – nie tylko tej dotyczącej edukacji, ale także każdego innego aspektu funkcjonowania w świecie coraz bardziej zależnym od swobodnych i niezakłóconych przepływów informacji i danych.

Informacja stanowi także o bezpieczeństwie, niezależnie od tego, w jakim aspekcie jest rozpatrywana: ofensywnym – który pozwala gromadzić wiedzę o przeciwniku i jego działaniach, czy defensywnym – który pozwala chronić własne zasoby przed cudzą ingerencją i manipulacją.

Zasoby informacyjne stanowią zatem o efektywności systemu przeciwdziałania terroryzmowi, tak samo, jak niemal każdego innego podsystemu bezpieczeństwa państwa, czy też jego gospodarki i życia społecznego.

Rozdział 4

Zarządzanie zasobami informacyjnymi w systemie przeciwdziałania terroryzmowi

4. 1 Zarządzanie zasobami informacyjnymi

Zarządzanie zasobami informacyjnymi jest środkiem optymalizacji i racjonalizacji procesów informacyjnych w organizacji (IRM – *Information Resource Management*)[117]. Definicja zarządzania zasobami informacyjnymi nie została ostatecznie sformułowana, jednak wśród najważniejszych prób zdefiniowania tego procesu wymienić należy[118]:

- IRM jest zarządzaniem zasobami informacji – głównym elementem odpowiedzialności strategicznej zarówno warstwy zarządzającej / kierowniczej, jak i użytkowników, a także przede wszystkim tradycyjnego zarządzania systemami informacyjnymi;[119]
- gospodarowanie zasobami informacyjnymi; jego skuteczność określana jest przez zaspokojenie potrzeb informacyjnych użytkowników w sposób ścisły i wyczerpujący, we właściwym czasie i po uzasadnionych kosztach; spełnia następujące funkcje:
  - pozyskiwanie informacji,
  - zabezpieczanie informacji,
  - użytkowanie informacji,
  - rozpowszechnianie i promowanie informacji (w związku z pożytkami płynącymi z posiadania informacji lub możliwości korzystania z nich);[120]

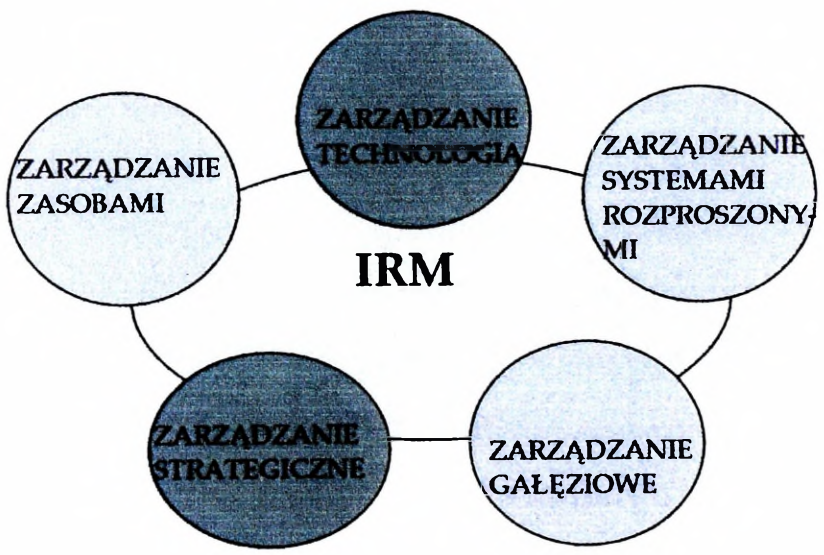
---

[117] Sienkiewicz P., Wieleba R., Wocial J., Kuca M., Skoczylas M., *Wartość informacji w dowodzeniu i zarządzaniu. Metodologia analizy potrzeb informacyjnych*, AON Warszawa 2002, s. 109.
[118] Ibidem, s. 109.
[119] O'Brien J.A., *Management Information Systems, A Managerial End User Perspective*, Irwin, Homewood Ill, Boston 1990 [cyt. za:] Sienkiewicz P., Wieleba R., Wocial J., Kuca M., Skoczylas M., *Wartość informacji w dowodzeniu i zarządzaniu. Metodologia analizy potrzeb informacyjnych,* op.cit., s. 110.
[120] Ward J., Griffiths P. and Whitmore P., *Strategic planning for information systems*, Wiley 1992 [cyt. za:] Sienkiewicz P., Wieleba R., Wocial J., Kuca M., Skoczylas M., *Wartość informacji w dowodzeniu i zarządzaniu. Metodologia analizy potrzeb informacyjnych,* op.cit., s. 110.

- proces w obszarze zarządzania informacją służący do osiągania celu; służy danej instytucji do wykorzystania informacji w traki sposób, aby możliwe było osiągnięcie celu całościowego poprzez wykorzystanie, wdrożenie i optymalizację zasobów informacji; jest menadżerskim połączeniem zbioru informacji z celami i zamierzeniami organizacji.[121]

Można wyróżnić pięć wymiarów zarządzania zasobami informacyjnymi: zarządzanie zasobami, zarządzanie technologią, zarządzanie systemami rozproszonymi, zarządzanie gałęziami oraz zarządzanie strategiczne. Wymiary te określają różne obszary odniesienia do zarządzani całą organizacją. W tym ujęcie przedmiot zarządzania stanowią[122]:

- zasoby informacyjne organizacji (ich rejestrowanie, przetwarzanie, gromadzenie i dostarczanie / dystrybucja),
- technologie komputerowe,
- rozproszone systemy informacyjne,
- gałęzie działalności organizacji,
- strategia informacyjna organizacji.



Rys. 11: Ujęcie ideowe wymiarów IRM
Źródło: O'Brien J.A., *Management Information Systems, A Managerial End User Perspective*, Irwin, Homewood Ill, Boston 1990[123]

---

[121] Burk, C. and Horton, F. *Infomap: a complete guide to discovering corporate information resources*, Englewood Cliffs: N.J. Prentice-Hall 1988 [cyt. za:] Sienkiewicz P., Wieleba R., Wocial J., Kuca M., Skoczylas M., *Wartość informacji w dowodzeniu i zarządzaniu. Metodologia analizy potrzeb informacyjnych*, op.cit., s. 110.
[122] Sienkiewicz P., Wieleba R., Wocial J., Kuca M., Skoczylas M., *Wartość informacji w dowodzeniu i zarządzaniu. Metodologia analizy potrzeb informacyjnych*, op.cit., s. 112.
[123] cyt. za: O'Brien J.A., *Management Information Systems, A Managerial End User Perspective*, Irwin, Homewood Ill, Boston 1990, op.cit., s. 112.

Wśród funkcji zarządzania zasobami informacyjnymi organizacji jako jej zasobami strategicznymi wyróżnić należy[124]:

- *określenie systemu informacyjnego oraz potrzeb informacyjnych organizacji,*
- *stworzenie standardów przygotowania informacji wewnętrznej i zewnętrznej do realizacji celów i zadań organizacji oraz koordynacji obiegu dokumentów w ramach organizacji,*
- *określenie standardów operowania informacją na różnych etapach jej „życia",*
- *dobór odpowiednich technik informacyjnych,*
- *dobór odpowiedniego personelu,*
- *zabezpieczenie informacji przed nieuprawnionym dostępem oraz utratą,*
- *umożliwienie zastosowania informacji do procesu zarządzania organizacją.*

Powyższe ramy teoretyczne wyznaczają warunki efektywnego funkcjonowania organizacji w kontekście wykorzystywanie znajdujących się w jej posiadaniu i gromadzonych zasobów informacyjnych.

Z tego względu kolejne podrozdziały niniejszej części rozprawy doktorskiej należy rozpatrywać w kontekście przedstawionych powyżej warunków optymalnego funkcjonowania – tylko w wypadku ich wypełnienia zasoby informacyjne w systemie przeciwdziałania terroryzmowi będą w pełni wykorzystywane dla realizacji jego podstawowego celu, tj. proaktywnego przeciwdziałania zagrożeniom terrorystycznych i ochrony przed nimi państw, jego obywateli i interesów zarówno na terytorium kraju, jak i poza jego granicami.

4.2 Zbieranie (pozyskiwanie) informacji

Dla skutecznego prowadzenia rozpoznania, a zatem gromadzenia (pozyskiwania) informacji konieczne jest jako warunek pierwotny określenie potrzeb informacyjnych podmiotu, który gromadzi informacji na użytek ich przetwarzania, przechowywania i podejmowania na ich podstawie krótko-, średnio- i długoterminowych decyzji

[124] Ibidem, s. 116.

i działań. Ustalenie potrzeb informacyjnych powinno odbywać się w procesie odpowiadania na pytania o to, do jakich celów wykorzystywana będzie informacja. Dopiero wiedząc, co będziemy chcieli osiągnąć, możemy jasno sformułować odpowiedź na pytanie o to, czego potrzebujemy[125]. Ustalenie potrzeb informacyjnych państwach zaczyna się zatem przede wszystkim od określenia jago celów w zakresie polityki i bezpieczeństwa. Kolejnym krokiem w zakresie określania potrzeb informacyjnych państwa jest określenie horyzontu czasowego realizacji zapotrzebowania na informacje.

Ogólnie rzecz biorąc założyć można, że po działaniach w zakresie rozpoznania, a więc zbierania (pozyskiwania) informacji spodziewać się należy dostarczenia danych dotyczących dwóch najważniejszych zagadnień, tj. informacji o przedmiocie działania (w wypadku systemów bezpieczeństwa o przeciwniku i stwarzanych przez niego zagrożeniach) oraz informacji o otoczeniu, w którym podmiot działa[126].

Wśród metod pozyskiwania informacji, szczególnie na potrzeby systemu bezpieczeństwa, wyróżnić należy dwie podstawowe ich grupy, tj. metody związane z korzystaniem ze źródeł otwartych, ogólnodostępnych oraz metody oparte głównie na prowadzeniu czynności operacyjno – rozpoznawczych, które realizowane są przede wszystkim przez służby specjalne i o charakterze policyjnym.

Wśród metod operacyjno – rozpoznawczych wyróżnić należy[127]:

1) wywiad – pozyskiwanie informacji przez prowadzenie odpowiednio ukierunkowanych rozmów;
2) penetracja terenu –sprawdzanie wyznaczonych miejsc w celu odnalezienia osób, zwłok, rzeczy lub śladów;
3) zasadzka – niejawne rozmieszczenie sił i środków w miejscu, w którym mogą znaleźć się osoby podejrzane lub poszukiwane, w celu ich zatrzymania lub odzyskania przedmiotów mających związek z przestępstwem;

---

[125] Borowiecki R., Romanowska M. (red.), *System informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa*, Warszawa 2001, Diffin, s. 175.

[126] Wrzosek M., *Potrzeby informacyjnego wsparcia procesu decyzyjnego w działaniach wojsk lądowych* [w:] Nowacki G. (red.), *Informacja w walce zbrojnej, Materiały z sympozjum naukowego*, Warszawa 2002, AON, s. 119.

[127] Opracowanie własne na podstawie: Zalewski S., *Służby specjalne w państwie demokratycznym*, Warszawa 2002, AON, s 58 i dalsze oraz poselskiego projektu ustawy o metodach operacyjno- rozpoznawczych, tekst dostępny na stronie Sejmu RP o adresie: [http://orka.sejm.gov.pl/Druki6ka.nsf/wgdruku/353].

4) eksperyment – przeprowadzenie w ściśle określonych warunkach doświadczeń lub odtwarzanie zdarzeń w celu weryfikacji lub uzupełnienia własnej wiedzy;
5) analiza operacyjna – to poszukiwanie powiązań między informacjami dotyczącymi danego zdarzenia;
6) obserwacja osób, miejsc i środków transportu – śledzenie osób, miejsc, rzeczy i środków transportu w stosunku do których istnieją prawne podstawy do podjęcia takich czynności;
7) pułapka – wykorzystanie specjalnie urządzeń lub środków do oznaczania osób albo rzeczy, utrwalenia cech identyfikacyjnych albo dokonania zatrzymania;
8) kontrola korespondencji;
9) środki techniczne: podsłuch rozmów telefonicznych, podsłuch i podgląd pomieszczeń i osób, podsłuch techniczny środków łączności przewodowej i radiowej, nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu, nadzór elektroniczny środków łączności przewodowej i radiowej,
10) zakup kontrolowany;
11) przesyłka niejawnie nadzorowana.

Drugie źródło, z którego podmioty odpowiedzialne za bezpieczeństwo państwa mogą pozyskiwać informacje związane ze swoimi działaniami w zakresie antyterroryzmu to tzw. źródła otwarte. Korzystanie ze źródeł otwartych określane jest także często mianem „białego wywiadu". W przeciwieństwie do powszechnego przekonania to właśnie biały wywiad zapewnia większość strategicznie istotnych informacji, dotyczących długoterminowego planowania działań[128]. W wyniku gromadzenia i analizy powszechnie dostępnych informacji określić można strategiczne trendy rozwojowe społeczne i gospodarcze na świcie. Ponadto analiza jawnych działań podmiotów funkcjonujących na arenie międzynarodowej, zarówno państw, jak i organizacji międzynarodowych oraz ugrupowań terrorystycznych pozwala na przewidywanie tego, jaki najprawdopodobniej przybierze kształt rzeczywistość międzynarodowa – globalna i regionalna – w której działań będzie dany podmiot.

[128] Borowiecki R., Romanowska M. (red.), *System informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa*, op. cit., s. 335.

Zwiększaniu udziału informacji zdobytych w ramach prowadzenia „białego wywiadu" w zasobach informacyjnych sprzyjają trendy określające funkcjonowanie otoczenia krajowego i międzynarodowego różnych podmiotów, np. rosnąca jawność życia publicznego. W dyspozycji osób zajmujących się białym wywiadem znajduje się do 95% informacji niezbędnych dla funkcjonowania podmiotów poruszających się jedynie w sferze gospodarczej[129], zakładać zatem można, że mniejsza – ale wciąż stanowiąca znaczącą, strategiczną wręcz, część niezbędnych informacji – ilość danych niezbędnych dla funkcjonowania systemu przeciwdziałania terroryzmowi znajduje się w obrocie jawnym. W największej części źródłami informacji dla „białego wywiadu" są: media, oficjalne dokumenty rządów i organizacji pozostających w zainteresowaniu, raporty, opracowania i analizy instytucji naukowo-badawczych, sprawozdania i informacje dotyczące wydarzeń na arenie międzynarodowej.

Opracowanie powyższych informacji następować powinno oczywiście w korelacji i z wykorzystaniem informacji pochodzących z rozpoznania operacyjnego, danych szpiegowskich itp. Pamiętać także warto, że część wiedzy, która potrzebna jest dla zaplanowania bądź realizacji danych działa może znajdować się w posiadaniu pracowników lub funkcjonariuszy instytucji, która w danym momencie prowadzi działania mające na celu gromadzenie informacji. Dlatego też często doprowadzenie do kontaktu i wymiany informacji pomiędzy poszczególnymi działami i pracownikami firmy może przynieść niezwykle cenne rezultaty[130].

Informacje pozyskiwane w procesie rozpoznania pochodzić mogą z różnych źródeł jest to co więcej pożądane, ponieważ dywersyfikacja źródeł pozyskiwania informacji pozwala na weryfikację tych informacji. Wyróżnia się następujące klasyfikacje źródeł informacji:

- na źródła osobowe (z ang. *humint*) oraz techniczne: podział ten dotyczy dwóch zasadniczych źródeł, z których pozyskiwać można informacje – tj. od człowieka, jako źródła informacji o sobie samym i o świecie oraz ze źródeł technicznych[131];

---

[129] Ibidem, s. 335.
[130] Ibidem, s. 176.
[131] *Systemy informacji geoprzestrzennej a budowa przewagi informacyjnej w sferze bezpieczeństwa państwa*, Zeszyty Naukowe Akademii Obrony Narodowej nr 1(58)A, Warszawa 2005, s. 171

- podział (za Tomaszem Aleksandrowiczem) na ogólnodostępne, o ograniczonej dostępności oraz relatywnie niedostępne[132] - tj. źródła podobne do omawianych wcześniej źródeł otwartych, źródeł, których wykorzystanie pociąga za sobą określone koszty oraz źródła , do wykorzystanie których konieczne jest skorzystanie z niejawnych metod dostępu.

4.3 Przetwarzanie informacji

4.3.1 Pojęcie cyklu analitycznego

Zgodnie z klasycznym ujęciem cykl analityczny składa się z 5 podstawowych elementów: zadarniowania, zebrania informacji, przetworzenia informacji i ich analizy oraz dystrybucji produktu analitycznego. Poszczególne elementy cyklu to[133]:

- **zadaniowanie:** decyzja o potrzebie opracowania analizy; najczęściej w postaci konkretnego zamówienia od odbiorcy, realizacji planowego zadania lub też inicjatywa własna, wynikająca z oceny rozwoju sytuacji w określonej dziedzinie. Praca analityka sprowadza się na tym etapie do stwierdzenia kto i w jakim terminie oczekuje odpowiedzi, czego dotyczyć ma analiza, czy jej temat został sformułowany prawidłowo;
- **zebranie informacji:** ocena, jakie informacje są potrzebne do opracowania analizy, w jaki sposób można do nich dotrzeć, a następnie - zebrać wszelkie informacje; istotne na tym etapie jest, że ilość informacji może osłabić ich wagę, bowiem ta właściwa, może umknąć uwadze analityka pośród zalewu innych. bycie dobrze poinformowanym z punktu widzenia potrzeb analizy oznacza więc wejście w posiadanie właściwej informacji we właściwym czasie;
- **przetworzenie informacji:** proces nadania informacji formy, w jakiej analityk będzie mógł ją wykorzystać bezpośrednio w pracy, np. poprzez określenie wiarygodności źródła, tłumaczenie dokumentu z języka obcego etc. Wszystkie zebrane dane należy uporządkować, tworząc na tej podstawie wstępną strukturę dokumentu;
- **analiza i wykonanie**: w tej fazie zebrane i przetworzone informacje zostają poddane analizie, na podstawie której wyciąga się wnioski, aby następnie nadać im

[132] Aleksandrowicz T., *Analiza informacji w administracji i biznesie*, Warszawa 1999, WSHiP, s. 93-96.
[133] Ibidem, s. 52.

odpowiednią formę w postaci ostatecznego raportu; możliwe jest także włączenie w tę fazę zadania w postaci oceny analizy, a zatem procesu określenia, w jakim stopniu gotowe opracowanie spełnia zapotrzebowania odbiorcy przedstawione przez niego podczas zadaniowania.[134]

- **dystrybucja przygotowanego materiału:** cykl analityczny może okazać się cyklem *otwartym* lub *zamkniętym*, odbiorca może wykorzystać ją przy podejmowaniu określonych decyzji lub też polecić opracowanie kolejnego materiału na dany temat.[135]

Cykl analityczny można przedstawić również w postaci tabeli, zaprezentowanej poniżej.

Tab. 9: Cykl analityczny

OBIEG INFORMACJI	PROCES ANALITYCZNY
PLANOWANIE I WYZNACZANIE KIERUNKÓW	ROZPOZNANIE PROBLEMU
	Kto oczekuje odpowiedzi dotyczących zagrożeń terrorystycznych?
	Kiedy? Ile jest czasu na sporządzenie analizy i przeciwdziałanie zagrożeniu?
	Czego dotyczy sprawa? Jaki jest temat analizy?
	Czy zagadnienie zostało właściwie postawione? Jak można je określić inaczej?
	Wstępne określenie perspektywy, *focusing*, wstępne hipotezy i założenia.
GROMADZENIE DANYCH	PROWADZENIE BADAŃ
	Co już wiadomo? Co zostało już dokonane?
	Czego nie wiadomo? Jakich informacji potrzeba? Jakim dostępem do źródeł informacji dysponujemy?
	Pozyskanie wszystkich niezbędnych informacji i zgromadzenie ich do dyspozycji analityka.
PRZETWARZANIE	PORZĄDKOWANIE DANYCH
	Nadanie wszystkim zebranym informacjom formy umożliwiającej ich bieżące wykorzystanie przez analityka.
	Wybór informacji potrzebnych do analizy.
	Określenie wiarygodności.
	Utworzenie modelu struktury dokumentu i uporządkowanie danych pod tym kątem.
	Wstępne interpretacje, hipotezy, wnioski, prognozy.

[134] Zob. np.: Winkler I., *Corporate Espionage. What It Is, Why It Is Happening In Your Company, What You Must Do About It*. Prima Publishing, Rocklin, California 1997, ss. 25 – 26.
[135] Por. na ten temat: *The Intelligence Cycle* (w:) *Factbook on Intelligence*. http://www.odci.gov/cia/publications.

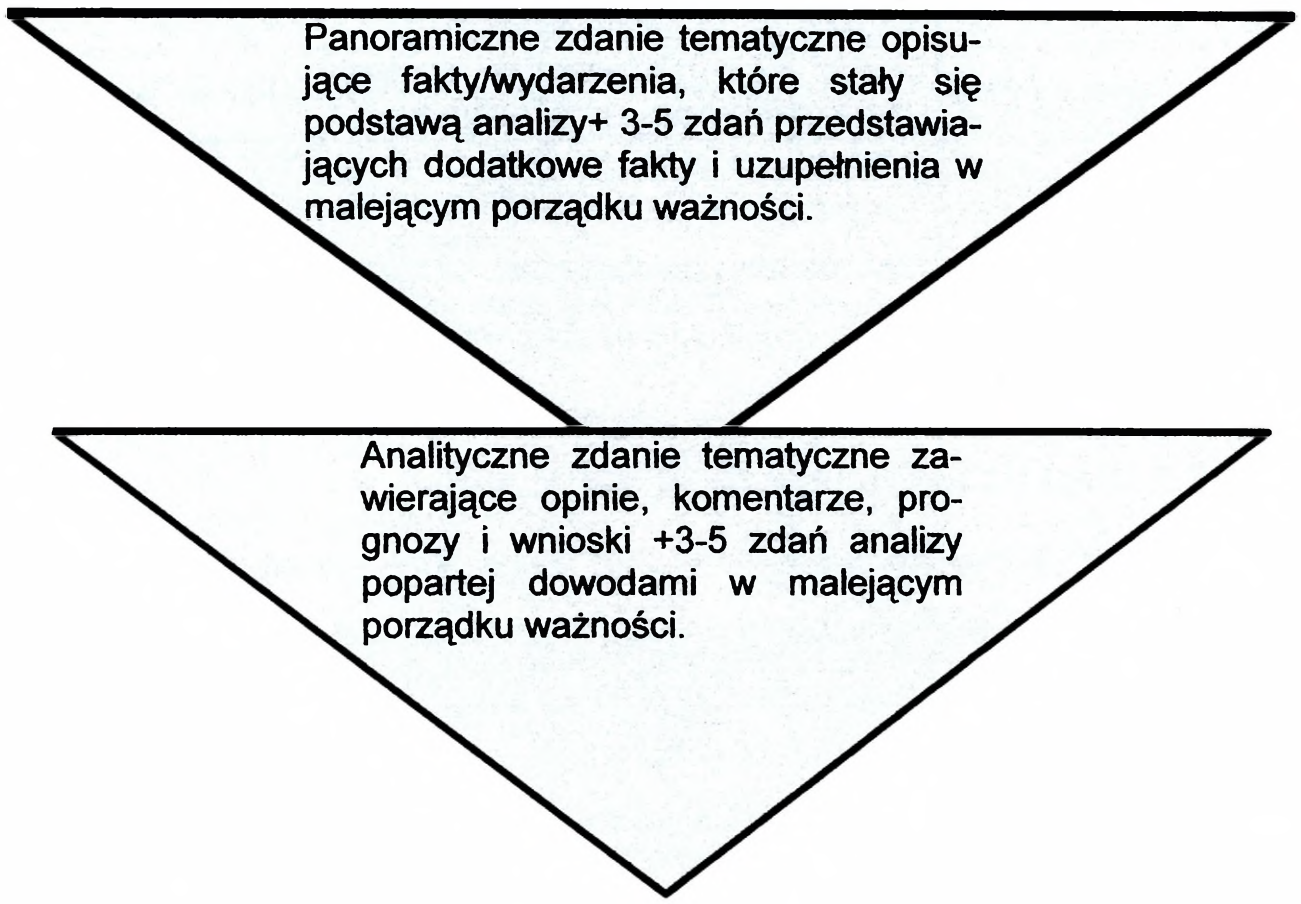
ANALIZA I TWORZENIE DOKUMENTU	WŁAŚCIWY PROCES ANALITYCZNY	
	Sformułowanie interpretacji, ocen, wniosków, hipotez i prognoz.	
	Przygotowanie ostatecznej wersji dokumentu i nadanie mu odpowiedniej formy graficznej.	
	Autokorekta, samoredagowanie.	
	Zatwierdzenie dokumentu, ew. poprawki.	
DYSTRYBUCJA	PRZEKAZANIE DOKUMENTU ODBIORCOM	
	Informacja zwrotna	Brak reakcji (cykl zamknięty).
		Nowe zadanie analityczne (cykl otwarty).

Źródło: Aleksandrowicz T., *Analiza informacji w administracji i w biznesie*, Warszawa, 1999[136].

4.3.2 Struktura dokumentu analitycznego

Dokument analityczny zaczyna się od tytułu, który powinien odzwierciedlać treść analizy. Następnym elementem dokumentu jest czołówka, w której znajduje się informacja nt. podstawowych kwestii: powód sporządzenia analizy, czyli ogólna zawartość dokumentu. Kolejnym elementem struktury są tzw. główne punkty analizy. Dokument kończy się rozszerzonymi wnioskami, zawierającymi w miarę możliwości elementy prognozy rozwoju sytuacji[137].

[136] Aleksandrowicz T., *Analiza informacji w administracji i w biznesie*, Warszawa 1999, s. 55-56.
[137] Aleksandrowicz T., *Analiza informacji w administracji i w biznesie,* op. cit., s. 72.



Rys. 12: Struktura dokumentu analitycznego
Źródło: Aleksandrowicz T., *Analiza informacji w administracji i w biznesie*[138].

4.3.3 Techniki analityczne (techniki twórczego myślenia)

Techniki analityczne, zwane także niekiedy technikami twórczego myślenia, służą osiągnięciu najważniejszego celu analizy informacji, a więc stworzeniu swoistej *wartości dodanej*. Informacja określa bowiem jedynie zmianę rzeczywistości, dając odpowiedź na pytanie *„co?"* (co się stało, jakie nowe fakty zaistniały). Tworzenie wartości dodanej polega na udzieleniu odpowiedzi na pytanie *„co z tego"?* (co z tego wynika? Jakie są konsekwencje? Dlaczego tak się stało?)[139].

Do podstawowych technik analitycznych można zaliczyć[140]:

a) cofanie się – technika ta zwana jest także „myśleniem do tyłu" i stosowana przy budowie prognoz, kiedy za punkt wyjścia przyjmuje się, że wydarze-

[138] Ibidem, s. 75.
[139] Aleksandrowicz T., *Analiza informacji w administracji i w biznesie,* op. cit., s. 140.
[140] Ibidem, s. 151 i dalsze.

nie, którego prawdopodobieństwo należy zbadać, już nastąpiło, a następnie dąży się do stwierdzenia, co musiałoby się stać, aby doszło do danego wydarzenia;

b) odwrócenie problemu (myślenie negatywne) – badanie przeciwieństwa danego problemu, tj. „odwrócenia" go, dla zbadania wszystkich jego aspektów;
c) kwestionowanie założeń; służyć temu może matryca założeń, która pozwala nie uporządkować znane fakty, a także podjąć próbę znalezienia aspektów nieznanych i ukrytych założeń
d) gry – wcielanie się w rolę określonego podmiotu i przeprowadzenia symulacji zachowań;
e) techniki grupowe; np. burza mózgów i różne jej modyfikacje;
f) strukturalizacja – wykorzystanie faktu, że każda całość złożona posiada strukturę wewnętrzną, którą można badać z użyciem form graficznych, jak listy, matryce, diagramy, schematy etc.

Inna narzędzie analityczne również przybierać mogą formę strukturalizującą badany obiekt, sytuację bądź zespół okoliczności. Należą do nich między innymi[141]:

– przywołana wcześniej matryca założeń, którą zaprezentować można na przykładzie poniższej tabeli:

Tab. 10: Matryca założeń

WIEMY	NIE WIEMY	ZAŁOŻENIA UKRYTE	ZAKŁADAMY	WSKAŹNIKI
Jakie fakty rozpatrujemy?	Jakich faktów nie znamy?	Jakie założenia traktujemy aksjomatycznie?	Założenie 1.	Co świadczy o tym, że założenie jest prawdziwe?
			Założenie 2.	Co świadczy o tym, że założenie jest prawdziwe?
			Założenie 3.	Co świadczy o tym, że założenie jest prawdziwe?

Źródło: Aleksandrowicz T., Analiza informacji w administracji i w biznesie[142].

[141] Ibidem, s. 158.
[142] Ibidem, s. 167.

- schemat powiązań (relacji): tworzy się go poszukując wzajemnych relacji pomiędzy poszczególnymi podmiotami,;
- schemat przepływów: podobny do schematu relacji, jednak w tym przypadku zadaniem jest ustalenie, jakimi drogami porusza się dany obiekt łączący podmioty pojawiające się w danej sprawie;
- schemat kontaktów;
- matryca opcji: najbardziej skomplikowane narzędzie analityczne, służące zarówno do oceny bieżącej sytuacji, jak też do budowy prognoz.

Tab. 11: Matryca opcji

OPCJA HIPOTEZA ZAŁOŻENIE	KORZYŚCI	STRATY	POTENCJALNE REZULTATY	IMPLIKACJE	WSKAŹNIKI
	Jakie korzyści odniesie podmiot podejmujący działanie określone w założeniu (przesłanki pozytywne)	Jakie straty poniesie podmiot podejmujący działanie określone w założeniu (przesłanki negatywne)	Jakie rezultaty może przynieść działanie określone w założeniu/jakie mogą nastąpić zmiany w sytuacji	Jakie będą konsekwencje dla nas podjęcia działania określonego w założeniu	Co wskazuje na to, że Działanie określone w założeniu zostało podjęte (założenie jest prawdziwe)
Opcja 1.					
Opcja 2.					

Źródło: Aleksandrowicz T., *Analiza informacji w administracji i w biznesie*[143]

Nie w każdym przypadku konieczne jest wykorzystywanie każdego z podanych wyżej punktów, zależy to zarówno od przedmiotu analizy, jak też i jej celu; każdy schemat można dopasowywać w zależności od aktualnych potrzeb.

4.3.4 Analiza ryzyka jako kluczowy element w planowaniu antyterrorystycznym

Podstawową rolą systemu przeciwdziałania terroryzmowi jest ochrona państwa i społeczeństwa przed terroryzmem poprzez wymienione już elementy systemu przeciwdziałania: profilaktykę, zapobieganie, zwalczanie i likwidację skutków. Funkcjonowanie każdego z wymienionych elementów systemu pociąga za sobą nie tylko

[143] Ibidem, s. 168.

skutki w postaci nakładów pracy, wysiłku organizacyjnego oraz nakładu sił i środków. Ich funkcjonowanie skutkuje także w postaci nakładów finansowych finansowanych z budżetu państwa.

Szczególną rolę w tak pojmowanych działaniach analitycznych pełni metoda określana jako „szacowanie ryzyka". Ostatecznym celem zarówno rozpoznania, jak i analizy, jest takie sformułowanie przetworzonych informacji, które pozwoli na optymalizację decyzji dotyczących przeciwdziałania terroryzmowi, które zapadają na szczeblu politycznym. Działanie to zmierza do stanu, w którym siły i środki alokowane są zgodnie z opartą na alternatywnych modelach redukcji ryzyka zasadą efektywności ponoszonych na zabezpieczenie antyterrorystyczne kosztów. Dzięki temu alokacja zasobów proporcjonalna jest do dystrybucji ryzyka pomiędzy podmiotami, które są przedmiotem zabezpieczenia antyterrorystycznego.

Ryzyko ze strony terroryzmu powinno być postrzegane jako składające się z trzech podstawowych elementów :

- zagrożenia, jakie terroryzm stanowi w stosunku do celu,
- podatności celu na atak terrorystyczny,
- konsekwencji potencjalnego, udanego ataku na cel.

Miarą ryzyka ze strony terroryzmu są zatem oczekiwane konsekwencje istniejącego zagrożenia, które dla danego celu, danego sposobu ataku oraz danego typu szkód mogą zostać wyrażone jako[144]*:*

RYZYKO = ZAGROŻENIE x PODATNOŚĆ x KONSEKWENCJE

Dany podmiot może stanowić zagrożenie, jeśli ma zarówno zamiar, jak i środki do przeprowadzenia zamachu terrorystycznego. Zagrożenie dla celu powinno natomiast być definiowane jako prawdopodobieństwo, że określony cel zostanie w określony sposób zaatakowanych w określonym czasie. Należy przy tym zauważyć, że ani zdolność do przeprowadzenia ataku bez takiej intencji, ani też intencje bez zdolności nie stanowią zagrożenia, jedynie w sytuacji, w której spełnione są oba warunki, możne mówić o powstaniu zagrożenia zamachem terrorystycznym.

Tym samym alokowanie środków bezpieczeństwa powinno odbywać się odpowiednio do tego, jakie cele w konkretnych regionach mogą stać się przedmiotem ja-

[144] Willis H., Korral A., Kelly T., Medby J., *Estimating Terrorism Risk*, RAND Corp. 2005, tekst dostępny na stronie o adresie [www.RAND.org/pubs/monographs/2005/RAND_MG388.pdf].

kiego ataku. Jeśli spektrum zagrożenia postrzegane jest przez pryzmat określonej grupy celów, które mogą zostać zaatakowane w określony sposób e określonym czasie, prawdopodobieństwo może stać się miarą tego, jak możliwy jest określony atak[145].

Aby w pełni opisać spektrum zagrożeń, należałoby przeanalizować oddzielnie każdy cel w kontekście każdego rodzaju ataku (atak radiologiczny będzie przeprowadzony w inny sposób i spowoduje inne skutki, niż atak nuklearny). W praktyce jednak często wystarczające jest skupienie się na sposobach ataków najbardziej reprezentatywnych dla poszczególnych zagrożeń terrorystycznych z grupy CBRN oraz z użyciem materiałów wybuchowych[146].

Taka perspektywa postrzegania zagrożenia różni się od perspektywy często przyjmowanej przez służby bezpieczeństwa państwa. Podmioty takie postrzegają często zagrożenie, jako intencję pokreślonej grupy osób, dotyczącą zniszczenia określonego celu i szukają sposobów powstrzymania tej grupy. Jednak postrzeganie ataku poprzez pryzmat potencjalnego celu jest znacznie pożyteczniejsze ze względu na alokację sił i środków bezpieczeństwa, ponieważ decyzje z tym związane znacznie częściej dotyczą tego, jaki cel i w jaki sposób zostanie zaatakowany, niż kto ten atak przeprowadzi[147].

Podatność na atak określić można natomiast prawdopodobieństwo, że szkody się pojawią, w razie zaistnienia zagrożenia. Do szkód tych zaliczyć można ofiary śmiertelne, rannych, straty w mieniu lub inne – dla każdego rodzaju szkód potrzebna będzie osobna ocena podatności. Ten sam rodzaj ataku może spowodować różne konsekwencje w zależności od tego, przeciwko jakiemu celowi zostanie skierowany, na przykład atak z użyciem samochodu wyładowanego materiałami wybuchowymi spowoduje znacznie poważniejsze skutki w wypadku hotelu lub centrum handlowego niż w przypadku ufortyfikowanego budynku militarnego.

Można powiedzieć, że podatność na tak to zdolność atakowanego systemu do reagowania na dane zagrożenie. W wypadku takiego podejścia, aby określić podatność na tak konieczne jest udzielenia odpowiedzi na pytanie „jaki atak?".[148] Podatność jest zatem prawdopodobieństwem tego, że atak określonego rodzaju, skiero-

[145] Ibidem, s. 6.
[146] Ibidem, s. 6.
[147] Ibidem s. 7.
[148] Ibidem, s. 7.

wany przeciwko określonemu celowi powiedzie się, jeśli zostanie przeciwko niemu skierowany. Jednocześnie mierzy jedynie podatność na określony rodzaj szkód (oddzielny pomiar wymagany jest dla podatności na ofiary śmiertelne w wyniku ataku, zranienia, zniszczenia dóbr materialnych, itp.). Należy także odnotować, że pomiar ten nie dotyczy wielkości szkód, a jedynie prawdopodobieństwo ich wystąpienia.

Wielkości i powagi szkód dotyczy kolejny składnik czynnik uwzględniany w analizie ryzyka, to jest konsekwencje będą to rozmiary i rodzaj szkód, które wystąpią w wypadku udanego ataku terrorystycznego[149]. Konsekwencje wyrażone mogą być w postaci ofiar śmiertelnych, zranień, strat ekonomicznych lub innego typu szkód. Można rozważać także inne typy konsekwencji ataku, szczególnie jeśli te konsekwencje rozważane są nie tylko w odniesieniu do bezpośredniego celu ataku, ale także w stosunku do całego społeczeństwa. Na potrzeby analizy ryzyka ataku terrorystycznego warto jednak ograniczyć definiowanie konsekwencji do śmiertelności, zranień oraz strat ekonomicznych (materialnych) w punkcie ataku, aby jak najlepiej ocenić prawdopodobieństwo skierowania konkretnego ataku przeciwko konkretnemu celowi.

Ryzyko jest funkcją wszystkich trzech wymienionych czynników, tj. zagrożenia, podatności na to zagrożenie oraz konsekwencji potencjalnego ataku. Ryzyko ataku terrorystycznego jest zatem wartością, która reprezentuje oczekiwane konsekwencje ataku, biorąc pod uwagę prawdopodobieństwo tego, że do ataku dojdzie oraz to, że jeśli do niego dojdzie, to będzie on udany. Z punktu widzenia probabilistyki ryzyko ataku określonego rodzaju jest bezwarunkową oczekiwaną wartością strat określonego typu[150].

Podejmowanie działań w obszarach wskazanych powyżej, a zatem kompleksowej oceny kraju w kontekście:

- zagrożenia terroryzmem,
- podatności na atak terrorystyczny,
- przewidywanych konsekwencji takich ataków,

stanowić powinno stały element raportów analitycznych docierających do czynników decyzyjnych na poziomie politycznym. Na podstawie bowiem takich właśnie, szcze-

[149] Ibidem, s. 10.
[150] Ibidem, s. 10.

gólnych rodzajów analiz, podejmowane powinny być decyzje kierunkowe nie tyle dla działań służb, ile organizacji całego systemu przeciwdziałania terroryzmowi i alokacji zasobów systemu bezpieczeństwa państwa[151].

4.4 Przechowywanie (bazy danych)

Bez racjonalnie zbudowanego systemu przechowywania informacji, żaden system zarządzania zasobami informacyjnymi nie będzie wydolny. Zarówno zebrane informacje, skumulowane dane, jak i wyniki ich analiz, muszą być dostępne dla osób i podmiotów do takiego dostępu uprawnionych – w przeciwnym wypadku praca włożona w pozyskanie i przetworzenie informacji pozbawiona jest racji bytu. Ponadto nie wszystkie informacje zdobyte w procesie pozyskiwania podlegają natychmiastowemu wykorzystaniu. Często zdarzy się, iż informacje pozyskana w danym momencie z określonego źródła okaże się wartościowa dopiero w kombinacji z inną informację, pozyskaną w innym czasie i innych okolicznościach.

Dlatego też gromadzone dane przechowywane są w postaci różnych baz danych. Mogą być one dzięki temu używane nie tylko do podejmowania decyzji o charakterze strategicznym, bazujących na danych pozyskanych w długim okresie, ale także być wykorzystywane do konfrontacji z nowymi danymi i informacjami na bieżąco pozyskiwanymi w procesie rozpoznania. Inna determinanta, która pociąga za sobą konieczność tworzenia baz danych, to poszerzanie kompetencji podmiotów, które gromadzą i przetwarzają informacje. Wraz ze wzrostem zakresu kompetencji i realizowanych zadań powiększa się ilość obszarów, w których konieczne jest gromadzenie informacji.[152]

Stworzenie bazy danych zapewnia realizację grupy potrzeb, wynikających z dążenia do efektywnego funkcjonowania instytucji lub organizacji. Wśród najważniejszych potrzeb tego rodzaju wymienić należy:

- zapewnienie dostępu do co najmniej minimum danych, informacji i produktów ich przetwarzania wszystkim osobom i grupom osób, które mu-

[151] Patrz także: Liedel K., *Bezpieczeństwo imprez masowych w dobie zamachów terrorystycznych*, [w:] *Badania Operacyjne i Systemowe – BOS 2008* Polskiego Towarzystwa Badań Operacyjnych i Systemowych, Rembertów 18-20 września 2008r.
[152] Pawłowska A., *Zasoby informacyjne w administracji publicznej w Polsce. Problemy zarządzania*, Lublin 2002, UMCS, s. 135.

szą mieć dostęp do wspólnego obrazu sytuacji (jest to szczególnie istotne w wypadku osób realizujących swoje zadania w strukturach odpowiedzialnych za bezpieczeństwo),
- ograniczenie niespójności informacji pozostających do dyspozycji wszystkich podmiotów, które zarówno dostarczają dane do bazy, jak i są jej klientami informacyjnymi,
- istnieje możliwość wprowadzania komentarzy i uzupełniania danych dotyczących wcześniej wprowadzonych rekordów,
- zgromadzenie danych w bezpiecznej bazie zwiększa ich bezpieczeństwo.

Bazy danych, w ostatnich latach przekształcające się w hurtownie danych[153], to jeden z najważniejszym elementów systemu zarządzania informacjami, zawierają bowiem nie tylko materiał przetwarzany w systemie, ale także efekty prac analitycznych, czyli procesu przetwarzania.

Pojęcie hurtowni danych, jako ewolucyjny następca bazy danych, łączy następujące cechy:
- zbiór danych,
- możliwość wydobywania danych,
- możliwość analitycznego przetwarzania on-line.[154]

Pojęcie „hurtowni danych" wprowadzone zostało przede wszystkim ze względu na uwzględnienie części składowej, która umożliwia agregowanie i analizę surowych danych operacyjnych[155]. To ten element agregujący dane stwarza możliwość połączenia ze sobą dwóch rodzajów systemów: statycznych baz danych z systemami analitycznymi.

Dane zgromadzone w hurtowni danych mogą zostać zorganizowane w sposób hierarchiczny. Zbiór zasobów zawarty w danej bazie może zostać podzielony na klasy ze względy na atrybuty przypisanych do danych klas informacji i danych. W ten sposób zasób mniej złożony zawiera się w zasobie bardziej złożonym. Zasoby bardziej złożone są w tej koncepcji zasobami nadrzędnymi, zasoby mnie złożone – za-

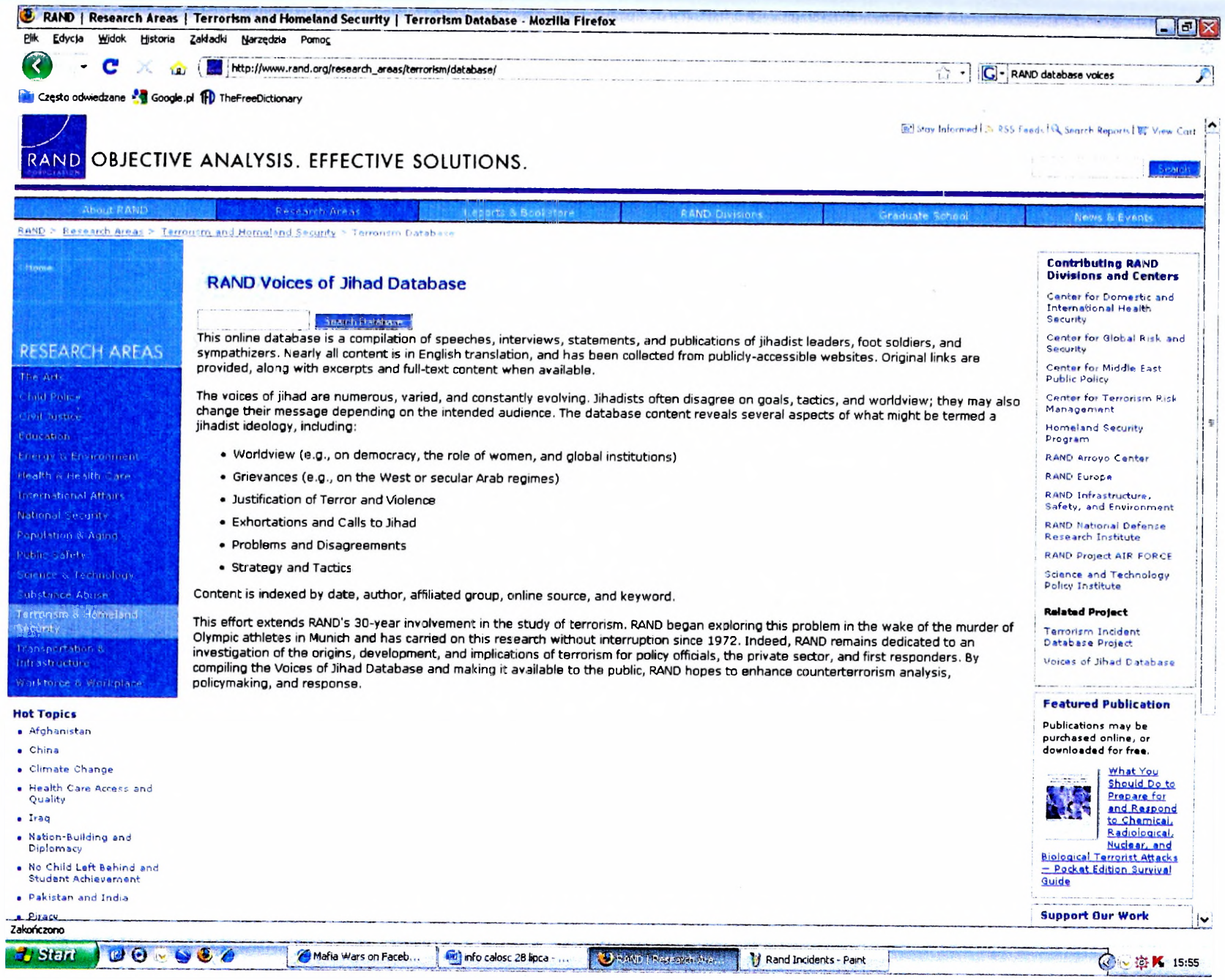
[153] Praca zbiorowa, red. Michalski A., *Zarządzanie informacjami w przedsiębiorstwie*, Gliwice 1999, Wyd. Politechniki Śląskiej, s. 45.
[154] Ibidem, s. 47.
[155] Ibidem, s. 49.

sobami podrzędnymi. Zasoby podrzędne zawarte w tym samym zasobie nadrzędnym są w tej sytuacji zasobami równo rzędnymi. Pewien rodzaj zasobów, jak pojedyncze dane i informacje, ma charakter elementarny i nie zawiera w sobie innych zasobów[156].

Dostęp do zasobów zawartych w hurtowni danych przyznawany powinien być na podstawie zasady *need-to-know* (potrzeby posiadania dostępu do danego rodzaju zasobu) oraz przyznawany przez odpowiednią instytucję lub komórkę administrującą bezpieczeństwem systemu zgodnie z posiadanym stanowiskiem służbowym oraz realizowanymi zadaniami.

Istotne jest także branie pod uwagę baz danych istniejących na świecie w postaci baz on-line. Bazy te tworzone są przez organizacje i instytucja o charakterze naukowo badawczym. Przykładem baz danych tworzonych przez takie instytucje mogą być na przykład dwie bazy stworzone przez RAND Corporation: *Voices of Jihad Database* (rys. 7) oraz *Worldwide Terrorism Incidents Database* (rys. 8).

[156] Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, op. cit., s. 237.



Rys. 13: RAND Voices of Jihad Database

Źródło: portal RAND Corp., [www.RAND.org]

RAND | ISE | Projects | RAND Database of Worldwide Terrorism Incidents - Mozilla Firefox

Plik Edycja Widok Historia Zakładki Narzędzia Pomoc

http://smapp.rand.org/rwtid/search_form.php

RAND database

Często odwiedzane Google.pl TheFreeDictionary

RAND Home Stay Informed Search Reports View Cart

RAND Database of Worldwide Terrorism Incidents
A RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT PROJECT

Search RAND Search ISE

About RAND | Research Areas | Reports & Bookstore | RAND Divisions | Graduate School | News & Events

RAND > ISE > Projects & Resources > RAND Database of Worldwide Terrorism Incidents

INFRASTRUCTURE SAFETY AND ENVIRONMENT

- RDWTI Home
- About RDWTI
  - Database Scope
  - Research Coverage
  - Contact Us
- Subscribe to RDWTI
- Search RDWTI
  - RDWTI Demo
  - Search Instructions
- Research Publications

Related Resources
- RAND Voices of Jihad Database

BOOKMARK

EMAIL

Terrorism Database Search

DEMO MODE SEARCHING

You are using the RDWTI Database in the **free demonstration mode**. The demo mode is fully functional in all ways, but will only return less than one tenth of the actual results that the full product would return.

To order a subscription to the full RDWTI Database, fill out the RDWTI Database Subscription Request Form.

Instructions for searching the RDWTI

1. Select values on which to subset your search (selecting no values will result in a search of the entire database).
2. Select the type of output you want: Incident list, pie chart, or chronological graph.
   - For **pie chart**, you must select the plot button next to the variable you want plotted.
   - For **chronological chart**:
     - select plot next to "Injuries" or "Fatalities" for cumulative bar charts
     - deselect all plot buttons to produce bar charts showing the number of returned incidents
3. Press the search button.

1. Select Search Values

Search Term: *search incident descriptions*

Start Date: Clear Date

End Date: Clear Date

Region: ALL, Africa, East & Central Asia, Eastern Europe, Latin America — plot

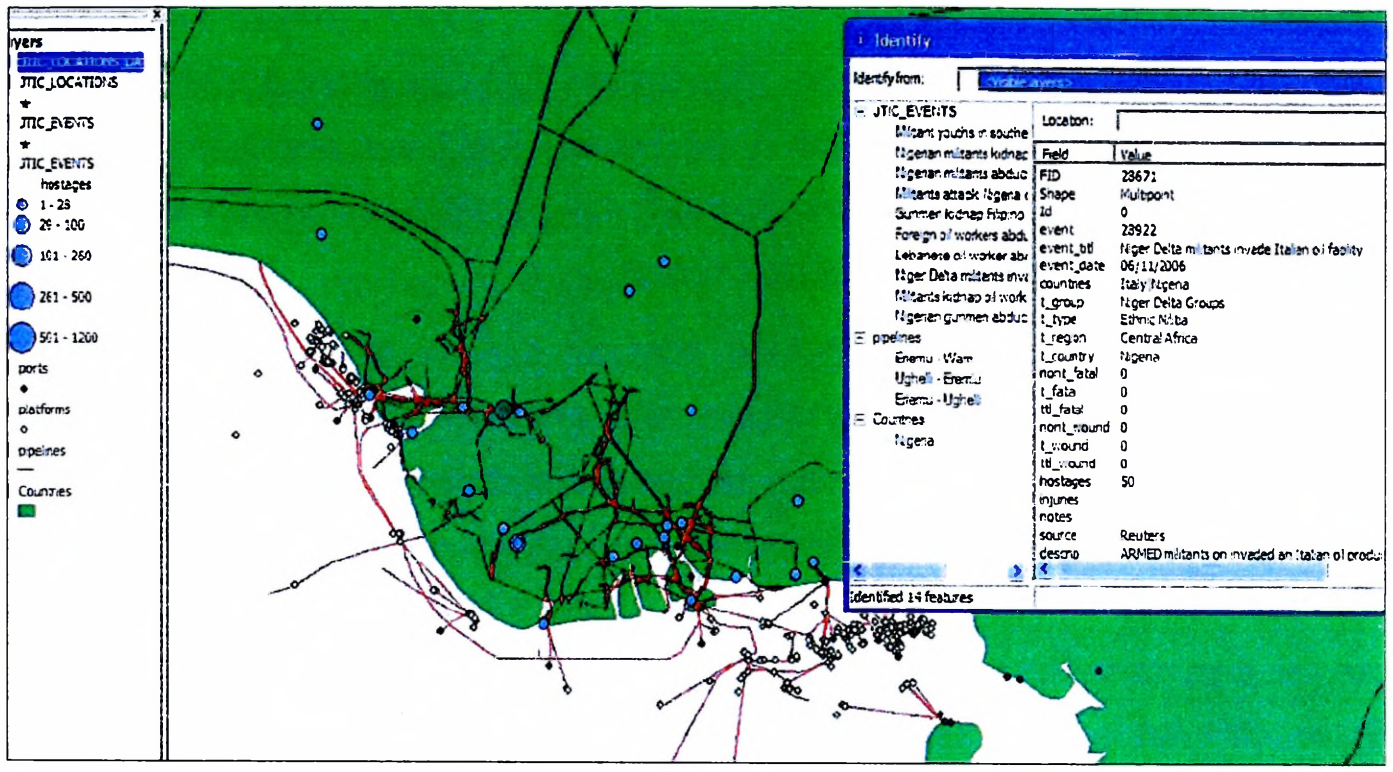
Country: ALL, Afghanistan, Albania, Algeria, Angola — plot

Zakończono

Start | Mafia Wars on Faceb... | info calosc 28 lipca - ... | RAND | ISE | Projects... | 15:54

Rys. 14: RAND Worldwide Terrorism Incidents Database Źródło: portal RAND Corp., [www.RAND.org]

Zaznaczyć należy także, że oprócz istnienia baz niekomercyjnych, jak bazy RAND, narzędzia tego rodzaju udostępniane są także przez instytucje komercyjne, jak Jane's Information Group (rys.9).



Rys. 15: Jane's terrorism events data. Terrorism Events Spatial Lay
Źródło: portal Jane's Information Group,
[http://www.janes.com/press/press/pc080515_1.shtml]

4.5 Udostępnianie informacji

Udostępnianie informacji to jeden z najistotniejszych elementów systemu zarządzania zasobami informacyjnymi. Dopiero w momencie, w którym następuje udostępnienie informacji, system zarządzania tym zasobem spełnia swoją właściwą role, tj. pozwala osobom / instytucjom zarządzającym organizacją (lub państwem) podjąć decyzję w sposób racjonalny, w oparciu o konkretne przesłanki i rekomendacje zawarte w dokumentach analitycznych. Dla pełnej efektywności planowania strategicznego konieczna jest umiejętność nie tylko analizy bieżących wydarzeń, ale także podjęcie próby ekstrapolacji na podstawie posiadanych danych zdarzeń w przyszłości, które stanowić mogą o zagrożeniu dla danego podmiotu. Wątek te poruszany był już zresztą w części pracy poświęconej analizie ryzyka jako kluczowemu elementowi systemu przeciwdziałania terroryzmowi.

Udostępniane dane powinny umożliwić czynnikom decyzyjnym na stworzeniem kompleksowej wizji otoczenia zewnętrznego państwa oraz sytuacji wewnętrznej, któ-

ra pozwoli na podejmowanie trafnych, długo-, średnio- i krótkoterminowych decyzji. Jednak nawet najlepsze opracowanie, w którym zawarte są najtrafniejsze rekomendacje nie spełni swojego zadania, jeśli nie trafi w odpowiednie ręce. Dlatego właśnie system udostępniania i przekazywania powinien być drożny i działać dynamicznie, funkcjonując nie tylko na podstawie określonych terminów przekazywania okresowych raportów i opracowań, ale także uwzględniać możliwość elastycznego reagowania w sytuacji pojawienia się nowych informacji i analiz o charakterze krytycznym dla wydarzeń, które w danym momencie następują.

Udostępniana informacja powinna przybrać odpowiednią, przejrzystą formę, najlepiej w postaci opartej na omówionym w poprzednim podrozdziale pracy schemacie dokumentu analitycznego, który zapewnia przejrzystość i zwięzłość formy i treści. Istotne cechy przekazywanych opracowań i raportów wiążą się z omawianymi w rozdziale pierwszy pracy cechami informacji, decydującymi o jej wartości, co oznacza, że dokumenty takie powinny być aktualne, wiarygodne, na temat i kompletne. Szczególnie istotna jest aktualność informacji. Pamiętać należy, że każda napływająca informacje tworzy nową sytuację decyzyjną i powiększa zasób informacji, na podstawie których podejmowane są decyzje[157]. Biorąc pod uwagę to, że to kierunki działania wyznaczają potrzeby informacyjne, a zmieniający się zasób informacyjny zmienia decyzje o kierunkach działania, założyć można, że pomiędzy decyzjami o strategicznych kierunkach działania i pozyskiwaniem informacji istnieje sprzężenie zwrotne, a te dwa zjawiska są silnie od siebie zależne.

Ponadto pamiętać należy o tym, że udostępnianie informacji nie odbywa się wyłącznie w płaszczyźnie wertykalnej (tj. od służb do czynników decyzyjnych), ale także w płaszczyźnie horyzontalnej (tj. pomiędzy służbami). Dlatego właśnie tak potrzebne są racjonalnie zbudowane, z precyzyjnie określonym systemem dostępowym bazy danych. W płaszczyźnie wymiany horyzontalnej to właśnie bazy danych, zawierające zarówno wyniki pozyskiwania informacji, jak też przetwarzania tychże, stanowią najważniejszy mechanizm komunikacyjny. Do jego funkcjonowania konieczne jest jednak nie tylko spełnienie warunków technicznych, tj. zbudowanie baz danych, ale także – o czym wspomniano wcześniej – systemu dostępowego opartego na spójnych przepisach dotyczących ochrony informacji niejawnych, ich udostępniania i wymiany.

---

[157]Nowak A., *Informacja w rozpoznaniu* [w:] Nowacki G. (red.), *Informacja w walce zbrojne., Materiały z sympozjum naukowego*, Warszawa 2002, AON, s. 129.

Informowanie jest procesem, co oznacza, że trwa w czasie. Ponadto jest to ciąg realizowany podczas trwania sytuacji informacyjnych, a wreszcie zaspokaja potrzeby uczestników sytuacji informacyjnej[158]. Systemy informacyjne, których celem jest zaspokajanie istniejących potrzeb informacyjnych można podzielić na trzy kategorie[159]:

- systemy masowego informowania, służące zaspokajaniu społecznych potrzeb informacyjnych,
- systemy informowania kierownictwa – zaspokajające potrzeby informacyjne czynników decyzyjnych w organizacji, państwie bądź pomiocie gospodarczym,
- specjalistyczne systemy informacyjne – służące informowaniu i wymianie informacji pomiędzy ekspertami.

Zgodnie z prezentowaną przez prof. P. Sienkiewicza teorią oba ostatnie systemy – a zatem te, które interesują autora z punktu widzenia dystrybucji informacji systemie bezpieczeństwa państwa – charakteryzować się muszą zdolnością przekazywania informacji z maksymalnym zachowaniem wierności informacji oryginalnej. Jest to konieczne ze względu na to, że decyzje, szczególnie w obszarze bezpieczeństwa instytucji, podejmowane być muszą na jak najpewniejszych przesłankach i mieć oparcie w faktycznym stanie sytuacji wewnętrznej (potencjału instytucji) oraz otoczenia danego podmiotu.

Udostępniane i przekazywane w procesie dystrybucji informacje oceniane są zasadniczo pod jednym względem: ich wartość wyznacza różnica efektów decyzji, która podjęta została pod wpływem posiadania danej informacji i efektów decyzji, która zostałaby podjęta, gdyby udostępniona informacja nie zaistniała w systemie informacyjnym[160]. To ostatnie zdanie podsumowuje zresztą wagę systemu dystrybucji informacji w organizacjach, instytucjach i strukturach państwa: informacje, które są przez odpowiednie służby i komórki gromadzone, przetwarzane i przechowywane istnieją tylko po to, aby zostać udostępnione – i w ten sposób wpłynąć na kształt strategicznych planów i decyzji, które wpływają na przyszłość danego podmiotu i jego otoczenia. Przytoczyć można, za prof. Sienkiewiczem, pogląd Chestera Barnarda,

[158] Sienkiewicz P., *Systemy kierowania*, Wiedza Powszechna, Warszawa 1989, s. 130.
[159] Ibidem, s. 131.
[160] Ibidem, s. 132.

który stwierdził, iż organizacja powstaje wtedy, gdy kierując się chęcią wspólnej pracy ludzie potrafią wymieniać informacje.[161]

4.6 Media masowe a terroryzm – wykorzystanie mediów w przeciwdziałaniu terroryzmowi

Terroryzm, mimo iż jego bezpośrednimi skutkami są poważne ofiary w ludziach oraz liczone nieraz w miliardach dolarów straty materialne, z punktu widzenia państwa ma skutki znacznie groźniejsze, to jest podważa stabilność społeczną i polityczną państwa, dążąc do delegitymizacji jego władz i podważenia prawa rządu sprawującego władzę do sprawowania jej. Stosowany mechanizm jest prosty: społeczeństwo, oddając w demokratycznych wyborach władzę, zawiera z nowo wybraną władzą kontrakt, zgadzając się na płacenie podatków, przestrzeganie prawa, oraz inne obciążenia wynikające z bycia obywatelem danego państwa w zamian za opiekę, jaką państwo sprawować powinno nad swoimi obywatelami.

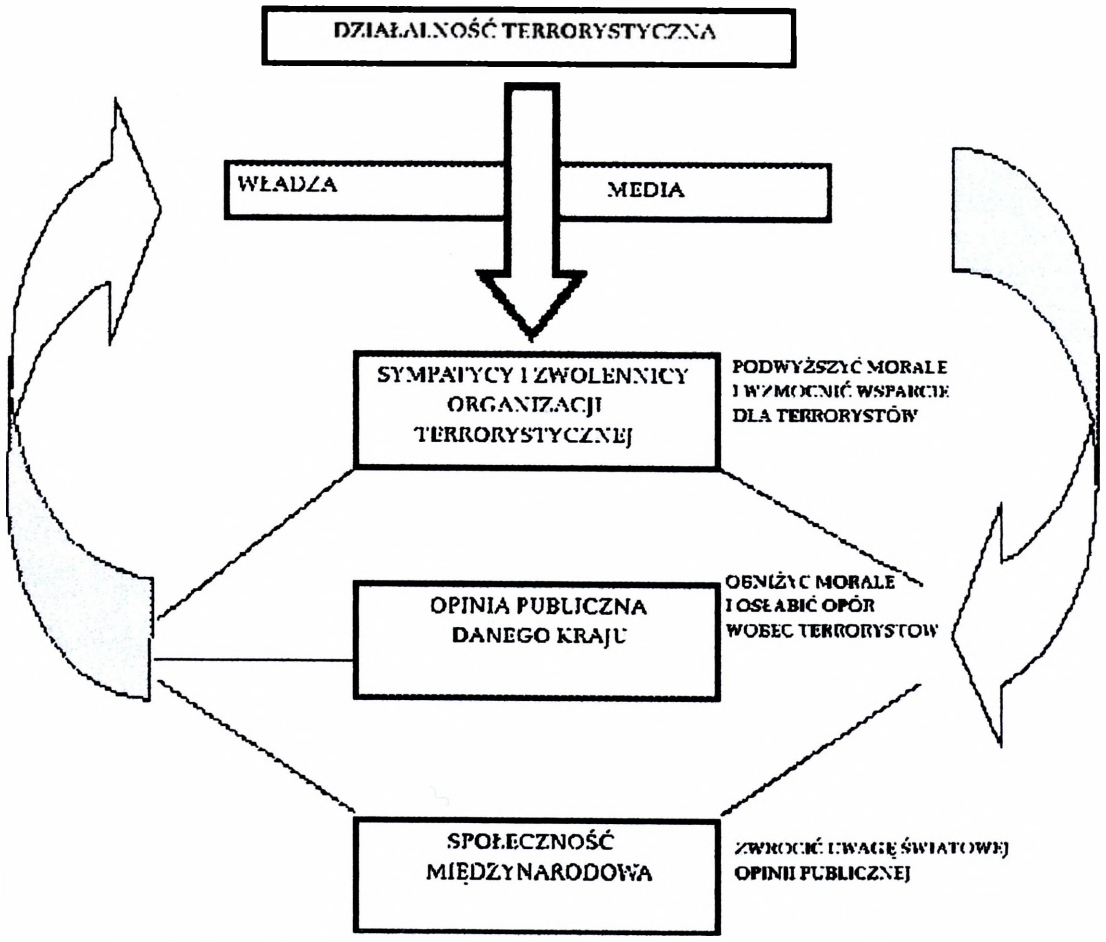
Opieka ta szczególnie postrzegana jest w dziedzinie bezpieczeństwa. Zapewnienie go jest jednym z najważniejszych obowiązków władz, przy użyciu wszystkich dostępnych im instrumentów i narzędzi, tj. sił policyjnych, wojska, służb specjalnych itd. Z tego względu atak terrorystyczny, przeprowadzony na terytorium danego państwa, w którym giną jego obywatele, a gospodarka ponosi poważne straty, interpretowany jest jako niedotrzymanie przez władze ich części umowy. Dlatego też tak wielkie siły angażowane są w zapobieganie atakom terrorystycznym, a jeżeli zapobieżenie im nie jest możliwe – w minimalizację i likwidację ich skutków.[162]

Przekonanie społeczeństwa, że władze są w stanie podołać wyzwaniu, jakie stanowi zbliżający się – bądź trwający w danym momencie – kryzys terrorystyczny, jest warunkiem początkowym dla rozpoczęcia procesu efektywnego przeciwdziałania terroryzmowi. Utrzymanie przez rząd legitymizacji podejmowanych przez niego działań w obszarze bezpieczeństwa stanowi gwarancję przeprowadzenia tych działań do końca – albo w celu zapobieżenia atakowi, albo w celu poradzenia sobie przez państwo z jego skutkami. Platformą, która może posłużyć do przekazania społeczeństwu takiego komunikatu na skalę masową są współczesne media.

---

[161] Ibidem, s. 134.
[162] Patrz także: Liedel K., Piasecka P., *Jak przetrwać w dobie zagrożeń terrorystycznych? Elementy edukacji antyterrorystyczne:*, Warszawa 2008, s. 23.

Z tego właśnie względu media są czynnikiem, który odgrywa poważną rolę w systemie przeciwdziałania terroryzmowi – o ile państwo posiada prawno – organizacyjne warunki do wykorzystywania ich oraz strategię współpracy, która pozwala na prowadzenie takich działań. W innych okolicznościach media pozostają niewiadomą w sytuacji zagrożenia terrorystycznego, czynnikiem, który równie dobrze może posłużyć realizacji celów rządu, jak i przysłużyć się do realizacji celów, które założyła sobie podczas przygotowań do ataku organizacja terrorystyczna. Termin „media" jest – co warto podkreślić – terminem o szerokim znaczeniu, obejmującym wszelkie rodzaje mediów. Oznacza on nie tylko media tradycyjne, ale także Internet, który stał się w XXI wieku nieodłącznym elementem życia społecznego i politycznego. Umiejętne wykorzystywanie tego narzędzia w celu informowania, edukowania i komunikowania ze społeczeństwem może stać się niezwykle cennym elementem systemu przeciwdziałania zagrożeniom terrorystycznym.



Rys. 16: Relacje: ataki terrorystyczne – media – ośrodki opinii publicznej – władza

Źródło: *ICT Papers on Terrorism*, The International Policy Institute for Counter-Terrorism, Jerusalem[163].

[163] *ICT Papers on Terrorism*, The International Policy Institute for Counter-Terrorism, Jerusalem, Israel 2002, s. 27 [cyt. za:] Kuba Jałoszyński, *Współczesny wymiar antyterroryzmu*, Warszawa 2008, s. 63.

Pamiętać trzeba, że media są we współczesnym świecie wszechobecne. Ich wpływowi podlegają nie tylko szerokie grupy społeczne, do których skierowany jest przekaz masowy. Przekaz medialny wpływa – bezpośrednio lub pośrednio – zarówno na zwykłych obywateli, jak i na wybrane przez nich (wybrane to w tym wypadku słowo – klucz) władze, ofiary ataków terrorystycznych i ich rodziny, inne media oraz samych terrorystów.

Terroryści na społeczeństwo wpływać mogą zasadniczo jedynie poprzez media. Atak terrorystyczny wywiera ogromny wpływ na ofiary, jak i ich najbliższych, ale do szeroko pojętej opinii publiczne dociera jedynie poprzez przekaz medialny. Także przekaz ideologiczny terrorystów, określający ich cele i wyjaśniający stosowaną strategię przepływa przede wszystkim poprzez media. Bez mediów, z ich wolnością, umiejętnością dotarcia wszędzie i przekazania praktycznie każdego wydarzenia w czasie niemalże rzeczywistym, komunikacja terrorystów ze społeczeństwem byłaby niemalże niemożliwa.

Trzeba poświęcić szczególną refleksję temu, jakie niebezpieczne, z punktu widzenia społecznej i polityczne stabilności państwa, przynosić mogą relacje medialne związane z działalnością terrorystyczną. Pierwszym zagadnieniem, które w związku z tym trzeba poddać analizie, jest oczywiście fakt, że relacja medialna może uczynić z – w intencji obiektywnej – relacji płaszczyznę ekspresji poglądów terrorystów. Nie bez powodu od kilkudziesięciu lat społeczność międzynarodowa dąży do sporządzenia definicji terroryzmu. Jest to zjawisko, które ze względu na swoją polityczną naturę powiązane jest często ze szczytnymi sprawami, takimi jak walka o wolność, niepodległość, prawo do stanowienia o sobie – pod takimi hasłami terroryści atakują. Przekaz medialny, który pomija środki używane przez terrorystów, a zatem zabijanie niewinnych osób, nienawiść skierowaną przeciwko całemu kręgowi cywilizacyjnemu, oderwaną od konkretnych dążeń politycznych – taki przekaz może sprawić, że społeczeństwo usłyszy racje tylko jednej strony, czyli terrorystów.

Kolejny poważny problem to fakt, iż spektakularność ataków i efekt, jaki wywołują one w poszczególnych państwach, oraz sposób, w jaki wpływają one na funkcjonowanie całej społeczności międzynarodowej, może stanowić dla innych ugrupowań zachętę do naśladowania takich taktyk i strategii.

Ostatni, lecz z pewnością nie najmniej ważny, aspekt stanowiący o konieczności stosowania przez rząd odpowiednich strategii komunikacyjnych i współpracy z mediami, to sytuacja, w której prowadzona jest operacja antyterrorystyczna. Jak już zostało powiedziane, media są wszechobecne. Terroryści – co również zostało wskazane – tak samo jak rządy i społeczeństwa – podlegają ich wpływowi. W wypadku kryzysu zakład niczego może to być bardzo zasadniczy wpływ – emitowane na żywo przygotowania pododdziałów antyterrorystycznych do szturmu mogą uniemożliwić skuteczne przeprowadzenie akcji antyterrorystycznej, eliminując element zaskoczenia i umożliwiając terrorystom przygotowanie się na szturm.

Wśród badaczy pojawia się pogląd, że media traktować należy jako „ratowników – pierwszych na miejscu zdarzenia" (ang. first responders).[164] Często przybywają na miejsce zdarzenia, zanim zareagować zdąży ktokolwiek inny – dlatego mogą odegrać niezmiernie istotną rolę w zapobieganiu fali paniki, która może nastąpić po zamachu terrorystycznym. Dlatego właśnie w miarę możliwości przyjąć należy wobec mediów postawę sojusznika, a nie wroga, nie traktować ich jako dodatkowego ciężaru. Dotyczy to zresztą nie tylko urzędników szczebla centralnego, ale – może nawet bardziej – lokalnych sztabów zarządzania kryzysowego. Wskazówki dla ludności co do pożądanego sposobu zachowania, informacje o miejscach, w których można uzyskać pomoc najłatwiej przekazać jest właśnie poprzez media.[165]

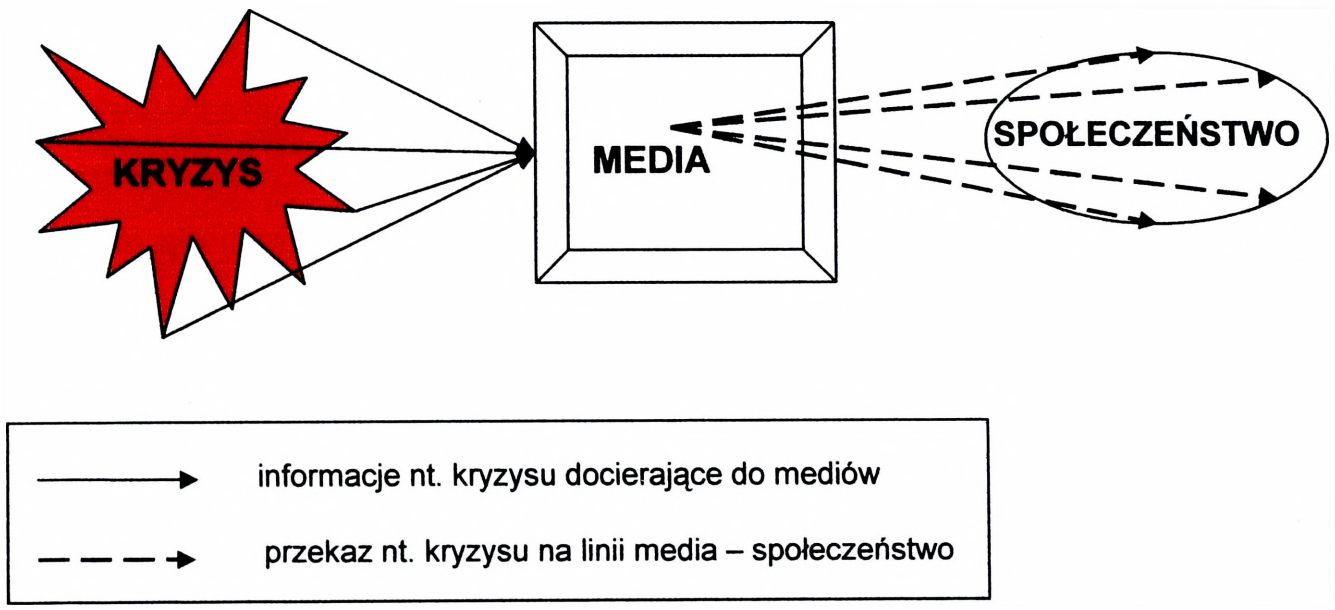
Nie można także pominąć kwestii określanej przez administrację amerykańską jako „wygrywanie serc i dusz". Realizowanie działań propagandowych, skierowanych do społeczeństwa, niewątpliwie wymaga pośrednictwa mediów. Żadne ze współczesnych państw nie może pozwolić sobie na pominięcie tego aspektu przeciwdziałania terroryzmowi. Co ważne w tym wypadku nie wystarczy samo poleganie na dobrej woli mediów. Dla przedstawiania publicznie i masowo informacji, które rząd bądź nawet społeczność międzynarodowa chcą przekazać, potrzebna jest też stosowana ilość wiedzy u przedstawicieli mediów, którzy przygotowują materiały na temat kryzysu bądź możliwości zaistnienia kryzysu. Dlatego istotne jest w procesie budowania mechanizmów współpracy pomiędzy mediami i administracją publiczną uwzględnienie zapewnienia możliwości edukacyjnych, prezentujących wieloaspektowe podejście

[164] Ethiel N. (ed.), *Terrorism: Informing the Public,* Chicago, Illinois 2002, s. 174.
[165] Ibidem, s. 175.

do problemu, który jest przyczyną kryzysu. Wsparcie mediów w tym zakresie leży w najlepiej pojętym interesie rządu państwa i jego obywateli.

Media występują w życiu społecznym w czterech podstawowych rolach[166]:

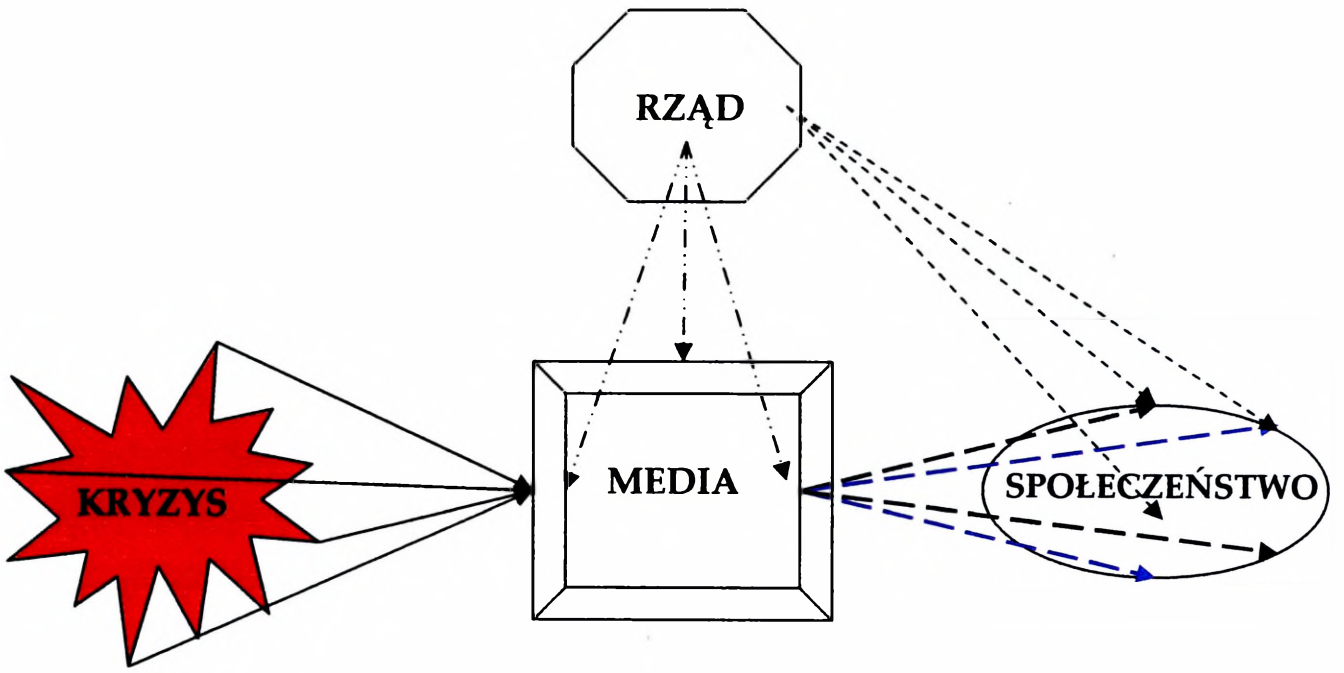
- tłumacza rzeczywistości – łącząc i przedstawiając powiązania pomiędzy faktami z życia publicznego nadają sens wydarzeniom, które w innym wypadku mogłyby się wydać społeczeństwu niezrozumiałe,
- płaszczyzny prezentacji informacji, poglądów i opinii,
- drogowskazu – rekomendującego określony sposób postępowania w danej sytuacji,
- filtru rzeczywistości – prezentującego wybrane wydarzenia i wybrane ich interpretacje.



Rys. 17: Docieranie informacji o kryzysie do społeczeństwa za pośrednictwem mediów – bez udziału administracji
Źródło: opracowanie własne

Wszystkie te role, a nawet każda z nich osobno, sprawiają, że administracja publiczna powinna w mediach szukać raczej sprzymierzeńca, niż toczyć z nim spory – szczególnie w sytuacji kryzysu i zagrożenia ładu i porządku publicznego.

[166] Jabłoński W., *Kreowanie informacji. Media relations*, op. cit., s. 56.



Rys. 18: Docieranie informacji o kryzysie do społeczeństwa za pośrednictwem mediów – z udziałem administracji
Źródło: opracowanie własne

W sytuacji wystąpienia kryzysu media bez wątpienia pełnią wspomniane wcześniej role: filtru rzeczywistości i jej tłumacza. Właściwie skonstruowana strategia komunikacyjna rządu, skierowana nie tylko do społeczeństwa, ale także specyficznie do samych mediów, może umożliwić pewną modyfikację przekazów medialnych w taki sposób, aby służyły one realizacji celów polityki antyterrorystycznej rządu, tj.:

- minimalizacji paniki,
- informowaniu społeczeństwa o działaniach podejmowanych przez administrację publiczną w celu minimalizacji i likwidacji kryzysu i jego skutków,
- informowaniu społeczeństwa o pożądanych zachowaniach,

– informowaniu społeczeństwa o potencjalnych, wtórnych zagrożeniach.

Teoretycznie wydaje się, ze rozwiązaniem byłoby doprowadzenie do tego, aby media – kierując się albo mechanizmami autoregulacji, albo narzuconymi z zewnątrz mechanizmami regulacji prawnych – zaprzestały relacjonowania wydarzeń związanych z terroryzmem. Jednak we współczesnym świecie, którego cechą jest niezwykle szybki postęp technologiczny w dziedzinie narzędzi komunikacji, w dobie coraz bardziej powszechnego dostępu do Internetu, taka efektywna i powszechna cenzura nie jest możliwa – i to tylko biorąc pod uwagę względy techniczne. Nie można bowiem zapominać o tym, że zastosowanie takich rozwiązań, nie byłoby niczym innym, jak poddaniem sposobu funkcjonowania współczesnych państw wpływowi ugrupowań terrorystycznych, a zatem ustąpieniem pola w walce o kształt i prawo do nadawania tego kształtu mechanizmów społecznych zgodnie z wolą obywateli, a nie próbujących ich zastraszyć terrorystów. Wydaje się zatem, że celem odpowiedzialnej władzy powinno być poszukiwanie takich sposobów współpracy z mediami, które ustanowią sojusz na rzecz bezpieczeństwa i wolności, zamiast czynienia z mediów narzędzie ideologicznego przekazu ugrupowań terrorystycznych.

Aby podjąć próbę budowania mechanizmów takiej współpracy pomiędzy mediami i administracją publiczną, warto zastanowić się, na jakich płaszczyznach – w porównaniu do ugrupowań terrorystycznych, mogą rządy wykorzystywać media[167].

Tab. 12: Wykorzystanie mediów przez ugrupowania terrorystyczne i administrację publiczną

WYKORZYSTANIE MEDIÓW	
UGRUPOWANIE TERRORYSTYCZNE	**ADMINISTRACJA PUBLICZNA**
Propaganda	Propaganda
Komunikacja	Komunikacja
Dezinformacja	Dezinformacja
Szkolenie	Szkolenie
Zdobywanie informacji	Zdobywanie informacji

Źródło: opracowanie własne na podstawie Bartosz Bolechów, *Terroryzm i media*, w: *Hiszpania: media masowe i wybory w obliczu terroryzmu,* op. cit.

[167] Bolechów B., *Terroryzm i media*, w: *Hiszpania: media masowe i wybory w obliczu terroryzmu*, (red.) Bogusława Dobek-Ostrowska, Michał Kuś, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2007, s. 29.

Pierwszą z nich jest z całą pewnością płaszczyzna propagandowa. Warto zastanowić się nad tym, że jeśli terroryści mogą wykorzystywać media, jako narzędzie rozpowszechniania własnego przekazu, to podobnie może – i powinien! – postępować rząd. Społeczeństwo ma prawo wiedzieć – a rząd ma obowiązek informować – jakie działania w imieniu tegoż społeczeństwa są podejmowane. Rząd powinien być w stanie jasno przedstawić nie tylko swoją strategię antyterrorystyczną, ale też wyjaśnić, jakiemu właściwie zagrożeniu ma ona przeciwdziałać.

To ostatnie ma związek z kolejnym istotnym aspektem wykorzystywania mediów w walce z terroryzmem. Terroryzm nie jest zjawiskiem, które dałoby się określić, jako rozumiane instynktownie. Ze względu na to, że służy ono efektywne realizacji celów politycznych – szerokiego wachlarza celów politycznych – istnieje niebezpieczeństwo przegrania przez rząd tzw. wojny o rząd dusz, czego dotyczyła wcześniejsza refleksja. Pamiętać jednak należy, że perswazja nie jest podstawową metodą używaną przez terrorystów. Najważniejszą z metod używanych przez takie ugrupowania jest strach. Panika, jaką sieje udany zamach terrorystyczny, może zakłócić funkcjonowanie całych grup społecznych nie tylko w czasie trwania kryzysu, ale także długo po jego zakończeniu. Z tego względu niezwykle istotna jest funkcja edukacyjna, jaką spełniać mogą media. Panika to stan emocjonalny, którego występowanie wiąże się przede wszystkim z lękiem przed nieznanym, z zetknięciem z sytuacją, której nie jesteśmy w stanie stawić czoła – głównie ze względu na brak wiedzy o tym, czym jest zagrożenie, jakie ze sobą niesie. Z tego względu niezmiernie ważnym elementem systemu przeciwdziałania terroryzmowi jest rola informacyjna, jaką pełnić mogą media w sytuacji zaistnienia kryzysu terrorystycznego, przekazując społeczeństwu wskazówki, dotyczące optymalnych algorytmów zachowania w sytuacji bezpośredniego zagrożenia życia.

Działania takie powinny zresztą mieć charakter długofalowy, zapewniając trwałą edukację społeczeństwa i zapewniając, że będzie ono nie tylko w stanie zapewnić sobie maksymalne bezpieczeństwo poprzez właściwe reagowanie na zbliżające się niebezpieczeństwo, ale także będzie w stanie stać się partnerem służb stojących na straży bezpieczeństwa państwa – choćby poprzez informowanie o podejrzanych zachowaniach, które mogą stanowić symptomy przygotowań do przeprowadzenia ataku terrorystycznego.

Dezinformacja, która stanowi kolejną płaszczyznę potencjalnego wykorzystania mediów w walce z terroryzmem, posłużyć może przede wszystkim zapobieżeniu katastrofalnym skutkom bieżącego przekazu medialnego w sytuacji przygotowywania operacji antyterrorystycznej. Wystarczy bowiem wspomniany już wyżej brak elementu zaskoczenia w odniesieniu do przygotowywanego szturmu, aby ofiarami braku dbałości o właściwą komunikację i kontakty z mediami padli zarówno funkcjonariusze biorący udział w szturmie, jak i ci, którym mają oni nieść pomoc.

Innym aspektem potencjalnego wykorzystania mediów dla zapobiegania terroryzmowi może być gromadzenie informacji. Media docierają do osób i miejsc, do których często mają wyłączny dostęp. Śledzenie doniesień medialnych, nie tylko w odniesieniu do działań samych ugrupowań terrorystycznych, ale też zmieniających się warunków i okoliczności, które mogą zwiększyć bądź zmniejszyć ryzyko ataku terrorystycznego, pozwala na utrzymanie systemu przeciwdziałania terroryzmowi w stanie optymalnej gotowości do działania.

Przedstawione powyżej płaszczyzny, na jakich rozpatrywać można wykorzystywanie mediów jako elementu systemu przeciwdziałania terroryzmowi wskazują, że lekceważenie mediów jako elementu życia społecznego i politycznego, jest nie tylko niewskazane – jest po prostu niemożliwe. Zapomnienie o mediach i o zaplanowaniu strategii postępowania z nimi spowodować może tylko jeden skutek: wykorzystane zostaną one przez terrorystów.

Dlatego też ważne jest określenie celów, do realizacji jakich dążyć powinna administracja publiczna w kontaktach z mediami w sytuacji zagrożenia terrorystycznego. Jednym z najważniejszych z nich jest oczywiście stabilizowanie sytuacji społecznej w sytuacji kryzysu i komunikowanie się ze społeczeństwem w celu informowania o podejmowanych działaniach dla zapewnienia bezpieczeństwa państwa i jego obywateli[168].

Działania takie mają jednak często – przynajmniej w krótkiej perspektywie – postać, która może okazać się uciążliwa dla społeczeństwa. Tak odbierane mogą być na przykład działania dla zapewnienia bezpieczeństwa lotnictwa cywilnego, to jest szczegółowe kontrole bezpieczeństwa przed wejściem na pokład samolotu, czy też zakaz wnoszenia płynów na pokład statku powietrznego. Dlatego też celem, do któ-

[168] *Is the Public Getting Sound Information on Terrorism?* [w:] Ethiel N. (ed.), *Terrorism: Informing the Public (Cantigny Conference Series Conference Report)*, op. cit., s. 41.

rego dążyć powinna administracja publiczna jest zapewnienie odpowiedniego odbioru podejmowanych przez nią działań, a zatem kształtowanie pozytywnego obrazu podejmowanych działań. Jest to niezmiernie istotne z punktu widzenia zapewnienia współpracy społeczeństwa w przeciwdziałaniu terroryzmowi. Poinformowanie obywateli o tym, jaki cel i sens mają zintensyfikowane kontrole bezpieczeństwa pozwoli nie tylko na wyjaśnienie przyczyn ich wprowadzenia: odpowiednio zakomunikowane może uświadomić społeczeństwu, że rząd podejmuje wszelkie dostępne działania na rzecz bezpieczeństwa obywateli. W ten sposób zamiast przyczyną rosnącego niezadowolenia społecznego z powodu uciążliwości, może stać się pomostem pomagającym w zrozumieniu mechanizmów, jakich wykorzystywanie konieczne jest dla bezpieczeństwa i porządku publicznego.

Kolejnym ważnym celem administracji publicznej w budowaniu strategii komunikacyjnej i systemu wykorzystania mediów w obszarze bezpieczeństwa publicznego powinno być nawiązanie współpracy z przedstawicielami mediów dla celów uwydatnienia cech terroryzmu, które sprawiają, że jest on nieakceptowany z moralnego i społecznego punktu widzenia. Wśród takich działań znaleźć się powinno przede wszystkim dążenie do podkreślania kryminalnego charakteru czynów o charakterze terrorystycznym. Nie wolno bowiem dopuścić do wspomnianego już rozmycia świadomości przestępczego charakteru aktów terrorystycznych w debacie o ideologicznych i politycznych przyczynach zamachów terrorystycznych. Posiadanie społeczeństwa jako sojusznika nie może wynikać ze strachu lub tylko regulacji prawnych – przekonanie zatem obywateli o słuszności współpracy z rządem w zakresie zwalczania czynu, który pod względem moralnym nie może znaleźć swojego miejsca w demokratycznym społeczeństwie nie tylko pozwoli na przedstawicie we właściwym świetle działań rządowych, ale długofalowo służyć może zapobieganiu rozpowszechniania się terroryzmu jako metody realizacji celów politycznych, o którym to zagrożeniu wspomniano wcześniej.

Szczególne zasady dotyczące relacji mediów z rządem powinny mieć swoje twarde podstawy prawne w sytuacji trwającego incydentu terrorystycznego. Jest to zresztą jeden z obszarów, w których państwo wypracować powinno właśnie regulacje prawa powszechnego, a nie jedynie strategii komunikacyjnej. W sytuacji bezpośredniego zagrożenia życia i zdrowia konieczne jest posiadanie przez administrację publiczną i wchodzące w jej skład służby narzędzi, które umożliwią nie tylko współ-

pracę z mediami, ale także narzucenie im jej zasad. Nie wynika to bynajmniej z braku wiary w dobre chęci przedstawicieli mediów. Jednak w sytuacji, w której trwający kryzys terrorystyczny i przygotowywana reakcja służb odbywają się według algorytmów postępowania często obcych światu mediów, konieczne może stać się – ze względu na ochronę życia i zdrowia ludzi – zmuszenie mediów do postępowania pod dyktando przedstawicieli prawa.

Omówione kwestie, dotyczące postępowania z mediami - i prawnych podstaw tegoż postępowania – w sytuacji trwającego kryzysu terrorystycznego, stanowią punkt wyjścia dla kolejnych rozważań, związanych z zarządzaniem kryzysem terrorystycznym poprzez informację, jej zdobywanie i dystrybucję.

Pierwszą – i zapewne najważniejszą – zasadą kontaktów z mediami podczas kryzysu terrorystycznego, jest konieczność dostarczenia im wiarygodnych informacji co do przebiegu podejmowanych działań na poziomie strategicznym.[169] Tak, jak niezbędne jest chronienie informacji na poziomie operacyjnym i taktycznym ze względu na zagrożenia dla życia i zdrowia ludzi, jakie mogłoby spowodować ujawnienie takich informacji, tak konieczne jest zapewnienie przedstawicielom mediów dostępu do informacji o ogólnym przebiegu kryzysu. Skąd przekonanie, że w sytuacji kryzysu takie postępowanie jest konieczne?

Media są wszechobecne i stanowią – zarówno dla rządu, jak i dla terrorystów – najlepszą platformę komunikacji ze społeczeństwem. Przedstawicielom administracji publicznej nie wolno o tym fakcie zapominać. Media muszą zdobywać informacje. Od przygotowania przedstawicieli administracji publicznej zależy, jakie będą źródła tych informacji i jak zostaną one zinterpretowane. Jeśli administracja publiczna zaniedba tego, co w języku angielskim określane jest mianem „karmienia bestii" (ang. *feeding the beast*)[170], zadba o to ktoś inny. Media znajdą swoje źródła informacji. Może stać się nim administracja publiczna, przedstawiająca swoją wizję sytuacji, kierująca za pośrednictwem mediów określony przekaz do społeczeństwa. Jest to szczególnie istotne, jeśli wziąć pod uwagę to, co powiedziano już wcześniej o potrzebie kształtowania właściwego obrazu podejmowanych działań i kształtowaniu pozytywnego obrazu zarówno tych działań, jak też ogólnej sytuacji i starań podejmowanych przez rząd na rzecz państwa i jego obywateli.

---

[169] Ibidem, s. 71.
[170] Bolechów B., *Terroryzm i media*, op. cit., s. 31.

Istotnym elementem starań o zachowanie pozytywnego wizerunku rządu i jego działań jest także monitorowanie relacji medialnych oraz dynamiczne reagowanie na zmiany w tych przekazach. Szczególnie w wypadku pojawiania się szkodliwych plotek, albo relacji zniekształcających obraz akcji podejmowanych dla przeciwdziałania zagrożeniu konieczne jest dementowanie takich pogłosek i zapobieganie przejęciu kontroli nad przekazem medialnym przez terrorystów i ich punkt widzenia na społeczną i polityczną rzeczywistość, w tym zapobieganie sprzyjającemu terrorystom przekazowi opisującymi działania rządu jako nieudolne i nie spełniające wymogów sytuacji.

Istotnym skądinąd mechanizmem, który można wykorzystać w takiej sytuacji, jest realny dialog z mediami. Jego przedmiotem powinno być nie tylko relacjonowanie samego kryzysu terrorystycznego, ale także same relacje rząd – media. Powinny być one relacjami umożliwiającymi traktowanie mediów jako odpowiedzialnego partnera, skłonnego do tego, aby w sytuacji kryzysowej stosować pewne mechanizmy autoregulacji, które pozwolą mediom na uniknięcie manipulacji organizacji terrorystycznych.

Powyższe zasady, dotyczące budowania relacji z mediami oraz zarządzania kryzysem terrorystycznym poprzez odpowiednie gromadzenie i dystrybucję informacji nie są zasadami czysto teoretycznymi. Stosowane są przez wiele państw w związku z ich doświadczeniami z atakami terrorystycznymi i wymogami, jakie państwo musi spełnić, aby efektywnie im przeciwdziałać oraz minimalizować i likwidować ich skutki. Przykładem analizy działań koniecznych dla efektywnej współpracy z mediami jest sporządzony przez amerykańską Grupę Zadaniową ds. Zamieszek i Terroryzmu raport[171]. Warto przytoczyć najważniejsze zawarte w nim rekomendacje, które mogą pomoc w całościowym spojrzeniu na to, jakie mechanizmy są konieczne dla zbudowania prawidłowej relacji pomiędzy administracją publiczną i mediami w sytuacji zagrożenia terrorystycznego,

Jednym z najważniejszych zapisów raportu jest zalecenie dotyczące konieczności wyznaczenia grupy reporterów, którzy relacjonować będą atak terrorystyczny w imieniu wszystkich mediów. Zastosowanie takiego mechanizmu ułatwia nie tylko monitoring przekazu, ale także indywidualne postępowanie z poszczególnymi przedstawicielami mediów oraz komunikowanie się z nimi w kontekście zamierzonych ce-

[171] Ibidem, s. 32.

lów prowadzonej operacji. Jest to bardzo ważne nie tylko w odniesieniu do merytorycznej zawartości realizowanego przekazu, ale także w kontekście możliwości nałożenia potencjalnych ograniczeń technicznych (jak użycie oświetlenia, kamer i in. nowoczesnych technologii rejestrowania informacji), które mogą ułatwić przeprowadzenie operacji antyterrorystycznej.

W zakresie merytorycznego kształtowania przekazu medialnego szczególnie istotne są zasady dotyczące ograniczenia wywiadów z terrorystami w czasie kryzysów z wzięciem zakładników. Umożliwia to zachowanie równowagi pomiędzy relacjonowaniem propagandy terrorystycznej i konkurującego z nią stanowiska źródeł oficjalnych.

Do podobnej kategorii należą zasady związane z opóźnianiem lub ograniczaniem publikowania i nagłaśniania szczegółów, które mogłyby zaognić sytuację. W trakcie kryzysu zakładniczego nieodpowiedzialne podchodzenie do relacji medialnych może spowodować podjęcie przez terrorystów radykalnych decyzji i doprowadzenie do nieodwracalnych działań, na przykład zabicia zakładników.

Zasady bezpieczeństwa, które stosowane mają być nie tyle przez media, ile przez przedstawicieli administracji publicznej w kontaktach z mediami obejmują natomiast przede wszystkim ochronę informacji. W wypadku informacji taktycznych, dotyczących szczegółów planowanej operacji, zapewnienie bezpieczeństwa informacyjnego stanowić może o różnicy pomiędzy udaną a nieudaną akcję antyterrorystyczną, a stuki zaniedbań w tym obszarze liczone są ilością ofiar.

Powyższe zasady dotyczą przede wszystkim reagowania w sytuacji trwającego kryzysu terrorystycznego. Nie można jednak nie zauważyć, że pozostają one w bezpośrednim związku z opisywaną powyżej ogólną strategią zarządzania kryzysem terrorystycznym: zarówno na poziomie kształtowania pozytywnego wizerunku działań służb państwowych, kształtowania relacji z mediami poprzez traktowanie ich jako partnera z wykorzystaniem mechanizmów autoregulacji, jak i w obszarze ochrony informacji i narzucania określonych zasad reagowania w sytuacji bezpośredniego zagrożenia życia i zdrowia ludzkiego.

Są to zasady, które przyświecać powinny rządowej strategii komunikowania kryzysowego zarówno na poziomie strategicznym, jak i w sytuacji reagowania na bieżące wydarzenia. Tak zwany dobry PR (public relations) jest niezbędnym warun-

kiem funkcjonowania każdej administracji, a szczególnie prawdziwa staje się ta zasada w sytuacji kryzysowej – jest warunkiem efektywnego realizowania zadań przez te administrację.

W obszarze bezpieczeństwa zawsze będą takie kategorie informacji, których ujawnić nie wolno – ich ujawnienie sprowadzić mogłoby zagrożenie dla państwa i jego obywateli. W każdym kryzysie zidentyfikować można jednak również kategorię informacji, które przekazywać nie tylko można, ale nawet trzeba: informacje dotyczące tego, jak obywatele mogą sami przyczynić się do zwiększenia swojego bezpieczeństwa, jak mogą współpracować z państwem w celu ochrony siebie i swoich bliskich, co rząd robi dla ich bezpieczeństwa i jak mogą się w te działania zaangażować.

4.7 Bezpieczeństwo informacyjne

4.7.1 Bezpieczeństwo i ochrona informacji niejawnych

Rozważając kwestie przechowywania danych dotyczących terroryzmu i przeciwdziałania temu zjawisku, pamiętać należy o tym, że w znacznej większości dane te mają charakter niejawny – szczególnie dotyczy to danych gromadzonych w ramach działań operacyjno – rozpoznawczych. Zapewnienie bezpieczeństwa tych informacji w systemie zarządzania jest jednym z najważniejszych elementów funkcjonowania systemu – w przeciwnym wypadku zebrane przez dany podmiot lub instytucję informacje, dane i produkty ich przetwarzania mogą zostać obrócone przeciwko wytwórcy, zamiast służyć realizacji jego celów.

Z tego względu szczególnie istotne jest takie skonstruowanie przepisów dotyczących ochrony informacji niejawnych, które nie tylko zabezpieczają te dane w sposób efektywny, ale także pozwalają na ich wymianę i wykorzystanie ich w systemie przeciwdziałania terroryzmowi. Środki bezpieczeństwa ustalone w celu ochrony informacji niejawnych w systemie przeciwdziałania terroryzmowi muszą zatem spełniać kilka podstawowych warunków:

- muszą odnosić się i obejmować wszystkie osoby mające dostęp do informacji niejawnych, wszystkie urządzenia służące obróbce informacji niejawnych, nośniki informacji oraz pomieszczenia, w których przechowywane są informacje, urządzenia służące ich przetwarzaniu,

- muszą także być tak skonstruowane, aby wykrywać osoby, których zatrudnienie mogłoby naruszyć bezpieczeństwo informacji niejawnych, a także prowadzić do zwolnienia takich osób,
- muszą uniemożliwiać dostęp osób nieuprawnionych do informacji niejawnych,
- muszą zapewniać, że informacje przekazywane są według zasady *need-to-know*, czyli tylko w razie zaistnienia takiej potrzeby.

Podstawą dla ochrony informacji niejawnych jest ich właściwa klasyfikacja, która ma na celu ochronę tych informacji, których ochrona jest konieczna – a z drugiej strony unikanie zawyżania klauzul ochronnych dla informacji, które powinny być dystrybuowane pomiędzy poszczególnymi podmiotami działającymi w systemie bezpieczeństwa państwa.

Informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo innej zleconej pracy.

Za ochronę informacji niejawnych odpowiedzialne powinny być służby ochrony państwa. Ochrona ta powinna zapewniać bezpieczeństwo informacji w szczególności przed:

1) działaniem obcych służb specjalnych;
2) zamachem terrorystycznym lub sabotażem;
3) kradzieżą lub zniszczeniem materiału;
4) próbą wejścia osób nieuprawnionych;
5) nieuprawnionym dostępem pracowników do materiałów oznaczonych wyższą klauzulą tajności[172].

Systemy i sieci teleinformatyczne, w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego przez służby ochrony państwa.

Bezpieczeństwo informacji niejawnych zapewniane być musi w czterech podstawowych płaszczyznach:

- organizacyjno – proceduralnej,

[172] Janczak J., Świdzikowski G., *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*, AON - Warszawa 2004, s. 39

- personalnej,
- fizycznej,
- technicznej[173].

Rys. 19: Klasyfikacja środków bezpieczeństwa informacji
Źródło: opracowanie własne.

4.7.2 Ujęcie proceduralno – organizacyjne

Płaszczyzna proceduralno – organizacyjna to płaszczyzna związana z obowiązującymi w danym państwie przepisami dotyczącymi ochrony informacji niejawnych. Przepisy takie muszą określać[174]:

1) sposób organizowania ochrony informacji niejawnych;
2) klasyfikowania informacji niejawnych;
3) udostępniania informacji niejawnych;
4) postępowania sprawdzającego, w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy;
5) szkolenia w zakresie ochrony informacji niejawnych;

[173] Ibidem, s. 39.
[174] Forystek M., *Audyt informatyczny*, Warszawa 2005, s. 155.

6) ewidencjonowania, przechowywania, przetwarzania i udostępniania danych uzyskiwanych w związku z prowadzonymi postępowaniami o ustalenie rękojmi zachowania tajemnicy, w zakresie określonym w ankiecie bezpieczeństwa osobowego oraz w kwestionariuszu bezpieczeństwa przemysłowego;
7) organizacji kontroli przestrzegania zasad ochrony informacji niejawnych;
8) ochrony informacji niejawnych w systemach i sieciach teleinformatycznych;
9) stosowania środków fizycznej ochrony informacji niejawnych.

4.7.3 Bezpieczeństwo personalne

Bezpieczeństwo personalne dotyczy przede wszystkim zapewnienia, że osoby, które uzyskują dostęp do informacji niejawnych dają rękojmię zachowania tajemnicy. W celu upewnienia się, że dana osoba spełnia takie wymagania przeprowadza się postępowanie sprawdzające. W toku postępowania sprawdzającego ustala się, czy dana osoba nie jest podejrzewana o[175]:

1) uczestnictwo, współpracę lub popieranie działalności szpiegowskiej, terrorystycznej, sabotażowej albo innej wymierzonej przeciwko państwu;
2) ukrywanie informacji mających znaczenie dla ochrony informacji niejawnych, a także występowanie związanych z tą osobą okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji;
3) nieprzestrzeganie porządku prawnego danego państwa;
4) zagrożenia ze strony obcych służb specjalnych w postaci prób werbunku lub nawiązania kontaktu, a zwłaszcza obawy o wywieranie w tym celu presji;
5) potencjalne niewłaściwe postępowanie z informacjami niejawnymi;
6) nieuzasadnioną różnicę między poziomem życia a uzyskiwanymi dochodami;
7) chorobę psychiczną lub inne zakłócenia czynności psychicznych ograniczające sprawność umysłową i mogące negatywnie wpłynąć na zdolność do zajmowania stanowiska albo wykonywania prac związanych z dostępem do informacji niejawnych stanowiących tajemnicę państwową;

[175] Opracowanie własne na podstawie *Ustawy o ochronie informacji niejawnych*, Dz.U. 1999.11.95.

8) uzależnienie od alkoholu lub narkotyków.

W celu dokonania powyższych ustaleń służba ochrony państwa powinna mieć uprawnienia do zobowiązania danej osoby do poddania się specjalistycznym badaniom oraz udostępnienia wyników tych badań. W systemie pranym regulującym powyższe kwestie powinno także zaistnieć uregulowanie mówiące, że w razie niedających się usunąć wątpliwości, co do rękojmi zachowania tajemnicy prze daną osobą, interes ochrony informacji niejawnych ma pierwszeństwo przed innymi prawnie chronionymi interesami.

W celu zapewnienia pełnego bezpieczeństwa personalnego informacji niejawnych, system bezpieczeństwa informacji, powinien zapewniać także, że osoby mające dostęp do informacji niejawnych:

- przechodzą odpowiednie przeszkolenia w zakresie postępowania z informacjami niejawnymi,
- zostali uświadomieni w zakresie celów polityki zabezpieczenia informacji niejawnych[176].

4.7.4 Bezpieczeństwo fizyczne

Bezpieczeństwo fizyczne informacji niejawnych zapewniane być powinno przy wzięciu pod uwagę odpowiednich uwarunkowań, tj.:

- stopnia tajności i kategorii chronionych informacji,
- liczby informacji i ich formy,
- upoważnień wydanych personelowi przez odpowiednie władze bezpieczeństwa,
- oceny zagrożeń ze strony obcych służb wywiadowczych, aktów sabotażu i terroryzmu, oraz innych działań o charakterze antypaństwowym bądź kryminalnym[177].

[176] Janczak J., Świdzikowski G., *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym,* op. cit., s. 44.
[177] Ibidem, s. 46.

W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych, należy w szczególności:

- wydzielić strefy bezpieczeństwa, które poddane są szczególnej kontroli wejść i wyjść oraz kontroli przebywania;
- wydzielić wokół stref bezpieczeństwa strefy administracyjne służące do kontroli osób lub pojazdów;
- wprowadzić system przepustek lub inny system określający uprawnienia do wejścia, przebywania i wyjścia ze strefy bezpieczeństwa, a także przechowywania kluczy do pomieszczeń chronionych, szaf pancernych;
- zapewnić kontrolę stref bezpieczeństwa i stref administracyjnych przez przeszkolonych zgodnie z ustawą pracowników pionu ochrony;
- stosować wyposażenie i urządzenia służące ochronie informacji niejawnych, którym na podstawie odrębnych przepisów przyznano certyfikaty lub świadectwa kwalifikacyjne.

Strefy bezpieczeństwa, ustanawiane w procesie organizacji bezpieczeństwa informacji niejawnych, mogą być chronione różnorodnymi środkami[178]:

- służba wartownicza,
- sejfy, szafy [pancerne i skarbce,
- drzwi i zamki,
- okna i kraty.

4.7.5 Bezpieczeństwo techniczne

Szczególną rolę w gromadzeniu, przetwarzaniu i przekazywanie informacji – również informacji niejawnych – odgrywają coraz częściej systemy teleinformatyczne. Dzieje się tak przede wszystkim ze względu na zapewnianą przez nie możliwość szybkiego dostępu do zgromadzonych informacji, symultanicznego przetwarzania znacznych ilości danych, a także przesyłania danych w czasie rzeczywistym. Z tego względu szczególną uwagę poświęcić należy technicznemu zabezpieczeniu systemów telekomunikacyjnych i informatycznych służących przetwarzaniu, gromadzeniu

[178] Forystek M., *Audyt informatyczny,* op. cit., s. 166.

oraz dystrybucji informacji niejawnych. Systemy i sieci teleinformatyczne, w których mają być wytwarzane, przechowywane lub przekazywane informacje niejawne, powinny zostać akredytowane przez służby ochrony państwa.

Szczegółowe przepisy powinny określić w szczególności podstawowe wymagania bezpieczeństwa teleinformatycznego w zakresie ochrony fizycznej, elektromagnetycznej, kryptograficznej, niezawodności transmisji, kontroli dostępu w sieciach lub systemach teleinformatycznych służących do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych. W dokumentach szczególnych wymagań bezpieczeństwa określić należy środki ochrony kryptograficznej, elektromagnetycznej, technicznej i organizacyjnej systemu lub sieci teleinformatycznej. Procedury bezpiecznej eksploatacji obejmować powinny sposób i tryb postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych oraz określają zakres odpowiedzialności użytkowników systemu lub sieci teleinformatycznych i pracowników mających do nich dostęp.[179]

4.7.6 Ochrona informacji niejawnych w NATO i Unii Europejskiej

Współczesne państwa, które funkcjonują na arenie międzynarodowej i są aktywnymi uczestnikami stosunków międzynarodowych, dla zachowania pełnej zdolności do funkcjonowania na formach międzynarodowych przyjmują na siebie zobowiązania do przestrzegania prawno-międzynarodowych reżimów dotyczących najważniejszych obszarów funkcjonowania organizacji międzynarodowych, których są członkami.

W odniesieniu do zagadnień związanych z bezpieczeństwem antyterrorystycznym państwa, które związane jest z aktywnym przeciwdziałaniem zagrożeniu o charakterze globalnym, konieczne jest wzięcie pod uwagę przepisów ochrony informacji niejawnych narzucanych przez najważniejsze instytucje, na forum których prowadzona jest aktywna współpraca międzynarodowa w tym zakresie: Unii Europejskiej oraz organizacji Traktatu Północnoatlantyckiego.

W odniesieniu do ochrony informacji niejawnych, przepisy tych dwóch organizacji są do siebie zbliżone ze względu na wykorzystanie w systemie unijnym doświad-

[179] Ibidem, s. 167.

czeń NATO. Dokumenty prawno-międzynarodowe, które tworzą zręby systemów ochrony informacji niejawnych dystrybuowanych w Unii Europejskiej i NATO, to:

- Umowa pomiędzy stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzona w Brukseli dnia 6 marca 1997 r.,
- Umowa pomiędzy stronami Traktatu Północnoatlantyckiego o współpracy w dziedzinie informacji atomowych, sporządzona w Paryżu dnia 18 czerwca 1964 r.,
- C-M (2002) 49 – Bezpieczeństwo w ramach Organizacji Traktatu Północnoatlantyckiego oraz dokumenty wykonawcze,
- Decyzji RADY z dnia 19 marca 2001 r. w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa 2001/264/WE z dnia 19 marca 2001 r.,
- Decyzja KOMISJI zmieniająca jej regulamin wewnętrzny 2001/844/WE, EWWiS, Euratom z dnia 29 listopada 2001 r.

Podstawowe cele bezpieczeństwa, wspólne dla obu systemów, określone między innymi w Decyzji RADY z dnia 19 marca 2001 r. w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa[180], są następujące:

a) zabezpieczenie informacji niejawnych przed szpiegostwem, ujawnieniem lub nieuprawnionym rozpowszechnieniem;
b) zabezpieczenie informacji przetwarzanych w systemach i sieciach łączności i informacji przed groźbą naruszenia ich integralności i dostępności;
c) zabezpieczenie obiektów służących do przechowywania informacji przed sabotażem oraz złośliwym, umyślnym uszkodzeniem;
d) w przypadku nie zachowania środków bezpieczeństwa, dokonanie oceny powstałych szkód, ograniczenie ich konsekwencji i przyjęcie niezbędnych środków zaradczych.

Informacje zarówno NATO, jak i UE, o charakterze niejawnym udostępniane są na zasadzie *need-to-know*, czyli wspomniane w poprzednim podrozdziale zasadzie potrzeby dostępu do danej informacji. Są zatem udostępniane wyłączeni osobom, którym są niezbędne w celu wykonywanie powierzonych im obowiązków i tylko w niezbędnym do tego celu zakresie.

---

[180] DECYZJA RADY z dnia 19 marca 2001 r. w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa, (2001/264/WE), Dz.U. UE L z dnia 11 kwietnia 2001 r.

Obie organizacje stosują własne klasyfikacje informacji niejawnych, zapewniając w ten sposób odpowiednią ochronę poszczególnym ich kategoriom. Zgodnie z przepisami, dotyczącymi nakładania klauzul niejasności, informacja powinna być objęta klauzulą tajności tylko wtedy, gdy jest to konieczne. Klauzula musi być wyraźnie i prawidłowo naniesiona. Może być utrzymywana tylko przez niezbędny okres. Wyłącznie wytwórca odpowiada za nadanie klauzuli oraz, następnie, za jej obniżenie lub zniesienie. Urzędnicy i inni pracownicy organów tych organizacji międzynarodowych mogą nadawać klauzule, obniżać je lub znosić wyłącznie na polecenie lub za zgodą dyrektora departamentu.

Na mocy przepisów obu organizacji w każdym kraju zobowiązanym do stosowania standardów NATO i UE w zakresie ochrony informacji niejawnych wyodrębnia się wyspecjalizowane podmioty, które odpowiadają za implementację zobowiązań w tym zakresie. Określane są one mianem „krajowych władz bezpieczeństwa".

Osoby, które mają mieć dostęp do informacji niejawnych NATO i UE powinna podlegać sprawdzeniu prowadzonemu przez „krajowe władze bezpieczeństwa". Procedury te, podobnie jak krajowe postępowania sprawdzające, mają na celu stwierdzenie, czy dana osoba daje gwarancję lojalności, swoim, zachowaniem i cechami charakteru zapewnia właściwe postępowanie z informacjami niejawnymi, a także czy może być podatna na naciski ze strony obcych i zewnętrznych instytucji bądź osób. Osoby, które zostaną pozytywnie zweryfikowane, muszą przejść odpowiednie szkolenie w zakresie ochrony informacji klasyfikowanych oraz złożyć oświadczenie, w którym potwierdzają fakt przeszkolenia oraz świadomość odpowiedzialności za ujawnienie informacji klasyfikowanych.

Obie organizacje w przepisach dotyczących ochrony informacji niejawnych, zapewniają funkcjonowanie także fizycznych środków bezpieczeństwa, odpowiednio zabezpieczonych (w tym przed podglądem i podsłuchem) stref bezpieczeństwa oraz odpowiednich kancelarii tajnych. Obiekty, w których przechowywane są informacje niejawne NATO i UE muszą podlegać szczegółowej kontroli dostępu, a także zaopatrzone być w plany reagowania w sytuacjach kryzysowych.

Przepisy formułowane przez obie organizacje dotyczą także bezpieczeństwa teleinformatycznego (INFOSEC). Obejmuje ono określenie i zastosowanie środków ochrony informacji przetwarzanych, przechowywanych lub przesyłanych w syste-

mach teleinformatycznych lub innych elektronicznych, przed utratą ich poufności, integralności i dostępności, zarówno przypadkową, jak i zamierzoną. Wymagane jest podjęcie odpowiednich środków przeciwdziałania w celu zapobiegania przypadkom: uzyskania dostępu do informacji klasyfikowanych UE przez osoby nieupoważnione, uniemożliwienia uzyskania dostępu osobom upoważnionym oraz wprowadzania nieupoważnionych zmian lub niszczenia informacji klasyfikowanych UE. Obie instytucje posiadają także odpowiednie organy doradcze, konsultacyjne i wykonawcze, odpowiedzialne za koordynację i realizację polityki bezpieczeństwa informacyjnego.

Poniżej zaprezentowane zostały wytyczne dotyczące zakładania klauzul bezpieczeństwa na informacje niejawne wytwarzane w państwach członkowskich. Ich analiza pozwala na zrozumienie filozofii bezpieczeństwa, która stanowi podstawę systemu ochrony informacji niejawnych w UE[181]:

Tab. 13: Klauzule klasyfikacji informacji niejawnych w UE

KLAUZULA NIEJAWNOŚCI INFORMACJI	WARUNKI NAŁOŻENIA KLAUZULI	UPRAWNIENIA DO NADANIA KLAUZULI	UPRAWNIENIA DO ZNIESIENIA LUB OBNIŻENIA KLAUZULI
TRES SECRET UE/EU TOP SECRET	Klauzulę nadaje się tylko informacji lub materiałowi, których nieupoważnione ujawnienie mogłoby spowodować: bezpośrednie zagrożenie wewnętrznej stabilności UE lub jednego z Państw Członkowskich lub państwa przyjaźnie nastawionego, narazić na wyjątkowo duże szkody stosunki z przyjaźnie nastawionymi rządami, bezpośrednio spowodować utratę życia wielu osób, wyrządzić wyjątkowo duże szkody operacyjnym zdolnościom lub bezpieczeństwu Państw Członkowskich lub sił zbrojnych innych uczestników, lub też utrzymaniu skuteczności wyjątkowo ważnych działań wywiadowczych lub w sferze bezpieczeństwa, spowodować poważne i długotrwałe szkody gospodarcze w skali UE lub poszczególnych Państw Członkowskich.	klauzulę nadają odpowiednio upoważnione osoby (wytwórcy), dyrektorzy generalni, szefowie służb. Wytwórcy są zobowiązani do określenia daty lub okresu, gdy klauzula informacji może zostać obniżona lub zniesiona, w przeciwnym razie są oni zobowiązani do przeprowadzania przynajmniej raz na 5 lat przeglądu dokumentów w celu dokonania oceny, czy nadana klauzula nadal jest konieczna.	zniesienia lub obniżenia klauzuli dokonać może wyłącznie jej wytwórca; jest on zobowiązany do poinformowania o zmianie wszystkich odbiorców informacji, do których przesłał dokument lub dla których wykonał jego kopię.

[181] Ibidem.

KLAUZULA NIEJAWNOŚCI INFORMACJI	WARUNKI NAŁOŻENIA KLAUZULI	UPRAWNIENIA DO NADANIA KLAUZULI	UPRAWNIENIA DO ZNIESIENIA LUB OBNIŻENIA KLAUZULI
SECRET UE	klauzulę nadaje się tylko informacji lub materiałowi, których nieupoważnione ujawnienie mogłoby spowodować: napięcia w stosunkach międzynarodowych, narazić na szkodę stosunki z przyjaźnie nastawionymi rządami, wywołać zagrożenie utraty życia lub poważnie zagrozić porządkowi publicznemu, bezpieczeństwu osób lub ich swobodom, wyrządzić poważne szkody operacyjnym zdolnościom lub bezpieczeństwu Państw Członkowskich lub sił zbrojnych innych uczestników, lub też utrzymaniu skuteczności ważnych działań wywiadowczych lub w sferze bezpieczeństwa, spowodować istotne szkody materialne dla UE lub dla finansowych, monetarnych, ekonomicznych lub handlowych interesów któregoś z Państw Członkowskich,	klauzulę nadają odpowiednio upoważnione osoby (wytwórcy), dyrektorzy generalni, szefowie służb. Wytwórcy są zobowiązani do określenia daty lub okresu, gdy klauzula informacji może zostać obniżona lub zniesiona, w przeciwnym razie są oni zobowiązani do przeprowadzania przynajmniej raz na 5 lat przeglądu dokumentów w celu dokonania oceny, czy nadana klauzula nadal jest konieczna.	zniesienia lub obniżenia klauzuli dokonać może wyłącznie jej wytwórca; jest on zobowiązany do poinformowania o zmianie wszystkich odbiorców informacji, do których przesłał dokument lub dla których wykonał jego kopię.
CONFIDENTIEL UE	klauzulę nadaje się tylko informacji lub materiałowi, których nieupoważnione ujawnienie mogłoby spowodować: istotną szkodę w zakresie stosunków dyplomatycznych, tzn. spowodować formalne protesty lub zastosowanie innych sankcji, narazić na szkodę bezpieczeństwo osób lub ich swobody, zaszkodzić operacyjnym zdolnościom lub bezpieczeństwu Państw Członkowskich lub sił zbrojnych innych uczestników, lub też skuteczności ważnych działań wywiadowczych lub w sferze bezpieczeństwa, poważnie osłabić finansowe podstawy funkcjonowania istotniejszych organizacji, utrudnić prowadzenie śledztwa lub ułatwić popełnienie poważnego przestępstwa, być niezgodne z finansowymi, monetarnymi, ekonomicznymi lub handlowymi interesami UE lub jej Państw Członkowskich, poważnie utrudnić rozwój lub realizację istotnych kierunków polityki UE, zablokować lub w inny sposób istotnie przeszkodzić w prowadzeniu ważnych działań UE	klauzulę nadają odpowiednio upoważnione osoby (wytwórcy), dyrektorzy generalni, szefowie służb. Wytwórcy są zobowiązani do określenia daty lub okresu, gdy klauzula informacji może zostać obniżona lub zniesiona, w przeciwnym razie są oni zobowiązani do przeprowadzania przynajmniej raz na 5 lat przeglądu dokumentów w celu dokonania oceny, czy nadana klauzula nadal jest konieczna.	zniesienia lub obniżenia klauzuli dokonać może wyłącznie jej wytwórca; jest on zobowiązany do poinformowania o zmianie wszystkich odbiorców informacji, do których przesłał dokument lub dla których wykonał jego kopię.

KLAUZULA NIEJAWNOŚCI INFORMACJI	WARUNKI NAŁOŻENIA KLAUZULI	UPRAWNIENIA DO NADANIA KLAUZULI	UPRAWNIENIA DO ZNIESIENIA LUB OBNIŻENIA KLAUZULI
RESTREINT UE	Klauzulę nadaje się tylko informacji lub materiałowi, których nieupoważnione ujawnienie mogłoby spowodować: istotną szkodę w zakresie stosunków dyplomatycznych, spowodować istotne niedogodności dla osób, utrudnić utrzymanie operacyjnych zdolności lub bezpieczeństwa Państw Członkowskich lub sił zbrojnych innych uczestników, spowodować straty finansowe lub też ułatwić czerpanie nieuzasadnionych zysków lub korzyści przez osoby lub przedsiębiorców, naruszyć właściwe rozwiązania przyjęte w celu zachowania poufności informacji przekazanych przez strony trzecie, naruszyć obowiązujące ograniczenia dotyczące ujawniania informacji, utrudnić prowadzenie śledztwa lub ułatwić popełnienie przestępstwa, niekorzystnie wpłynąć na przebieg handlowych lub politycznych negocjacji prowadzonych przez UE lub Państwa Członkowskie z innymi podmiotami, utrudnić rozwój lub realizację istotnych kierunków polityki UE, utrudnić odpowiednie zarządzanie UE i jej działaniami.	Klauzulę nadają odpowiednio upoważnione osoby (wytwórcy), dyrektorzy generalni, szefowie służb. Wytwórcy są zobowiązani do określenia daty lub okresu, gdy klauzula informacji może zostać obniżona lub zniesiona, w przeciwnym razie są oni zobowiązani do przeprowadzania przynajmniej raz na 5 lat przeglądu dokumentów w celu dokonania oceny, czy nadana klauzula nadal jest konieczna.	Zniesienia lub obniżenia klauzuli dokonać może wyłącznie jej wytwórca; jest on zobowiązany do poinformowania o zmianie wszystkich odbiorców informacji, do których przesłał dokument lub dla których wykonał jego kopię.

Źródło: opracowanie własne

Podobna analiza potrzebna jest w odniesieniu do klauzul, którymi oznacza swoje informacje niejawne NATO.

Tab. 14: Klauzule klasyfikacji informacji niejawnych w NATO

KLAUZULA NIEJAWNOŚCI INFORMACJI	RODZAJ INFORMACJI OZNACZONYCH KLAUZULĄ
COSMIC TOP SECRET (CTS)	Klauzulą oznaczane są informacje, których nieupoważnione ujawnienie spowodowałoby szczególnie poważne szkody w stosunku do całego Sojuszu Północnoatlantyckiego.
NATO SECRET (NS)	Klauzulą oznacza się informacje, których nieupoważnione ujawnienie spowodowałoby poważne szkody w stosunku do całego Sojuszu Północnoatlantyckiego.
NATO CONFIDENTIAL (NC)	Klauzulą oznacza się informacje, których nieupoważnione ujawnienie spowodowałoby powstanie szkód w zakresie interesów NATO.
NATO RESTRICTED (NR)	Klauzulą oznacza się informacje, których nieuprawnione ujawnienie spowodowałoby, że interesy NATO zostałyby postawione w niekorzystnej sytuacji.

KLAUZULA NIEJAWNOŚCI INFORMACJI	RODZAJ INFORMACJI OZNACZONYCH KLAUZULĄ
ATOMAL	Klauzulą oznaczane są informacje niejawne USA, które obłożone zostały klauzulą na mocy ustawy o energii atomowej z 1954 r. lub informacje niejawne Wielkiej Brytanii o klauzuli ATOMIC, które zostały przekazane NATO.
NATO UNCLASSIFIED (NU)	Klauzulę oznacza się informacje, które są własnością NATO, ale nie spełniają kryteriów wymaganych dla nałożenia na nie klauzuli niejawności – dostęp do nich dla osób spoza NATO jest dozwolony, o ile nie będzie szkodliwy dla NATO

Źródło: opracowanie własne

4.8 Wnioski

Jak wykazano w poprzednich dwóch rozdziałach pracy, informacja jest tym czynnikiem, który warunkuje efektywność wszelkich działań na rzecz bezpieczeństwa państwa – a także każdego innego podmiotu, który może stać się obiektem jakiegokolwiek ataku.

Bezpieczeństwo informacyjne jest zatem – mimo, iż pośrednio – warunkiem *sine qua non* bezpieczeństwa państwa. Właściwie skonstruowane mechanizmy pozwalające zarówno na ochroną własnych informacji pod względem technicznym, fizycznych, personalnym i organizacyjnym, są niezbędnym elementem systemu bezpieczeństwa państwa.

Szczególna sytuacja występuje jednak w odniesieniu do przeciwdziałania zagrożeniom o charakterze terrorystycznym. Ze względu na to, iż terroryzm jest zjawiskiem immanentnie międzynarodowym, podobny charakter muszą mieć także mechanizmy jego zwalczania. Z tego względu międzynarodowa współpraca w przeciwdziałaniu terroryzmowi jest tym komponentem przeciwdziałania zjawisku, który nie może zostać wyeliminowany.

Konieczne zatem jest uwzględnienie nie tylko krajowych mechanizmy zabezpieczania informacji, ale także mechanizmów tworzonych i wdrażanych na forach organizacji międzynarodowych, szczególnie tych, które prowadzą aktywne działania w zakresie przeciwdziałania terroryzmowi, jak Unia Europejska i NATO.

Rozdział 5

Systemy informacji w przeciwdziałaniu terroryzmowi – wybrane rozwiązania

5.1 System amerykański – Narodowe Centrum Kontr-Terrorystyczne

W amerykańskim systemie przeciwdziałania terroryzmowi jedną z najważniejszych ról odgrywa Narodowe Centrum Kontr-Terrorystyczne (*National Counter Terrorism Center – NCTC*)[182]. Instytucja ta powołana została w ramach Biura Dyrektora Wywiadu Narodowego na mocy Ustawy o Reformie Wywiadu, wprowadzającej liczne poprawki do Aktu Bezpieczeństwa Narodowego z 1947 r.

Do zadań Narodowego Centrum Kontr-terrorystycznego należy:

- pełnienie funkcji podstawowej organizacji Rządu USA odpowiedzialnej za analizowanie i integrowanie wszystkich informacji wywiadowczych posiadanych i zdobywanych przez Rząd USA, dotyczących terroryzmu i kontr-terroryzmu, z wyjątkiem informacji odnoszących się do terroryzmu wewnętrznego,
- prowadzenie strategicznego planowania operacyjnych działań kontr-terrorystycznych, integrujących wszystkie elementy i możliwości kraju, z włączeniem narzędzi dyplomatycznych, finansowych, militarnych, wywiadowczych, bezpieczeństwa wewnętrznego oraz służb wdrażania prawa zarówno wewnątrz, jak i pomiędzy agencjami,
- przypisywanie ról i odpowiedzialności, jako część realizowania obowiązku planowania strategicznego, wiodącym Departamentom i agencjom zajmującym się kontr-terroryzmem w zakresie działań kontr-terrorystycznych, ale nie nadzorowanie wykonania żadnych wynikających z tego przypisania operacji,

[182] Opracowanie na podstawie materiałów z wizyty studyjnej autora pracy (jako Naczelnika Wydziału ds. Przeciwdziałania zagrożeniom terrorystycznym w MSWiA) w National Counterterrorism Center w listopadzie i grudniu 2006 r.

- zapewnić dostęp agencji do informacji wywiadowczych ze wszystkich źródeł, niezbędnych do realizowania planów kontr-terrorystycznych i wykonywania niezależnych, alternatywnych analiz,
- zapewnić dostęp agencji do informacji wywiadowczych niezbędnych do wykonania przypisanych im zadań,
- służyć jako centralny bank wspólnej wiedzy na temat znanych i domniemanych terrorystów i międzynarodowych grup terrorystycznych, ich celów, strategii, zdolności, sieci kontaktów i wsparcia.

Narodowe Centrum Kontr-terrorystyczne może mieć dostęp, za zgodą Prezydenta, do informacji dotyczących terroryzmu wewnętrznego, z jakiegokolwiek federalnego, stanowego bądź lokalnego źródła, niezbędnych do realizowania jego zadań, a także przechowywać i dystrybuować takie informacje.

Każda agencja, która w zakresie swoich kompetencji ma prowadzenie działań kontr-terrorystycznych, może zwrócić się do Narodowego Centrum Kontr-terrorystycznego o informacje, które stanowiłyby pomoc w wypełnianiu jej zadań.

W skład NCTC wchodzą przedstawiciele następujących instytucji:

- Federalne Biuro Śledcze,
- Departament Obrony,
- Centralna Agencja Wywiadowcza,
- Departament Bezpieczeństwa Wewnętrznego,
- Departament Stanu,
- Departament Energii,
- Komisja Regulacji Nuklearnych,
- Departament Zdrowia i Usług dla Ludności,
- Departament Rolnictwa,
- Policja Kapitolu,
- Departament Skarbu.

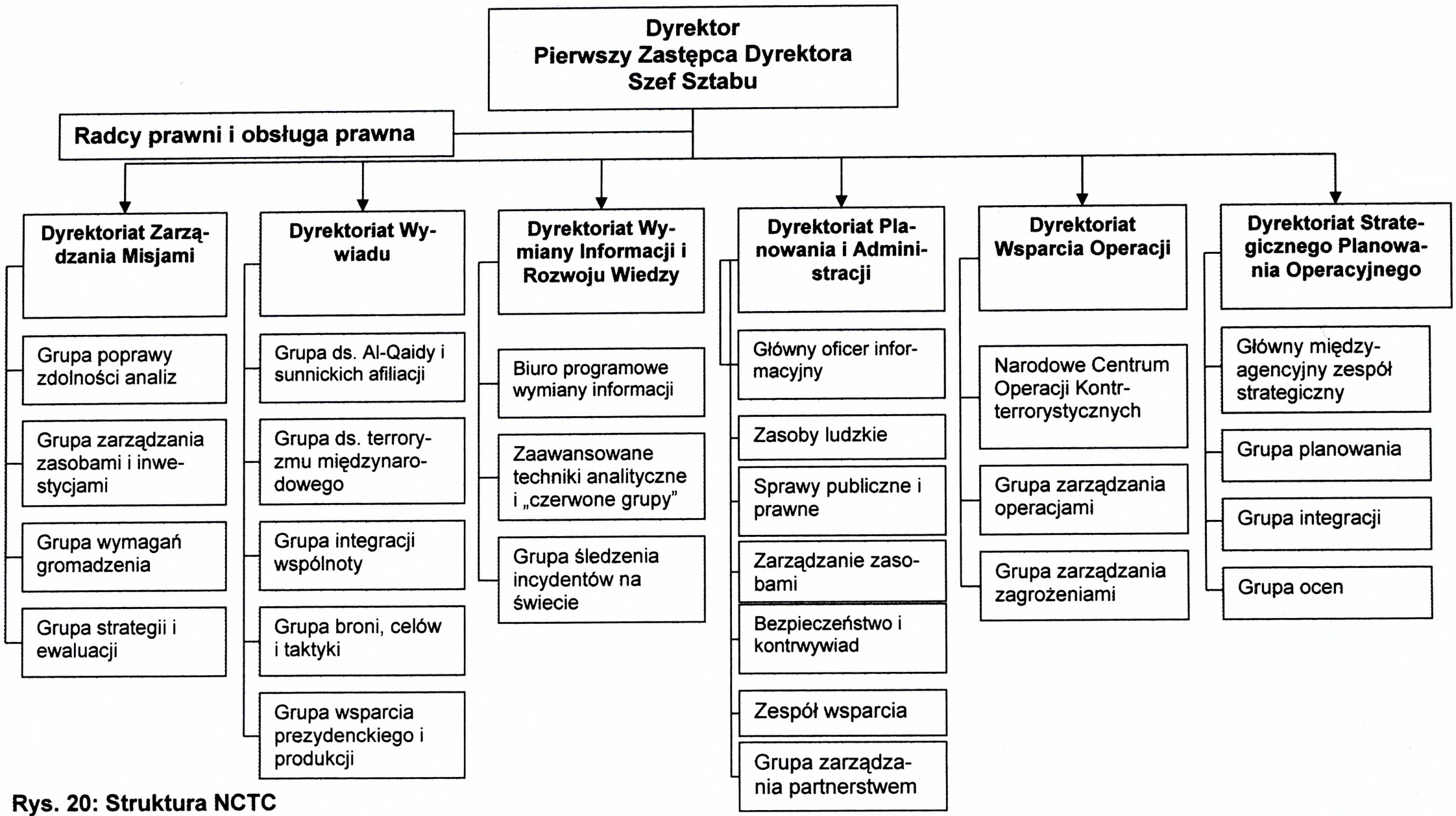
Przedstawiciele poszczególnych instytucji zatrzymują uprawnienia właściwe dla macierzystych jednostek.

W skład NCTC wchodzą także osoby reprezentujące instytucje rządu amerykańskiego spoza wspólnoty wywiadowczej ustanowionej Aktem Bezpieczeństwa Na-

rodowego. Wspierają oni strategiczne grupy planistyczne i reprezentują ponad 200 podmiotów należących do struktur rządu federalnego.

NCTC wspierane jest także przez partnerów udzielających wsparcia w zakresie technologii informacyjnych oraz wsparcia operacyjnego.

Zgodnie z informacjami przedstawianymi przez NCTC w dalszych planach pozostaje stworzenie struktury organizacyjnej składającej się z małej, stałej kadry tworzącej rdzeń organizacji wspieranej przez delegatów innych instytucji w celu zapewnienia wysokiej zdolności NCTC do działania z jednoczesną ochroną praw podmiotów wnoszących wkład w jego funkcjonowanie.



Rys. 20: Struktura NCTC
Źródło: niepublikowane materiały z wizyty studyjnej

Filarami NCTC określane są dwa piony istniejące w systemie bezpieczeństwa narodowego USA:

- wywiad, podlegający Dyrektorowi Wywiadu Narodowego (*Director of National Intelligence*) oraz
- strategiczne planowanie operacyjne, podlegające Prezydentowi USA.

Filar wywiadowczy zapewnia zarządzanie misjami w zakresie zapewniania bezpieczeństwa państwa, analizę oraz właściwą wymianę informacji. Filar strategicznego planowania operacyjnego przyczynie się do koordynowania wszystkich elementów narodowej siły, tj. potencjału ekonomicznego, dyplomatycznego, militarnego, bezpieczeństwa wewnętrznego, sił prawa i porządku publicznego oraz wywiadu. Jest on niezbędny dla integrowania wysiłków w tych wszystkich obszarach oraz zapewnienia możliwości oceny podejmowanych działań.

Strategiczne planowanie operacyjne, zgodnie z doktryną amerykańską, wypełnia luką pomiędzy polityką i tworzeniem strategii a wykonywaniem operacji kontrterrorystycznych. Strategię i politykę bezpieczeństwa narodowego w USA tworzą Narodowa Rada Bezpieczeństwa i Dyrektor Wywiady Narodowego. Operacje kontrterrorystyczne wykonują odpowiedzialne za poszczególne obszary bezpieczeństwa narodowego departamenty i agencje.

NCTC pełni zadania, które znajdują się na drodze pomiędzy polityką i strategią, a operacjami, które służą ich realizacji. Realizując te zadania, NCTC:

- nie kieruje wykonaniem żadnych operacji,
- określa bezpośrednie cele i zadania dla departamentów i agencji,
- koordynuje międzyagencyjne plany operacyjne,
- przypisuje departamentom i agencjom obszary, w których pełnią rolę wiodącą,
- dokonuje przeglądu alokacji zasobów,
- dokonuje ocen wyników działań podejmowanych przez poszczególne agencje i departamenty.

Wszystkie powyższe działania realizowane są w ramach tworzonego przez NCTC Narodowego Planu Wdrożeniowego oraz Kontr-Terrorystycznego Planu Wywiadowczego.

Wśród elementów Narodowego Planu Wdrożeniowego znajdują się segmenty zawierające plany w dziedzinie:

- ochrony i obrony (*Protect and Defend – ProDef*),
- atakowania terrorystów (*Attack Terrorists – ATC*),
- przeciwdziałania radykalnemu islamowi (*Counter Violent Islamic Terrorism – CVIE*),
- zapobieganiu użyciu / zdobycie przez terrorystów broni masowego rażenia (*Prevent Terrorist Use/Acq of WMD – WMD-T*).

Realizacji Planu we wszystkich jego obszarach towarzyszy rozwijanie partnerstwa międzynarodowego oraz dążenie do instytucjonalizacji strategii w wymiarze narodowym i międzynarodowym.

Na poziomie wykonawczym – Plan realizowany jest przez Departamenty, Agencje oraz Narodowe Centrum Kontr-terrorystyczne. Dla celów realizacji Planu poszczególne w/w podmioty tworzą odpowiednio:

- Departamenty i Agencje – Plany Wsparcia (*Supporting Plans*),
- NCTC – wybrane Narodowe Plany Działania(np. Narodowy Plan Zwalczania Użycia przez Terrorystów Internetu i Narodowy Plan Zwalczania Zagranicznych Bojowników).

5.1.1 Analiza

Jednym z najważniejszych zadań NCTC jest pozostawanie wiodącą siłą w zakresie analizy wywiadowczej. W tym obszarze za najważniejszy priorytet uznawane jest formułowanie ostrzeżeń o zagrożeniu, drugim zadaniem zaś jest dokonywanie analiz strategicznych.

Te dwie kategorie zadań realizowane są poprzez powstawanie „produktów analitycznych", wśród których znajdują się:

- Raport o Terroryzmie dla Wyższych Urzędników,
- specjalne analizy NCTC,
- wywiadowcze oceny, alerty i ostrzeżenia,
- *Terrorism Dispatch*, biuletyn tygodniowy,
- *Terrorism Review*, biuletyn dwutygodniowy,

- *Wątki zagrożenia*.

Z tych „produktów analitycznych" korzystają, realizując swoje bieżące działania, zarówno czynniki decyzyjne odpowiedzialne za politykę bezpieczeństwa państwa, jak i podmioty wykonawcze w administracji rządowej, Kongres, zagraniczni łącznicy oraz stanowe i lokalne urzędy.

Analizy te są szczególne ze względu na kilka czynników. Pierwszym z nich jest zmienny skład zespołów opracowujących poszczególne pozycje – są to przedstawiciele 15 agencji wchodzących w skład amerykańskiej „wspólnoty wywiadów". W trakcie opracowywania raportów i analiz mają oni dostęp do informacji, jakiego nie zapewnia żadna instytucja poza NCTC. Ponadto wszystkie wymienione „produkty analityczne" podejmują wyzwania prognostyczne. Celem ich powstawania jest zatem nie tylko analizowanie tego, co już się stało, ale także przewidywanie tego, co może się zdarzyć w przyszłości. Dla zapewnienia trwania tych wartości dodanych płynących z funkcjonowania NCTC, instytucja ta podejmuje liczne działania.

Pierwszym z nich jest zapewnienie funkcjonowania licznych forów i mechanizmów wymiany informacji nt. terroryzmu. Stworzone zostało na przykład Narodowe Centrum Kontr-terrorystyczne on-line (NCTC Online), które zapewnia reprezentantom wspólnoty wywiadowczej dostęp do informacji nt. terroryzmu, rozpoczęte i zakończone procesy analizy wywiadowczej, wątki czasowe rozwoju wydarzeń związanych z zagraniami terrorystycznymi oraz portale do innych baz danych. W ramach NCTC Online funkcjonuje 5 500 indywidualnych kont użytkowników, którzy miesięcznie przeglądają za ich pośrednictwem ponad 1 milion stron. Ta platforma informatyczna zapewnia jednocześnie funkcjonowanie forów internetowych użytkowników, konta e-mail oraz chat, umożliwiając szeroko pojętą wymianę informacji i doświadczeń.

W ciągu każdego dnia NCTC przygotowuje i prowadzi trzy telekonferencje z udziałem przedstawicieli Narodowej Rady Bezpieczeństwa oraz przedstawicieli wspólnoty wywiadowczej. Oprócz utrzymywanych na bieżąco aktywnych kontaktów z przedstawicielami instytucji odpowiedzialnych za bezpieczeństwo USA, NCTC utrzymuje bogate kontakty w ramach swojej współpracy z partnerami międzynarodowymi. W toku tych kontaktów następuje wymiana informacji, analiz oraz poglądów na zagadnienia związane z terroryzmem międzynarodowym. W toku tych kontaktów wy-

korzystywane są środki elektroniczne, dla zapewnienia łączności z kluczowymi centrami kontr-terrorystycznymi na świecie.

NCTC utrzymuje bazę danych pochodzących ze wszystkich dostępnych źródeł. Zawiera ona między innymi 400 000 nazwisk i aliasów reprezentujących ponad 300 000 osób powiązanych z międzynarodowym terroryzmem. Zapewnia ona informacje dotyczące tożsamości poszczególnych terrorystów, a także dane osób znajdujących się na liście podejrzanych, stanowiącej fazę przejściową do administrowanego przez FBI Centrum Obserwacji Terrorystów (*Terrorist Screening Center*).

5.1.2 Wsparcie operacyjne

NCTC udziela instytucjom zajmującym się przeciwdziałaniem terroryzmowi również wsparcia operacyjnego. Czyni to zarówno dostarczając informacji o zagrożeniu terrorystycznym i incydentach związanych z tym zagrożeniem, ale także poprzez alokację zasobów wywiadowczych w stosunku do tych obszarów zaangażowania, które istotne są dla czynników decyzyjnych w państwie.

W celu realizacji powyższych zadań w NCTC powołano następujące jednostki organizacyjne:

- Narodowe Centrum Operacji Kontr-terrorystycznych (*National Counter-terrorism Operations Center – NCTOC*):
  - utrzymuje stały monitoring globalnej sytuacji odnośnie terroryzmu,
  - powiadamia instytucje zajmujące się przeciwdziałaniem terroryzmowi o bieżącej sytuacji w obszarze zagrożenia terroryzmem,
  - prowadzi krzyżową międzyagencyjną wymianę informacji w celu wsparcia operacji kontr-terrorystycznych,
  - wspiera zarządzanie kryzysowe na wypadek zagrożeń terrorystycznych,
  - identyfikuje potrzeby informacyjne w obszarze przeciwdziałania terroryzmowi;
- Grupa Zarządzania Operacjami (*Operations Management Group – OMG*):

- przewodzi udziałowi NCTC w wydarzeniach rangi narodowej, w tym ćwiczeniach i kryzysach,
- zarządza działaniami rozlokowanych w terenie zespołów NCTC wspierających większe zdarzenia oraz ułatwia wymianę informacji pomiędzy obecnymi na miejscu służbami i ich koordynatorami,
- dostarcza bieżących informacji o poziomie zagrożenia i informuje kierownictwo NCTC oraz decydentów politycznych o najnowszych wydarzeniach i dostarcza obrazu sytuacji;

– Grupa Zarządzania Zagrożeniem (*Threat Management Group – TMG*):

- śledzi istotne lub bezpośrednie zagrożenia dla USA na terytorium kraju oraz interesów narodowych poza granicami kraju,
- utrzymuje monitoring trendów zagrożenia terrorystycznego,
- identyfikuje najważniejsze informacje nt. zagrożenia terrorystycznego w celu włączenia ich do baz danych wspierających działania instytucji zajmujących się przeciwdziałaniem terroryzmowi.

Dla celów zapewnienia pełnej funkcjonalności NCTC jako źródła informacji i bazy danych, instytucja ta czyni starania mające na celu stworzenie możliwości elektronicznego wyszukiwania w magazynie danych, który będzie dostępny dla wszystkich federalnych instytucji odpowiedzialnych za przeciwdziałanie terroryzmowi. Prowadzi się również działania zmierzające do stworzenia Wspólnego Środowiska Komputerowego NCTC (*NCTC Common Computing Environment – NCCE*) w celu poprawy dostępności danych dla analityków. Kolejne realizowane przedsięwzięcie związane jest z tworzeniem architektury systemu uwzględniającej potrzeby funkcjonalne – dla zapewnienia możliwości oddzielenia danych od aplikacji oraz integralność funkcjonalności systemu komputerowego. Ostatnim krokiem jest próba stworzenia wersji systemu NCTC Online „wrażliwe, ale jawne informacje".

5.1.3 Zarządzanie misjami

Memorandum Polityczne nr 2005-100-2 z dnia 15 listopada 2005 r. ustanowiło NCTC Managerem Misji Kontr-terrorystycznych dla wspólnoty wywiadowczej. Dokument ten zakreśla ramy ekspansywnego mandatu, którego celem jest skupienie wysiłków społeczności kontr-terrorystycznej i przewodzenie wspólnemu przedsięwzięciu w tej dziedzinie. Zgodnie z tym mandatem, Manager Misji:

- ma zrozumienie potrzeb wszystkich „klientów",
- ocenia jakość analiz,
- identyfikuje luki w systemie gromadzenia danych i tworzy zintegrowane strategie gromadzenia,
- zapewnia prowadzenie równoległych, „konkurencyjnych" analiz w odniesieniu do priorytetowych zagadnień i pojawiających się zagrożeń,
- ustanawia systemy odniesienia w celu oceny efektywności działań społeczności kontr-terrorystycznej,
- formułuje dla Dyrektora Wywiadu Narodowego rekomendacje dotyczące transferów personelu i funduszy w ramach wspólnoty wywiadowczej w celu poprawienia efektywności realizowanych zadań.

Celem funkcjonowania NCTC jako Managera Misji jest osiągnięcie zaplanowanej redundancji oraz alternatywnej analizy. Istnienie Managera Misji ma także zapewnić agresywne zbieranie informacji oraz racjonalną alokację ograniczonych zasobów.

5.2 System niemiecki – Wspólne Centrum Walki z Terroryzmem (GTAZ)

Wspólne Centrum Walki z Terroryzmem (GTAZ) jest strukturą funkcjonującą w specyficznych warunkach służb policyjnych i bezpieczeństwa państwa federalnego. Centrum to działa w ramach Departamentu Bezpieczeństwa Państwa Federalne-

go Urzędu Kryminalnego (Bundeskriminalamt – BKA). Departament ten podlega Szefowi BKA[183].

GTAZ powstał w roku 2004 w celu koordynowania działań związanych z zagrożeniem terroryzmem islamistycznym. Komórkami odpowiedzialnymi za funkcjonowanie Centrum są jednostki: ds. policyjnej służby informacji i analiz oraz ds. analiz raportów i oceny zagrożenia terrorystycznego w komórce „przestępczość polityczna oraz popełniana przez obcokrajowców – ekstremizm religijny – terroryzm islamistyczny" Departamentu Bezpieczeństwa Państwa BKA.

Wśród celów wymienianych jako cele stworzenia i funkcjonowania niemieckiego Wspólnego Centrum Walki z Terroryzmem, jego twórcy wymieniają przede wszystkim wzmocnienie między-urzędowej współpracy przez:

- skrócenie i strukturyzację dróg komunikacji,
- grupowanie, zagęszczanie i ocenę występujących informacji,
- zwalczanie w ramach podziału pracy oparte na różnych kompetencjach,
- uzgadnianie działań operacyjnych.

Kolejnym efektem uzyskanym w procesie funkcjonowania GTAZ jest intensyfikacja między-urzędowej współpracy przy ściganiu karnym, w szczególności z Generalnym Prokuratorem Federalnym.

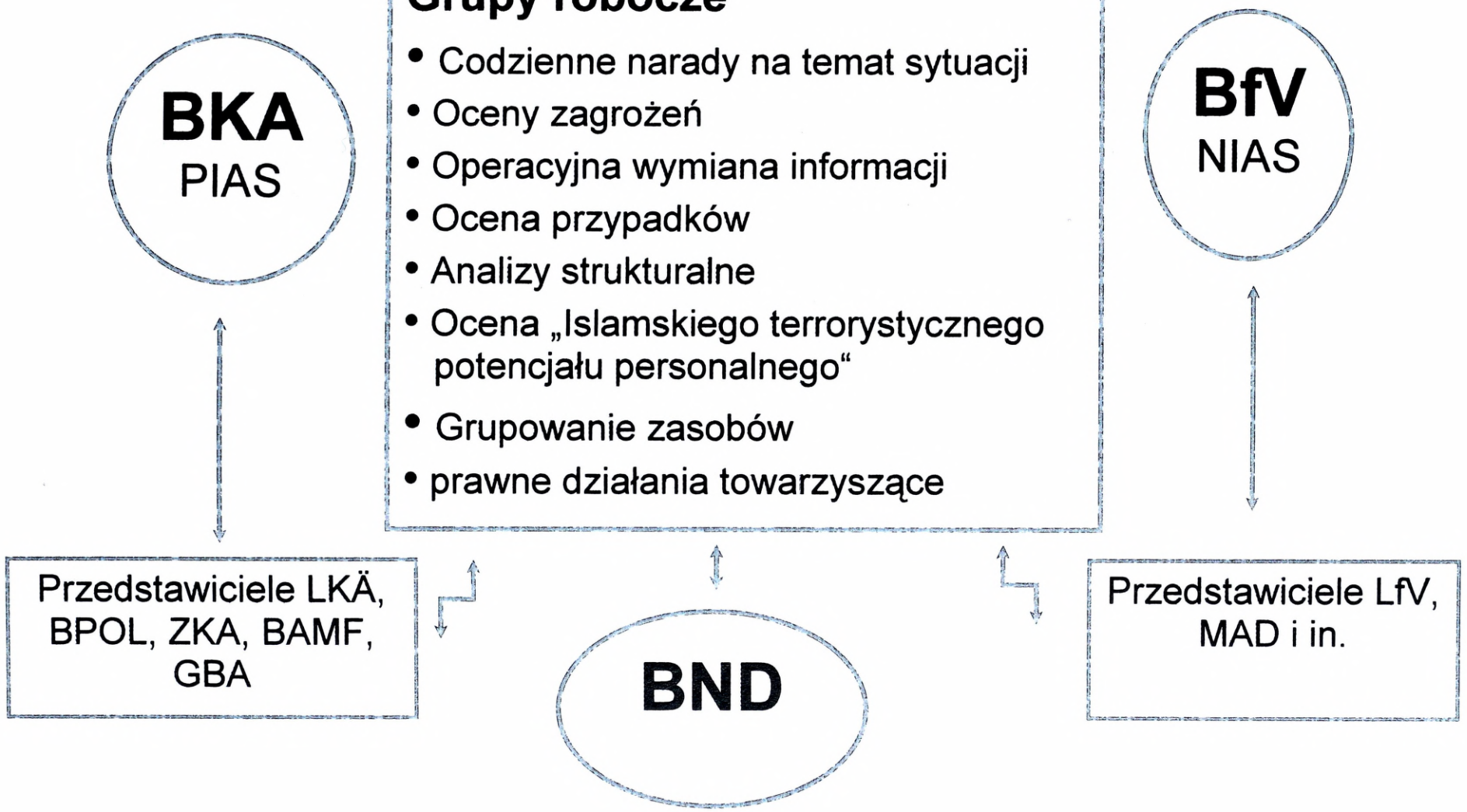
Powyższe cele osiągnięte zostały z zachowaniem i przestrzeganiem wszystkich kompetencji i istniejących dróg meldunkowych, co jest dowodem na istnienie możliwości stworzenia efektywnego centrum koordynacji i wymiany informacji bez konieczności narzucania wiodącej roli przywódczej któremukolwiek z elementów systemu przeciwdziałania terroryzmowi.

W skład GTAZ wchodzą następujący uczestnicy:

- Federalny Urząd Kryminalny,
- Federalny Urząd ds. Ochrony Konstytucji,
- Federalna Służba Wywiadowcza,
- Policja Federalna,
- Śledcza Służba Celna,
- Wojskowa Służba Bezpieczeństwa,
- Federalny Urząd ds. Migracji i Uchodźców,

[183] Opracowanie własne na podstawie materiałów udostępnionych przez GTAZ podczas wizyty autora pracy (jako naczelnika Wydziału ds. Przeciwdziałania Terroryzmowi w MSWiA) w tej instytucji w listopadzie 2006 r.

- Przedstawiciele Krajowych Urzędów Kryminalnych,
- Przedstawiciele Krajowych Urzędów ds. Ochrony Konstytucji,
- Przedstawiciel Generalnego Prokuratora Federalnego.



Rys. 21: Struktura Wspólnego Centrum Walki z Terroryzmem
Źródło: niepublikowane materiały z wizyty studyjnej

Centrum nie posiada zwierzchnika – szefa, funkcjonuje na bazie zespołów roboczych, którym powierzono zadania związane z poszczególnymi etapami procesu zarządzania informacją. Funkcję wiodącą w kolejnych zespołach roboczych powierzono poszczególnym służbom wchodzącym w skład systemu bezpieczeństwa państwa. Istnieje 8 podstawowych zespołów roboczych.

Zespół codziennych narad na temat sytuacji:

- kierownictwo: BKA (Federalny Urząd Kryminalny),
- uczestnicy: wszystkie urzędy,
- rytm: w każdy dzień roboczy,
- przedmiot obrad:
    i. wymiana aktualnych informacji dnia na temat sytuacji,
    ii. sporządzanie pierwszych ocen dotyczących konkretnych okazji,
    iii. uzgodnienie działań, jakie mają zostać podjęte.

Wszystkie instytucje biorące udział w obradach Zespołu mają prawo do zgłaszania tematów, jakie będą poruszane podczas spotkania. Wiodącym tematem obrad są kwestie związane z terroryzmem islamistycznym jako zagrożeniem dla Republiki Federalnej Niemiec. Ze względu na częstotliwość spotkań zazwyczaj ich długość trwania nie przekracza 2-3 min., ale w sytuacji dużej ilości kwestii do omówienia mogą trwać znacznie dłużej.

Z każdego spotkania sporządzany jest raport, przesyłany do wszystkich uczestników Zespołu. Istnieje centralne baza gromadząca wszystkie raporty.

W sytuacji, w której omawiana jest sprawa szczególnie poważna tworzy się grupy zadaniowe do pracy nad takim tematem.

Zespół oceny zagrożeń:

- kierownictwo: BKA (Federalny Urząd Kryminalny),
- uczestnicy: BfV (Federalny Urząd ds. Ochrony Konstytucji), BND (Federalna Służba Wywiadowcza, BKA (Federalny Urząd Kryminalny),
- rytm: w związku z konkretną sytuacją zagrożenia,
- przedmiot obrad: sporządzanie i aktualizacja uzgodnionych ocen zagrożeń.

Zespół ten istnieje przede wszystkim jako platforma wymiany informacji pomiędzy policją i służbami specjalnymi. Założeniem jej funkcjonowania jest działanie prewencyjne – zapobieganie zamachom w fazie ich przygotowania.

Zespół przede wszystkim zajmuje się omawianiem informacji o zagrożeniu, która w następnej kolejności jest poddawana weryfikacji przez poszczególne służby uczestniczące w pracach Zespołu.

Z chwilą pozytywnego zweryfikowania informacji przez służby i przekazania jej do rozpoczęcia oficjalnych czynności dochodzeniowo – śledczych, praca Zespołu zostaje formalnie zakończona.

W przypadku przekazywania władzom Niemiec rekomendacji, mających na celu podjęcie określonych działań prewencyjnych na poziomie kraju, przedstawiciele władzy nie uzyskują żadnych danych na temat źródła informacji o zagrożeniu.

Zespół operacyjnej wymiany informacji („*Informationboard*"):

- kierownictwo: BKA (Federalny Urząd Kryminalny),
- uczestnicy: BfV (Federalny Urząd ds. Ochrony Konstytucji), BND (Federalna Służba Wywiadowcza, BKA (Federalny Urząd Kryminalny) i inni uczestnicy w związku z konkretną potrzebą,
- rytm: poniedziałki, środy i piątki oraz w związku z konkretną sytuacją zagrożenia,
- przedmiot obrad:
    i. identyfikacja podstaw dochodzeniowych,
    ii. uzgadnianie działań operacyjnych,
    iii. intensywne przekazywanie policyjnych wyników działań dochodzeniowych do BfV i BND.

Zadaniem Zespołu jest przede wszystkim koordynacja informacji w zakresie zagrożeń. Przekazywane informacje są weryfikowane, poszerzane o dodatkowe i poddawane analizie, a następnie przekazywane właściwej terytorialnie policji landowej.

Rolą BKA jako instytucji wiodącej w Zespole jest opracowanie zaleceń i wskazywanie najważniejszych aspektów danej sprawy, które należy brać pod uwagę, ale nie instruowanie danej policji co do tego, jak ma wykonywać swoje czynności w sprawie. Najważniejszym zadaniem Zespołu jest dokonanie oceny zagrożenia atakami w Niemczech oraz na obiekty niemieckie poza granicami kraju.

Zespół ds. oceny przypadków („Assessmentboard")

- kierownictwo: BfV (Federalny Urząd ds. Ochrony Konstytucji),
- uczestnicy: BfV (Federalny Urząd ds. Ochrony Konstytucji), BND (Federalna Służba Wywiadowcza, BKA (Federalny Urząd Kryminalny) i inni uczestnicy w związku z konkretną potrzebą,
- rytm: w związku z konkretną potrzebą,
- przedmiot obrad: sporządzanie wykraczających poza indywidualne przypadki ocen sytuacji i analiz dotyczących wybranych dziedzin islamskiego terroryzmu odnoszącego się do Niemiec.

Zespół ds. analiz strukturalnych

- kierownictwo: BfV (Federalny Urząd ds. Ochrony Konstytucji),
- uczestnicy: BfV (Federalny Urząd ds. Ochrony Konstytucji), BND (Federalna Służba Wywiadowcza, BKA (Federalny Urząd Kryminalny) i inni uczestnicy w związku z konkretną potrzebą,
- rytm: w związku z konkretną potrzebą,
- przedmiot obrad: przeprowadzanie podstawowych projektów dotyczących struktur i sposobów funkcjonowania islamskich sieci.

Zespół ds. islamistycznego terrorystycznego potencjału ludzkiego

- kierownictwo: BfV (Federalny Urząd ds. Ochrony Konstytucji),
- uczestnicy: BfV (Federalny Urząd ds. Ochrony Konstytucji), BKA (Federalny Urząd Kryminalny) i BND (Federalna Służba Wywiadowcza) w związku z konkretną potrzebą,
- rytm: dwa razy w tygodniu,
- przedmiot obrad: podsumowanie i porównanie ocen policji i służby wywiadowczej dotyczących islamskiego terrorystycznego potencjału personalnego.

Zespół ds. alokacji zasobów

- kierownictwo: BfV (Federalny Urząd ds. Ochrony Konstytucji)
- uczestnicy: BfV (Federalny Urząd ds. Ochrony Konstytucji), BND (Federalna Służba Wywiadowcza), BKA w związku z konkretną okazją KI 26 – TeSIT[184] i odpowiednie ośrodki krajowe
- rytm: w związku z konkretną potrzebą (także TSK[185]),
- przedmiot obrad:
  i. wymiana rozpoznań związanych z Internetem i wyników oceny,
  ii. uzgodnienie postępowania opartego na podziale pracy przy poszukiwaniach internetowych,
  iii. uzgodnienie pomocy urzędowych przy tłumaczeniach,
  iv. koordynacja przy tworzeniu i administrowaniu wspólnych baz danych w dziedzinie terroryzmu.

Zespół ds. prawnych działań towarzyszących:

- kierownictwo: BAMF,
- uczestnicy: BAMF, BfV, BKA, BMI, (inni uczestnicy w związku z konkretną okazją: LKÄ, krajowe urzędy ds. cudzoziemców etc.)
- rytm: w związku z konkretną potrzebą - przynajmniej raz w miesiącu,
- przedmiot obrad:
  i. w przypadku osób związanych z terroryzmem islamistycznym uzyskanie zakończenia pobytu,
  ii. niedopuszczenie do wjazdu bądź ponownego wjazdu takich osób i podjęcie bądź uzyskanie koniecznych do tego prawnych podstaw w prawie azylowym, prawie o cudzoziemcach i prawie o obywatelstwie, które są konieczne do osiągnięcia tych celów.

[184] (KI 26 – TeSIT) – Techniczne Centrum Serwisowe ds. technologii informacyjnej i komunikacyjnej w BKA.
[185] (TSK) Telekonferencja.

5.3 System francuski – Jednostka ds. Koordynacji Zwalczania Terroryzmu (UCLAT)

Działania związane z przeciwdziałaniem terroryzmowi we Francji oparte są na pięciu podstawowych zasadach: wywiad, prewencja, ściganie, koordynacja i współpraca międzynarodowa. W styczniu 2006 r. weszła w życie nowa ustawa, zwiększająca uprawnienia służb odpowiedzialnych za bezpieczeństwo i porządek publiczny. Równolegle wprowadzane są regulacje zaostrzające środki administracyjne, które mogą być stosowane w odniesieniu do osób podejrzanych o terroryzm. Ponadto we Francji wdrażane są i dopracowywane w zależności od potrzeb plany prewencji i bezpieczeństwa. W obszarze profilaktyki terroryzmu istotne znaczenie ma również funkcjonowanie instytucji o nazwie Francuska Rada Muzułmańska, która stanowi podmiot współpracujący z rządem francuskim w celu zapobiegania radykalizacji i rekrutacji do grup terrorystycznych[186].

Zwalczanie terroryzmu nie jest przypisane we Francji konkretnej jednostce ani służbie. Fundamentalną zasadą realizowaną we Francji jest mobilizacja wszystkich służb, które mogą przyczynić się do zapobiegania i zwalczania terroryzmu, niezależnie od tego, czy znajdują się one pod nadzorem ministerstwa spraw wewnętrznych, czy innego departamentu ministerialnego.

Funkcje wywiadowcze przypisane są dwóm służbom policyjnym:

- Dyrekcji Centralnej Wywiadu Ogólnego – zajmujący się kwestiami terroryzmu wewnętrznego z ewentualnymi związkami międzynarodowymi,
- Francuska Służba Bezpieczeństwa – zajmująca się kwestiami międzynarodowego terroryzmu wspieranego przez państwa lub grupy działające poza granicami Francji.

Inne służby, poza policją francuską, zajmujące się kwestiami zbierania informacji wywiadowczych, to także Francuska Służba Bezpieczeństwa Zagranicznego, Dyrekcja Ochrony i Bezpieczeństwa Obronnego. Także Narodowa Dyrekcja ds. Dochodzeń Kryminalnych, mimo że nie jest to jedna z jego podstawowych funkcji, może zajmować się zbieraniem informacji związanych z terroryzmem.

---

[186] Opracowanie własne na podstawie materiałów udostępnionych przez Christophe Chaboud, Szefa UCLAT, podczas jego wizyty w Polsce (MSWiA) we wrześniu 2005 r. – organizatorem wizyty był Wydział ds. Przeciwdziałania Zagrożeniom Terrorystycznym, kierowany przez autora niniejszej pracy.

Akty terrorystyczne to akty przestępcze, których ściganiem zajmuje się Narodowa Dyrekcja ds. Dochodzeń Kryminalnych. Terroryzmem wewnętrznym zajmuje się wyspecjalizowana jednostka: Narodowa Jednostka Antyterrorystyczna. Jednakże, na poziomie sądowniczym, także Francuska Służba Bezpieczeństwa prowadzi dochodzenia w sprawach wynikających z zebranego przez jego służby materiału wywiadowczego, tak jak i w sprawach dotyczących fundamentalizmu islamskiego.

Inne elementy policji narodowej również mogą wnosić wkład do zbierania materiałów wywiadowczych, z włączeniem działań prewencyjnych i zwalczania terroryzmu, na przykład Policja Graniczna, Miejskie Siły Policyjne (Departament Bezpieczeństwa Publicznego) oraz Żandarmeria Francuska (w szczególności w odniesieniu do terenów wiejskich).

W kontekście funkcjonowania wielu służb odpowiedzialnych za przeciwdziałanie terroryzmowi, a tym samym potrzeby skoordynowania podejmowanych przez nie działań podjęta została decyzja o stworzeniu w dniu 8 października 1984 r. Jednostki Koordynacji Zwalczania Terroryzmu – UCLAT – pod nadzorem Dyrektora Generalnego Policji Narodowej Francji.

Podstawowe zadania UCLAT dotyczą trzech grup zagadnień: związanych z wywiadem i zbieraniem informacji, prewencją i represjami. Co tydzień (lub w razie zaistnienia konieczności częściej) Szef UCLAT, który jest wysokim oficerem policji, zwołuje spotkanie przedstawicieli ze wszystkich wymienionych wcześniej służb zaangażowanych w zwalczanie terroryzmu i jednostki antyterrorystycznej RAID oraz Francuskiej Służby Bezpieczeństwa Zewnętrznego.

UCLAT nie koordynuje każdej akcji, ani operacji i charakterze kontrterrorystycznym. Jest jednostką, która służy wsparciem podmiotom bezpośrednio odpowiedzialnym za przeciwdziałanie terroryzmowi. Przekazywanie do niego informacji, jak i przekazywanie mu koordynacji działań odbywa się na zasadzie pełnej dobrowolności ze strony służb i instytucji.

Głównym zadaniem UCLAT jest ciągłe monitorowanie zagrożenia terrorystycznego i dostarczanie ministrowi spraw wewnętrznych informacji koniecznych do właściwej oceny wymaganego poziomu bezpieczeństwa. Ta ocena ma dwa aspekty: zagrożenie ze strony ugrupowań terrorystycznych i zagrożenia dla wielkich wydarzeń masowych (Igrzysk Olimpijskich, szczytów głów państw i rządów itp.).

UCLAT działa w ramach dwufazowego procesu mającego na celu zwiększenie bezpieczeństwa osób, mienia, infrastruktury krytycznej i ważnych osób:

1. zbieranie informacji,
2. porównywanie informacji (podczas spotkań).

UCLAT utrzymuje okresowe kontakty Dyrekcją ds. Wizyt Oficjalnych, Dyrekcją ds. Personelu i Szkoleń, ze służbą celną, Ministerstwem Finansów i Dyrekcją Ochrony i Bezpieczeństwa Obronnego Ministerstwa Obrony. Te kontakty mają żywotną wagę dla zapewnienia właściwej współpracy pomiędzy wszystkimi uczestnikami tej walki. Komórka koordynacyjna UCLAT powstała także w Baskonii.

Dodatkowo, UCLAT reprezentuje Generalną Dyrekcją Policji Narodowej na międzynarodowych spotkaniach związanych z kwestiami dotyczącymi terroryzmu. W tym kontekście UCLAT bierze udział w spotkaniach grup roboczych UE, G-8 i innych kompetentnych forów. UCLAT jest również gospodarzem francuskich biur brytyjskich, niemieckich, hiszpańskich, włoskich i belgijskich służb wyspecjalizowanych w zwalczaniu terroryzmu i wysyła oficerów łącznikowych w krajach, które podpisały dwustronne porozumienia w zakresie zwalczania terroryzmu (Niemcy, Włochy, Hiszpania, Wielka Brytania i Belgia).

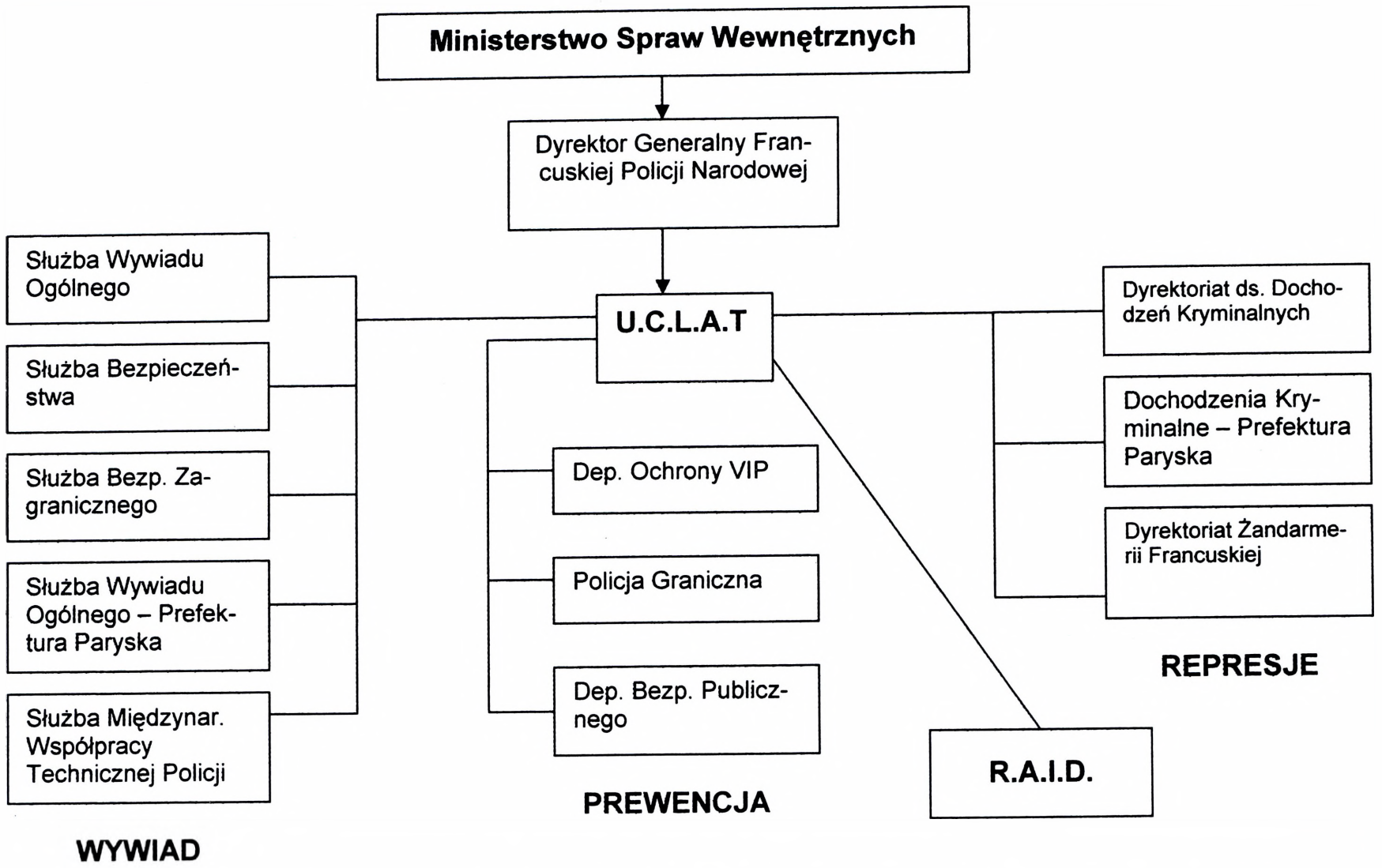
UCLAT koordynuje także zagadnienia związane z terroryzmem i jego zwalczaniem na posiedzeniach Rady Bezpieczeństwa Wewnętrznego. Na czele tego ciała stoi Prezydent Francji. Decyduje ono o politycznym wymiarze i priorytetach bezpieczeństwa wewnętrznego, zapewnia zgodność działań prowadzonych przez różne ministerstwa oraz dostępność koniecznych środków. Zostało reaktywowane dekretem nr 2002-890 z 15 maja 2002 r., aby odgrywać główną rolę w walce z terroryzmem. Jego głównym zadaniem jest nadawać impuls polityce bezpieczeństwa wewnętrznego, nadzorować koordynację i dystrybucją potrzebnych środków.

Na poziomie rządowym koordynację w zakresie bezpieczeństwa zajmują się także: Międzyresortowy Komitet ds. Wywiadu oraz Międzyresortowy Komitet Kontrterrorystyczny. Na poziomie ministerstwa spraw wewnętrznych dodatkową koordynacją w odniesieniu do kwestii wywiadowczych zapewnia także Narodowy Komitet Wywiadu.

Jak już nadmieniono, UCLAT funkcjonuje w oparciu o trzy filary działań:

1. Wywiad – w którym wiodące role odgrywają następujące służby:
   - Francuska Służba Bezpieczeństwa Zagranicznego,
   - Francuska Służba Bezpieczeństwa,
   - Służba Wywiadu Ogólnego,
   - Służba Międzynarodowej Współpracy Technicznej Policji,
   - Służby wywiadowcze Policji Granicznej;
2. Prewencja – w którym wiodące role odgrywają następujące służby:
   - Dyrektoriat Bezpieczeństwa Publicznego,
   - Dyrektoriat Żandarmerii Francuskiej,
   - Dyrektoriat Policji Granicznej,
   - Departament Ochrony Ważnych Osób (VIP),
   - Dyrektoriat ds. Wolności Obywatelskich i Spraw Sądowych
3. Represje – w którym wiodące role odgrywają następujące służby:
   - Dyrektoriat ds. Dochodzeń Kryminalnych,
   - Dyrektoriat Żandarmerii Francuskiej,
   - Francuska Służba Bezpieczeństwa.

Cały pion systemu bezpieczeństwa w zakresie zwalczania i przeciwdziałania terroryzmowi podlega Ministrowi Spraw Wewnętrznych. Oprócz wymienionych wyżej instytucji, posiadających uprawnienia i obowiązki w obszarze przeciwdziałania terroryzmowi, wymienić należy dodatkowo RAID – narodową francuską jednostkę antyterrorystyczną, odpowiedzialną za fizyczne zwalczania terroryzmu.



Rys. 22: Zwalczanie terroryzmu we Francji – rola UCLAT: koordynacja działań służb policyjnych
Źródło: niepublikowane materiały z wizyty studyjnej

Misją UCLAT jest przede wszystkim zapewnienie operacyjnej koordynacji działań służb policyjnych, głównie poprzez przekazywanie informacji. W tym celu przedstawiciele wszystkich służb reprezentowanych w UCLAT spotykają się w regularnych, tygodniowych odstępach czasu – chyba, że zachodzi nagła potrzeba spotkania w związku z zaistnieniem sytuacji kryzysowej.

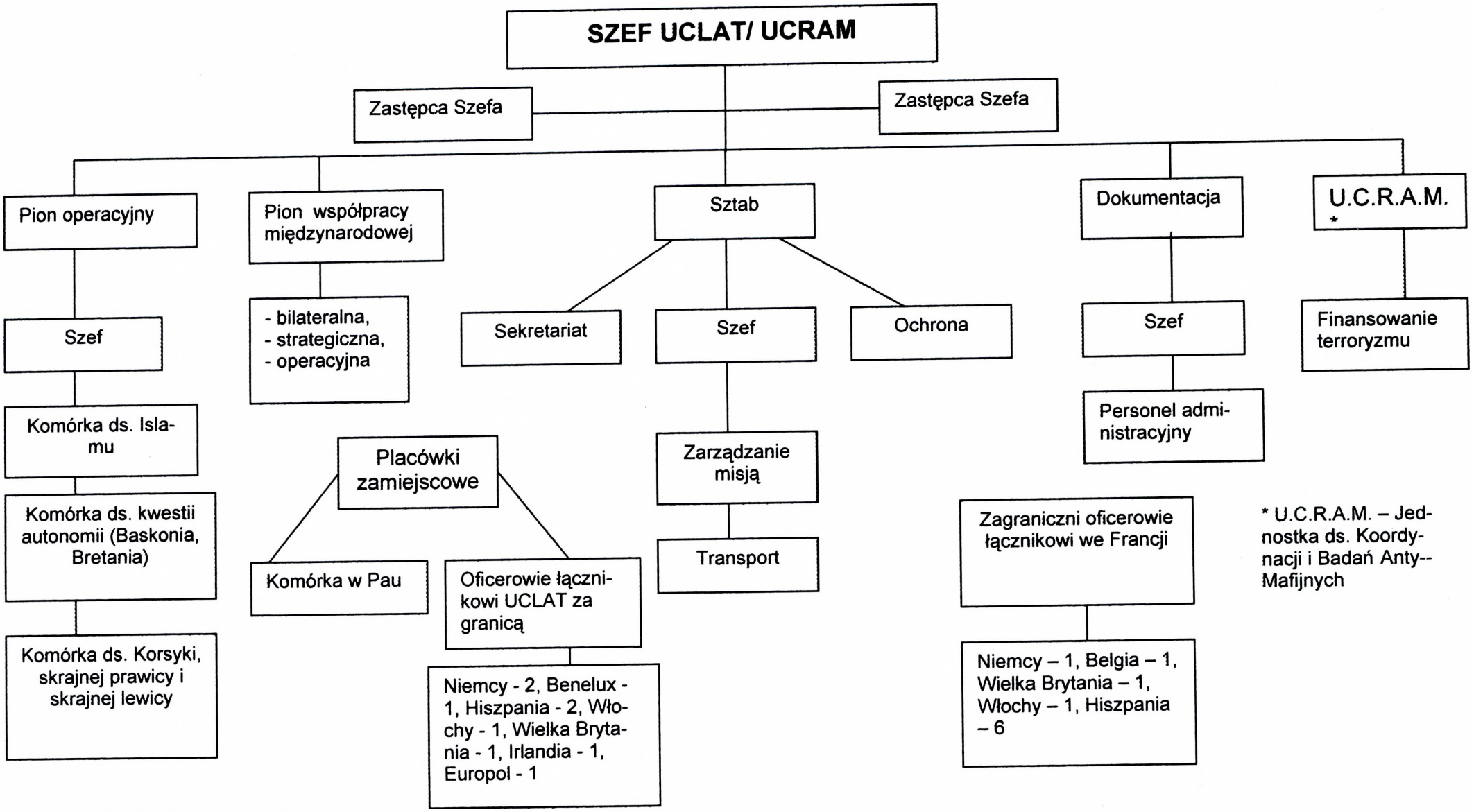
Ponadto UCLAT przygotowuje dokumenty związane z oceną zagrożenia terroryzmem we Francji. Oceny te przygotowywane są na podstawie danych wywiadu, nie tylko dla celów planowania bieżących działań kontr-terrorystycznych, ale także w celu przekazywania informacji czynnikom politycznym i decyzyjnym.

Warto podkreślić, że dla potrzeb poziomu politycznego decydowania, szczegółowe i specjalistyczne analizy wywiadu przekształcane są przez UCLAT w sposób umożliwiający efektywne wykorzystywanie ich przez osoby nie zajmujące się zawodowo analizą informacji wywiadowczych.

Podkreślenia wymagają także dwie kwestie wspomniane już wcześniej:

1. UCLAT nie koordynuje wszystkich działań kontr-terrorystycznych we Francji – czyni to jedynie na wniosek instytucji realizujących bezpośrednio działania o takim charakterze;
2. UCLAT działa w systemie 24-godzinnym.

Dla zapewnienia wysokiej efektywności realizacji określonej wyżej misji UCLAT, nadano mu specyficzną formę i organizację.



Rys. 23: Struktura UCLAT
Źródło: niepublikowane materiały z wizyty studyjnej

5.4 System brytyjski – Wspólne Centrum Analiz Terroryzmu (Joint Terrorism Analysis Centre – JTAC) oraz system zarządzania kryzysowego

5.4.1 Wspólne Centrum Analiz Terroryzmu (JTAC)

JTAC jest strukturą powołaną w celu analizy i oceny informacji wywiadowczych związanych z międzynarodowym terroryzmem, zarówno w odniesieniu do terytorium Wielkiej Brytanii, jak i poza jej granicami. Ustala poziom zagrożenia obowiązujący w kraju i formułuje ostrzeżenia o zagrożeniu terrorystycznym dla podmiotów administracji publicznej (rządowych departamentów i agencji), a także opracowuje pogłębione raporty nt. trendów, sieci terrorystycznych i ich zdolności działania.[187]

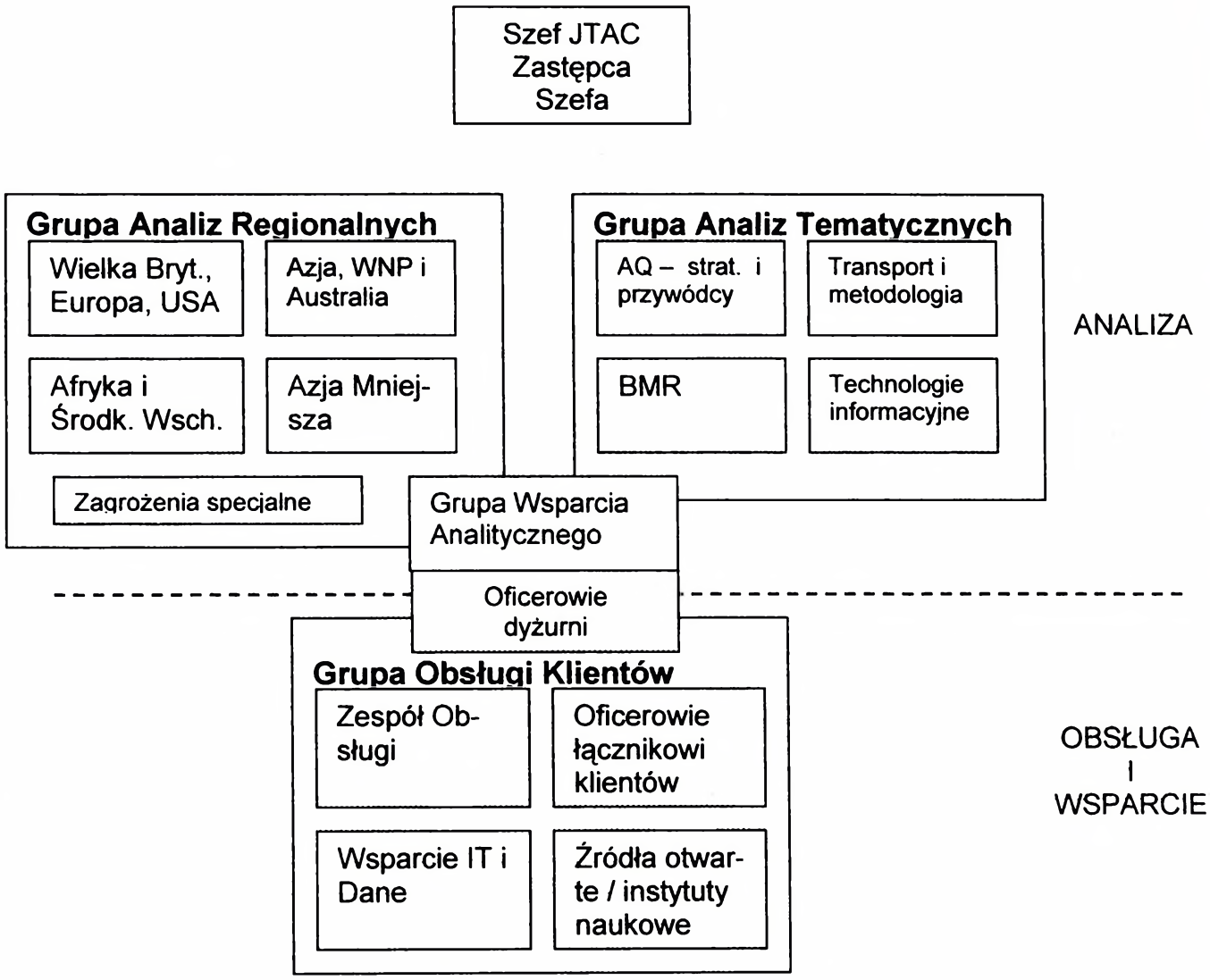
Szef JTAC odpowiada przed Dyrektorem Generalnym Służby Bezpieczeństwa (MI5), który następnie przekazuje raporty Rządowemu Połączonemu Komitetowi ds. Wywiadu. Model ten sprawdził się w Wielkiej Brytanii, a JTAC stał się kluczowym elementem *National Intelligence Machinery* („Narodowej Maszynerii Wywiadowczej"), czyli wspólnoty gromadzącej wszystkie podmioty realizujące zadania w zakresie gromadzenia i analizy informacji.

Wśród najważniejszych zadań JTAC wymienić można: pełnienie roli brytyjskiego centrum analiz międzynarodowego terroryzmu (źródło dostępu do informacji wywiadowczych funkcjonujące całodobowo), zapewnienie wsparcie dla podmiotów gromadzących informacje wywiadowcze oraz partnerów w wykrywaniu, prewencji i minimalizowaniu konsekwencji terroryzmu, ustanawianie poziomów zagrożenia dla Wielkiej Brytanii i jej interesów zarówno w kraju, jak poza jego granicami, sporządzanie analiz zagrożenia w razie zaistnienia potrzeby, uczestnictwo w posiedzeniach komitetów rządowych ds. zwalczania terroryzmu.

Wśród podmiotów biorących bezpośredni udział w dostarczaniu i otrzymywaniu informacji do i z JTAC wymienić należy m.in.: Ministerstwo Spraw Wewnętrznych, Ministerstwo Spraw Zagranicznych, Ministerstwo Obrony, Kwatera Główna Komunikacji Rządowej, Służba Bezpieczeństwa MI 5, Tajna Służba Wywiadowcza MI 6, Policja, służby celne, imigracyjne i podatkowe.

---

[187] Piasecka P., *Koordynacja przeciwdziałania terroryzmowi w Wielkiej Brytanii* [w:] Liedel K., Prońko J., Wiśniewski B., *Administracja publiczna w systemie przeciwdziałania nadzwyczajnym zagrożeniom dla ludzi i środowiska*, Warszawa – Bielsko-Biała 2007, s. 97 i dalsze.



Rys. 24: Struktura JTAC
Źródło: niepublikowane materiały z wizyty studyjnej

5.4.2 Koordynacja reagowania w sytuacjach kryzysowych

Za zarządzanie kryzysowe i obronę cywilną w Wielkiej Brytanii w znacznym stopniu odpowiada instytucja o nazwie *Civil Contingencies Secretariat* – Sekretariat Cywilnego Reagowania Kryzysowego.[188]

Do jego podstawowych zadań należy prowadzenie analizy potencjalnych zagrożeń dla kraju. Niezbędnym elementem takiej analizy jest – w następstwie – dokonanie oceny ich wpływu na kondycję państwa w wypadku zaistnienia związanego z nimi kryzysu. Bazując na sporządzanych corocznie analizach zagrożeń, Sekretariat Cywilnego Reagowania Kryzysowego stworzył matryce zagrożeń bezpieczeństwa pu-

[188] Piasecka P., *Koordynacja przeciwdziałania terroryzmowi w Wielkiej Brytanii,* op. cit., s. 99.

blicznego w Wielkiej Brytanii. Zawarte w nich zestawienia potencjalnych zagrożeń, wraz z analizą prawdopodobieństwa wystąpienia, rozpatrywane w aspekcie okresu sprzyjającego danemu rodzajowi zagrożenia, stanowią punkt odniesienia dla planowania cywilnego w zakresie reagowania kryzysowego.

Podstawową rolą tej organizacji jest zatem posiadanie wiedzy o tym, co może się zdarzyć oraz określanie środków reagowania na takie wydarzenie – czyli budowanie gotowości na wszystkich poziomach, włącznie z poziomem lokalnych ratowników, którzy jako pierwsi znajdują się na miejscu zdarzenia. Sekretariat Cywilnego Reagowania Kryzysowego odpowiada zatem również za tworzenie planów reagowania kryzysowego, powiązanych z analizą potencjalnych zagrożeń.

Cel działań Sekretariatu to zapewnienie istnienia planów koordynacji współpracy różnych poziomów reagowania (centralnego, regionalnego i lokalnego). Plany reagowania dla tych poszczególnych poziomów tworzone są na zasadzie kaskadowej, poczynając od poziomu centralnego, określanego w Wielkiej Brytanii mianem „złotego". Istnienie tych planów ma gwarantować ciągłość dostarczania podstawowych usług dla społeczeństwa (funkcjonowania służby zdrowia, dostaw wody, żywności, transportu i usług finansowych) i utrzymanie zdolności reagowania na wypadek zdarzeń o charakterze kryzysowym.

5.5 Inne rozwiązania

5.5.1 Centrum Antyterrorystyczne polskiej Agencji Bezpieczeństwa Wewnętrznego

Centrum Antyterrorystyczne stanowiące część struktur Agencji Bezpieczeństwa Wewnętrznego powołane zostało Zarządzeniem Nr 102 Prezesa Rady Ministrów z dnia 17 września 2008 r. zmieniającym zarządzenie w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego[189].

Centrum Antyterrorystyczne ma za zadanie, jak pisze prof. B. Hołyst w swojej książce *Terroryzm*[190]:

---

[189] Zarządzenie Nr 102 Prezesa Rady Ministrów z dnia 17 września 2008 r. zmieniające zarządzenie w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego, tekst aktu dostępny na stronie [http://www.bip.abw.gov.pl/index.php?id=85].

[190] Hołyst B., *Terroryzm*, LexisNexis, Warszawa 2009, s. 119 i dalsze.

1. „wspomaganie procesów decyzyjnych w wypadku 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 zarządzania kryzysowego;
2. koordynacja działań operacyjno – rozpoznawczych w zakresie zwalczania terroryzmu – realizowana m.in. przez:
    a. 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,
    b. stałe przekazywanie sygnałów o potencjalnych zagrożeniach dla kierownictw instytucji współpracujących z CAT celem podejmowania na bieżąco działań zgodnie z algorytmami reagowania w sytuacjach zagrożenia,
    c. monitoring aktywności organizacji terrorystycznych i ich członków oraz struktur wspierających działalność fundamentalistów na terytorium RP,
    d. monitoring poziomu bezpieczeństwa obiektów – potencjalnych celów ataku terrorystycznego;
3. zadania analityczno – informacyjne w zakresie:
    a. sporządzania aktualnych, syntetycznych i całościowych informacji dla kierownictwa państwa (Prezydenta RP, prezesa Rady Ministrów) na temat poziomu zagrożenia terrorystycznego kraju oraz działań podejmowanych przez służby i instytucje państwowe w celu zniwelowania niebezpieczeństw,
    b. prognoz długo- i krótkookresowych poziomu zagrożenia terrorystycznego Polski,
    c. analiz zagrożenia terrorystycznego w innych państwach w kontekście bezpieczeństwa strategicznych interesów i obywateli RP,

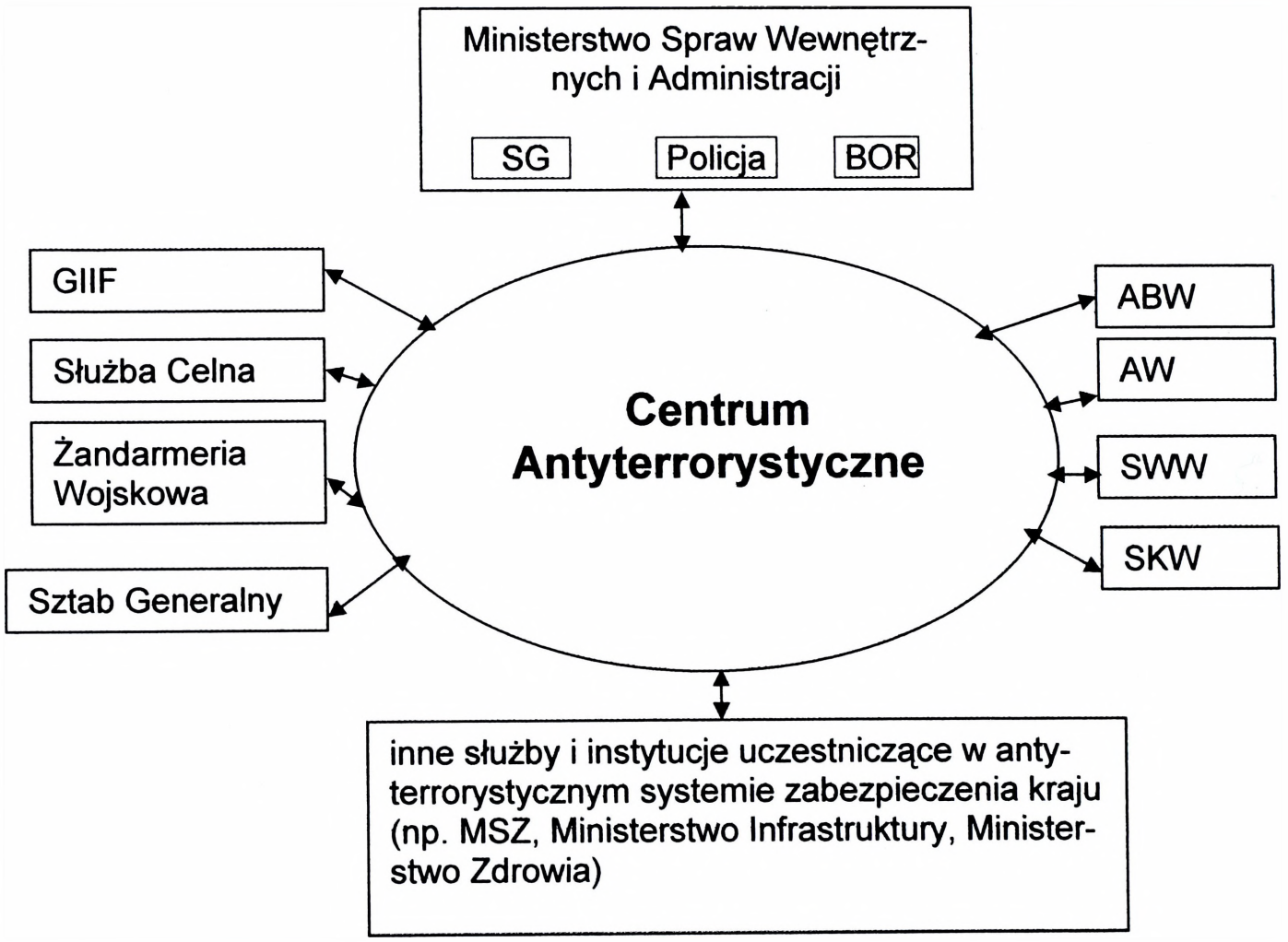
d. udziału w sporządzaniu ocen funkcjonowania systemów ochrony elementów infrastruktury krytycznej kraju pod kątem usunięcia ewentualnych nieprawidłowości;

4. monitoring mediów muzułmańskich;
5. udział w opracowaniu i nowelizowaniu procedur reagowania kryzysowego na wypadek ataku oraz sporządzanie algorytmów działań przed zamachem;
6. wspomaganie po ewentualnych zamachu terrorystycznym – na płaszczyźnie analityczno-informacyjnej – działań służb podległych MSWiA oraz innych podmiotów uczestniczących w ochronie antyterrorystycznej Polski;
7. współpraca z analogicznymi centrami antyterrorystycznymi w innych państwach – m.in. brytyjskim *Joint Terrorism Analysis Centre* (JTAC), amerykańskim *National Counterterrorism Center* (NCTC), niemieckim *Gemeinsames Terrorismusabwehrzentrum* (GTAZ), belgijskim *Organe de Coordination pour l'Analyse de la Menace* (OCNAM), holenderskim *National Coordinator Terrorismebestrijdieng* (NCtB), hiszpańskim *Centro National do Coordinacion Antiterrorista* (CNCA), duńskim *Centre for Terrorism Analysis* (CTA) i włoskim *Comitato di Analisi Strategica Antiterrorismo* (CASA) – w zakresie bieżącej wymiany informacji na temat potencjalnych zagrożeń terrorystycznych,
8. w perspektywie nawiązanie kooperacji z centrami antyterrorystycznymi państw Organizacji na Rzecz Demokracji i Rozwoju (GUAM), w tym przede wszystkim z Centrum funkcjonującym przy Służbie Bezpieczeństwa Ukrainy;
9. zadania dydaktyczno – szkoleniowe."

Zgodnie z założeniami, które przyjęli twórcy CAT, instytucja ta ma działać w systemie 24-godzinnym. Służbę w CAT pełnić mają funkcjonariusze, pracownicy oraz żołnierze z instytucji takich, jak Agencja Bezpieczeństwa Wewnętrznego, Policja, Straż Graniczna, oraz inne instytucje wchodzące w skład systemu przeciwdziałania terroryzmowi w Polsce[191].

[191] Ibidem, s. 120.

System komunikacji użytkowany w toku realizacji zadań CAT oparty ma być przede wszystkim na bezpiecznych połączeniach on-line z większością najważniejszych instytucji państwowych (kancelarie Prezydenta i prezesa Rady Ministrów, MON oraz MSWiA), krajowych instytucji i podmiotów uczestniczących w systemie przeciwdziałania terroryzmowi oraz partnerami zagranicznymi.[192]



Rys. 25: Schemat obiegu informacji w ramach CAT
Źródło: Brunon Hołyst, Terroryzm, LexisNexis, Warszawa 2009, s. 121

Centrum Antyterrorystyczne przy Agencji Bezpieczeństwa Wewnętrznego ma pełnić role podobne do tych, które pełnione są przez jego zagraniczne odpowiedniki. Jednak do chwili obecnej nie są dostępne żadne dane dotyczące podstaw prawnych dla przekazywania informacji przez partnerów wchodzących w skład sytemu przeciwdziałania terroryzmowi do CAT.

Ponadto warto zwrócić uwagę na to, że oprócz regulacji wewnętrznych CAT, nie ma do chwili obecnej aktów prawnych uprawniających je do wykonywania jakich-

[192] Ibidem, s. 120.

kolwiek czynności w zakresie koordynacji zadań realizowanych przez podmioty wchodzące w skład tego systemu. Służby takie, jak Policja, ABW, SG, SWW, SKW czy resorty, w skład zadań których wchodzą zadania związane z przeciwdziałaniem terroryzmowi, są podmiotami funkcjonującymi na podstawie właściwych im ustaw. Co najmniej problematycznym wydaje się powołanie instytucji, której zadaniem ma być koordynacja ich działań – i zapewnienie jej funkcjonowaniu podstaw prawnych na poziomie zarządzania prezesa Rady Ministrów o zmianie statutu Agencji Bezpieczeństwa Wewnętrznego oraz wewnętrznych regulacji na poziomie regulaminu wewnętrznego.

Istnieje zagrożenie, iż funkcjonowanie CAT nie będzie tak efektywne, jak wymagałaby tego powaga zadań, do pełnienia których zostało powołane – w szczególności zapewnienia płynnego funkcjonowania instytucji i procesów, których celem jest zapewnienie bezpieczeństwa państwa w kontekście zagrożenia terroryzmem międzynarodowym.

5.5.2 Prace Centrum Badań nad Terroryzmem Collegium Civitas

W 2005 r. powstała w Collegium Civitas, warszawskiej niepublicznej szkole wyższej, jednostka badawcza pod nazwą Centrum Badań nad Terroryzmem[193]. Wśród badań prowadzonych przez Centrum pod kierunkiem jego Dyrektora są między innymi następujące[194]:

„Model systemu wykorzystania środków masowego przekazu w przeciwdziałaniu i walce z terroryzmem w warunkach RP"

Wśród badań prowadzonych przez Centrum Badań nad Terroryzmem znajdują się między innymi badania nad rolą mediów we współczesnym świecie w kontekście przeciwdziałania terroryzmowi, realizowane w ramach programu badawczego „Model systemu wykorzystania środków masowego przekazu w przeciwdziałaniu i walce z terroryzmem w warunkach RP", który finansowany jest ze środków KBN, w ramach europejskiego programu COST 24.

"Czy Polsce potrzebne jest ustawodawstwo antyterrorystyczne?"

Wewnętrzny program badawczy Centrum Badań nad Terroryzmem mający na celu udzielenie odpowiedzi na pytanie o to, czy obowiązujący obecnie

[193] Inicjatorem powstania tej jednostki, najpierw dyrektorem ds. programowych, a obecnie dyrektorem Centrum, jest autor niniejszej pracy.
[194] Informacje pochodzą z witryny CBnT (Centrum Badań nad Terroryzmem) o adresie [http://www.terroryzm.org].

w Polsce system prawny zawiera wystarczające rozwiązania organizacyjne i funkcjonalne w zakresie zwalczania terroryzmu. Ostatecznym efektem programu ma być powstanie ustawy bądź ustaw wraz z przepisami wykonawczymi, które stanowić będą podstawę prawną przeciwdziałania terroryzmowi w Polsce.

"Bezpieczeństwo Mistrzostw Europy w Piłce Nożnej EURO 2012 w kontekście zagrożeń terrorystycznych"

Wewnętrzny program badawczy Centrum Badań nad Terroryzmem skoncentrowany wokół zagadnień przygotowania Polski do EURO 2012 w kontekście zapewnienia bezpieczeństwa uczestnikom i kibicom Mistrzostw.
Centralne kwestie, wokół których skupione są badania Centrum to:
- bezpieczeństwo imprez masowych wobec zagrożenia samobójczymi zamachami,
- koordynacja działań instytucji zaangażowanych w organizację i zabezpieczanie EURO 2012,
- organizacja procesu bezpieczeństwa w sytuacji symultanicznej organizacji masowych.

"Profilowanie sprawców aktów terrorystycznych jako element badań nad terroryzmem"

Wewnętrzny program badawczy, którego podstawowym celem jest dokonanie przeglądu metod profilowania sprawców aktów terrorystycznych. Założenia programu stanowią, że dokonane zostanie porównanie podstawowych cech profilu sprawcy w okresie III i IV fali terroryzmu (za Davidem C. Rappaportem). Efektem przeprowadzonych badań ma być ustalenie przydatności profilowania jako narzędzia przeciwdziałania terroryzmowi ponowoczesnemu.

"Edukacja antyterrorystyczna jako element profilaktyki zagrożeń terroryzmu"

Program badawczy skoncentrowany na praktycznym wymiarze badań i analiz terroryzmu oraz elementów jego zwalczania. Podstawowym celem badań jest gromadzenie wiedzy oraz rozwijanie metod jej najbardziej efektywnego przekazywania w zakresie prawidłowych zachowań w sytuacji zagrożenia atakiem terrorystycznym. Celem programu jest zatem stworzenie:
- podręczników, które pozwalałyby obywatelom na nabycie podstawowej wiedzy o pożądanych algorytmach zachowania w sytuacji zaistnienia ataku terrorystycznego bądź prawdopodobieństwa takiego ataku,
- programów szkoleń pozwalających na przekazanie takiej wiedzy w formie wykładów i dyskusji.

Jak nietrudno zauważyć, w co najmniej w jednym z powyższych programów pojawiają się kwestie dotyczące koordynacji działań w zakresie przeciwdziałania terroryzmowi. Jest to program wewnętrznych CBnT zatytułowany "Bezpieczeństwo Mi-

strzostw Europy w Piłce Nożnej EURO 2012 w kontekście zagrożeń terrorystycznych", który jako integralne elementy uwzględnia zagadnienia koordynacji działań instytucji zaangażowanych w organizację i zabezpieczanie imprezy oraz - organizacji procesu bezpieczeństwa.

Jednym z elementów badań o charakterze ciągłym, których wyniki publikowane są w kolejnych opracowaniach Centrum Badań nad Terroryzmem, są badania dotyczące efektywności systemu przeciwdziałania terroryzmowi w Polsce. Badania te realizowane są w ramach programu "Rola koordynacji w systemie przeciwdziałania zagrożeniom terrorystycznym". W powyższych badaniach wewnętrznych CBnT, których podstawowym przedmiotem jest koordynowanie działań służb i instytucji zaangażowanych w przeciwdziałanie terroryzmowi w państwie, podstawowe zagadnienia to:

- definiowanie obszarów odpowiedzialności w zakresie zwalczania terroryzmu,
- podział zadań między podmiotami zaangażowanymi w przeciwdziałanie terroryzmowi,
- organizacja współdziałania między tymi podmiotami w zakresie realizacji zadań w sytuacji nakładania się bądź zbiegania zakresów kompetencji.

W ramach prowadzonych prac wypracowane zostały wstępne rekomendacje, które dotąd nie były publikowane w postaci zwartego raportu z badań, jednak sygnalizowane były w poszczególnych publikacjach CBnT i Collegium Civitas. Wśród najważniejszych z nich zidentyfikować można[195]:

- powołanie instytucji koordynujące działania podmiotów zaangażowanych w przeciwdziałanie terroryzmowi jest niezbędnym warunkiem efektywności funkcjonowania systemu antyterrorystycznego państwa,
- zapewnienie zoptymalizowanego przepływu informacji, którego funkcjonowanie pozwala zarówno na szybkie, jak i uwzględniające potrzeby zapewniania bezpieczeństwa, przekazywanie informacji, zapewnia możliwość płynnego funkcjonowania systemu antyterrorystycznego państwa,
- monitorowanie, analizowanie, prognozowanie i ocena zagrożeń oraz dostarczanie czynnikom decyzyjnym w państwie raportów z powyższych

[195] Materiały badawcze Centrum Badań nad Terroryzmem, wersja robocza – niepublikowana.

działań umożliwiają strategiczne kierowanie systemem antyterrorystycznym na poziomie centralnym,

- koordynacja działań antyterrorystycznych konieczna jest nie tylko na poziomie krajowym, ale także w perspektywie międzynarodowej, zatem system / ogniwo koordynacyjne w systemie powinno posiadać zdolność i kompetencje do reprezentowania podmiotu poza granicami w ramach swoich kompetencji,
- system koordynacji przeciwdziałania terroryzmowi, a także organizowane przez niego przepływy informacji powinny być regularnie weryfikowane i oceniane – nie tylko dla sprawdzenia ich bieżącej funkcjonalności, ale także dla zapewnienia mechanizmu dostosowania w wypadku zaistnienia zmian w otoczeniu podmiotu,
- koordynacja w systemie przeciwdziałania terroryzmowi powinna być uwzględniana w narodowych planach i strategiach przeciwdziałania terroryzmowi, a także w ustawodawstwie antyterrorystycznym, aby zapewnić współdziałanie wszystkich podmiotów w systemie z organem koordynacyjnym,
- kompetencje organu koordynacyjnego powinny zostać również w odniesieniu do zarządzania kryzysowego w wypadku kryzysów, które występują w wyniku aktu terrorystycznego (szczególnie w aspekcie komunikacji społecznej w okresie kryzysu oraz prowadzenia dochodzeń i śledztw oraz informowania o ich wynikach),
- wprowadzenie mechanizmu testowania systemu przeciwdziałania terroryzmowi ze szczególnym uwzględnieniem roli organu koordynacyjnego, z udziałem wszystkich zaangażowanych podmiotów, w tym najwyższych władz państwowych, są konieczne dla sprawnego działania systemu w sytuacji zaistnienia realnego, bezpośredniego zagrożenia.

5.5.3 Prace RAND Corporation

Kwestie związane z pozyskiwaniem i analizą informacji w kontekście zapewniania bezpieczeństwa narodowego stanowią jeden z tematów, wokół których skupione są prace RAND Corporation. Z tego względu ta instytucja badawcza tworzy analizy, które wpływać mogą na sposób funkcjonowania mechanizmów wymiany informacji

oraz zwiększać efektywność wykorzystania zgromadzonych zasobów informacyjnych.

W ramach takich badań RAND Corporation prowadzi analizy rozwoju politycznego, organizacyjnego i prawnego na terytorium USA, które jednak – po poddaniu stosownej analizie i dostosowaniu do warunków lokalnych – mogą być zastosowane także w innych państwach. Biorąc jednak pod uwagę międzynarodowy wymiar przeciwdziałania terroryzmowi RAND prowadzi także szeroko zakrojone badania nad koordynacją, wyminą i pozyskiwaniem informacji nie tylko w USA, ale także w innych krajach – oraz w wymiarze międzynarodowym. Dowodem na to jest choćby przekrojowe opracowanie *Confronting the »Enemy Within«. Security Intelligence, the Police, and Counterterrorism in Four Democracies* ("Konfrontacja z "wewnętrznym wrogiem". Wywiad bezpieczeństwa, policja i kontrterroryzm w czterech demokracjach")[196].

Monografia ta poświęcona jest zagadnieniom, które stanowią przedmiot zainteresowania badaczy RAND już od wielu lat. RAND traktowany jest bowiem zarówno przez jego pracowników, jak i przez administrację rządową w USA jako instytucja ekspercka, której istnienie pozwala na outsourcing prac badawczych i analitycznych, do których wykonania lepiej predysponowane są jednostki pozarządowe, zatrudniające naukowców i badaczy, niż sama administracja, która wykonywać powinna zadania związane z bieżącym funkcjonowaniem państwa.

W ramach swoich prac dotyczących przepływów informacji na poziomie lokalnym, stanowym i federalnym, RAND stworzył monografie dotyczące różnorodnych aspektów funkcjonowania systemu bezpieczeństwa państwa[197].

---

[196] Chalk P., Rosenau W., *Confronting the "Enemy Within". Security Intelligence, the Police, and Counterterrorism in Four Democracies*, RAND Corp. 2004.

[197] Patrz: *State and Local Intelligence in the War on Terrorism* (Stanowe i lokalne służby wywiadowcze w wojnie z terroryzmem), K. Jack Riley Gregory F. Treverton, Jeremy M. Wilson Lois M. Davis, RAND Corporation 2005; *Analytic Support to Intelligence in Counterinsurgencies* (Wsparcie analityczne w zwalczaniu powstań), Walter L. Perry, John Gordon IV, RAND Corporation 2008; *Assessing the Tradecraft of Intelligence Analysis* (Ocena jakości w analizie informacji wywiadowczych), Gregory F. Treverton, C. Bryan Gabbard, RAND Corporation 2008; *Information Sharing and Emergency Responder Safety Management* (Wymiana informacji i zarządzanie bezpieczeństwem służb kryzysowych), BRIAN A. JACKSON, Wystąpienie przed Komitetem ds. Reformy Rządu, 30 marca 2006; *Domestic Terrorism. A National Assessment of State and Local Preparedness* (Terroryzm wewnętrzny. Narodowa ocena stanowej i lokalnej gotowości), Kevin Jack Riley, Bruce Hoffman, RAND Corporation 1995; *Combating Terrorism. How Prepared Are State and Local Response Organizations*? (Zwalczanie terroryzmu. Jak są przygotowane stanowe I lokalne organizacje kryzysowe?), Lois M. Davis, Louis T. Mariano, Jennifer E. Pace, Sarah K. Cotton, Paul Steinberg, RAND Corporation 2006; *Network Technologies for Networked Terrorists. Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations* (Technologie sieciowe dla sieciowych organizacji

Podsumowanie prac RAND Corporation w dziedzinie bezpieczeństwa wewnętrznego wymagałoby stworzenia odrębnej monografii poświęconej jedynie tematom, które instytucja ta porusza w obszarze bezpieczeństwa. Kolejna zaś potrzebna byłaby, aby zaprezentować choćby najważniejsze wnioski z tych prac płynące.

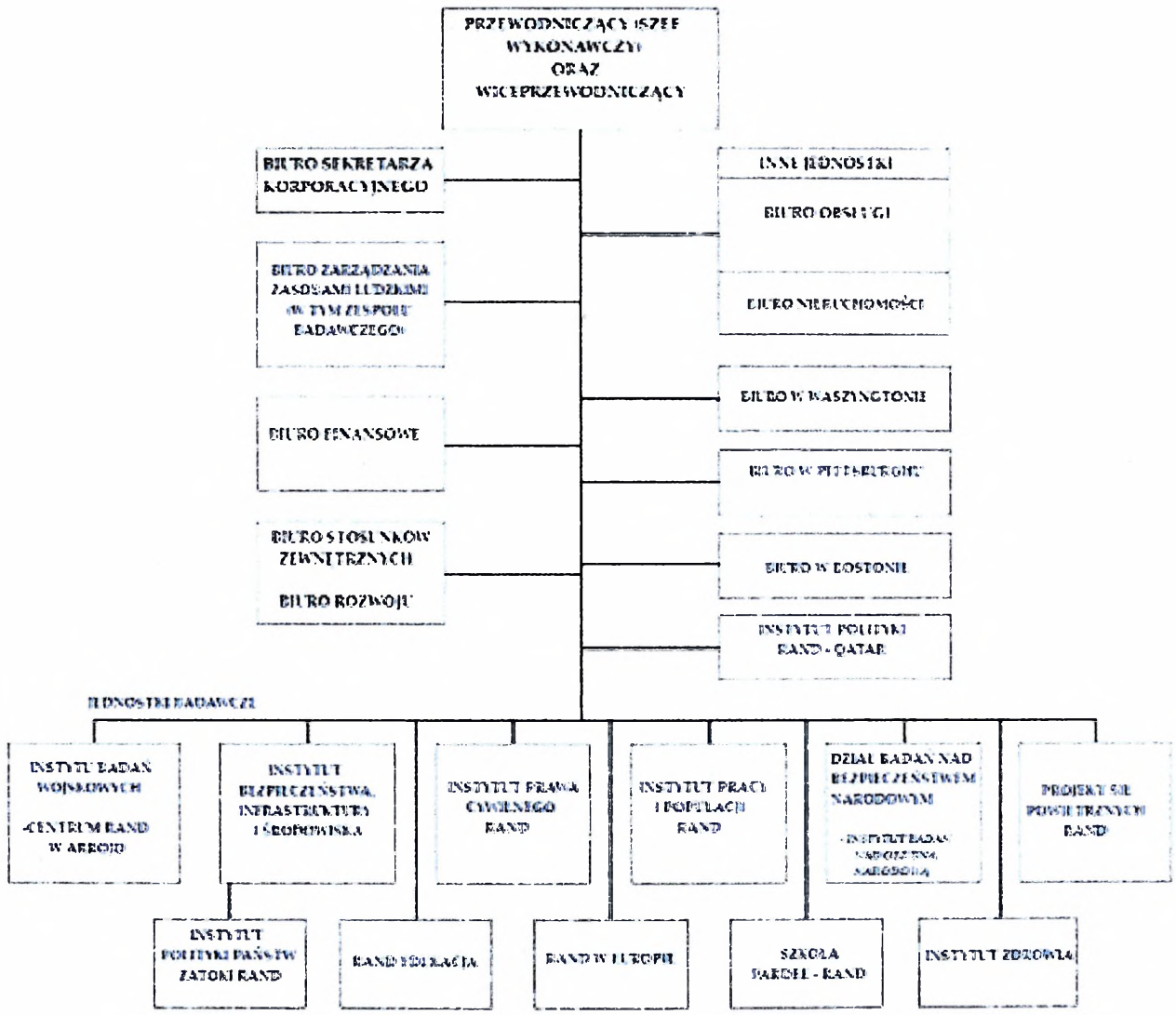
Można jednak zauważyć, że choćby pobieżna analiza wymienionych powyżej tytułów pozwala na dostrzeżenie jednego wspólnego aspektu wszystkich podejmowanych problemów: są one rozpatrywane i analizowane pod kątem systemowym i sieciowym. RAND Corporation kładzie bowiem w swoich pracach nacisk na współistnienie i współzależności pomiędzy aktorami działającymi w poszczególnych obszarach życia publicznego, politycznego i społecznego.

Dlatego właśnie tak silnie akcentowana jest w pracach analityków RAND współpraca i współdziałanie poszczególnych podmiotów, konieczność wymiany informacji oraz konsultacji podejmowanych działań. Wnioski dotyczące tych właśnie obszarów funkcjonowania instytucji i podmiotów w obszarze bezpieczeństwa i wywiadu bezpieczeństwa prezentuje między innymi przywołana wyżej praca *Confronting the »Enemy Within«. Security Intelligence, the Police, and Counterterrorism in Four Democracies.* Analizując systemy bezpieczeństwa w pięciu krajach w kontekście istniejących dla tych państw zagrożeń,, analitycy RAND stworzyli tabelę, która pozwala na zrozumienie podstawowych różnic w ich podejściu do zwalczania terroryzmu. Przedstawiając struktury i zadania oraz uprawnienia poszczególnych służb stworzyli zatem materiał analityczny, który pozwala na przyjrzenie się mechanizmom funkcjonowania służb odpowiedzialnych za bezpieczeństwo omawianych w monografii państw. Analitycy RAND wskazują przy tym wartość poszczególnych rozwiązań, przybliżając je czytelnikowi w drodze analizy porównawczej. W podsumowaniu pracy dokonują oceny poszczególnych rozwiązań, wskazując ich wady i zalety, poglądy swoje popierają zaś przykładami konkretnych elementów historii poszczególnych służb.

---

terrorystycznych. Ocena wartości technologii informacyjnych i komunikacyjnych dla współczesnych organizacji terrorystycznych), Bruce W. Don, David R. Frelinger, Scott Gerwehr, Eric Landree, Brian A. Jackson, RAND Corporation 2007; *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection* (Modelowanie ryzyka terrorystycznego dla analizy informacji wywiadowczych i ochrony infrastruktury), Henry H. Willis, Tom LaTourrette, Terrence K. Kelly, Scot Hickey, Samuel Neill, RAND Corporation 2007.

Tego rodzaju opracowania stanowią o istocie prac badawczych RAND, nie tylko w zakresie bezpieczeństwa zresztą. Prace te bowiem mają nie tylko niezwykły walor badawczy i poznawczy – odnoszą się bowiem także do rzeczywistości krajowej i międzynarodowej w sposób praktyczny, co umożliwia wykorzystanie wyników zawartych w nich badań do implementowania nowych rozwiązań w innych niż badane instytucjach.



Rys. 26: Struktura organizacyjna korporacji badawczej RAND
Źródło: portal RAND Corp. o adresie [www.rand.org]

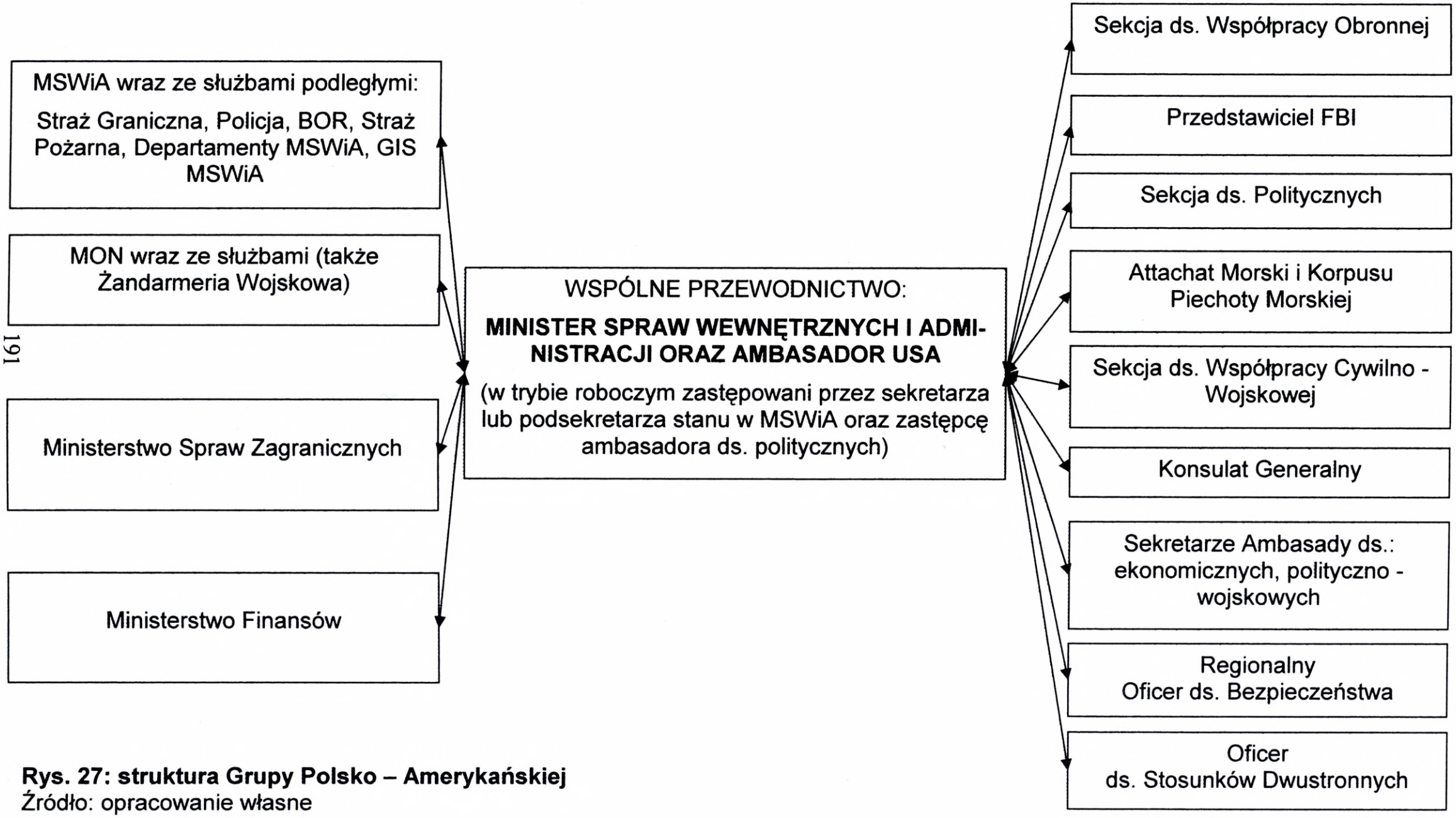
5.5.4 Wspólna Polsko-Amerykańska Grupa Robocza ds. Zwalczania Terroryzmu

W ramach współpracy polsko - amerykańskiej Ministerstwo Spraw Wewnętrznych i Administracji RP uczestniczy w pracach Wspólnej Polsko – Amerykańska Grupy Roboczej ds. Zwalczania Terroryzmu, która została powołana z inicjatywy Ministerstwa Spraw Wewnętrznych i Administracji RP oraz Ambasady USA w Warszawie w pierwszym kwartale 2005 r.[198]

W pracach Grupy uczestniczą ze strony polskiej przedstawiciele: Ministerstwa Spraw Wewnętrznych i Administracji (Departamentu Bezpieczeństwa Publicznego oraz Departamentu Zarządzania Kryzysowego), Głównego Inspektora Sanitarnego MSWiA, Komendy Głównej Policji, Komendy Głównej Straży Granicznej, Agencji Wywiadu, Agencji Bezpieczeństwa Wewnętrznego, Biura Ochrony Rządu, Żandarmerii Wojskowej, Ministerstwa Spraw Zagranicznych, Ministerstwa Obrony Narodowej, Ministerstwa Finansów.

Ze strony amerykańskiej w grupie udział biorą przedstawiciele Ambasady i innych jednostek administracji amerykańskiej: Doradca Polityczny Ambasadora, Sekretarz ds. Polityczno-Wojskowych, Attaché Morski i Korpusu Piechoty Morskiej, Oficer ds. Stosunków Dwustronnych, Biuro Współpracy ds. Obronnych, Biuro Współpracy Cywilno – Wojskowej, Konsulatu Generalnego, Sekretarz ds. Ekonomicznych, Regionalny Oficer ds. Bezpieczeństwa, Federalnego Biura Śledczego.

[198] Autor pracy był jednym z inicjatorów i twórców polsko-amerykańskiej grupy, a organizacją spotkań, opracowywaniem agend pierwszych spotkań, strukturalizujących prace grupy zajmował się podległy mu wydział w Departamencie Bezpieczeństwa Publicznego MSWiA.



Rys. 27: struktura Grupy Polsko – Amerykańskiej
Źródło: opracowanie własne

Kwestie, które są przedmiotem obrad i współpracy w Grupie, to:

- bezpieczeństwo podróży i granic;
- finansowanie terroryzmu i przestępczość zorganizowana;
- bioterroryzm;
- cyber-terroryzm i cyber-przestępczość;
- potencjalna współpraca wojsko – wojsko;
- działania dyplomatyczne wspierające kontr-terroryzm;
- zarządzanie kryzysowe po ataku terrorystycznym;
- koordynacja przeciwdziałania terroryzmowi na poziomie krajowym;
- fizyczna ochrona obiektów infrastruktury krytycznej państwa.

Wymienione wyżej kwestie omawiane i dyskutowane są zarówno na szczeblu współpracy o charakterze politycznym, jak i na szczeblu roboczym pomiędzy przedstawicielami poszczególnych służb i jednostek organizacyjnych w odniesieniu do szczegółowych, praktycznych kwestii i poszukiwania rozwiązań poruszanych problemów. Podczas obrad Grupy poruszane są także kwestie współpracy związanej z organizacją i prowadzeniem szkoleń dla polskich służb porządku publicznego, w znacznej części finansowanych przez Rząd USA.

Zaangażowanie resortu spraw wewnętrznych i administracji daje możliwość pogłębiania współpracy polsko – amerykańskiej w dziedzinie zapewniania bezpieczeństwa i pokoju międzynarodowego, zapewniając forum współpracy zarówno na poziomie roboczym, jak i politycznym. Co więcej, przedstawiony mechanizm stanowi nie tylko forum wymiany informacji pomiędzy stroną polską i amerykańską – na szczeblu politycznej współpracy taka wymiana informacji nie może dotyczyć szczególnie wrażliwych lub poufnych danych. Jest to jednak narzędzie facylitacji odpowiednich kontaktów pomiędzy podmiotami odpowiedzialnymi za przeciwdziałanie terroryzmowi po stronie polskiej i amerykańskiej, co służy nie tylko bezpośredniej współpracy, ale także długoterminowej poprawie bezpieczeństwa obu państw.

5.6 Wnioski

We wszystkich omówionych systemach występują ogniwa odpowiedzialne za gromadzenie informacji. Nie wymaga szczególnego podkreślania, że źródła informacji nie są tożsame z mechanizmami zarządzania informacją, dlatego właśnie zapewnieniem dopływu informacji we wszystkich przedstawionych systemach zajmują się służby wchodzące w skład systemu przeciwdziałania terroryzmowi, których przedstawiciele uczestniczą w pracach poszczególnych systemów zarządzania informacją.

W systemie niemieckim gromadzeniem informacji zajmują się takie służby, jak na przykład:

- Federalny Urząd Kryminalny (także na poziomie landów),
- Federalny Urząd ds. Ochrony Konstytucji (także na poziomie landów),
- Federalna Służba Wywiadowcza,
- Policja Federalna,
- Śledcza Służba Celna,
- Wojskowa Służba Bezpieczeństwa,
- Federalny Urząd ds. Migracji i Uchodźców.

Instytucje te gromadzą w zakresie swoich kompetencji (niezmienionych w wyniku powstania GTAZ) informacje dotyczące wszelkich kwestii, które związane są z potencjalnym atakiem terrorystycznym, a wymianie podlegają w ramach mechanizmu, który omówiony zostanie w następnej części podsumowania.

W Wielkiej Brytanii, uczestnicy JTAC odpowiedzialni za gromadzenie informacji w toku prowadzonych działań rozpoznawczych, to między innymi:

- Służba Bezpieczeństwa MI 5,
- Tajna Służba Wywiadowcza MI 6,
- Policja,
- służby celne, imigracyjne i podatkowe.

Informacje w systemie przeciwdziałania terroryzmowi w Wielkiej Brytanii gromadzone są również na poziomie minimalizacji i likwidacji skutków ataków terrorystycznych, a zatem na poziomie zarządzania kryzysowego. Zgodnie z omówionym wcześniej mechanizmem odpowiada za to działanie Sekretariat Cywilnego Reago-

wania Kryzysowego, tworzący matryce zagrożeń oraz plany reagowania na wypadek zaistnienia zagrożenia.

We Francji wśród służb odpowiedzialnych za gromadzenie informacji w systemie znajdują się:

- Dyrekcja Centralna Wywiadu Ogólnego,
- Francuska Służba Bezpieczeństwa,
- Francuska Służba Bezpieczeństwa Zagranicznego,
- Dyrekcja Ochrony i Bezpieczeństwa Obronnego,
- Narodowa Dyrekcja ds. Dochodzeń Kryminalnych,
- Policja Graniczna,
- Miejskie Siły Policyjne (Departament Bezpieczeństwa Publicznego),
- Żandarmeria Francuska (w szczególności w odniesieniu do terenów wiejskich).

Jak zostało zaznaczone wcześniej, przekazywanie informacji przez wszystkich wymienione podmioty w systemie francuskim odbywa się na zasadzie pełnej dobrowolności, nie istnieje zatem prawny nakaz takiego działania.

W systemie amerykańskim obowiązuje prawny rygor dzielenia się informacjami. Wśród jednostek, które uczestniczą w działania systemu i podlegają temu rygorowi, wymienić można:

- Federalne Biuro Śledcze,
- Centralną Agencję Wywiadowczą,
- Policję Kapitolu,

a także innych członków wspólnoty wywiadowczej.

W zakresie przetwarzania informacji, przedstawione systemy zarządzania informacją realizują jedną ze swoich najważniejszych funkcji. Stanowiąc wspólny punkt analiz informacji gromadzonych w procesie rozpoznania i identyfikacji zagrożeń metodami poza-operacyjnymi, są punktem odniesienia dla poszczególnych uczestników systemu, zapewniając jednocześnie stabilną płaszczyznę odniesienia dla czynników decyzyjnych.

Taką rolę bez wątpienia pełnią zespoły robocze niemieckiego GTAZ, na forum których odbywa się nie tylko wymiana informacji, ale także ich ocena i analiza. Szczególną uwagę w tym kontekście poświęcić jednak należy:

- Zespołowi oceny zagrożeń,
- Zespołowi ds. oceny przypadków,
- Zespołowi ds. analiz strukturalnych,
- Zespołowi ds. islamistycznego terrorystycznego potencjału ludzkiego.

Każdy z tych zespołów stanowi nie tylko forum wymiany informacji, ale także platformę współpracy umożliwiającą wspólną ocenę zagrożeń oraz wszechstronną analizę informacji, mogących stanowić sygnał o zaistnieniu zagrożenia atakiem terrorystycznym.

W systemie brytyjskim cała struktura mechanizmu zarządzającego informacjami, a zatem JTAC oparta jest o podstawową potrzebę sporządzania wspólnych analiz. Dlatego właśnie JTAC, składając się zasadniczo z 4 części, dwie z nich, tj. Grupę Analiz Regionalnych oraz Grupę Analiz Tematycznych, poświęca samej analizie, a trzecią – Grupę Wsparcia Analitycznego – wsparciu procesu analitycznego.

Trzeba podkreślić, że jednym z podstawowych zadań JTAC, identyfikowanych przez jego założycieli i uczestników, jest analiza i ocena informacji wywiadowczych związanych z międzynarodowym terroryzmem, zarówno w odniesieniu do terytorium Wielkiej Brytanii, jak i jej interesów poza granicami państwa.

W systemie francuskim sporządzanie analiz odbywa się w ramach dwufazowego procesu, podzielonego na zbieranie i porównywanie informacji podczas spotkań przedstawicieli instytucji zaangażowanych w działania UCLAT.

Informacje te przetwarzane są przez UCLAT na dwóch poziomach:

- analizy informacji o charakterze operacyjnym, na potrzeby działań operacyjnych niezbędnych dla przeprowadzania akcji poszczególnych służb kontr-terrorystycznych,
- analiz o charakterze taktycznym i strategicznym, sporządzanych na potrzeby czynników rządowych.

Szczególne miejsce przetwarzanie informacji zajmuje w systemie amerykańskim. W NCTC wydzielono odrębny pion, Dyrektoriat Strategicznego Planowania Operacyjnego, który odpowiedzialny jest za sporządzanie ocen i analiz, a także tworzenie na podstawie przetworzonych informacji planów działań. Komórki związane z przetwarzanie informacji funkcjonują także w innych pionach NCTC:

- Grupa poprawy zdolności analiz w Dyrektoriacie Zarządzania Misjami,
- Zaawansowane techniki analityczne i „czerwone grupy" w Dyrektoriacie Wymiany Informacji i Rozwoju Wiedzy.

W związku z tak bogatymi strukturami dedykowanymi zagadnieniom analitycznym, NCTC dysponuje również całą grupą „produktów analitycznych", z których korzystają zarówno czynniki decyzyjne, jak i podmioty wykonawcze.

Przechowywanie informacji związanych z funkcjonowaniem systemów kontrterrorystycznych na świecie obciążone jest koniecznością zapewnienia bezpieczeństwa informacji, które z racji swojego charakteru oraz bezpośredniego wpływu na bezpieczeństwo państwa w znacznej większości mają charakter niejawny, chroniony przez systemy prawne poszczególnych państw.

Przechowywanie tych informacji podlega rygorom bezpieczeństwa nie tylko ze względu na prawodawstwo narodowe, ale także z racji zobowiązań międzynarodowych państw. Walka z terroryzmem we współczesnym świecie ma charakter międzynarodowy – i taki charakter ma również realizowana w toku współpracy z partnerami wymiana informacji. W takiej sytuacji konieczne jest branie pod uwagę zapisów dwustronnych umów o wzajemnej ochronie informacji niejawnych, a także regulacji odnośnych regulacji organizacji międzynarodowych, jak NATO i Unia Europejska.

Właściwe normy bezpieczeństwa obowiązują więc w odniesieniu do wszystkich form zapisu informacji, zarówno tradycyjnych, jak i bezpieczeństwa systemów teleinformatycznych (koniecznych w wypadku baz danych tworzonych w poszczególnych systemach, jak baza raportów z posiedzeń Zespołu codziennych narad na temat sytuacji w GTAZ lub amerykańskiej wspólnej bazy NCTC oraz baz danych poszczególnych podmiotów realizujących zadania w zakresie przeciwdziałania terroryzmowi).

Jednym z najistotniejszych aspektów funkcjonowania krajowych systemów zarządzania informacjami zdobywanymi w toku i na potrzeby działań związanych z przeciwdziałaniem terroryzmowi, jest dostarczanie stosownego obrazu sytuacji czynnikom decyzyjnym, odpowiedzialnym za decydowanie o kształcie narodowych działań w tym zakresie. Dystrybucja odbywa się także w płaszczyźnie horyzontalnej,

na poziomie wymiany informacji pomiędzy poszczególnymi podmiotami realizującymi zadania w zakresie przeciwdziałania terroryzmowi.

W systemie niemieckim funkcję dystrybucji informacji na poziom rządowy w sposób bezpośredni realizuje Zespół ds. oceny zagrożeń, który przekazuje władzom Niemiec rekomendacje, mające na celu podejmowanie określonych działań na poziomie krajowym. Pozostałe zespoły robocze stanowią fora wymiany informacji, które w dalszej fazie, w postaci raportów, są dystrybuowane do wszystkich uczestników GTAZ, którzy danych informacji potrzebują.

W systemie brytyjskim funkcję tę realizuje JTAC jako całość, bowiem przygotowywane przez tę instytucję analizy stanowią podstawę określania poziomu zagrożenia, decydującego o działaniach podejmowanych przez podmioty państwowe w całym kraju. Ponadto zaznaczyć należy, że Szef JTAC odpowiada przed Dyrektorem Generalnym MI5, który przekazuje jego raporty nt. zagrożenia Rządowemu Połączonemu Komitetowi ds. Wywiadu. Przedstawiciele JTAC uczestniczą także w roli ekspertów w posiedzeniach rządowych komitetów ds. zwalczania terroryzmu. Nadmienić należy także, że JTAC, poza poziomem rządowym, działa w odpowiedzi na potrzeby innych tzw. „klientów", czyli instytucji administracji publicznej – uczestników JTAC, którym przekazuje niezbędne dla prawidłowej realizacji ich działań analizy i oceny sytuacji.

System francuski charakteryzuje się, podobnie jak niemiecki, przede wszystkim horyzontalnym przepływem informacji, odbywającym się pomiędzy uczestnikami UCLAT podczas cotygodniowych spotkań. Na poziom rządowy informacja ze strony UCLAT dociera poprzez:

- informacje przekazywane przez Szefa UCLAT ministrowi spraw wewnętrznych,
- koordynowanie spraw związanych ze zwalczaniem terroryzmu na posiedzeniach Rady Bezpieczeństwa Wewnętrznego,
- informacje eksperckie UCLAT wykorzystywane są także w pracach Międzyresortowego Komitetu ds. Wywiadu, Międzyresortowego Komitetu Kontr-terrorystycznego oraz funkcjonującego na poziomie ministerstwa spraw wewnętrznych Narodowego komitetu Wywiadu.

Bogatą działalność w zakresie dystrybucji informacji prowadzi również amerykańskie NCTC. Wśród jego zadań wyróżnia się bowiem następujące:

- zapewnianie dostępu agencji do informacji wywiadowczych ze wszystkich źródeł, niezbędnych do wykonania przypisanych im zadań,
- stanowieni centralnego banku wspólnej wiedzy na temat znanych i domniemanych terrorystów i międzynarodowych grup terrorystycznych, ich celów, strategii, zdolności, sieci kontaktów i wsparcia.

NCTC w ciągu każdego dnia, jak zostało opisane we wcześniejszej części pracy, prowadzi trzy telekonferencje z udziałem przedstawicieli Narodowej Rady Bezpieczeństwa oraz wspólnoty wywiadowczej. Ponadto, w zakresie dystrybucji informacji konieczne jest wskazanie NCTC Online, czyli Narodowego Centrum Kontrterrorystycznego online, które zapewnia bieżący dostęp do informacji, a także zapewnia istnienie forów internetowych dla uczestników systemu, kont e-mail oraz chatu, umożliwiających wymianę informacji i doświadczeń.

Przedstawione w niniejszej części pracy systemy zarządzania informacjami i koordynacji powstały w określonych warunkach prawno – organizacyjnych poszczególnych państwa, których struktury wzięte zostały pod uwagę podczas prowadzonych badań. Koordynacja zwalczania terroryzmu, jako proces oparty na gromadzeniu i przetwarzaniu informacji wymaga wprowadzania rozwiązań, które pozwolą na efektywne prowadzenie działań w tych dwóch obszarach. W związku z powyższym w państwach zagrożonych przez terroryzm tworzone są systemy, które wprowadzają takie rozwiązania prawno – organizacyjne, a ich funkcjonowanie jest oparte na zasadach konstytucyjnych kształtujących środowisko prawne państwa.

Jednak, ze względu na to, że przedmiotem niniejszej pracy jest próba stworzenia optymalnego, niezwiązanego z żadnym szczególnym systemem prawnym mechanizmu, konieczne jest podsumowanie powyższych analiz rozwiązań krajowych z wyciągnięciem wniosków, które przyczynią się do stworzenia wspomnianego modelu optymalnego.

Wśród elementów omawianych systemów znajdują się mechanizmy, które umożliwiają:

– gromadzenie, analizę, dystrybucję i przechowywanie informacji,

- planowanie strategiczne i operacyjne,
- określanie zakresów zadań i odpowiedzialności poszczególnych podmiotów odpowiedzialnych za różne fazy przeciwdziałania terroryzmowi.

Wśród uczestników systemów znajdują się zatem instytucje, które wśród swoich zadań realizują między innymi zadania niezbędne dla funkcjonowania systemu, a więc zajmujące się:

- rozpoznawaniem zagrożeń,
- tworzeniem stosownych baz danych, na podstawie których tworzone mogą być wspólne bazy, dostępne dla wszystkich uczestników,
- analizą i tworzeniem reportów na temat zagadnień związanych z międzynarodowym terroryzmem oraz metodami jego zwalczania,
- planowaniem zadań w zakresie przeciwdziałania terroryzmowi.

Obserwowane są różne modele uczestnictwa w systemach koordynacji i zarządzania informacjami. W zależności od tego, jakie założenia przyjęte zostały w fazie wstępnej planowania mechanizmu, uczestnictwo podmiotów (od poziomu przekazywania informacji począwszy, a na wspólnym prowadzeniu informacji skończywszy) jest opcjonalne lub obowiązkowe.

W systemie francuskim (UCLAT) zastosowane zostało pierwsze rozwiązanie. Podmioty odpowiedzialne za przeciwdziałanie terroryzmowi we Francji funkcjonują w systemie w sytuacji, w której same podejmą decyzję o przekazaniu informacji i powierzeniu koordynacji danej operacji do UCLAT.

W systemie amerykańskim (NCTC) obowiązki i uprawnienia poszczególnych podmiotów w odniesieniu do funkcjonowania w ramach NCTC zostały uregulowane ustawowo. Jest to instytucja, która z mocy ustawy integruje wszystkie informacje posiadane przez agendy rządowe w związku z terroryzmem. Instytucja ta odpowiada także za planowanie strategiczne działań operacyjnych, a także przypisuje role i zakresy odpowiedzialności poszczególnym podmiotom.

Podobne rozwiązanie obowiązuje w systemie niemieckim i brytyjskim, gdzie uczestnictwo oraz przekazywanie informacji mechanizmowi zarządzającemu informacją (a tym samym jednostce koordynującej działania) odbywa się na zasadzie obligatoryjnej. Odnotować w tym miejscu należy jednak pewną odmienność systemu niemieckiego, w którym Centrum ds. Walki z Terroryzmem nie posiada zwierzchnika,

a jedynie zespoły robocze, w których odbywa się wymiana informacji – przy czym różnym zespołom przewodniczą różne instytucje uczestniczące w systemie.

Jak wynika z powyższych obserwacji, dotyczących poszczególnych systemów zarządzania informacją oraz koordynacji działań w systemach przeciwdziałania terroryzmowi, są one zróżnicowane ze względu na:

- systemy konstytucyjno – prawne obowiązujące w poszczególnych państwach,
- dominującą w poszczególnych krajach kulturę organizacyjną, przekładającą się na zdolność współpracy (np. bez obligacji prawnej),
- doświadczenie państwa w zakresie przeciwdziałania terroryzmowi oraz zdolność dostosowania obowiązujących reguł do dynamicznej groźby, jaką stanowi terroryzm,
- poziom zagrożenia potencjalnymi atakami terrorystycznymi.

W celu stworzenia optymalnego modelu systemu zarządzania informacji w sytuacji zagrożenia bezpieczeństwa państwa przez terroryzm, użyte zostaną wzorce stworzone i sprawdzone pod kątem swojej funkcjonalności. Jednak, aby zapewnić największą, z punktu widzenia celów tej pracy, funkcjonalność tworzonego modelu, poszczególne elementy zostaną wybrane z różnych systemów, systemów sposób ich funkcjonowania zmodyfikowany pod kątem optymalnego wyniku podejmowanych w ramach systemu działań.

Rozdział 6

Model zarządzania zasobami informacyjnymi w systemie przeciwdziałania terroryzmowi

6.1 Podstawowe funkcje zarządzania

Działania prowadzone w systemie przeciwdziałania terroryzmowi oparte są na systemie obiegu informacji i zarządzania nią. Warto zatem poddać analizie wielopoziomowość działań związanych w przeciwdziałaniem terroryzmowi w państwie.

Przede wszystkim zauważyć należy, że zgodnie z teorią zarządzania w każdym systemie, którego dotyczy proces zarządzania, wyróżnić można cztery podstawowe mechanizmy działania. Należą do nich: planowanie, organizowanie, przewodzenie oraz kontrola. Pojęcia te muszą podlegać specyficznej interpretacji będąc rozpatrywane w odniesieniu do zarządzania systemem przeciwdziałania terroryzmowi, ze szczególnym uwzględnieniem obiegu informacji.

Pierwszą zatem kwestią, którą należy w tym kontekście poruszyć jest planowanie. Na poziomie budowania bezpieczeństwa państwa w stosunku do zagrożenia, jakim jest terroryzm, przez planowanie rozumieć należy tworzenie strategii państwa w zakresie przeciwdziałania terroryzmowi. Dokument taki powinien być zatwierdzany przez rząd państwa i nadawać wspólny kierunek wszelkim działaniom podmiotów odpowiedzialnych za przeciwdziałanie terroryzmowi.

Łatwo jednak dostrzec, że rząd państwa tylko pod względem formalnym zatwierdza strategię zwalczania terroryzmu. Nie jest możliwe bowiem stworzenie takiego dokumentu, wymagającego szczegółowej wiedzy eksperckiej w zakresie zarówno potencjalnych zagrożeń ze strony terroryzmu, jak i metod jego zwalczania, na wysokim szczeblu rządowym. Tak zatem konieczne jest wskazanie w systemie podmiotu, który będzie przedstawiał rządowi propozycję strategii, wnosząc tym samym znaczący wkład w element systemu określany mianem planowania.

Zadanie takie spełniać może – czy też raczej powinno – funkcjonujące na szczeblu rządowym wyspecjalizowane ciało koordynacyjne. Model takiego ciała ko-

ordynacyjnego, wraz z zakresem zadań, jakie powinno ono realizować przedstawiony zostanie w kolejnym podrozdziale.

Należy ponadto zauważyć, że dla pełnej efektywności systemu, a także ze względu na konieczność dokonywania kontroli jego osiągnięć, strategia powyższa nie powinna być jedynie deklaracją celów o charakterze politycznym. Zawierać ona powinna konkretne zadania w skali krótko-, średnio- i długookresowej.

Kolejny element zarządzania w systemie przeciwdziałania terroryzmowi to organizacja. W przeciwieństwie do innych sytuacji, w których stosowane są mechanizmy zarządzania w systemie przeciwdziałania terroryzmowi, proces organizacji musi ukonstytuować się w ramy organizacyjne zanim system rozpocznie właściwe działanie. Dlatego też etap „organizowanie" w zarządzaniu w systemie przeciwdziałania terroryzmowi stanowić będzie kształt organizacji przeciwdziałania terroryzmowi, nadający właściwą formę współdziałaniu podmiotów odpowiedzialnych za realizację takich zadań. Zasadniczym punktem tego systemu, ram organizacyjnych działań podmiotów realizujących zadania w obszarze przeciwdziałania, będzie centrum koordynacyjne.

Element „kierowania" w systemie przeciwdziałania terroryzmowi również przyjmie szczególną postać. Jak zostanie to zobrazowane w części dotyczącej koordynacji działań w tym systemie, jego składowe stanowią służby i instytucje, które z mocy prawa posiadają własne, autonomicznie realizowane zadania. Co więcej, na mocy przepisów pranych, służby i instytucje, o których mowa, nie są sobie wzajemnie podległe. Sprawna zaś realizacja wszystkich wykonywanych przez nie zadań jest niezbędna dla zapewnienia bezpieczeństwa państwu. Z tego względu element kierowania w systemie przeciwdziałania terroryzmowi powinien przyjąć formę koordynacji działań, a zatem, zgodnie z definicją podawaną przez *Słownik wyrazów obcych* PWN:

> *uporządkowanego współdziałania, zharmonizowania, uzgodnienia wzajemnego działania.*[199]

Koordynację taką zapewnić powinna instytucja, która nie jest odpowiedzialna bezpośrednio za realizację zadań w zakresie poszczególnych etapów przeciwdziałania terroryzmowi, a tym samym nie posiada szczególnych kompetencji przysługują-

[199] Tokarski J. (red.), *Słownik wyrazów obcych*, Warszawa 1980, s. 390.

cych istniejącym służbom policyjnym oraz specjalnym. Zapewni to nie tylko gwarancję bezstronnego podejścia do koordynowania zadań istniejących w systemie przeciwdziałania terroryzmowi.

Tab. 15: Zarządzanie w systemie przeciwdziałania terroryzmowi

Zarządzanie w systemie przeciwdziałania terroryzmowi		
1. Planowanie	CENTRUM KOORDYNACYJNE	Strategia przeciwdziałania terroryzmowi zatwierdzana przez rząd państwa
2. Organizowanie		System przeciwdziałania terroryzmowi
3. Koordynacja		CENTRUM KOORDYNACYJNE
4. Kontrola		Doroczny przegląd realizacji strategii

Źródło: opracowanie własne.

Element kierowania / koordynacji w systemie przeciwdziałania terroryzmowi pokrywa się z elementem koordynującym w systemie zarządzania zasobami informacyjnymi gromadzonymi w systemie przeciwdziałania. Z tego względu element ten omówiony zostanie szczegółowo – na poziomie organizacji wewnętrznej i realizowanych zadań – w podrozdziale dotyczącym koordynacji w systemie przeciwdziałania terroryzmowi – dystrybucji i rozpowszechniania informacji.

Poziom kontrolny w systemie przeciwdziałania terroryzmowi realizowany powinien być na poziomie dorocznych przeglądów realizacji zadań przewidzianych w strategii przeciwdziałania terroryzmowi. Jak wspomniano wcześniej, strategia ta, oprócz elementów politycznych, powinna zawierać konkretne działania, założone jako cele funkcjonowania systemu przeciwdziałania terroryzmowi.

Przegląd ten powinien być realizowany , a jego ostateczne efekty zatwierdzane przez czynniki polityczne na poziomie rządowym[200]. Pamiętać jednak należy, że podobnie, jak w wypadku przygotowania zapisów strategii, merytoryczny przegląd, wraz z formalnym raportem z realizacji przeglądu powinien być przygotowywany przez

[200] „Czynniki polityczne" dla potrzeb tej pracy oznaczają wszystkie podmioty i organy, które mają konstytucyjne i ustawowe uprawnienia do kierowania służbami i instytucjami wchodzącymi w skład systemu przeciwdziałania terroryzmowi oraz do kształtowania polityki i strategii państwa w zakresie przeciwdziałania terroryzmowi, jak: prezydent, premier, właściwi ministrowie, szefowie służb i agencji rządowych, a także przedstawiciele ciał parlamentarnych wchodzący w skład ciał i organów mających wpływ na działania związane z bezpieczeństwem państwa; w dalszych schematach podmioty te określane będą wspólnym mianem "CZYNNIK POLITYCZNY"

kompetentne ciało. Podobnie, jak w wypadku przygotowania strategii, ciałem tym powinno być centrum koordynacyjne.

6.2 Koordynacja w systemie przeciwdziałania terroryzmowi

Zagadnienie koordynacji działań podejmowanych przez instytucje państwowe w procesie przeciwdziałania terroryzmowi przywołane zostało już w rozdziale I niniejszej pracy, w części poświęconej profilaktyce społecznej. Niemniej jednak konieczne jest dalsze skupienie się na tej kwestii, przede wszystkim ze względu na fakt, iż brak koordynacji działań w dowolnym systemie powoduje dublowanie podejmowanych działań, interferencje pomiędzy działaniami podejmowanymi przez poszczególne podmioty, a w najgorszym przypadku – wzajemną destrukcję potencjalnych zamierzonych efektów tych działań.

Jest to szczególnie istotne ze względu na wielość podmiotów, które realizują zadania związane z przeciwdziałaniem terroryzmowi[201]. Zaliczyć do nich można bowiem:

1. cywilne służby specjalne:
   - wywiad – podlegający ministerstwu spraw zagranicznych,
   - kontrwywiad – podlegający resortowi spraw wewnętrznych,
2. wojskowe służby specjalne: wywiad i kontrwywiad – podlegające ministerstwu obrony narodowej
3. służby o charakterze policyjnym – podlegające ministerstwu spraw wewnętrznych,
4. służby odpowiedzialne za zwalczanie finansowania terroryzmu – podległe ministerstwu finansów:
   - inspektorat informacji finansowej,
   - służby celne,
   - inspekcja skarbowa,
   - służby antykorupcyjne – podległe premierowi,

[201] Wszystkie podmioty, będące służbami i instytucjami oraz agencjami rządowymi, mającymi zadania bądź uprawnienia, w związku z którymi stanowią część krajowego systemu przeciwdziałania terroryzmowi wyliczane w zestawieniu, w dalszych schematach dotyczących projektowanego Centrum Koordynacji, Analiz i Łączności określane będą wspólnym mianem „SŁUŻBA".

5. resort spraw zagranicznych – placówki dyplomatyczne gromadzące informacje pochodzące ze źródeł otwartych.

Koordynacja zadań realizowanych przez powyższe podmioty z racji samej ich wielości musi być niezwykle złożonym zadaniem. Jeśli wziąć pod uwagę także fakt, że każdy z nich swoje zadania realizuje na podstawie innej pragmatyki, wcielając w życie różne algorytmy działań, a wreszcie, że stają przed nimi inne ustawowe zadania, poziom komplikacji zadań związanych z koordynacją wzrasta niepomiernie.

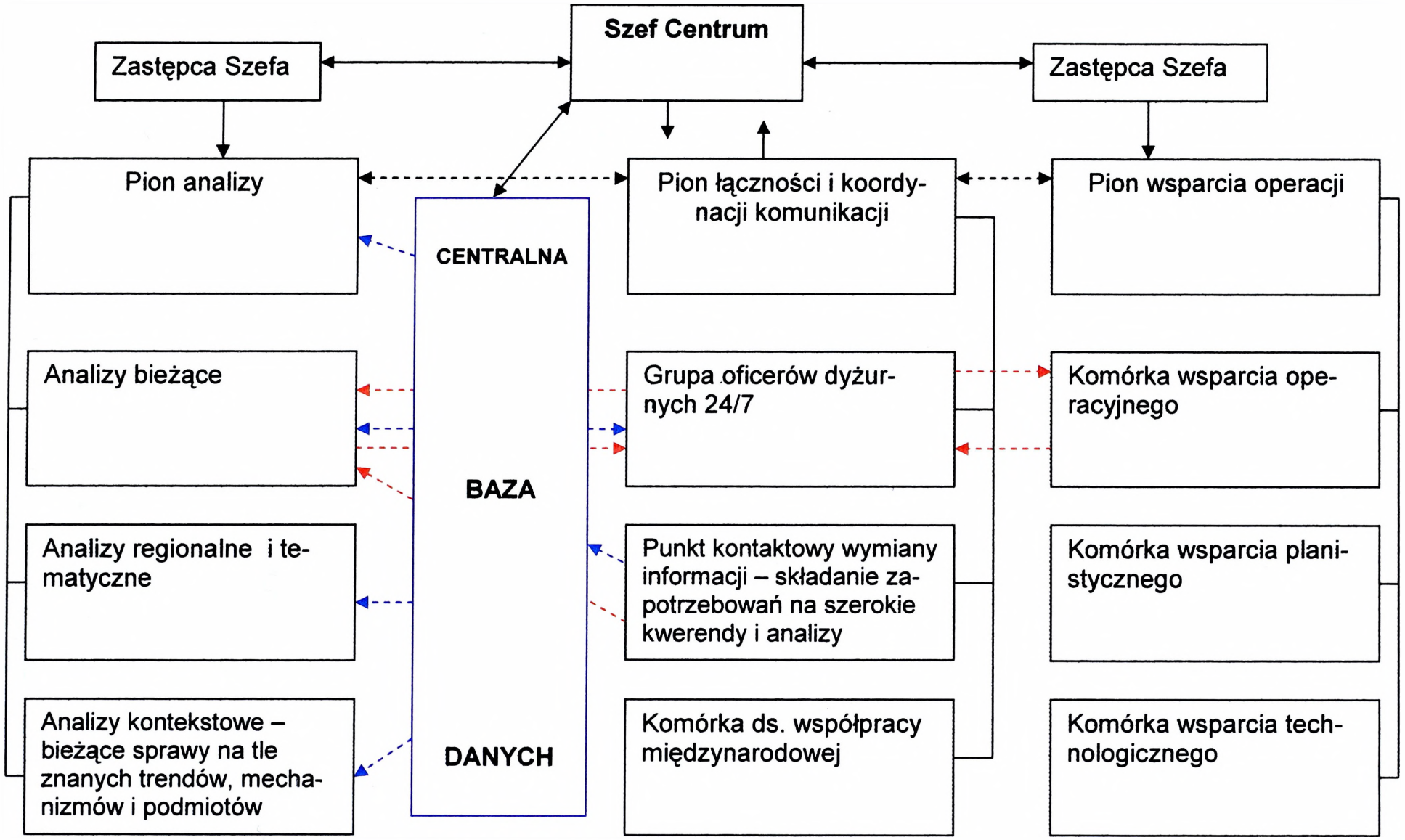
Dlatego dla właściwej realizacji koordynacji konieczne jest stworzenie zewnętrznego podmiotu koordynacyjnego, wspomnianego w podrozdziale dotyczącym zarządzania w systemie przeciwdziałania terroryzmowi.

Do zadań takiego centrum koordynacyjnego zaliczyć należałoby:

- monitorowanie zagrożeń o charakterze terrorystycznym, a także przedstawianie opinii i wniosków dla rządu,
- analizowanie i integrowanie wszystkich informacji wywiadowczych posiadanych i zdobywanych przez rząd poprzez jego służby, agencje i instytucje, dotyczących terroryzmu i kontr-terroryzmu,
- zapewnienie dostępu podmiotów odpowiedzialnych za przeciwdziałanie terroryzmowi do informacji wywiadowczych ze wszystkich źródeł, niezbędnych do realizowania planów kontr-terrorystycznych i wykonywania niezależnych, alternatywnych analiz oraz wykonania przypisanych im zadań,
- opracowywanie projektów standardów i procedur w zakresie zwalczania terroryzmu, w szczególności standardów oceny występowania zagrożenia i określania jego poziomu;
- inicjowanie, koordynowanie i monitorowanie działań podejmowanych przez właściwe organy administracji rządowej, w szczególności w zakresie wykorzystania informacji oraz rozpoznawania, przeciwdziałania i zwalczania terroryzmu;
- prowadzenie strategicznego planowania operacyjnych działań kontr-terrorystycznych, integrujących wszystkie elementy i możliwości kraju, z włączeniem narzędzi dyplomatycznych, finansowych, militarnych, wywiadowczych, bezpieczeństwa wewnętrznego oraz służb wdrażania prawa zarówno wewnątrz, jak i pomiędzy agencjami,

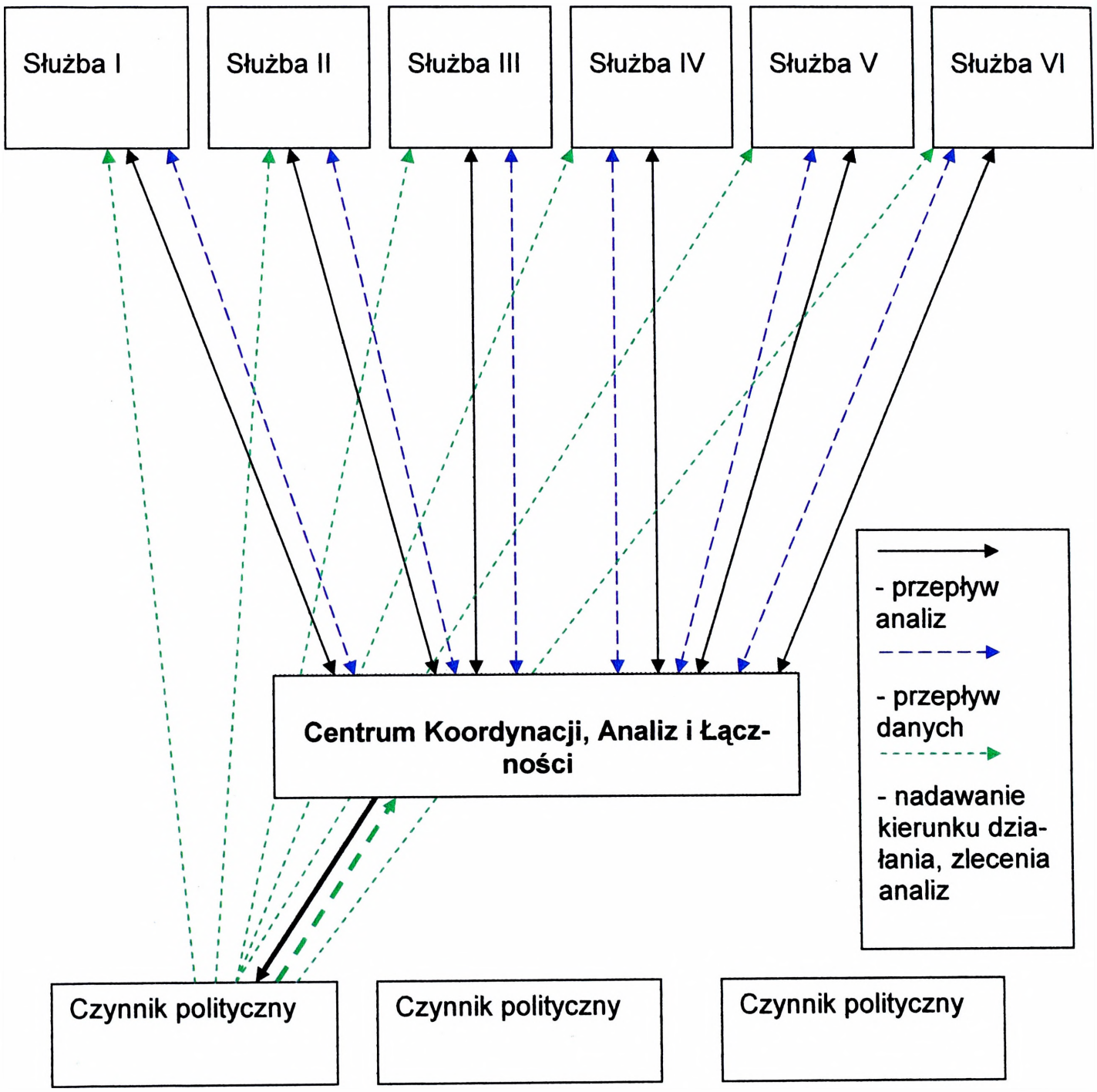
- organizowanie współpracy z organami innych państw w zakresie zwalczania terroryzmu oraz koordynacja wymiany informacji i organizowanie wspólnych operacji,
- inicjowanie szkoleń i konferencji dotyczących zwalczania terroryzmu,
- projektowanie kierunków przedsięwzięć przeciwdziałających terroryzmowi,
- nadzorowanie działania zespołów zadaniowych i ocena efektów ich działań, których funkcjonowanie zostanie omówione w dalszej części rozdziału.

Poniższy schemat ilustruje proponowaną strukturę organizacyjną omawianego centrum koordynacyjnego.



Rys. 28: Schemat organizacyjny Centrum Koordynacji, Analizy i Łączności
Źródło: opracowanie własne

Poziom koordynacji działań służb i instytucji odpowiedzialnych za bezpieczeństwo kraju nie jest jednak wystarczający, aby opisać pełne funkcjonowanie systemu bezpieczeństwa – poprzez pryzmat obiegu w nim informacji, ani też dla opisania pełnej roli organu koordynacyjnego. Aby zrozumieć jego miejsce w systemie przeanalizować należy jego związki ze służbami i instytucjami koordynowanymi oraz z czynnikami decyzyjnymi na szczeblu politycznym.



Rys. 29: Relacje „Centrum Koordynacji - służby - czynnik polityczny" z uwzględnieniem 1 czynnika politycznego[202]
Źródło: opracowanie własne.

[202] Patrz przypis nr 200, s. 203 oraz 201, s. 204.

Wyjaśniwszy, jakie zasadniczo zadania spełniać powinno przedstawione centrum koordynacyjne, należy szczegółowo przedstawić również związki i relacje, zachodzące pomiędzy centrum i służbami oraz pomiędzy centrum i czynnikami politycznymi.

Centrum pełni w systemie rolę koordynacyjną, a jednocześnie usługową w stosunku zarówno do służb odpowiedzialnych za przeciwdziałanie terroryzmowi, jak i w stosunku do czynników politycznych.

Na linii kontaktów „centrum – służby" zdefiniować można następujące relacje:

- Centrum gromadzi informacje pochodzące od służb,
- Centrum przekazuje poszczególnym służbom informacje pochodzące od innych służb w wypadku złożenia przez nie kwerendy dotyczącej określonej kwestii,
- Centrum stanowi działające w systemie 24-godzinnym centrum dostępu do informacji – poprzez działającą 24/7 grupę oficerów dyżurnych,
- Centrum udziela służbom wsparcia operacyjnego w wypadku zgłoszenia przez nie takiego zapotrzebowania poprzez:
  - współudział w przygotowaniu planów operacji,
  - współudział w przygotowaniu technologicznym operacji
  - dostarczanie bieżących informacji uzyskanych z innych źródeł,
  - identyfikowanie potrzeb informacyjnych w zakresie przeciwdziałania terroryzmowi,
- Centrum zapewnia dostęp służb do przygotowanych analiz bieżących, regionalnych i tematycznych, a także przygotowuje szeroko zakrojone analizy na potrzeby służb.

Na linii kontaktów „centrum – czynniki polityczne" zdefiniować można następujące relacje:

- Centrum przygotowuje analizy i rekomendacje dla czynników politycznych, umożliwiające strategiczne planowanie w zakresie przeciwdziałania terroryzmowi,

- Centrum wspiera poziom polityczny w przygotowaniu stanowisk w zakresie współpracy międzynarodowej w przeciwdziałaniu terroryzmowi na poziomie politycznym poprzez zapewnienie odpowiedniej ekspertyzy,
- w wyniku zleceń kierunkowych od czynników politycznych Centrum przygotowuje długoterminowe raportu w dziedzinie zagrożenia państwa przez terroryzm.

W procesie omawiania powyższych kwestii nie wolno zapomnieć, że odnośnie realizacji zadań służb w zakresie przeciwdziałania terroryzmowi, kompetentne czynniki polityczne na szczeblu rządowym mają prawo i obowiązek kierować działaniami służb również bez pośrednictwa centrum koordynacyjnego. Wynika to z faktu, że rola koordynacyjna centrum ma mieć charakter facylitacyjny, a nie kierowniczy.

Jak wynika z przedstawionych relacji pomiędzy poszczególnymi elementami systemu oraz przepływów informacji pomiędzy nimi, istnienie centrum koordynacyjnego zapewnia płynną wymianę informacji pomiędzy zainteresowanymi podmiotami, a także koordynację zamierzonych przedsięwzięć.

6.3 Rozpoznanie sytuacji zagrożeń

Proces rozpoznania w systemie zarządzania zasobami informacyjnymi w obszarze przeciwdziałania terroryzmowi stanowi punkt wejścia do systemu. To dzięki działaniom operacyjno – rozpoznawczym system jest zasilany w informacje, które na dalszych etapach funkcjonowania systemu posłużą pogłębianiu wiedzy

Rozpoznanie w systemie przeciwdziałania terroryzmowi służy realizacji celów prewencyjnych, opisanych we wstępnej części pracy. Dla realizacji tych celów konieczne jest gromadzenie informacji dotyczących kilku podstawowych obszarów tematycznych.

Tab. 16: Obszary prowadzenia rozpoznania antyterrorystycznego

RODZAJ ROZPOZNAWANEJ SYTUACJI	SZCZEGÓŁOWE GROMADZONE INFORMACJE dot.:
Informacje o planowanych zamachach	– o celu zamachu, – o potencjalnym sprawcy, – o planowanym sposobie ataku,

	– o środkach, które mają zostać użyte, – o motywie ataku, – o planowanym czasie dokonania zamachu
Informacje o sposobach działania organizacji terrorystycznych	– strategii organizacji terrorystycznych, – taktyce działań organizacji terrorystycznych, – zamachach przeprowadzonych wcześniej przez organizację, – zamachach udaremnionych (planowanym celu, metodach etc.), – metodach przeprowadzania ataków stosowanych przez organizacje terrorystyczne;
Informacje o funkcjonowaniu organizacji terrorystycznych	– nazwach i aliasach nazw organizacji terrorystycznych, – programie ideologicznym (informacje i ostrzeżenia autorstwa kierownictwa organizacji oraz manifesty ideologiczne organizacji), – współpracy z innymi organizacjami terrorystycznymi, – rejonie funkcjonowania organizacji terrorystycznych, – kierownictwie i członkach organizacji terrorystycznych (ustalone), – osobach podejrzewanych o przynależność do organizacji terrorystycznej, – strukturach partyjnych (legalnych, politycznych odłamach organizacji), – zapleczu logistycznym organizacji terrorystycznych, – finansowaniu organizacji terrorystycznych (sponsoring państwowy, działalność kryminalna organizacji, działalność legalna – np. charytatywna organizacji)
Informacje o poszczególnych członkach organizacji terrorystycznych	– dane personalne, – dane dotyczące używanych personaliów (fałszywe dokumenty), – używane pseudonimy, – kontakty osobowe, – wykształcenie, umiejętności, – dane dotyczące preferencji seksualnych, – dane dotyczące wyznawanej religii, – nawyki, – choroby, – dane dot. karalności, – dane dot. pojawiania się w aktach dotyczących spraw kryminalnych (szczególnie zamachów terrorystycznych), – dane dot. członków rodziny.

Źródło: opracowanie własne

Aby w sposób precyzyjny określić sposób funkcjonowania podsystemu rozpoznania w systemie zarządzania zasobami informacji należy przedstawić listę podmiotów, które realizują zadania w dziedzinie rozpoznania oraz zadania, które w tym zakresie nakładają na nie prawo i wewnętrzne uregulowania organizacyjne.

Wśród podmiotów realizujących zadania w zakresie rozpoznania w obszarze przeciwdziałania terroryzmowi wyróżnić można podmioty, które wskazane zostały jako realizujące zadania w zakresie przeciwdziałania terroryzmowi we wcześniejszej części tego rozdziału. Realizowane w tym celu czynności polegają w szczególności na:

- uzyskiwaniu, gromadzeniu, przetwarzaniu i sprawdzaniu w sposób jawny i niejawny informacji o potencjalnych zagrożeniach we wszystkich ich aspektach,
- uzyskiwaniu dokumentacji, próbek i materiałów porównawczych w celu ujawnienia lub zabezpieczenia dowodów przestępstwa[203].

Realizując swoje zadania w zakresie działań operacyjno – rozpoznawczych, wymienione podmioty posługują się następującymi metodami[204]:

2. rozpoznanie osobowe – może być prowadzone w postaci zakonspirowanych działań wywiadowczych, fizycznego penetrowania obszaru, który wymaga rozpoznania; może zostać podzielona na:
   a. rozpoznanie agenturalne,
   b. rozpoznanie patrolowe,
   c. rozpoznanie specjalne;
3. rozpoznanie techniczne – przy użyciu systemów wykorzystujących środki techniczne, które rejestrować mogą dowolne zjawiska fizyczne; można je podzielić na:
   a. rozpoznanie radiowe,
   b. rozpoznanie radiolokacyjne, rozpoznanie optoelektroniczne,
   c. rozpoznanie informatyczne.

---

[203] Opracowanie własne na podstawie: Zalewski S., *Służby specjalne w państwie demokratycznym*, Warszawa 2002, AON, s 58 i dalsze oraz poselskiego projektu ustawy o metodach operacyjno- rozpoznawczych, tekst dostępny na stronie Sejmu RP o adresie [http://orka.sejm.gov.pl/Druki6ka.nsf/wgdruku/353].

[204] *Systemy informacji geoprzestrzennej a budowa przewagi informacyjnej w sferze bezpieczeństwa państwa*, op. cit., s. 171.

Wśród form czynności operacyjno – rozpoznawczych wyróżnić można natomiast:

1. sprawdzenie – weryfikacja jednostkowej informacji,
2. rozpoznanie – uzyskanie, gromadzenie i sprawdzanie informacji,
3. rozpracowanie – zespół czynności operacyjno – rozpoznawczych prowadzonych wobec danego podmiotu w sytuacji zaistnienia podejrzenia usiłowania lub dokonania przestępstwa,
4. poszukiwanie – zespół czynności, którego celem jest zatrzymanie lub ustalenie miejsca pobytu osoby objętej zainteresowaniem danej służby.

6.4 Analiza informacji w systemie przeciwdziałania Terroryzmowi

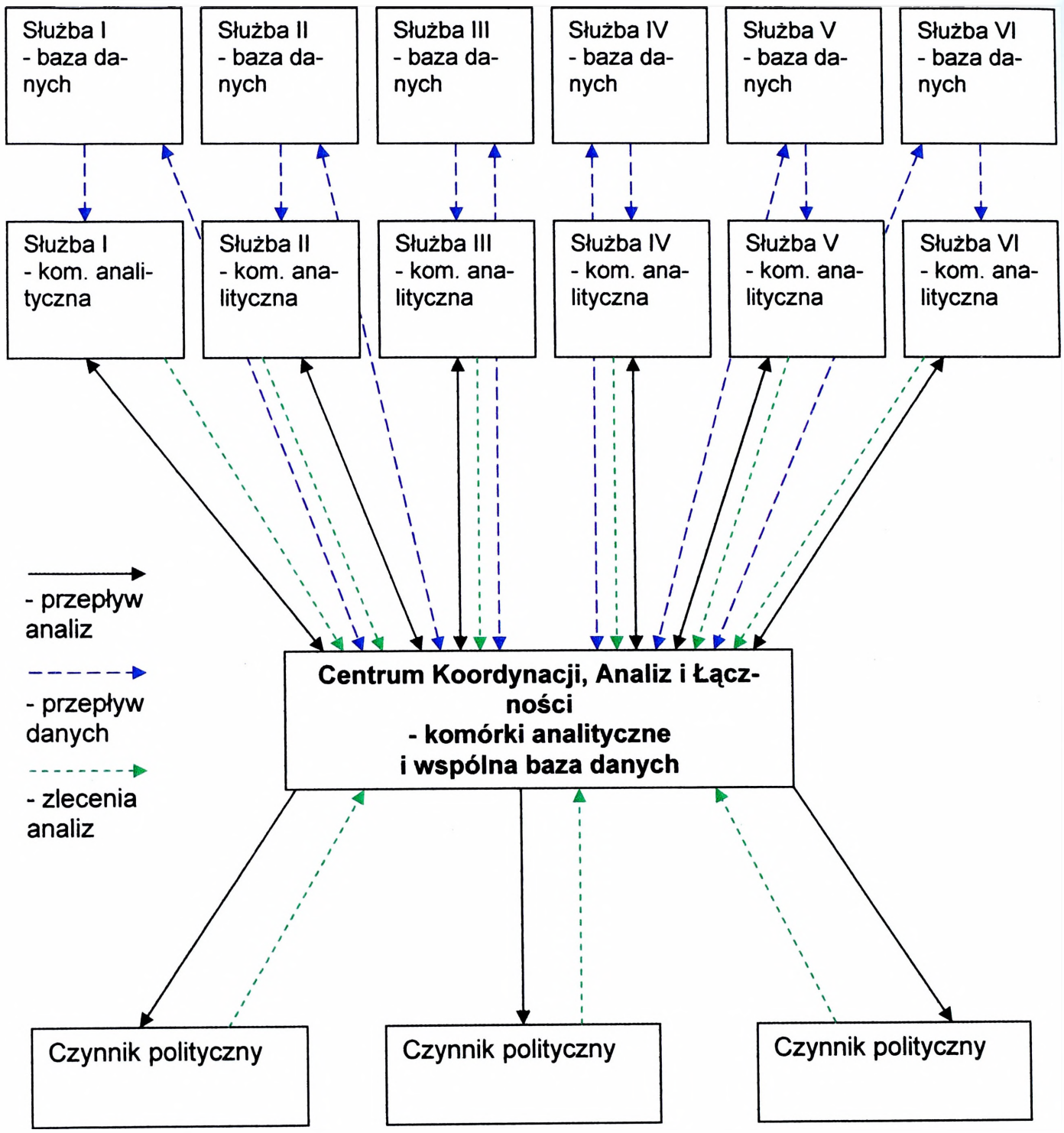
Analiza informacji służy budowaniu obrazu całości na podstawie odrębnych fragmentów, interpretacji dostępnych danych, a także wyciągania wniosków, tworzenia prognoz oraz scenariuszy rozwoju wydarzeń.

Bez analizy informacji nawet najobszerniejszy zbiór danych na temat potencjalnego zagrożenia będzie bezużyteczny, ze względu na brak możliwości zbudowania obrazu sytuacji na podstawie wycinkowych informacji. Zaś bez obrazu sytuacji, pozwalającego na kompleksowy ogląd zarówno sytuacji bieżącej, jak i istniejących trendów i potencjalnych możliwości rozwoju wydarzeń, niemożliwe jest planowanie działań w zakresie przeciwdziałania terroryzmowi. Dlatego niezmiernie istotnym elementem systemu informacyjnego w obszarze przeciwdziałania terroryzmowi jest element analityczny.

Na potrzeby systemu informacyjnego, którego uczestnikami są zasadniczo podmioty funkcjonujące na trzech podstawowych poziomach:

- operacyjnym – służby odpowiedzialne za bezpieczeństwo państwa,
- koordynacyjnym – centrum koordynacyjne,
- strategiczno-decyzyjnym – czynniki polityczne,

celowym wydaje się zaprojektowanie modelu systemu analitycznego, który będzie modelem wielopoziomowym.



Rys. 30: Model struktur analitycznych w systemie przeciwdziałania terroryzmowi[205]
Źródło: opracowanie własne

Przedstawiony powyżej diagram stanowi zarys przepływów analiz, danych służących ich przygotowaniu oraz zleceń analiz. Warto w tym wypadku podkreślić, wobec złożoności diagramu, kierunki przepływów pomiędzy poszczególnymi elementami systemu:

– przepływy danych odbywają się:

[205] Patrz przypis nr 200, s. 203 oraz 201, s. 204.

- z baz danych służb do komórek analitycznych służb,
- z baz danych służb do baz danych centrum,
- z bazy danych centrum do baz danych służb (w wypadku skierowania odpowiedniej kwerendy do centralnej bazy danych),

– przepływy analiz odbywają się:
- z komórek analitycznych służb do komórek analitycznych centrum,
- z komórek analitycznych centrum do komórek analitycznych służb (w wypadku skierowania przez służby zapotrzebowania na analizę w określonym zakresie),
- z komórek analitycznych centrum do czynników politycznych;

a. przepływy zleceń analiz odbywają się:
- od czynników politycznych do komórek analitycznych centrum,
- od komórek analitycznych służb do komórek analitycznych centrum.

6.5 Przechowywanie – bazy danych

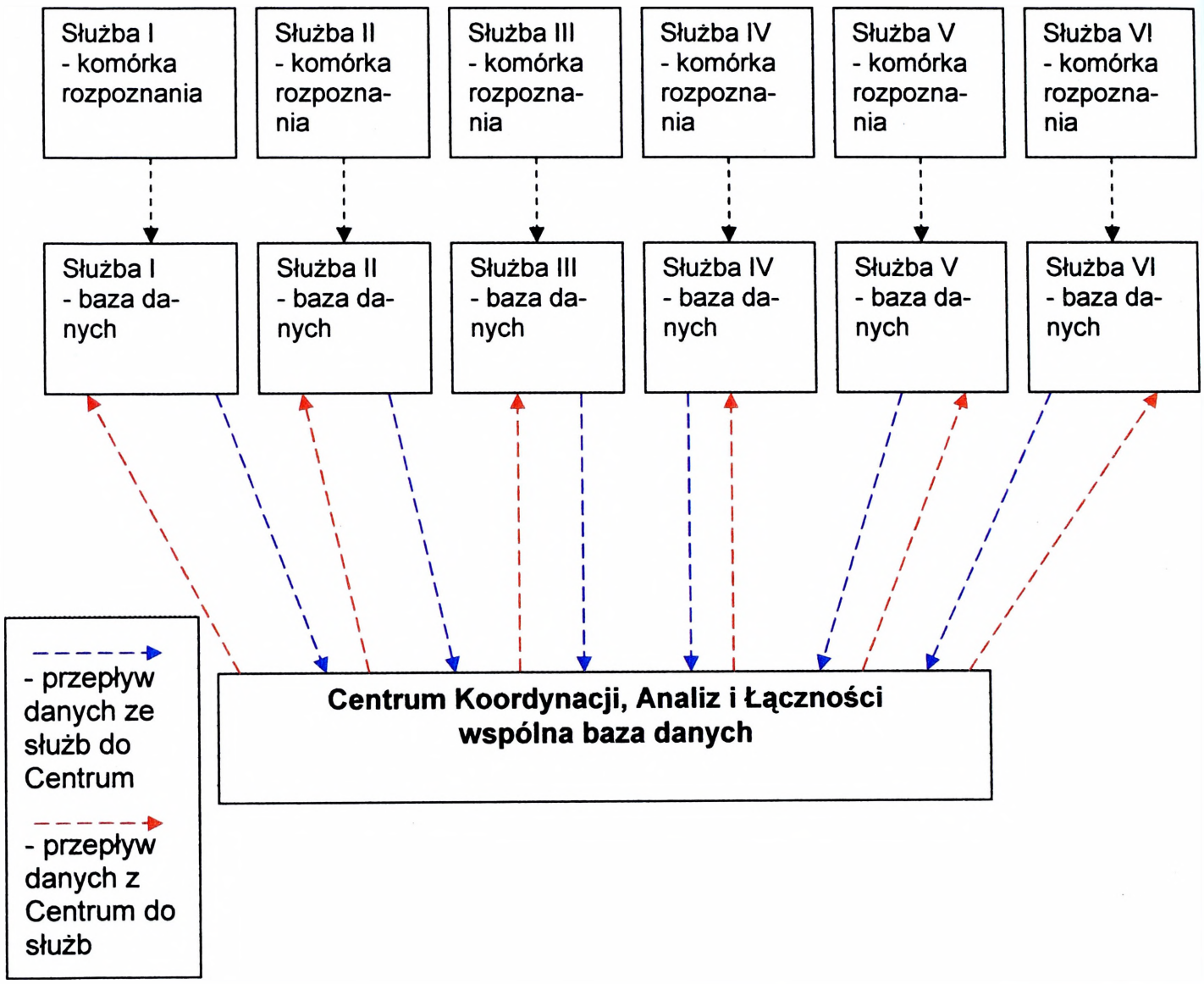
W celu przechowywania informacji gromadzonych w systemie przeciwdziałania terroryzmowi konieczne jest stworzenie baz danych, które spełniać będą określone warunki:

– zapewnią odpowiednią ochronę zgromadzonych informacji,
– zapewnią stosowny, efektywny dostęp do informacji podmiotom, które są do tego upoważnione,
– zapewnią możliwość bezpiecznej obróbki zgromadzonych danych.

Zgromadzenie w jednym miejscu informacji dotyczących przeciwdziałania terroryzmowi pozwala na stworzenie jednego źródła, dzięki któremu zainteresowane podmioty odpowiedzialne za przeciwdziałanie terroryzmowi uzyskują dostęp do kompleksowych informacji zgromadzonych przez Centrum koordynacyjne.

Dane w systemie przechowywania informacji powinny być przekazywane i gromadzone w formie elektronicznej, co gwarantuje sprawny przepływ danych i stwarza możliwość wymiany informacji w czasie rzeczywistym.

Podmioty uprawnione do włączania informacji do bazy danych, ale także do otrzymywania tych informacji z bazy obejmować powinny wszystkie instytucje realizujące działania w zakresie przeciwdziałania terroryzmowi na poziomie operacyjnym i analitycznych, wymienione w części dotyczącej koordynacji systemu.



Rys. 31: Przepływ danych pomiędzy bazami danych służb i Centrum Koordynacji, Analiz i Łączności[206]
Źródło: opracowanie własne

Omawiając kwestie przechowywania danych w systemie zarządzania zasobami informacyjnymi w zakresie przeciwdziałania terroryzmowi, a także przepływów tych informacji pomiędzy bazami danych trzeba zwrócić uwagę na kilka podstawowych procesów, zachodzących w tym obszarze.

Pierwszym z nich jest wprowadzanie informacji do baz danych poszczególnych instytucji i służb odpowiedzialnych za przeciwdziałanie terroryzmowi. Zbieranie in-

[206] Patrz przypis nr 201, s. 204.

formacji przez poszczególne podmioty odbywać się może na drodze prowadzenia czynności operacyjno – rozpoznawczych, ale także poprzez gromadzenie informacji dostępnych ogólnie – tzw. „biały wywiad".

Wszelkie informacje przed wprowadzeniem ich do baz danych podlegać powinny weryfikacji w postaci sprawdzenia, bądź w drodze konfrontacji z innymi źródłami, bądź innych czynności pozwalających na potwierdzenie ich wiarygodności.

Każda poszczególna informacja powinna by opisana i zapisana w odpowiednim dokumencie — rejestrze. Poniższa proponowana ,,Matryca źródła i informacji"[207] jest uniwersalną metodą porządkowania danych według wiarygodności źródła i wartości informacji:

Tab. 17: Matryca korelacji wiarygodności źródeł i wartości informacji

Wiarygodność źródła		**Wartość informacji**	
Organa ścigania lub inne sprawdzone źródła oficjalne	**A**	Faktyczna lub potwierdzona	**1**
Źródła znane i dotychczas wiarygodne	**B**	Prawdopodobnie prawdziwa, zgodna z przeszłymi sprawozdaniami	**2**
Źródła znane, ale nie zawsze wiarygodne	**C**	Potencjalnie prawdziwa, brak zgodności z przeszłymi sprawozdaniami	**3**
Wiarygodność źródła jest nieznana i/lub niemożliwa do ustalenia	**D**	Prawdziwość nieznana i nie może być potwierdzona	**4**

Źródło: materiały szkoleniowe FBI

Wśród zadań, które realizować powinna centralna baza danych w systemie przeciwdziałania terroryzmowi (prowadzona przez Centrum Koordynacji, Analiz i Łączności), powinny znaleźć się trzy podstawowe ich kategorie, czyli zadania związane z gromadzeniem, przechowywanie i przekazywaniem uprawnionym podmiotom informacji w celu wykrywania i ścigania sprawców ataków terrorystycznych oraz zapobiegania takim zamachom.

Szczegółowe zadania, które muszą być realizowane w powyższych kategoriach, to między innymi:

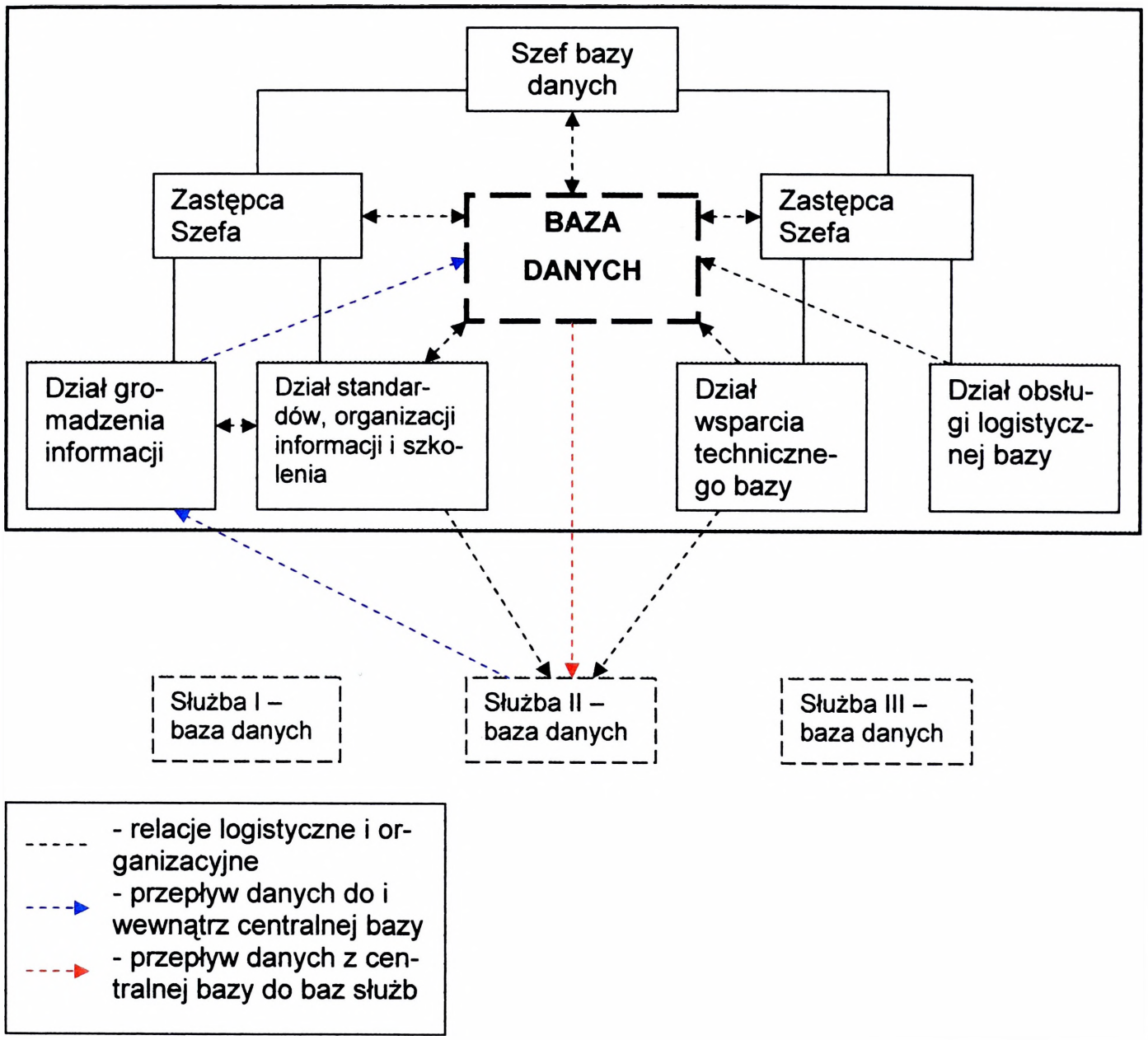
- prowadzenie centralnej bazy danych,
- tworzenie standardów prowadzenia baz danych przez poszczególne służby i instytucje,

[207] Materiały szkoleniowe FBI.

- określanie warunków organizacyjnych oraz technicznych sposobów prowadzenia baz danych,
- określenie standardu (formularza w formie papierowej oraz formularza w formie elektronicznej) przekazywania informacji do baz danych w celu usprawnienia ich wprowadzania do baz i przetwarzania,
- zapewnienie bezpieczeństwa gromadzonym i przetwarzanym informacjom,
- prowadzenie działalności szkoleniowej w zakresie procedur współdziałania z centralną bazą danych dla podmiotów współpracujących.

Centralna baza danych powinna spełniać trzy podstawowe funkcje, aby w pełni realizować swoje zadania w zakresie przeciwdziałania terroryzmowi. Do tych funkcji zaliczyć należy:

- ewidencjonowanie informacji gromadzonych w systemie oraz organizowanie ich w sposób umożliwiający ich efektywne wykorzystanie przez komórki analityczne,
- dystrybuowanie informacji do podmiotów analitycznych informacji w drodze kwerend od podmiotów współpracujących,
- współudział w podsystemie koordynacyjnym poprzez automatyczne generowanie informacji przeznaczonych dla właściciela rejestracji informacji o odczytaniu jej przez inny podmiot lub o jakichkolwiek modyfikacjach dokonanych w jej obszarze.



Rys. 32: Struktura organizacyjna centralnej bazy danych i relacji ze służbami z uwzględnieniem 1 służby[208]

Źródło: opracowanie własne

Jak wskazano na powyższym diagramie ilustrującym strukturę organizacyjną centralnej bazy danych i relacje ze służbami, komórki organizacyjne bazy utrzymują bezpośrednie kontakty nie tylko pomiędzy sobą, ale także z bazami służb.

Służby przekazują dane ze swoich baz bezpośrednio do komórki gromadzenia danych centralnej bazy danych, gdzie poddawane są one wstępnej selekcji i przyporządkowaniu do właściwych obszarów gromadzenia informacji centralnej bazy. Jest to podstawowe zjawisko funkcjonujące pomiędzy służbami i centralną bazą w kierunku „służby -> centralna baza".

[208] Patrz przypis nr 201, s. 204.

Większą ilość przepływów pomiędzy służbami a centralną bazą zidentyfikować można analizując kierunek „centralna baza -> służby":

- przepływ wiedzy w zakresie standardu przekazywania informacji do baz danych w celu usprawnienia ich wprowadzania do baz i przetwarzania z komórki „Dział standardów, organizacji informacji i szkolenia",
- przepływ wiedzy i wsparcia technicznego z komórki „Dział wsparcia technicznego bazy",
- przepływ informacji z centralnej bazy danych do baz służb.

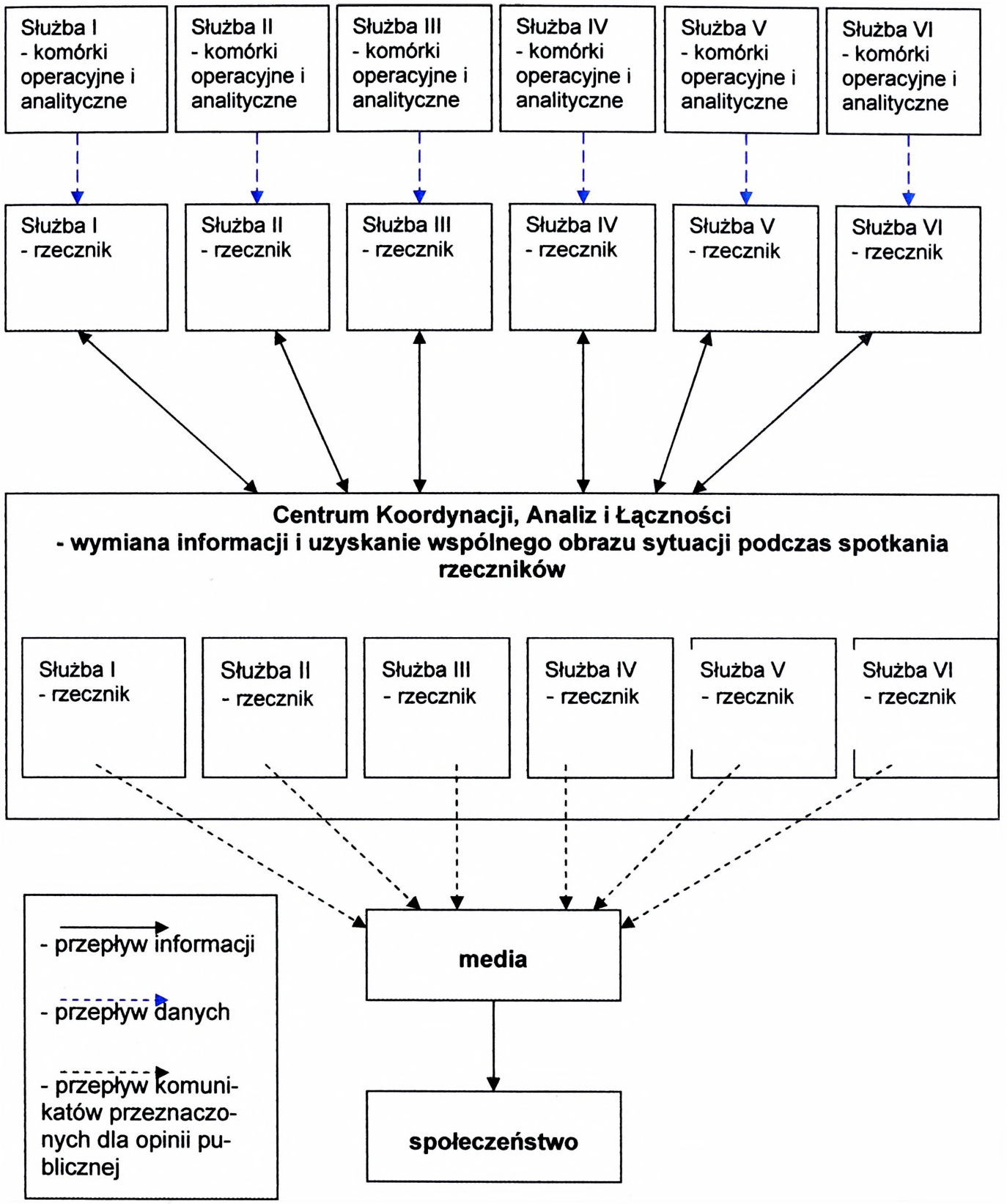
Szczególnego wyjaśnienia wymaga ten ostatni punkt. Otóż informacje przekazywane są z centralnej bazy danych do baz danych służb w sytuacji, w której dana służba do wykonania swoich zadań potrzebuje wsparcia informacyjnego od innych służb. Ze względu na to, że wszystkie służby kierują dane do centralnej bazy danych, w wypadku skierowania do niej kwerendy dotyczące konkretnej kwestii, służba uzyska z centralnej bazy danych kompleksową informację na zadany temat.

6.6 Komunikacja ze społeczeństwem i media w systemie przeciwdziałania terroryzmowi

Terroryzm jako zjawisko, które narusza podstawy funkcjonowania współczesnych państwa wywiera szczególny wpływ zwłaszcza w wymiarze politycznym.

Dlatego ważne jest stworzenie systemu efektywnej komunikacji społecznej, a tym samym powołanie instytucji odpowiedzialnych za komunikację pomiędzy rządem a społeczeństwem. Jej podstawowym zadaniem powinno być zapewnianie istnienia forum wymiany informacji pomiędzy komórkami prasowymi poszczególnych służb i instytucji podczas potencjalnej sytuacji kryzysowej. Umożliwia to tworzenie tak zwanego „wspólnego obrazu sytuacji". Dzięki funkcjonowaniu takiego mechanizmu społeczeństwo otrzymuje ze strony instytucji rządowych spójny komunikat.

Wymaga to doprowadzenia do powstania takiej platformy porozumienia dla komórek odpowiedzialnych za kontakty z mediami, która umożliwi ich spotkanie, uzgodnienie – poprzez wymianę informacji – wspólnego obrazu sytuacji. Platforma ta powinna zarazem zapewnić, że polityka medialna i strategia komunikacyjne każdej z kontaktujących się z mediami instytucji i służb nie będzie sprzeczna ze strategią rządową i strategiami pozostałych służb i instytucji.



Rys. 33: Koordynacja komunikacji społecznej i kontaktów z mediami[209]
Źródło: opracowanie własne.

[209] Patrz przypis nr 201, s. 204.

W sytuacji zagrożenia niewłaściwie zorganizowana komunikacja społeczna może wyrządzić olbrzymie szkody. Podważenie zaufania społecznego do instytucji rządowych poprzez publikowanie sprzecznych informacji może być nie do naprawienia. Podobne szkody mogą zostać wyrządzone w wyniku prasowych i telewizyjnych spekulacji na temat przyczyn kryzysu oraz przyszłego rozwoju wypadków. Znacznie lepszym rozwiązaniem jest otwarta komunikacja ze społeczeństwem, a nawet poinformowanie o niepełnym stanie wiedzy na temat poszczególnych kwestii związanych z kryzysem, niż milczące przyzwolenie na kumulowanie się niepotwierdzonych informacji, które mogą powodować niepotrzebne niepokoje społeczne, a nawet panikę.

Aby budować poprawne stosunki z mediami trzeba – w miarę możliwości – włączać ich przedstawicieli w proces ćwiczeń i przygotowań na wypadek kryzysu. Nie tylko pomoże to we współpracy podczas kryzysu, ale może także powstrzymać zaangażowane media przed krytyką wszystkich poczynań władz, której część płynie z nieznajomości warunków i wymogów stawianych przez sytuację kryzysową, a część z realizacji podstawowego celu mediów, to jest dążenia do znalezienia nośnego tematu wiadomości.

Dlatego od rządu i służb oraz instytucji mu podległych, dla efektywnego funkcjonowania komunikacyjnego elementu systemu przeciwdziałania terroryzmowi, wymagany być powinien odpowiedni dobór osób, które z ramienia powyższych podmiotów z mediami współpracują. Osoby te powinny nie tylko mieć świadomość roli, jaką media mogą odegrać w zarządzaniu kryzysem, ale też być odpowiednio przygotowane do nawiązania z nimi współpracy w pożądanym zakresie. Przygotowanie to obejmować powinno co najmniej świadomość kilku podstawowych zasad, które rządzą kreowaniem poprawnych stosunków z mediami. Wśród najważniejszych z tych zasad wymienić należy:

- poznanie zasad, które obowiązują w świecie mediów i przestrzeganie ich tak dalece, jak pozwalają na to przepisy prawa i wymogi troski o bezpieczeństwo państwa i jego obywateli,
- odbycie stosownych szkoleń w zakresie komunikacji społecznej i stosunków z mediami,
- organizowanie regularnych spotkań w przedstawicielami mediów,
- przygotowanie i wykorzystywanie stosownych narzędzi współpracy z mediami, tj. listy kontaktów, baz danych o mediach i ich reprezentantach,

- nawiązywanie i podtrzymywanie kontaktów z przedstawicielami mediów,
- wyciąganie wniosków ze współpracy z mediami i wdrażanie ich do systemu komunikacji medialnej.[210]

Jak pokazuje przytoczona powyżej lista wymagań, których spełnienie konieczne jest dla zbudowania poprawnego systemu komunikacji społecznej – w tym z wykorzystaniem pośrednictwa mediów – właściwa organizacja tego komponentu systemu przeciwdziałania terroryzmowi może być niezwykle wymagającym zadaniem. Konieczne jest jednak poświęcenie mu odpowiednich nakładów sił i środków, ponieważ system bezpieczeństwa państwa, również w aspekcie przeciwdziałania terroryzmowi, ma rolę służebną w stosunku do obywateli państwa. Prowadząc zaś prace w tym zakresie wykazać należy szczególną uwagę ze względu na to, że funkcjonowanie – poprawne – tego elementu systemu wymaga współpracy z podmiotami, których funkcjonowanie w sferze publicznej nie podlega rygorom i obostrzeniom nakładanym przez regulaminy i procedury obowiązujące w administracji publicznej.

6.7 Warunki realizacji modelu

Aby możliwe było zrealizowanie wprowadzenia przedstawionego powyżej modelu koordynacji w życie, konieczne jest spełnienie warunków, które stanowią o stworzeniu postaw funkcjonowania całego mechanizmu w rzeczywistości. Warunki te podzielić można na trzy grupy:

- legislacyjne,
- organizacyjne,
- logistyczne.

Wśród warunków legislacyjnych zidentyfikować należy:

- stworzenie aktu prawnego stanowiącego podstawę funkcjonowania centrum koordynacyjnego Centrum Koordynacji, Analiz i Łączności,
- stworzenie aktów prawnych wykonawczych, określających w szczegółach kompetencje Centrum Koordynacji, Analiz i Łączności w odniesieniu do monitorowania planów i wyników prac innych instytucji zaangażowanych w realizację zadań w zakresie przeciwdziałania terroryzmowi,

[210] Patrz także: Jabłoński W., *Kreowanie informacji. Media relations*, Warszawa 2006, PWN, s. 28.

- stworzenie aktów prawnych wykonawczych, stanowiących podstawę przekazywania informacji do i z Centrum Koordynacji, Analiz i Łączności, szczególnie informacji oznaczonych klauzulą niejawności,
- stworzenie podstaw prawnych do ewentualnego delegowania funkcjonariuszy i pracowników innych służb i instytucji do pełnienia zadań w centrum koordynacyjnym (jeśli centrum nie będzie zatrudniać osób na wszystkich stworzonych stanowiskach),
- stworzenie wewnętrznych regulaminów i procedur regulujących funkcjonowanie centrum koordynacyjnego.

W zakresie koniecznych warunków organizacyjnych:

- powołanie struktur organizacyjnych centrum koordynacyjnego,
- stworzenie rozwiązań technicznych na poziomie informatycznym zapewniających możliwość sprawnego i bezpiecznego przekazywania danych i informacji,
- dokonanie rozstrzygnięć co do zasobów ludzkich centrum koordynacyjnego, tj. podjęcie decyzji o tym, czy centrum ma zatrudniać własnych pracowników na wszystkich stanowiskach, czy też część stanowisk ma być obsadzona osobami delegowanymi z innych służb i instytucji

W zakresie koniecznych warunków logistycznych:

- zapewnienie odpowiedniego finansowania centrum koordynacyjnego, zarówno w odniesieniu do zapewnienia pomieszczeń, sprzętu, jak i zatrudnienia (finansowania delegowania) zespołu ludzkiego,
- w razie zaistnienia takiej możliwości wygospodarowanie części zaplecza logistycznego (budynków i sprzętu) z istniejących zasobów administracji publicznej.

ZAKOŃCZENIE

Współczesne systemy bezpieczeństwa budowane przez rządy oraz organizacje międzynarodowe spełniają istotną rolę w zakresie nie tylko bezpośredniej dbałości o bezpieczeństwo państwa i jego obywateli i porządek publiczny, ale także w podtrzymywaniu obowiązującego ładu wewnętrznego i międzynarodowego. Terroryzm, jako zagrożenie, które rozpatrywane być może w stosunku do wszystkich powyższych wartości, powinien być przedmiotem intensywny działań wszystkich podmiotów, w zakresie kompetencji których pozostaje dbałość o nie.

Ze względu na cechy tego zagrożenia, a także istotne jego konsekwencje, zapobieganie mu pozostaje najefektywniejszym środkiem przeciwdziałania zagrożeniom terrorystycznym. W celu optymalnej realizacji tego zadania konieczne jest zatem tworzenie takich systemów przeciwdziałania terroryzmowi, które zapewnią warunki skutecznej realizacji działań i wykonywania zadań mających na celu ochronę państw przed zagrożeniem terrorystycznym.

Przeprowadzone na bazie teoretycznej – modelowania systemowego, a także na bazie obserwacji i analizy praktycznych rozwiązań stosowanych w rożnych narodowych systemach przeciwdziałania terroryzmowi badania pozwalają stwierdzić, że najważniejszym elementem efektywnego systemu jest element koordynacji.

Koordynacja w systemie przeciwdziałania terroryzmowi nie istnieje bez sprawnego systemu zarządzania zasobami informacyjnymi. Przedstawiony w praco model oparty został o kanony organizacyjne rządzące systemami wymiany informacji obowiązujące na świecie, a także zapewniające sprawną komunikację na wszystkich poziomach systemu przeciwdziałania terroryzmowi. Rozwiązanie to, zastosowane zgodnie z zaprezentowanym modelem, zapewni nie tylko sprawną wymianę informacji, ale także właściwą koordynację działań w systemie przeciwdziałania terroryzmowi. Zabezpieczony zgodnie z przedstawionym systemem ochrony informacji, system pozwoli także na ochronę informacji wrażliwych z punktu widzenia państwa.

Stworzenie modelu spełniającego powyższe wymagania pozwala na stwierdzenie, że cel pracy, tj. opracowanie modelu systemu zarządzania zasobami informacyjnymi gromadzonymi w procesie rozpoznania zagrożeń o charakterze terrorystycznym w sytuacji zagrożenia bezpieczeństwa państwa przez terroryzm został zrealizowany.

Cele szczegółowe pracy, tj.:

- określenie wpływu zasobów informacyjnych na kształtowanie strategii państwa w przeciwdziałaniu terroryzmowi,
- określenie elementów, procedur i relacji stanowiących części składowe systemu zarządzania informacją w odniesieniu do instytucji i służb odpowiedzialnych za przeciwdziałanie terroryzmowi w państwie,
- dokonanie analizy rozwiązań stosowanych w powyższym zakresie w innych państwach

zrealizowane zostały w poszczególnych etapach rozwiązywania problemów badawczych.

Literatura

PUBLIKACJE ZWARTE

1. Aldiss Anne, Herd Greame P. (ed.), *The Ideological War on Terror. Worldwide strategies for counter-terrorism*, Routledge, London and New York 2007.
2. Aleksandrowicz Tomasz, *Analiza informacji w administracji i w biznesie*, WS-HiP, Warszawa 1999.
3. Alexander Yonah, Hoenig Milton, *Superterroryzm biologiczny, chemiczny i nuklearny*; Dom Wydawniczy Bellona; Warszawa 2001.
4. Bączek Piotr, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006.
5. Baker Stewart, Kavanagh John (ed.), *Patriot Debates. Experts Debate the USA Patriot Act*, ABA, Chicago 2005.
6. Barcik Jacek, *Akt terrorystyczny i jego sprawca w świetle prawa międzynarodowego i wewnętrznego*, AON, Warszawa 2004.
7. Berman Czesław, *Informacja i aspekty komunikacji*, „Zagadnienia Nauko-znawstwa", nr 3-4, 1991.
8. Białas Andrzej, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wyd. Naukowo-Techniczne, Warszawa 2006.
9. Białek Tomasz, *Terroryzm manipulacja strachem*; Studio Emka; Warszawa 2005.
10. Bieleń Stanisław (red.), *Prawo w stosunkach międzynarodowych. Wybór dokumentów*, Wydawnictwo Uniwersytetu Warszawskiego, Warszawa 1998.
11. Bobrow Davis B., Haliżak Edward, Zięba Ryszard, red. nauk., *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, Fundacja Studiów Międzynarodowych, Warszawa 1997.
12. Bolechów Bartosz, *Terroryzm w świecie podwubiegunowym*, Wydawnictwo Adam Marszałek; Toruń 2004.
13. Borkowski Robert, *Terroryzm ponowoczesny. Studium z antropologii polityki*, Wydawnictwo Adam Marszałek; Toruń 2006.
14. Borowiecki Ryszard, Romanowska Maria (red.), *System informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa*, Warszawa 2001
15. Cieślarczyk Marian, Dębska Anna (red. nauk.), *Wojsko wobec wyzwań współczesnego świata*, Akademia Obrony Narodowej - Wydział Wydawniczy; Warszawa 2005.
16. Ciupiński Andrzej, Malak Kazimierz (red. i oprac.), *Bezpieczeństwo polityczne i wojskowe*, Akademia Obrony Narodowej, Warszawa 2004.
17. Cronin, Audrey Kurth, Ludes James M. (red.), *Attacking Terrorism. Elements of a GRAND Strategy,* Georgetown UP., Washington, D.C. 2004.
18. Czaja Stanisław, Tyszkiewicz Elżbieta, *Unia Europejska, NATO a bezpieczeństwo Polski*, Bellona, Warszawa 2000.

19. Czekaj Jacek, *Metody zarządzania informacją w przedsiębiorstwie*, Kraków 2000
20. Dawidczyk Andrzej, Gryz Jarosław, Koziej Stanisław, *Zarządzanie strategiczne bezpieczeństwem: teoria, praktyka, dydaktyka,* Wydawnictwo Wyższej Szkoły Humanistyczno-Ekonomicznej, Łódź 2006.
21. Dębski Sławomir, Górka-Winter Beata, red., *Kryteria bezpieczeństwa międzynarodowego państwa*, Polski Instytut Spraw Międzynarodowych , Warszawa 2003.
22. Dobek-Ostrowska Bogusława, Kuś Michał (red.), *Hiszpania: media masowe i wybory w obliczu terroryzmu,* Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2007.
23. Dziuba Dariusz Tadeusz, *Gospodarki nasycone informacją i wiedzą*, Warszawa 2000.
24. *Encyklopedia szpiegostwa*, Wyd. SPAR, Warszawa 1995.
25. Ethiel Nancy (ed.), *Terrorism: Informing the Public,* McCormick Foundation, Chicago, Illinois 2002.
26. Fehler Włodzimierz, Tymanowski Józef (red.), *Międzynarodowe i wewnętrzne aspekty członkostwa Polski w NATO*, Wyd. Adam Marszałek, Toruń 2001.
27. Feler Włodzimierz (red. nauk.), *Współczesne bezpieczeństwo*, Wydaw. Adam; Marszałek, Toruń 2003.
28. Flis Józef, Jakubczak Ryszard (red. nauk.), *Bezpieczeństwo narodowe Polski w XXI wieku*, Dom Wydawniczy Bellona, Warszawa 2006.
29. Goban-Klas T., *Media i komunikowanie masowe – teoria i analizy prasy, radia, telewizji i Internetu*. Warszawa, 2004.
30. Goban-Klas Tomasz, Sienkiewicz Piotr, *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999.
31. Górski Adam, Sakowicz Andrzej, *Zwalczanie przestępczości w Unii Europejskiej: współpraca sądowa i policyjna w sprawach karnych*, Lexis-Nexis, Warszawa 2006.
32. Gryz Jarosław, *System zarządzania kryzysowego*, Wyd. Adam Marszałek, Toruń 2007.
33. Haber Lesław *Społeczeństwo informacyjne. Wizja czy rzeczywistość?* (red), wyd. Uczelniane Wydawnictwa Naukowo–Dydaktyczne, Kraków, 2004.
34. Haber Lesław, *Od robotnika do internauty – w kierunku społeczeństwa informacyjnego*. AGH, Kraków, 2008.
35. Haliżak Edward (red.), *Bezpieczeństwo narodowe Polski: geopolityczne i geoekonomiczne uwarunkowania - materiały z Konferencji Polskiego Towarzystwa Nauk Politycznych*, Rembertów k. Warszawy, 22-23 października 1994 r., Wydaw. Adam Marszałek, Toruń 1995.
36. Haliżak Edward i Tabor Marek (red.), *Polska w środowisku międzynarodowym: problemy współzależności* - praca zbiorowa, Dom Wydawniczy i Handlowy "Elipsa", Warszawa 1993.

37. Hanausek Tadeusz, *Kryminalistyka. Zarys wykładu*, Zakamycze, Kraków 2005.
38. Hoc Stanisław, *Zagadnienia odpowiedzialności karnej za szpiegostwo*, Akademia Spraw Wewnętrznych, Warszawa 1985
39. Hoffman Bruce, *Oblicza terroryzmu*, Politeja, Warszawa 1999.
40. Hołyst Brunon, *Kryminologia*, LexisNexis, Warszawa 2000.
41. Hołyst Brunon, *Terroryzm*, LexisNexis, Warszawa 2009.
42. Horgan John, *Psychologia terroryzmu*, PWN, Warszawa 2008.
43. Horgan John, *The Psychology of Terrorism*, Routledge, London and New York 2005.
44. Howard Russell D., Sawyer Reid L (ed.), *Defeating Terrorism: Shaping the New Security Environment,* The McGrawHill Companies, Guilford 2004.
45. Howard Russell D., Sawyer Reid L. (ed.), *Terrorism and Counterterrorism. Understanding the New Security Environment*, The McGrawHill Companies, Guilford 2005.
46. Indecki Krzysztof (red.), *Przestępczość terrorystyczna*; Wydawnictwo WiS; Poznań 2006.
47. Jabłoński W., *Kreowanie informacji. Media relations*, PWN, Warszawa 2006.
48. Jakubczak Ryszard, Flis Józef, *Bezpieczeństwo narodowe Polski w XXI wieku*, Bellona, Warszawa 2006.
49. Jakubczak Ryszard, Skrabacz Aleksandra, *Społeczeństwo w tworzeniu bezpieczeństwa narodowego Polski w XXI wieku*, Wydawnictwo Akademii Podlaskiej, Siedlce 2006.
50. Jałoszyński Kuba, *Koncepcja współczesnych działań antyterrorystycznych*, Akademia Obrony Narodowej, Warszawa 2003.
51. Jałoszyński Kuba, *Terroryzm antyizraelski : przedsięwzięcia kontrterrorystyczne w Izraelu*, Wydawnictwo Adam Marszałek, Toruń 2006.
52. Jałoszyński Kuba, *Terroryzm czy terror kryminalny w Polsce?*, AON, Warszawa 2001.
53. Jałoszyński Kuba, *Terroryzm i walka z nim we współczesnym świecie*, Centrum Szkolenia Policji, Legionowo 2002.
54. Jałoszyński Kuba, Wiśniewski Bernard, *Terroryzm. Diagnoza, zadania administracji publicznej w przeciwdziałaniu zjawisku*, Wyższa Szkoła Administracji Bielsko-Biała, Bielsko-Biała 2007.
55. Jałoszyński Kuba, *Współczesny wymiar antyterroryzmu*, Wydawnicwto TRIO, Warszawa 2008.
56. Janczak Józef, Świdzikowski Grzegorz, *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*, AON - Warszawa 2004.
57. *Jednostka i społeczeństwo wobec zagrożeń terroryzmem*, Biuro Informacji Rady Europy; Warszawa 2002.

58. Jemioło Tadeusz, Malak Kazimierz, *Bezpieczeństwo zewnętrzne Rzeczypospolitej Polskiej*, AON Warszawa 2002.

59. Kaczmarek Waldemar, *Natarcie związku taktycznego*, rozprawa habilitacyjna, „Zeszyty Naukowe AON" 1997, nr 4(29), dodatek do nr 4.

60. Kahn Herman, Mann Irwin, *Techniques of Systems Analysis,* Rand, Santa Monica 1956.

61. Kamiński Antoni Z., *Raport o stanie bezpieczeństwa państwa: aspekty zewnętrzne*, Polski Instytut Spraw Międzynarodowych, Warszawa 1995.

62. Kisielnicki Jerzy, *Kryteria jakości systemów informatycznych funkcjonujących w gospodarce narodowej*, „Systemy informatyczne", 1987, nr

63. Kitowski Zygmunt, Lisowski Józef (red. nauk.), *Perspektywy i rozwój systemów ratownictwa, bezpieczeństwa i obronności w XXI wieku*, Akademia Marynarki Wojennej, Gdynia 2004.

64. Knopka Jacek, Mierzejewski Donat Jerzy (red.), *Bezpieczeństwo narodowe i regionalne w procesach globalizacji*, Państwowa Wyższa Szkoła Zawodowa im. Stanisława Staszica w Pile, Piła 2006.

65. Kowalczyk Krzysztof, Wróblewski Wiesław, *Terroryzm: globalne wyzwanie*, Centrum Szkolenia Policji, Legionowo 2002

66. Koziej Stanisław, *Bezpieczeństwo narodowe i obronność Rzeczypospolitej Polskiej*, Wydaw. Adam Marszałek, Toruń 1996.

67. Koziej Stanisław, *Między piekłem a rajem: szare bezpieczeństwo na progu XXI wieku*, Wydaw. Adam Marszałek, Toruń 2006.

68. Koziej Stanisław, *Polska doktryna obronna i jej modyfikacja w obliczu integracji z NATO*, Wydaw. Adam Marszałek, Toruń 1996.

69. Koziej Stanisław, *Szkic do dyskusji o przyszłej strategii poszerzonego NATO: spojrzenie z polskiej perspektywy*, Wydaw. Adam Marszałek, Toruń 1998.

70. Koziej Stanisław, *Tezy i komentarze do prac nad strategią bezpieczeństwa i obronności Rzeczypospolitej Polskiej*, Wydaw. Adam Marszałek, Toruń 1998.

71. Koziej Stanisław, *Współczesne problemy bezpieczeństwa międzynarodowego i narodowego: studium analityczne*, Wydaw. Biura Badań Strategicznych Prywatnej Wyższej Szkoły Businessu i Administracji, Warszawa 2003.

72. Kuźniar Roman, *Polityka i siła: studia strategiczne. Zarys problematyki*, Wydawnictwo Scholar, Warszawa 2005.

73. Kuźniar Roman, Zdzisław Lachowski, red., *Bezpieczeństwo międzynarodowe czasu przemian. Zagrożenia – Koncepcje – Instytucje*, Polski Instytut Spraw Międzynarodowych, Warszawa 2003.

74. Kwećka Roman, *Informacja w walce zbrojnej*, AON, Warszawa 2001.

75. Kwećka Roman, *Siły specjalne w kontekście współczesnych zagrożeń*, AON Wydział Wydawniczy, Warszaw 2002.

76. Lankosza Kazimierz, Chorośnicki Michał, Czubik Paweł, *Walka z terroryzmem w świetle prawa międzynarodowego*, Wydawnictwo STO, Bielsko – Biała 2004.

77. Laqueur Walter (ed.), *Voices of Terror. Manifestos, writings, and manuals of Al Qaeda, Hamas, and other terrorists from around the world and throughout the ages*, Reed Press, New York 2004.
78. Libicki Martin C., Chalk Peter, Melanie Sisson W., *Exploring Terrorist Targeting Preferences*, RAND 2007.
79. Liedel Krzysztof (red. nauk.), *Terroryzm - anatomia zjawiska*, Wyd. Naukowe Scholar – Collegium Civitas Press, Warszawa 2006.
80. Liedel Krzysztof, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa państwa*, Wyd. Adam Marszałek, Warszawa 2004.
81. Liedel Krzysztof, *EURO 2012: Mistrzostwa Europy w cieniu terroryzmu*, Collegium Civitas Press, Warszawa 2007.
82. Liedel Krzysztof, Marszałek-Kawa Joanna, Wudarski Szymon (red.); *Polityczne metody zwalczania terroryzmu*; Wydawnictwo Adam Marszałek, Toruń 2006.
83. Liedel Krzysztof, Piasecka Paulina, *Jak przetrwać w dobie zagrożeń terrorystycznych? Elementy edukacji antyterrorystycznej*, Wydawnictwo TRIO, Warszawa 2008.
84. Liedel Krzysztof, Piasecka Paulina, *Współpraca międzynarodowa w zwalczaniu terroryzmu*, Oficyna Wydawniczo-Poligraficzna "Adam", Warszawa 2004.
85. Liedel Krzysztof, Prońko Jarosław, Wiśniewski Bernard, *Administracja publiczna w systemie przeciwdziałania nadzwyczajnym zagrożeniom dla ludzi i środowiska*, Wyższa Szkoła Administracji Bielsko-Biała, Bielsko-Biała Warszawa 2007.
86. Liedel Krzysztof, *Terroryzm – znak naszych czasów*, Oficyna Wydawniczo-Poligraficzna "Adam", Warszawa 2005.
87. Liedel Krzysztof; *Zwalczanie terroryzmu lotniczego: aspekty prawnomiędzynarodowe*; Zakład Wydawnictw i Usług Prawniczych "Jurysta", Warszawa 2003.
88. Machińska Hanna, *Przeciwdziałanie korupcji i zorganizowanej przestępczości*, CEUW, Warszawa 1999.
89. Madej Marek, *Międzynarodowy terroryzm polityczny*, Warszawa 2001.
90. Madej Marek, *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Polski Instytut Spraw Międzynarodowych, Warszawa 2007.
91. Madejski Andrzej, Zieliński Jerzy, *Siły Zbrojne Polski wobec nowych wyzwań*, Polski Instytut Spraw Międzynarodowych, Warszawa 1992.
92. Malec Mieczysław, *Percepcja bezpieczeństwa: definicje, wymiary, paradygmaty*, Ministerstwo Obrony Narodowej - Departament Polityki Obronnej, Warszawa 2006.
93. Malendowski Włodzimierz (red.), *Świat u progu XXI wieku: wybrane problemy*, Wydawnictwo Naukowe Instytutu Nauk Politycznych i Dziennikarstwa Uniwersytetu im. Adama Mickiewicza, Poznań 2003.
94. Maniszewska Katarzyna, *Terroryzm a media*, ATUT, Wrocław 2006.
95. McLuhan Marshall, *Zrozumieć media*. WNT, Warszawa, 2004.

96. Michalski Andrzej (red.), *Zarządzanie informacjami w przedsiębiorstwie*, Gliwice 1999, Wyd. Politechniki Śląskiej.

97. Mioduszewska Grażyna, red., *Strategie bezpieczeństwa narodowego Polski po 1989 roku*. Cz. 1-2, Akademia Dyplomatyczna Ministerstwa Spraw Zagranicznych, Warszawa 2004.

98. Multan Wojciech, *Wizje bezpieczeństwa europejskiego*, Elipsa, Warszawa 1997.

99. Niedźwiedziński M., *Cechy informacji – próba systematyzacji*, „Systemy informatyczne", 1987, nr 1.

100. Nowacki Gabriel (red.), *Informacja w walce zbrojnej: materiały z sympozjum naukowego*, AON, Warszawa 2002.

101. Pacholski Piotr, *Aktywność Polski w zwalczaniu proliferacji broni masowego rażenia i terroryzmu międzynarodowego*, Departament Polityki Obronnej MON, Warszawa 2004.

102. Parzymies Stanisław, Zięba Ryszard, *Instytucjonalizacja wielostronnej współpracy międzynarodowej w Europie*, Wydawnictwo Naukowe Scholar, Warszawa 2004.

103. Patman Robert G., *Globalization and Conflict. National Security in a 'new' strategic era*, Routledge, London and New York 2006.

104. Pawłowska Agnieszka, *Zasoby informacyjne w administracji publicznej w Polsce. Problemy zarządzania*, UMCS, Lublin 2002.

105. Pawłowski Jacek (red.), *Terroryzm we współczesnym świecie*, Bellona, Warszawa 2001.

106. Pawłowski Jacek, *Strategiczne problemy i dylematy we współczesnym świecie*, Wyd. Adam Marszałek, Toruń 2004.

107. Piątek Zbigniew, *Współczesny wymiar terroryzmu*, Akademia Obrony Narodowej, Zielonka 2006.

108. Pikulski Stanisław, *Prawne środki zwalczania terroryzmu*, Olsztyn 2000.

109. Płudowski Tomasz (ed.), *Terrorism. Media. Society*, Wydawnictwo Adam Marszałek i Collegium Civitas, Toruń 2006.

110. Pływaczewski Emil W.; *Przestępczość zorganizowana: świadek koronny, terroryzm w ujęciu praktycznym*; Wolters Kluwer Polska - OFICYNA, 2005.

111. Prońko Jarosław, *Bezpieczeństwo państwa. Zarys teorii problemu i zadań administracji publicznej*, Wyższa Szkoła Administracji, Bielsko-Biała 2007.

112. Quade E. S., Boucher Wayne I. (ed.), *Systems Analysis and Policy Planning. Applications in Defense,* Rand, Santa Monica 1968.

113. Rotfeld Adam Daniel, *Europejski system bezpieczeństwa in statu nascendi*, Polski Instytut Spraw Międzynarodowych, Warszawa 1990.

114. Rotfeld Adam Daniel, *Polska w niepewnym świecie*, Polski Instytut Spraw Międzynarodowych, Warszawa 2006.

115. Rutkowski Cezary, *Przegląd strategiczny jako narzędzie polityki*, "Elipsa", Warszawa 2003.

116. Siemaszko Andrzej, *Atlas przestępczości w Polsce*, Oficyna Naukowa, Warszawa 2009.

117. Sienkiewicz Piotr, *10 wykładów*, AON, Warszawa 2005.

118. Sienkiewicz Piotr, *Analiza systemowa,* Warszawa 1995

119. Sienkiewicz Piotr, *Systemy kierowania*, Wiedza Powszechna, Warszawa 1989.

120. Sienkiewicz Piotr, Wieleba Ryszard, Wocial Janusz, Kuca Marceli, Skoczylas Magdalena, *Wartość informacji w dowodzeniu i zarządzaniu. Metodologia analizy potrzeb informacyjnych*, AON, Warszawa 2002.

121. Sieńko Jan, *Bezpieczeństwo wewnętrzne państwa w dobie walki z terroryzmem*, Zespół Redakcyjno-Wydawniczy Marynarki Wojennej, Warszawa, Gdynia 2005.

122. Soroka Paweł, *Polistrategia bezpieczeństwa zewnętrznego Polski: ujęcie normatywne*, Oficyna Wydawniczo-Poligraficzna "Adam", Warszawa 2005.

123. Stern Jessica, *The Ultimate Terrorists*, Harvard University Press – Cambridge Massachusetts, London 1999.

124. Stolarczyk Mieczysław (red.), *Bezpieczeństwo Polski i bezpieczeństwo europejskie na początku XXI wieku: wybrane aspekty*, Wydaw. UŚ, Katowice 2004.

125. Strasburger Dominik, Doraczyńska Anna, Kostka Ewa, Pawlikowska Anna (zespół red.), *Systemy informacji geoprzestrzennej a budowa przewagi informacyjnej w sferze bezpieczeństwa państwa. Materiały opracowane na podstawie wniosków i tez z konferencji naukowej zorganizowanej prze Wydział Strategiczno-Obronny AON*, Zeszyty Naukowe Akademii Obrony Narodowej nr 1(58)A, Warszawa 2005

126. Strzelczyk Joanna (red.), *Bezpieczeństwo Narodowe*, BBN, Warszawa 2006.

127. Strzoda Marek, *Zarządzanie informacjami w organizacji*, AON, Warszawa 2004.

128. Szafrański Jerzy (red.); *Współczesne zagrożenia terroryzmem oraz metody działań antyterrorystycznych*, Wydział Wydawnictw i poligrafii Wyższej Szkoły Policji w Szczytnie, Szczytno 2007.

129. Szafrański Jerzy; *Organizacyjne i prawne aspekty działań antyterrorystycznych*; Wydział Wydawnictw i poligrafii Wyższej Szkoły Policji w Szczytnie, Szczytno 2002.

130. Szafrański Jerzy; *Współdziałanie jednostek obrony terytorialnej i policji w walce z terroryzmem*; Wydział Wydawnictw i poligrafii Wyższej Szkoły Policji w Szczytnie, Szczytno 2004.

131. Szlachter Damian, *Walka z terroryzmem w Unii Europejskiej-nowy impuls*, Wydawnictwo Adam Marszałek, Toruń 2006.

132. Tokarski Jan (red.), *Słownik wyrazów obcych*, Warszawa 1980.

133. Tomasiewicz Jarosław; *Terroryzm na tle przemocy politycznej. Zarys encyklopedyczny*; Apis, Wrocław 2000.

134. Verton Dan, *Black Ice: niewidzialna groźba cyberterroryzmu*, Helion, Warszawa 2004

135. Wentkowska Aleksandra, Kaczmarczyk Michał (red.), *System międzynarodowy: koncepcje, wyzwania, perspektywy*, Wyższa Szkoła Zarządzania i Marketingu, Sosnowiec 2005.

136. Whittaker David. J., *Terrorists and terrorism in the contemporary world*, Routledge, London and New York 2004.

137. Wierzbołowski Józef, *Aksjologiczne i społeczne skutki przekształcenia informacji w zasób*, Warszawa 1997

138. Winkler Ira, *Corporate Espionage. What It Is, Why It Is Happening In Your Company, What You Must Do About It*. Prima Publishing, Rocklin, California 1997

139. Wnuk-Lipiński Edmund, Socjologia życia publicznego, Wydawnictwo Naukowe Scholar, Warszawa 2005.

140. Wnuk-Lipiński Edmund, *Świat międzyepoki. Globalizacja – demokracja – państwo narodowe*, Wydawnictwo Znak, ISP PAN, Kraków 2004.

141. Wojciechowski Sebastian, Wallas Tadeusz; *The power of terrorism*; Wyd. Instytutu Nauk Politycznych i Dziennikarstwa Uniwersytetu Adama Mickiewicza; Poznań 2005.

142. Wojciechowski Sebastian; *The Faces of Terrorism*; Wyd. Instytutu Nauk Politycznych i Dziennikarstwa Uniwersytetu Adama Mickiewicza; Poznań 2006.

143. Wójcik Jerzy Wojciech, *Przeciwdziałanie finansowaniu terroryzmu*, Oficyna a Wolters Kluwer Business; Warszawa, Kraków 2007.

144. Wojtaszczyk Konstanty Adam (red. nauk.), *Bezpieczeństwo Polski w perspektywie członkostwa w Unii Europejskiej*, WDZiNP UW, Warszawa 2002.

145. Wróbel Izabela, *Polityka Unii Europejskiej w dziedzinie Wymiaru Sprawiedliwości i Spraw Wewnętrznych*; Arboretum; Wrocław 2002.

146. Zacher Lech, *Społeczeństwo sieci*. Wyd. Naukowe PWN, Warszawa, 2007

147. Zacher Lech, *Transformacje społeczeństw od informacji do wiedzy*. C.H. Beck, Warszawa, 2007.

148. *Zagrożenia dla bezpieczeństwa informacyjnego państwa. Identyfikacja, analiza zagrożeń i ryzyka) Tom I – Raport z badań*, praca zbiorowa, Warszawa 2004

149. Zalewski Sławomir, *Służby Specjalne w państwie demokratycznym*, AON, Warszawa 2002.

150. Zięba Ryszard, *Instytucjonalizacja bezpieczeństwa europejskiego*, Wydawnictwo Naukowe Scholar; Warszawa 2004.

151. Zięba Ryszard, *Wspólna Polityka Zagraniczna i Bezpieczeństwa Unii Europejskiej*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2007.

DOKUMENTY

1. Ustawa z dnia 12 października 1990 r. o ochronie granicy państwowej (Dz.U. z 1990 r. nr 78 poz.461 z późn. zm.)
2. Ustawa z dnia 12 października 1990 r. o Straży Granicznej (Dz.U. z 1990 r. Nr 78, poz. 462 z późn. zm.)
3. Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu (tekst jednolity Dz.U. z 2003 r. nr 153 poz. 1505)
4. Ustawa z dnia 16 marca 2001 r. o Biurze Ochrony Rządu (tekst jednolity Dz.U.04.163.1712 z późn. zm.)
5. Ustawa z dnia 21 czerwca 2002 r. o materiałach wybuchowych do użytku cywilnego (Dz.U. 2002 nr 117 poz. 1007 z późn. zm.)
6. Ustawa z dnia 21 maja 1991 r. o broni i amunicji, (Dz.U. 1999 nr 53 poz. 549)
7. Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (tekst jednolity Dz.U. z 2004 nr 241, poz. 2416 z późn. zm.)
8. Ustawa z dnia 24 lipca 1999 r. o Służbie Celnej (tekst jednolity Dz.U z 2004 r. nr 156, poz. 1641 z późn. zm.)
9. Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2002 r. Nr 74, poz. 676 z późn. zm.)
10. Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (tekst jednolity Dz.U. z 2002 r. nr 147, poz. 1230 z późn. zm.)
11. Ustawa z dnia 24 sierpnia 2001 r . o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz.U. z 2001 r. nr 123 poz. 1353 z późn. zm.)
12. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590)
13. Ustawa z dnia 4 października 1997 o działach administracji rządowej (Dz.U. 1997 nr 141 poz. 943 z późn. zm.)
14. Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny. (Dz.U. 1997 nr 88 poz. 553 z późn. zm.)
15. Ustawa z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego (Dz.U. 1997 nr 89 poz. 555 z późn. zm.)
16. Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. 2006 nr 104 poz. 709)
17. Ustawa z dnia 9 lipca 2003 r. o Wojskowych Służbach Informacyjnych (Dz.U. z 2003 r. nr 139, poz. 1326 z późn. zm.)
18. Ustawa z dnia 9 listopada 2000 r. o bezpieczeństwie morskim (Dz. U. 2000 nr 109 poz. 1156)
19. Ustawa z dnia 6 kwietnia 1990 r. o Policji (tekst jednolity Dz.U. z 2002 r. nr 7 poz.58 z późn. zm.)

20. DECYZJA RADY z dnia 19 marca 2001 r. w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa, (2001/264/WE), Dz.U. UE L z dnia 11 kwietnia 2001 r.

INTERNET

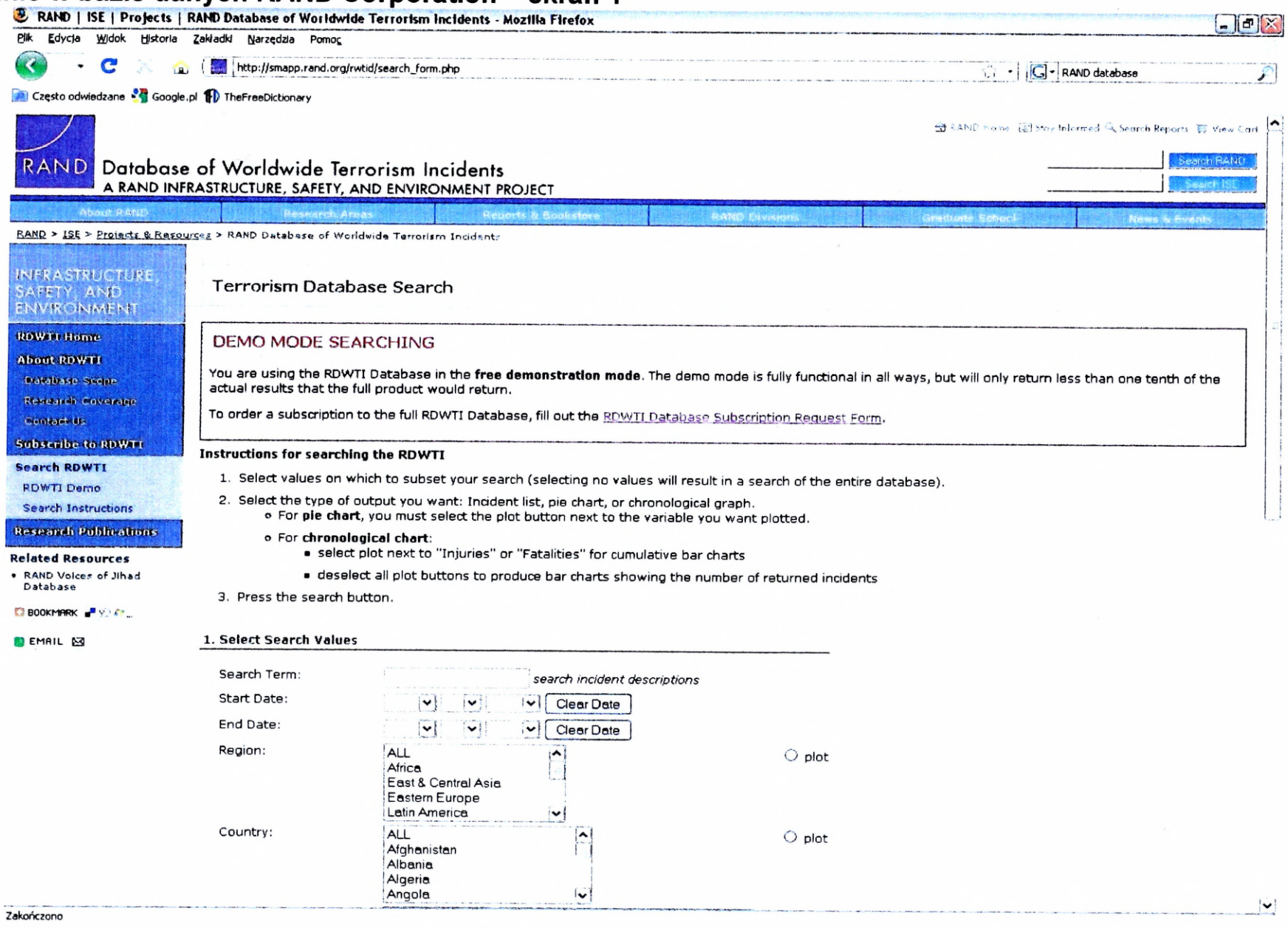
1. *Information Management. Information Security Classification, Government of Alberta*, Alberta 2005, tekst dostępny na stronie o adresie [http://www.im.gov.ab.ca/publications/pdf/InfoSecurityClassification.pdf].
2. Put Dariusz, *Integracja zasobów informacyjnych w systemach heterogenicznych* [w:] Kozielski S., Małysiak B., Kasprowski P., Mrozek D. (red.), *Bazy Danych: Rozwój metod i technologii*, WKŁ 2008, tekst dostępny na stronie o adresie [http://zti.inf.polsl.pl/BDAS/2008/BDAS%6008%20-%20Integracja%20zasob%C3%B3w%20informacyjnych%20w%C2%A0systemach%C2%A0heterogenicznych.pdf?Id=523&val=1].
3. *The Intelligence Cycle* (w:) *Factbook on Intelligence*, tekst dostępny na stronie [http://www.odci.gov/cia/publications].
4. *University of Colorado Boulder (campus) Guidance on Information Asset Classification*, tekst dostępny na stronie o adresie: [http://www.colorado.edu/its/security/assetinventory/UCB%20Guidance%20on%20Information%20Asset%20Classification.pdf].
5. Willis H., Korral A., Kelly T., Medby J., *Estimating Terrorism Risk*, RAND Corp. 2005, tekst dostępny na stronie: [http://www.RAND.org/pubs/monographs/2005/RAND_MG388.pdf].

PRASA:

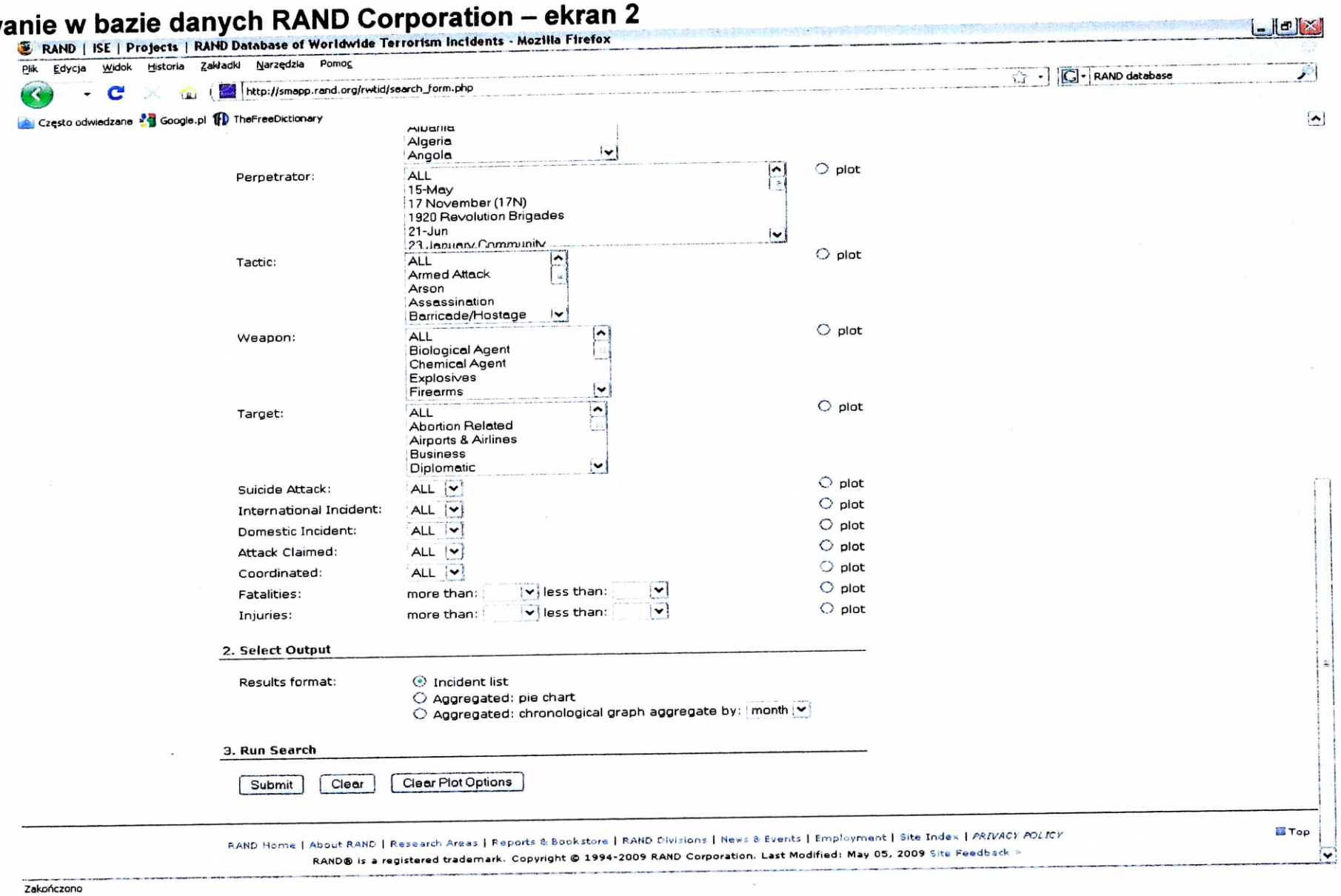
1. *Terroryzm – co robić w sytuacji zagrożenia?*, dodatek do dziennika „Rzeczpospolita" z dnia 25 lutego 2005 r.
2. Liedel Krzysztof, *Działania proaktywne w zwalczaniu terroryzmu*, „Terroryzm: zagrożenia – prewencja – przeciwdziałanie", nr 1/2008.
3. Kubiak Krzysztof, *Wojna asymetryczna i terroryzm jako zagrożenie bezpieczeństwa państwa* [w: Konferencja *naukowa Bezpieczne niebo*], Warszawa 2002
4. *Terroryzm – co robić w sytuacji zagrożenia?,* dodatek do Rzeczpospolitej, 23 lutego 2005 r.
5. Liedel Krzysztof, *NATO i jego aktywny udział w zwalczaniu terroryzmu międzynarodowego,* Magazyn Prawniczy JURYSTA, nr 4/04
6. Liedel Krzysztof, *Wielopłaszczyznowe podejście do zwalczania terroryzmu międzynarodowego*, Magazyn Prawniczy JURYSTA, nr 9/04
7. Liedel Krzysztof, *Normy prawa międzynarodowego w zwalczaniu terroryzmu po 11 wrześniu 2001 r.*, Magazyn Prawniczy JURYSTA, nr 3/04

8. Wnuk-Lipiński Edmund, *Oblicza globalizacji – konceptualizacja pojęcia*, w: I. Krzemiński (red.): „Socjologia a przemiany współczesnego świata", Wydawnictwo Naukowe Scholar, Warszawa 2004

ZAŁĄCZNIK 1
Wyszukiwanie w bazie danych RAND Corporation – ekran 1

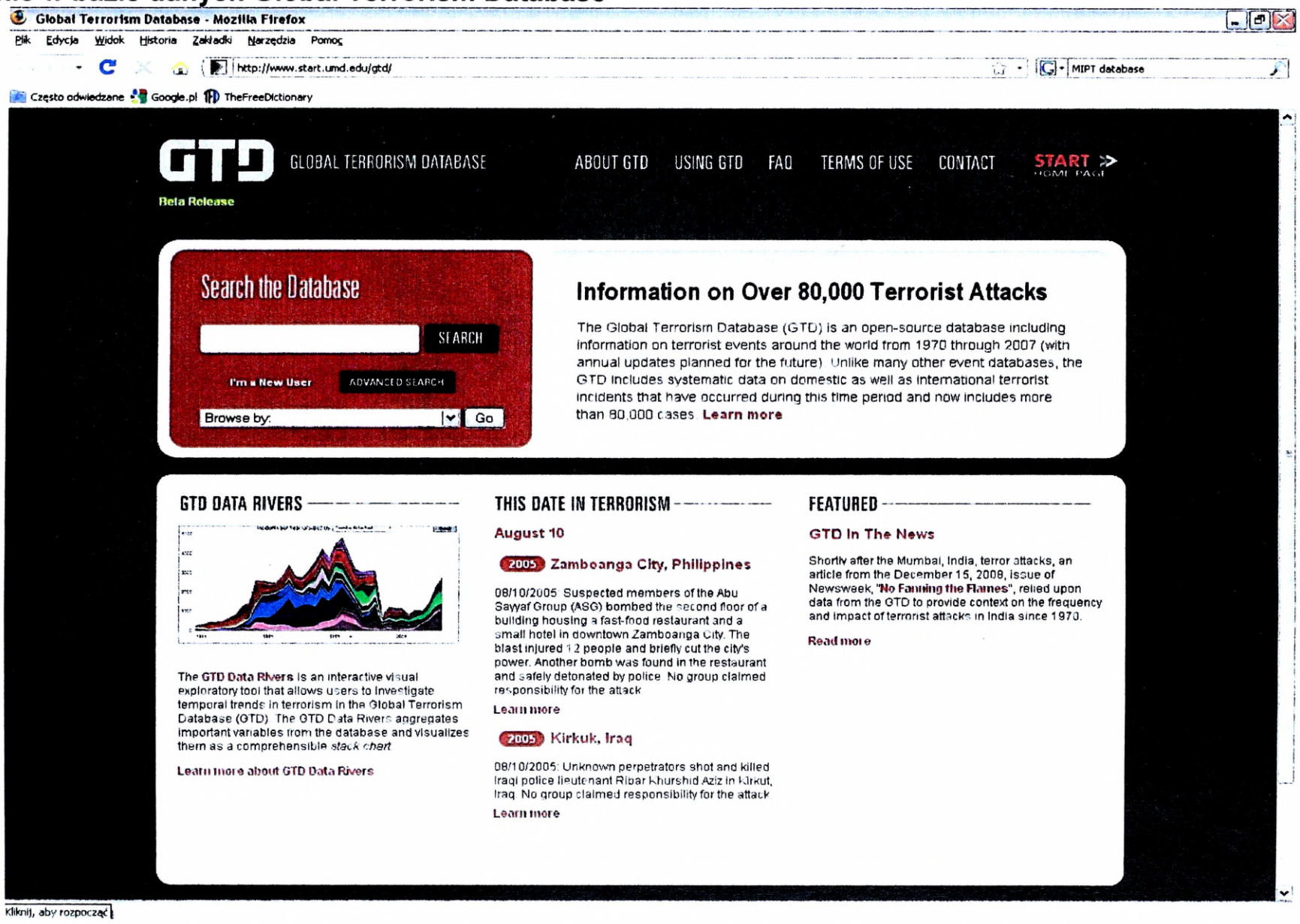


Wyszukiwanie w bazie danych RAND Corporation – ekran 2



ZAŁĄCZNIK 2

Wyszukiwanie w bazie danych Global Terrorism Database



Wyszukiwanie w bazie danych Global Terrorism Database – według typu ataku z zadanym okresie i obszarze

GTD Search Results - Mozilla Firefox

Plik Edycja Widok Historia Zakładki Narzędzia Pomoc

http://www.start.umd.edu/gtd/search/Results.aspx?chart=attack&casualties_type=b&casualties_max=&start_yearonly=2001&end_yearonly=2007&dtp; MIPT database

Często odwiedzane Google.pl TheFreeDictionary

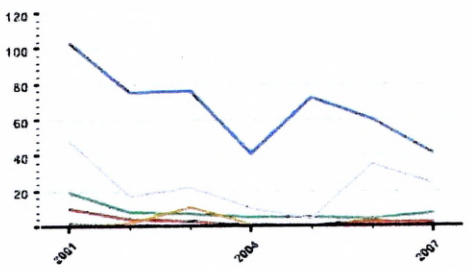
Search the Database | SEARCH | ADVANCED SEARCH | Browse by: | Go

Back to Advanced Search | Export | Email | Print

SEARCH RESULTS: 689 INCIDENTS

CHART RESULTS: | LINE CHART | BAR CHART | PIE CHART

- ATTACK TYPE
- WEAPON TYPE
- REGIONS



SEARCH CRITERIA:

Years: (between 2001 and 2007)

All incidents regardless of doubt.

Region: (Western Europe)

EVENT ID	DATE	COUNTRY	CITY	PERPETRATOR	FATALITIES	INJURED	TARGET TYPE
200712230004	2007-12-23	Corsica	Ajaccio	Corsican National Liberation Front (FLNC)	0	0	Government (General)
200712230003	2007-12-23	Corsica	Ajaccio	Corsican National Liberation Front (FLNC)	0	2	Police,Private Citizens & Property
200712200003	2007-12-20	Corsica	Ajaccio	Corsican National Liberation Front (FLNC)	0	1	Government (General)
200712200002	2007-12-20	Corsica	Ajaccio	Corsican National Liberation Front (FLNC)	0	0	Police

Przeczytano www.start.umd.edu

Wyszukiwanie w bazie danych Global Terrorism Database – według celu ataku z zadanym okresie i obszarze

GTD Search Results - Mozilla Firefox

Plik Edycja Widok Historia Zakładki Narzędzia Pomoc

http://www.start.umd.edu/gtd/search/Results.aspx?chart=target&casualties_type=b&casualties_max=&start_yearonly=2001&end_yearonly=2007&dtp:

MIPT database

Często odwiedzane Google.pl TheFreeDictionary

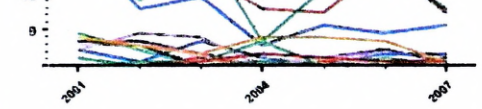
Search the Database SEARCH ADVANCED SEARCH Browse by: Go

Back to Advanced Search Export Email Print

SEARCH RESULTS: 689 INCIDENTS

CHART RESULTS: LINE CHART BAR CHART PIE CHART

TARGET TYPE



Business
Government (General)
Police
Military
Abortion Related
Airports, Airlines
Government (Diplomatic)
Educational Institution
Food or Water Supply
Journalists, Media
Maritime
NGO
Other
Private Citizens, Pro..
Religious Figures/Inst..
Telecommunication
Terrorists
Tourists
Transportation
Unknown
Utilities
Violent Political Party

SEARCH CRITERIA :

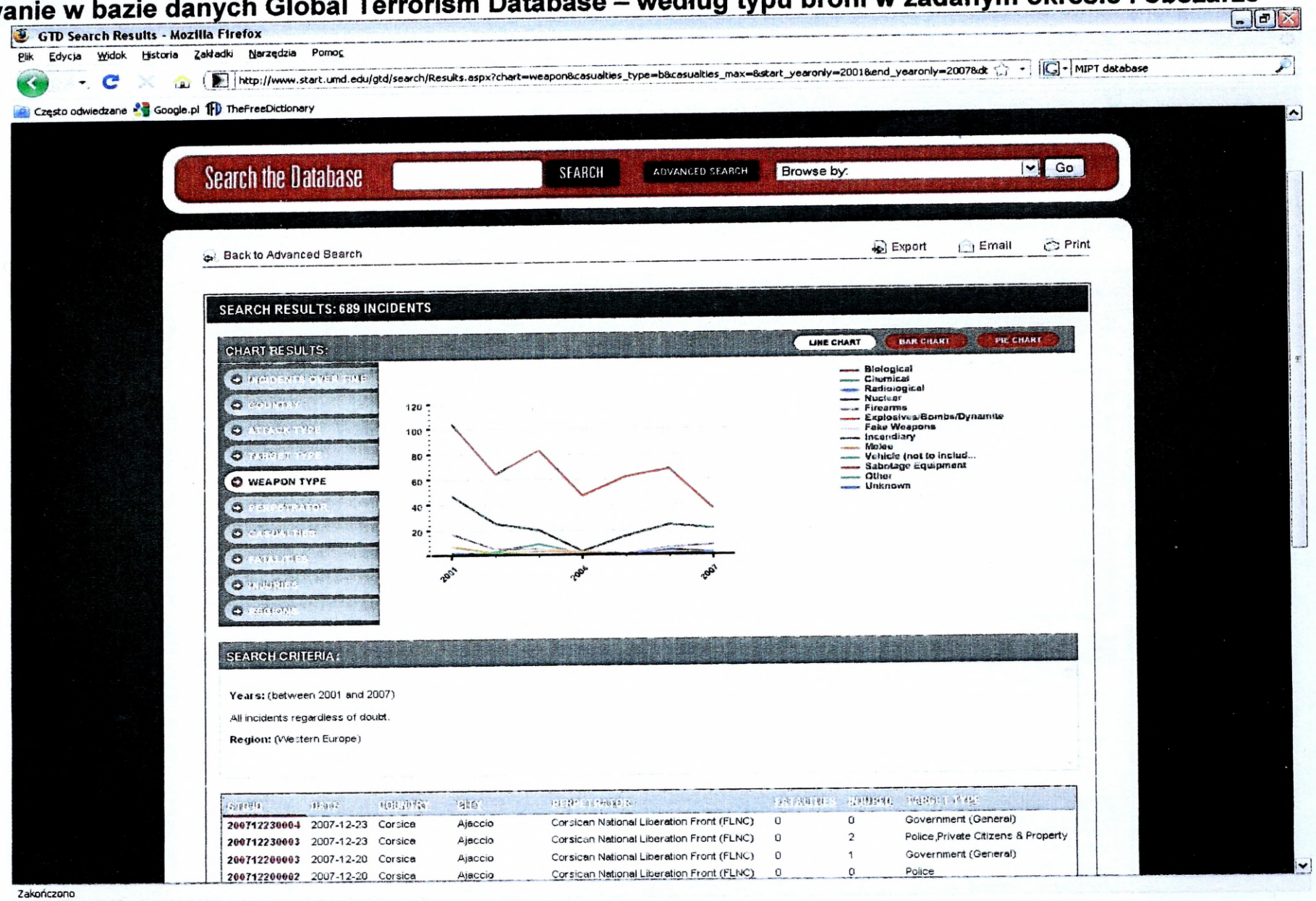
Years: (between 2001 and 2007)

All incidents regardless of doubt.

Region: (Western Europe)

200712230004	2007-12-23	Corsica	Ajaccio	Corsican National Liberation Front (FLNC)	0	0	Government (General)
200712230003	2007-12-23	Corsica	Ajaccio	Corsican National Liberation Front (FLNC)	0	2	Police,Private Citizens & Property
200712200003	2007-12-20	Corsica	Ajaccio	Corsican National Liberation Front (FLNC)	0	1	Government (General)
200712200002	2007-12-20	Corsica	Ajaccio	Corsican National Liberation Front (FLNC)	0	0	Police

Wyszukiwanie w bazie danych Global Terrorism Database – według typu broni w zadanym okresie i obszarze



ZAŁĄCZNIK 3
Akt prawny powołujący Centrum Antyterrorystyczne w Agencji Bezpieczeństwa Wewnętrznego

Monitor Polski Nr 69 — 3442 — Poz. 622

622

ZARZĄDZENIE Nr 102 PREZESA RADY MINISTRÓW

z dnia 17 września 2008 r.

zmieniające zarządzenie w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego

Na podstawie art. 20 ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. Nr 74, poz. 676, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. W zarządzeniu nr 73 Prezesa Rady Ministrów z dnia 26 czerwca 2002 r. w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego (M. P. Nr 26, poz. 432, z późn. zm.[2)]) w załączniku do zarządzenia w § 3 w ust. 1 po pkt 8 dodaje się pkt 8a w brzmieniu:

„8a) Centrum Antyterrorystyczne;".

§ 2. Zarządzenie wchodzi w życie z dniem 1 października 2008 r.

Prezes Rady Ministrów: *D. Tusk*

[1)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2003 r. Nr 90, poz. 844, Nr 113, poz. 1070, Nr 130, poz. 1188 i Nr 166, poz. 1609, z 2004 r. Nr 109, poz. 1159, Nr 171, poz. 1800, Nr 267, poz. 2647 i Nr 273, poz. 2703, z 2006 r. Nr 104, poz. 708 i 711 i Nr 218, poz. 1592, z 2007 r. Nr 25, poz. 162 oraz z 2008 r. Nr 11, poz. 59.

[2)] Zmiany wymienionego zarządzenia zostały ogłoszone w M. P. z 2005 r. Nr 46, poz. 634, z 2006 r. Nr 21, poz. 241, z 2007 r. Nr 21, poz. 243 i Nr 67, poz. 744 oraz z 2008 r. Nr 3, poz. 36.

ZAŁĄCZNIK 4

Patriot Act – zawartość aktu prawnego oraz rozdziały dotyczące:
- zwiększenia uprawnień w zakresie nadzoru technicznego
- wsparcia działań wywiadowczych

HR 3162 RDS

107th CONGRESS

1st Session

H. R. 3162
IN THE SENATE OF THE UNITED STATES

October 24, 2001

AN ACT

To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes. *Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

SECTION 1. SHORT TITLE AND TABLE OF CONTENTS.

(a) SHORT TITLE- This Act may be cited as the `Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001'. (b) TABLE OF CONTENTS- The table of contents for this Act is as follows:

Sec. 1. Short title and table of contents.
Sec. 2. Construction; severability.

TITLE I--ENHANCING DOMESTIC SECURITY AGAINST TERRORISM

Sec. 101. Counterterrorism fund.

Sec. 102. Sense of Congress condemning discrimination against Arab and Muslim Americans.

Sec. 103. Increased funding for the technical support center at the Federal Bureau of Investigation.

Sec. 104. Requests for military assistance to enforce prohibition in certain emergencies.

Sec. 105. Expansion of National Electronic Crime Task Force Initiative.

Sec. 106. Presidential authority.

TITLE II--ENHANCED SURVEILLANCE PROCEDURES

Sec. 201. Authority to intercept wire, oral, and electronic communications relating to terrorism.

Sec. 202. Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses.

Sec. 203. Authority to share criminal investigative information.

Sec. 204. Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications.

Sec. 205. Employment of translators by the Federal Bureau of Investigation.

Sec. 206. Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978.

Sec. 207. Duration of FISA surveillance of non-United States persons who are agents of a foreign power.

Sec. 208. Designation of judges.

Sec. 209. Seizure of voice-mail messages pursuant to warrants.

Sec. 210. Scope of subpoenas for records of electronic communications.

Sec. 211. Clarification of scope.

Sec. 212. Emergency disclosure of electronic communications to protect life and limb.

Sec. 213. Authority for delaying notice of the execution of a warrant.

Sec. 214. Pen register and trap and trace authority under FISA.

Sec. 215. Access to records and other items under the Foreign Intelligence Surveillance Act.

Sec. 216. Modification of authorities relating to use of pen registers and trap and trace devices.

Sec. 217. Interception of computer trespasser communications.

Sec. 218. Foreign intelligence information.

Sec. 219. Single-jurisdiction search warrants for terrorism.

Sec. 220. Nationwide service of search warrants for electronic evidence.

Sec. 221. Trade sanctions.

Sec. 222. Assistance to law enforcement agencies.

Sec. 223. Civil liability for certain unauthorized disclosures.

Sec. 224. Sunset.

Sec. 225. Immunity for compliance with FISA wiretap.

TITLE III--INTERNATIONAL MONEY LAUNDERING ABATEMENT AND ANTI-TERRORIST FINANCING ACT OF 2001

Sec. 301. Short title.

Sec. 302. Findings and purposes.

Sec. 303. 4-year congressional review; expedited consideration.

Subtitle A--International Counter Money Laundering and Related Measures

Sec. 311. Special measures for jurisdictions, financial institutions, or international transactions of primary money laundering concern.

Sec. 312. Special due diligence for correspondent accounts and private banking accounts.

Sec. 313. Prohibition on United States correspondent accounts with foreign shell banks.

Sec. 314. Cooperative efforts to deter money laundering.

Sec. 315. Inclusion of foreign corruption offenses as money laundering crimes.

Sec. 316. Anti-terrorist forfeiture protection.

Sec. 317. Long-arm jurisdiction over foreign money launderers.

Sec. 318. Laundering money through a foreign bank.

Sec. 319. Forfeiture of funds in United States interbank accounts.

Sec. 320. Proceeds of foreign crimes.

Sec. 321. Financial institutions specified in subchapter II of chapter 53 of title 31, United States code.

Sec. 322. Corporation represented by a fugitive.

Sec. 323. Enforcement of foreign judgments.

Sec. 324. Report and recommendation.

Sec. 325. Concentration accounts at financial institutions.

Sec. 326. Verification of identification.

Sec. 327. Consideration of anti-money laundering record.

Sec. 328. International cooperation on identification of originators of wire transfers.

Sec. 329. Criminal penalties.

Sec. 330. International cooperation in investigations of money laundering, financial crimes, and the finances of terrorist groups.

Subtitle B--Bank Secrecy Act Amendments and Related Improvements

Sec. 351. Amendments relating to reporting of suspicious activities.

Sec. 352. Anti-money laundering programs.

Sec. 353. Penalties for violations of geographic targeting orders and certain recordkeeping requirements, and lengthening effective period of geographic targeting orders.

Sec. 354. Anti-money laundering strategy.

Sec. 355. Authorization to include suspicions of illegal activity in written employment references.

Sec. 356. Reporting of suspicious activities by securities brokers and dealers; investment company study.

Sec. 357. Special report on administration of bank secrecy provisions.

Sec. 358. Bank secrecy provisions and activities of United States intelligence agencies to fight international terrorism.

Sec. 359. Reporting of suspicious activities by underground banking systems.

Sec. 360. Use of authority of United States Executive Directors.

Sec. 361. Financial crimes enforcement network.

Sec. 362. Establishment of highly secure network.

Sec. 363. Increase in civil and criminal penalties for money laundering.
Sec. 364. Uniform protection authority for Federal Reserve facilities.
Sec. 365. Reports relating to coins and currency received in nonfinancial trade or business.
Sec. 366. Efficient use of currency transaction report system.

Subtitle C--Currency Crimes and Protection

Sec. 371. Bulk cash smuggling into or out of the United States.
Sec. 372. Forfeiture in currency reporting cases.
Sec. 373. Illegal money transmitting businesses.
Sec. 374. Counterfeiting domestic currency and obligations.
Sec. 375. Counterfeiting foreign currency and obligations.
Sec. 376. Laundering the proceeds of terrorism.
Sec. 377. Extraterritorial jurisdiction.

TITLE IV--PROTECTING THE BORDER

Subtitle A--Protecting the Northern Border

Sec. 401. Ensuring adequate personnel on the northern border.
Sec. 402. Northern border personnel.
Sec. 403. Access by the Department of State and the INS to certain identifying information in the criminal history records of visa applicants and applicants for admission to the United States.
Sec. 404. Limited authority to pay overtime.
Sec. 405. Report on the integrated automated fingerprint identification system for ports of entry and overseas consular posts.

Subtitle B--Enhanced Immigration Provisions

Sec. 411. Definitions relating to terrorism.
Sec. 412. Mandatory detention of suspected terrorists; habeas corpus; judicial review.
Sec. 413. Multilateral cooperation against terrorists.
Sec. 414. Visa integrity and security.
Sec. 415. Participation of Office of Homeland Security on Entry-Exit Task Force.
Sec. 416. Foreign student monitoring program.
Sec. 417. Machine readable passports.
Sec. 418. Prevention of consulate shopping.

Subtitle C--Preservation of Immigration Benefits for Victims of Terrorism

Sec. 421. Special immigrant status.

Sec. 422. Extension of filing or reentry deadlines.
Sec. 423. Humanitarian relief for certain surviving spouses and children.
Sec. 424. `Age-out' protection for children.
Sec. 425. Temporary administrative relief.
Sec. 426. Evidence of death, disability, or loss of employment.
Sec. 427. No benefits to terrorists or family members of terrorists.
Sec. 428. Definitions.

TITLE V--REMOVING OBSTACLES TO INVESTIGATING TERRORISM

Sec. 501. Attorney General's authority to pay rewards to combat terrorism.
Sec. 502. Secretary of State's authority to pay rewards.
Sec. 503. DNA identification of terrorists and other violent offenders.
Sec. 504. Coordination with law enforcement.
Sec. 505. Miscellaneous national security authorities.
Sec. 506. Extension of Secret Service jurisdiction.
Sec. 507. Disclosure of educational records.
Sec. 508. Disclosure of information from NCES surveys.

TITLE VI--PROVIDING FOR VICTIMS OF TERRORISM, PUBLIC SAFETY OFFICERS, AND THEIR FAMILIES

Subtitle A--Aid to Families of Public Safety Officers

Sec. 611. Expedited payment for public safety officers involved in the prevention, investigation, rescue, or recovery efforts related to a terrorist attack.
Sec. 612. Technical correction with respect to expedited payments for heroic public safety officers.
Sec. 613. Public safety officers benefit program payment increase.
Sec. 614. Office of Justice programs.

Subtitle B--Amendments to the Victims of Crime Act of 1984

Sec. 621. Crime victims fund.
Sec. 622. Crime victim compensation.
Sec. 623. Crime victim assistance.
Sec. 624. Victims of terrorism.

TITLE VII--INCREASED INFORMATION SHARING FOR CRITICAL INFRASTRUCTURE PROTECTION

Sec. 711. Expansion of regional information sharing system to facilitate Federal-State-local law enforcement response related to terrorist attacks.

TITLE VIII--STRENGTHENING THE CRIMINAL LAWS AGAINST TERRORISM

Sec. 801. Terrorist attacks and other acts of violence against mass transportation systems.

Sec. 802. Definition of domestic terrorism.

Sec. 803. Prohibition against harboring terrorists.

Sec. 804. Jurisdiction over crimes committed at U.S. facilities abroad.

Sec. 805. Material support for terrorism.

Sec. 806. Assets of terrorist organizations.

Sec. 807. Technical clarification relating to provision of material support to terrorism.

Sec. 808. Definition of Federal crime of terrorism.

Sec. 809. No statute of limitation for certain terrorism offenses.

Sec. 810. Alternate maximum penalties for terrorism offenses.

Sec. 811. Penalties for terrorist conspiracies.

Sec. 812. Post-release supervision of terrorists.

Sec. 813. Inclusion of acts of terrorism as racketeering activity.

Sec. 814. Deterrence and prevention of cyberterrorism.

Sec. 815. Additional defense to civil actions relating to preserving records in response to Government requests.

Sec. 816. Development and support of cybersecurity forensic capabilities.

Sec. 817. Expansion of the biological weapons statute.

TITLE IX--IMPROVED INTELLIGENCE

Sec. 901. Responsibilities of Director of Central Intelligence regarding foreign intelligence collected under Foreign Intelligence Surveillance Act of 1978.

Sec. 902. Inclusion of international terrorist activities within scope of foreign intelligence under National Security Act of 1947.

Sec. 903. Sense of Congress on the establishment and maintenance of intelligence relationships to acquire information on terrorists and terrorist organizations.

Sec. 904. Temporary authority to defer submittal to Congress of reports on intelligence and intelligence-related matters.

Sec. 905. Disclosure to Director of Central Intelligence of foreign intelligence-related information with respect to criminal investigations.

Sec. 906. Foreign terrorist asset tracking center.

Sec. 907. National Virtual Translation Center.

Sec. 908. Training of government officials regarding identification and use of foreign intelligence.

TITLE X--MISCELLANEOUS

Sec. 1001. Review of the department of justice.

Sec. 1002. Sense of congress.

Sec. 1003. Definition of `electronic surveillance'.

Sec. 1004. Venue in money laundering cases.

Sec. 1005. First responders assistance act.

Sec. 1006. Inadmissibility of aliens engaged in money laundering.

Sec. 1007. Authorization of funds for dea police training in south and central asia.

Sec. 1008. Feasibility study on use of biometric identifier scanning system with access to the fbi integrated automated fingerprint identification system at overseas consular posts and points of entry to the United States.

Sec. 1009. Study of access.

Sec. 1010. Temporary authority to contract with local and State governments for performance of security functions at United States military installations.

Sec. 1011. Crimes against charitable americans.

Sec. 1012. Limitation on issuance of hazmat licenses.

Sec. 1013. Expressing the sense of the senate concerning the provision of funding for bioterrorism preparedness and response.

Sec. 1014. Grant program for State and local domestic preparedness support.

Sec. 1015. Expansion and reauthorization of the crime identification technology act for anti-terrorism grants to States and localities.

Sec. 1016. Critical infrastructures protection.

TITLE II--ENHANCED SURVEILLANCE PROCEDURES

SEC. 201. AUTHORITY TO INTERCEPT WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS RELATING TO TERRORISM.

Section 2516(1) of title 18, United States Code, is amended--
(1) by redesignating paragraph (p), as so redesignated by section 434(2) of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104-132; 110 Stat. 1274), as paragraph (r); and
(2) by inserting after paragraph (p), as so redesignated by section 201(3) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (division C of Public Law 104-208; 110 Stat. 3009-565), the following new paragraph:

`(q) any criminal violation of section 229 (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2339A, or 2339B of this title (relating to terrorism); or'.

SEC. 202. AUTHORITY TO INTERCEPT WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS RELATING TO COMPUTER FRAUD AND ABUSE OFFENSES.

Section 2516(1)(c) of title 18, United States Code, is amended by striking `and section 1341 (relating to mail fraud),' and inserting `section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse),'.

SEC. 203. AUTHORITY TO SHARE CRIMINAL INVESTIGATIVE INFORMATION.

(a) AUTHORITY TO SHARE GRAND JURY INFORMATION-
(1) IN GENERAL- Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure is amended to read as follows:
`(C)(i) Disclosure otherwise prohibited by this rule of matters occurring before the grand jury may also be made--

`(I) when so directed by a court preliminarily to or in connection with a judicial proceeding;

`(II) when permitted by a court at the request of the defendant, upon a showing that grounds may exist for a motion to dismiss the indictment because of matters occurring before the grand jury;

`(III) when the disclosure is made by an attorney for the government to another Federal grand jury;

`(IV) when permitted by a court at the request of an attorney for the government, upon a showing that such matters may disclose a violation of state criminal law, to an appropriate official of a state or subdivision of a state for the purpose of enforcing such law; or

`(V) when the matters involve foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in clause (iv) of this subparagraph), to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties.

`(ii) If the court orders disclosure of matters occurring before the grand jury, the disclosure shall be made in such manner, at such time, and under such conditions as the court may direct.

`(iii) Any Federal official to whom information is disclosed pursuant to clause (i)(V) of this subparagraph may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information. Within a reasonable time after such disclosure, an attorney for the government shall file under seal a notice with the court stating the fact that such information was disclosed and the departments, agencies, or entities to which the disclosure was made.

`(iv) In clause (i)(V) of this subparagraph, the term `foreign intelligence information' means--

`(I) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--

`(aa) actual or potential attack or other grave hostile acts of-a foreign power or an agent of a foreign power;

`(bb) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

`(cc) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of foreign power; or

`(II) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

`(aa) the national defense or the security of the United States; or

`(bb) the conduct of the foreign affairs of the United States.'.

(2) CONFORMING AMENDMENT- Rule 6(e)(3)(D) of the Federal Rules of Criminal Procedure is amended by striking `(e)(3)(C)(i)' and inserting `(e)(3)(C)(i)(I)'.

(b) AUTHORITY TO SHARE ELECTRONIC, WIRE, AND ORAL INTERCEPTION INFORMATION-

(1) LAW ENFORCEMENT- Section 2517 of title 18, United States Code, is amended by inserting at the end the following:

`(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.'.

(2) DEFINITION- Section 2510 of title 18, United States Code, is amended by--

(A) in paragraph (17), by striking `and' after the semicolon;

(B) in paragraph (18), by striking the period and inserting `; and'; and

(C) by inserting at the end the following:

`(19) `foreign intelligence information' means--

`(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--

`(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

`(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

`(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

`(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

`(i) the national defense or the security of the United States; or

`(ii) the conduct of the foreign affairs of the United States.'.

(c) PROCEDURES- The Attorney General shall establish procedures for the disclosure of information pursuant to section 2517(6) and Rule 6(e)(3)(C)(i)(V) of the Federal Rules of Criminal Procedure that identifies a United States person, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)).

(d) FOREIGN INTELLIGENCE INFORMATION-

(1) IN GENERAL- Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(2) DEFINITION- In this subsection, the term `foreign intelligence information' means--

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States.

SEC. 204. CLARIFICATION OF INTELLIGENCE EXCEPTIONS FROM LIMITATIONS ON INTERCEPTION AND DISCLOSURE OF WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS.

Section 2511(2)(f) of title 18, United States Code, is amended--

(1) by striking `this chapter or chapter 121' and inserting `this chapter or chapter 121 or 206 of this title'; and
(2) by striking `wire and oral' and inserting `wire, oral, and electronic'.

SEC. 205. EMPLOYMENT OF TRANSLATORS BY THE FEDERAL BUREAU OF INVESTIGATION.

(a) AUTHORITY- The Director of the Federal Bureau of Investigation is authorized to expedite the employment of personnel as translators to support counterterrorism investigations and operations without regard to applicable Federal personnel requirements and limitations.

(b) SECURITY REQUIREMENTS- The Director of the Federal Bureau of Investigation shall establish such security requirements as are necessary for the personnel employed as translators under subsection (a).

(c) REPORT- The Attorney General shall report to the Committees on the Judiciary of the House of Representatives and the Senate on--

(1) the number of translators employed by the FBI and other components of the Department of Justice;

(2) any legal or practical impediments to using translators employed by other Federal, State, or local agencies, on a full, part-time, or shared basis; and

(3) the needs of the FBI for specific translation services in certain languages, and recommendations for meeting those needs.

SEC. 206. ROVING SURVEILLANCE AUTHORITY UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

Section 105(c)(2)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(c)(2)(B)) is amended by inserting `, or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons,' after `specified person'.

SEC. 207. DURATION OF FISA SURVEILLANCE OF NON-UNITED STATES PERSONS WHO ARE AGENTS OF A FOREIGN POWER.

(a) DURATION -

(1) SURVEILLANCE- Section 105(e)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(e)(1)) is amended by--

(A) inserting `(A)' after `except that'; and

(B) inserting before the period the following: `, and (B) an order under this Act for a surveillance targeted against an agent of a foreign power, as defined in section 101(b)(1)(A) may be for the period specified in the application or for 120 days, whichever is less'.

(2) PHYSICAL SEARCH- Section 304(d)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824(d)(1)) is amended by--

(A) striking `forty-five' and inserting `90';

(B) inserting `(A)' after `except that'; and

(C) inserting before the period the following: `, and (B) an order under this section for a physical search targeted against an agent of a foreign power as defined in section 101(b)(1)(A) may be for the period specified in the application or for 120 days, whichever is less'.

(b) EXTENSION-

(1) IN GENERAL- Section 105(d)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(d)(2)) is amended by--

(A) inserting `(A)' after `except that'; and

(B) inserting before the period the following: `, and (B) an extension of an order under this Act for a surveillance targeted against an agent of a foreign power as defined in section 101(b)(1)(A) may be for a period not to exceed 1 year'.

(2) DEFINED TERM- Section 304(d)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824(d)(2) is amended by inserting after `not a United States person,' the following: `or against an agent of a foreign power as defined in section 101(b)(1)(A),'.

SEC. 208. DESIGNATION OF JUDGES.

Section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)) is amended by--

(1) striking `seven district court judges' and inserting `11 district court judges'; and

(2) inserting `of whom no fewer than 3 shall reside within 20 miles of the District of Columbia' after `circuits'.

SEC. 209. SEIZURE OF VOICE-MAIL MESSAGES PURSUANT TO WARRANTS.

Title 18, United States Code, is amended--

(1) in section 2510--

(A) in paragraph (1), by striking beginning with `and such' and all that follows through `communication'; and

(B) in paragraph (14), by inserting `wire or' after `transmission of'; and

(2) in subsections (a) and (b) of section 2703--

(A) by striking `CONTENTS OF ELECTRONIC' and inserting `CONTENTS OF WIRE OR ELECTRONIC' each place it appears;

(B) by striking `contents of an electronic' and inserting `contents of a wire or electronic' each place it appears; and

(C) by striking `any electronic' and inserting `any wire or electronic' each place it appears.

SEC. 210. SCOPE OF SUBPOENAS FOR RECORDS OF ELECTRONIC COMMUNICATIONS.

Section 2703(c)(2) of title 18, United States Code, as redesignated by section 212, is amended--

(1) by striking `entity the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber' and inserting the following: `entity the--

`(A) name;

`(B) address;

`(C) local and long distance telephone connection records, or records of session times and durations;

`(D) length of service (including start date) and types of service utilized;

`(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

`(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber'; and

(2) by striking `and the types of services the subscriber or customer utilized,'.

SEC. 211. CLARIFICATION OF SCOPE.

Section 631 of the Communications Act of 1934 (47 U.S.C. 551) is amended--

(1) in subsection (c)(2)--

(A) in subparagraph (B), by striking `or';

(B) in subparagraph (C), by striking the period at the end and inserting `; or'; and

(C) by inserting at the end the following:

`(D) to a government entity as authorized under chapters 119, 121, or 206 of title 18, United States Code, except that such disclosure shall not include records revealing cable subscriber selection of video programming from a cable operator.'; and

(2) in subsection (h), by striking `A governmental entity' and inserting `Except as provided in subsection (c)(2)(D), a governmental entity'.

SEC. 212. EMERGENCY DISCLOSURE OF ELECTRONIC COMMUNICATIONS TO PROTECT LIFE AND LIMB.

(a) DISCLOSURE OF CONTENTS-

(1) IN GENERAL- Section 2702 of title 18, United States Code, is amended--

(A) by striking the section heading and inserting the following:

`Sec. 2702. Voluntary disclosure of customer communications or records';

(B) in subsection (a)--

(i) in paragraph (2)(A), by striking `and' at the end;

(ii) in paragraph (2)(B), by striking the period and inserting `; and'; and

(iii) by inserting after paragraph (2) the following:

`(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.';

(C) in subsection (b), by striking `EXCEPTIONS- A person or entity' and inserting `EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS- A provider described in subsection (a)';

(D) in subsection (b)(6)--

(i) in subparagraph (A)(ii), by striking `or';

(ii) in subparagraph (B), by striking the period and inserting `; or'; and

(iii) by adding after subparagraph (B) the following:

`(C) if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.'; and

(E) by inserting after subsection (b) the following:

`(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS- A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

`(1) as otherwise authorized in section 2703;

`(2) with the lawful consent of the customer or subscriber;

`(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

`(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or

`(5) to any person other than a governmental entity.'.

(2) TECHNICAL AND CONFORMING AMENDMENT- The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2702 and inserting the following:

`2702. Voluntary disclosure of customer communications or records.'.

(b) REQUIREMENTS FOR GOVERNMENT ACCESS-

(1) IN GENERAL- Section 2703 of title 18, United States Code, is amended--

(A) by striking the section heading and inserting the following:

`Sec. 2703. Required disclosure of customer communications or records';

(B) in subsection (c) by redesignating paragraph (2) as paragraph (3);

(C) in subsection (c)(1)--

(i) by striking `(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may' and inserting `A governmental entity may require a provider of electronic communication service or remote computing service to';

(ii) by striking `covered by subsection (a) or (b) of this section) to any person other than a governmental entity.

`(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity' and inserting `)';

(iii) by redesignating subparagraph (C) as paragraph (2);

(iv) by redesignating clauses (i), (ii), (iii), and (iv) as subparagraphs (A), (B), (C), and (D), respectively;

(v) in subparagraph (D) (as redesignated) by striking the period and inserting `; or'; and

(vi) by inserting after subparagraph (D) (as redesignated) the following:

`(E) seeks information under paragraph (2).'; and

(D) in paragraph (2) (as redesignated) by striking `subparagraph (B)' and insert `paragraph (1)'.

(2) TECHNICAL AND CONFORMING AMENDMENT- The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2703 and inserting the following:

`2703. Required disclosure of customer communications or records.'.

SEC. 213. AUTHORITY FOR DELAYING NOTICE OF THE EXECUTION OF A WARRANT.

Section 3103a of title 18, United States Code, is amended--

(1) by inserting `(a) IN GENERAL- ' before `In addition'; and

(2) by adding at the end the following:

`(b) DELAY- With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if--

`(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705);

`(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and

`(3) the warrant provides for the giving of such notice within a reasonable period of its execution, which period may thereafter be extended by the court for good cause shown.'.

SEC. 214. PEN REGISTER AND TRAP AND TRACE AUTHORITY UNDER FISA.

(a) APPLICATIONS AND ORDERS- Section 402 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1842) is amended--

(1) in subsection (a)(1), by striking `for any investigation to gather foreign intelligence information or information concerning international terrorism' and inserting `for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution';

(2) by amending subsection (c)(2) to read as follows:

`(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.';

(3) by striking subsection (c)(3); and

(4) by amending subsection (d)(2)(A) to read as follows:

`(A) shall specify--

`(i) the identity, if known, of the person who is the subject of the investigation;

`(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

`(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order.'.

(b) AUTHORIZATION DURING EMERGENCIES- Section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843) is amended--

(1) in subsection (a), by striking `foreign intelligence information or information concerning international terrorism' and inserting `foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution'; and

(2) in subsection (b)(1), by striking `foreign intelligence information or information concerning international terrorism' and inserting `foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution'.

SEC. 215. ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.

Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503 and inserting the following:

`SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.

`(a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

`(2) An investigation conducted under this section shall--

`(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

`(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

`(b) Each application under this section--

`(1) shall be made to--

`(A) a judge of the court established by section 103(a); or

`(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

`(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to protect against international terrorism or clandestine intelligence activities.

`(c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

`(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

`(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

`(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

`SEC. 502. CONGRESSIONAL OVERSIGHT.

`(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 402.

`(b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period--

`(1) the total number of applications made for orders approving requests for the production of tangible things under section 402; and

`(2) the total number of such orders either granted, modified, or denied.'.

SEC. 216. MODIFICATION OF AUTHORITIES RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES.

(a) GENERAL LIMITATIONS- Section 3121(c) of title 18, United States Code, is amended--

(1) by inserting `or trap and trace device' after `pen register';

(2) by inserting `, routing, addressing,' after `dialing'; and

(3) by striking `call processing' and inserting `the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications'.

(b) ISSUANCE OF ORDERS-

(1) IN GENERAL- Section 3123(a) of title 18, United States Code, is amended to read as follows:

`(a) IN GENERAL-

`(1) ATTORNEY FOR THE GOVERNMENT- Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

`(2) STATE INVESTIGATIVE OR LAW ENFORCEMENT OFFICER- Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

`(3)(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify--

`(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;

`(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;

`(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and

`(iv) any information which has been collected by the device.

To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.

`(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).'.

(2) CONTENTS OF ORDER- Section 3123(b)(1) of title 18, United States Code, is amended--

(A) in subparagraph (A)--

(i) by inserting `or other facility' after `telephone line'; and

(ii) by inserting before the semicolon at the end `or applied'; and

(B) by striking subparagraph (C) and inserting the following:

`(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and'.

(3) NONDISCLOSURE REQUIREMENTS- Section 3123(d)(2) of title 18, United States Code, is amended--

(A) by inserting `or other facility' after `the line'; and

(B) by striking `, or who has been ordered by the court' and inserting `or applied, or who is obligated by the order'.

(c) DEFINITIONS-

(1) COURT OF COMPETENT JURISDICTION- Section 3127(2) of title 18, United States Code, is amended by striking subparagraph (A) and inserting the following:

`(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated; or'.

(2) PEN REGISTER- Section 3127(3) of title 18, United States Code, is amended--

(A) by striking `electronic or other impulses' and all that follows through `is attached' and inserting `dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication'; and

(B) by inserting `or process' after `device' each place it appears.

(3) TRAP AND TRACE DEVICE- Section 3127(4) of title 18, United States Code, is amended--

(A) by striking `of an instrument' and all that follows through the semicolon and inserting `or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;'; and

(B) by inserting `or process' after `a device'.

(4) CONFORMING AMENDMENT- Section 3127(1) of title 18, United States Code, is amended--

(A) by striking `and'; and

(B) by inserting `, and `contents' after `electronic communication service'.

(5) TECHNICAL AMENDMENT- Section 3124(d) of title 18, United States Code, is amended by striking `the terms of'.

(6) CONFORMING AMENDMENT- Section 3124(b) of title 18, United States Code, is amended by inserting `or other facility' after `the appropriate line'.

SEC. 217. INTERCEPTION OF COMPUTER TRESPASSER COMMUNICATIONS.

Chapter 119 of title 18, United States Code, is amended--

(1) in section 2510--

(A) in paragraph (18), by striking `and' at the end;

(B) in paragraph (19), by striking the period and inserting a semicolon; and

(C) by inserting after paragraph (19) the following:

`(20) `protected computer' has the meaning set forth in section 1030; and

`(21) `computer trespasser'--

`(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

`(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.'; and

(2) in section 2511(2), by inserting at the end the following:

`(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--

`(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

`(II) the person acting under color of law is lawfully engaged in an investigation;

`(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

`(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.'.

SEC. 218. FOREIGN INTELLIGENCE INFORMATION.

Sections 104(a)(7)(B) and section 303(a)(7)(B) (50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B)) of the Foreign Intelligence Surveillance Act of 1978 are each amended by striking `the purpose' and inserting `a significant purpose'.

SEC. 219. SINGLE-JURISDICTION SEARCH WARRANTS FOR TERRORISM.

Rule 41(a) of the Federal Rules of Criminal Procedure is amended by inserting after `executed' the following: `and (3) in an investigation of domestic terrorism or international terrorism (as defined in section 2331 of title 18, United States Code), by a Federal magistrate judge in any district in which activities related to the terrorism may have occurred, for a search of property or for a person within or outside the district'.

SEC. 220. NATIONWIDE SERVICE OF SEARCH WARRANTS FOR ELECTRONIC EVIDENCE.

(a) IN GENERAL- Chapter 121 of title 18, United States Code, is amended--

(1) in section 2703, by striking `under the Federal Rules of Criminal Procedure' every place it appears and inserting `using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation'; and

(2) in section 2711--

(A) in paragraph (1), by striking `and';

(B) in paragraph (2), by striking the period and inserting `; and'; and

(C) by inserting at the end the following:

`(3) the term `court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.'.

(b) CONFORMING AMENDMENT- Section 2703(d) of title 18, United States Code, is amended by striking `described in section 3127(2)(A)'.

SEC. 221. TRADE SANCTIONS.

(a) IN GENERAL- The Trade Sanctions Reform and Export Enhancement Act of 2000 (Public Law 106-387; 114 Stat. 1549A-67) is amended--

(1) by amending section 904(2)(C) to read as follows:

`(C) used to facilitate the design, development, or production of chemical or biological weapons, missiles, or weapons of mass destruction.';

(2) in section 906(a)(1)--

(A) by inserting `, the Taliban or the territory of Afghanistan controlled by the Taliban,' after `Cuba'; and

(B) by inserting `, or in the territory of Afghanistan controlled by the Taliban,' after `within such country'; and

(3) in section 906(a)(2), by inserting `, or to any other entity in Syria or North Korea' after `Korea'.

(b) APPLICATION OF THE TRADE SANCTIONS REFORM AND EXPORT ENHANCEMENT ACT- Nothing in the Trade Sanctions Reform and Export Enhancement Act of 2000 shall limit the application or scope of any law establishing criminal or civil penalties, including any executive order or regulation promulgated pursuant to such laws (or similar or successor laws), for the unlawful export of any agricultural commodity, medicine, or medical device to--

(1) a foreign organization, group, or person designated pursuant to Executive Order 12947 of January 23, 1995, as amended;

(2) a Foreign Terrorist Organization pursuant to the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104-132);

(3) a foreign organization, group, or person designated pursuant to Executive Order 13224 (September 23, 2001);

(4) any narcotics trafficking entity designated pursuant to Executive Order 12978 (October 21, 1995) or the Foreign Narcotics Kingpin Designation Act (Public Law 106-120); or

(5) any foreign organization, group, or persons subject to any restriction for its involvement in weapons of mass destruction or missile proliferation.

SEC. 222. ASSISTANCE TO LAW ENFORCEMENT AGENCIES.

Nothing in this Act shall impose any additional technical obligation or requirement on a provider of a wire or electronic communication service or other person to furnish facilities or technical assistance. A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to section 216 shall be reasonably compensated for such reasonable expenditures incurred in providing such facilities or assistance.

SEC. 223. CIVIL LIABILITY FOR CERTAIN UNAUTHORIZED DISCLOSURES.

(a) Section 2520 of title 18, United States Code, is amended--

(1) in subsection (a), after `entity', by inserting `, other than the United States,';

(2) by adding at the end the following:

`(f) ADMINISTRATIVE DISCIPLINE- If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.'; and

(3) by adding a new subsection (g), as follows:

`(g) IMPROPER DISCLOSURE IS VIOLATION- Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).

(b) Section 2707 of title 18, United States Code, is amended--

(1) in subsection (a), after `entity', by inserting `, other than the United States,';

(2) by striking subsection (d) and inserting the following:

`(d) ADMINISTRATIVE DISCIPLINE- If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or

she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.'; and

(3) by adding a new subsection (g), as follows:

`(g) IMPROPER DISCLOSURE- Any willful disclosure of a `record', as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.'.

(c)(1) Chapter 121 of title 18, United States Code, is amended by adding at the end the following:

`Sec. 2712. Civil actions against the United States

`(a) IN GENERAL- Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages--

`(1) actual damages, but not less than $10,000, whichever amount is greater; and

`(2) litigation costs, reasonably incurred.

`(b) PROCEDURES- (1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code. `(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.'.

`(3) Any action under this section shall be tried to the court without a jury.

`(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

`(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title

31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

`(c) ADMINISTRATIVE DISCIPLINE- If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the possible violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

`(d) EXCLUSIVE REMEDY- Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

`(e) STAY OF PROCEEDINGS- (1) Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).

`(2) In this subsection, the terms `related criminal case' and `related investigation' mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical.

`(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party.'.

(2) The table of sections at the beginning of chapter 121 is amended to read as follows:

`2712. Civil action against the United States.'.

SEC. 224. SUNSET.

(a) IN GENERAL- Except as provided in subsection (b), this title and the amendments made by this title (other than sections 203(a), 203(c), 205, 208, 210, 211, 213, 216, 219, 221, and 222, and the amendments made by those sections) shall cease to have effect on December 31, 2005.

(b) EXCEPTION- With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in subsection (a) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect.

SEC. 225. IMMUNITY FOR COMPLIANCE WITH FISA WIRETAP.

Section 105 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805) is amended by inserting after subsection (g) the following:

`(h) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act.'.

TITLE IX--IMPROVED INTELLIGENCE

SEC. 901. RESPONSIBILITIES OF DIRECTOR OF CENTRAL INTELLIGENCE REGARDING FOREIGN INTELLIGENCE COLLECTED UNDER FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

Section 103(c) of the National Security Act of 1947 (50 U.S.C. 403-3(c)) is amended--

(1) by redesignating paragraphs (6) and (7) as paragraphs (7) and (8), respectively; and

(2) by inserting after paragraph (5) the following new paragraph (6):

`(6) establish requirements and priorities for foreign intelligence information to be collected under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that Act is disseminated so it may be used efficiently and effectively for foreign intelligence purposes, except that the Director shall have no authority to direct, manage, or undertake electronic surveillance or physical search operations pursuant to that Act unless otherwise authorized by statute or executive order;'.

SEC. 902. INCLUSION OF INTERNATIONAL TERRORIST ACTIVITIES WITHIN SCOPE OF FOREIGN INTELLIGENCE UNDER NATIONAL SECURITY ACT OF 1947.

Section 3 of the National Security Act of 1947 (50 U.S.C. 401a) is amended--

(1) in paragraph (2), by inserting before the period the following: `, or international terrorist activities'; and

(2) in paragraph (3), by striking `and activities conducted' and inserting `, and activities conducted,'.

SEC. 903. SENSE OF CONGRESS ON THE ESTABLISHMENT AND MAINTENANCE OF INTELLIGENCE RELATIONSHIPS TO ACQUIRE INFORMATION ON TERRORISTS AND TERRORIST ORGANIZATIONS.

It is the sense of Congress that officers and employees of the intelligence community of the Federal Government, acting within the course of their official duties, should be encouraged, and should make every effort, to establish and maintain intelligence relationships with any person, entity, or group for the purpose of engaging in lawful intelligence activities, including the acquisition of information on the identity, location, finances, affiliations, capabilities, plans, or intentions of a terrorist or terrorist organization, or information on any other person, entity, or group (including a foreign government) engaged in harboring, comforting, financing, aiding, or assisting a terrorist or terrorist organization.

SEC. 904. TEMPORARY AUTHORITY TO DEFER SUBMITTAL TO CONGRESS OF REPORTS ON INTELLIGENCE AND INTELLIGENCE-RELATED MATTERS.

(a) AUTHORITY TO DEFER- The Secretary of Defense, Attorney General, and Director of Central Intelligence each may, during the effective period of this section, defer the date of submittal to Congress of any covered intelligence report under the jurisdiction of such official until February 1, 2002.

(b) COVERED INTELLIGENCE REPORT- Except as provided in subsection (c), for purposes of subsection (a), a covered intelligence report is as follows:

(1) Any report on intelligence or intelligence-related activities of the United States Government that is required to be submitted to Congress by an element of the intelligence community during the effective period of this section.

(2) Any report or other matter that is required to be submitted to the Select Committee on Intelligence of the Senate and Permanent Select Committee on Intelligence of the House of Representatives by the Department of Defense or the Department of Justice during the effective period of this section.

(c) EXCEPTION FOR CERTAIN REPORTS- For purposes of subsection (a), any report required by section 502 or 503 of the National Security Act of 1947 (50 U.S.C. 413a, 413b) is not a covered intelligence report.

(d) NOTICE TO CONGRESS- Upon deferring the date of submittal to Congress of a covered intelligence report under subsection (a), the official deferring the date of submittal of the covered intelligence report shall submit to Congress notice of the deferral. Notice of deferral of a report shall specify the provision of law, if any, under which the report would otherwise be submitted to Congress.

(e) EXTENSION OF DEFERRAL- (1) Each official specified in subsection (a) may defer the date of submittal to Congress of a covered intelligence report under the jurisdiction of such official to a date after February 1, 2002, if such official submits to the committees of Congress specified in subsection (b)(2) before February 1, 2002, a certification that preparation and submittal of the covered intelligence report on February 1, 2002, will impede the work of officers or employees who are engaged in counterterrorism activities.

(2) A certification under paragraph (1) with respect to a covered intelligence report shall specify the date on which the covered intelligence report will be submitted to Congress.

(f) EFFECTIVE PERIOD- The effective period of this section is the period beginning on the date of the enactment of this Act and ending on February 1, 2002.

(g) ELEMENT OF THE INTELLIGENCE COMMUNITY DEFINED- In this section, the term `element of the intelligence community' means any element of the intelligence community specified or designated under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

SEC. 905. DISCLOSURE TO DIRECTOR OF CENTRAL INTELLIGENCE OF FOREIGN INTELLIGENCE-RELATED INFORMATION WITH RESPECT TO CRIMINAL INVESTIGATIONS.

(a) IN GENERAL- Title I of the National Security Act of 1947 (50 U.S.C. 402 et seq.) is amended--

(1) by redesignating subsection 105B as section 105C; and

(2) by inserting after section 105A the following new section 105B:

`DISCLOSURE OF FOREIGN INTELLIGENCE ACQUIRED IN CRIMINAL INVESTIGATIONS; NOTICE OF CRIMINAL INVESTIGATIONS OF FOREIGN INTELLIGENCE SOURCES

`SEC. 105B. (a) DISCLOSURE OF FOREIGN INTELLIGENCE- (1) Except as otherwise provided by law and subject to paragraph (2), the Attorney General, or the head of any other department or agency of the Federal Government with law enforcement responsibilities, shall expeditiously disclose to the Director of Central Intelligence, pursuant to guidelines developed by the Attorney General in consultation with the Director, foreign intelligence acquired by an element of the Department of Justice or an element of such department or agency, as the case may be, in the course of a criminal investigation.

`(2) The Attorney General by regulation and in consultation with the Director of Central Intelligence may provide for exceptions to the applicability of paragraph (1) for one or more classes of foreign intelligence, or foreign intelligence with respect to one or more targets or matters, if the Attorney General determines that disclosure of such foreign intelligence under that paragraph would jeopardize an ongoing law enforcement investigation or impair other significant law enforcement interests.

`(b) PROCEDURES FOR NOTICE OF CRIMINAL INVESTIGATIONS- Not later than 180 days after the date of enactment of this section, the Attorney General, in consultation with the Director of Central Intelligence, shall develop guidelines to ensure that after receipt of a report from an element of the intelligence community of activity of a foreign intelligence source or potential foreign intelligence source that may warrant investigation as criminal activity, the Attorney General provides notice to the Director of Central Intelligence, within a reasonable period of time, of his intention to commence, or decline to commence, a criminal investigation of such activity.

`(c) PROCEDURES- The Attorney General shall develop procedures for the administration of this section, including the disclosure of foreign intelligence by elements of the Department of Justice, and elements of other departments and agencies of the Federal Government, under subsection (a) and the provision of notice with respect to criminal investigations under subsection (b).'.

(b) CLERICAL AMENDMENT- The table of contents in the first section of that Act is amended by striking the item relating to section 105B and inserting the following new items:

`Sec. 105B. Disclosure of foreign intelligence acquired in criminal investigations; notice of criminal investigations of foreign intelligence sources.

`Sec. 105C. Protection of the operational files of the National Imagery and Mapping Agency.'.

SEC. 906. FOREIGN TERRORIST ASSET TRACKING CENTER.

(a) REPORT ON RECONFIGURATION- Not later than February 1, 2002, the Attorney General, the Director of Central Intelligence, and the Secretary of the Treasury shall jointly submit to Congress a report on the feasibility and desirability of reconfiguring the Foreign Terrorist Asset Tracking Center and the Office of Foreign Assets Control of the Department of the Treasury in order to establish a capability to provide for the effective and efficient analysis and dissemination of foreign intelligence relating to the financial capabilities and resources of international terrorist organizations.

(b) REPORT REQUIREMENTS- (1) In preparing the report under subsection (a), the Attorney General, the Secretary, and the Director shall consider whether, and to what extent, the capacities and resources of the Financial Crimes Enforcement Center of the Department of the Treasury may be integrated into the capability contemplated by the report.

(2) If the Attorney General, Secretary, and the Director determine that it is feasible and desirable to undertake the reconfiguration described in subsection (a) in order to establish the capability described in that subsection, the Attorney General, the Secretary, and the Director shall include with the report under that subsection a detailed proposal for legislation to achieve the reconfiguration.

SEC. 907. NATIONAL VIRTUAL TRANSLATION CENTER.

(a) REPORT ON ESTABLISHMENT- (1) Not later than February 1, 2002, the Director of Central Intelligence shall, in consultation with the Director of the Federal Bureau of Investigation, submit to the appropriate committees of Congress a report on the establishment and maintenance within the intelligence community of an element for purposes of providing timely and accurate translations of foreign intelligence for all other elements of the intelligence community. In the report, the element shall be referred to as the `National Virtual Translation Center'.

(2) The report on the element described in paragraph (1) shall discuss the use of state-of-the-art communications technology, the integration of existing translation capabilities in the intelligence community, and the utilization of remote-connection capacities so as to minimize the need for a central physical facility for the element.

(b) RESOURCES- The report on the element required by subsection (a) shall address the following:

(1) The assignment to the element of a staff of individuals possessing a broad range of linguistic and translation skills appropriate for the purposes of the element.

(2) The provision to the element of communications capabilities and systems that are commensurate with the most current and sophisticated communications capabilities and systems available to other elements of intelligence community.

(3) The assurance, to the maximum extent practicable, that the communications capabilities and systems provided to the element will be compatible with communications capabilities and systems utilized by the Federal Bureau of Investigation in securing timely and accurate translations of foreign language materials for law enforcement investigations.

(4) The development of a communications infrastructure to ensure the efficient and secure use of the translation capabilities of the element.

(c) SECURE COMMUNICATIONS- The report shall include a discussion of the creation of secure electronic communications between the element described by subsection (a) and the other elements of the intelligence community.

(d) DEFINITIONS- In this section:

(1) FOREIGN INTELLIGENCE- The term `foreign intelligence' has the meaning given that term in section 3(2) of the National Security Act of 1947 (50 U.S.C. 401a(2)).

(2) ELEMENT OF THE INTELLIGENCE COMMUNITY- The term `element of the intelligence community' means any element of the intelligence community specified or designated under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

SEC. 908. TRAINING OF GOVERNMENT OFFICIALS REGARDING IDENTIFICATION AND USE OF FOREIGN INTELLIGENCE.

(a) PROGRAM REQUIRED- The Attorney General shall, in consultation with the Director of Central Intelligence, carry out a program to provide appropriate training to officials described in subsection (b) in order to assist such officials in--

(1) identifying foreign intelligence information in the course of their duties; and

(2) utilizing foreign intelligence information in the course of their duties, to the extent that the utilization of such information is appropriate for such duties.

(b) OFFICIALS- The officials provided training under subsection (a) are, at the discretion of the Attorney General and the Director, the following:

(1) Officials of the Federal Government who are not ordinarily engaged in the collection, dissemination, and use of foreign intelligence in the performance of their duties.

(2) Officials of State and local governments who encounter, or may encounter in the course of a terrorist event, foreign intelligence in the performance of their duties.

(c) AUTHORIZATION OF APPROPRIATIONS- There is hereby authorized to be appropriated for the Department of Justice such sums as may be necessary for purposes of carrying out the program required by subsection (a).

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Akademii Obrony Narodowej
Nr ewid. 75500

S/7595

~~orgt. Rappr. avt~~