23

AKADEMIA
OBRONY
NARODOWEJ

kmdr por. mgr inż. Ernest LICHOCKI

MODEL SYSTEMU ZARZĄDZANIA KRYZYSOWEGO W WARUNKACH ZAGROŻEŃ CYBERTERRORYSTYCZNYCH DLA BEZPIECZEŃSTWA INFORMACYJNEGO SIŁ ZBROJNYCH RZECZYPOSPOLITEJ POLSKIEJ

Rozprawa doktorska

Biblioteka Główna
Akademii Obrony Narodowej
S/7596
05-007596-001-0

75501

Warszawa

AKADEMIIA OBRONY NARODOWEJ

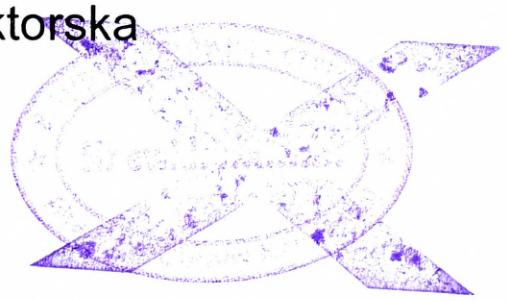
WYDZIAŁ BEZPIECZEŃSTWA NARODOWEGO

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 75501
Akademii Obrony Narodowej

kmdr por. mgr inż. Ernest LICHOCKI

MODEL SYSTEMU ZARZĄDZANIA KRYZYSOWEGO W WARUNKACH ZAGROŻEŃ CYBERTERRORYSTYCZNYCH DLA BEZPIECZEŃSTWA INFORMACYJNEGO SIŁ ZBROJNYCH RZECZYPOSPOLITEJ POLSKIEJ

Rozprawa doktorska



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

WARSZAWA **2009**



SPIS TREŚCI

WSTĘP 7

ROZDZIAŁ I
PODSTAWY METODOLOGICZNE BADAŃ ZAGROŻEŃ CYBERTERRORYSTYCZNYCH DLA BEZPIECZEŃSTWA INFORMACYJNEGO SIŁ ZBROJNYCH RP 13

1.1. Uzasadnienie wyboru tematu 13

1.2. Przedmiot badań 18

1.3. Cel badań 20

1.4. Problem badawczy 20

1.5. Założenia 22

1.6. Ograniczenia 23

1.7. Hipotezy robocze, zmienne zależne i niezależne 23

1.8. Obszar i organizacja badań 26

1.9. Metody, techniki i narzędzia badawcze 29

1.10. Charakterystyka literatury przedmiotu badań 34

1.11. Stan wiedzy na podstawie badań własnych 36

ROZDZIAŁ II
CYBERTERRORYZM JAKO NOWA FORMA ZAGROŻEŃ DLA BEZPIECZEŃSTWA 39

2.1. Teoria wojny informacyjnej 39

2.2. Podstawy teoretyczne cyberterroryzmu 51

2.3 Bezpieczeństwo informacyjne i jego zagrożenie 64

2.4. Istota Infowar, Cyberwar, Netwar 70

2.5. Sieciocentryczne pole walki 73

2.5.1. Działania w warunkach sieciocentrycznego pola walki 74

2.5.2. Technologiczne determinanty 79

2.5.3. Zagrożenia wewnętrzne i zewnętrzne 81

2.5.4. Obrona przed zagrożeniami 85

2.6. Wnioski 88

ROZDZIAŁ III
POLITYKA BEZPIECZEŃSTWA INFORMACYJNEGO POLSKI **91**

3.1. Bezpieczeństwo informacyjne Polski **91**

3.2. Infrastruktura krytyczna w Polsce **102**

3.3. Infrastruktura krytyczna w Siłach Zbrojnych Rzeczypospolitej Polski **117**

3.4. Istota operacji informacyjnych Sił Zbrojnych Rzeczypospolitej Polski **123**

3.5. Prawne regulacje polityki bezpieczeństwa informacyjnego Polski **128**

3.6. Przestępstwa cybernetyczne w prawie polskim **131**

3.7. Wnioski **135**

ROZDZIAŁ IV
MODEL SYSTEMU ZARZĄDZANIA KRYZYSOWEGO W SIŁACH ZBROJNYCH RZECZYPOSPOLITEJ POLSKI W WARUNKACH ZAGROŻEŃ CYBERTERRORYZMU **137**

4.1. Cele i zadania **137**

4.2. Wymagania i ograniczania systemowe **140**

4.3. Koncepcja funkcjonowania systemu zarządzania kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski **143**

4.4. Współpraca z resortami cywilnymi **161**

4.5. Teleinformatyczna infrastruktura systemu zarządzania kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski **164**

4.5.1. Systemy teleinformatyczne **165**

4.5.2. Ochrona kryptograficzna Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski **170**

4.6. Kierunki rozwoju systemu zarządzania kryzysowego **171**

4.7. Wnioski **173**

ZAKOŃCZENIE **175**

BIBLIOGRAFIA **181**

SPIS TABEL, RYSUNKÓW I UJĘĆ GRAFICZNYCH **191**

ZAŁĄCZNIKI **193**

1. Broń elektromagnetyczna **195**
2. Wybrane przykłady ataków cyberterrorystycznych na świecie **205**
3. Regulacje prawne normalizujące politykę bezpieczeństwa informacyjnego Polski **215**
4. Sektory oraz składniki sektorów Infrastruktury Krytycznej w wybranych państwach na świecie **225**
5. Kwestionariusz ankiety do rozprawy doktorskiej **227**
6. Raport z badań przeprowadzonych w okresie 22.02. – 01.06.2007 r. **245**
7. Spis systemów teleinformatycznych w resorcie obrony narodowej **279**

STRESZCZENIE **283**

WSTĘP

„Cyberataki nie wymagają użycia ani jednego żołnierza czy naruszenia granic, jednak mogą sparaliżować kraj. Przerwanie dostaw energii może zakłócić funkcję społeczne i ekonomiczne państwa w sposób przypominający skutki wojny. Bez jednego wystrzału."

Jaapa de Hoop Scheffer – sekretarz generalny NATO
Spotkanie ministrów obrony, Kraków, dnia 19 lutego 2009 r.

Bezpieczeństwo teleinformatyczne, to składnik bezpieczeństwa informacyjnego. W Siłach Zbrojnych Rzeczypospolitej Polski (SZRP) bezpieczeństwo informacyjne postrzegane jest jako jeden z bardzo ważnych obszarów prawidłowego funkcjonowania SZ RP. Duży wpływ wywarły również ostatnie wydarzenia w Estonii w kwietniu 2007 r., gdzie na kilka tygodni poprzez cyberatak typu DoS i DDoS[1], zostały zablokowane internetowe strony władz (prezydenta i parlamentu), partii politycznych, wszystkich ministerstw, mediów (czołowe gazety) i banków (dwa największe banki).

Zaawansowane technicznie ataki cybernetyczne, jakimi są ataki DoS i DDoS oraz użycie broni o częstotliwości radiowej [2] mogą w poważny sposób zdezorganizować pracę systemów teleinformatycznych lub ich najistotniejszych elementów funkcjonalnych oraz doprowadzić do trudnych do przewidzenia konsekwencji zarówno wewnętrznych, jak i zewnętrznych czyli negatywnych

---

[1] *Denial of Service* (DoS, odmowa usługi) — atak w cyberprzestrzeni, polegający na zablokowaniu pojedynczej usługi sieciowej, bądź zawieszeniu pracy całego serwera w taki sposób, aby konieczna była interwencja administratora. W niektórych przypadkach może on również polegać na takim przeciążeniu sieciowego serwera niezliczoną ilością zapytań, aby odwołania rzeczywistych jego użytkowników nie mogły zostać zrealizowane.
Distributed Denial of Service (DDoS, atak rozproszony odmowy usługi) - zmodyfikowana wersja ataku DoS, wprowadzająca kilka istotnych innowacji zwiększających skuteczność ataku i utrudniających zlokalizowanie agresora. Atak przeprowadzany jest z wielu komputerów na raz, w sposób ściśle skoordynowany, a sama maszyna, z której uruchamiany jest proces „cyberataku", w ogóle w nim nie uczestniczy, co utrudnia jej namierzenie.

[2] Urządzenia emitujące promieniowanie elektromagnetyczne należące do widma radiowego. Używa się jej do zniszczenia technicznych urządzeń elektronicznych oraz zbiorów informatycznych. Celowe użycie energii elektromagnetycznej o dużej mocy. Taka broń nie wymaga bezpośredniego trafienia w cel, co często bywa trudne. Zapewne największa zaletą tej broni jest to, że nosi ona etykietkę "nie zabójczej".

implikacji dla innych systemów teleinformatycznych wykorzystywanych w Siłach Zbrojnych RP.

Globalna sieć łączności, jaką jest Internet oraz systemy teleinformatyczne, stały się w obecnych czasach prowadzenia asymetrycznej walki zbrojnej nieodłączną częścią naszego codziennego życia w wojsku. Skuteczność Sił Zbrojnych RP w dobie prowadzenia działań sieciocentrycznych jest wypadkową między innymi bezpieczeństwa teleinformatycznego oraz przepustowej i niezawodnej sieci teleinformatycznej.

O zamachach cyberterrorystycznych wymierzonych w systemy teleinformatyczne i teleinformacyjne mówi wiele jawnych i niejawnych dokumentów publikowanych przez rządy wielu państw począwszy od lat 80-tych. Cyberterroryzm, nie jest zjawiskiem nowym. Sam termin pojawił się już w 1979 r., kiedy to szwedzkie Ministerstwo Obrony umieściło go w swoim raporcie o zagrożeniach komputerowych.

Należy wspomnieć, że w Tallinie w sierpniu 2008 r. powstało po wydarzeniach w Estonii, natowskie centrum ostrzegania przed cyberatakami (*NATO Cooperative Center of Exellence In Cyber Defence* - Centrum Doskonalenia Obrony przez Cyberatakami)[3]. Brak udziału personelu bezpieczeństwa teleinformatycznego z Polski w tej wyspecjalizowanej grupie zajmującej się przeciwdziałaniem skutkom cyberatakom oraz analizą powypadkową jest bardzo niepokojącym faktem.

W Stanach Zjednoczonych, prezydent Barack Obama stworzył 29.05.2009 r. stanowisko „cybercara". Ma on koordynować zabezpieczenie systemów komputerowych przed elektronicznym szpiegostwem i cyberterroryzmem. Ma on koordynować walkę z hakerami, szpiegami i cyberterrorystami. Ma on tytuł specjalnego asystenta prezydenta i biuro w strukturze Rady Bezpieczeństwa Narodowego oraz będzie współpracował z Krajową Radą Ekonomiczną w Białym Domu[4].

Po wygranych wyborach prezydent Barack Obama nadał cyberzagrożeniom rangę istotnego zagrożenia dla bezpieczeństwa narodowego. Przegląd tak zwanej „Narodowej Inicjatywy Cyberbezpieczeństwa", czyli specjalnego programu walki z przestępczością w Internecie stworzono pod koniec rządów prezydenta George'a W. Busha.

---

[3] Znane też jako K 5.

[4] Barack Obama doskonale zdaje sobie sprawę z cyberzagrozeń, ponieważ sam padł ofiarą hakerów, którzy w 2008 r. włamali się do komputerów w jego sztabie wyborczym, zdobywając informację dotyczące między innymi planów podróży kandydata na prezydenta. Należy nadmienić, że również podczas kompanii wyborczej komputery w sztabach obu kandydatów atakowali hakerzy. Chcieli oni zdobyć informacje dotyczące polityki przyszłego prezydenta.

Nakłady na ochronę sieci zwiększa także Departament Obrony, który w najbliższej przyszłości zamierza otworzyć nowe „cyberdowództwo" odpowiedzialne przede wszystkim za bezpieczeństwo sieci komputerowych. Na odnowę systemów teleinformatycznych po szkodach wyrządzonych przez szpiegów i hakerów Pentagon przeznaczył na początku roku 2009 100 milionów dolarów.

Rozprawa składa się z czterech rozdziałów oraz wstępu i zakończenia. Każdy z rozdział merytorycznych zakończony jest wnioskami, oprócz rozdziału pierwszego, który jest rozdziałem metodologicznym. Bibliografia, spis tabel, rysunków i ujęć graficznych oraz załączniki są zamieszczone w części pozamerytorycznej.

Rozdział pierwszy traktuje o metodologicznych podstawach badań i odnosi się do uzasadnienia wyboru tematu, przedmiotu badań, celu badań, problemów badawczych, hipotez roboczych oraz opisany jest stan wiedzy na podstawie badań własnych z charakterystyką literatury przedmiotu badań.

W rozdziale drugi przedstawiono elementy wojny informacyjnej oraz podstawy teoretyczne cyberterroryzmu. Opisano też zagrożenia dla rozwoju społeczeństwa informatycznego oraz przedstawiono istotę *Infowar, Cyberwar i Netwar*. W tym rozdziale pokazano również aspekty sieciocentrycznego pola walki (ang. NCW – *Network Centric Warfare*), a mianowicie opisano: działania w warunkach NCW, technologiczne determinanty oraz zagrożenia wewnętrzne i zewnętrzne.

Trzeci rozdział zawiera analizę polityki bezpieczeństwa informacyjnego państwa oraz Sił Zbrojnych Rzeczypospolitej Polskiej. Przedstawiono analizę bezpieczeństwa informacyjnego Polski, opisano Infrastrukturę Krytyczną oraz pokazano, na podstawie badań przeprowadzonych w 2007 r. Infrastrukturę Krytyczną w Siłach Zbrojnych RP. Należy nadmienić, że jest to pierwsza próba zdefiniowania tego zagadnienia. Rozdział ten zawiera również zagadnienia związane z prawnymi regulacjami polityki bezpieczeństwa informacyjnego Polski i opisane zostały przestępstwa informatyczne ujęte w prawie polskim.

W czwartym rozdziale sformułowano model funkcjonowania systemu zarządzania kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski w warunkach zagrożeń cyberterroryzmu. Przedstawiono w nim cele i zadania systemu, wymagania i ograniczania systemowe dla systemu oraz koncepcję funkcjonowania systemu zarządzania kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski. W modelu tym

opisano również zagadnienie związane ze współpracą z resortami cywilnymi. Zaprezentowano w modelu bardzo szczegółowe zadania poszczególnych elementów trójszczeblowego systemu zarządzania kryzysowego. Przedstawiony model opisuje również najbardziej skomplikowane relację wymiany informacji zachodzące w poszczególnych elementach składowych tego systemu. W podsumowaniu, rozdział zawiera kierunki rozwoju systemu zarządzania kryzysowego.

Zakończenie rozprawy doktorskiej zawiera określenie stopnia osiągnięcia celu badań oraz weryfikację hipotez roboczych.

W załącznikach pokazano materiał wspierający proces badań oraz zebrano istotne informacje, dotyczące bezpieczeństwa teleinformatycznego. Zamieszczono również kwestionariusz ankiety oraz wyniki z przeprowadzonych badań dotyczących Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.

Niniejsze rozprawa doktorska może być wykorzystana przez środowiska akademickie oraz personel bezpieczeństwa teleinformatycznego Sił Zbrojnych RP.

* * *

Przez cały okres mojej służby zawodowej do roku 2007, zajmowałem się praktycznie obszarem działań związanym z bezpieczeństwem teleinformatycznym. Pracowałem w strukturach bezpieczeństwa kryptograficznego Marynarki Wojennej RP od szczebla okrętu do flotylli. Byłem czynnie zaangażowany w proces wdrażania narodowych i sojuszniczych dokumentów, narzędzi i urządzeń ochrony teleinformatycznej (urządzeń ochrony kryptograficznej). Brałem również udział w kursach bezpieczeństwa teleinformatycznego[5], konferencjach, spotkaniach sojuszniczych grup roboczych, kontaktach i konsultacjach z osobami funkcyjnymi narodowych i sojuszniczych władz bezpieczeństwa i służb ochrony państwa. Od roku 2005 prowadziłem zajęcia dydaktyczne (przez okres trzech lat) z zakresu problematyki bezpieczeństwa informacji oraz bezpieczeństwa teleinformatycznego

---

[5] Zaoczne studia podyplomowe w zakresie bezpieczeństwa informacyjnego - Akademia Obrony Narodowej (AON) - 2005 r.;
UHF Systems Technical (A – 101 – 0138) - 2000 r.;
Crypto Custodian Course – 2000 r.;
Link - 11 Course – 2001 r.;
Communications Course in NATO Procedures – 2001 r.;
Operator and Maintainer Familiarizations Course Integrated Communication System ORKAN Class - 2003 r.;
Operation and Maintenance Training for the Link – 11 Cryptographic Device the Multi Link Encrypted – 2005 r.;
Ochrona danych osobowych i informacji niejawnych w praktyce – 2007 r.

w Akademii Marynarki Wojennej i Wyższej Szkole Międzynarodowych Stosunków Gospodarczych i Politycznych w Gdyni.

W tym miejscu chcę podziękować personelowi bezpieczeństwa teleinformatycznego Wojskowego Biura Bezpieczeństwa Łączności i Informatyki Sił Zbrojnych, którzy przyczynili się do powstania tej dysertacji. Trudno by było znaleźć gdziekolwiek lepszą grupę współpracowników. Specjalne podziękowania należą się dla Pana płk Dariusza Osmólskiego.

Chcę także podziękować obecnemu i byłemu personelowi służb ochrony państwa, zajmującemu się problematyką bezpieczeństwa teleinformatycznego, którzy poświęcali mi swój czas i umożliwiali z korzystania z ekspertyz i raportów.

Jestem również wdzięczny Panu gen. broni w st. spocz. dr hab. inż. Józefowi Buczyńskiemu, byłemu rektorowi Akademii Obrony Narodowej, za pomoc w przeprowadzeniu badań nad Infrastrukturą Krytyczną Sił Zbrojnych Rzeczypospolitej Polski na potrzeby rozprawy doktorskiej.

Na specjalne podziękowanie zasłużyli również moi rodzice i moja rodzina. Dziękuję: Mamie, Tacie oraz Żonie i Synowi za duchowe wsparcie podczas pisania niniejszej dysertacji, zwieńczone zakończeniem dzieła.

Pragnę serdecznie podziękować mojemu promotorowi Panu płk w st. spocz. prof. dr hab. inż. Piotrowi Sienkiewiczowi za podtrzymaniu mnie na duchu i wierze o zasadności pracy nad tematem rozprawy doktorskiej. Niniejsza praca bez wsparcia Pana Profesora na pewno by nie powstała.

ROZDZIAŁ I

PODSTAWY METODOLOGICZNE BADAŃ ZAGROŻEŃ CYBERTERRORYSTYCZNYCH DLA BEZPIECZEŃSTWA INFORMACYJNEGO SIŁ ZBROJNYCH RP

1.1. Uzasadnienie wyboru tematu

Problem bezpieczeństwa teleinformatycznego w Siłach Zbrojnych Rzeczypospolitej Polski, stał się postrzegany przez instytucje Ministerstwa Obrony Narodowej jako jeden z bardzo ważnych obszarów prawidłowego funkcjonowania Sił Zbrojnych RP[6]. Na zmianę poglądów istotny wpływ wywołały wydarzenia w Estonii w kwietniu 2007 r., gdzie na kilka tygodni poprzez cyberatak typu DoS i DDoS, zostały zablokowane internetowe strony władz Estonii (prezydenta i parlamentu), partii politycznych, wszystkich ministerstw, mediów (czołowe gazety) i banków (dwa największe banki). Po pierwszej fali ataków zostały zablokowane kolejno strony firm komunikacyjnych i przedsiębiorstw transportowych. Zostały uszkodzone łącza teleinformatyczne z Unią Europejską i NATO[7]. Straty, wynikłe z zakłócenia działalności tych instytucji, szacuje się na miliony euro[8].

Autor w niniejszej rozprawie doktorskiej przyjął, że zaawansowane technicznie ataki cybernetyczne, wykorzystujące słabość systemów teleinformatycznych wykorzystywanych w Sił Zbrojnych RP, mogą w poważny sposób zdezorganizować pracę lub ich najistotniejszych elementów funkcjonalnych oraz doprowadzić do trudnych do przewidzenia konsekwencji zarówno wewnętrznych,

---

[6] Lichocki E., *Bezpieczeństwo teleinformatyczne Sił Zbrojnych Rzeczypospolitej Polski w dobie zagrożeń cybernetycznych*, Konferencja naukowa „Cyberterroryzm nowe wyzwania XXI wieku", Wyższa Szkoła Informatyki , Zarządzania i Administracji, Warszawa 18.05.2009 r. oraz Jemioło T., Kisielnicki J., Rajchel K., *Cyberterroryzm nowe wyzwania XXI wieku*, Wyższa Szkoła Policji, Warszawa 2009 r. s. 582.

[7] Głównymi celami ataków w Estonii były: główny serwer DNS.ee, strony internetowe prezydenta, rządu, parlamentu, resortu spraw zagranicznych, policji, największe banki, np. SEB Eesti Uhisbank, Hansapank (atak przy użyciu 85000 komputerów, około 5 mln zapytań na minutę), strony internetowe gazet Postimees i Ariaev, serwery telefonii komórkowej EMT, firmy telekomunikacyjne Elion i Elisa i autonomiczne systemy routerów (AS).

[8] Lichocki E., *Cyberterrorystyczne zagrożenie dla bezpieczeństwa teleinformatycznego państwa polskiego*, Instytut Badań Systemowych PAN Polskie Towarzystwo Badań Operacyjnych i Systemowych, Warszawa 2008 r. s. 179.

jak i zewnętrznych czyli negatywne implikacje dla innych systemów teleinformatycznych wykorzystywanych w Siłach Zbrojnych.

Internet oraz szeroko rozumiany sprzęt teleinformatyczny stał się w XXI wieku nieodłączną częścią działania Sił Zbrojnych RP. Należy uświadomić, że skuteczność Sił Zbrojnych RP w dobie prowadzenia działań sieciocentrycznych jest wypadkową między innymi bezpieczeństwa teleinformatycznego oraz pożądanej przepustowości i niezawodnej sieci teleinformatycznej.

O niebezpieczeństwie zamachów cyberterrorystycznych wymierzonych w systemy teleinformatyczne przy pomocy urządzeń teleinformatycznych mówi wiele jawnych i niejawnych dokumentów publikowanych przez rządy wielu państw począwszy od lat 80-tych.

Cyberterroryzm jest w dobie społeczeństwa informacyjnego i prowadzenia działań sieciocentrycznych jednym z najpoważniejszych zagrożeń, bo w odróżnieniu od klasycznego terroryzmu ataków dokonuje się w cyberprzestrzeni. Zjawisko to stanowi, zagrożenie bezpieczeństwa teleinformatycznego dla państwa polskiego i Sił Zbrojnych RP. Cyberterroryzm jest zjawiskiem z pogranicza różnych obszarów takich jak: bezpieczeństwa teleinformatycznego, technologii teleinformatycznej, bezpieczeństwa osobowego, bezpieczeństwa elektromagnetycznego, bezpieczeństwa fizycznego oraz regulacji prawnych narodowych i międzynarodowych.

Z analizy literatury przedmiotu, należy wysunąć wniosek, że cyberataków nie prowadzą tylko ugrupowania terrorystyczne, które posiadają w swoim orężu nowoczesne narzędzia teleinformatyczne wymuszające przemoc w sieci. Sprawcami tych ataków mogą być również: hakerzy, aktywiści, crackerzy, frustraci, wandale, szpiedzy, ruchy narodowo – wyzwoleńcze oraz służby ochrony państwa, czy też podmioty gospodarcze operujące w sieciach teleinformatycznych[9]. Cyberatakiem na systemy teleinformatyczne obezwładnić można system obronny państwa. Rozważania te na obecnym poziomie wiedzy informatycznej nie są już tylko elementami fantastyki czy prac naukowych, ale stały się faktem, będąc podstawą scenariuszy walki informacyjnej. Niejednokrotnie wiele państw na świecie lekceważy fakt, że cyberterrorystyczne ataki mogą przerodzić się w zagrożenie dla bezpieczeństwa narodowego i międzynarodowego.

W teoretycznych rozważaniach należy się zastanowić, dlaczego wojskowi w krajach gdzie infrastruktura teleinformatyczna jest szeroko rozwinięta, obecnie

[9] Ibidem, s. 180.

uważają cyberterroryzm za jedno z najważniejszych wyzwań XXI wieku. Istnieją bardzo istotne powody, które mogą skłonić terrorystów do ataków w cyberprzestrzeni (Tabela 1.1.).

Tabela 1.1. Powody, które skłaniają terrorystów do ataku w cyberprzestrzeni

Powód	***Wywierany wpływ na bezpieczeństwo informacyjne***	***Identyfikacja zagrożeń***
Niskie koszty przeprowadzenia ataku	Każdy może zostać cyberterrorystą. Wystarczy mieć komputer lub laptopa, odpowiedni program i trochę umiejętności.	**Krytyczna Infrastruktura Teleinformatyczna Sił Zbrojnych Rzeczypospolitej Polski**[10]
Działania nad wyznaczonymi granicami państw	Nie wiadomo, skąd pochodzi atak, kto atakuje i kto za tym atakiem stoi.	
Przewidywanie zagrożeń ataków.	Nie wiadomo, które zagrożenie jest realne, a które tylko pozorne.	
Wykrycie i zlokalizowanie cyberataków	Nie wiadomo, jakie są zdolności i intencje atakujących.	
Cel ataku	Nie wiadomo, co będzie dokładnie celem ataku, ani w jaki sposób będzie on wykonany.	
Budowa koalicji	Nie wiadomo, kto jest w koalicji, a kto nieprzyjacielem.	

Źródło: opracowanie własne według: Bógdał – Brzezińska A., Gawrycki M. F., *Cyberterroryzmi problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003 r.

W Tallinie w sierpniu 2008 r. powstało natowskie centrum ostrzegania przed cyberatakami, Centrum Doskonalenia Obrony przez Cyberatakami. Porozumienie w sprawie powołania Centrum, podpisano 14 maja 2008 r. Lokalizacja Centrum w Tallinie nie jest przypadkowa, wybór Tallina, jego lokalizacja ma wymiar symboliczny. Personel i fundusze dostarcza siedem krajów Sojuszu: Estonia, Łotwa, Litwa, Niemcy, Włochy, Hiszpania i Słowacja[11]. Stany Zjednoczone dołączą do projektu w charakterze obserwatora, a inne kraje członkowskie być może przyłączą się później. Amerykański generał James Mattis, odpowiadający za modernizację sił zbrojnych NATO, powiedział: „że w tym wspólnym wysiłku chodzi o to, by zebrać się w jednym miejscu najlepszych ludzi od cyberterroryzmu". W Centrum pracuje kilkudziesięciu pracowników (specjalistów) od cyberterroryzmu. Prowadzą oni badania i szkolenia w dziedzinie walki z cyberterroryzmem. Są oni

[10] Krytyczna Infrastruktura Teleinformatyczna: obejmująca systemy teleinformatyczne niezbędne dla prowadzenia podstawowych działań i funkcjonowania Sił Zbrojnych RP.
[11] Finlandia, jako kraj neutralny, zamierza w roku 2009 przystąpić do programu.

także gotowi do pomocy krajom NATO w razie przyszłych cyberataków na ich sieci komputerowe. Formalne otwarcie centrum zaplanowano na 2009 r.

Brak udziału Polski w tej grupie jest bardzo niepokojący. Nasz kraj może spotkać taki podobny los, co Estonię. Przykładem jest kryzys energetyczny w północno-zachodniej Polsce, który pokazał, że nie jesteśmy przygotowani na tego typu sytuacje. Precyzyjny wymierzony atak cyberterrorystów, może wywołać bardzo podobne następstwa.

Zaawansowane technicznie ataki cybernetyczne, typu DoS lub DDoS, mogą być przeprowadzone na następujące systemy teleinformatyczne wykorzystywane w SZ RP:

- systemy dowodzenia i kierowania obronnością Sił Zbrojnych (Państwa);
- systemy kontroli i naprowadzania lotnictwa;
- satelitarne i radiowe systemy nawigacyjne;
- systemy łączności radiowej;
- systemy łączności cyfrowej;
- systemy łączności satelitarnej;
- zautomatyzowane systemy dowodzenia;
- systemy kierowania systemami walki;
- systemy rozpoznania;
- systemy teleinformatyczne, bazy danych, oprogramowanie;
- systemy opto – elektroniczne techniki bojowej;
- systemy powiadamiania;
- stacjonarne i mobilne systemy telekomunikacyjne (sieci wymiany informacji).

W realiach państwa polskiego najbardziej prawdopodobne są cyberataki na eksploatowane cywilne systemy teleinformatyczne. Poziom zabezpieczenia tych systemów jest niższy niż wojskowych systemów teleinformatycznych. W latach 2007 – 2008 również były przeprowadzone cyberataki na strony administrowane przez Siły Zbrojne RP[12].

W Polsce tak jak w innych krajach europejskich obserwuje się ciągły rozwój technologii teleinformatycznej, a co idzie za tym, rozwój sieci bezprzewodowych. Brak uświadomienia niebezpieczeństwa wynikającego z niedostatecznych zabezpieczeń teleinformatycznych sieci bezprzewodowych przed cyberatakiem jest

---

[12] Dla przykładu, w 2007 r. dwa razy, zostały zaatakowane internetowe witryny Ministerstwa Obrony Narodowej (serwer Dowództwa Operacyjnego i Departamentu Kadr MON).

głównym zagrożeniem dla bezpieczeństwa teleinformatycznego jednostek organizacyjnych podległych Ministerstwu Obrony Narodowej. Brak dostatecznego wykształcenia czy wyobraźni administratorów sieci może prowadzić do szkód trudnych do oszacowania.

Obecnie ryzyko wystąpienia ataku cyberterrorystycznego wymierzonego w Krytyczną Infrastrukturę Teleinformatyczną Sił Zbrojnych Rzeczypospolitej Polski mimo, że dotychczas nie odnotowano żadnego zdarzenia spełniającego warunki kwalifikacji według definicji, do kategorii cyberataku. Istotnym zadaniem obecnie jest, umiejętność wykrywania incydentów w cyberprzestrzeni i zabezpieczenia się przed ich oddziaływaniem na podsektory infrastruktury.

Nie istnieje jasna, przejrzysta wizja cyberprzestrzeni, dlatego nie ma żadnego punktu skąd moglibyśmy dostrzec nadchodzące ataki i obserwować ich rozprzestrzenianie się. Cyberprzestrzeń z Internetem stworzyła istotne zależności, które w nieprzewidywalny i groźny sposób zmieniają swoją naturę. Systemy teleinformatyczne, a szczególnie oprogramowanie zawarte w nich mają wiele słabych punktów, które mogą umożliwić przeprowadzenia cyberataku obniżając w istotny sposób bezpieczeństwo teleinformatyczne i informacyjne.

Należy nadmienić, że wiele organizacji terrorystycznych (np. Hamas, Al Kaida) dostrzegło możliwości prowadzenia działań terrorystycznych w cyberprzestrzeni, zwłaszcza przeciw państwom Unii Europejskiej, w coraz większym stopniu uzależnionych od systemów teleinformatycznych. Niemniej jednak, ewentualność prowadzenia działalności cyberterrorystycznej jest obecnie znacznie ograniczona, głównie ze względu na brak wykwalifikowanych kadr informatycznych. Dlatego zagrożenie wyżej wymienionych systemów ze strony terrorystów wydaje się obecnie niewielkie, gdyż przeprowadzone przez nich cyberataki są w większości prymitywne pod względem formy i łatwe do zneutralizowania. Duże zagrożenie stanowią natomiast nieliczne dotychczas, profesjonalne grupy hakerskie, działające w imieniu organizacji terrorystycznych, przede wszystkim z powodów ideologicznych, a rzadziej finansowych. Wydaje się, że w przyszłości działania cyberterrorystyczne będą niszową formą działań terrorystycznych lub składową wojny informacyjnej co pokazały nam wydarzenia w Estonii, Litwie i Gruzji.

W tym miejscu należy nadmienić, że w Ministerstwie Obrony Narodowej prowadzone są prace nad zintegrowanym, trójszczeblowym Systemem Reagowania na Incydenty Komputerowe (SRnIK) Ministerstwa Obrony Narodowej. Jak najszybsze zakończenie prac i uzgodnień pomiędzy poszczególnymi departamentami

Ministerstwa Obrony Narodowej i Służbami Ochrony Państwa (dotyczy to Służby Kontrwywiadu Wojskowego), jest warunkiem aby prawidłowo zabezpieczyć bezpieczeństwo teleinformatyczne w resorcie.

Prawdopodobieństwo wystąpienia zagrożeń związanych z przeprowadzeniem ataków typu DoS i DDoS (cyberataków) zwiększają zdarzenia zaistniałe w ostatnim okresie. Na podstawie oświadczeń przedstawicieli rosyjskiej armii, dotyczącej „asymetrycznej odpowiedzi" wygłaszanych w kontekście planów rozmieszczenia elementów tarczy antyrakietowej w Polsce i Czechach, pojawia się szereg spekulacji co do jej charakteru.[13] Może tu chodzić o atak zbliżony do tego jaki miał miejsce w Estonii i Gruzji. **Biorąc pod uwagę charakter i kontekst przeprowadzonych wcześniej cyberataków na wymienione powyżej kraje oraz możliwe prawdopodobne ataki lub incydenty[14] w związku z zaangażowaniem militarnym i dyplomatycznym Polski, cyberatak na instytucje rządowe (np. Kancelarię Prezydenta RP, Ministerstwo Obrony Narodowej lub Ministerstwo Spraw Zagranicznych) wydaje się być prawdopodobny.**

Aby zapewnić ochronę przed cyberterroryzmem należy **określić właściwą i jednolitą politykę bezpieczeństwa informacyjnego (teleinformatycznego) Sił Zbrojnych Rzeczypospolitej Polski.**

1.2. Przedmiot badań

Identyfikacja przedmiotu badań jest zawsze procesem myślowym poprzedzającym proces badawczy. Proces badawczy rozpatruje się jako: „Postępowanie, którego celem jest poznanie nieznanych lub mało znanych przemian stanowiących fragment jakieś wybranej rzeczywistości"[15]. Badanie naukowe odnosi się do rzeczywistości, jakkolwiek jest traktowane, jako: „Wieloetapowy proces zróżnicowanych wewnętrznie działań, które mają zapewnić obiektywne, dokładne i wyczerpujące poznanie wybranego wycinka rzeczywistości"[16] albo pojmowane jest

---

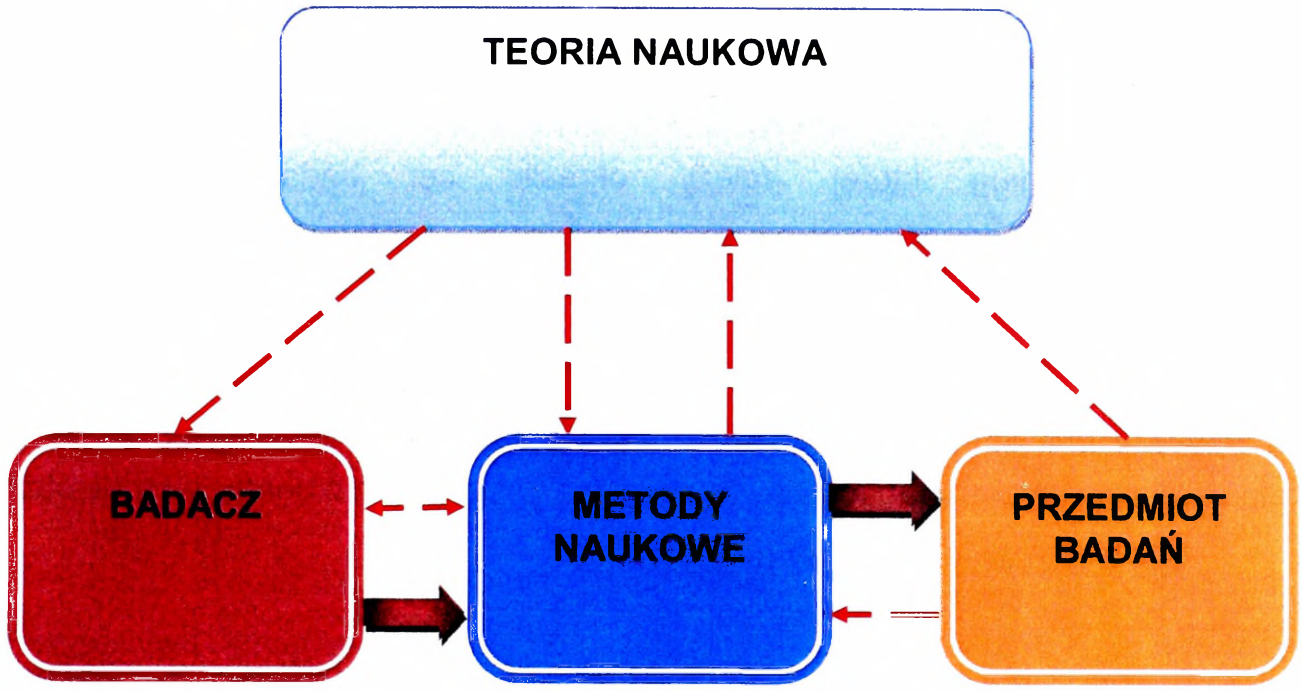
[13] Pismo z dnia 12.08.2008 r. Biura Bezpieczeństwa Narodowego Departamentu Bezpieczeństwa Wewnętrznego skierowane do Szefa Biura Bezpieczeństwa Narodowego w sprawie zagrożeń w cyberprzestrzeni.

[14] W dniu 11.08.2008 r. rosyjski ambasador na Łotwie Aleksander Wieszniakow ostrzegł Polskę i kraje nadbałtyckie, że „będą musiały zapłacić" za ostrą krytykę Rosji w jej konflikcie z Gruzją. Wiceszef rosyjskiej dyplomacji Grigorij Karasin nazwał deklaracje Polski i krajów nadbałtyckich cyniczną i niefortunną.

[15] Kolman R., *Poradnik dla doktorantów i habilitantów*, Bydgoszcz 1996 r.

[16] Żaczyński W., *Praca badawcza nauczyciela*, Warszawa 1995 r.

jako: „Próba poznania wybranej rzeczywistości lub jej części za pomocą metody naukowej”[17]. Korzystając z wiedzy o metodzie, którą umożliwia poznanie przedmiotu badań (Rys. 1.1.) i odpowiada na pytania jak badać, aby zachodził proces naukowy[18].



Rysunek 1.1. Relacje przy doborze metod naukowych i określeniu przedmiotu badań

Źródło: Opracowano na podstawie: Sienkiewicz P., *Seminaria doktoranckie*, AON, Warszawa 2008 r.

Metoda naukowa powinna, aby zachodził proces naukowy, pozwolić na poszukiwania odpowiedzi na pytania:

- kto ma prowadzić badania? — podmiot (badacz);
- co ma być badane? — przedmiot badań;
- po co to robić? — cel badań;
- jak? — metody badawcze;
- czym? — narzędzia badawcze (sens fizyczny);
- kiedy? — czas badań.

Na tej podstawie zdefiniowano i osadzono w otaczającej rzeczywistości Sił Zbrojnych Rzeczypospolitej Polski przedmiot badań dla potrzeb badawczych niniejszej dysertacji.

---

[17] Cieślarczyk M., *Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich*, AON, Warszawa 2006 r. s. 27.

[18] Sienkiewicz P., *Cykl wykładów: Metodologia badań naukowych*, ASG (AON), Warszawa 1992 r.

Przedmiot badań rozprawy doktorskiej są Siły Zbrojne Rzeczypospolitej Polski (Marynarka Wojenna, Wojska Lądowe oraz Wojska Lotnicze) jako obiekt zagrożeń cyberterrorystycznych, a w szczególności Krytyczna Infrastruktura Teleinformatyczna (KITI) Sił Zbrojnych Rzeczypospolitej Polski.

1.3. Cel badań

Postępując zgodnie z przyjętą strategią postępowania przyjmujemy procedury badawcze, według której należy określić cel badań przy założeniu, że będzie on pozostawał w ścisłej korelacji z problemem naukowym oraz postawioną hipotezą.

Istotnym dla procesu badawczego jest uzasadniona pewność[19] ze zgromadzone informacje, są wystarczające i spełniają warunki dla formułowania celu badań i problemu naukowego są w związku logicznym z postawiona hipotezą.

Jako cel główny rozprawy przyjęto:

Opracowanie modelu systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa Sił Zbrojnych Rzeczypospolitej Polski.

Z głównego celu badań wynikają następujące cele szczegółowe rozprawy:

- identyfikacja Krytycznej Infrastruktury Teleinformatycznej (KITI) w Siłach Zbrojnych Rzeczypospolitej Polski.
- określenie elementów systemu ochrony zasobów teleinformatycznych niezbędnych dla prawidłowego funkcjonowania KITI Sił Zbrojnych Rzeczypospolitej Polski.

1.4. Problem badawczy

Ważnym elementem pracy jest sformułowanie i postawienie problemu badawczego, postrzeganego jako kwestia do rozwiązania, stawiana w formie

[19] Uważamy jakiś osąd za pewny, jeśli nie wątpimy w jego prawdziwość. Blackburn S., *Oksfordzki słownik filozoficzny*, KiW, Warszawa 2004 r.

pytania. Powinien on pozostawać w silnych związkach z celami pracy. Stawiany problem powinien być przy tym odzwierciedleniem nie tyle kategorii źródeł, do jakich ma dostęp badacz, lecz także wyrazem wątpliwości w postaci pytań[20].

Sformułowanie problemu badawczego jest więc początkiem rzeczywistych badań. Jego sprecyzowanie uzasadnienie oraz wyłuszczenie pytań określających jego istotę stanowią podstawowe zadanie każdej pracy badawczej[21].

Problem badawczy wynika z zadanej sytuacji problemowej i stanowi ogólnie sformułowane pytania (z reguły złożone), na które nie mamy gotowej odpowiedzi. W zależności od stopnia złożoności sytuacji problemowej pytanie (pytania) mogą mieć charakter rozstrzygnięcia lub dopełnienia[22].

Przy formułowaniu problemu badawczego winny być przestrzegane określone warunki poprawności:

- problem badawczy musi określać efektywność poszukiwanych działań;
- musi być empirycznie rozstrzygalny;
- musi mieć wartość praktyczną.

Problematyka bezpieczeństwa Sił Zbrojnych Rzeczypospolitej Polski, w tym bezpieczeństwo teleinformatyczne ma szczególnie złożoną istotę i nie może być sprowadzone do prostych poszukiwań wybranych płaszczyzn, czynników lub zmiennych mających udowodnić wpływ lub zależność. Prawdziwy wymiar bezpieczeństwa Sił Zbrojnych RP nie może być uchwycony jedynie w postaci „generalizacji statystycznej". Bezpieczeństwo teleinformatyczne Sił Zbrojnych RP jest w okresie dynamicznych zmian technologicznych i społeczno – ekonomicznych. Biorąc pod uwagę uwarunkowania wewnętrzne i zewnętrzne można przyjąć, że główny problem badawczy niniejszej rozprawy polega na:

Jaki jest aktualny poziom zabezpieczenia Krytycznej Infrastruktury Teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polski przed zagrożeniami cyberterrorystycznymi oraz jakie działania należy podjąć, aby zapewnić prawidłowy poziom bezpieczeństwa informacyjnego Sił Zbrojnych Rzeczypospolitej Polski?

---

[20] Stachowiak Z., *Metodyka i metodologia pisania prac kwalifikacyjnych*, AON, Warszawa 2001 r. s. 58.
[21] Pieter J., *Praca naukowa*, Śląsk, Katowice 1960 r. s. 55.
[22] Ajdukiewicz K., *Logika pragmatyczna*, PWN, Warszawa 1965 r. s. 15.

Wychodząc z tak zdefiniowanego głównego problemu badawczego można wskazać następujące, niżej wymienione szczegółowe problemy badawcze:

1. **W jaki sposób można zabezpieczyć podmioty właściwe wchodzące w skład Infrastruktury Krytycznej w Sił Zbrojnych Rzeczypospolitej Polski przed atakami cyberterrorrystycznymi?**

2. **Czy cyberterroryzm stanowi zagrożenie realne dla bezpieczeństwa Sił Zbrojnych Rzeczypospolitej Polski do 2015 r.?**

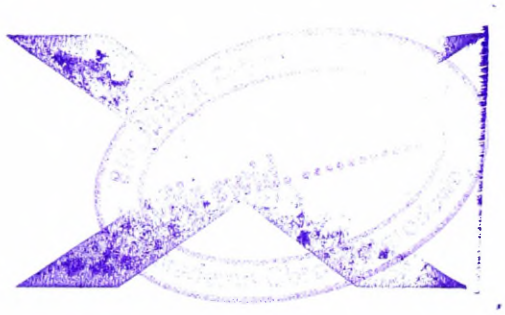
3. **Jakie czynniki kształtują politykę bezpieczeństwa informacyjnego Sił Zbrojnych Rzeczypospolitej Polski, w jakim stopniu uwzględniają one zagrożenie cyberterrorystyczne?**

Przedstawiony powyżej problem badawczy i szczeblowe problemy badawcze nie wyczerpują wszystkich zagadnień związanych z zagrożeniem cyberterrorystycznym i bezpieczeństwem teleinformatycznym, które należy podjąć realizując projektowany temat badań. Konieczne jest ich dalsze rozwijanie w kolejnych etapach procesu badawczego i również podjęcie badań ewaluacyjnych, aby dać pełniejsze odpowiedzi na tak postawione problemy.

1.5. Założenia

W niniejszej rozprawie doktorskiej przyjęto następujące założenie:

Bezpieczeństwo informacyjne (teleinformatycznego) w Siłach Zbrojnych Rzeczypospolitej Polski jest jednym z krytycznych obszarów prawidłowego funkcjonowania Sił Zbrojnych RP.



1.6. Ograniczenia

W niniejszej rozprawie doktorskiej przyjęto następujące ograniczenia:

1. **Obiektem są jednostki bojowe Sił Zbrojnych Rzeczypospolitej Polski Marynarki Wojennej, Wojsk Lądowych oraz Sił Powietrznych (od związku taktycznego do związków operacyjnych, z wyłączeniem samodzielnych jednostek szczebla niższego).**
2. **Badaniem nie zostały objęte jednostki Wojsk Specjalnych.**
3. **Zakres informacji, która została poddana badaniom, nie stanowi, w myśl Ustawy,[23] tajemnicy służbowej ani państwowej.**

1.7. Hipotezy robocze, zmienne zależne i niezależne

Na podstawie własnych doświadczeń z działalności związanej z procesem integracji Sił Zbrojnych Rzeczypospolitej Polski do Organizacji Traktatu Północnoatlantyckiego (wdrażanie sojuszniczych systemów ochrony kryptograficznej w Marynarce Wojennej RP), aktywności zawodowej w obszarze bezpieczeństwa teleinformatycznego i w wyniku dokonanej analizy systemów bezpieczeństwa teleinformatycznego Unii Europejskiej i krajów wchodzących w skład Paktu Północnoatlantyckiego – po przeanalizowaniu i zapoznaniu się z literaturą przedmiotu i z wynikami dotychczasowych badań – autor przyjął w rozprawie następujące hipotezy robocze:

HIPOTEZA 1

W pierwszej dekadzie XXI w. jest możliwe stworzenie skutecznego i niezawodnego systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla Sił Zbrojnych Rzeczypospolitej Polski.

---

[23] Ustawa z dnia 22 stycznia 1999 r. *O ochronie informacji niejawnych* Tekst ujednolicony po zmianach z dnia 15 kwietnia 2005 r. Dz. U. 1999.11.95; Tekst ujednolicony Dz. U. 2005.196.1631 - akty zmieniające.

HIPOTEZA 2

Aktualny stan bezpieczeństwa Krytycznej Infrastruktury Teleinformacyjnej jest niezadowalający, gdyż brak jest jednolitej polityki bezpieczeństwa teleinformatycznego Sił Zbrojnych Rzeczypospolitej Polski oraz państwa polskiego.

HIPOTEZA 3

W systemie bezpieczeństwa teleinformatycznego, pomimo wprowadzanych zmian legislacyjnych, strukturalnych, organizacyjnych i technicznych - nadal występują liczne niedociągnięcia organizacyjne, braki w świadomości i wyszkoleniu osób funkcyjnych (personel bezpieczeństwa teleinformatycznego), ma miejsce opóźnienie we wprowadzaniu wspólnych sojuszniczych zasad, zawartych w dokumentach normatywnych.

HIPOTEZA 4

Duża liczba stwierdzonych naruszeń bezpieczeństwa teleinformatycznego świadczy o braku lub o niskiej efektywności istniejących zabezpieczeń, narzędzi analizy zagrożeń oraz mechanizmów ich wprowadzania.

HIPOTEZA 5

Ze względu na trwający proces ujednolicania standardów narodowych, utrudniona jest współpraca międzynarodowa i wymiana informacji podlegających ochronie, a udział w programach wdrożeniowych nie jest w pełni efektywny. Służby ochrony państwa (ABW, SKW) wydają dyrektywy i rozporządzenia nie konsultując się wzajemnie.

HIPOTEZA 6

Zastosowanie nowoczesnych technik pomiaru jakości bezpieczeństwa teleinformatycznego oraz wykorzystanie szansy rozszerzenia profilu kształcenia i szkolenia z dziedziny bezpieczeństwa informacyjnego - wystąpi możliwość zapewnienia bezpieczeństwa teleinformatycznego Sił Zbrojnych Rzeczypospolitej Polski.

HIPOTEZA 7

Upowszechnienie nowoczesnych metod i narzędzi pomiaru i analizy zagrożeń bezpieczeństwa teleinformatycznego przy jednoczesnym właściwym doborze treści, form i środków kształcenia i szkolenia stanowi jeden z istotnych warunków bezpieczeństwa Sił Zbrojnych Rzeczypospolitej Polski.

W wyniku określenia przedmiotu badań i analizy zależności pomiędzy zagadnieniami określonymi jako szczegółowe problemy badawcze, autor wyróżnił następujące zmienne:

Zmienne zależne:

- wartość informacji;
- jakość narzędzi analizy bezpieczeństwa teleinformatycznego;
- jakość metod szkolenia w zakresie bezpieczeństwa teleinformatycznego;
- nakłady na bezpieczeństwo teleinformatyczne.

Zmienne niezależne:

- stan prawny w zakresie bezpieczeństwa teleinformatycznego;
- normy narodowe w zakresie bezpieczeństwa teleinformatycznego;
- kryteria i atrybuty bezpieczeństwa;
- dostosowanie standardów bezpieczeństwa teleinformatycznego Sił Zbrojnych Rzeczypospolitej Polski do wymogów NATO.

Doboru i zakwalifikowania zmiennych zależnych i niezależnych dokonano kierując się zasadą stosowalności i skuteczności w zadanej sytuacji problemowej, według metodologii określającą, że: „przez zmienne niezależne rozumie się pewne czynniki powodujące określone zmiany w innych czynnikach (zmiennych), a przez zmienne zależne – czynniki, polegające wyraźnym wpływom ze strony zmiennych niezależnych”[24].

Zależności między wymienionymi powyżej zmiennymi nie charakteryzują się jednolitością, gdyż na przykład wskaźniki ze zbioru zmiennych niezależnych, jakie będą uwzględniane w badaniach, jako mające wpływ na zmienne zależne, jedynie przy uproszczeniu procedur maja charakter stały. W celu najbardziej wiarygodnego wykazania zależności miedzy zmiennymi należy zastosować najbardziej

[24] Łobocki M., *Metody badań pedagogicznych*, PWN, Warszawa 1978 r. s.74.

odpowiednią metodę w odniesieniu do przedmiotu badań, która umożliwi weryfikacje sformułowanych hipotez i doprowadzi do rozwiązania problemu badawczego.

Biorąc pod uwagę stopień komplikacji problemu badawczego należy zastosować metodę, która umożliwi weryfikacje projektującą, co oznacza, że umożliwi ona spełnienie warunków założonych w hipotezie, co przy występowaniu zależności o charakterze złożonym, weryfikacja ta powinna mieć charakter analityczny, syntetyczny i odnosić się do poziomu zdolności Sił Zbrojnych Rzeczypospolitej Polski.

Takiej weryfikacji może sprostać metoda analizy systemowej, która zawiera wszystkie wymienione elementy weryfikacyjne. Uzasadnienie jej wyboru, dokonanie jej opisu oraz usytuowania w zbiorze narzędzi pomiaru i doskonalenia, jakości systemów będzie przedmiotem rozważań w niniejszej rozprawie doktorskiej.

1.8. Obszar i organizacja badań

Obszarem badań niniejszej rozprawy są Siły Zbrojne Rzeczypospolitej Polski (Marynarka Wojenna, Wojska Lądowe oraz Siły Powietrzne) jako obiekt zagrożeń cyberterrorystycznych a w szczególności Krytyczna Infrastruktura Teleinformatyczna (KITI) Sił Zbrojnych Rzeczypospolitej Polski.

Dla celów niniejszej rozprawy doktorskiej przyjęto trójetapową organizację badań.

PIERWSZY ETAP:

Badania empiryczne. Został poświęcony badaniom wstępnym, które posłużyły do weryfikacji problemów, narzędzi i metod badawczych. Praca badawcza na tym etapie była głównie ukierunkowana na wyselekcjonowaniu i studiowaniu literatury przedmiotu dotyczącej szeroko pojmowanemu bezpieczeństwu teleinformatycznemu. Dla osiągnięcia zamierzonego efektu przeprowadzono analizę:

- metodologii prowadzenia badań naukowych;
- terminologii, definicji, skrótów i akronimów;
- dotychczasowych doświadczeń w aspekcie bezpieczeństwa teleinformatycznego.

DRUGI ETAP:

Badania podstawowe. W badaniach tych dokonano stanu bezpieczeństwa teleinformatycznego Sił Zbrojnych Rzeczypospolitej Polski, jego powiązań z miarami efektywności na współczesnym polu walki oraz w działaniach sieciocentrycznych. Ukazano mechanizmy pomiaru zagrożeń i zapewnienia bezpieczeństwa teleinformatycznego. W etapie tym, poza funkcją opisowo – charakteryzującą objął również elementy podejścia pozytywnego, czyli uwypuklenie dodatnich cech narodowego systemu bezpieczeństwa teleinformatycznego obowiązującego w Siłach Zbrojnych Rzeczypospolitej Polski.

TRZECI ETAP:

Wielofunkcyjna analiza systemowa. Badania zostały ukierunkowane na eliminację stwierdzonych mankamentów przedmiotu badań oraz zaproponowaniu modelu procesu analizy zagrożeń i zarządzaniem ryzykiem informacyjnym, uwzględniającego wskazane w wyniku analizy wymogi obszaru badań.

Badania empiryczne przeprowadzono w 2007 roku, zakres działań analitycznych realizowany przez autora badań i zarazem autora rozprawy bazował na:

- doświadczeniu zawodowym nabytym w czasie pracy w obszarze związanym z bezpieczeństwem teleinformatycznym;
- zaangażowaniu w proces wdrażania w Marynarce Wojennej narodowych i sojuszniczych dokumentów, narzędzi i urządzeń ochrony teleinformatycznej (urządzeń ochrony kryptograficznej);
- studiowaniu przedmiotowej literatury narodowej i sojuszniczej;
- konferencjach, spotkaniach grup roboczych, kontaktach[25] i konsultacjach z osobami funkcyjnymi[26] narodowych władz bezpieczeństwa i służb ochrony państwa;
- bezpośrednich kontaktach zagranicznych:
  - udział w pracach projektowania i wdrażania sojuszniczych systemów i urządzeń ochrony kryptograficznej;
  - udział w pracach wyspecjalizowanych grup roboczych Paktu Północnoatlantyckiego;

[25] W tym kontakty korespondencyjne.
[26] Personel bezpieczeństwa teleinformatycznego.

- ❖ uczestnictwo w zagranicznych szkoleniach i kursach związanych z bezpieczeństwem teleinformatycznym;
- ❖ uczestnictwo w zagranicznych konferencjach związanych z bezpieczeństwem informacyjnym;

➢ prowadzeniu zajęć dydaktycznych, przez okres trzech lat, z zakresu problematyki bezpieczeństwa informacji oraz bezpieczeństwa teleinformatycznego w Akademii Marynarki Wojennej i Wyższej Szkole Międzynarodowych Stosunków Gospodarczych i Politycznych w Gdyni[27].

➢ wykorzystaniu zasobów bibliotecznych narodowych i zagranicznych ośrodków specjalizujących się w problematyce bezpieczeństwa teleinformatycznego;

➢ wykorzystaniu niepublicznych i publicznych sieci komputerowych.

Terenem badań jest w szerokim stopniu ogólnie rozumiany obszar bezpieczeństwa teleinformatycznego w Siłach Zbrojnych Rzeczypospolitej Polskiej bez powiązań do określonej jednostki organizacyjnej podległej Ministrowi Obrony Narodowej, co wynika z uniwersalnego charakteru problemu badawczego.

Autor zakłada, że w wyniku przeprowadzonej pracy badawczej zostanie wykazana potrzeba doskonalenia bezpieczeństwa teleinformatycznego Sił Zbrojnych Rzeczypospolitej Polski i zostanie wypracowany model systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informacyjnego Sił Zbrojnych RP w tym obszarze. Tym samym zostanie osiągnięty cel badań.

Wyniki badań i analiz odzwierciedlone są w kolejnych rozdziałach i załączniku niniejszej rozprawy doktorskiej.

---

[27] Podczas prowadzenia zajęć dydaktycznych autor jako wykładowca akademicki opracował niżej wymienione programy autorskie:
Program autorski do przedmiotu: *Zasady łączności i manewrowania według dokumentów NATO*, AMW, Gdynia 2006 r.
Program autorski do przedmioty: *Zintegrowane systemy dowodzenia*, AMW, Gdynia 2006 r.
Program autorski do przedmiotu: *Bezpieczeństwo informacji i ochrona informacji niejawnych*, Wyższa Szkoła Międzynarodowych Stosunków Gospodarczych i Politycznych, Gdynia 2006 r.
Program autorski do przedmiotu: *Przysposobienie obronne studentów*, Wyższa Szkoła Międzynarodowych Stosunków Gospodarczych i Politycznych, Gdynia 2007 r.
Program autorski do przedmiotu: *Międzynarodowe systemy bezpieczeństwa*, Wyższa Szkoła Międzynarodowych Stosunków Gospodarczych i Politycznych, Gdynia 2007 r.

1.9. Metody, techniki i narzędzia badawcze

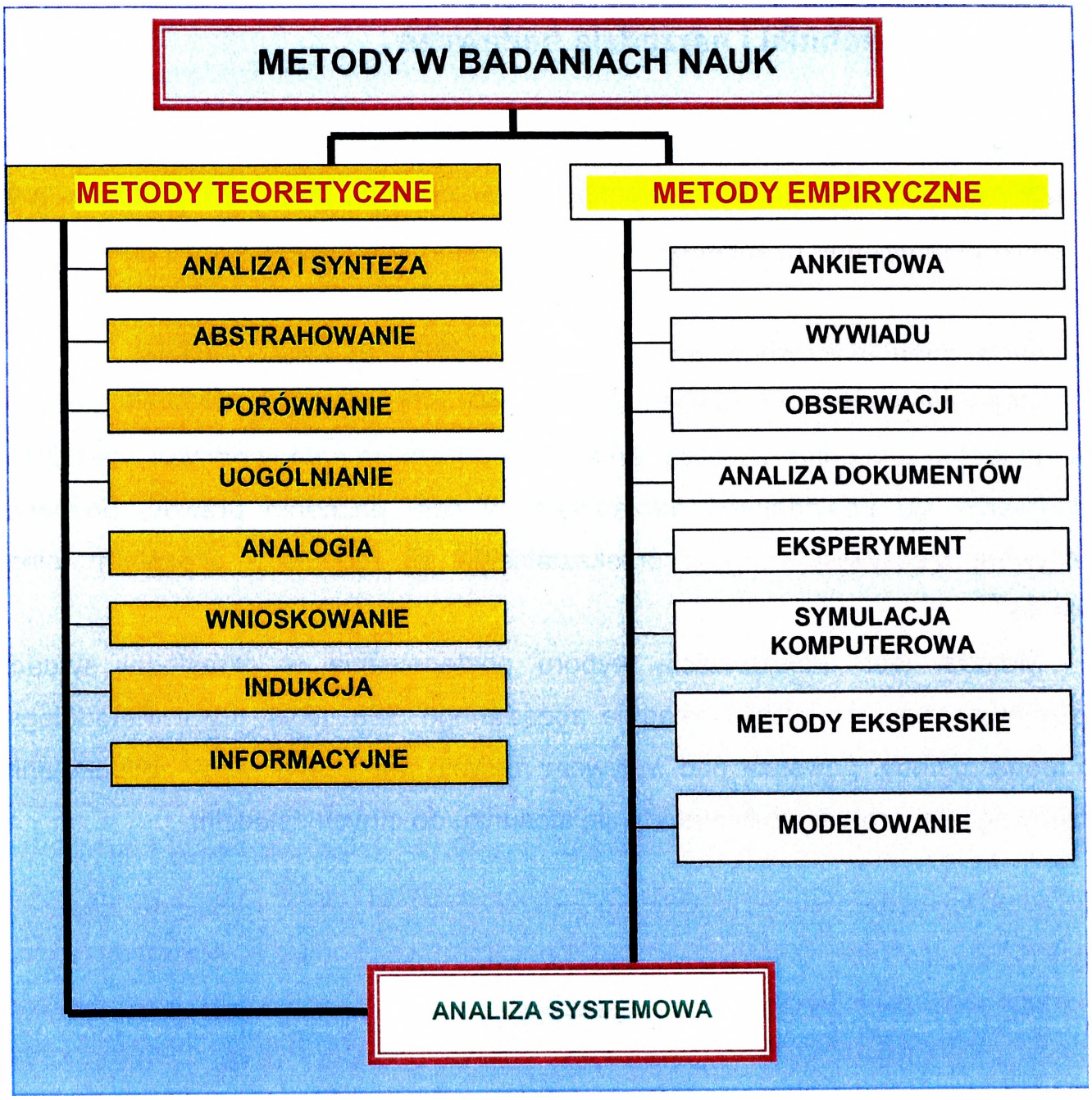
Metodę określa się jako „sposób wykonania działania, charakteryzujący się szczególnym doborem i układem elementów składowych, przy czym jest to sposób uprzednio przemyślany i zaplanowany, a jednocześnie nadający się do powtórzenia w sytuacjach takich samych lub zbliżonych”[28]. Wyodrębnia się takie metody, jak: obserwację, badanie wytworów pracy, zbieranie opinii oraz diagnozowanie.

W licznych pracach z zakresu teorii zarządzania i analizy systemowej przyjęto: „metoda jest to procedura postępowania, która umożliwia nam w danych warunkach posługiwanie się posiadanymi narzędziami w celu poznania prawdy, poznania obiektywnej rzeczywistości oraz przekształcenia jej zgodnie z przyjętym celem działania”[29].

Metoda, jest umiejętnością wyboru postępowania w określonej sytuacji problemowej, która umożliwia osiągnie pożądanego celu, (Rys. 1.2.). Metodologia jako teoria metody, powstała pod wpływem rozwoju nauki jako wyraz zaspokojenia potrzeby ogólnej problematyki metody, jej stosunku do innych dziedzin.

---

[28] Nowacki T., *Metodologia pedagogiki pracy*, WSiP, Warszawa 1978 r. s. 53 – 59.
[29] Sienkiewicz P., *Analiza systemowa. Podstawy i zastosowania*, Bellona, Warszawa 1994 r. s. 35.



Rysunek 1.2. Klasyfikacja metod badawczych.
Źródło: Opracowanie własne na podstawie: Sienkiewicz P., *Seminaria doktoranckie, AON*, Warszawa 2008 r., Stachowiak Z., *Metodyka i metodologia pisania prac kwalifikacyjnych*, AON, Warszawa 2001 r., Cieślarczyk M, *Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich*, AON, Warszawa 2006 r. oraz Jemioło T., Dawidczyk A., *Wprowadzenie do metodologii badań bezpieczeństwa*, AON, Warszawa 2008 r.

Kierując się dalej się przytoczonymi wyżej definicjami metody, dostrzegając w pełni złożoność problematyki, jaką stanowi sfera bezpieczeństwa informacyjnego (bezpieczeństwo teleinformatyczne i teleinformacyjne) w Polsce i Siłach Zbrojnych Rzeczypospolitej polski, zastosowano w niniejszej pracy następujące metody i techniki badawcze:

- nowoczesną metodę badawczą, stanowiącą jednocześnie zbiór technik analitycznych oraz procedur diagnostycznych, prognostycznych, optymalizacyjnych - **analizę systemową;**

- techniki heurystyczne (burza mózgów, technika Gordona, technika delficka oraz krytyczna ocena i analiza);
- metoda ankietowa;
- metoda opracowywania scenariuszu zagrożeń (metoda RAND Co.);
- technika ocen ekspertów;
- analiza dokumentów.

Niska efektywność systemu bezpieczeństwa teleinformatycznego Sił Zbrojnych RP oraz brak bezpośrednich i efektywnych więzi tego systemu ze źródłami informacji poza resortem Ministerstwa Obrony Narodowej, stanowi jedną z głównych barier rozwoju. W warunkach polskich jest to jeden z wielu czynników hamujących przebieg transformacji systemowej, utrudniających zapewnienie interoperacyjności z sojusznikami i organami NATO i przyśpieszenie przemian zmierzających do ogólnej racjonalizacji działania w tym zakresie.

Złożoność sfery bezpieczeństwa informacyjnego Sił Zbrojnych Rzeczypospolitej Polski państwa wymaga podejścia i działań systemowych. Według J. Koniecznego *Zrozumieć współczesny świat może tylko ten, kto rozumie systemy w nim występujące. Otaczający nas świat jest bowiem pełen systemów, wśród których wypadło nam żyć i działać. Rządzą się one swoistymi, obiektywnymi prawami, które człowiek współczesny musi poznać, aby być świadomym podmiotem działania w tym świecie systemów. Widzenie i myślenie systemowe stało się dzisiaj nie tylko modną rozrywką, lecz także życiową koniecznością. Muszą dziś zgłębić systemowe prawa planiści i projektanci, producenci, badacze i nauczyciele, czyli uczestnicy złożonych działań realizowanych w złożonych realnych systemach.*

Wielkie zalety analizy systemowej jako metody badań przedstawił przekonywująco A. K. Koźmiński, pisząc, że:

- analiza systemowa, traktując organizację jako system sprzyja podejmowaniu decyzji z całościowego punktu widzenia, przeciwdziałając tym samym tendencjom do suboptymalizacji, czyli traktowania poszczególnych części jako „samych dla siebie" i usprawniania ich ze szkodą dla funkcjonowania całości;
- analiza systemowa stwarza dogodną płaszczyznę współpracy między ekspertami reprezentującymi różne dziedziny wiedzy, rozwijające się dotąd w izolacji od siebie, oraz między interdyscyplinarnymi zespołami ekspertów, a kierownictwem organizacji;

- analiza systemowa stwarza szansę rozwiązywania na naukowych podstawach zasadniczych dla funkcjonowania organizacji problemów słabo ustrukturalizowanych, które dotąd rozwiązywano opierając się jedynie na intuicji, doświadczeniu, wyczuciu itp.;
- analiza systemowa pozwala na syntezę elementów tak różnych, jak intuicja, wyczucie, opis wywodzący się z nauk społecznych i badania operacyjne. Stwarza ona szansę przezwyciężenia sprzeczności między kwantyfikowanymi i niekwantyfikowanymi metodami i procedurami podejmowania decyzji;
- dzięki zastosowaniu badań operacyjnych wszędzie tam, gdzie to możliwe, analiza systemowa czyni procedury decyzyjne bardziej precyzyjnymi, obiektywnymi i sprawdzalnymi. Równocześnie jednak nie zawiera w sobie postulatu stosowania wyłącznie metod kwantyfikowanych, pozwalając uświadomić granice ich stosowania i tym samym zapobiec ogromnym nieraz kosztom pomyłek, wynikających z nadmiernych uproszczeń[30].

Rozwiązywanie sytuacji problemowych wymaga działań i metod systemowych. Tworzenie, rozwijanie i doskonalenie tych metod to zadanie współczesnych badań systemowych. Już Arystoteles stwierdził, że **„całość to więcej niż suma poszczególnych części"**. Tą całością, będącą przedmiotem badań jest **SYSTEM**, w niniejszej dysertacji – **system zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informacyjnego Sił Zbrojnych RP.**

Systemem określa się każdy złożony obiekt wyróżniony w badanej rzeczywistości, stanowiący całość tworzoną przez zbiór obiektów elementarnych i powiązań między nimi[31].

Do podstawowych zalet analizy systemowej należy zaliczyć takie cechy, jak: wprowadzenie znacznej dozy obiektywizmu do procesu, który jest w znacznej mierze subiektywny, uwzględnienie szerszego kontekstu do badań obiektu, a także uwzględnienie czynnika niepewności i ryzyka. Ponadto analiza systemowa pozwala skoncentrować uwagę na skutkach działania, dzięki czemu może sprzyjać ujawnieniu nieprzewidzianych następstw analizowanego działania. Niepodważalną zaletą metody jest niejako zmuszenie uczestników rozwiązywania problemu do jednolitej i systematycznej oceny i racjonalnego porównywania wariantów systemów.

---

[30] Koźmiński A. K., *Analiza systemowa organizacji*, WP, Warszawa 1976 r. s. 41.
[31] Sienkiewicz P., *Analiza systemowa…, op.cit.*, s. 37.

Celem określenia najbardziej efektywnego kierunku doskonalenia bezpieczeństwa teleinformatycznego (bezpieczeństwa informacyjnego) - należy zastosować metodę, która w praktyce sprowadza się do wykorzystania zbioru procedur analitycznych. Procedury analityczne ukierunkowane na rozwiązanie systemowych sytuacji decyzyjnych są oparte na zadanych wstępnie warunkach, narzędziach weryfikacji i możliwie pełnym banku danych. Jednym z kryteriów klasyfikacji analizy systemowej jest kryterium ilościowo-jakościowe. Z kolei według kryterium rodzaju wyniku analizy wyróżnia się analizę: problemową, identyfikacyjną, diagnostyczną, prognostyczną, efektywności i decyzyjną.

W niniejszej rozprawie przyjęto, że analiza systemowa, jest:

- zbiorem technik analitycznych, ocenowych i decyzyjnych, służących racjonalnemu rozwiązywaniu systemowych sytuacji decyzyjnych;
- badaniem wspomagającym działania osób odpowiedzialnych za decyzje lub linie postępowania w warunkach niepewności lub ryzyka[32].

Ma ona na celu określenie pożądanego działania lub linii postępowania przez rozpoznanie i rozważenie dostępnych wariantów oraz porównanie przewidywanych ich, bliższych i dalszych, następstw[33].

Analizę systemowa różni się od analizy to, że postrzega ona w całości badany obiekt jako system. Ważną jej cechą jest kompleksowość i wielowątkowość metody badawczej. Analiza systemowa posiłkuje się wieloma rodzajami dociekań zaczerpniętych z różnych dziedzin naukowych.

Z uwagi na swoją kompleksowość analiza systemowa stanowi cenne narzędzie poznania i sprawdzania zaprojektowanych systemów teleinformatycznych. Ponadto należy nadmienić, że analiza ryzyka stanowi jedno z zasadniczych jej zagadnień. Wydaje się poddanie projektu systemu bezpieczeństwa teleinformatycznego ścisłym rygorom analizy systemowej może przynieść istotne oceny przedsięwzięcia. Za pomocą analizy systemowej można dokonać całościowego przeglądu projektu, czy też funkcjonującego rozwiązania. Jeśli nawet, jeśli nie rozstrzygnie wszystkich dylematów, to na pewno znacząco uzupełni naszą wiedzę.

W celu oceny przydatności tego narzędzia badawczego – należy przeprowadzić analizę identyfikacyjną problemu. Identyfikacja sytuacji problemowej

---

[32] Sienkiewicz P., *Analiza systemowa. Podstawy i zastosowania*, Warszawa 1994 r. s. 37.
[33] Ibidem, s. 38.

polega na określeniu zadania stanowiącego problem. W niniejszej rozprawie, głównym problemem badawczym jest: **jaki jest aktualny poziom zabezpieczenia Krytycznej Infrastruktury Teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polski przed zagrożeniami cyberterrorystycznymi oraz jakie działania należy podjąć, aby zapewnić prawidłowy poziom bezpieczeństwa informacyjnego Sił Zbrojnych Rzeczypospolitej Polski?**

Należy nadmienić, że pierwszy krok analizy identyfikacyjnej pozwala na zdefiniowaniu obiektu jako systemu, ponieważ bezpieczeństwo teleinformatyczne państwa, a ściśle Sił Zbrojnych Rzeczypospolitej Polski niewątpliwie stanowi wielki system.

1.10. Charakterystyka literatury przedmiotu badań

Obszar badań wyznaczył kierunki w gromadzeniu różnego rodzaju opracowań i literatury fachowej oraz dostępu do zasobów elektronicznych różnych baz danych[34]. W czasie, kiedy tworzono koncepcję rozprawy doktorskiej w Siłach Zbrojnych Rzeczypospolitej Polski zachodziły zmiany związane z bezpieczeństwem teleinformatycznym[35]. Ukazywały się nowe wytyczne, zarządzenia i rozporządzenia dotyczące polityki bezpieczeństwa.

W trakcie studiowania literatury przedmiotu odnoszącej się do problemów badawczych stwierdzono, że pomimo bardzo wielu dokumentów niektóre zagadnienia związane z bezpieczeństwem teleinformatycznym a szczególnie problemami związanymi z reagowaniem na incydenty komputerowe są prezentowane w sposób ogólnikowy, a niejednokrotnie niejednoznaczny. Brak jest również doprecyzowania pojęć i definicji.

Poszczególne etapy prowadzonych badań były związane ze studiowaniem literatury, która umożliwiła prowadzenie w sposób naukowy procesu badawczego realizując osiąganie celu badań i rozwiązywanie problemów badawczych. Dokonano weryfikacji materiału badawczego ze względu na obszary funkcjonalne: bezpieczeństwo teleinformatyczne, bezpieczeństwo oprogramowania,

---

[34] W rozprawie doktorskiej są brane pod uwagę tylko informację nie stanowiące tajemnicy służbowej i państwowej w myśl Ustawy z dnia 22 stycznia 1999 r. *O ochronie informacji niejawnych* Tekst ujednolicony po zmianach z dnia 15 kwietnia 2005 r. Dz. U. 1999.11.95; Tekst ujednolicony Dz. U. 2005.196.1631 - akty zmieniające.

[35] Powstały nowe służby ochrony państwa zajmujące się bezpieczeństwem Sił Zbrojnych RP. Zmiany związane były z rozwiązaniem WSI i tworzenie od nowa nowej służby – SKW.

bezpieczeństwo fizyczne, bezpieczeństwo elektromagnetyczne, bezpieczeństwo sprzętu, bezpieczeństwo dokumentów, bezpieczeństwo osobowe oraz ochronę informacji niejawnych.

Można przyjąć, że możliwe jest poddanie źródeł i gatunków literatury przedmiotu pewnej klasyfikacji na następujące kategorie:

- publikacje dotyczące metodologii badań naukowych (rekomendowane przez promotora);
- publikację i dokumenty normatywne służb ochrony państwa[36];
- publikację i dokumenty normatywne organów bezpieczeństwa teleinformatycznego Sił Zbrojnych Rzeczypospolitej Polski[37];
- publikację i dokumenty normatywne organów bezpieczeństwa teleinformatycznego państw NATO[38];
- praca dydaktyczna z zakresu problematyki bezpieczeństwa informacji oraz bezpieczeństwa teleinformatycznego i teleinformacyjnego w Akademii Marynarki Wojennej i Wyższej Szkole Międzynarodowych Stosunków Gospodarczych i Politycznych w Gdyni;
- wystąpienia i prezentacje przygotowywane na krajowe kursy i konferencję związane z bezpieczeństwem teleinformatycznym[39];

---

[36] W rozprawie doktorskiej są brane pod uwagę tylko dokumenty i informację nie stanowiące tajemnicy służbowej i państwowej w myśl Ustawy z dnia 22 stycznia 1999 r. *O ochronie informacji niejawnych* Tekst ujednolicony po zmianach z dnia 15 kwietnia 2005 r. Dz. U. 1999.11.95; Tekst ujednolicony Dz. U. 2005.196.1631 - akty zmieniające.

[37] Decyzja Nr 448/MON Ministra Obrony Narodowej z dnia 04.10.2007 r. *W sprawie trybu akredytacji bezpieczeństwa fizycznego i technicznego pomieszczeń specjalnych.*
Decyzja Nr 24/MON Ministra Obrony Narodowej z dnia 31.01.2006 r. *W sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej.*
Decyzja Nr 488/MON Ministra Obrony Narodowej z dnia 30.11.2006 r. *W sprawie wprowadzenia do użytku w resorcie obrony narodowej Tymczasowej instrukcji organizacji obiegu informacji niejawnych o klauzuli zastrzeżone w resortowej sieci teleinformatycznej MIL – WAN.*
Decyzja Nr 20/MON Ministra Obrony Narodowej z dnia 31.01.2006 r. *W sprawie powoływania pełnomocników, zastępców pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów i sieci teleinformatycznych oraz inspektorów bezpieczeństwa teleinformatycznego w Ministerstwie Obrony Narodowej oraz w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych.*
Decyzja Nr 357/MON Ministra Obrony Narodowej z dnia 29.07.2008 r. *W sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej.*
Inne dokumenty normatywne zamieszczone w Załączniku 3.
Konferencja *Bezpieczeństwo teleinformatyczne państwa. Transnarodowy problem, międzynarodowa współpraca*, Polski Instytut Spraw Międzynarodowych, Warszawie 23.04.2008 r.
Konferencja naukowa *Cyberterroryzm nowe wyzwania XXI wieku*, Wyższa Szkoła Informatyki, Zarządzania i Administracji, Warszawa 18.05.2009 r.

[38] *Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji*, sporządzona w Brukseli dnia 6 marca 1997 r.
Dyrektywa bezpieczeństwa AD-70-1.

[39] *Doktryna Operacji Informacyjnych Sił Zbrojnych Rzeczypospolitej Polski w aspekcie działań cybernetycznych, Aspekty bezpieczeństwa nawodnego i podwodnego oraz lotów nad morzem.* X Konferencja Morska pod patronatem Dowódcy Marynarki Wojennej RP, AMW, Gdynia 2007 r.

- porozumienia standaryzacyjne STANAG, procedury operacyjne SOP oraz różne opracowania dotyczące skrótów i akronimów stosowanych w NATO[40].

Dogłębne badanie literatury potwierdza, że stworzenie odpowiedniego systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych zwiększy w znacznym stopniu bezpieczeństwo teleinformatyczne Sił Zbrojnych Rzeczypospolitej Polski.

1.11. Stan wiedzy na podstawie badań własnych

Przeprowadzone badania, stanowią pierwszą próbę kompleksowego określenia i spojrzenia na ochronę Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski[41], a w tym na Krytyczną Infrastrukturę Teleinformatyczną, która jest kluczowa dla bezpieczeństwa teleinformatycznego. Kwestionariusz ankiety opracowany prze autora, został zaadaptowany do warunków i potrzeb rozprawy doktorskiej. Jednocześnie trzeba zaznaczyć, że kilkanaście jednostek organizacyjnych podległych Ministrowi Obrony Narodowej[42], nie udzieliło odpowiedzi, pomimo wcześniej zgłoszonych telefonicznie deklaracji.

Cyberterroryzm państwowy i niepaństwowy – początki, skutki i formy. Konferencja naukowa „Ewolucja terroryzmu na przełomie XX i XXI wieku", Klub Riwiera (Uniwersytet Gdański), Gdynia 2007 r.
Bezpieczeństwo danych w Krytycznej Infrastrukturze Teleinformatyczne. Konferencja naukowa „Współczesny wymiar terroryzmu. Przeciwdziałanie zjawisku.", Instytut Bezpieczeństwa Narodowego WSO AON we współpracy z Szefem Obrony Cywilnej Kraju i Stowarzyszenie Ruch Wspólnot Obronnych, Warszawa 21.11.2007 r.
Cyberterrorystyczne zagrożenie dla bezpieczeństwa teleinformatycznego państwa polskiego. Instytut Badań Systemowych PAN Polskie Towarzystwo Badań Operacyjnych i Systemowych, Warszawa 2008 r.
Bezpieczeństwo teleinformatyczne Sił Zbrojnych Rzeczypospolitej Polski w dobie zagrożeń cybernetycznych. Konferencja naukowa „Cyberterroryzm nowe wyzwania XXI wieku", Wyższa Szkoła Informatyki , Zarządzania i Administracji, Warszawa 18.05.2009 r.
Cyberterrorystyczne zagrożenie dla bezpieczeństwa teleinformatycznego Unii Europejskiej. AMW, Konferencja naukowa „Europa – Integracja, Polityka, Bezpieczeństwo, Gdynia 28 – 30.05.2009 r.
[40] AAP-6 *NATO Glossary of Terms and Definitions*.
AAP-15 *NATO Glossary of Abbreviations Used in NATO Documents and Publications*.
AAP-31A *NATO Glossary of Communication and Information Systems Terms and Definitions*.
Procedury SOP (dotyczące bezpieczeństwa teleinformatycznego i ochrony kryptograficznej) wykorzystywane w jednostkach szczebla taktycznego Marynarki Wojennej RP podczas działań w relacjach sojuszniczych.
[41] Dokładne wyniki badań przedstawiono w Załączniku 6 niniejszej rozprawy doktorskiej.
[42] Dokładnie 24 jednostki organizacyjne podległe Ministrowi Obrony Narodowej nie udzieliły odpowiedzi. Jest to spowodowane brakiem odpowiednio przygotowanego personelu, który mógłby szerzej spojrzeć się na ochronę Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski oraz prawdopodobnie błędnym rozumowaniem ochrony informacji niejawnych.

Pojęcia związane z Infrastrukturą Krytyczna przedstawione w kwestionariuszu ankiety zdaniem autora nie powinny sprawiać żadnych trudności w przedstawieniu stanu ochrony sektorów Infrastruktury Krytycznej. Autor uważa, że zniekształcenie (w niektórych przypadkach) wyników ankiety, spowodowane jest brakiem odpowiednio przygotowanego personelu, który mógłby w sposób kompetentny rozpatrzyć problem ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.

Jedną z najważniejszych wad, wynikających obecnie z przyjętych zasad obowiązujących w Siłach Zbrojnych RP, jest utożsamianie wszystkich sektorów Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski z jednym tylko elementem – funkcjonowaniem Sił Zbrojnych w czasie stanów zagrożeń i wojny.

Wyniki kwestionariusza ankiety pokazują brak zrozumienia jednostek organizacyjnych w realizacji zadań związanych z polityką bezpieczeństwa państwa oraz, że nie mają one opracowanych kompleksowych planów ochrony sektorów Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Prawdopodobnie nie opracowały także odpowiednich wytycznych w tym zakresie. Brak zorganizowanej polityki bezpieczeństwa dla podmiotów odpowiedzialnych za bezpieczeństwo Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski naraża Siły Zbrojne na bardzo duże straty oraz chaos organizacyjny w przypadku ewentualnych ataków cyberterrorystycznych lub zakłóceń w kluczowych węzłach sektorów infrastruktury (efekt kaskadowy).

Należy nadmienić, że wyniki kwestionariusza ankiety nie wykazały w żadnym stopniu istnienia koordynacji działań oraz współpracy między sektorami w zakresie ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.

Bardzo dużą wartość stanowią materiały nadesłane w kwestionariuszach ankiety, które mogą stać się punktem wyjścia dla przyszłych badań w zakresie ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski oraz Infrastruktury Krytycznej Państwa.

Najbardziej wrażliwymi sektorami Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski okazały się: energia, woda, żywność, transport oraz systemy i technologia teleinformatyczna, łączność, ICT. Jest to bardzo prawidłowy trend, który w pełni oddaje poczucie nowych zagrożeń asymetrycznych, które uwydatniły się po atakach na World Trade Center (WTC) 11 września 2001 r[43]. Coraz większe

[43] W *Raporcie z badań* Departamentu Bezpieczeństwa Powszechnego Ministerstwa Spraw Wewnętrznych i Administracji z września 2002 r., „zwycięzcami rankingu" na wytypowanie najbardziej

znaczenie nabiera bezpieczeństwo sektora: systemy i technologia teleinformatyczna, łączność, ICT[44]. W rozwiązaniach przyjętych w Stanach Zjednoczonych, Kanadzie, Wielkiej Brytanii, Finlandii oraz Niemczech główny nacisk kładzie się na bezpieczeństwo w „cyberprzestrzeni". Również w Siłach Zbrojnych i administracji państwowej stanie się to istotnym wyzwaniem, zwłaszcza po przyjęciu wszystkich ustaw związanych z przetwarzaniem informacji w systemach teleinformatycznych[45]. Coraz częściej technologia teleinformatyczna umożliwiać będzie w niektórych segmentach „usług administracyjnych", a w szczególności w Siłach Zbrojnych bezpośrednie komunikowanie się i przesyłanie danych służbowych jawnych i niejawnych. Stąd problematyka bezpieczeństwa informacyjnego (teleinformatycznego) zasługuje na szczególną uwagę w dalszych pracach badawczych.

Używane w rozprawie pojęcia i terminy oparto na dokumentach normatywnych obowiązujących w kraju[46].

---

wrażliwych sektorów (segmentów) infrastruktury krytycznej okazały się: energetyka, bezpieczeństwo powszechne i telekomunikacja.

[44] Chodzi tu głownie o bezpieczeństwo teleinformatyczne.

[45] Po wdrożeniu Ustaw z dnia 18 lipca 2002 r. *O świadczeniu usług drogą elektroniczną* Dz. U. 2002.144.1204; z dnia 18 września 2001 r. *O podpisie elektronicznym* Dz. U. 2001.130.1450; z dnia 27 lipca 2001 r. *O ochronie baz danych* Dz. U. 2001.128.1402.

[46] Ustawa *O ochronie informacji niejawnych* z dnia 22.01.1999 r. Tekst ujednolicony po zmianie 15.04.2005 r., Dz. U. 2007.25.162.
Decyzja Nr 448/MON Ministra Obrony Narodowej z dnia 04.10.2007 r. *W sprawie trybu akredytacji bezpieczeństwa fizycznego i technicznego pomieszczeń specjalnych.*
Decyzja Nr 24/MON Ministra Obrony Narodowej z dnia 31.01.2006 r. *W sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej.*
Decyzja Nr 20/MON Ministra Obrony Narodowej z dnia 31.01.2006 r. *W sprawie powoływania pełnomocników, zastępców pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów i sieci teleinformatycznych oraz inspektorów bezpieczeństwa teleinformatycznego w Ministerstwie Obrony Narodowej oraz w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych.*
Decyzja Nr 357/MON Ministra Obrony Narodowej z dnia 29.07.2008 r. *W sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej.*

ROZDZIAŁ II

CYBERTERRORYZM JAKO NOWA FORMA ZAGROŻEŃ DLA BEZPIECZEŃSTWA

2.1. Teoria wojny informacyjnej

Na początku lat osiemdziesiątych ubiegłego wieku dostrzeżono rewolucyjne zmiany w dziedzinie wojskowości [47]. Zmiany w technice wojskowej skłoniły do podjęcia prób wskazania głównych czynników, które będą w przyszłości decydowały o charakterze przyszłych działań i potencjale bojowym sił zbrojnych. Zmierzano do określenia charakteru i dynamiki procesów rozwojowych w siłach zbrojnych, w technice wojskowej i cywilnej oraz w strukturach państwa. W ocenie specjalistów wojskowych, istotą obecnej (piątej) rewolucji technicznej w dziedzinie wojskowości jest koncepcja osiągnięcia zwycięstwa przez wykorzystanie instrumentów walki informacyjne[48].

Nadrzędnym celem walki informacyjnej jest zdobycie panowania nad przeciwnikiem w dziedzinie informacyjnej. Praktycznie oznacza to stworzenie takiej sytuacji, w której baza informacyjna organów dowodzenia własnych wojsk jest pełniejsza, dokładniejsza, wiarygodniejsza i bardziej aktualna niż organów dowodzenia przeciwnika. W ramach koncepcji walki informacyjnej mają być zintegrowane rozproszone dotychczas działania zmierzające do sparaliżowania swobody decyzyjnej przeciwnika.

Pojęcie walki informacyjnej pojawiło się w literaturze wojskowej pod koniec lat osiemdziesiątych, najczęściej w kontekście informatyzacji sił zbrojnych państw

---

[47] W literaturze anglojęzycznej używa się określenia *The RMA (Revolution In Military Affairs* lub *The IRMA (Information Revolution In Military Affairs)* J. Kamieński *Technologia i wojna przyszłości,* UJ, Kraków 2009 r.

[48] Rosjanie twierdzą, że środki ogniowe precyzyjnego rażenia, nie jądrowe środki ogniowe do wykonywania głębokich uderzeń i systemy integrujące rewolucjonizują wszystkie aspekty sztuki wojennej i struktur organizacyjnych sił zbrojnych, powodując zwiększenie możliwości bojowych o milion razy w stosunku do okresu II wojny światowej. Rosjanie twierdzą, że technika informacyjna jest "najważniejszą bronią XXI wieku", a pod względem skuteczności oddziaływania jest porównywana z bronią masowego rażenia.

NATO. Poniżej przedstawiam kilka istniejących w literaturze definicji walki informacyjnej (Tabela 2.1.)[49].

Tabela 2.1. Definicje walki informacyjnej

AUTOR	DEFINICJA
Widnall S. **Fogleman R.**	*Walka informacyjna to jakiekolwiek działania mające na celu wzbranianie przeciwnikowi dostępu do informacji i jej funkcji lub ich eksploatację, obniżanie jej wartości bądź niszczenie; ochrona siebie przeciwko takim działaniom oraz eksploatowanie własnych militarnych funkcji informacji.*
Schwartau W.	*Walka informacyjna jest elektronicznym konfliktem, w którym informacja jest strategicznym dobrem wartym podboju lub destrukcji.*
Arquilla J. **Ronfeldt D.**	*Walka informacyjna w najogólniejszym sensie jest użyciem informacji dla osiągnięcia naszych narodowych celów. Podobnie jak dyplomacja, ekonomiczna rywalizacja czy użycie sił zbrojnych, informacja sama w sobie jest kluczowym czynnikiem narodowej potęgi. Ponadto, co jeszcze ważniejsze, informacja staje się głównym narodowym zasobem, który wspiera dyplomację ekonomiczną rywalizację oraz przemoc militarną. Walka informacyjna w tym sensie może być postrzegana jako konflikt między państwami lub narodami, prowadzony częściowo przez globalnie połączoną infrastrukturę informacyjną i komunikacyjną.*
Stark R.	*Walka informacyjna jest konfliktem, w którym informacja jest jednocześnie zasobem, obiektem ataku i bronią. Walka informacyjna obejmuje także fizyczną destrukcję infrastruktury, która wykorzystywana jest przez przeciwnika do działań operacyjnych.*
Ciborowski L.	*Walka informacyjna to działania kooperacji negatywnej wzajemnej, w których cel destrukcyjnego oddziaływania skoncentrowany jest na systemach informacyjno – sterujących przeciwnych sobie stron. Przedmiotem waliki informacyjnej jest system informacyjno – sterujący.*
Sienkiewicz P.	*Walka informacyjną nazywamy całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych). Istotą tak rozumianej walki jest:* *a) zniszczenie (lub degradacja wartości) zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych;* *b) zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych.*

Opracowanie własne na podstawie: Szpyra R., *Militarne operacje informacyjne,* AON, Warszawa 2003 r.

[49] Szpyra R., *Militarne operacje informacyjne,* AON, Warszawa 2003 r., s. 97.

Analiza doświadczeń z działań bojowych prowadzonych przez koalicję antyiracką uświadomiła, że postęp dokonany w dziedzinie informatycznego wsparcia systemów dowodzenia, łączności i rozpoznania wojskowego, nowy poziom jakościowy precyzji rażenia celów, skali obezwładniania radioelektronicznego systemów dowodzenia, łączności i kierowania ogniem, izolacji informacyjnej przeciwnika oraz możliwość wprowadzania destrukcyjnych informacji do systemów informacyjnych przeciwnika pozwalają na wydzielenie walki informacyjnej jako dziedziny sztuki wojennej.

Jako wojskowo - techniczne źródła walki informacyjnej wymienia się informatyzację sił zbrojnych, wzrost możliwości systemów łączności wszystkich szczebli dowodzenia, wysokie nasycenie wojsk nowoczesnymi środkami rozpoznania (w tym przechodzenie od optycznych do elektrooptycznych urządzeń rozpoznania obrazowego) i stosunkowo szerokie stosowanie precyzyjnych środków rażenia.

Do pozawojskowych źródeł walki informacyjnej zaliczono natomiast:

- powstanie i rozwój globalnej platformy informatycznej o zasięgu ogólnopaństwowym (często ponadpaństwowym);
- komputeryzację wszystkich sfer życia gospodarczego (w tym finansowego);
- upowszechnienie systemów łączności cyfrowej;
- istnienie licznych i różnorodnych baz danych oraz masowy charakter wykorzystania komputerów osobistych.

Uważa się, że walka informacyjna może naruszyć parytet strategiczny i równowagę między głównymi aktorami na globalnej scenie politycznej. Z tych względów konieczne jest wszechstronne śledzenie wprowadzania środków walki informacyjnej w siłach zbrojnych światowych potęg i systematyczne dokonywanie oceny efektywności funkcjonowania systemów przeciwdziałania tym środkom. Jest to nie tylko problem pozyskania środków technicznych i opracowania metod wykrywania skutków oddziaływani broni informacyjnej, lecz także zbudowania systemu wczesnego wykrywania symptomów stosowania przez przeciwnika narzędzi walki informacyjnej.

Podkreśla się także konieczność pogłębionej i rzetelnej oceny aktualnej sytuacji, określenia specyficznych charakterystyk oraz prognozy rozwoju środków walki informacyjnej i sposobów ich stosowania. Ocena ma stanowić punkt wyjścia do kształtowania polityki wewnętrznej i zagranicznej. Wojskowe i wojskowo - techniczna składowe tej polityki powinny zapobiegać lub przeciwdziałać powstałym

zagrożeniom i stanowić niezawodne gwarancje bezpieczeństwa państwa. W całym tym procesie kierownictwo wojskowe kieruje się tezą, że zagrożenia stwarzane przez walkę informacyjną w szerokim kontekście przyjmują formę ukrytej presji polityczno - wojskowej a czasem zastraszenia.

Ponadto podkreślana jest konieczność doskonalenia i rozwoju narzędzi obrony informacyjnej, w tym środków technicznych i oprogramowania uniemożliwiających utratę, zniekształcenie, zniszczenie lub przechwycenie informacji. Metody te mają być wspierane przedsięwzięciami legislacyjnymi i organizacyjno - gospodarczymi wzmacniającymi ochronę państwowych zasobów informacji.

Bezpieczeństwo państwa wymaga wyrównania poziomów potencjału walki informacyjnej; potencjalny przeciwnik musi zdawać sobie sprawę, że znajduje się w zasięgu zagrożenia informacyjnego. Możliwości walki informacyjnej rosną wraz z doskonaleniem i upowszechnianiem systemów mikroelektroniki, systemów szybkiego przetwarzania i transmisji danych oraz nowoczesnych systemów rozpoznania.

Instalacjami najbardziej wrażliwymi na środki walki informacyjnej są kompleksy, których skuteczne działanie jest uzależnione od zdolności do nieprzerwanego i szybkiego funkcjonowania w czasie rzeczywistym[50].

Walkę informacyjną można umieścić między "zimną" wojną obejmującą wojnę ekonomiczną, a wojną "gorącą" z użyciem broni konwencjonalnej (jądrowej). W porównaniu z wojną ekonomiczną, obliczoną na długotrwałe konsekwentne działania, wojna informacyjna może spowodować natychmiastowe zerwanie funkcjonowania elementów infrastruktury cywilnej i wojskowej przeciwnika. Przedsięwzięcia walki informacyjnej nie zmierzają do niszczenia fizycznego infrastruktury materialnej przeciwnika. Ich celem jest obezwładnienie funkcjonalne podstawowych elementów infrastruktury decydujących o możliwościach przetrwania społeczności przeciwnika we współczesnych warunkach cywilizacyjnych i globalnej konkurencji.

Określa się walkę informacyjną jako kompleks przedsięwzięć, obejmujących wsparcie, przeciwdziałanie i obronę informacyjną, prowadzonych według jednolitej koncepcji i planu, w celu wywalczenia i utrzymania panowania nad przeciwnikiem

---

[50] Na przykład celowe zakłócanie działania zautomatyzowanego systemu wczesnego ostrzegania o zagrożeniu rakietowym i lotniczym systemu dowodzenia obroną przeciwrakietową i innych systemów o znaczeniu strategicznym może spowodować katastrofę porównywalną z uderzeniem jądrowym. Prawdopodobieństwo szybkiego odtworzenia sprawności takich systemów poddanych atakowi informacyjnemu jest stosunkowo niskie, co zwiększa atrakcyjność wojskową walki informacyjnej.

w dziedzinie informacyjnej podczas przygotowania operacji wojskowych oraz prowadzenia działań bojowych[51].

Pojęcie walki informacyjnej zawiera trzy podstawowe elementy składowe:

- przedsięwzięcia obejmujące zdobywanie, przetwarzanie i wymianę (w ramach struktur dowodzenia) informacji o potencjalnym przeciwniku oraz warunkach konfliktu (w tym o sytuacji polityczno-wojskowej, radioelektronicznej, rozbudowie inżynieryjnej, warunkach meteorologicznych, itp.). Zdobyte informacje powinny być wiarygodne, pełne, a ich transmisja powinna być selektywna i spełniać warunki aktualności. Ten kompleks przedsięwzięć jest określany jako "wsparcie informacyjne systemu dowodzenia wojsk i kierowania środkami ogniowymi";
- przedsięwzięcia obejmujące uniemożliwianie przeciwnikowi korzystania ze wsparcia informacyjnego (określane jako przeciwdziałanie informacyjne). Problematyka ta obejmuje blokadę zdobywania, przetwarzania i wymiany informacji oraz wprowadzanie dezinformacji na wszystkich szczeblach wsparcia informacyjnego wojsk przeciwnika;
- przedsięwzięcia obejmujące ochronę przed przeciwdziałaniem informacyjnym (określane jako obrona informacyjna), do których należą odblokowanie informacji koniecznych do realizacji funkcji dowodzenia i zablokowanie dopływu dezinformacji wprowadzanej do systemu dowodzenia przez przeciwnika. Obrona informacyjna zwiększa skuteczność wsparcia informacyjnego w warunkach stosowania przez przeciwnika aktywnych i pasywnych form przeciwdziałania informacyjnego.

Celem walki informacyjnej jest:

- uzyskanie przewagi nad potencjalnym przeciwnikiem w dziedzinie wywiadu i rozpoznania wojskowego;

---

[51] Walka informacyjna rozumiana jest jako kooperacja negatywna wzajemna, przynajmniej dwupodmiotowa, realizowana w sferach: zdobywania informacji (rozpoznania), zakłócania informacyjnego i obrony informacyjnej, gdzie każdemu działaniu jednej strony przyporządkowane zostało działanie antagonistyczne strony drugiej. L. Ciborowski *Walka informacyjna*, ECE, Toruń, 1999 r.
Działania informacyjne to przedsięwzięcia, których celem jest wpływanie na postrzeganie (poglądy) i nastawienie określonych jednostek i grup, prowadzące do zachowań korzystnych z własnego punktu widzenia. To przedsięwzięcia mające wpływ na podejmowanie decyzji ***politycznych i wojskowych*** *przez* ***oddziaływanie na informację****, podstawowe procesy informacyjne oraz systemy dowodzenia, kierowania, łączności i informatyki przeciwnika, a także chroniące własne informacje, procesy i systemy informacyjne. Regulamin działań Wojsk Lądowych,* 2006, s. 79.

- zapewnienie sobie możliwości demoralizowania przeciwnika oraz odcięcia dowództw od podległych im wojsk z jednej, a struktur państwowych z drugiej strony;
- zneutralizowanie przewagi przeciwnika w dziedzinie łączności i informatyki;
- zerwanie procesów informatycznych, obezwładnianie lub zniszczenie systemów informatycznych.

Celem ofensywnych form walki informacyjnej jest:

- wprowadzanie przeciwnika w błąd, dezorganizowanie lub niszczenie jego infrastruktury informacyjnej;
- wprowadzanie zamieszania i zdezorganizowanie lub całkowite zerwanie procesów dowodzenia wojskami operacyjnymi przeciwnika;
- stworzenie warunków do szybkiego zneutralizowania oporu przeciwnika.

Celem stosowania defensywnych form walki informacyjnej jest ochrona własnych i sojuszniczych systemów informatycznych oraz systemów dowodzenia, łączności i rozpoznania przed działaniami przeciwnika.

Zamierza się osiągnąć wyznaczone na poszczególnych etapach cele walki informacyjnej następującymi sposobami:

- w czasie pokoju, przez „elektroniczne zastraszenie";
- w czasie narastania kryzysu, przez selektywne (pod względem celów) i zmasowane (pod względem intensywności) użycie środków elektronicznych przeciwko wojskowym i cywilnym strukturom dowódczym i informacyjnym przeciwnika;
- w czasie trwania konfliktu zbrojnego, przez zmasowane użycie zarówno środków radioelektronicznych, jak i ogniowych przeciwko wojskowym i cywilnym strukturom dowódczym i informacyjnym przeciwnika.

Uzyskanie przewagi na gruncie nowej rewolucji technologicznej w dziedzinie wojskowości jest możliwe przez zdobywanie dominującej pozycji w dziedzinie systemów dowodzenia, łączności i rozpoznania. Sukces w działaniach wojskowych można osiągnąć przez zdobycie kolejno panowania w eterze, w powietrzu, a następnie przez umiejętne wprowadzenie do walki żołnierzy sił lądowych. Kontrastuje to z okresem II Wojny Światowej, kiedy warunkiem sukcesu było w dużym stopniu wywalczenia panowania w powietrzu; w czasie I Wojny Światowej sukces zależał od efektywności zastosowania środków ogniowych sił lądowych,

w tym głównie środków artyleryjskich. Współczesny konflikt zbrojny powinien być rozpatrywany w świetle synergizmu działania dwóch elementów składowych:

- sprzężenia systemów ognia i elektroniki;
- systemów informacyjnych.

Każdy z tych elementów składowych ma własne specyficzne dla niego cele, środki i metody. Przez pojęcie sprzężenia „ognia i elektroniki" rozumie się potencjał bojowy środków ogniowych i środków walki radioelektronicznej, to znaczy środki bezpośredniego oddziaływania na technikę bojową i siłę żywą przeciwnika. Pod pojęciem składowej informacyjnej mieszczą się możliwości systemów zdobywania informacji (rozpoznanie) i ich wykorzystanie (dowodzenia) w celu zwiększenia potencjału bojowego środków bezpośredniego oddziaływania bojowego na przeciwnika (środków ogniowych i walki radioelektronicznej).

Do narzędzi i metod walki informacyjnej zalicza się:[52]

- wirusy komputerowe, zdolne do samo powielania i podczepiania się do programów komputerowych, Mogą być przenoszone za pośrednictwem środków łączności i sieci transmisji danych. Wirusy te pa wniknięciu do aparatury elektronicznych central telefonicznych i systemów dowodzenia powodują w odpowiednim momencie zablokowanie ich funkcjonowania;
- „bomby logiczne", czyli aplikacje programowe wcześniej wprowadzone do systemów informacyjnych: w tym działających na rzecz systemów dowodzenia, aktywowane na określony sygnał lub w wyznaczonym czasie. Aktywacja „bomb logicznych" prowadzi do zniszczenia albo zniekształcenia funkcjonowania sprzętu lub oprogramowania. Jedną z odmian „bomby logicznej" jest "koń trojański", który umożliwia potajemne wniknięcie do baz informacyjnych przeciwnika i wydobywania danych interesujących służby wywiadowcze;
- blokowanie wymiany informacji w sieciach łączności: fałszowanie informacji znajdujących się w sieciach przeciwnika oraz wprowadzanie w obieg transmisyjny odpowiednich informacji za pośrednictwem środków masowego przekazu, kanałów łączności rządowej i wojskowych kanałów systemów dowodzenia
- sposoby umożliwiające wprowadzenie wirusów komputerowych i bomb logicznych do rządowych oraz komercyjnych sieci i systemów informatycznych, jak również układów zdalnego sterowania tymi systemami. Obejmują one szeroki zakres

[52] Autor szerzej opisuje metody ataków w podrozdziale 2.2. niniejszej rozprawy. Patrz: (Tabela: Typologia metod ataków na systemy i obiekty informatyczne.).

przedsięwzięć, między innymi takich jak wprowadzanie na rynek światowy mikroprocesorów skażonych wirusami i innych skażonych elementów elektronicznych przeznaczonych do zastosowania w międzynarodowych sieciach i systemach informacyjnych zarządzanych przez Siły Zbrojne i państwa sprzymierzone.

Wirusy komputerowe, „bomby logiczne" oraz "skażone" komputerowe elementy elektroniczne zainstalowane w broni lub sprzęcie wojskowym dostarczanym potencjalnemu przeciwnikowi, mogą w wybranym przez eksportera momencie unieszkodliwić technikę wojskową przeciwnika[53].

Narzędziem walki informacyjnej mają być również generatory impulsu elektromagnetycznego bardzo dużej mocy (przeznaczone do niszczenia urządzeń elektronicznych nie wyposażonych w specjalne układy ochronne)[54], a nawet środki biologiczne (specjalne mikroby) zdolne do niszczenia obwodów elektronicznych i materiałów izolacyjnych.

Groźba spowodowania nieodwracalnych szkód w zasobach informacyjnych państwa i struktur pozapaństwowych staje się nowym czynnikiem odstraszania w skali globalnej w konfrontacji między ugrupowaniami państw. Najbardziej skomplikowaną formą agresji informacyjnej jest sterowanie procesami decyzyjnymi struktur państwowych przeciwnika przez wprowadzenie do obiegu określonej informacji lub dezinformacji. Można spotkać się z następującymi typami ataku informacyjnego:

- zerwanie procedur wymiany informacji;
- manipulowanie informacją (dezinformacja, zatajenie, zniekształcenie);
- korzystanie z nieautoryzowanego dostępu do zasobów informacyjnych oraz nielegalne zbieranie i używanie informacji;

---

[53] Podczas pierwszej wojny w Zatoce Perskiej, dzięki wirusowi komputerowemu AF/91 (April Fools), podrzuconemu Irakijczykom w układach scalonych drukarek, udało się sparaliżować podczas pierwszych ataków system teleinformacyjny armii Saddama Husajna. Inni autorzy podają inna wersję wydarzeń. Podobno pół roku przez działaniami bojowymi w Zatoce Perskiej, Amerykanie sprzedali do Iraku drukarki komputerowe, wewnątrz których zamontowali specjalne mikronadajniki, które codziennie podawały swoją pozycję do satelitów wywiadowczych. Wywiad wiedział, że są one w centrach dowodzenia armii irackiej. Amerykanie w ten sposób mieli pełny obraz rozmieszczenia celów do uderzeń lotniczych wojsk sprzymierzonych w pierwszym etapie operacji.

[54] Światowe osiągnięcia w dziedzinie budowy generatorów impulsu elektromagnetycznego wytwarzanego metodą wybuchową umożliwiają obecnie produkcję urządzeń użytkowych, o rozmiarach zwykłej walizki, nadających się do zastosowania w siłach zbrojnych. W najbliższym czasie generatory impulsu elektromagnetycznego ulegną dalszej miniaturyzacji i będą mogły być montowane w głowicach pocisków rakietowych lub w bombach. Patrz Załącznik 1 niniejszej rozprawy doktorskiej.

- nielegalne kopiowanie danych zawartych w systemach informatycznych, w tym w bazach i bankach danych;
- masowe niszczenie oprogramowania specjalnego.

Działania tego typu mogą mieć katastrofalne skutki nawet dla strony o wyżej rozwiniętym potencjale informatycznym. Ta forma ataku jest w pewnych sytuacjach zdolna zablokować użycie zarówno broni masowego rażenia, jak i broni konwencjonalnej. Tak więc walka informacyjna stała się ważnym czynnikiem gwarancji stabilności polityczno - wojskowej.

Rozwój sposobów walki informacyjnej nie eliminuje zagrożenia wojskowego, a tylko określa konieczność uwzględniania w programach reform, wojskowych problemów tego typu walki.

Gwarantem sukcesu w działaniach bojowych ma być równoczesne zastosowanie (z najwyższą intensywnością) wszystkich metod i środków walki informacyjnej oraz koncentracja głównego wysiłku na niszczeniu lub obezwładnieniu najważniejszych systemów infrastruktury informacyjnej przeciwnika i systemów dowodzenia. Do grupy najważniejszych systemów zostały zaliczone:

- stacje i posterunki radiolokacyjne;
- sprzęt rozpoznania;
- węzły i linie łączności;
- urządzenia nadawcze i odbiorcze węzłów łączności;
- stacje przekaźnikowe;
- stacjonarne urządzenia systemów nawigacyjnych (w tym satelitarne systemy nawigacyjne);
- stacje radiowe i telewizyjne.

Innymi ważnymi systemami tej kategorii są elementy infrastruktury pomocniczej, takie jak:

- elektrownie;
- linie zasilania;
- stacje transformatorowe[55].

Do listy ważnych systemów wojskowych wprowadzono również te elementy systemów dowodzenia, których zniszczenie lub obezwładnienie może spowodować gwałtowne obniżenie sprawności dowodzenia wojskami i zmniejszyć efektywność

[55] Sektory Infrastruktury Krytycznej Państwa.

prowadzonych operacji wojskowych. Lista ta obejmuje wyposażenie elektroniczne wojskowych i cywilnych struktur kierowania (dowodzenia), takie jak systemy teleinformatyczne, zautomatyzowane systemy dowodzenia, zautomatyzowane systemy wspomagania walki, systemy transmisji danych, systemy łączności, urządzenia zobrazowania sytuacji bojowej. Ponadto zalicza się tu również satelitarne systemy rozpoznania, łączności i nawigacji.

Szczególną formą walki informacyjnej jest zastosowanie środków nieniszczących (broni elektronicznej) przeciwko najważniejszym ogniwom przemysłu zbrojeniowego i regionalnej infrastruktury cywilnej. Ta forma działań może obejmować, na przykład, obezwładnianie systemu dostaw energii elektrycznej, łączności, transportu lub innych ważnych instalacji.

Obecnie wyróżnia się pięć form walki informacyjnej, którymi są podstęp, ochrona tajemnicy wojskowej, operacje psychologiczne, niszczenie fizyczne i walka radioelektroniczna.

Podstęp jest elementem gry strategicznej, która ma umożliwić wpływanie na posunięcia przeciwnika przez wykreowanie w nim fałszywego obrazu istniejącej sytuacji oraz stanu przeciwstawnych mu sił, koncepcji, czasu, charakteru i miejsca ich działań. Ma to skłonić przeciwnika do działania w przewidywalny sposób zgodny z zasugerowanym scenariuszem.

Ochrona tajemnicy obejmuje różnorodne metody ochrony własnych systemów informacyjnych, działania kontrwywiadowcze, maskowanie, ochronę kontrwywiadowczą koncepcji przygotowywanych i prowadzonych operacji oraz przeciwdziałanie radioelektroniczne.

Operacje psychologiczne w walce informacyjnej obejmują podkreślanie i wysoką ocenę własnego stylu życia, zastraszanie żołnierzy i ludności przeciwnika potęgą własnej machiny wojskowej, podkopywanie zaufania strony przeciwnej do jej przywódców wojskowych i cywilnych, budzenie niezadowolenia i stanów psychozy, podburzanie do nieposłuszeństwa i dezercji, nakłanianie do poddania się, rozbudzanie nastrojów defetystycznych.

Niszczenie fizyczne jest realizowane środkami ogniowymi wszystkich rodzajów sił zbrojnych. Atak taki jest wymierzony w pierwszej kolejności przeciwko systemowi łączności, dowodzenia i rozpoznania, w tym w pierwszej kolejności przeciwko systemom wczesnego ostrzegania zarówno naziemnym, powietrznym jak i satelitarnym. Przewiduje się, że w przyszłości fizyczne niszczenie będzie zastąpione przez obezwładnianie funkcjonalne przy użyciu tak zwanej "zdalnej broni

wirusowej" zdolnej do sparaliżowania systemów komputerowych. Wirusy komputerowe mają być wprowadzane zdalnie za pośrednictwem fal radiowych i łączy laserowych rozwiniętych między centralnym komputerem i terminalami użytkowników. Trudno przecenić niebezpieczeństwa związane z możliwościami zdalnego wprowadzania wirusów komputerowych, szczególnie w odniesieniu do zautomatyzowanych systemów dowodzenia strategicznymi siłami rakietowymi.

Walka radioelektroniczna jest jedną z podstawowych form walki informacyjnej, przy czym dużego znaczenia w walce informacyjnej nabierze broń mikrofalowa, wykorzystująca generatory ultrakrótkich fal radiowych pasma SHF. Broń ta ma umożliwić czasowe obezwładnienie systemów dowodzenia, kierowania uzbrojeniem, łączności oraz rozpoznania na wybranych kierunkach i w wyselekcjonowanych rejonach, głównie w wyniku silnych lokalnych zakłóceń radioelektronicznych.

Doświadczenia z ćwiczeń i wojen lokalnych wskazują, że z punktu widzenia efektywnego wykorzystania środków finansowych wzrost liczbowy sprzętu jest obecnie złym kierunkiem zwiększania potencjału bojowego wojsk. Wyposażenie w nowe urządzenia radioelektroniczne i komputerowe środków ogniowych, walki radioelektronicznej, systemów rozpoznania i dowodzenia jest obecnie najszybszą metodą zwiększania efektywności bojowej sił zbrojnych. Możliwości bojowe systemów rozpoznania, dowodzenia i walki radioelektronicznej muszą być uwzględniane przy wszelkich analizach i ocenach sił ugrupowania bojowego zarówno przeciwnika jak i własnego.

Rosnące możliwości bojowe środków ogniowych są rezultatem "intelektualizacji"[56] i jednym ze źródeł obecnej rewolucji w dziedzinie wojskowości. Pierwsza faza procesu "intelektualizacji" powinna doprowadzić do radykalnych zmian w uzbrojeniu wojsk i zasadach zastosowania bojowego środków walki. W następnej fazie, kiedy automatyzacja obejmie procesy decyzyjne dotyczące użycia broni w siłach zbrojnych może dojść do radykalnych zmian organizacyjnych. Doprowadzi to do robotyzacji pola walki i spowoduje radykalne zmniejszenie stanu liczebnego sił zbrojnych przy równoczesnym zwiększeniu potrzeb szkoleniowych. Najprawdopodobniej w tej fazie również zajdą zmiany strukturalne i funkcjonalne w rodzajach wojsk i służb.

---

[56] „Intelektualizacja" uzbrojenia i sprzętu wojskowego to pojęcie, które zostało wprowadzone przez Rosjan dla określenia procesu automatyzacji wykorzystującego cyfrową technikę komputerową.

Procesy "intelektualizacji" środków ogniowych najprawdopodobniej ograniczą ilościową rozbudowę arsenałów zbrojeniowych i zostaną zorientowane na rozwój programów wariantujących warunki i sposoby zwalczania celów. Spowoduje to akumulację "sztucznego potencjału intelektualnego" w programowanych środkach walki. Wyścig zbrojeń wkracza więc w dziedzinę oprogramowania; im bogatszy wachlarz przydatnych programów w funkcjonowaniu autonomicznych środków walki i w systemach podejmowania decyzji, tym większa możliwość skutecznego ich użycia w warunkach bojowych.

Reasumując, współczesne zjawisko waliki informacyjnej posiada następujące cechy[57]:

1. Misją jest zawsze uzyskanie przewagi informacyjnej (przewagi wiedzy nad przeciwnikiem na współczesnym polu walki).
2. Przeciwnik jest „niewidzialny", to znaczy funkcjonuje on w „strukturze wirtualnej" którą tworzą relacje tworzone ad hoc w „przestrzeni cybernetycznej".
3. Terenem działań jest „przestrzeń cybernetyczna" (*cyberspace*), czyli dowolny obszar sieci (globalnej sieci teleinformatycznej i wojskowych sieci teleinformacyjnych oraz łączności satelitarnej).
4. Podstawową formą są „cyberataki" o wielorakich źródłach i różnorodnych formach (w tym „cyberterrorystyczne").
5. Obiektem „cyberataków" jest Krytyczna Infrastruktura Państwa, jej poszczególne elementy i podsystemy oraz elementy infrastruktury systemów np. typu C4ISR (Infrastruktura Krytyczna Sił Zbrojnych).
6. Czynnikiem krytycznym jest czas, w tym zdolność do wykonania cybernetycznych uderzeń uprzedzających prowadzących do dezorganizacji i utraty zdolności sterowania przez podstawowe systemy przeciwnika.
7. Walka informacyjna może:
   - stanowić element każdej operacji militarnej, a także „operacji innej niż wojna";
   - mieć ograniczony zasięg (np. tylko dany rejon lub region);
   - mieć zasięg nieograniczony, czyli może być prowadzona w dowolnym miejscu i w dowolnym czasie;

---

[57] Opracowano na podstawie Sienkiewicz P., Świeboda H., *Teoretyczne podstawy walki informacyjnej*, Zeszyty Naukowe Nr 2 (72), AON, Warszawa 2008 r.

- może mieć zasięg globalny, czego skutkiem może być dezorganizacja globalnej sieci informacyjnej.

8. Walka informacyjna (*cyberwar*) wymaga rekonstrukcji paradygmatu bezpieczeństwa i obrony państwa oraz prowadzenia wojny.
9. Nowy paradygmat „wojny cybernetycznej" wymaga odejścia od liniowego postrzegania sytuacji i przyjęcia „sieciowego" myślenia i działania, zakładającego konieczność postrzegania sytuacji jako „sieci nieliniowych sprzężeń zwrotnych".
10. „Walka cybernetyczna" może w przyszłości stworzyć warunki do osiągnięcia celów wojny (celów politycznych) nie na „tradycyjnym" polu walki, lecz w „przestrzeni cybernetycznej" za pomocą środków informacyjnych skierowanym przeciw systemom (zasobom) informacyjnym.

2.2. Podstawy teoretyczne cyberterroryzmu

Na przełomie wieków dwa zjawiska zdominowały myślenie o przyszłości. Jedno to globalizacja obejmująca przede wszystkim trzy podstawowe sfery: ekonomię (gospodarkę), politykę i kulturę. Wymaga ona przyjęcia perspektywy interdyscyplinarnej i holistyczno - systemowej w analizowaniu złożonej i dynamicznej rzeczywistości. Istotne znaczenie ma także wymiar technologiczny globalizacji, który – związany ze wzrostem dynamiki zmian w komunikacji i informacji – przyniósł zjawisko swoistego „kurczenia się czasu i przestrzeni" w skali globalnej. Drugim zjawiskiem jest przyspieszony rozwój technologii informacyjnych (teleinformatycznych), którego najbardziej spektakularnym wyrazem jest powstanie Internetu i jego, w zasadzie niekontrolowany rozwój[58].

Oczywiste są konsekwencje rozwoju Internetu dla bezpieczeństwa narodowego i międzynarodowego. Nie należy zapominać i o tym, że pierwsza sieć komputerowa ARPANET[59], powstała w ramach programu realizowanego na zlecenie

---

[58] Sienkiewicz P., Świeboda H., Lichocki E., *Analiza systemowa zjawiska cyberterroryzmu*, Zeszyty Naukowe Nr 2 (63), AON, Warszawa 2006 r. s. 7.

[59] ARPANET powstał jako inicjatywa Departamentu Obrony USA (Pentagonu). W 1958 roku po szoku wywołanym wysłaniem Sputnika w kosmos przez ZSRR powołano rządową agencję ARPA, której zadaniem było obserwowanie i wspieranie inicjatyw powstających na uczelniach w USA, które miały szczególne znaczenie dla obronności Stanów Zjednoczonych. W 1967 roku odbyła się konferencja naukowa ARPA na temat technicznych możliwości budowy rozległych sieci komputerowych o rozproszonym zarządzaniu. Przewodnią ideą tej konferencji było ustalenie, czy możliwe jest

Departamentu Obrony USA. O I wojnie w Zatoce Perskiej w 1991 roku napisano, że była to *The First Information War* (A. Campen). Niedługo potem pojawiły się takie pojęcia jak *Cyberwar, Netwar* oraz *Network Centric Warfare*.

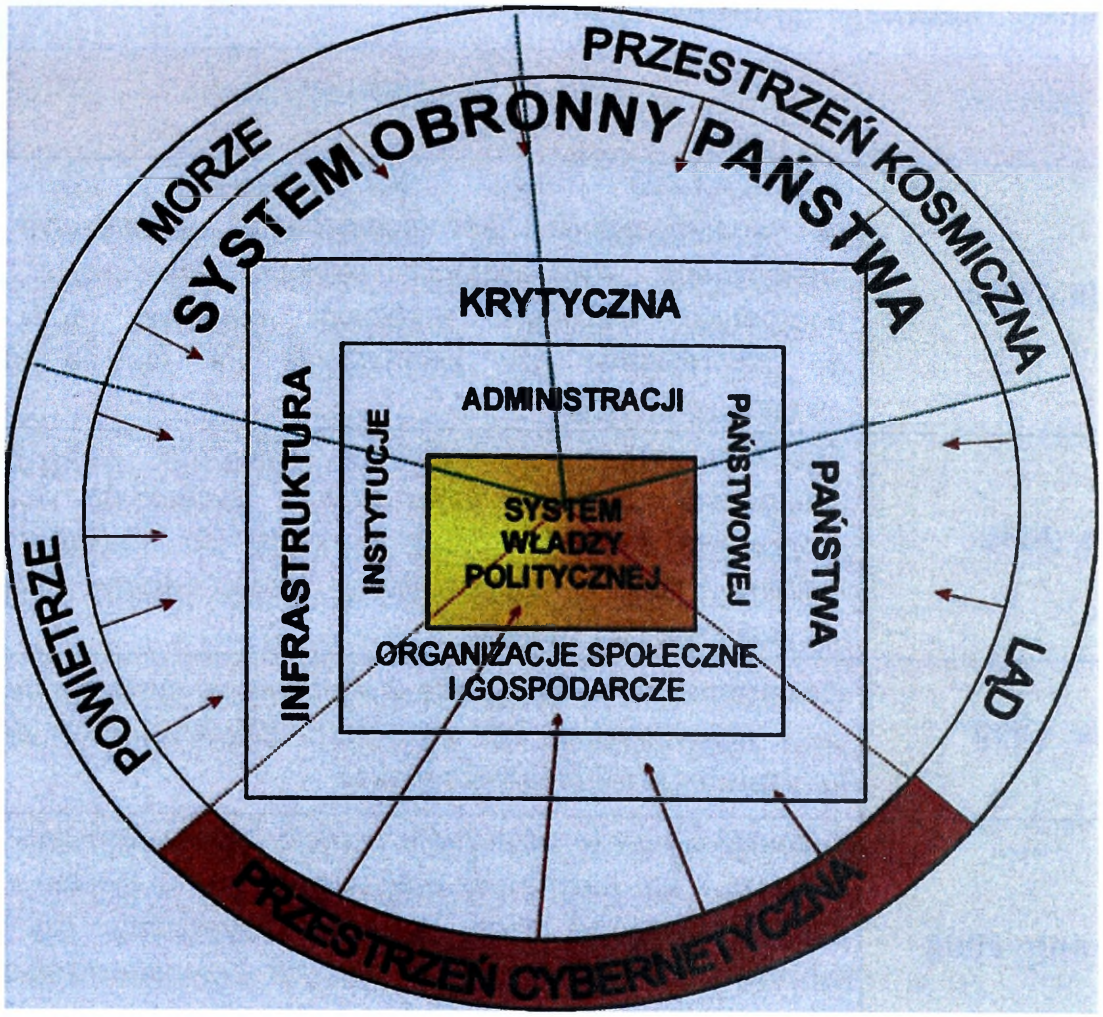
Niejako równolegle do nowych koncepcji walki zbrojnej postępował proces coraz silniejszego uzależniania się od technologii teleinformatycznych we wszystkich niemal sferach życia społecznego, co niewątpliwie wpływało stymulująco na ich efektywność. Jednakże wraz z pojawieniem się nowych zagrożeń w postaci przestępstw komputerowych, istotnym problemem stał się wzrost podatności na zagrożenia informacyjne poszczególnych sektorów Krytycznej Infrastruktury Państwa[60]. Powstało bowiem zjawisko cyberterroryzmu. W 2001 roku prezydent G. W. Bush zwracał uwagę na potrzebę „nowej strategii ogólnej, która wyjdzie poza doktryny zimnej wojny i będzie dotyczyła głównie zagrożeń nowego stulecia – takich jak cyberterroryzm, stosowanie broni masowego rażenia, rakiet – znajdujących się w rękach tych, dla których stosowanie terroru i szantażu jest sposobem na życie [...]."

Na początku lat 90-tych minionego stulecia w popularnym dziś „Modelu Wardena" wyróżniano już piąty wymiar wojny – przestrzeń cybernetyczną (*cyberspace*) (Rys. 2.1.).

---

za pomocą komputerów skonstruowanie takiej sieci łączności (sieci teleinformatycznej), która by nie posiadała węzłów łączności (które wróg może łatwo zniszczyć), lecz umożliwiała automatyczne wyszukiwanie połączeń między dowództwem i jednostkami wojskowymi nawet przy dużym stopniu zniszczenia infrastruktury telekomunikacyjnej kraju. Okazało się to potencjalnie możliwe. Najciekawsze rozwiązanie zaproponował Alex McKenize z Uniwersytetu Stanforda, który zaproponował ideę pakietu informacji z przypisanym do niej adresem, który by automatycznie krążył po sieci "szukając" swojego odbiorcy tak, jak to się dzieje z listami pocztowymi. ARPA zdecydowała się wesprzeć projekt Alexa McKenzie, który stworzył kilkudziesięcioosobowy zespół pracujący na Uniwersytecie Stanford, UCLA i Uniwersytecie Utah. Zespół ten stworzył zręby protokołu TCP (pierwotnie nazwanego IMP) oraz w 1968 wykonał pokaz automatycznego trasowania połączeń w sieci liczącej kilkanaście serwerów rozproszonych na tych trzech uniwersytetach. W latach 1967 - 1972 eksperymentalna sieć rozrastała się na kolejne uczelnie, a rozrost ten był hojnie wspierany finansowo przez ARPA. Badania i rozwój sieci były częściowo tajne, gdyż równolegle z pracami naukowców cywilnych trwały prace nad zaimplementowaniem ich do celów wojskowych. W 1971 roku ARPA zdecydowała się odtajnić protokół TCP/IP i zezwoliła na przyłączanie do ARPANETU lokalnych sieci akademickich. Pierwszą siecią akademicką przyłączoną do ARPANETU była sieć na kampusie UCLA. W latach 1972-1979 kolejne uczelnie USA przyłączały się do projektu ARPANETU i jednocześnie ARPA śledziła wszystkie nowinki techniczne wymyślane na uczelniach i część z nich przekazywała na rzecz tajnych projektów wojskowych. Wielu akademickich użytkowników ARPANETU zaczęło nazywać tę sieć Internetem, ze względu na to, że łączyła ona wiele różnych sieci lokalnych. W 1980 roku, po kilku efektownych włamaniach crackerów do serwerów ARPANETU, ARPA zdecydowała się rozdzielić całkowicie wojskową część ARPANETU od części akademickiej. Część wojskowa nadal ma nazwę ARPANET (MILNET), zaś część cywilna została już oficjalnie nazwana Internetem i zaczęła się od tej pory rozwijać samodzielnie.

[60] Infrastruktura Krytyczna Państwa została szczegółowo opisana w Rozdziale 3 niniejszej rozprawy doktorskiej.



Rysunek 2.1. Przestrzeń zagrożeń bezpieczeństwa w społeczeństwie informacyjnym

Źródło: Opracowano na podstawie: Sienkiewicz P., Świeboda H., Lichocki E., *Analiza systemowa zjawiska cyberterroryzmu*, Zeszyty Naukowe Nr 2 (63), AON, Warszawa 2006 r.

Jak dotąd nie przyjęto na świecie jednolitej definicji cyberterroryzmu. Naukowcy i specjaliści zajmujący się problematyką tego zjawiska, wskazują na kłopot w zdefiniowaniu tego zagadnienia. Ciężko jest obecnie stwierdzić, czy mieliśmy już do czynienia z atakiem cyberterrorystycznym, czy też nie. Poniżej przedstawiam kilka istniejących w literaturze definicji cyberterroryzmu (Tabela 2.2.)[61].

[61] Jemioło T., Kisielnicki J., Rajchel K., *Cyberterroryzm nowe wyzwania XXI wieku*, Wyższa Szkoła Policji, Warszawa 2009 r. s. 585.

Tabela 2.2. Definicje cyberterroryzmu

AUTOR	DEFINICJA
Lewis, 2002	*Wykorzystanie sieci komputerowych jako narzędzia do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka transport, instytucje rządowe, itp.), bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań.*
Pollit, 2005	*Cyberterroryzm to przemyślany, politycznie umotywowany atak, skierowany przeciw informacjom, systemom komputerowym, programom i danym, który prowadzi do oddziaływania na nie militarne cele, przeprowadzony przez grupy narodowościowe lub przez tajnych agentów.*
White, 1998	*Cyberterroryzm to świadome wykorzystanie systemu informacyjnego, sieci komputerowej lub jej części składowych w celu wsparcia lub ułatwienia terrorystycznej akcji.*
Denning, 2000	*Cyberterroryzm to połączenie pojęcia cyberprzestrzeni i terroryzmu. To groźba lub bezprawny atak wymierzony w system informatyczny lub zgromadzone dane, w celu zastraszenia czy wymuszenia na władzach państwowych lub jej przedstawicielach, ustępstw lub oczekiwanych zachowań, w celu wsparcia określonych celów (np. politycznych).*
Kośla, 2002	*Działania blokujące, niszczące lub zniekształcające w stosunku do informacji przetwarzanej, przechowywanej i przekazywanej w systemach teleinformatycznych oraz niszczące (obezwładniające) te systemy.*
Verton, 2004	*Politycznie umotywowana, przemyślana działalność grup narodowych lub innych wrogich sił wymierzona przeciw informacji, systemom komputerowym, programom i danym, która powoduje straty cywilne.*
Sienkiewicz, 2009	*Działania terrorystyczne w cyberprzestrzeni.*

Opracowanie własne na podstawie: Denning D. E., *Cyberterrorism, Global Dialogue*, August 24, 2000, [URL - http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc] 16.11.2005 r., Kośla R., *Cyberterroryzm - definicja zjawiska i zagrożenie dla Polski.* Wystąpienie na konferencji w Bemowie, 29 listopada 2002 r.,[URL http://www.abw.gov.pl/] 11.02.2005 r., Lewis J. A., Assessing *The risk of cyber terrorism, cyber war and other cyber threats*, Center for Strategic and International Studies 2002 r., [URL - http://www.csis.org/tech/0211_lewis.pdf] 14.11.2005 r., Pollit M. M., *Cyberterrorism - Fact or Fancy?*, [URL – http://www.cs.georgetown.edu/~denning/infosec/pollitt.html] 14.11.2005 r., White K. C., *Cyber Terrorism: Modem Mache*, Carlisle 1998 r. oraz Jemioło T., Kisielnicki J., Rajchel K., *Cyberterroryzm nowe wyzwania XXI wieku*, Wyższa Szkoła Policji, Warszawa 2009 r.

Należy nadmienić, że D. M. Denning uzupełniła swoją definicję o stwierdzenie, że za atak cyberterrorystyczny można uznać tylko taki akt, który powoduje bezpośrednie szkody człowiekowi i jego mieniu lub przynajmniej jest na tyle

znaczący, że budzi strach. Jako przykład podaje śmierć człowieka, obrażenia ciała, wybuch, zderzenie samolotów lub spowodowanie strat finansowych. Akty nie wywołujące takich skutków, według niej, nie są atakami cyberterrorystycznymi. W definicji cyberterroryzmu może mieść się również wykorzystywanie systemów teleinformatycznych do dezinformacji oraz walki psychologicznej[62]. Celem ataku jest najczęściej informacja przetwarzana, a nie system jako taki[63].

Powyższe definicje cyberterroryzmu nie są niczym innym, jak tylko różnymi ujęciami definicji terroryzmu rozszerzonego o spektrum cyberprzestrzeni. Pomimo różnic definicyjnych autorzy tych definicji starają się podawać znaczenia rozszerzające. Prawdopodobnie, by uniknąć pominięcia okolicznych interakcji i reakcji towarzyszących definiowanemu zjawisku. Dla potrzeb niniejszej rozprawy, przyjęto następującą definicję:

Cyberterroryzm to przemyślany politycznie lub militarnie motywowany atak albo groźba ataku na systemy teleinformatyczne oraz zgromadzone dane w celu sparaliżowania lub poważnego zniszczenia Infrastruktury Krytycznej Państwa oraz zastraszenia i wymuszenia na rządzie lub społeczności daleko idących polityczno – militarnych działań. Cyberatak może być przeprowadzony jako część składowa większej polityczno – militarnej akcji lub samodzielnego ataku.

Cyberterroryzm jest to również świadome wykorzystanie systemów teleinformatycznych oraz globalnej sieci Internet przez organizacje terrorystyczne do propagandy, rekrutacji, komunikacji, mobilizacji, zbierania informacji o potencjalnych celach ataku, planowania i koordynacji akcji oraz szeroko pojętej dezinformacji i walki psychologicznej.

Cyberterroryzm traktowany jako *soft terrorism*, rozumiany jest najczęściej, jako działania mające na celu niszczenie bądź zniekształcanie informacji przesłanej, przetwarzanej i przechowywanej w systemach teleinformatycznych. Można także najkrócej ująć to jako działania terrorystyczne w przestrzeni cybernetycznej. Mogą

---

[62] Kośla R., *Cyberterroryzm - definicja zjawiska i zagrożenie dla Polski.* Wystąpienie na konferencji w Bemowie,29 listopada 2002 r.,[URL http://www.abw.gov.pl/] 11.02.2005 r

[63] Lichocki E., *Bezpieczeństwo teleinformatyczne Sił Zbrojnych Rzeczypospolitej Polski w dobie zagrożeń cybernetycznych*, Konferencja naukowa „Cyberterroryzm nowe wyzwania XXI wieku", Wyższa Szkoła Informatyki , Zarządzania i Administracji, Warszawa 18.05.2009 r.

być one dziełem wielu wielce zróżnicowanych podmiotów, tak jak różne, to jest o różnej skali i intensywności, mogą być ich następstwa.

Przyjmując cyberterroryzm, jako politycznie motywowany atak lub groźbę 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, możemy wyróżnić dwa rodzaje akcji cyberterrorystycznych:

- destrukcyjne działania informacyjne w cyberprzestrzeni;
- ataki fizyczne na systemy teleinformatyczne[64].

Powyższe oczywiście akcje mogą się wzajemnie uzupełniać. Zapewne w niedalekiej przyszłości możemy być świadkami zsynchronizowanego ataku, polegającego na cybernetycznym sparaliżowaniu sieci telefonicznej lub elektrycznej i jednoczesnym użyciu np. materiałów wybuchowych. Organizacje terrorystyczne doskonale zdają sobie sprawę ze znaczenia zasobów informacyjnych we współczesnym świecie, a także zakładają, że atak paraliżujący infrastrukturę teleinformatyczną może przynieść większy efekt, niż „zwykły" akt terrorystyczny.

Po raz pierwszy termin „cyberterroryzm" pojawił się w raporcie o zagrożeniach komputerowych w Szwecji, w 1979 r. Obejmował on wszelką działalność z użyciem komputerów mającą na celu niszczenie systemów teleinformatycznych, systemów nadzoru i kontroli, programów, danych itp., a w konsekwencji zastraszanie rządów i społeczeństw, wywieranie presji psychologicznej, doprowadzenie do zagrożenia życia lub powstania znacznych strat materialnych.

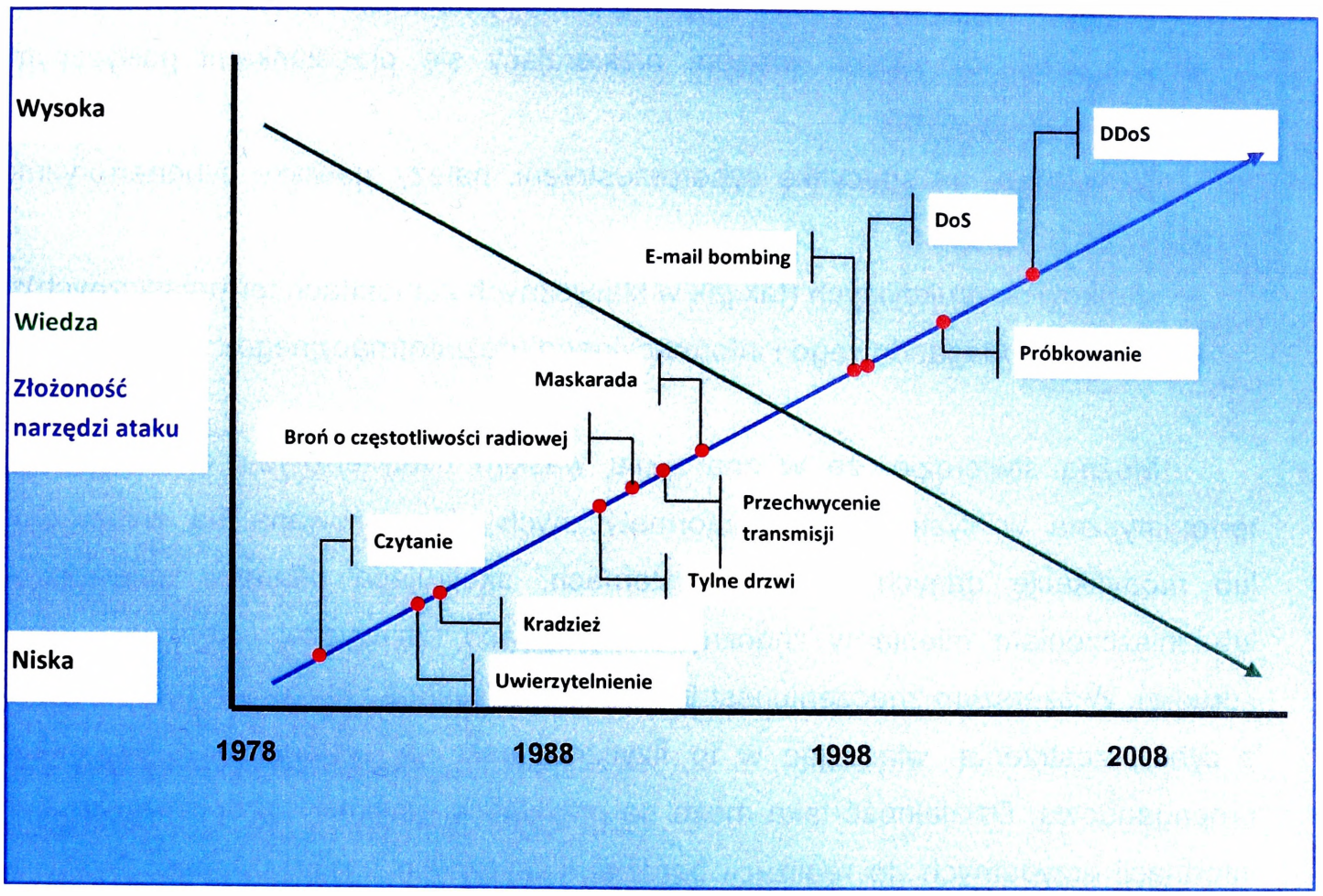
W latach 80-tych terminem cyberterroryzmu posługiwano się w amerykańskich służbach specjalnych, wskazując na możliwości przeprowadzenia ataków elektronicznych przez wrogów Stanów Zjednoczonych. W 1998 r. w Centrali FBI utworzono Centrum Ochrony Infrastruktury Narodowej (NIPC), którego zadaniem jest koordynowanie działań w zakresie gromadzenia informacji o zagrożeniach, reagowanie na zagrożenia informacyjne lub zamachy na elementy Krytycznej Infrastruktury Państwa.

Umasowienie dostępu do komputerów sprawia, że stają się one coraz prostsze w obsłudze. Obecnie wystarczy wiedzieć, gdzie się włącza komputer, aby móc się nim posługiwać. Podobnie jest z narzędziami potrzebnymi do dokonywania cyberataków. W Internecie można znaleźć bardzo wiele programów,

---

[64] Sienkiewicz P., Świeboda H., Lichocki E., *Analiza systemowa*..., op.cit., s. 8.

które umożliwią odszyfrowanie kodu dostępu do komputera lub bazy danych, czy włamanie się do systemu. Wraz ze zmniejszaniem się potrzebnych umiejętności do przeprowadzenia cyberataku, zwiększa się skuteczność i jakość programów mających to ułatwić. W konsekwencji każdy może zostać „cyberterrorystą" (Rys. 2.2.).



Rysunek 2.2. Przykładowa skuteczność narzędzi do cyberataku, przy jednoczesnym zmniejszeniu się wiedzy potrzebnej do jego dokonania

Źródło: Opracowanie własne.

Po wydarzeniach z 11 września 2001 r. zwrócono uwagę na możliwość podobnych ataków terrorystycznych na całym świecie, w tym na możliwe i prawdopodobne zmasowane „cyberataki" na systemy teleinformatyczne USA i sprzymierzeńców wykorzystywane w walce ze światowym terroryzmem. Wówczas w amerykańskiej ustawie antyterrorystycznej rozszerzono definicję terroru o cyberterroryzm[65].

[65] Ustawa o *Bezpieczeństwie Krajowym* z 2002 r. (*np. hakerska penetracja systemów informacyjnych o dużym znaczeniu dla bezpieczeństwa narodowego zagrożona jest w USA nawet karą dożywotniego więzienia).*

W raporcie pod tytułem: "Cyberataki podczas wojny z terroryzmem", opracowanym przez *Institute for Security Technology Studiem* wyróżniono cztery podstawowe potencjalne kategorie źródeł cyberterroryzmu, a mianowicie:

- typowe grupy terrorystyczne;
- „państwa zbójeckie", do których mogą dołączyć inne kraje np. Chiny, Kuba, Rosja);
- sympatycy terrorystów oraz antyamerykańscy hakerzy;
- poszukiwacze silnych wrażeń, niekierujący się przesłankami politycznymi lub ideologicznymi.

Ze względu na specyfikę cyberprzestrzeni, należy zjawisko cyberterroryzmu rozpatrywać w aspekcie:

- skutków destrukcyjnych (tak jak w klasycznych zamachach terrorystycznych);
- środka propagandowego i informacyjnego (dezinformacyjnego).

Można stwierdzić, że w znaczeniu wąskim cyberterroryzm to działalność terrorystyczna w systemach teleinformatycznych ukierunkowana na zniszczenie lub modyfikację danych w tych systemach, skutkująca ofiarami śmiertelnymi lub zniszczeniem mienia w znacznych rozmiarach (zazwyczaj celem jest jedno i drugie). W szerszym znaczeniu jest to wszelka działalność terrorystyczna związana z cyberprzestrzenią, włączając w to fizyczne ataki na systemy oraz aktywność propagandową. Działalność taka może na przykład przyczynić się do pozyskiwania informacji przydatnych do realizacji bardziej klasycznych akcji terrorystycznych, na przykład zamachów bombowych[66].

Aktywność w sieciach teleinformatycznych umożliwia organizacjom terrorystycznym:

- możliwość destrukcyjnego wpływu na działalność szeregu instytucji zarówno państwowych (cywilnych oraz wojskowych), jak i niepaństwowych[67];
- bezpieczne komunikowanie się ze sobą, w tym przesyłanie danych;

---

[66] Liczne przykłady funkcjonowania stron www poświęconych terroryzmowi (szacuje się, że stron poświęconych tylko dżihadowi jest w sieci około 200 – 300) potwierdzają efektywne i często efektowne narzędzie propagandy terrorystów. W sieci można przeczytać o organizacjach i ich celach. Niektóre z nich oferują sprzedaż „gadżetów", takich jak koszulki, plakaty, kasety video itp.; inne werbują za pomocą Internetu ochotników do walki ze swoimi przeciwnikami, oferują informacje typu jak dokonać zamachu terrorystycznego, skonstruować bombę, na niektórych wreszcie są informacje jak dofinansować przedsięwzięcia o charakterze przestępczym.

[67] Adamski J., *Nowe technologie w służbie terrorystów*, Collegium Civitas TRIO, Warszawa 2007 r. s. 92.

- działalność informacyjno – propagandową. Zdolność zakłócania mediów i przestawiania fałszywego obrazu sytuacji;
- pozyskiwanie informacji z różnych działań w tym pozyskanych z penetracji stron www;
- możliwość działalności o zasięgu ogólnoświatowym;
- niski koszt przygotowania operacji;
- małe ryzyko dla wykonawców akcji terrorystycznych;
- działalność terrorystyczną sensu stricte, na przykład próby spowodowania katastrofy samolotowej na skutek zniekształcenia danych w systemach kontroli lotnisk.

Internet stał się pozbawionym granic swoistym obozem szkoleniowym, trudnym do zlokalizowania dzięki sprawności i szybkości zacierania śladów działań w sieci. Specjaliści prognozują nasilenie tego typu działalności szczególnie islamskich terrorystów. Od kilku lat w sieci toczy się „cyberwojna", nasilona od momentu przedruku karykatur Mahometa, efektem której są natężone ataki hakerów islamskich na strony internetowe państw zachodnich.

Cyberterroryzm nie jest oczywiście jedynym, ale jest z pewnością najważniejszym z zagrożeń bezpieczeństwa teleinformatycznego (Rys. 2.3.).



Rysunek 2.3. Typologia zagrożeń dla bezpieczeństwa
Źródło: Opracowano na podstawie: Sienkiewicz P., Świeboda H., Lichocki E., *Analiza systemowa zjawiska cyberterroryzmu*, Zeszyty Naukowe Nr 2 (63), AON, Warszawa 2006 r.

Oprócz znanych zagrożeń „naturalnych" (np.: pożary, awarie budynków itp.) oraz zagrożeń wynikających z zawodności środków technicznych i programowych, szczególne znaczenie mają te, które są rezultatem działalności ludzi. Mniej groźne wydają się być zagrożenia niezamierzone, będące konsekwencjami niewłaściwego doboru personelu lub ich ograniczeniami zawodowymi (niedostateczne kwalifikacje, brak opanowania określonych procedur itp.) Nie można ich jednak lekceważyć, gdyż ignorancja i arogancja była niemal zawsze przyczyną poważnych katastrof technicznych i technologicznych. Natomiast szczególne znaczenie mają zagrożenia związane z celowymi działaniami podejmowanymi zarówno przez własny personel (np.: niezadowoleni pracownicy, sfrustrowani, dążący do zemsty z powodu realnych i urojonych krzywd doznanych ze strony pracodawców, ale także w celu uzyskania korzyści materialnych), jak i tych, które są dziełem zewnętrznych hakerów, crakerów i terrorystów. Dostępne dane statystyczne wskazują na szczególną dotkliwość przestępstw dokonywanych przez własnych pracowników instytucji publicznych i prywatnych. Straty spowodowane zmasowanym cyberatakiem na Krytyczną Infrastrukturę Państwa są po prostu trudne do oszacowania, bowiem mogą spowodować paraliż funkcjonowania wielu sfer życia społecznego. Eksperci z Pentagonu oszacowali, że odpowiednio przygotowane i skoordynowane cyberuderzenie przez około 30 specjalistów od systemów teleinformatycznych i teleinformacyjnych, rozlokowanych na całym świecie, z budżetem około 10 mln dolarów, może Stany Zjednoczone „rzucić na kolana"[68].

Imperatywem rozwoju staje się modernizacja, budowa i ochrona Krytycznej Infrastruktury, a polityka w tym zakresie stanowi i stanowić będzie w najbliższych latach jedną z priorytetowych części strategii bezpieczeństwa państwa. Ogólnie biorąc, Krytyczna Infrastruktura Państwa, to - części infrastruktury kraju wraz procesami zachodzącymi między nimi, których ciągłość działania jest na tyle ważna dla funkcjonowania państwa, że jej utrata, przerwy w działaniu czy znaczące obniżenie jakości działania mogą spowodować poważne konsekwencje ekonomiczne, społeczne, zagrażające życiu i funkcjonowaniu społeczeństwa.

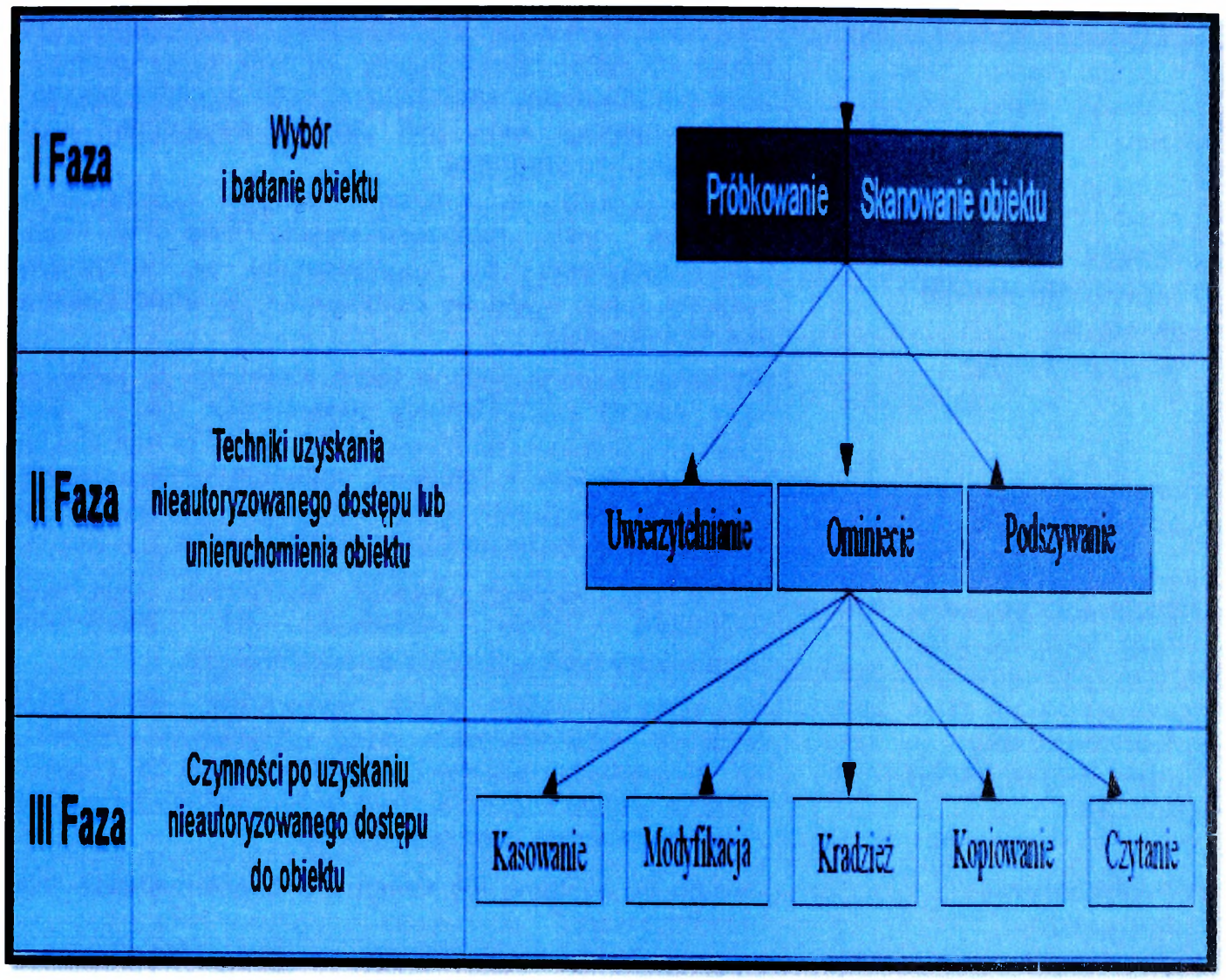
W typowym procesie „cyberataku" można wyróżnić trzy podstawowe fazy (Rys. 2.4.), z których:

- pierwsza obejmuje „próbkowanie" (skanowanie), będące formą rozpoznania słabych stron obiektu (systemu);

---

[68] Sienkiewicz P., Świeboda H., Lichocki E., *Analiza systemowa zjawiska cyberterroryzmu*, Zeszyty Naukowe Nr 2 (63), AON, Warszawa 2006 r. s.8.

- druga wiąże się z uzyskaniem dostępu do zasobów systemu;
- trzecia zaś stanowi realizację właściwego celu działania.



Rysunek 2.4. Model cyberataku na obiekty i teleinformatyczne
Źródło: Opracowano na podstawie: Sienkiewicz P., Świeboda H., Lichocki E., *Analiza systemowa zjawiska cyberterroryzmu*, Zeszyty Naukowe Nr 2 (63), AON, Warszawa 2006 r.

Sprawców zagrożeń informacyjnych dla bezpieczeństwa organizacji i instytucji można podzielić na dwie kategorie:

- sprawców zagrożeń „ustrukturalizowanych", do których należy zaliczyć organizacje państwowe (agendy, specjalistyczne jednostki), organizacje terrorystyczne i różnego rodzaju transnarodowe jednostki (grupy) przestępcze;
- sprawców zagrożeń „nieustukturalizowanych" (np.: przestępcy, frustraci, wandale, hakerzy, crakerzy itp.).

W Tabeli 2.3. przedstawiono typologię metod ataków na systemy teleinformatyczne.

Tabela 2.3. Typologia metod ataków na systemy i obiekty informatyczne

METODA ATAKU	CEL DZIAŁANIA, RODZAJ MOŻLIWYCH ATAKÓW
Wirusy, robaki, bakterie (oprogramowanie złośliwe) (ang. *malware*)	**Wirus** to samo reprodukujący się kod, który uszkadza dane lub programy, zmieniając sposób działania sprzętu. Inaczej mówiąc, wirus jest „obcym" fragmentem kodu dołączonym do programu. **Robak** (worm), to program, którego podstawowym zadaniem jest rozprzestrzenianie się w sieci teleinformatycznej. Po zagnieżdżeniu się w nowym systemie robak może się zachowywać jak wirus, bakteria albo koń trojański. **Bakteria** (bakteria, zwana także królikiem), to program, który wprost nie powoduje uszkodzenia plików. Jego jedynym zadaniem jest rozmnażanie. Bakterie reprodukują się wykładniczo i zajmują ogromną ilość pamięci procesora, przestrzeni dyskowej i innych zasobów, przez co użytkownik nie może z nich dalej korzystać.
Bomba logiczna (ang. *logic bomb*)	Aktywizacja nowych funkcji elementów logicznych komputera, która prowadzi do zniszczenia lub zdeformowania sprzętu i oprogramowania.
Koń trojański (ang. *trojan, trojan horse*)	To program, który może wykonywać niepożądane działanie, nieprzewidziane przez użytkownika programu, np. usuwać pliki, ponownie formatować dysk lub przesłać dane do swego twórcy, oczywiście bez zgody użytkownika programu a nieraz i bez jego wiedzy.
Próbkowanie (ang. *probe*)	Dostęp do systemu lub komputera poprzez analizę jego charakterystyki.
Uwierzytelnianie (ang. *authenticate*)	Przedstawienie się jako osoba uprawniona oraz w razie konieczności przekazanie informacji potrzebnej do poprawnego uwierzytelniania.
Ominięcie (ang. *bypass*)	Ominięcie procesu zabezpieczającego system poprzez zastosowanie alternatywnej drogi osiągnięcia obiektu.
Czytanie (ang. *read*)	Dostęp do informacji, do której brak jest uprawnienia.
Kopiowanie (ang. *copy*)	Możliwość tworzenia kopii informacji przez osoby nieuprawnione.
Kradzież (ang. *steal*)	Przejęcie zasobów systemu lub komputera przez osobę nieuprawnioną, bez pozostawienia kopii w obiekcie.
Modyfikacja (ang. *modilfy*)	Zmiana zawartości danych lub charakterystyki obiektu ataku.
Usunięcie (ang. *delete*)	Zniszczenie obiektu ataku.
Złośliwe podzespoły (ang. *chipping*)	Umieszczanie w komputerach chipów, które mogłyby zawierać programy, dające dostęp do systemów lub wady konstrukcyjne, które umożliwiły by zniszczenie sprzętu komputerowego.

Tylne drzwi (ang. *back door*)	Twórcy oprogramowania są w stanie zostawić sobie „furtkę", przez którą mogą się dostać do komputerów osób korzystających z ich programów.
Podszywanie się, maskarada (ang. *IP spoofing*)	Polega na udawaniu przez atakującego jednego z użytkowników systemu, który posiada własny adres IP. Przedstawienie się lub modyfikowanie pakietów w trakcie połączenia, aby osiągnąć prawo dostępu do zasobów.
Przechwycenie transmisji (ang. *hijacking*)	Przechwycenie transmisji odbywającej się między dwoma systemami czy komputerami. Dzięki temu, możliwe jest uzyskanie dostępu do poszczególnych chronionych informacji i programów.
Tropienie, podsłuchiwanie (ang. *sniffing*)	Polega na śledzeniu ruchu w sieci. Specjalne programy wyłapują wiadomości przemieszczające się w sieci i wybrane kopiują na dysk.
Receptor van Ecka (ang. *Electromagnetic Radiation – EMR*)	Podsłuchiwacz, dysponujący odpowiednim sprzętem, może oglądać na oddzielnym monitorze repliki obrazów wyświetlanych na ekranie atakowanego komputera.
DoS (ang. *Denial of service*), DDoS (ang. *distributed denial of service*)	Są to działania typu przepełnienia (ang. flooding), mające na celu zablokowanie konkretnego serwisu sieciowego lub zawieszania komputera, poprzez przesłanie olbrzymiego pakietu danych z różnych źródeł. Ataki tego typu mogą doprowadzić do awarii sieci teleinformatycznej lub teleinformacyjnej. DoS różni się od DDoS tym, że ten drugi typ ataku poprzedzony jest spenetrowaniem przez cyberterrorystę wielu internetowych serwerów i zamienienie ich w zombies. W ten sposób wykonuje się atak z wielu źródeł na ten sam cel jednocześnie[69].
E – mail bombing	Bombardowanie serwera pocztowego ogromną ilością poczty elektronicznej, niejednokrotnie z załączonymi wielkimi załącznikami. Skrzynka adresata (ofiary) jest przepełniona i żaden list nie ma szans się dostać.
Broń o częstotliwości radiowej (ang. *Electromagnetic Pulse, EMP*)	Urządzenia emitujące promieniowanie elektromagnetyczne należące do widma radiowego. Używa się jej do zniszczenia technicznych urządzeń elektronicznych oraz zbiorów informatycznych. Celowe użycie energii elektromagnetycznej o dużej mocy. Taka broń nie wymaga bezpośredniego trafienia w cel, co często bywa trudne. Zapewne największa zaletą tej broni jest to, że nosi ona etykietkę "nie zabójczej". Nie trzeba niszczyć wszystkiego[70].

Źródło: Opracowanie własne na podstawie: Bógdał – Brzezińska A., Gawrycki M. F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie,* Warszawa 2003 r., Sienkiewicz P., Świeboda H., Lichocki E., *Analiza systemowa zjawiska cyberterroryzmu*, Zeszyty Naukowe Nr 2 (63), AON, Warszawa 2006 r. oraz Adamski J., *Nowe technologie w służbie terrorystów*, Collegium Civitas TRIO, Warszawa 2007 r.

[69] Najczęściej wykonywana obecnie metoda ataku przez cyberterrorystów.
[70] CBS NEWS w wiadomościach z dnia 25.03.2003 r. doniosło o użyciu w Bagdadzie przez U.S AIR FORCE po raz pierwszy bojowo eksperymentalnej broni wykorzystującej impuls elektromagnetyczny, zwanej „Bombą – E".

Złożoność samego zjawiska i świadomość braku doskonałych systemów zabezpieczeń powoduje, że zagrożenie bezpieczeństwa teleinformatycznego, w szczególności zaś cyberterroryzm stały się nowym wyzwaniem dla bezpieczeństwa narodowego a zarazem bezpieczeństwa informacyjnego Sił Zbrojnych Rzeczypospolitej Polski.

2.3. Bezpieczeństwo informacyjne i jego zagrożenia

W dobie rozwoju systemów teleinformatycznych zmieniają się również sposoby rozumienia terminów, dochodzi bardzo często do mieszania pojęć. Dlatego na wstępie należy doprecyzować poszczególne pojęcia.

Słownik Języka Polskiego definiuje termin bezpieczeństwo jako „Stan niezagrożenia, spokoju, pewności [71] . Możemy wiec powiedzieć, że bezpieczeństwo jest stanem, w którym nie istnieje żadne zagrożenie[72].

W inny sposób pojęcie bezpieczeństwa interpretuje się w środowisku wojskowym. S. Koziej uważa, że „W sensie najogólniejszym (bezpieczeństwo) to zdolność przeciwstawiania się wszelkiego rodzaju zagrożeniom"[73].

Na skutek gwałtownych przewartościowań geostrategicznych w ostatnim dwudziestoleciu, znaczenie terminu „bezpieczeństwo" uległo rozszerzeniu a nawet częściowemu przesunięciu [74] . Zmodyfikowane w erze powszechnej globalizacji pojęcie bezpieczeństwa ma propagować model rozwoju współczesnego świata, którego celem jest tworzenie ponadnarodowych organizacji polityczno – gospodarczych. Specjaliści od bezpieczeństwa nie ukrywają, że tego typu model niesie obecnie za sobą więcej zagrożeń niż ewentualnych korzyści[75].

Bezpieczeństwo jest pojęciem używanym do określenia stanu pewności, spokoju i braku zagrożenia. Obejmuje ono zaspokojenie takich potrzeb jak: istnienie, przetrwanie, integralność, tożsamość, niezależność, spokój, posiadanie, pewność rozwoju itp.

---

[71] Słownik Języka Polskiego, PWN, Tom I, Warszawa 1978 r., s. 147.
[72] Słownik Języka Polskiego, PWN, Tom I, Warszawa 2000 r., s. 84.
[73] Koziej S., *Koncepcja wspólnego bezpieczeństwa w Europie a obronność Polski*, Wystarczalność Obronna, Warszawa 1996 r., s. 18.
[74] Czaputowicz J., *System czy nieład? Bezpieczeństwo europejskie u progu XXI wieku*, Warszawa 1998 r., s. 23 – 26.
[75] Mąka D., *Ryzyko w systemie bezpieczeństwa informacyjnego państwa w aspekcie standardów NATO i Unii Europejskiej*, Rozprawa doktorska, AON, Warszawa 2004 r. s. 41.

W ujęciu wewnętrznym obejmuje stabilność i harmonijność danego podmiotu, a w ujęciu zewnętrznym - brak zagrożenia ze strony innych podmiotów lub czynników zewnętrznych. Z kolei, ujęcie negatywne bezpieczeństwa wskazuje na brak zagrożeń dla istotnych wartości podmiotu (bezpieczeństwo definiowane jest jako przeciwieństwo zagrożenia), pozytywne natomiast – uwypukla kształtowanie pewności przetrwania, posiadania i swobód rozwojowych podmiotu (zapewnienie kreatywnej aktywności podmiotu).

W znaczeniu potocznym pojęcie bezpieczeństwa jest związane z osiąganiem stanu spokoju, niezagrożenia i od wieków odnosi się do różnych działalności człowieka. Wraz z rozwojem technologii teleinformatycznych pojawił się problem zapewnienia bezpieczeństwa teleinformatycznego oraz środowisk, w których są zastosowane, tak by przetwarzaną w nich informację (wytwarzanie, przesyłanie, odbieranie, przechowywanie oraz niszczenie) można było uważać za bezpieczne. W tym przypadku bezpieczeństwo teleinformatyczne rozumiane jest jako niezakłócone funkcjonowanie systemów teleinformatycznych podczas realizacji wyznaczonych dla nich zadań.

Ogólnie bezpieczeństwo informacji na szersze znaczenie niż bezpieczeństwo teleinformatyczne ponieważ obejmuje także informację znajdującą się poza systemami teleinformatycznymi, a więc występującą na przykład w postaci dokumentów papierowych lub mikrofilmów oraz w postaci zapamiętanych i wymienianej przez człowieka bezpośrednio lub za pomocą środków łączności[76].

Podstawową rolę dla współczesnych Sił Zbrojnych RP odgrywa elektroniczna postać informacji przesyłana w systemach, z czego wynika wielkie znaczenie bezpieczeństwa teleinformatycznego, choć jak można zauważyć nie pokrywa ono całości zagadnienia związanego z bezpieczeństwem informacji. Stąd też bezpieczeństwo informacji jest bardzo często w literaturze fachowej utożsamiane z bezpieczeństwem teleinformatycznym.

Z punktu widzenia technicznego, wymaga się bardziej precyzyjnego określenia pojęcia „bezpieczeństwa", niż wcześniej przytoczone definicję. Bezpieczeństwo teleinformatyczne, czyli odnoszące się do systemów teleinformatycznych (ang. *Information and Communication Technology ICT*), jest ściśle związane ze spełnieniem wartości zwanych atrybutami bezpieczeństwa

[76] Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa 2006 r. s. 27.

w systemach oraz w ich otoczeniu. Do atrybutów bezpieczeństwa zalicza się: integralność, poufność, dostępność, autentyczność, rozliczalność oraz niezawodność. Należy jeszcze nadmienić, że systemy pracują dla człowieka[77] i są obsługiwane przez człowieka. Komplikuje to całość problematyki i wnosi do nich dodatkowe, pozatechniczne wymiary, takie jak: prawny, socjologiczny oraz psychologiczny.

Systemy teleinformatyczne występują w coraz bardziej odpowiedzialnych zastosowaniach w Siłach Zbrojnych RP, stąd ich bezpieczeństwo nabiera coraz bardziej szczególnie dużego znaczenia. Należy tutaj wspomnieć o ochronie Krytycznej Infrastruktury Teleinformatycznej Sił Zbrojnych RP (KITI SZ RP) oraz o wdrażaniu i rozwoju technologii teleinformatycznych w Siłach Zbrojnych RP.

Zarządzenie bezpieczeństwem teleinformatycznym ma na celu zapewnienie bezpieczeństwa systemów i znajdującym się w nich informacji [78] w sytuacji występowania wielu trudności i przeciwieństw. Największe z nich to:

- systemy teleinformatyczne są trudne do zarządzania, gdyż są bardzo złożone, rozproszone, szybkie i niezwykle zróżnicowane pod względem technologicznym;
- systemy teleinformatyczne i ich otoczenie ulegają permanentnym zmianom;
- środowisko zagrożeń jest zmienne i trudne do pełnej identyfikacji;
- procesy zarządzania są bardzo różnorodne, interdyscyplinarne i złożone – występują w nich sprzężenia zwrotne, zależności wzajemne często nie do końca poznane;
- wiele zagadnień jest trudnych do identyfikacji, a przez czynnik ludzki tu występujący, także nieprzewidywalnych[79].

Ogólnie mówiąc definicja bezpieczeństwa jako stanu niezagrożenia, spokoju, niezakłóconego funkcjonowania, odnosi się zawsze do pewnego obiektu. W rozważanym tu przypadku jest nim całość systemów teleinformatycznych i teleinformacyjnych Sił Zbrojnych Rzeczypospolitej Polski, wraz z informacjami zawartymi w systemach. Bezpieczeństwo teleinformacyjne jest warunkiem koniecznym, ale niewystarczającym bezpieczeństwa informacji. Trzeba zwrócić uwagę, że część tych atrybutów, jak na przykład integralność odnosi się

---

[77] Czynnik ludzki.
[78] Mówimy tu o informacji zarówno jawnej i niejawnej przetwarzanej w systemach teleinformatycznych i teleinformacyjnych.
[79] Białas A., *Bezpieczeństwo informacji…*, op.cit., s. 30.

do wszystkich elementów systemu. Część atrybutów odnosi się tylko do wybranych części, jak rozliczalność. Należy zauważyć, że dla informacji najważniejszymi atrybutami są: integralność, tajność, poufność, autentyczność oraz dostępność (Tabela 2.4.).

Tabela 2.4. Określenia atrybutów bezpieczeństwa, właściwości bezpieczeństwa.

Lp.	Nazwa atrybutu bezpieczeństwa	Określenie atrybutu
1.	**Tajność**	Stopień ochrony informacji, jakiej ma ona podlegać. Stopień ten jest uzgadniany przez osoby lub jednostki organizacyjne dostarczające i otrzymujące informacje.
2.	**Poufność**	Informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, jednostkom organizacyjnym lub procesom. Jest to prawo jednostki do decydowaniu o tym, jakimi informacjami i z kim chce się podzielić i jakie jest skłonna przyjąć.
3.	**Autentyczność**	Tożsamość podmiotu (instytucji, jednostki organizacyjnej) lub osoby jest taka jak deklarowana: dotyczy użytkowników, procesów, systemów lub instytucji [80]. Autentyczność jest związana z badaniem, czy ktoś lub coś jest tym lub czym za kogo lub za co się podaje.
4.	**Dostępność**	System jest dostępny i możliwy do wykorzystania na żądanie w założonym czasie przez kogoś lub coś, kto lub co ma do tego prawo. Dane, procesy i aplikacje są dostępne zgodnie z wymogami użytkownika lub wymogami na system.
5.	**Integralność danych**	Dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany. Informuje, czy dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji.
6.	**Integralność systemu**	System realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej.
7.	**Integralność**	Integralność danych oraz integralność systemu.
8.	**Rozliczalność**	Działania podmiotu (instytucji, jednostki organizacyjnej, osoby) – użytkownika mogą być jednoznacznie przypisane tylko temu podmiotowi.
9.	**Niezawodność**	Spójne, zamierzone zachowanie i skutki.

Źródło: Opracowanie własne na podstawie Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa 2006 r., Lehtinen R., Russell D., *Podstawy ochrony komputerów*, HELION, Gliwice 2007 r., Jemioło T., Kisielnicki J., Rajchel K., *Cyberterroryzm nowe wyzwania XXI wieku*, Wyższa Szkoła Policji, Warszawa 2009 r. oraz Sutton R. J., *Bezpieczeństwo telekomunikacji*, WKŁ, Warszawa 2004 r.

Bezpieczeństwo teleinformatyczne rozumiane jest jako zespół procesów zmierzających do zdefiniowania, osiągnięcia i utrzymania założonego poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności,

[80] W tym kontekście jednostek organizacyjnych podległych Ministrowi Obrony Narodowej.

czyli atrybutów bezpieczeństwa w systemach teleinformatycznych[81]. Dlatego też, możemy powiedzieć, że:

Bezpieczeństwo teleinformatyczne jest to całokształt przedsięwzięć zmierzających do zapewnienia bezpieczeństwa terminalom, systemów i sieci teleinformatycznych (teleinformacyjnych) oraz ochrony informacji wytwarzanej, przetwarzanej, przechowywanej, niszczonej lub przekazywanej w tych systemach i sieciach przed przypadkowym lub celowym ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwienie jej przetwarzania poprzez zastosowanie w sposób kompleksowy techniczny, programowy, kryptograficzny oraz organizacyjnych środków i metod.

Polityka bezpieczeństwa - określa się jako plan lub sposób działania przyjęty w celu zapewnienia bezpieczeństwa systemów i ochrony danych.[82]

Polityka bezpieczeństwa określa wykaz zasad, co należy chronić, dlaczego i w jaki sposób, aby systemy teleinformatyczne prawidłowo działały w realizacji zadań stawianych przez jednostki organizacyjne. W rozważanym tu wypadku miarą skuteczności jest możliwość niezakłóconej realizacji zadań przez jednostki organizacyjne.

Opracowanie polityki wymaga poznania dość złożonych relacji między procesami przekazywania informacji w jednostkach organizacyjnych a bezpieczeństwem wspierających je środków teleinformatyczne. Wdrażanie i realizacja polityki bezpieczeństwa jest związana z procesami zarządzania bezpieczeństwem informacji w jednostkach organizacyjnych i sprowadza się zawsze do utrzymania kompromisu między realnym zagrożeniem a stosowanym zabezpieczeniem teleinformatycznym z szerokim uwzględnieniem spraw związanych z ekonomia.

Bezpieczeństwo informacyjne funkcjonuje zawsze nieodłącznie w powiązaniu z szeregiem tradycyjnych wymiarów bezpieczeństwa, takich jak:

- bezpieczeństwo systemów obrony militarnej;
- bezpieczeństwo środowiska naturalnego;

---

[81] Białas A., *Bezpieczeństwo informacji...*, op.cit., s. 33.
[82] PN – I – 02000: *Zabezpieczenia w systemach informatycznych – Terminologia*, PKN, Warszawa, 1998 r.

- bezpieczeństwo komunikacji i transportu;
- bezpieczeństwo połączeń telekomunikacyjnych;
- bezpieczeństwo i poufność informacji;
- stabilność ochrony systemów zdrowia;
- życia i mienia obywatela[83].

Odniesienie do tak licznych dziedzin życia publicznego[84], które w ostatniej dekadzie zostały przesycone technologiami teleinformatycznymi, czynią kwestię bezpieczeństwa państwa bardziej dynamiczną, a równocześnie bardziej newralgiczną. Wykazują też nieprzewidywalność nowych zagrożeń, nieprzygotowanie służb państwowych do ich zwalczania oraz ich operacyjną impotencję. Wiele państw na świecie lekceważy fakt, że cyberterrorystyczne ataki mogą przerodzić się w śmiertelne zagrożenie poprzez:

- możliwość destrukcyjnego wpływu na działalność szeregu instytucji zarówno państwowych (cywilnych i wojskowych), jak i niepaństwowych;
- przeciążania i zakłócenia funkcjonowania komunikacji telefonicznej blokującej powiadamianie alarmowe (numer telefonu 112 lub 911 USA);
- zakłócenia ruchu lotniczego;
- uszkadzanie i rekonfigurację oprogramowania używanego w szpitalach i ratownictwie medycznym;
- manipulacje treściami receptur w skomputeryzowanych liniach produkcyjnych firm farmaceutycznych;
- zmiany ciśnienia w ropociągach i gazociągach prowadzące do wybuchów;
- kradzież tożsamości;
- uzyskiwanie dostępu do sieci teleinformatycznych i teleinformacyjnych i zmiana danych krytycznych;
- zdolność zakłócania mediów i przedstawienia fałszywego obrazu sytuacji (np. Internet);
- sabotaż danych na rynkach finansowych[85].

---

[83] Bógdał – Brzezińska A., Gawrycki M. F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, ASPRA-JR, Warszawa 2003 r. s. 41.

[84] Wyżej wymienione dziedziny życia publicznego są niczym innym jak sektorami Krytycznej Infrastruktury Państwa.

[85] Lichocki E., *Cyberterrorystyczne zagrożenie dla bezpieczeństwa teleinformatycznego państwa polskiego*, Instytut Badań Systemowych PAN Polskie Towarzystwo Badań Operacyjnych i Systemowych, Warszawa 2008 r. s. 181.

Należy stwierdzić, że ugrupowania terrorystyczne, dzięki wyciągnięciu wniosków z dokonującej się globalnej rewolucji technicznej i postępującej informatyzacji na świecie, zaczęły coraz szerzej stosować elementy walki informacyjnej. Występuje ponadto wiele przesłanek świadczących o dążeniu ugrupowań terrorystycznych do prowadzenia działalności cyberterrorystycznej. Mimo to ataki cyberterrorystyczne są obecnie zjawiskiem rzadkim. Spowodowane jest to głównie brakiem wykształconych informatyków, przywiązanie przywódców organizacji terrorystycznych do klasycznych form terroru oraz niedocenienia przez nich potencjalnych negatywnych następstw ataków cyberterrorystycznych dla Infrastruktury Krytycznej Państwa. Znaczenie cyberterroryzmu doceniają natomiast przywódcy młodszego pokolenia, szczególnie organizacji islamistycznych.

Ponadto terroryzm cybernetyczny może stać się atrakcyjną alternatywą dla ugrupowań ekstremistycznych działających w państwach zachodnich. W krajach tych, gdzie społeczeństwa z niechęcią odnoszą się do klasycznych aktów terroru, pociągających za sobą często śmierć niewinnych osób, cyberterroryzm może okazać się efektywną bronią, niepowodującą bezpośrednio skutków śmiertelnych[86].

2.4. Istota Infowar, Cyberwar, Netwar

Walka jest zawsze wtedy, kiedy mamy dwie strony, które dążą do konfliktu między sobą. Strony te zaczynają wykorzystywać różne techniki do zdobywania przewagi. Zawsze występuje walka informacyjna, która ma za zadanie:

- zdobywanie informacji o przeciwniku;
- zdobywanie informacji o terenie działania przeciwnika.

Poglądy Infowar pojawiły się po raz pierwszy na początku lat 90. Operacja „Pustynna Burza" według analityków jest to pierwsza informacyjna wojna lub walka. Nigdy wcześniej nie było tak dużo zgromadzonych środków elektronicznych podczas prowadzenia działań operacyjno – strategicznych. Po 1991 r. zaczęły się pojawiać nowe koncepcje i nowe rozwiązania wojny informacyjnej. W XXI wieku walka informacyjna zaczęła obejmować[87]:

- walkę o przewagę w dowodzeniu (*Command and control warfare* C2W);

---

[86] Adamski J., *Nowe technologie*..., op.cit., s. 146.

[87] Sienkiewicz P., *Współczesne koncepcje walki informacyjnej*, AON, Warszawa, 23 styczeń 2003 r.

- walkę bazującą na wiedzy rozpoznawczej (*Intelligence - based warfare* IBW);
- walkę elektroniczną (*Electronic Warfare* EW); uniemożliwianie przeciwnikowi dostępu do dokładnej informacji;
- działania psychologiczne (*Psychological informations* PSYOPS), używanie informacji do wpływu na jego rozumowanie;
- wojnę hakerską (*Hackerwar*); ataki softwareowe na systemy informacyjne;
- informacyjną walkę ekonomiczną (*Information economic warfare* IEW), wojna za pomocą kontroli informacji handlowej;
- cyberwojnę (*Cyberwar)*, walka w wirtualnej rzeczywistości;
- dezinformację militarną (*Military Deception*); wprowadzanie w błąd co domożliwości i zamiarów;
- fizyczne niszczenie (*Physical Destruction*); użycie spektrum broni od konwencjonalnej do impulsu elektromagnetycznego;
- przedsięwzięcia bezpieczeństwa (*Security Measures*)[88].

Cyberwar według poglądów amerykańskich,to potencjalne wykorzystanie urządzeń teleinformatycznych, Internetu i innych środków przechowywania lub rozprzestrzeniania informacji w celu przeprowadzania ataków w na systemy teleinformatyczne wroga.

Cyberwar od klasycznych wojen odróżnia środowisko pola walki – muszą występować w nim systemy teleinformatyczne. W takiej wojnie strona atakująca przy minimalnych nakładach materialnych zdolna byłaby w znacznym stopniu sparaliżować kluczową Infrastrukturę Krytyczną Państwa lub gospodarkę państwa przeciwnika - o ile ta oparta jest w wystarczająco wysokim stopniu na systemach teleinformatycznych[89]. *Cyberwar* jest konfliktem w dużym stopniu asymetrycznym, co pozwoliłoby na prowadzenie tego rodzaju wojen państwom słabszym przeciwko silniejszym.

W ramach tych działań, napastnik może dążyć do realizacji rozmaitych celów strategicznych, od rozpowszechniania propagandy lub wywoływania paniki pośród ludności cywilnej, po trwałe uszkodzenie kluczowych elementów Infrastruktury Krytycznej Państwa (np. elektrownie, systemy komunikacyjne). Ataki te mogą też być narzędziem wywiadu technologicznego i pozyskiwania informacji.

---

[88] Lichocki E., *Zagrożenie cyberterroryzmem w polityce bezpieczeństwa informacyjnego Polski*, Praca dyplomowa, AON, Warszawa 2005 r., s.13.
[89] Przykładem takiego państwa jest np. Estonia.

W zależności od celu, ataki mogą wykorzystywać pełną gamę narzędzi: komputery zombie używane do ataków DoS i DDoS, *exploity*[90] pozwalające na przejęcie kontroli nad systemami w tym metody socjotechniczne zmierzające do manipulacji ludźmi. Ataki tego typu mogą osłabić w znacznym stopniu lub uszkodzić systemy teleinformatyczne wykorzystywane przez siły zbrojne przeciwnika.

Cyberwar jest to walka w przestrzeni cybernetycznej. Jest ona możliwa i prawdopodobna, kiedy to na dzień dzisiejszy dokładnie nie wiemy. Wykonanie ataku cyberwar na Infrastrukturę Krytyczną Państwa (np. energetyka, transport, systemy teleinformatyczne itp.) jest możliwe w każdej chwili i w każdym rejonie świata.

Netwar jest pojęciem zaproponowanym przez RAND Co.[91]. Jest to konflikt o niskiej intensywności, przestępczości i aktywizmu prowadzony w sieci. Typowe *netwar* podmioty mogą obejmować ponadnarodowych terrorystów, organizację przestępcze, działaczy grup i ruchy społeczne.

Netwar jest to typowe sieciocentryczne pole walki. Działania wojenne są prowadzone za pomocą sensorów. Wojna sieciowa jest konfliktem[92] o niskiej intensywności, podczas którego walczy się głównie przesyłanymi informacjami. Wygrywa ten, kto zdoła uruchomić efekt sieci, dzięki któremu informacje namnażają się lawinowo. Proces ten wymyka się spod kontroli, chodzi w nim nie tyle o przedstawienie jednej „prawdy", ile o jej relatywizację, zakwestionowanie roszczeń do jedynego słusznego stanowiska.

---

[90] Exploit - program mający na celu wykorzystanie błędów w oprogramowaniu. Najczęściej program taki wykorzystuje jedną z kilku popularnych technik, na przykład przepełnienie bufora, przepełnienie sterty, format string. Exploit wykorzystuje występujący w oprogramowaniu błąd programistyczny i przejmuje kontrolę nad działaniem procesu – wykonując odpowiednio spreparowany kod bajtowy, który najczęściej wykonuje wywołanie systemowe uruchamiające powłokę systemową z uprawnieniami programu, w którym wykryto lukę w zabezpieczeniach.

[91] RAND Corporation - amerykański „think tank" i organizacja badawcza non-profit, pierwotnie sformowana dla potrzeb Sił Zbrojnych Stanów Zjednoczonych. Założona 14 maja 1948 r. w Santa Monica w Kalifornii na bazie rozpoczętego w końcu 1945 r. wojskowego Projektu RAND (pierwszy raport RAND u ukazał się już w maju 1946 r.). W późniejszym okresie organizacja pracowała także dla innych organizacji rządowych i komercyjnych. Obecnie RAND posiada około 1600 pracowników w sześciu siedzibach - trzech w USA: Santa Monica w Kalifornii, Arlington w Wirginii i Pittsburghu (Pensylwania), oraz trzech w Europie: Lejdzie w Holandii, Berlinie i brytyjskim Cambridge. Korporacja RAND jest znana z dużego wkładu w naukę, zwłaszcza w metody ilościowe, na polu między innymi badań operacyjnych, rozwoju badań nad sztuczną inteligencją czy Internetu. Obecnie RAND prowadzi badania na tak różnych polach jak obronność i terroryzm, stosunki międzynarodowe, edukacja czy zdrowie publiczne.

[92] Pierwszym modelowym przykładem *netwar* jest powstanie w Chiapas przeciwko rządowi w Meksyku.

2.5. Sieciocentryczne pole walki

Współczesne pole walki ogranicza prowadzenie autonomicznych, izolowanych działań (operacji)[93], co wymusza nowe spojrzenie na współdziałanie, koordynację i synchronizację działań. Zasady, przyjęte dla przyszłych działań, zostały sformułowane w postaci koncepcji określonej „sieciocentrycznymi działaniami wojennymi" (ang. *Network Centric Warfare* - NCW)[94]. W kontekście dowodzenia mówi się coraz częściej o „operacjach sieciocentrycznych" - NCO (ang. *Network Centric Operations*) [95] . Operacjami NCO nazwano działania operacyjne wykorzystujące informacje przekazywane bezpiecznymi środkami teleinformatycznymi zarówno na etapie planowania, jak i szybkiego, terminowego, precyzyjnego i zdecydowanego prowadzenia operacji przeciwko siłom zbrojnym przeciwnika.

Według analityków z RAND Corporation głównym wyzwaniem dla współczesnego pola walki jest wykorzystanie koncepcji NCW w obszarze C4ISR (*Command, Control, Communications, Computers/Coordination, Surveillance and Reconnaissance*), czyli w szeroko pojętej strukturze dowodzenia i łączności, celem osiągnięcia przewagi informacyjnej i skuteczności decyzyjnej[96].

W Polsce na szeroką skale prowadzone są działania dotyczące przybliżenia Sił Zbrojnych Rzeczypospolitej Polski do osiągnięcia zdolności sieciocentrycznych na wsól czesnym polu walki. W 2006 roku, został powołany w ramach Sztabu Generalnego specjalny zespól zadaniowy koordynujący przedsięwzięcia związane z opracowaniem i wdrażaniem tych zdolności w Siłach Zbrojnych RP.

Przedsięwzięcia te obejmują szeroki zakres działań koncepcyjnych, projektowych i wykonawczych, w które zaangażowane są dowództwa, uczelnie wojskowe, instytucję badawczo – rozwojowe oraz przedsiębiorstwa związane z przemysłem obronnym[97].

---

[93] Działania asymetryczne.

[94] Istniejąca literatura fachowa stosuje do opisu tego rodzaju działań różnorakie terminy: *Network Centric Warfare, Net – Centric Operations, - Network Centric War*. Pojawiają się także określenia w rodzaju: walka zbrojna ery cyfrowej, walka wielowymiarowa, operacja połączona w środowisku rozproszonym, rozległa operacja połączona oraz połączone działania sił rozproszonych.

[95] Keus H. E., *Network Centric Operations. Implications for Allied and Coalition Operations*, Konferencja SMI Conferences on Network Centric Warfare, London, 4 - 5 October 2000 r.

[96] Sienkiewicz P., Mąka D., *Sieciocentryczna infrastruktura procesów decyzyjnych,* Zeszyty Naukowe AON, Nr 4 (74), Warszawa 2008 r.

[97] Kręcikij J., *Działania sieciocentryczne. Wybrane problemy*, AON, Warszawa 2008 r. s. 36.

2.5.1. Działania w warunkach sieciocentrycznego pola walki

Świadomość, że posiadanie informacji, może być istotną przesłanką do osiągnięcie sukcesu na polu walki, a szczególnie przy prowadzeniu działań asymetrycznych[98], spowodowała zainteresowanie możliwościami wykorzystania sieci teleinformatycznych w działaniach bojowych. Szybkość zbierania danych, wielość i różnorodność źródeł informacji, prędkość transmisji w połączeniu z wypracowaniem efektywnych metod magazynowania i przetwarzania tak zebranych danych staje się wyzwaniem dla dowódców. Stało się również, wyzwaniem dla nauczenia się wykorzystywania tych danych na współczesnym polu walki.

Wyzwanie to nosi nazwę *Network Centric Warfare*. Zasadniczą cechą tych działań jest nagromadzenie środków pozwalających na: gromadzenie, przetwarzanie i analizę danych oraz dostępność, bez względu na odległość, różnorodnych baz danych wynikającą z bardzo zaawansowanej technologii teleinformatycznej. To nagromadzenie i manipulowanie danymi pozwala na łatwiejsze rozwiązywanie problemów związanych z koniecznością zrozumienia sytuacji na polu walki, wzbogaca proces analizy niezbędnej do podjęcia decyzji, a także daje możliwości przekazywania jasnych i zrozumiałych komunikatów dla wszystkich zaangażowanych w realizację podjętych działań.

Koncepcja NCW charakteryzuje się[99][100]:

1. Dążeniem do zdobycia w pierwszej kolejności przewagi informacyjnej.
2. Zwiększeniem możliwości dzielenia się informacją (wspólną świadomością sytuacyjną) dzięki silnemu nasyceniu środkami sieciowymi wszystkich elementów związanych z realizacją zadania.
3. Szybkim cyklem dowodzenia.
4. Poprawą jakości rozumienia sytuacji, przez wszystkie podmioty, które w rozwiązywaniu tej sytuacji biorą udział, dzięki szybszemu, przejrzystszemu i łatwiejszemu dzieleniu się informacją.

---

[98] Ich istota polega na tym, że w starciu dwóch stron – z której jedna jest niewspółmierne słabsza pod względem militarnym od drugiej – słabszy chwyta się metod absolutnie niekonwencjonalnych, osiągając zarazem przy minimum środków maksimum efektu (także politycznego. Można zauważyć, że wojna o Kosowo wiosną 1999 r. miała już charakter działań asymetrycznych.

[99] Modelowanie procesów walki informacyjnej. Model „cyberwar", praca zbiorowa pod red. M. Kinasiewicz, AON, Warszawa, 2006 r. s. 70.

[100] Opracowano na podstawie: Kręcikij J., *Działania sieciocentryczne. Wybrane problemy*, AON, Warszawa 2008 r. oraz Posobiec J., *Organizacja dowodzenia w środowisku sieciocentrycznym*, AON, Warszawa 2008 r.

5. Umożliwieniem lepszej współpracy i synchronizacji działań, a także poprawieniem sprawności i szybkości dowodzenia wynikających ze wspólnego, jednakowego rozumienia rozwiązywanej sytuacji.
6. Zwiększoną efektywnością realizowanych zadań wynikającą z powyższych cech.
7. Masowym użyciem sensorów.
8. Nielinearnym polem (przestrzenią) walki.
9. Rozproszeniem sił.
10. Zmniejszeniem różnic między poziomami działań zbrojnych oraz granic między rodzajami sił zbrojnych i wojsk.

Powyższe cechy stanowią zalety NCW, ale jednocześnie prowadzą do niebezpiecznej pokusy przerzucenia odpowiedzialności za podejmowanie decyzji z dowódcy na system sieciocentryczny. Tak rozumiane pojęcie walki i dowodzenia w środowisku sieciocentrycznym kłóci się z obowiązującymi i sprawdzonymi zasadami dowodzenia, mówiącymi o tym, że prawdziwym centrum efektywnego dowodzenia i kierowania pozostaje dowódca[101].

Zwiększenie możliwości związanych ze zrozumieniem sytuacji, wizualizacją czy podejmowaniem decyzji to jeden aspekt wykorzystania sieciocentryczności w trakcie działań bojowych, pozwalający na poprawę dowodzenia, w tym współpracy ze sztabem, podwładnymi, a nawet przełożonymi, drugi natomiast przejawia się w zwiększeniu możliwości prowadzenia dowodzenia w ruchu. Wymienione powyżej zalety stosowania zasad prowadzenia działań sieciocentrycznych nie wyczerpują jednak wszystkich istotnych cech tych działań, a są wśród nich i takie, które należałoby traktować jako wady. Należą do nich między innymi:

1. Otrzymywanie takiej ilości informacji, która może przepełnić możliwości ich przyjmowania i analizowania przez dowódcę i sztab. Jak mówią sceptycy problemem obecnego dowodzenia nie jest niezaspokojenie potrzeb informacyjnych, ale zrozumienie informacji już posiadanych[102].
2. Trudność rozpoznania najistotniejszych informacji wśród mnogości trywialnych danych.

---

[101] Lt. Gen. Wallace W. S., *Network-Enabled Battle Command*, Royal United Services Institute, Winter 2004/2005 r.
[102] Aldo Borgu A., The *Challenges and Limitations of Network Centric Warfare. The initial views of an NCW skeptic*, 17.09.2003 r.

3. Usiłowanie kierowania najmniejszymi nawet elementami przez wyższych dowódców mających dostęp do lepszej i szybszej informacji i wiedzy o prowadzonych działaniach.
4. Niedocenieniem potencjalnego przeciwnika.
5. Problemy z interoperacyjnością.
6. Niekontrolowany wypływ technologii informatycznych.
7. Niebezpieczeństwo wynikające z zagrożeń asymetrycznych[103].
8. Narażenie na ataki w cyberprzestrzeni[104].
9. Koncentracja na naukowym podejściu do kierowania i zaniedbanie sztuki dowodzenia.
10. Pomniejszanie roli dowódcy.

Dowodzenie współczesnymi środkami walki, czy też dowodzenie walką wymaga by centralnym punktem procesu decyzyjnego był dowódca, a sztab, wraz z wspierającą go technologią, pomagały w zrozumieniu sytuacji taktyczno - operacyjnej, podejmowaniu decyzji, przekazywaniu dyrektyw i nadzorowaniu wprowadzania ich w życie. Przywódcze aspekty dowodzenia przejawiają się w takich działaniach jak:

- wizualizacja – co jest zadaniem, polegającym na określeniu jakie są możliwości przeciwnika i możliwe jego działania, jakie są charakterystyki terenu działań, czy teren i pogoda są sprzyjające dla działań nieprzyjaciela, ile jest czasu przeznaczonego na realizację zadań, jakie czynniki wsparcia są najważniejsze i jaką rolę odgrywa czynnik cywilny;
- opisywanie – w trakcie którego dowódca przekazuje swoją wizję jako zamiar dowódcy a sztab i podwładni transformują go w plany i rozkazy. Jest to jasny, zwięzły przekaz o tym co siły muszą zrobić i z jakimi uwarunkowaniami, ze strony nieprzyjaciela i terenu mogą się spotkać;
- kierowanie walką.

---

[103] Kręcikij J., *Działania sieciocentryczne*..., op.cit., s. 51.

[104] Przeciwnicy koncepcji NCW podkreślają, że pomimo iż militarne systemy teleinformatyczne i teleinformacyjne są zabezpieczone, wciąż zdarzają się przypadki ataków cyberterrorystycznych, nierzadko zakończone powodzeniem. Nie można zatem wykluczyć możliwości iż państwo – strona przeciwna, lub organizacja o charakterze niepaństwowym uzyska zdolności do penetracji przestrzeni teleinformacyjnej. Tego rodzaju atak mógłby przynieść nieprzewidywalne groźne skutki dla działań sieciocentrycznych, dając z jednej strony możliwości zakłócania przepływu informacji – która jest istotą NCW lub, działając bardziej wyrafinowanie, jej fałszowaniem. Sytuacja taka, zdaniem przeciwników, doprowadzić może do paraliżu sił działających zgodnie z koncepcją NCW.

Wskazane powyżej uwarunkowania w sposób znaczący wpływają zarówno na sposób dowodzenia i jego jakość jak również na prowadzenie działań bojowych i to niezależnie od rodzaju wojsk. Prowadzenie działań bojowych w środowisku sieciocentrycznym powoduje zmiany w taktyce zarówno pododdziałów jak również pojedynczych żołnierzy. Pododdziały wyposażone w odpowiedni sprzęt umożliwiający działanie na polu walki z jednoczesnym „podłączeniem" do sieci pozwalającym na szybkie reagowanie na sytuację będą składały się z mniejszej liczby żołnierzy, których miejsce działań będzie zależało od aktualnych potrzeb i możliwości użycia. Będą one bardzo mobilne, a jednocześnie efektywne w realizacji zadań co spowoduje, że koszt wykonania misji powinien być znacznie mniejszy i to zarówno w rozumieniu możliwych strat ludzkich jak i ekonomicznym.

Działania pojedynczego żołnierza będą z jednej strony dawały mu możliwość uzyskania znacznie większej liczby informacji, związanych z realizowanym przez niego zadaniem jak również, na skutek możliwości śledzenia wykonania tego zadania, pomoc w sytuacjach krytycznych ze strony nadzorującego, odległego organu (centrum nadzoru nad realizacją misji). Pomoc ta realizowana w zbyt dużym stopniu może przerodzić się w próbę „zdalnego sterowania", które z jednej strony może być uzasadnione posiadaną wiedzą, a drugiej może nie uwzględniać tych uwarunkowań, które są niemożliwe lub bardzo trudne do zidentyfikowania przy pomocy sensorów nadzorujących pracę (walkę) w środowisku sieciocentrycznym. Możliwość wykorzystania technologii przetwarzających informacje powoduje zmniejszenie czasu niezbędnego do stwierdzenia, że zidentyfikowany obiekt jest nieprzyjacielem i podjęcia decyzji o unieszkodliwieniu go w zakresie wystarczającym do uniemożliwienia mu działania. Zakres unieszkodliwienia, wynikający w tradycyjnych działaniach głównie z wyszkolenia żołnierza będzie, w wypadku działań sieciocentrycznych w dużej mierze zależał od umiejętności wykorzystania posiadanych informacji.

Powyższe uwagi pozwalają na stwierdzenie, że zarówno dowodzenie jak i prowadzenie walki w warunkach sieciocentryczności, to nowa jakość w realizacji zadań przez wojska.

Uzależnienie jakości dowodzenia od informacji jest stałą cechą procesu podejmowania decyzji, ale w warunkach sieciocentryczności nabiera dodatkowego wymiaru polegającego na zwiększeniu liczby źródeł informacji, które pozwalają na uzyskanie znaczącej przewagi informacyjnej stając się jednocześnie celami oddziaływania przeciwnika, któremu zależy na unieszkodliwianiu tych elementów

składowych wojsk nieprzyjaciela, które do uzyskania takiej przewagi są najistotniejsze. Stąd pojawia się kolejne pole działań, walka w obszarze środków tworzących sieciocentryczne pole walki. Obezwładnienie systemu eliminuje z działań mniejsze i większe pododdziały, dla których podstawowymi źródłami informacji były zdalne bądź sterowane środki wchodzące w skład tej struktury sieciowej.

Z tego też powodu mówiąc o wojnie sieciocentrycznej musimy mówić o takich jej aspektach jak:

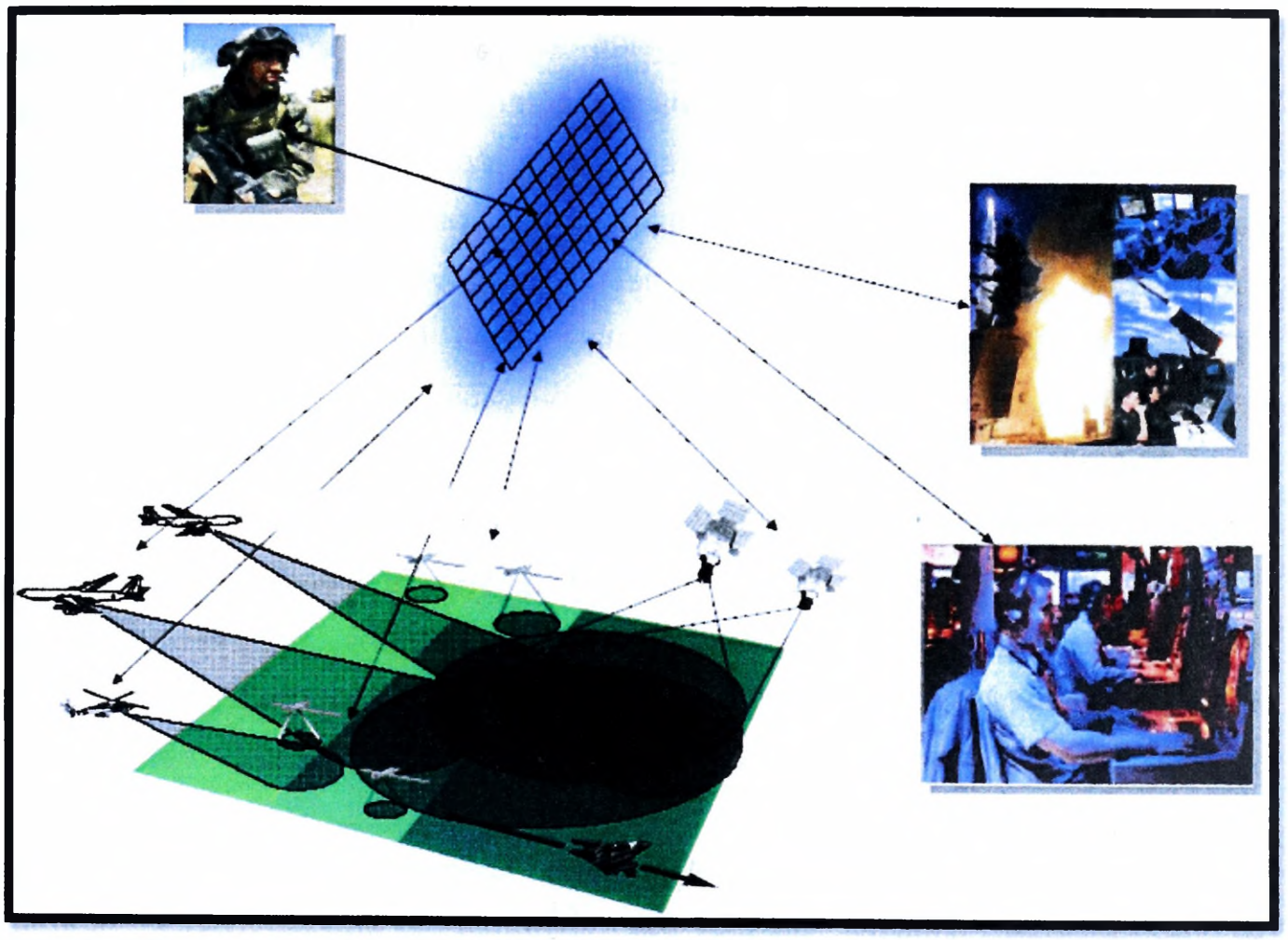
1. Jakość procesu dowodzenia w tych warunkach.
2. Wpływ dominującej roli informacji na zmiany w taktyce działania wojsk (poszczególnych jednostek, czy rodzajów wojsk).
3. Oddziaływanie na infrastrukturę sieciową przeciwnika – działania ofensywne.
4. Ochrona własnej struktury sieciowej (bezpieczeństwo teleinformatyczne i teleinformacyjne) przed oddziaływaniem nieprzyjaciela – działania defensywne.

Zmienność środowiska jakim jest cyberprzestrzeń, jej rozwój i obejmowany obszar zdają się potwierdzać tezę, że zachowania różnych elementów tego systemu są niemożliwe do przewidzenia, nie ma praw, które obowiązywałyby raz na zawsze. Zarówno rozwiązania techniczne jak i zachowania użytkowników systemu sieciocentrycznego wydają się nie podlegać jakiejkolwiek teorii. Oznacza to, że również formy realizowania działań zakłócających poprawne funkcjonowanie systemu są trudne do przewidzenia, a skoro tak to i trudno im przeciwdziałać. Rozwój technologii związanych z zapewnieniem właściwego poziomu bezpieczeństwa informacyjnego związany jest ze świadomością zagrożeń to znaczy, że zagrożenie nieświadome jest zagrożeniem realnym, mogącym wystąpić w najmniej spodziewanym momencie i miejscu. Na tym opiera się skuteczność ataku cyberterrorystycznego i taktyka działań informacyjnych.

Kolejną cechą charakterystyczną narzędzi cyberwojny jest ich dualny charakter. Narzędzie służące do skanowania systemu teleinformatycznego ma dać jego administratorowi odpowiedź na pytanie czy i w jakich miejscach system ma słabe punkty i to samo narzędzie w „rękach" napastnika realizuje zadanie wykrycia tych punktów systemu i otwiera drogę do realizacji działań niepożądanych.

2.5.2. Technologiczne determinanty

Na potrzeby NCW tworzona jest globalna sieć informacyjna (ang. *Global Information Grind*), która ma stanowić fizyczną platformę telekomunikacyjną zapewniającą realne funkcjonowanie przyjętej koncepcji sieciocentryczności (Rys. 2.5).



Rysunek 2.5. Globalna sieć informacyjna na potrzeby działań sieciocentrycznych

Źródło: Opracowano na podstawie: Przegląd Sił Powietrznych, kwiecień 2005 r.

W systemach sieciocentrycznych wyróżnić można trzy klasy wzajemnie powiązanych relacji i współdziałających podsieci:

- sieć środków rozpoznania określoną mianem sieci sensorów – (ang. *Sensor Grid*);
- sieć systemów stanowiska dowodzenia – (ang. *C2 Grid*);
- sieć systemów uzbrojenia, w której funkcjonują aktywne środki walki – (ang. *Shooter Grid*).

Architektura sieci teleinformatycznych powinna zapewnić połączenia tych trzech podzespołów w jeden sprawnie funkcjonujący mechanizm[105].

Walka sieciocentryczna czy sieciocentryczne działania bojowe związane są zawsze z rozwojem urządzeń i systemów teleinformatycznych, które służą do rozpoznawania, zbierania, przetwarzania i dystrybuowania informacji. Rozwój technologii telekomunikacyjnych[106] na przełomie XX i XXI wieku stworzył szereg nowych możliwości związanych z każdym z etapów przetwarzania danych[107].

Najważniejszym elementem działań sieciocentrycznych jest odpowiednia infrastruktura technologiczna, nazywana w literaturze fachowej infostrukturą[108]. Jest ona architekturą sieciową składającą się z przewodowych oraz bezprzewodowych środków transmisji danych realizowanych przez różnorodne media (urządzenia) transmisyjne, takie jak fale radiowe, sieci szkieletowe oparte na światłowodach, promieniowanie podczerwone czy mikrofale. Cała ta struktura łączy ze sobą nadajniki i odbiorniki informacji takie jak sensory i czujniki.

Poprawne działanie tak skomplikowanych i rozległych struktur możliwe będzie tylko przy zapewnieniu odpowiedniego oprogramowania, pozwalającego na szybkie i bezpieczne[109] przekazywanie informacji. W przypadku krajów zaawansowanych technologicznie jak również ich sojuszników bardzo ważnym elementem technologicznym NCW jest cywilny i militarny system satelitarny (np. EUTELSAT, INTELSAT, US SAT, INMARSAT, SATCOM) pozwalający na zbieranie i przekazywanie istotnych danych[110].

Kolejnym technologicznym elementem koncepcji walki sieciocentrycznej są bezzałogowe pojazdy służące do zbierania i przekazywania informacji ze środowiska powietrznego, wodnego jak i z powierzchni ziemi. Sprawne działanie tych urządzeń jest determinowane przez bardzo sprawnym i odpornym na zakłócenia systemem łączności.

---

[105] *Sieci teleinformatyczne w działaniach sieciocentrycznych*. Materiały z międzynarodowej konferencji naukowej, AON, Warszawa 2007 r.

[106] Rozwój technologii telekomunikacyjnych w działaniach w warunkach sieciocentryczności nieodzownie związany jest z urządzeniami i systemami teleinformatycznymi.

[107] *Modelowanie procesów walki informacyjnej. Model „cyberwar.*, praca zbiorowa pod red. M. Kinasiewicz, AON, Warszawa, 2006 r. s. 77.

[108] Garstka J. J., *Network Centric Warfare: An Overview of emerging Theory*.

[109] Mówimy tu o prawidłowej ochronie kryptograficznej przekazywanych informacji.

[110] Na przykład: o pogodzie czy terenie, ale również umożliwiający dzięki systemowi GPS (*Global Positioning System*) dokładne orientowanie w terenie zarówno swojego położenia jak i umiejscowienie przeciwnika czy celów z precyzją nieznaną w czasach „przedsieciowych".

Kolejne elementy technologiczne infrastruktury NCW związane są z rozwojem tradycyjnych technologii komputerowych [111], nanotechnologi – umożliwiających miniaturyzację składników struktury sieciocentrycznej i rozwojem oprogramowania sieciowego, ale również tego, które potrafi we właściwy sposób wykorzystać zebrane dane w procesach podejmowania decyzji (systemy wspomagania decyzji, systemy ekspertowe, modele sytuacyjne itp.)[112].

Istotą znacznej części stosowanych rozwiązań technicznych jest wykorzystywanie możliwości jakie niesie ze sobą rozwój technologii wykorzystania Internetu i oprogramowania. Z tego powodu bardzo istotnym zagadnieniem staje się zapewnienie bezpieczeństwa teleinformatycznego i teleinformacyjnego zarówno w fazie jej przesyłania, magazynowania jak i przetwarzania. Wiadomo, że sieci wojskowe, lub ich elementy są ulubionym celem ataku cyberterrorystów stawiających sobie za cel złamanie zabezpieczeń bez chęci zniszczenia danych. O ile druga z tych możliwości może stanowić sygnał ostrzegawczy, że przyjęte rozwiązania nie są bezpieczne, to pierwsza wykorzystana przez instytucje państw będących w konflikcie, lub organizacje terrorystyczne może doprowadzić do konsekwencji wynikających z uzyskania przewagi informacyjnej polegającej na znajomości przez nieprzyjaciela bardzo istotnych informacji związanych z zapewnieniem bezpieczeństwa państwa.

2.5.3. Zagrożenia wewnętrzne i zewnętrzne

Istnieje wiele możliwości oddziaływania na elementy systemu sieciocentrycznego. Jeżeli bierzemy pod uwagę fizyczną warstwę[113] tego systemu to oznacza to, że również możliwe jest fizyczne oddziaływanie na tę warstwę. Ostatnie lata dają możliwość naocznego stwierdzenia jakie istnieją zagrożenia dla

---

[111] Zgodnie z tzw. prawem Gordona Moore'a co 1,5 roku procesory dwukrotnie zwiększają liczbę zawartych elementów i prędkość działania, a ich cena pozostaje na tym samym poziomie.

[112] *Modelowanie procesów walki informacyjnej. Model „cyberwar"*, praca zbiorowa pod red. M. Kinasiewicz, AON, Warszawa, 2006 r. s. 78.

[113] Rozumiana jest jako tradycyjna przestrzeń, w której walczące siły prowadzą działania. Ma ona wymiar: lądowy, powietrzny, morski oraz kosmiczny. Obejmuje wszystkie poziomy: strategiczny, operacyjny i taktyczny. W tej domenie występują platformy bojowe, sensory oraz łączące je w sieć systemy teleinformatyczne. Tworzą je elementy istniejące realnie w sensie fizycznym. Znajdują się w niej cały potencjał komponentów systemów dowodzenia i wspomagania dowodzenia wchodzący w skład stanowisk dowodzenia oraz środki dowodzenia (sprzęt teleinformatyczny, teleinformacyjny i łączności tworzące system wymiany informacji. W publikacjach związanych z NCW, warstwa fizyczna nazywana jest czasami domeną fizyczną.

sieci globalnej Internet, a to co w działalności gospodarczej skutkować może utratą wiarygodności, w konflikcie międzynarodowym oznaczać może klęskę i podporządkowanie woli zwycięzcy.

Należy się liczyć z tym, że miejsca szczególnie cenne ze względu na ich rolę w systemach teleinformatycznych systemu dowodzenia i wsparcia dowodzenia Sił Zbrojnych Rzeczypospolitej Polski będą celem działań zmierzających do ich fizycznego unicestwienia zarówno w trakcie regularnych działań bojowych, jak i działań informatycznych (cyberterrorystycznych). Mówiąc o fizycznym oddziaływaniu na kluczowe elementy systemów teleinformatycznych mamy na myśli takie sposoby oddziaływania, które doprowadzą do fizycznej destrukcji tych elementów. Będą to więc zarówno oddziaływania tradycyjnymi środkami niszczącymi (używając klasycznych ładunków wybuchowych) jak i takie, które wykorzystują na przykład silny impuls elektromagnetyczny w celu zniszczenia zarówno urządzeń i systemów teleinformatycznych jak i danych przechowywanych na serwerach ulegających degradacji pod wpływem tego impulsu. Urządzenia te to między innymi:

- broń mikrofalowa wysokiej mocy (ang. *High Power Microwave*) – generująca elektromagnetyczny sygnał wielkiej mocy (rzędu gigawatów) o radiowej częstotliwości;
- broń o szerokim zakresie częstotliwości (ang. *Ultra Wide Band*) – generująca elektromagnetyczny sygnał dużej mocy na różnych zakresach częstotliwości;
- broń wysokiej energii radiowej częstotliwości (ang. *High Energy Radio Frequency*) – jako HPM;
- urządzenia generujące impuls elektromagnetyczny (ang. *Electromagnetic Pulse*) – które wybuchając w pobliżu atakowanych urządzeń systemu informatycznego, generują impuls elektromagnetyczny niszczący znajdujące się w pobliżu urządzenia elektroniczne[114].

Te ultranowoczesne sposoby niszczenia elementów infrastruktury teleinformatycznej z pewnością będą jednym z elementów prowadzenia działań w ramach NCW i z tego względu należy uwzględniać je w potencjale bojowym. Ten potencjał bojowy ma decydujący wpływ na sprawność systemu dowodzenia i wsparcia dowodzenia. Modelując tego rodzaju oddziaływanie należy odwoływać się do tradycyjnych pojęć możliwości niszczenia czy też intensywności niszczenia. Problemem natomiast staje ocena efektów zniszczenia określonych elementów

[114] Patrz Załącznik 1.

infrastruktury w odniesieniu do możliwości prowadzenia działań sieciocentrycznych, a raczej niemożliwości jej realizacji. Wiadomo, że zasada działania systemu opiera się na tym, że zniszczenie jednego, czy więcej węzłów systemu nie powoduje jej zniszczenia, ani nawet odczuwalnego ograniczenia możliwości.

Najbardziej wrażliwymi węzłami w tym systemie będą te, w których zlokalizowane są stałe bazy danych i oprogramowanie zarządzające gromadzeniem i przetwarzaniem danych. Istota rozproszonego przetwarzania danych i rozproszonych baz danych jest przeciwdziałaniem takiej sytuacji. Nie pozwalają one na zlokalizowanie miejsca węzła, ponieważ fizycznie on nie istnieje, a skoro tak to bardzo trudne staje się jego zniszczenie fizyczne.

Innym elementem NCW są sensory zbierające dane. Te bezobsługowe i obsługowe, zminiaturyzowane i widoczne urządzenia również mogą stać się celem oddziaływania przeciwnika, który broni się przed śledzeniem jego posunięć. Postęp techniczny pozwalający na wykorzystanie przestrzeni kosmicznej do rozmieszczenia bardzo czułych urządzeń obserwujących zjawiska zachodzące w związku z działaniami bojowymi toczącymi się na polu walki spowodował, że trudne jest również fizyczne unieszkodliwienie sensorów zbierających dane do podjęcia właściwych decyzji.

Te wymienione wyżej uwarunkowania powodują, że fizyczne zniszczenie infrastruktury służącej do gromadzenia i przetwarzania danych może się okazać bardzo trudne w realizacji. W związku z tym wykreowano szereg innych możliwości, bardzo często niskokosztowych, które pozwalają na takie wpływanie na działania sieciocentryczne by stały się one nieefektywne. Te metody, które wykazały już swoją przydatność w sferze „cywilnej" są ciągle doskonalone i przeciwdziałanie im stanowi wyzwanie dnia dzisiejszego dla użytkowników systemów teleinformatycznych.

Należy tu wspomnieć o takich metodach, które poprzez wykorzystanie luk w systemie bezpieczeństwa mają możliwość wpływania na procesy związane zarówno z przesyłaniem jak i przetwarzaniem danych. Mowa tu na przykład o takich działaniach jak:[115] wirusy, bakterie, robaki, „bomby logiczne", „konie trojańskie", próbkowanie, uwierzytelnianie, ominięcie, czytanie, modyfikacja, tylne drzwi, „chipping", podszywanie się, maskarada, przepełnienie itp.

[115] Szerzej, działania te zostały opisane w podrozdziale 2.2. niniejszej rozprawy doktorskiej.

Wymienione działania znajdują swoje odzwierciedlenie w klasyfikacji zaproponowanej przez Defense Advanced Research Projects Agency (DARPA)[116] – amerykańską agencję zajmująca się rozwojem najnowszych technologii i ich zastosowań w dziedzinie obronności. Agencja specyfikuje pięć kategorii zagrożenia dla infrastruktury sieciocentrycznego pola walki[117]:

1. Zewnętrzny atak pasywny, taki jak:
   - podsłuchiwanie czyli nasłuchiwanie danych przez sieć, poczty, haseł, kopiowanych plików;
   - analiza emisji ujawniającej czyli analiza promieniowania elektromagnetycznego urządzeń systemu teleinformatycznego;
   - analiza sygnałów akustycznych dochodzących ze stosowanych urządzeń;
   - analiza ruchu w systemie, jego intensywności, regularności, cech pozwalających na ocenę liczby realizowanych zadań w systemie co odzwierciedla fazę i intensywność procesu decyzyjnego.
2. Zewnętrzny atak aktywny:
   - zamiana lub wstawienie danych i (lub) procesów z wykorzystaniem oprogramowania złośliwego;
   - zagłuszanie (zakłócanie) transmisji poprzez niepotwierdzanie tożsamości lub przekierowywanie strumieni informacyjnych poprzez manipulowanie w strukturze sieci oraz przechwytywanie transmisji pomiędzy dwoma zdalnymi systemami teleinformatycznymi;
   - przepełnienie – realizowane przy pomocy ataków typu odmowa świadczenia usług polegających na ponawianiu żądania realizacji usługi z taką

---

[116] Defense Advanced Research Projects Agency - DARPA (Agencja Zaawansowanych Projektów Badawczych Obrony Departamentu Obrony Stanów Zjednoczonych) przekształcona w 1972 r. z ARPA. W latach 1958 - 1972 i 1993 - 1996 pod nazwą - Advanced Research Projects Agency - ARPA (Agencja Zaawansowanych Projektów Badawczych), to amerykańska agencja rządowa zajmująca się rozwojem technologii wojskowej. Na zlecenie Departamentu Obrony USA w 1967 r. rozpoczęła projekt budowy zdecentralizowanej sieci komputerowej, którą nazwano później ARPANET i która zapoczątkowała rozwój Internetu. Na początku lat 70. agencja DARPA współfinansowała opracowanie zestawu protokołów TCP/IP. DARPA nigdy nie prowadziła badań samodzielnie, zajmowała się finansowaniem wyższych uczelni, instytucji komercyjnych i innych organizacji (non-profit). W 1981 DARPA założyła grupę ekspertów - ICCB (Internet Configuration Control Board). Zadaniem grupy było zarządzanie przebiegiem prac badawczych prowadzonych w związku z siecią Internet. W 1984 agencja przekształciła ICCB w IAB (Internet Activities Board), która z kolei została podzielona na grupy robocze, zajmujące się takimi zagadnieniami jak zastosowanie, współdziałania, bezpieczeństwo i testowanie. Na koniec IAB została przekształcona w IETF (Internet Engineering Task Force) oraz w IRTF (Internet Research Task Force). Grupy te były odpowiedzialne za rozwój konstrukcji sieci Internet i badania nad rozwojami w tej dziedzinie. DARPA prowadzi badania, rozwija technicznie i koordynuje pod względem naukowym program globalnej obrony antybalistycznej USA.

[117] Opracowano na podstawie: *Modelowanie procesów walki informacyjnej. Model „cyberwar"*, praca zbiorowa pod red. M. Kinasiewicz, AON, Warszawa, 2006 r. s. 83.

częstotliwością, że system nie jest w stanie zrealizować żadnej usługi poza próbą odpowiedzi na żądanie nawiązania połączenia, realizowany jako atak:

- ❖ z pojedynczego komputera na pojedynczy cel,
- ❖ z pojedynczego komputera na wiele celów,
- ❖ rozproszony, z wielu komputerów na jeden cel,
- ❖ rozproszony, z wielu komputerów na wiele celów

➢ podszywanie się, omijanie przez hackera zabezpieczeń wprowadzonych do sieci przez jej administratora, podszywanie i udawanie innego komputera.

3. Ataki przeciwko działaniu systemu – kryptoanaliza, łamanie kryptograficznych zabezpieczeń (zabezpieczeń ochrony kryptograficznej) stosowanych w systemie.
4. Wewnętrzne ataki – kradzież usług, kradzież danych, zarówno bezpośrednio z systemu poprzez zastosowanie różnych technik jak również z archiwizowanych danych.
5. Atak połączony z dostępem i modyfikacją systemu – łamanie zabezpieczeń, omijanie zezwoleń, manipulowanie.

Wszystkie te działania zaliczyć należy do grupy ofensywnych oddziaływań nakierowanych na uniemożliwienie prowadzenia działań sieciocentrycznych. Próba wyliczenia wszystkich znanych sposobów zakłócania pracy systemu kończy się zawsze stwierdzeniem, że jest to pewien zidentyfikowany na dzień dzisiejszy wycinek zagrożeń, których paleta rozszerza się proporcjonalnie do rozwoju narzędzi pozwalających na działanie w systemu.

2.5.4. Obrona przed zagrożeniami

Jedyna i skuteczną metodą przeciwdziałania przed zagrożeniami jest systematyczne doskonalenie technik bezpieczeństwa teleinformatycznego i teleinformacyjnego przy wytwarzaniu, przechowywaniu, przesyłaniu i niszczeniu informacji niejawnych. Ochrona informacji w systemie teleinformatycznym i teleinformacyjnym to przedsięwzięcie techniczne i administracyjne mające na celu zabezpieczenie poszczególnych elementów systemu. Bezpieczeństwo systemów

teleinformatycznych i teleinformacyjnych musi zapewnić informacjom w nich przetwarzanym:[118]

- poufność – dostęp do informacji musi być ograniczony jedynie do grona uprawnionych użytkowników, im wyższy stopień poufności informacji tym mniej upoważnionych użytkowników;
- integralność – informację muszą być zachowane w swej oryginalnej postaci, nie mogą być przez nikogo zmanipulowane;
- dostępność – informacja musi być dostępna na każde żądanie uprawnionego użytkownika;
- rozliczalność – fizyczny dostęp do informacji może być przypisany tylko temu uprawnionemu użytkownikowi, który z niej korzysta (korzystał);
- autentyczność – pochodzenie informacji jest zgodna z zadeklarowanym;
- niezawodność – zachowanie i skutki działania (elementów lub urządzeń systemu zawierającego informacje chronione) są zgodne z zamierzonymi.

Najważniejszym dla zachowania tych cech jest umiejętność przewidywania zagrożeń dla systemu teleinformatycznego. Z analizy zagrożeń wynikają decyzje dotyczące zastosowania określonych rozwiązań sprzętowych, czy programowych zabezpieczenia systemów teleinformatycznych w Siłach Zbrojnych RP.

Do podstawowych przedsięwzięć, niezbędnych do tego, aby system teleinformatyczny zapewniał właściwy poziom bezpieczeństwa, należy:[119]

1. Stworzenie poprawnej konfiguracji wszystkich elementów, które decydują o bezpieczeństwie ruchu w sieci (systemie), a więc takich jak: serwery, stacje robocze, sensory i aplikacje na nich działające.
2. Stosowanie oprogramowania do przeciwdziałania nie uprawnionym działaniom w sieciach, takich jak:

   - oprogramowanie antywirusowe przeciwdziałające wymienionemu powyżej oprogramowaniu złośliwemu,

   - zapory sieciowe analizujące wchodzący ruch sieciowy zgodnie z zasadami określonymi przez administratora sieci,

   - systemy wykrywania intruzów dokonujące identyfikacji czy zdarzenie w sieci jest zagrożeniem czy też działaniem typowym,

---

[118] Janczak J., Świdzikowski G., *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym,* AON, Warszawa 2004 r., s. 11.

[119] Liderman K., *Podręcznik Administratora bezpieczeństwa teleinformatycznego*, MIKOM, Warszawa 2003 r., s. 43.

- skanery sieciowe poszukujące słabych punktów w istniejącym systemie bezpieczeństwa.[120]

3. Opracowanie i wdrożenie systemu tworzenia i przechowywania kopii bezpieczeństwa.
4. Wykorzystanie metod ochrony kryptograficznej w przesyłaniu danych oraz uwierzytelnianiu informacji i ich źródeł.
5. Dublowanie najbardziej wrażliwych elementów sieci.
6. Stosowanie właściwego poziomu ochrony fizycznej dla wszystkich elementów sieci.
7. Zapewnienie właściwego poziomu emisji ujawniającej.

W Siłach Zbrojnych RP wszystkie systemy teleinformatyczne przetwarzające informację niejawną muszą posiadać certyfikat Służby Kontrwywiadu Wojskowego. W myśl Ustawy „O ochronie informacji niejawnych" [121] dopuszcza się również certyfikat wydany przez Agencję bezpieczeństwa Wewnętrznego. W zakresie zagrożeń związanych z emisją ujawniającą w Siłach Zbrojnych RP i w krajach członkowskich NATO obowiązują rozwiązania oparte na normie amerykańskiej TEMPEST (ang. *Temporary Emanation and Spurious Transmission*), która została określona w ramach programu ochrony przed niekontrolowaną emisją ujawniającą, który powstał na początku lat 50-tych na zlecenie Pentagonu[122].

Ze względu na ograniczenia związane z bezpieczeństwem informacyjnym użytkownikami sprzętu teleinformatycznego i teleinformacyjnego klasy TEMPEST mogą być wyłącznie instytucje krajów członkowskich NATO. Sprzęt tej klasy jest wykorzystywany wyłącznie przez: siły zbrojne, agendy NATO, służby ochrony państwa, służby dyplomatyczne, łączność utajniona, łączność kryptograficzna, instytucję odpowiedzialne za ład i porządek oraz instytucję i ośrodki przewarzania danych niejawnych.

Z uwagi na fakt przystąpienia Polski do NATO sprzęt teleinformatyczny klasy TEMPEST jest dostępny w Siłach Zbrojnych RP.

---

[120] Chodzi tutaj o systemy bezpieczeństwa teleinformacyjnego.

[121] Ustawa z dnia 22 stycznia 1999 r. *O ochronie informacji niejawnych*" Tekst ujednolicony po zmianach z dnia 15 kwietnia 2005 r. Dz. U. 1999.11.95; Tekst ujednolicony Dz. U. 2005.196.1631 - akty zmieniające;

[122] Zarówno normy jak i technologia wytwarzania sprzętu klasy TEMPEST są utajnione, lecz pod koniec lat 70-tych umożliwiono jego wytwarzanie producentom prywatnym. Jednakże produkcja sprzętu, laboratoria pomiarowe oraz specjaliści podlegają rygorystycznej okresowej certyfikacji.

Stosowanie sprzętu klasy TEMPEST gwarantuje bezpieczeństwo elektromagnetyczne procesu przetwarzania danych. Można, więc zrezygnować, ze stosowania osłon elektromagnetycznych, filtrów, budowy specjalnych pomieszczeń czy budynków[123].

2.6. Wnioski

1. Nadrzędnym celem walki informacyjnej jest zdobycie panowania nad przeciwnikiem w dziedzinie informacyjnej. Oznacza to stworzenie takiej sytuacji, w której baza informacyjna organów dowodzenia jest pełniejsza, dokładniejsza, wiarygodniejsza i bardziej aktualna niż organów dowodzenia przeciwnika.
2. Cyberterroryzm, przełamuje dotychczasowe „tradycyjne" incydenty komputerowe w kierunku zsynchronizowanych uderzeń na systemy teleinformatyczne przy jednoczesnym zróżnicowaniu typów i metod ataków. Prawdziwym zadaniem jest umiejętność wykrywania zamachów w cyberprzestrzeni i zabezpieczenia się przed ich oddziaływaniem na Infrastrukturę Krytyczną Sil Zbrojnych Rzeczypospolitej Polski.
3. Polityka bezpieczeństwa informacyjnego określa wykaz zasad, co należy chronić, dlaczego i w jaki sposób, aby systemy teleinformatyczne prawidłowo działały w realizacji zadań stawianych przez jednostki organizacyjne. W rozważanym tu wypadku miarą skuteczności jest możliwość niezakłóconej realizacji zadań przez jednostki organizacyjne podległe Ministrowi Obrony Narodowej..
4. Idea działań sieciocentrycznych ma na celu pokazanie jak ważnym elementem współczesnego pola walki jest umiejętność posługiwania się informacją, to znaczy nie tylko gromadzenia jej, ale również, a może przede wszystkim przetwarzania i wyciągania odpowiednich wniosków.
5. Położenie nacisku na techniczną stronę, a więc wyposażenie Sił Zbrojnych RP w dodatkowe urządzenia poprawiające możliwości odbierania bodźców z otaczającego świata (sensorów) stanowi wypaczenie tej idei. Istotą jej jest umiejętność wykorzystania zdobytych danych i przekształcenia jak największej ich ilości w mądrość pozwalającą na efektywniejsze prowadzenie procesu

---

[123] *Modelowanie procesów walki informacyjnej. Model „cyberwar"*, praca zbiorowa pod red. M. Kinasiewicz, AON, Warszawa, 2006 r. s. 89.

wspierania dowodzenia. Oznacza to, że głównym beneficjentem uzyskania przewagi informacyjnej staje się dowódca, który musi umieć wykorzystać uzyskaną przewagę. Problemem pozostaje świadomość, że nie zawsze wiedzieć oznacza rozumieć, a dopiero rozumienie sytuacji z jaką spotykamy się na współczesnym polu walki pozwala na podejmowanie najlepszych decyzji. Jeśli do tego proces decyzyjny wsparty jest odpowiednimi systemami, to istnieje duże prawdopodobieństwo, że doprowadzi do osiągnięcia sukcesu.

6. Rozwojowi koncepcji NCW towarzyszą oczekiwania, że nastąpi wzrost efektywności dowodzenia operacjami, zaś głównym rezultatem ma być efekt synergiczny uzyskany dzięki skuteczniejszej koordynacji i synchronizacji działań, wyższej „świadomości sytuacyjnej". Oczekiwane efekty wiążą się przede wszystkim z racjonalizacją procesów decyzyjnych. Natomiast inną kwestią jest możliwa podatność poszczególnych elementów infostruktury na destrukcyjne oddziaływanie przeciwnika.

ROZDZIAŁ III

POLITYKA BEZPIECZEŃSTWA INFORMACYJNEGO POLSKI

3.1. Bezpieczeństwo informacyjne Polski

Punktem zwrotnym w rozwoju ICT (ang. *Information and Communication Technology*) była cyfryzacja (*digitalizacja*). Umożliwiło to znacznie szybsze, w wyższej jakości i bardziej urozmaicone przekazywanie informacji niezależnie od odległości między poszczególnymi ośrodkami. Rozpowszechnianie się cyfrowych form przekazu wiązało się z transformacją społeczeństw. Zmianie uległy i również wskaźniki rozwoju takie jak praca fizyczna i kapitał zostają stopniowo zastępowane przez informację i wiedzę. Zmiana społeczna następuje pod wpływem rozwoju nowej technologii informatycznej.

Powszechne wyposażenie w urządzenia zaliczane do grupy ICT[124] i dostęp do Internetu są niezbędnymi warunkami powstania i rozwoju społeczeństwa informacyjnego, a informacje w tym zakresie są podstawą dla dalszej analizy celów i sposobów korzystania oraz oceny wpływu stosowania tych technologii na procesy gospodarcze, wyniki ekonomiczne i strukturę organizacyjną przedsiębiorstw oraz na zmiany kulturowe w całym społeczeństwie[125].

Zachodzące w Polsce przemiany są dostrzegalne i dotyczą szeregu aspektów. Następuje zmiana „kurczenia" czasu i przestrzeni w nowym typie społeczeństwa – społeczeństwa informacyjnego. Przestrzeń życia jednostek poszerza się dzięki sieci teleinformatycznych i obejmuje nieomal cały glob. Nowoczesne technologie transportowe, telekomunikacyjne i teleinformatyczne sprawiły, że świat relatywnie się "skurczył". Rewolucja informatyczna ostatnich lat nie nastąpiła nagle, na jej rozwój złożyły się takie wynalazki jak: telegraf, telefon, film,

---

[124] Urządzenia zaliczane do grupy ICT (*Information and Communication Technology* – technologie informacyjno – komunikacyjne) to takie urządzenia jak: telefon stacjonarny, telefon mobilny (komórkowy), komputer osobisty, laptop, pantop etc.

[125] Główny Urząd Statystyczny, *Wykorzystanie technologii informacyjno – telekomunikacyjnych w 2005 r.*, Warszawa, 22.12.2005 r. s. 2.

radio, telewizja. Dopiero jednak wynalezienie komputera umożliwiło dokonanie jakościowej i ilościowej zmiany w charakterze pracy intelektualnej człowieka. Komputery osobiste to urządzenia, które umożliwiły gromadzenie i obróbkę bardzo dużej ilości danych przez dużą liczbę osób.

Według raportu ONZ w sprawie „Globalnego rozwoju Internetu", w którym wydzielono cztery grupy państw wyspecyfikowane pod względem skali zaawansowania wdrożeń ICT w administracji publicznej, Polska znalazła się w drugiej grupie o średnim wskaźniku osieciowania. Dla porównania: Rosja, Litwa, Łotwa, Ukraina, Węgry, Słowacja, Słowenia i Białoruś zostały zaliczone do tej samej grupy, co Polska, zaś Czechy i Estonia do państw najwyżej rozwiniętych[126].

Jest to zapóźnienie, którego przyczyn należy poszukiwać w nierównomiernym rozwoju polskiego sektora ICT. Specyfika polskiej telefonii wyraża się na przykład w dominacji telefonii ruchomej nad telefonią stacjonarną. Telekomunikacja opiera się na systemach cyfrowych, stanowiących substytut telefonii przewodowej. Kraj nasz uzupełnia w ten sposób dysproporcje rozwojowe, których ewidentnym dowodem było przedostatnie miejsce wśród krajów europejskich w zakresie współczynnika liczby abonentów telefonicznych na 100 obywateli. Listę tę w 1993 r. zamykała Albania. Telefonia komórkowa oceniana bywa jako istotny czynnik rozwoju cywilizacji informacyjnej, porównywalny z Internetem. Pomimo niskiego wskaźnika usieciowania oraz zapóźnienia w stosunku do Czech czy Węgier, polski rynek usług operatorów internetowych rozwija się w sposób bardziej konkurencyjny. Podczas, gdy u naszych sąsiadów obserwuje się zdecydowany monopol usług, w Polsce o klienta walczą ze sobą liczni usługodawcy tacy jak: Onet.pl, Telekomunikacja Polska, Tele 2, Intermedia, Multimedia, Netia, UPC oraz inni usługodawcy.

Jaką popularnością cieszy się, więc w Polsce Internet? Od kwietnia 2005 r. Główny Urząd Statystyczny przeprowadza rundę regularnych badań wykorzystania technologii informacyjno – telekomunikacyjnych w przedsiębiorstwach i gospodarstwach domowych oraz badanie pilotażowe wykorzystania ICT w przedsiębiorstwach sektora niefinansowego i finansowego oraz gospodarstwach domowych. Wynik tych badań przedstawiono w układzie priorytetów programu eEuropa+, przyjętego w 2001 r. przez 10 krajów kandydujących wówczas do Unii Europejskiej, jako odpowiednik planu eEuropa dla państw członkowskich:

1. Tworzenie podstaw społeczeństwa informacyjnego.

---

[126] A. Bógdał – Brzezińska, M. F. Gawrycki, *Cyberterroryzm i problemy*..., op.cit., s. 280.

2. Szybki bezpieczny Internet.
3. Inwestowanie w umiejętności.
4. Stymulowanie korzystania z Internetu[127].

Badania wykorzystania ICT w przedsiębiorstwach zostały przeprowadzone na reprezentatywnej próbie 14000 przedsiębiorstw. W przedsiębiorstwach sektora finansowego badaniem pilotażowym objęto pośrednictwo finansowe (poza działalnością Banku Centralnego) obejmując prawie 1500 przedsiębiorstw. Badania wykorzystania ICT w gospodarstwach domowych i wśród osób indywidualnych zostało przeprowadzone na reprezentatywnej próbie ponad 8200 gospodarstw domowych. Wzięło w nim udział prawie 14000 osób w wieku 12 – 74 lat.

Wyniki tych badań pokazały, że prawie we wszystkich dziedzinach życia społecznego i gospodarczego można zauważyć wzrost wykorzystania nowoczesnych technologii informacyjno – telekomunikacyjnych[128].

Z roku na rok przybywa gospodarstw domowych wyposażonych w komputery, telefony komórkowe oraz posiadających dostęp do Internetu. W tej ostatniej grupie szybko rośnie udział gospodarstw domowych posiadających łącza szerokopasmowe, co sprzyja bardziej intensywnemu korzystaniu z globalnej sieci i różnorodnych usług świadczonych za pomocą Internetu, w tym na przykład z handlu elektronicznego.

W Tabeli 3.1., przedstawiono charakterystykę popularności technologii informacyjno - teleinformatycznych i komunikacyjnych w Polsce.

---

[127] Główny Urząd Statystyczny, *Wykorzystanie technologii informacyjno – telekomunikacyjnych w 2005 r.*, Warszawa, 22.12.2005 r. s. 1.
[128] Główny Urząd Statystyczny, *Wykorzystanie technologii informacyjno – telekomunikacyjnych w 2006 r.*, Warszawa, 17.11.2006 r. s. 1.

Tabela 3.1. Popularność technologii informacyjno – teleinformatycznych i komunikacyjnych w Polsce

Lp.	Zagadnienia	Rok				
		2004	2005	2006	2007	2008
1.	Obecność telefonów komórkowych w gospodarstwach domowych		62% (47%)*	83%	70%***	
2.	Obecność telefonów stacjonarnych w gospodarstwach domowych		(80%)*		71%***	
3.	Obecność telefonów komórkowych umożliwiających dostęp do Internetu w gospodarstwach domowych	19%	23%			
4.	Obecność komputerów w gospodarstwach domowych	36%	40% (45%)*	45%	53%	59%
5.	Obecność Internetu w gospodarstwach domowych	26%	30% (26%)*	36%	40%	48%
6.	Przedsiębiorstwa wykorzystujące komputery	92%	93%	93%	94%	95%
7.	Przedsiębiorstwa posiadające dostęp do Internetu	85%	87%	89%	92%	93%
8.	Szerokopasmowy dostęp do Internetu w gospodarstwach domowych	8%	16%	22%	30%	38%
9.	Szerokopasmowy dostęp do Internetu w przedsiębiorstwach	28%	43%	46%		59%
10.	Korzystanie z komputera przez osoby indywidualne codziennie lub prawie codziennie	23%	28%	35%	40%	44%
11.	Korzystanie z komputera przez osoby indywidualne regularnie – raz w tygodniu	35%	40% (40%)*		39%	
12.	Korzystanie z komputera przez osoby indywidualne w ciągu ostatnich 3 miesięcy	40%	45% (43%)*			
13.	Korzystanie z Internetu przez osoby indywidualne codziennie lub prawie codziennie	12%	17%			
14.	Korzystanie z Internetu przez osoby indywidualne regularnie – raz w tygodniu	22%	29% (27%)*			
15.	Korzystanie z Internetu przez osoby indywidualne w ciągu ostatnich 3 miesięcy	29%	35% (33%)*			
16.	Osoby używające komputer w domu		(77%)*		43%	49%
17.	Osoby używające komputer w miejscu pracy		38% (38%)*	38%	35%	36%
18.	Osoby używające komputer w szkole lub na uczelni		(22%)*		10%	9%
19.	Osoby używające Internet w szkole lub innych placówkach edukacyjnych	8%	10% (24%)*		9%	9%
20.	Osoby używające Internet w miejscu pracy	21%	27% (32%)*			28%

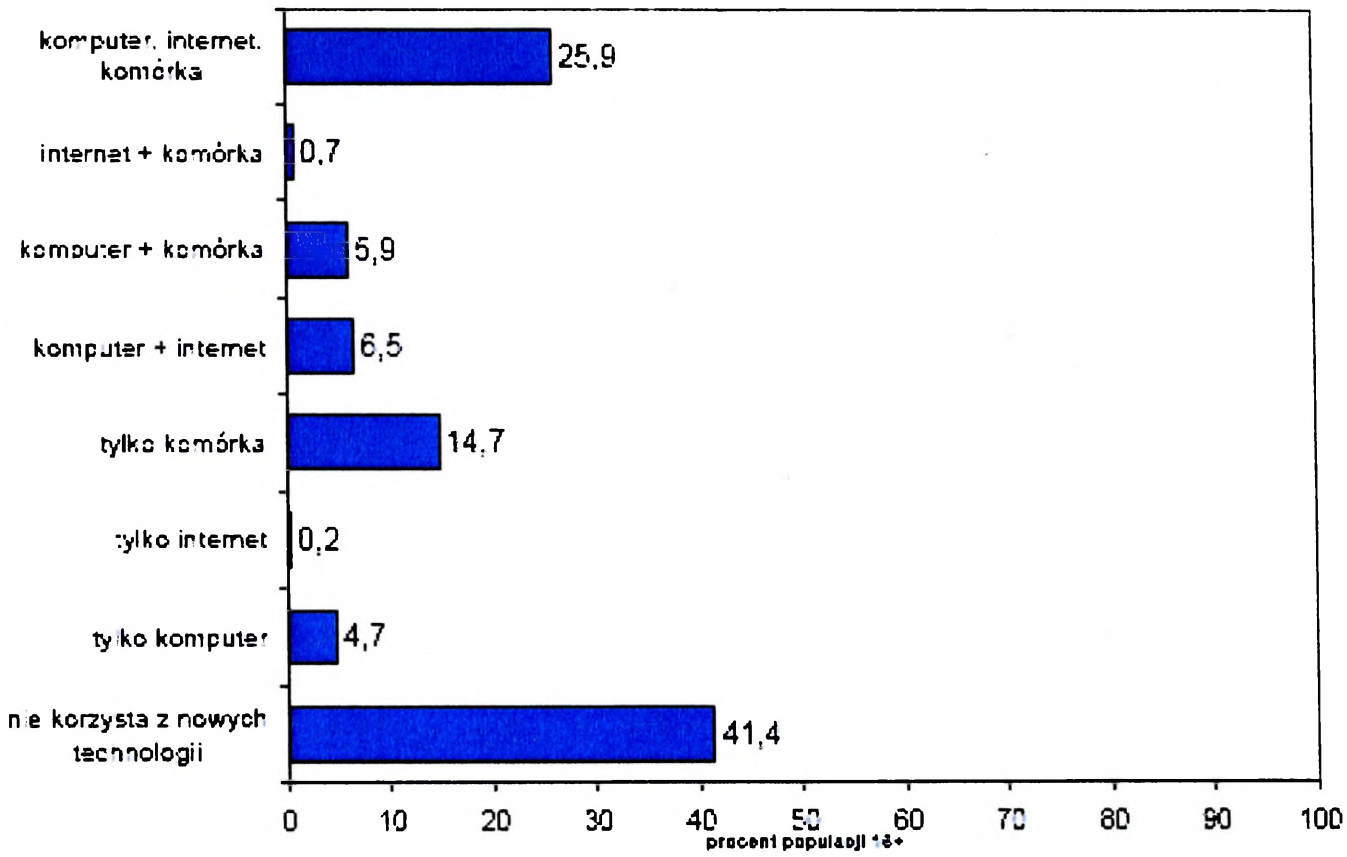
Lp.	Zagadnienia	Rok				
		2004	2005	2006	2007	2008
21.	Osoby używające Internet w domu	15%	20% (63%)*			44%
22.	Cel wykorzystania Internetu przez osoby indywidualne – komunikowanie się	24%	30%	34%	26%	31%
23.	Cel wykorzystania Internetu przez osoby indywidualne – wyszukiwanie informacji o towarach i usługach	15%	18%	25%	27%	33%
24.	Cel wykorzystania Internetu przez osoby indywidualne – czytanie, pobieranie czasopism on – line	14%	13%	17%	15%	19%
25.	Cel wykorzystania Internetu przez osoby indywidualne – korzystanie z usług bankowych	4%	6% (32%)*	9%	13%	17%
26.	Cel wykorzystania Internetu przez osoby indywidualne – kupowanie i zamawianie towarów i usług	4%	5%	12%	27%	33%
27.	Korzystanie z nowych technologii – komputera		(43%)*			
28.	Korzystanie z nowych technologii – Internet		(33%)*			
29.	Korzystanie z nowych technologii – telefon komórkowy		(48%)*			
30.	Korzystanie z nowych technologii – umiejętności korzystania z komputera		(1%)*			
31.	Korzystanie z technologii komunikacyjno – informacyjnych		(26%)*			

* *Diagnoza społeczna 2005*, praca zbiorowa pod red. Czapiński J., Panek T., Wyższa Szkoła Finansowa i Zarządzania w Warszawie, Warszawa,10 styczeń 2006 r.

** A. Bógdał – Brzezińska, M. F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, ASPRA – JR, Warszawa 2003 r. s. 281.

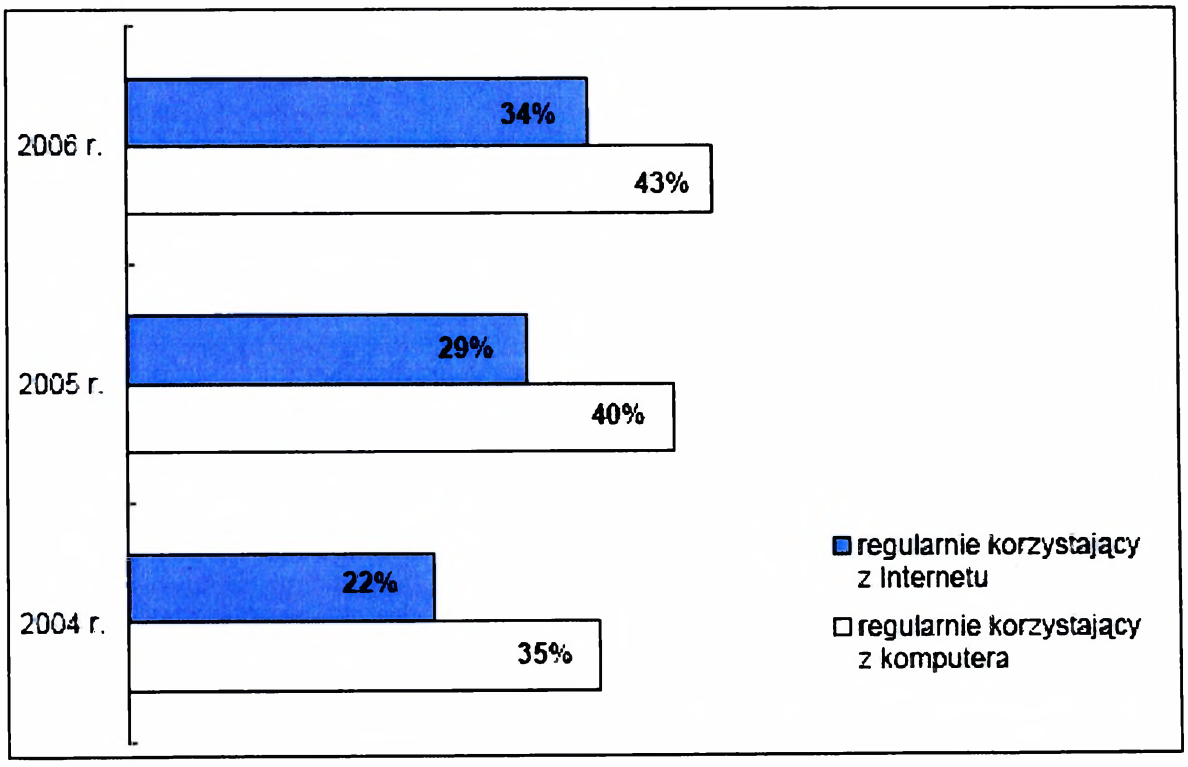
*** *Diagnoza społeczna 2007,* WNP, Konferencje, Warszawa 27.06.2007 r.

Źródło: Opracowanie własne na podstawie raportu z badań Głównego Urzędu Statystycznego, *Wykorzystanie technologii informacyjno – telekomunikacyjnych w 2005 r.*, Warszawa, 22.12.2005 r., *Wykorzystanie technologii informacyjno – telekomunikacyjnych w 2006 r.*, Warszawa, 17.11.2006 r., Główny Urząd Statystyczny, Wykorzystanie technologii informacyjno – telekomunikacyjnych w przedsiębiorstwach, gospodarstwach domowych i przez osoby prywatne w 2008 r., Warszawa, 2009 r. oraz Mały rocznik statystyczny polski 2009, GUS, Warszawa 2009 r.



Rysunek 3.1. Korzystanie z nowych technologii

Źródło: *Diagnoza społeczna 2005*, praca zbiorowa pod red. Czapiński J., Panek T., Wyższa Szkoła Finansowa i Zarządzania w Warszawie, Warszawa, 10 styczeń 2006 r.



Rysunek 3.2. Odsetek osób korzystających regularnie[129] z komputera i Internetu w latach 2004 - 2006

Źródło: Główny Urząd Statystyczny, *Wykorzystanie technologii informacyjno – telekomunikacyjnych w 2006 r.*, Warszawa, 17.11.2006 r.

W badaniach przeprowadzonych przez Główny Urząd Statystyczny poświęcono również miejsce zagadnieniu związanym z bezpieczeństwem

[129] Regularnie, znaczy co najmniej raz w tygodniu.

teleinformatycznym. W podrozdziale tym przedstawiono problematykę związaną ze środkami ostrożności stosowanymi przy korzystaniu z Internetu oraz z bezpieczeństwem w sieci.

Tabela 3.2., przedstawia stan bezpieczeństwa teleinformacyjnego w Polsce w 2007 r., oraz Tabelę 3.3., która przedstawia statystykę przestępczości komputerowej w Polsce.

Tabela 3.2. Stan bezpieczeństwa teleinformacyjnego w Polsce w 2007 r

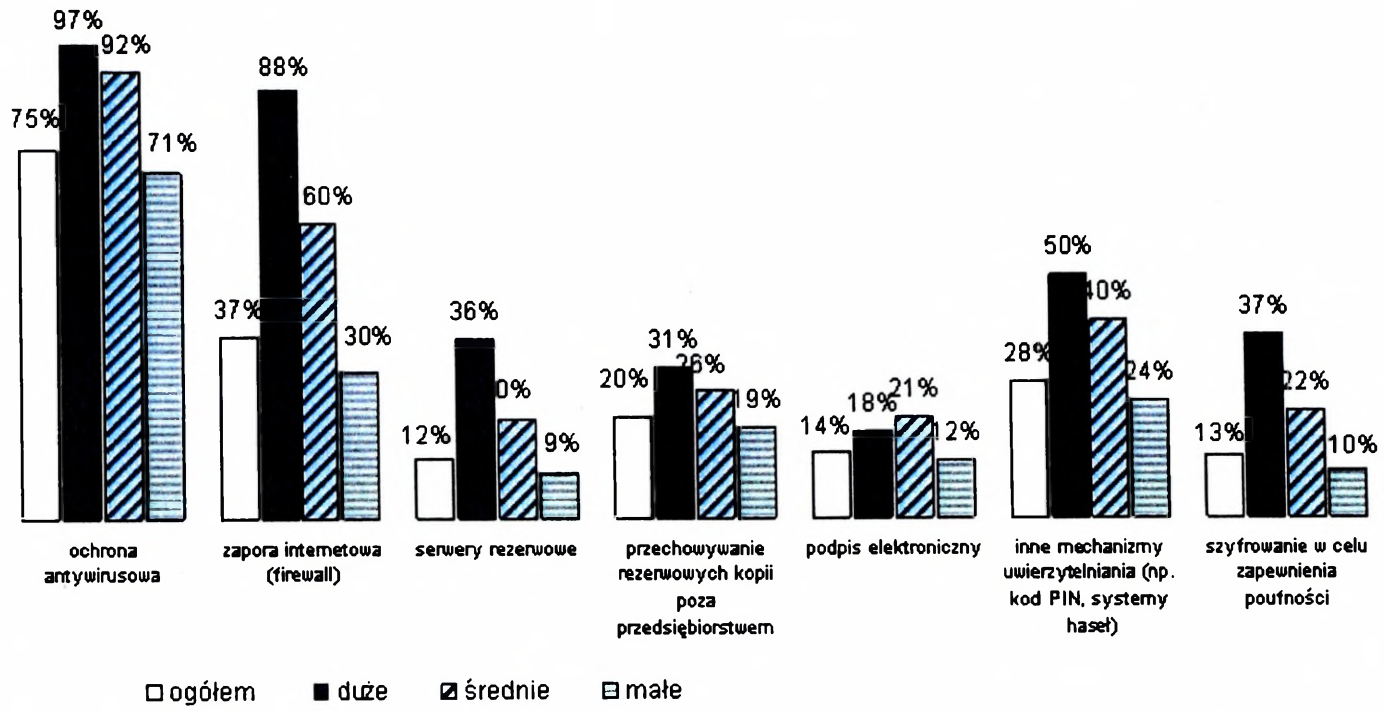
Lp.	Zagadnienie		Rok	
			2006	2007
1.	Osoby indywidualne mające problem z bezpieczeństwem korzystania z Internetu	Wirus komputerowy.	10%	12%
		Otrzymywanie niechcianych e-mail (spam).	11%	12%
2.	Przedsiębiorstwa mające problem związany z utrzymaniem bezpieczeństwa sieci lub danych	Ogółem.	23%	23%
		Małe.	20%	20%
		Średnie.	29%	30%
		Duże.	49%	42%
3.	Przedsiębiorstwa mające problem związany z utrzymaniem bezpieczeństwa sieci lub danych – zawirusowanie komputera	Małe.		19%
		Średnie.		29%
		Duże.		41%
4.	Przedsiębiorstwa mające problem związany z utrzymaniem bezpieczeństwa sieci lub danych – dostęp nieupoważnionej osoby	Małe.		1%
		Średnie.		1%
		Duże.		2%
5.	Środki ostrożności stosowane przy korzystaniu z Internetu rzez osoby indywidualne	Program antywirusowy.	14%	18%
		Korzystanie z metod identyfikacji on-line.	7%	13%
		Zapora internetowa.	4%	5%

Źródło: Opracowanie własne. Wszystkie dane pochodzą z badań Głównego Urzędu Statystycznego, *Wykorzystanie technologii informacyjno – telekomunikacyjnych w 2007 r.*, Warszawa, 22.12.2007 r.

Tabela 3.3. Statystyka przestępczości komputerowej w Polsce

Lp.	Rodzaj przestępstwa	Rok		
		2006	2007	2008
1.	Oszustwo komputerowe	444	492	404
2.	Uzyskanie informacji	370	384	505
3.	Zniszczenie lub zmiana istotnej informacji	136	168	249
4.	Sabotaż komputerowy	19	11	13
5.	Zniszczenie lub zmiana informacji	4	0	2

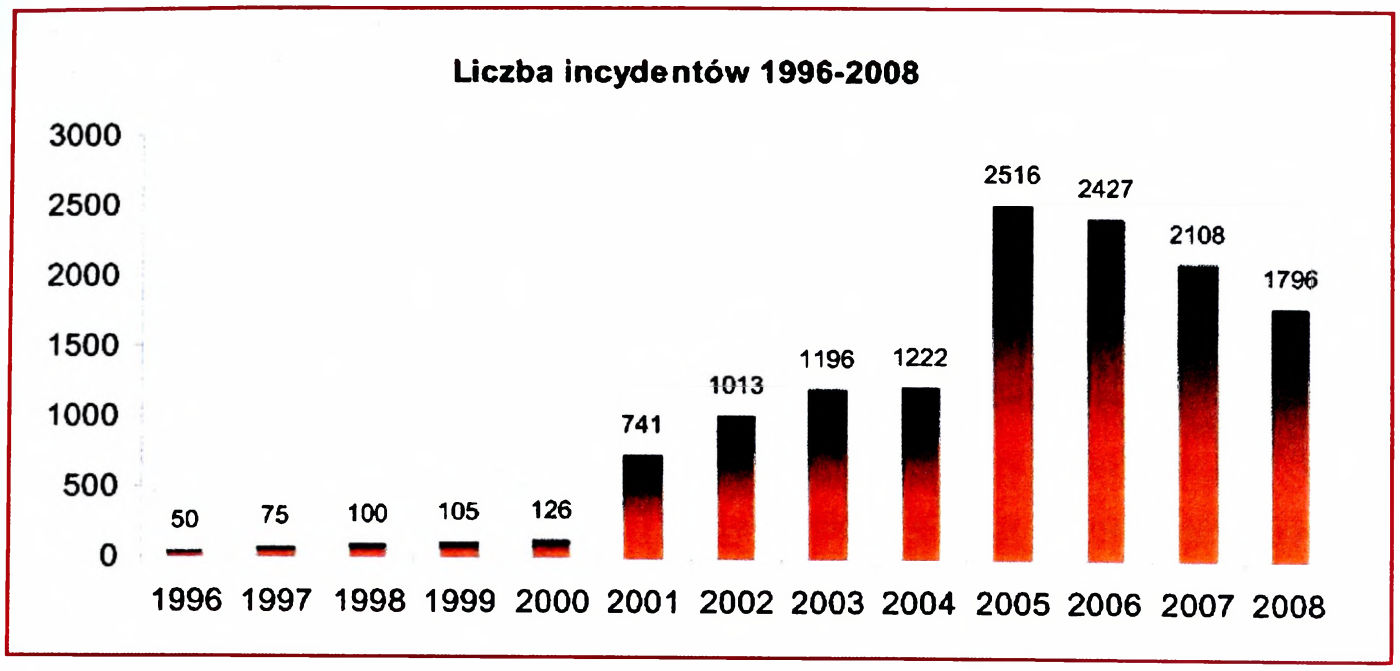
Źródło: Opracowanie własne. Wszystkie dane pochodzą z Komendy głównej Policji [URL – http://www.policja.pl/portal/pol/4/321/PRZESTEPCZOSC_KOMPUTEROWA.html] 24.09.2009 r. 10.20.



Rysunek 3.3. Odsetek przedsiębiorstw stosujących zabezpieczenia informatyczne w 2007 r. według rodzajów zabezpieczeń lub metod uwierzytelnienia

Źródło: Głównego Urzędu Statystycznego, *Wykorzystanie technologii informacyjno – telekomunikacyjnych w 2007 r.*, Warszawa, 22.12.2007 r.

Liczba osób, które napotkała jakiekolwiek problemy dotyczące bezpieczeństwa w sieci rośnie dożo wolniej niż przybywa użytkowników Internetu. Przedsiębiorstwa, w których wystąpił problem związany z bezpieczeństwem w sieci lub danych utrzymał się na tym samym poziomie i wynosi 23%. Najczęściej występującym problemem dotyczącym bezpieczeństwa sieci i danych było zawirusowanie komputera powodujące utratę danych (41% przedsiębiorstwa duże, 29% średnie i 19% małe). Najczęściej stosowanym zabezpieczeniem komputera domowego były programy antywirusowe. Zaporę internetową w postaci sprzętu teleinformatycznego lub oprogramowania wykorzystuje czterokrotnie mniej osób. Zabezpieczenia informatyczne stosowane przez przedsiębiorstwa pozostały na poziomie z 2006 r. czyli 79%, a najpopularniejszym rodzajem zabezpieczenia była ochrona antywirusowa.



Rysunek 3.4. Liczba zarejestrowanych incydentów komputerowych
Źródło: Opracowanie własne na podstawie CERT.GOV.PL.

W maju 2000 r. w Warszawie zorganizowana została konferencja pod tytułem „Information Society - Acceleratins European Integration", poświęcona zagadnieniom społeczeństwa informacyjnego[130]. W dokumencie końcowym konferencji Polska i inne kraje kandydujące zobowiązały się do współpracy z Komisją Europejską przy opracowaniu wspólnego dokumentu programowego eEurope+ oraz przygotowania krajowego planu działania inicjatywy - ePolska.

Deklaracja konferencji warszawskiej zakładała, że celami politycznymi, które mają osiągnąć kraje kandydackie poprzez wspólny plan działania eEurope+ są:

- zademonstrowanie opinii publicznej wspólnych wysiłków krajów „Piętnastki" oraz krajów kandydujących na rzecz realizacji wyzwań nowej ekonomii;
- wskazanie, że proces akcesji to coś znacznie większego niż tylko negocjowanie;
- polityczne wsparcie dla wysiłków czynionych przez kandydujące kraje w kierunku integracji europejskiej;
- zaprezentowanie komplementarności inicjatywy eEurope oraz planu eEurope+.

Jednocześnie podkreślano, że plan działania eEurope+ jest ofertą fakultatywną i nie będzie krajom tym narzucany, powinien natomiast korelować z narodowymi inicjatywami, do których należy ePolska.

W programie ePolska, autoryzowanym przez Ministerstwo Łączności, przedstawiono w czerwcu 2001 r. plan działań na rzecz rozwoju społeczeństwa

[130] A. Bógdał – Brzezińska, M. F. Gawrycki, *Cyberterroryzm i problemy*..., op.cit., s. 289.

informacyjnego w Polsce[131]. Program obejmuje, pięcioletni okres zmian, które nastąpią w wielu sektorach gospodarki pod patronatem rządu. Rozdziały dokumentu odpowiadają realizacji proponowanych przez Sejm i Komitet Badań Naukowych (KBN)[132] obszarów implementacji społeczeństwa informacyjnego:

- rozwojowi infrastruktury telekomunikacyjnej;
- szybkiej, powszechnej internetyzacji;
- programom edukacyjnym adresowanym do pracowników;
- wykorzystywaniu Internetu w administracji państwowej, sądownictwie, policji, ochronie zdrowia, opiece społecznej i w transporcie.

Ogólną koncepcję bezpieczeństwa informacyjnego przedstawiono w rozdziale pod tytułem „Bezpieczeństwo sieci". Wymieniono tu nowe rodzaje przestępstw: przestępstwa przeciwko poufności, integralności i dostępności danych oraz systemów. Zwraca się uwagę na wysokie koszty zaproponowanych zabezpieczeń oraz spowolnienie pracy systemów informacyjnych, dlatego też sugerowane jest zróżnicowanie technik bezpieczeństwa, pozostawiające sektorowi prywatnemu swobodę w ich doborze.

Wymienia się także instytucje działające na rzecz bezpieczeństwa informacyjnego, systematyzując ich obszary kompetencyjne. Zespół powstały w Wydziale ds. Przestępczości Gospodarczej Biura Koordynacji Służby Kryminalnej Komendy Głównej Policji zajmuje się od 1998 r. zwalczaniem cyberprzestępczości oraz koordynacją operacyjną w tym zakresie. Zespół ten zajmuje się ponadto przestępstwami popełnianymi na szkodę operatorów telefonii komórkowej i przewodowej. CERT Polska (ang. *Computer Emergency Response Team*), działający od 1996 r., monitoruje i rejestruje zdarzenia naruszające bezpieczeństwo sieci Internet. Powyższe struktury realizować mają następujące cele:

- podnosić stopień bezpieczeństwa sieci i dostępu do usług elektronicznych;
- nie ograniczać wolności wyboru zabezpieczeń przez podmioty prywatne;
- pogłębiać konwergencję zabezpieczeń w różnych rodzajach mediów;
- inspirować i wdrażać efekty współpracy z zagranicą w zakresie bezpieczeństwa sieciowego[133].

---

[131] Ministerstwo Gospodarki, *ePolska. Plan działania na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001 – 2006*, Warszawa, czerwiec 2001 r. s. 5.
[132] Należy pamiętać, że jest 2001 r.
[133] Ministerstwo Gospodarki, *ePolska. Plan działania na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001 – 2006*, Warszawa, czerwiec 2001 r. s. 17.

Celom tym podporządkowano sektorowe działania przewidziane do realizacji w okresie pięciu lat. Zadeklarowano opracowanie szczegółowej strategii bezpieczeństwa sieciowego, nowelizację i tworzenie aktów prawnych odnoszących się do cyberprzestępstw oraz pogłębienie kooperacji międzynarodowej. Koordynację strategii przydzielono Ministerstwom: Sprawiedliwości, Spraw Wewnętrznych i Administracji, Spraw Zagranicznych; Komitetu Badań Naukowych, CERT Polska i Komendy Głównej Policji.

Dążenie do poprawy bezpieczeństwa wewnętrznego państwa zostało opisane jako nadrzędny cel rozwoju łączności i technologii informacyjnej w policji[134]. Komunikacja intranetowa służyć ma przepływowi danych z systemów PESEL, REGON, Centralnej Ewidencji Kierowców i Pojazdów oraz Centralnego Rejestru Skazanych. Przewidywane są działania na rzecz budowy systemów analizy kryminalnej (ALERT i Ana - lyst's Notebook) oraz zacieśnienie współpracy w zakresie zdalnego obiegu danych z Interpolem i Europolem.

Stopień przygotowania Polski do wdrożenia strategii rozwojowej ePolska został przedstawiony po raz pierwszy w raporcie o implementacji programu eEurope+, podczas konferencji, zorganizowanej w Ljubljanie w czerwcu 2002 r. Przedstawiono tam zarówno raport z listopada 2000 r., jak również założenia Strategii na lata 2001 – 2006 r., a zaprezentowany poziom zaawansowania spotkał się z aprobatą władz Unii Europejskiej.

W przedstawionym dokumencie nie uwzględniono, strategii rozwoju systemów teleinformatycznych o „terenie", stanowiących bazę odniesienia dla zarządzania zasobami naturalnymi, funkcjonowania sądownictwa, służb geodezyjnych, transportu, budownictwa czyli infrastruktury krytycznej państwa. Nieporozumieniem wydaje się także zapis dotyczący planów budowy zamkniętych resortowych systemów teleinformatycznych (na przykład Policja, MON), przy jednoczesnym braku koncepcji tworzenia systemów teleinformatycznych warunkujących bezpieczeństwo społeczeństwa, takich jak: systemy monitorujące skażenia, pożary oraz systemy zarządzania w sytuacjach kryzysowych.

Zbyt małą wagę, przywiązuje się w dokumencie do nieuchronnej unifikacji systemów teleinformatycznych państwa z systemami Unii Europejskiej, brak jasno określonych działań w tym zakresie, a szczególnie w zakresie bezpieczeństwa teleinformatycznego. System Schengen i IDA to niewielki fragment problemu, który

[134] Ibidem, s. 46 – 47.

w efekcie stanowił będzie o społecznym odbiorze naszej obecności w Unii Europejskiej[135].

3.2. Infrastruktura krytyczna w Polsce

Urządzenia teleinformatyczne pracują obecnie dla wszystkich sektorów społeczeństwa, decydują o rozwoju każdej z dziedzin działalności człowieka w obecnym świecie. Kształtują one nowe rozwiązania techniczne od bezpiecznych systemów bankowych, poprzez nowoczesne i wydajne systemy produkcyjne, oświatę i ochronę zdrowia, aż po systemy teleinformatyczne zapewniające sprawną administracje państwową oraz bezpieczeństwo zewnętrzne i wewnętrzne kraju.

Z analizy wyznań i zagrożeń, przed którymi stają współczesne społeczeństwa, usprawiedliwionym wydaje się stwierdzenie, że gros z nich koncentruje się w obszarze funkcjonowania Infrastruktury Krytycznej Państwa, zwłaszcza w jej warstwie systemowej, coraz bardziej uzależnionej od postępującego wdrażania nowoczesnych technologii[136].

Po wydarzeniach z 11 września 2001 r. nakazem staje się ciągła budowa i ochrona Infrastruktury Krytycznej, a polityka bezpieczeństwa infrastruktury stanowić będzie przez długie lata najważniejszą część strategii bezpieczeństwa naszego państwa. Informacja a nie pieniądze, stała się na dzień dzisiejszy zasobem strategicznym. Przyszłe konflikty zbrojne będą konfliktami o dostęp do informacji. Z dnia na dzień zwiększa się groźba ataków terrorystycznych (cyberatak) na systemy teleinformatyczne i łączności, które grożą totalnym paraliżem administracji państwowej oraz gospodarki narodowej.

W Polsce uznaje się, że zagrożenie cyberterrorystyczne jest bardziej wymysłem filmowców i literatury niż realną groźbą dla współczesnego świata. Mówi się, że podobne przewidywania były już często formułowane, a jednak nie doszło do żadnego ataku cyberterrorystycznego na dużą skalę. Warto się jednak

---

[135] Uwagi do projektu dokumentu *„ePolska – Strategia rozwoju społeczeństwa Informacyjnego w Polsce na lata 2001 – 2006”* [URL – http://www.infoport.pl/kontent/?.html] 21.04.2007 r. 13.22.

[136] Sienkiewicz P., Błażejczyk W., Lichocki E., Jóźwiak M., Świeboda H., *Analiza systemowa cyberterroryzmu zagrożenie dla bezpieczeństwa państwa. Analiza systemowa zagrożeń informatycznych w środowisku bezpieczeństwa państwa*, Wydział Strategiczno – Obronny, AON, Warszawa 2006 r. s. 61.

zastanowić, czy brak „osiągnięć" terrorystów w wykorzystaniu Internetu do własnych celów jest dowodem na to, że znajduje się ona poza ich obszarem zainteresowania.

Internet przestał być już jednak traktowany jako tylko narzędzie rozrywki, coraz częściej słychać o nowych pomysłach związanych z wykorzystaniem globalnej sieci: podpis elektroniczny, e-government, e-commerce, głosowanie przez Internet i wiele innych. Wszystko to sprawia, że zwolna skraca się dystans dzielący nas od państw najbardziej „osieciowanych".

Należy powiedzieć, że prognozy nie są optymistyczne, ponieważ prognozuje się, że terroryści mogą zaatakować Infrastrukturę Krytyczną Państwa, za pomocą programów niszczących systemy teleinformatyczne (np. wirusów, robaków, koni trojańskich), zalać Internet i sieci teleinformatyczne olbrzymią liczbą przesyłanych informacji, co spowoduje jej zapchanie i praktyczną jej bezużyteczność, za pomocą na przykład wysokoenergetycznych fal elektromagnetycznych zniszczyć dane przechowywane w systemach i sieciach komputerowych. Tego rodzaju atak w połączeniu z atakiem konwencjonalnym, chemicznym, biologicznym lub jądrowym, może zwiększyć panikę i przerażenie, może tez w poważny sposób zakłócić działanie służb użyteczności państwowej. Najbardziej zdradziecką cecha terroryzmu mogą okazać się nie szkody fizyczne, lecz te które sami sobie wyrządzimy ze strachu przed nim.

Interpretacja definicji Infrastruktury Krytycznej Państwa, pozwoli zrozumieć i w sposób zrozumiały przedstawić podstawowe aspekty bezpieczeństwa teleinformatycznego w stosunku realizowanej rozprawy.

Infrastruktura Krytyczna to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalne obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura Krytyczna obejmuje systemy:

- ***zaopatrzenia w energię i paliwa;***
- ***łączności i sieci teleinformatycznych;***
- ***finansowe;***
- ***zaopatrzenia w żywność i wodę;***
- ***ochrony zdrowia;***
- ***transportowe i komunikacyjne;***
- ***ratownicze;***
- ***zapewniające ciągłość działania administracji publicznej;***
- ***produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych[137].***

Dla potrzeb niniejszej rozprawy doktorskiej oraz na potrzeby kwestionariusza ankiety przyjęto następującą definicję Infrastruktury Krytycznej Państwa:

Infrastruktura Krytyczna to fizyczne i wirtualne systemy o zasadniczym znaczeniu dla minimalnego funkcjonowania gospodarki, rządu i państwa. Niezdolność do działania Infrastruktury Krytycznej znacznie obniża sprawność obrony i bezpieczeństwo gospodarki danego państwa. Infrastruktura Krytyczna składa się z następujących infrastruktur - sektorów krytycznych:

---

[137] Definicja Infrastruktury Krytycznej zawarta w art. 3 ust. 2, Dz. U. Nr 89 poz. 590 (Dz. U. 07.89.590) z dnia 21 maja 2007 r.

Tabela 3.4. Lista sektorów Infrastruktury Krytycznej

Sektor	Składniki sektorów
I. Energia	1. Gaz, ropa naftowa, paliwa płynne. 2. Urządzenia do wydobywania, przetwarzania i przechowywania gazu, ropy naftowej i paliw płynnych. 3. Elektrownie. 4. Energetyczne sieci transmisyjne i dystrybucyjne dostarczające elektryczność, gaz, ropę naftową oraz paliwa płynne do użytkowników końcowych, m.in. do domów, agencji rządowych i różnego rodzaju firm.
II. Woda	5. Zasoby wodne, rezerwuary i zbiorniki wodne. 6. Systemy transportowania i dostarczania wody do domów i do celów przemysłowych. 7. Urządzenia do filtrowania i uzdatniania wody oraz system kontroli jakości wody. 8. System odbioru wody zużytej wraz z oczyszczalniami ścieków. 9. System dostarczania wody do instalacji przeciwpożarowych.
III. Transport	10. Transport drogowy wraz z drogami, autostradami, ciężarówkami i samochodami osobowymi. 11. Transport kolejowy wraz z siecią połączeń kolejowych, stacje kolejowe i tabor kolejowy. 12. Transport lotniczy wraz z siecią połączeń lotniczych z liniami lotniczymi, lotniska i samoloty. 13. Transport wodny – śródlądowy wraz z flotą handlową portami i drogami wodnymi. 14. Transport wodny – morski i oceaniczny wraz z flotą handlową portami i drogami wodnymi. 15. System dystrybucji towarów krytycznie ważnych dla bezpieczeństwa i stabilności gospodarki wraz z infrastrukturą.
IV. Systemy i technologia teleinformatyczna, łączność, ICT	16. Sieci teleinformatyczne, oprogramowanie, procesy i ludzie dbające o prawidłowe działanie i bezpieczeństwo. Instalacje służące pierwotnemu przechowywaniu i przetwarzaniu danych. 17. Systemy automatyki i kontroli (SCADA itd.). 18. Internet. 19. Stacjonarne systemy telekomunikacyjne. Centrale telefoniczne. 20. Mobilne systemy telekomunikacyjne (telefonia komórkowa). 21. Łączność i nawigacja radiowa. 22. Łączność i nawigacja satelitarna. 23. Systemy powiadamiania (Broadcasting).

Sektor	Składniki sektorów
V. Zdrowie	24. Szpitale. 25. Zdrowie publiczne. 26. Stacje przechowujące zapasy krwi. 27. Laboratoria i instytucje badawcze. 28. Przemysł farmaceutyczny.
VI. Żywność	29. Produkcja żywności. 30. Magazynowanie i dystrybucja żywności.
VII. Bankowość i finanse	31. Banki i bankowość. 32. Ubezpieczenia. 33. Giełda. 34. System rezerw finansowych.
VIII. Administracja państwowa	35. Ministerstwo Obrony. 36. Służba Ochrony Państwa. 37. Parlament (Sejm i Senat). 38. Kluczowe ministerstwa państwowe gwarantujące ciągłość działań rządu. 39. Służby ratunkowe (pogotowie ratunkowe, straż pożarna, policja, wszystkie systemy ratownictwa). 40. Elektrownie jądrowe. 41. Usługi doręczycielskie, poczta i spedycja. 42. Centra zarządzania kryzysowego.
IX. Narodowe pomniki i pamiątki	43. Budynki, pomniki i muzea o znaczeniu ogólnonarodowym, obiekty sportowe.
X. Istotny przemysł dla gospodarki	44. Przemysł zbrojeniowy. 45. Przemysł ciężki. 46. Produkcja i magazynowanie substancji niebezpiecznych (chemiczne, biologiczne i jądrowe). 47. Składowanie odpadów niebezpiecznych.
XI. Wymiar sprawiedliwości	48. Sądownictwo i wymiar sprawiedliwości.
XII. Przestrzeń kosmiczna, eksploracja kosmosu	49. Przestrzeń kosmiczna. 50. Prowadzenie prac badawczych i wprowadzanie nowych technologii w przestrzeni kosmicznej.
XIII. Kluczowe zasoby	51. Centra handlowe. 52. Budynki biurowe. 53. Stadiony, areny i obiekty sportowe. 54. Parki rozrywki. 55. Budynki szkolne. 56. Przemysł turystyczny.

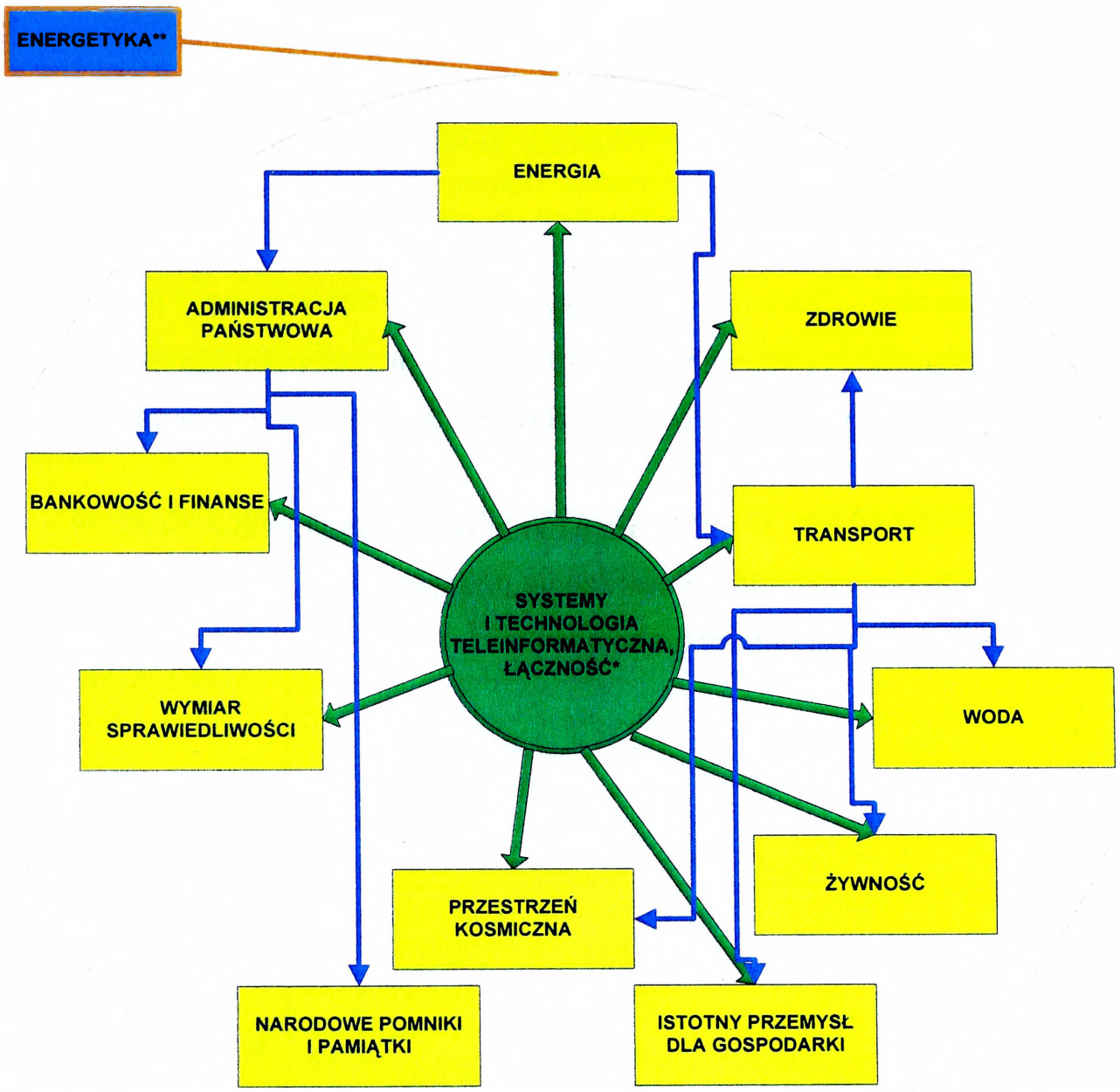
Źródło: Opracowanie własne na podstawie: *Trusted Information Sharing Network for Critical Infrastructure Protection, National Counter* – Terrorism Committee, Critical Infrastructure Protection in Australia, Australia 25 March 2003 r., *Zielona księga w sprawie europejskiego programu ochrony infrastruktury krytycznej, COM /2005/ 576 końcowy*, Bruksela 17.11 2005 r. oraz Liedel K., Piasecka P., *Jak przetrwać w dobie zagrożeń terrorystycznych. Elementy edukacji antyterrorystycznej*, Trio, Warszawa 2007 r.

Rozpatrując zagadnienia Infrastruktury Krytycznej Państwa, istnieje potrzeba zdefiniowania dwóch pojęć[138]odnosząc się do obiektów potencjalnego oddziaływania zewnętrznego (zasoby) oraz elementów łączące te obiekty (infrastruktura), a mianowicie:

Krytyczne zasoby (aktywa) teleinformatyczne definiowane jako zasoby wykorzystywane dla utrzymania bezpieczeństwa ekonomicznego państwa oraz wykorzystywane w systemie ochrony zdrowia i bezpieczeństwa publicznego.

Krytyczna Infrastruktura Teleinformatyczna (KITI) obejmująca systemy i sieci teleinformatyczne niezbędne dla prowadzenia podstawowych działań gospodarczych i funkcjonowania instytucji publicznych państwa[139].

[138] Definicja przedstawiona przez MSWiA. [URL – http://www.cert.pl.html] 06.05.2007 r. 21.26.
[139] Sienkiewicz P., Błażejczyk W., Lichocki E., Jóźwiak M., Świeboda H., *Analiza systemowa cyberterroryzmu*..., op.cit., s. 63.



* Krytyczna Infrastruktura Teleinformatyczna (KITI) czyli systemy i technologia teleinformatyczna oraz teleinformacyjna, łączność, ICT.

** Jeden z najważniejszych sektorów Infrastruktury Krytycznej Państwa. Jeżeli sektor ten będzie miał zakłócenia, to pozostałe sektory nie będą prawidłowo funkcjonować a w szczególności KITI. Trzeba zawsze pamiętać o zapasowych i alternatywnych źródłach zasilania (np. agregaty prądotwórcze).

Rysunek 3.5. Strefy współzależności sektorów Infrastruktury Krytycznej Państwa

Źródło: opracowanie własne.

Zabezpieczenie Infrastruktury Krytycznej wymaga wypracowania zasad i procedur, które zapewnią ciągłość świadczenia usług, niezawodność i stałą gotowość skutecznego reagowania, pozwalającą nabrać przekonania, że będzie ona mniej podatna na potencjalne zagrożenia. Oznacza to, że istnieje zdolność do ograniczania skutków ewentualnych zagrożeń, a także odtwarzania normalnego stanu działania systemu.

Można wyróżnić zasadnicze kategorie zagrożeń występujące w procesach Infrastruktury Krytycznej:

- fizyczne ataki na obiekty, które są składnikami tej infrastruktury;
- ataki z cyberprzestrzeni (cyberataki) ukierunkowanymi na informację, systemy teleinformatyczne oraz systemy zarządzania Infrastrukturą Krytyczną;
- zagrożenia związane z zarządzaniem bezpieczeństwem infrastruktury;
- zagrożenia związane z przyjętymi rozwiązaniami projektowymi infrastruktury i architekturą;
- zagrożenia związane z eksploatacją infrastruktury;
- zagrożenia związane z ilością i rodzajem transportowanego medium.

W Polsce do dnia dzisiejszego nie ma dokładnie zdefiniowanej Infrastruktury Krytycznej[140], której niezdolność do działania znacznie obniża sprawność obrony i bezpieczeństwo gospodarki Rzeczypospolitej Polski[141]. Nie mniej jednak przeprowadzono już pierwsze spotkania i rozmowy grup roboczych do spraw infrastruktury krytycznej, i tak:

- luty 2001 r. – pierwsze rozmowy CERT Polska i Biura Bezpieczeństwa Łączności i Informatyki UOP[142] dotyczące reagowania na incydenty bezpieczeństwa;
- listopad 2001 r. – Konferencja „SECURE 2001" – prezentacja działań NATO zmierzających do budowy NATO Computer Incident Response Capability (NCIRC);
- kwiecień 2002 r. – Dyskusja podczas Konferencji „Bezpieczna Infrastruktura – Koordynacja działań w skali kraju";
- wrzesień 2002 r. - w Pałacu Prezydenckim odbyło się seminarium na temat „Infrastruktura krytyczna w Polsce", zorganizowane przez Biuro Bezpieczeństwa Narodowego i Telekomunikację Polską S.A.;
- w lipcu i w październiku 2002 r. - odbyły się spotkania robocze w MSWiA poświęcone ochronie infrastruktury krytycznej;
- 2003 - 2006 r. – robocze spotkania przedstawicieli CERT Polska, DBTI ABW, KGP, „ABUSE Team" TP S.A.[143];

---

[140] Pierwsza próba została podjęta w Ustawie *O zarządzaniu kryzysowym* Dz. U. Nr 89 poz. 590 (Dz. U. 07.89.590) z dnia 21 maja 2007 r. Nie ma podziału wg. hierarchi: żywotne, krytyczne, wrażliwe i podstawowe. Pojęcie infrastruktury krytycznej przedstawiam w podrozdziale 2.4.1.

[141] Podczas pisania rozprawy, nie spotkałem się z żadną oficjalną definicją dotyczącą Infrastruktury Krytycznej w Polsce oprócz tej zawartej w Ustawie *O zarządzaniu kryzysowym* Dz. U. Nr 89 poz. 590 (Dz. U. 07.89.590) z dnia 21 maja 2007 r.

[142] Obecnie DBTI ABW.

[143] Kośla R., *Ochrona krytycznej infrastruktury teleinformatycznej w Polsce* – wstęp do dyskusji, Warszawa, 17 listopad 2004 r.

- 2004 – 2006 r. – robocze spotkania przedstawicieli CBT WSI[144] i DBTI ABW;
- kwiecień 2007 r. – międzyresortowe spotkanie poświęcone ochronie infrastruktury krytycznej. Mówiono o opracowaniu Krajowego Planu Ochrony Infrastruktury Krytycznej[145].

W dniu 17 lipca 2002 r. odbyło się spotkanie grupy roboczej, na którym zainicjowano prace nad założeniami metodologicznymi, procedurami tworzenia baz danych i reagowania w przypadkach wystąpienia zagrożeń. Opracowano i rozesłano do organów administracji państwowej „Kwestionariusz dotyczący ochrony infrastruktury krytycznej w Polsce". Dla potrzeb kwestionariusza przyjęto następującą definicję Infrastruktury Krytycznej:

Infrastruktura Krytyczna oznacza obiekty (budynki i budowle) i urządzenia, służby odpowiedzialne za obsługę tych obiektów i urządzeń, komputerowe systemy informatyczne istotne dla bezpieczeństwa i ekonomicznego dobrobytu państwa oraz jego efektywnego funkcjonowania obejmując: systemy energetyczne, telekomunikacyjne, finansowe i bankowe, zarządzania zasobami wodnymi, dostaw żywności i wody, opieki zdrowotnej, transportu, usługi w zakresie bezpieczeństwa powszechnego i porządku publicznego oraz zapewnienie prawidłowego funkcjonowania najważniejszych struktur administracji publicznej w sytuacjach nadzwyczajnych zagrożeń (w tym centra zarządzania kryzysowego i stanowiska kierowania) oraz ochrony przemysłu o strategicznym znaczeniu, w tym obronnego[146].

Przedstawiona powyżej definicja została oparta na zapisie zawartym w kwestionariuszu przygotowanym przez grupę studyjną Wysokiego Komitetu ds. Planowania Cywilnego w Sytuacjach Zagrożeń NATO i rozesłana do wszystkich krajów uczestniczących w pracach Euro – Atlantyckiej Rady Partnerstwa.

Podstawowym celem badań było przeprowadzenie szczegółowej diagnozy oraz zgromadzenie niezbędnych danych dotyczących infrastruktury krytycznej w Polsce.

Badania te stanowią jak na razie pierwszą i zarazem ostatnią znaną mi próbę spojrzenia na tą problematykę w Polsce. Złożona problematyka ochrony

---

[144] Obecnie SKW.
[145] Infrastruktura Krytyczna Państwa [URL – http://prawo.vagla.pl/node/7204html] 10.05.2007 r. 20.45.
[146] Ministerstwo Spraw Wewnętrznych Administracji. Departament Bezpieczeństwa Powszechnego. *Infrastruktura krytyczna w Polsce – Raport z badań*. Warszawa, wrzesień 2002 r. s. 2.

infrastruktury krytycznej wymusza natychmiast zmiany funkcjonujących niżej wymienionych poglądów dotyczących:

- bezpieczeństwa narodowego;
- ochrony obywateli;
- realizacji zadań obronnych w czasie pokoju;
- realizacji zadań obronnych w czasie zagrożeń.

Nakłada także, nowe zadania nie tylko na administrację państwową, ale również na podmiot sektora prywatnego, który jest tak istotny dla gospodarki narodowej i infrastruktury krytycznej państwa.

Wyniki raportu potwierdzają tezę, iż powszechnie przyjęte jest przekazywanie zadań, wynikających z konieczności budowy elastycznego systemu zarządzania kryzysowego, na podległe i nadzorowane urzędy centralne, służby i przedsiębiorstwa. Tam wiedza w tej dziedzinie jest największa. Trudności wynikają często z braku odpowiednich form koordynacji wykonywanych zadań z zakresu zarządzania kryzysowego i planowania cywilnego w ministerstwach oraz niedostatecznym przepływie informacji. Dotychczasowe, rozproszone wysiłki poszczególnych komórek organizacyjnych w resortach, muszą zostać skoordynowane, chociażby w celu uzyskania stosunkowo tanim kosztem efektu konsolidacji w zakresie ochrony Infrastruktury Krytycznej. Konieczne jest także zdecydowane przyspieszenie prac nad koncepcją utworzenia i utworzeniem Krajowego Systemu Ochrony Krytycznej Infrastruktury Teleinformatycznej (KSOKITI) oraz zagwarantowanie odpowiednich środków finansowych na ten cel[147].

Wyniki raportu ilustrują także brak zrozumienia dla idei partnerstwa publiczno – prywatnego w realizacji zadań związanych z polityką bezpieczeństwa państwa. Żaden z ankietowanych podmiotów[148] nie poruszył tego zagadnienia, tak jakby żaden z podmiotów prywatnych nie wchodził w obszar zainteresowania resortów pod kątem współpracy w zakresie ochrony i funkcjonowania Infrastruktury Krytycznej w Polsce. Tymczasem oczywistą rzeczą jest, iż najważniejsi partnerzy z sektora prywatnego, o istotnym znaczeniu dla gospodarki narodowej, powinni zostać włączeni w prace, dotyczące ochrony poszczególnych infrastruktur - sektorów infrastruktury krytycznej.

Raport obrazuje, że ministerstwa nie mają opracowanych kompleksowych planów ochrony odpowiednich segmentów Infrastruktury Krytycznej. Nie mają także

---

[147] Prace nad KSOKITI rozpoczęto w BBŁiI UOP (obecnie DBTI ABW) na początku 2001 r.

[148] W sumie poddano analizie 30 podmiotów, w tym: 9 ministerstw, 18 podmiotów podległych i nadzorowanych przez organy centralne (inspektoraty i urzędy) i 3 przedsiębiorstwa państwowe.

żadnych wytycznych w tym zakresie. Ministerstwa powinny przyjąć na siebie rolę inspiratora działań, zmierzających do opracowania szczególnych programów ochrony, a także do monitorowania stanu bezpieczeństwa we właściwych dla siebie sektorach Infrastruktury Krytycznej.

Brak kontroli monitorowania i funkcjonowania podmiotów odpowiedzialnych za bezpieczeństwo Infrastruktury Krytycznej naraża nasze państwo i gospodarkę narodową na duże straty oraz chaos organizacyjny w przypadku ewentualnych ataków lub zakłóceń w kluczowych sektorach infrastruktury, skutkujących tak zwanym „efektem kaskadowym".

Wyniki raportu nie wykazały istnienia koordynacji działań wewnątrz i między sektorowych w zakresie ochrony Infrastruktury Krytycznej w Polsce.

W ramach badań i sporządzonego raportu „zwycięzcą rankingu" na wytypowanie wrażliwych sektorów infrastruktury okazały się:

- energetyka;
- bezpieczeństwo powszechne;
- telekomunikacja[149].

Jest to prawidłowe spojrzenie na sytuacje, które w istocie oddaje poczucie nowych zagrożeń po 11 września 2001 r. Wydaje się, iż stale rośnie znaczenie bezpieczeństwa sektora teleinformatycznego i łączności. W rozwiązaniach przyjętych w USA, Kanadzie, Wielkiej Brytanii, Finlandii oraz Niemczech priorytet nadaje się „cyberprzestrzeni". Również w Polsce staje się to istotnym wyzwaniem, zwłaszcza po przyjęciu ustawy o podpisie elektronicznym i rozpoczęciu wdrażania w coraz większym zakresie technologii umożliwiających w niektórych segmentach „usług administracyjnych" bezpośrednie kontaktowanie się obywateli z organami administracji publicznej. Stąd problematyka bezpieczeństwa teleinformatycznego zasługuje na szczególną uwagę. Już teraz należy rozstrzygnąć wątpliwości dotyczące rozwiązań organizacyjnych służących jego ochronie. Na przykład:

- jaki będzie zakres działań instytucji MSWiA i służb ochrony państwa za opracowanie i wdrażanie sieci trunkingowych;
- kto opracuje i wdroży do użytku rządową cyfrową sieć łączności ochrony teleinformacyjnej wraz z teleinformatycznymi systemami wymiany informacji.

---

[149] Ministerstwo Spraw Wewnętrznych Administracji. Departament Bezpieczeństwa Powszechnego. *Infrastruktura krytyczna w Polsce* – Raport z badań. Warszawa, wrzesień 2002 r. s. 26.

Wartością przeprowadzonych po raz pierwszy w Polsce badań jest także uruchomienie procesu tworzenia metodologii z zakresu ochrony Infrastruktury Krytycznej. Musi on być obliczony w chwili obecnej na wiele lat.

Podjęcie w Polsce badań z zakresu Infrastruktury Krytycznej ma również walor edukacyjny. Przyczynia się do upowszechnienia tej „nieznanej" problematyki w całej administracji rządowej.

Systemy i technologia teleinformatyczna czyli Krytyczna Infrastruktura Teleinformatyczna (KITI) ma kluczowe znaczenie dla poszczególnych sektorów Infrastruktury Krytycznej Państwa. Wystarczy przez szybkie łącze „wpuścić" do Internetu szybko mnożącego się wirusa, który w ciągu kilku minut daje mu kontrole nad tysiącami, a może nawet milionami serwerów i komputerów osobistych na całym świecie. W pierwszej fazie, cyberatak wygląda na uciążliwy ale stosunkowo niegroźny. Wiążę się to z tym że, nie da się poprawnie oglądać stron WWW. Ostatecznie po pewnym czasie jednak problemy dotykają usług pośrednio związanych z Internetem, a mianowicie przestają działać bankomaty, telefony na numery alarmowe nie są przekierowywane do najbliższych „ komórek zarządzania kryzysowego"[150], przestają funkcjonować systemy rezerwacji biletów lotniczych i kolejowych. Po kilku godzinach następuje spowolnienie sieci, co odbija się na kluczowych sektorach infrastruktury krytycznej takich jak: energia, transport, zdrowie, systemy i technologia teleinformatyczna, bankowość i finanse oraz administracja państwowa. Dochodzi do chaosu i paraliżu, okazuje się że sprawne działanie systemów teleinformatycznych ma bezpośredni wpływ na funkcjonowanie Infrastruktury Krytycznej Państwa.

Celem ochrony Krytycznej Infrastruktury Teleinformatycznej w Polsce jest zapewnienie niezawodności i ciągłości działania systemów i sieci teleinformatycznych o szczególnie ważnym znaczeniu dla funkcjonowania i bezpieczeństwa państwa, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla struktur organizacyjnych państwa, obronności, życia lub zdrowia ludzi, dziedzictwa narodowego, środowiska naturalnego, a także spowodować poważne straty materialne w mieniu[151].

Dla celów ochrony Krytycznej Infrastruktury Teleinformatycznej powinno wykorzystywać się struktury organizacyjne tworzące „System Reagowania

---

[150] Komendy i posterunki policji, szpitale i stacje pogotowia ratunkowego oraz jednostki straży pożarnej a w przyszłości odpowiednich „komórek zarządzania kryzysowego".

[151] Projekt Ustawy *O ochronie Krytycznej Infrastruktury Teleinformatycznej*. Stan na dzień 15.04.2005 r.

na Incydenty Komputerowe". Zakres działania zarówno w sferze wojskowo – militarnej jak i typowo cywilnej obejmuje:

- obszar Polski;
- kontakty z NATO i krajami członkowskimi NATO;
- kontakty z Unią Europejską i krajami członkowskimi.

W obszarze cywilnym i wojskowym są tworzone struktury reagowania na incydenty komputerowe. W celu zapewnienia sprawnego współdziałania istniejących struktur na bazie Centrum Koordynacyjnego SKW i ABW musi być stworzone Krajowe Centrum Koordynacyjne Systemu Ochrony Krytycznej Infrastruktury Teleinformatycznej.

Krajowy System Ochrony Krytycznej Infrastruktury Teleinformatycznej muszą uzupełniać ponadto administratorzy systemów i sieci wchodzących w skład krytycznej infrastruktury teleinformatycznej oraz wykorzystywane przez nich systemy zarządzania wraz ze stosowanymi formami i metodami ich ochrony, a także właściwie zorganizowane współdziałanie pomiędzy nimi.

W celu zapewnienia poprawności i ciągłości działania ochrony Krytycznej Infrastruktury Teleinformatycznej państwa polskiego oraz wypracowania zasad i metod utrzymania i podnoszenia poziomu bezpieczeństwa teleinformatycznego państwa, jednostki organizacyjne muszą współdziałać w ramach Krajowego Systemu Ochrony Krytycznej Infrastruktury Teleinformatycznej.

Współdziałanie o którym mowa powyżej w szczególności musi obejmować:

- zgłaszanie przypadków wystąpienia incydentów naruszających bezpieczeństwo teleinformatyczne w systemach i sieciach teleinformatycznych do zespołów reagowania na incydenty komputerowe powołane w strukturach wojskowych i cywilnych;
- wczesne ostrzeganie o przewidywanych lub zaistniałych zagrożeniach dla Krytycznej Infrastruktury Teleinformatycznej, a także prewencję przeciw ich powstawaniu;
- identyfikację krytycznych elementów infrastruktury teleinformatycznej mających wpływ na funkcjonowanie systemów i sieci o szczególnie ważnym znaczeniu – Infrastrukturę Krytyczną Państwa;
- projektowanie i wdrażanie technologii informatycznych służących do zapobiegania powstawaniu incydentów oraz ich wykrywania i naprawiania szkód w infrastrukturze teleinformatycznej po wystąpieniu incydentów;

- współudział w opracowywaniu jednolitych metod klasyfikowania incydentów, rejestracji ich i reagowania w przypadku ich wystąpienia;
- współudział w opracowywaniu zaleceń dotyczących poprawy poziomu bezpieczeństwa teleinformatycznego mających wpływ na funkcjonowanie systemów i sieci o szczególnie ważnym znaczeniu dla bezpieczeństwa państwa.

Nadzór i koordynacja działań w zakresie ochrony Krytycznej Infrastruktury Teleinformatycznej powinna sprawować Służba Ochrony Państwa. Działania w zakresie ochrony krytycznej infrastruktury teleinformatycznej związanej z obronnością państwa i wykorzystywanej na potrzeby Sił Zbrojnych Rzeczypospolitej Polski należy do Szefa SKW, a w zakresie ochrony krytycznej infrastruktury teleinformatycznej nie związanej z obronnością państwa i nie wykorzystywanej na potrzeby Sił Zbrojnych Rzeczypospolitej Polski należy do Szefa ABW.

Do zadań Szefów Służb Ochrony Państwa w zakresie systemów ochrony Krytycznej Infrastruktury Teleinformatycznej w szczególności powinno należeć:

- koordynowanie współdziałania w ramach Krajowego Systemu Ochrony Krytycznej Infrastruktury Teleinformatycznej;
- prowadzenie wspólnego rejestru systemu i sieci Krytycznej Infrastruktury Teleinformatycznej;
- gromadzenie i przetwarzanie informacji w rejestrze oraz ich udostępnianie;
- zapewnienie bezpieczeństwa gromadzonych i przetwarzanych w rejestrze informacjom;
- gromadzenie, przetwarzanie, analizowanie informacji o naruszeniach i zagrożeniach dla krytycznej infrastruktury teleinformatycznej oraz ich udostępnianie jednostkom organizacyjnym;
- kontrola zgodności stosowanych metod i środków ochrony systemów i sieci teleinformatycznych wpisanych do rejestru;
- propagowanie wiedzy o metodach ochrony Krytycznej Infrastruktury Teleinformatycznej, w szczególności przez opracowanie zaleceń oraz prowadzenie szkoleń w zakresie ochrony systemów i sieci teleinformatycznych wchodzących w skład infrastruktury;
- inicjowanie i podejmowanie przedsięwzięć w zakresie ochrony Krytycznej Infrastruktury Teleinformatycznej;
- współpraca międzynarodowa w zakresie ochrony Krytycznej Infrastruktury Teleinformatycznej oraz reagowania na incydenty komputerowe.

Szefowie Służb Ochrony Państwa w relacjach międzynarodowych, muszą wreszcie pełnić odpowiednio funkcję – „krajowych władz ochrony krytycznej infrastruktury teleinformatycznej sfery cywilnej i wojskowej".

Na Krytyczną Infrastrukturę Teleinformatyczną państwa polskiego składają się systemy i sieci teleinformatyczne i teleinformacyjne o szczególnie ważnym znaczeniu dla bezpieczeństwa państwa lub zapewniające niezakłócone funkcjonowanie w państwie: transportu, łączności, zdrowia, bankowości i finansów, infrastruktury energetycznej, wodociągowej i gazowej oraz administracji państwowej, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa.

Ochrona Krytycznej Infrastruktury Teleinformatycznej ma na celu zapewnienie poprawności i ciągłości funkcjonowania systemów lub sieci teleinformatycznych wchodzących w skład tej infrastruktury oraz bezpieczeństwa przetwarzanym w tych systemach lub sieciach informacjom[152], w szczególności przez jej zabezpieczenie przed zniszczeniem, uszkodzeniem lub dostępem osób nieuprawnionych.

Nadzór i koordynację działań w zakresie ochrony Krajowego Systemu Krytycznej Infrastruktury Teleinformatycznej sprawować musi Służba Ochrony Państwa jako organ właściwy w sprawach ochrony bezpieczeństwa wewnętrznego i zewnętrznego państwa polskiego.

W Polsce systemy teleinformatyczne i ich bezpieczeństwo są regulowane wieloma aktami prawnymi, w tym przede wszystkim Ustawą z dnia 22 stycznia 1999 r. „O ochronie informacji niejawnych" wraz z późniejszymi zmianami oraz Ustawą z dnia 29 sierpnia 1997 r. „O ochronie danych osobowych" wraz z późniejszymi zmianami[153]. Główny problem jest w tym, że akty prawne, przepisy oraz rozporządzenia dotyczące bezpieczeństwa teleinformatycznego i ochrony informacji niejawnych, nie normalizują w sposób systematyczny żadnych standardów zabezpieczeń fizycznych czy elektromagnetycznych[154]. Prawie wszystkie urzędy państwowe opóźnia się w dostosowaniu do wymagań wyżej wymienionych ustaw. Polityka bezpieczeństwa nie jest znormalizowana jednolicie dla wszystkich urzędów

---

[152] Informacje stanowiące tajemnice służbową i państwową.

[153] Szerzej o aktach prawnych pisze w Rozdziale 3.4 oraz w Załączniku 3 niniejszej rozprawy doktorskiej.

[154] Służby Ochrony Państwa (ABW oraz SKW) upoważnione do wydawania stosownych dokumentów, prawdopodobnie nie konsultują między sobą dokumentów które normalizują ochronę informacji niejawnych – mamy różne standardy zabezpieczenia fizycznego i elektromagnetycznego dla tego samego poziomu bezpieczeństwa.

państwowych w Polsce, nie ma też spójnego systemu autoryzacji i identyfikacji użytkowników rządowych systemów teleinformatycznych.

W Polsce istnieje już wiele systemów teleinformatycznych, w których zakłócenie działalności mogło odbić się w negatywny sposób na funkcjonowanie państwa i bezpieczeństwo obywateli. Paradoksalnie, na dzień dzisiejszy pewne opóźnienia w informatyzacji kraju grają na naszą korzyść[155]. Bardzo dużo systemów teleinformatycznych jest dopiero w stadium projektu, budowy lub modernizacji[156], a to najwłaściwszy moment na zaprojektowanie skoordynowanego krajowego systemu bezpieczeństwa czyli Krajowego Systemu Ochrony Krytycznej Infrastruktury Teleinformatycznej (KSOKITI). Tego momentu nie można przeoczyć i zlekceważyć.

3.3. Infrastruktura krytyczna w Siłach Zbrojnych Rzeczypospolitej Polski

W Siłach Zbrojnych Rzeczypospolitej Polski do dnia dzisiejszego, nie ma zdefiniowanej infrastruktury krytycznej, której niezdolność do działania znacznie obniża sprawność funkcjonowania i obrony Sił Zbrojnych Rzeczypospolitej Polski[157].

Dla potrzeb rozprawy doktorskiej i po analizie kwestionariusza ankiety do niniejszej rozprawy doktorskiej przyjąłem następującą definicję Infrastruktury Krytycznej Sił Zbrojnych RP:

---

[155] Sienkiewicz P., Błażejczyk W., Lichocki E., Jóźwiak M., Świeboda H., *Analiza systemowa cyberterroryzmu*..., op.cit., s. 117.

[156] Przykłady odkładanej informatyzacji w administracji państwowej: podpis elektroniczny, elektroniczne rozliczanie podatków – e - Deklaracja, publikacja Monitora Polskiego, Pesel 2, e – PUAP, Centralny Rejestr Działalności Gospodarczej.

[157] Podczas pisania pracy, nie spotkałem się z żadnym opracowaniem dotyczącym Infrastruktury Krytycznej w Siłach Zbrojnych Rzeczypospolitej Polski.

Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski to fizyczne oraz wirtualne sektory i systemy (systemy teleinformatyczne i teleinformacyjne[158]) o zasadniczym znaczeniu dla minimalnego funkcjonowania Sił Zbrojnych. Niezdolność do działania Infrastruktury Krytycznej znacznie obniża sprawność działania i funkcjonowania Sił Zbrojnych.

Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski składa się z następujących infrastruktur - sektorów krytycznych:

- *energia;*
- *woda;*
- *transport;*
- *systemy i technologia teleinformatyczna oraz teleinformacyjna, łączność, ICT – Krytyczna Infrastruktura Teleinformatyczna Sił Zbrojnych RP;*
- *zdrowie*
- *żywność;*
- *administracja Sił Zbrojnych RP;*
- *istotny przemysł dla Sił Zbrojnych RP.*

Tabela 3.5. Lista sektorów infrastruktury krytycznej w Siłach Zbrojnych Rzeczypospolitej Polski.

Sektor	Składniki sektora
Energia	1. Ropa naftowa, paliwa płynne, gaz. 2. Urządzenia do przetwarzania i przechowywania ropy naftowej, paliw płynnych oraz gazu. 3. Elektrownie oraz zespoły prądotwórcze. 4. Energetyczne sieci transmisyjne i dystrybucyjne dostarczające elektryczność, ropę naftową, paliwa płynne oraz gaz do „użytkowników końcowych".
Woda	1. Zbiorniki wodne. 2. Systemy transportowania i dostarczania wody. 3. Urządzenia do filtrowania i uzdatniania wody oraz system kontroli jakości wody. 4. System odbioru wody zużytej wraz z oczyszczalniami ścieków. 5. System dostarczania wody do instalacji przeciwpożarowych.

[158] Określenie które występuje w dokumentach normatywnych MON dotyczących ochrony kryptograficznej.

Sektor	Składniki sektora
Transport	1. Transport lądowy. 2. Transport powietrzny. 3. Transport śródlądowy. 4. Transport morski. 5. System dystrybucji towarów szczególnie ważnych dla bezpieczeństwa i stabilności SZ RP wraz z infrastrukturą.
Systemy i technologia teleinformatyczna oraz teleinformacyjna, łączność, ICT ***Krytyczna Infrastruktura Teleinformatyczna Sił Zbrojnych RP***	1. Systemy dowodzenia i kierowania obronnością Sił Zbrojnych (Państwa). 2. Systemy kontroli i naprowadzania lotnictwa. 3. Satelitarne i radiowe systemy nawigacyjne. 4. Systemy łączności radiowej. 5. Systemy łączności cyfrowej. 6. Systemy łączności satelitarnej. 7. Zautomatyzowane systemy dowodzenia. 8. Systemy kierowania systemami walki. 9. Systemy rozpoznania. 10. Systemy teleinformatyczne, bazy danych, oprogramowanie. 11. Systemy opto – elektroniczne techniki bojowej. 12. Systemy powiadamiania (Broadcasting). 13. Stacjonarne i mobilne systemy telekomunikacyjne (sieci wymiany informacji).
Zdrowie	1. Szpitale. 2. Laboratoria i instytucje badawcze. 3. Służby ratunkowe. 4. Stacje przechowujące zapasy krwi.
Żywność	1. Produkcja żywności. 2. Magazynowanie i dystrybucja żywności.
Administracja Sił Zbrojnych RP	1. Ministerstwo Obrony Narodowej. 2. Dowództwa Rodzajów Sił Zbrojnych. 3. Centra Operacyjne. 4. Służba Ochrony Sił Zbrojnych RP[159]. 5. Poczta i spedycja.
Istotny przemysł dla Sił Zbrojnych RP	1. Przemysł zbrojeniowy.

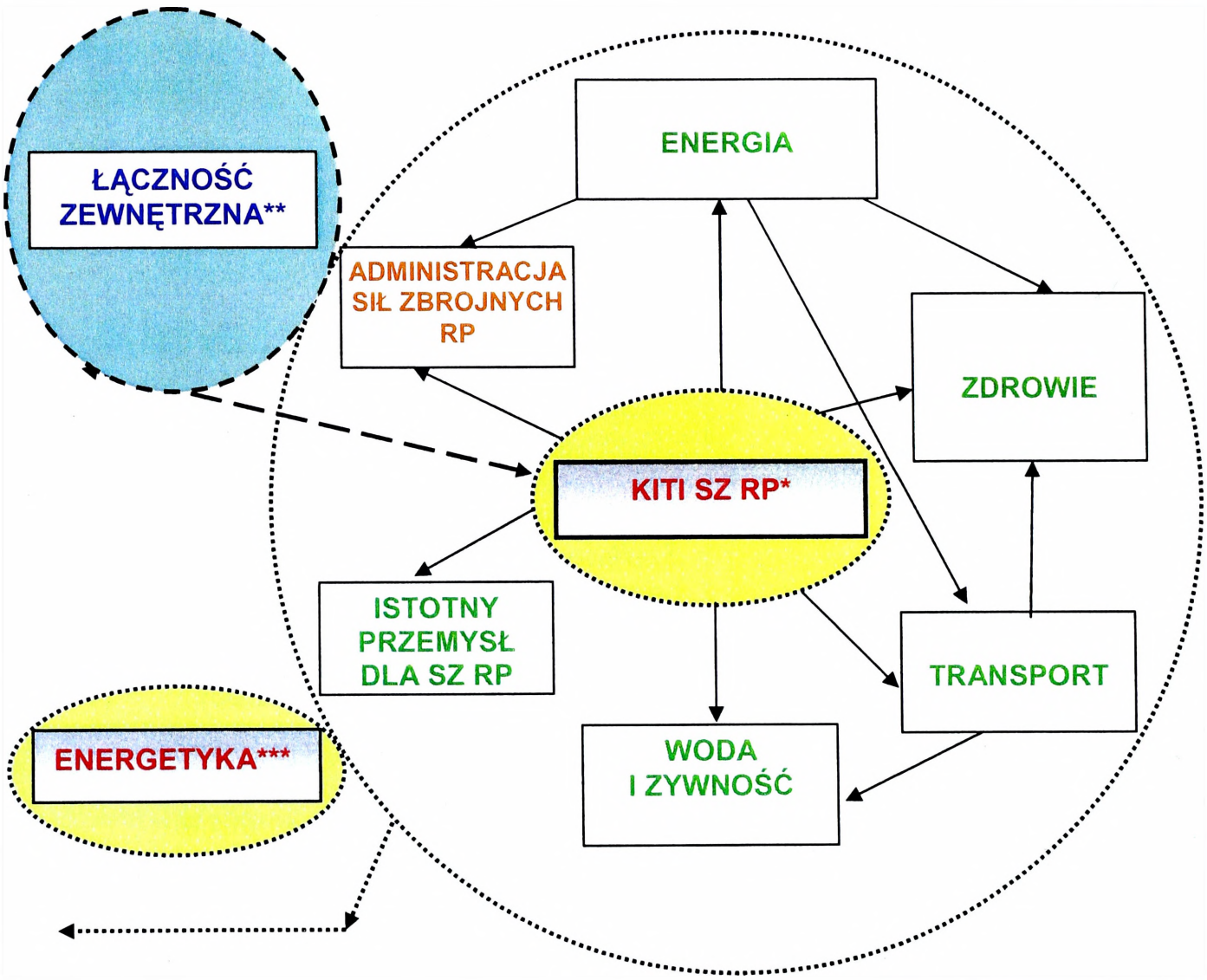
Źródło: Opracowanie własne na podstawie kwestionariusza ankiety (Załącznik 6).

Rozpatrując zagadnienie Infrastruktury Krytycznej w Siłach Zbrojnych Rzeczypospolitej Polski zachodzi potrzeba zdefiniowania dwóch pojęć odnoszących się do obiektów potencjalnego oddziaływania zewnętrznego (zasoby, obiekty) oraz elementów łączące te obiekty (infrastruktura teleinformatyczna). Generalnie możemy podzielić, że Krytyczna Infrastruktura Sił Zbrojnych RP to:

[159] Służba Kontrwywiadu Wojskowego i Służba Wywiadu Wojskowego.

- **krytyczne zasoby i obiekty:** (aktywa) teleinformatyczne definiowane jako zasoby wykorzystywane dla utrzymania bezpieczeństwa Sił Zbrojnych RP;
- **Krytyczna Infrastruktura Teleinformatyczna:** obejmująca systemy teleinformatyczne i teleinformacyjne niezbędne dla prowadzenia podstawowych działań i funkcjonowania Sił Zbrojnych RP.

Poniżej przedstawiam rysunek, który charakteryzuje strefy współzależności sektorów Infrastruktury Krytycznej Sił Zbrojnych RP (Rys. 3.6).



* **KITI SZ RP** – Krytyczna Infrastruktura Teleinformatyczna Sił Zbrojnych RP czyli systemy i technologia teleinformatyczna oraz teleinformacyjna, łączność, ICT.

** **ŁĄCZNOŚĆ ZEWNĘTRZNA** – czyli takie systemy jak: systemu dowodzenia i kierowania obronnością Sił Zbrojnych, systemy łączności radiowej, systemy łączności cyfrowej, systemy łączności satelitarnej, zautomatyzowane systemy dowodzenia, systemy teleinformatyczne i teleinformacyjne, systemy powiadamiania (Broadcasting).

*** **ENERGETYKA** – jeden z najważniejszych sektorów Infrastruktury krytycznej Sił Zbrojnych RP. Jeżeli sektor ten będzie miał zakłócenia, to pozostałe sektory nie będą prawidłowo funkcjonować a w szczególności KITI SZ RP. Trzeba zawsze pamiętać o zapasowych i alternatywnych źródłach zasilania (np. agregaty prądotwórcze).

Rysunek 3.6. Strefy współzależności sektorów Infrastruktury Krytycznej Sił Zbrojnych RP

Źródło: opracowanie własne na podstawie kwestionariusza ankiety (Załącznik 6).

Stałe i stabilne funkcjonowanie wszystkich wymienionych sektorów Infrastruktury Krytycznej Sił Zbrojnych RP jest uzależnione przede wszystkim od sektora energetycznego oraz od systemów i technologii teleinformatycznej i teleinformacyjnej, łączność, ICT czyli od Krytycznej Infrastruktury Teleinformacyjnej Sił Zbrojnych RP. Jednocześnie wiele z nich nie może prawidłowo funkcjonować w przypadku, gdy inne sektory mają postoje, znaczne uszkodzenia lub awarie.

Systemy teleinformatyczne i teleinformacyjne mają kluczowe znaczenie dla następujących sektorów Infrastruktury Krytycznej Sił Zbrojnych RP:

- energii;
- wody;
- transportu;
- zdrowie;
- żywność;
- administracja Sił Zbrojnych RP;
- istotny przemysł dla Sił Zbrojnych RP.

Z analizy wyników ankiety wynika, że najbardziej wrażliwymi sektorami Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski okazały się: energia, woda, żywność, transport oraz systemy i technologia teleinformatyczna, łączność, ICT. Jest to bardzo prawidłowy trend, który w pełni oddaje poczucie nowych zagrożeń asymetrycznych, które uwydatniły się po atakach na *World Trade Center* (WTC) 11 września 2001 r. Coraz większe znaczenie nabiera bezpieczeństwo systemów teleinformatycznych i teleinformacyjnych. W rozwiązaniach przyjętych w Stanach Zjednoczonych, Kanadzie, Wielkiej Brytanii, oraz innych krajach NATO, główny nacisk kładzie się na bezpieczeństwo w „cyberprzestrzeni". Również w Siłach Zbrojnych Rzeczypospolitej Polski stanie się to istotnym wyzwaniem. Coraz częściej technologia teleinformatyczna umożliwiać będzie bezpośrednie komunikowanie się i przesyłanie danych służbowych jawnych i niejawnych. Stąd problematyka bezpieczeństwa teleinformatycznego zasługuje na szczególną uwagę w dalszych pracach badawczych.

Jednostki organizacyjne podległe Ministrowi Obrony Narodowej zawężają obecnie pojęcie Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski do posiadanych przez siebie zasobów (systemy i technologia teleinformatyczna, łączność, ICT oraz zdrowie i żywność). Jednocześnie, najczęściej podawały one: energię, wodę, żywność, transport oraz systemy i technologia teleinformatyczna, łączność, ICT jako najbardziej istotne sektory Infrastruktury Krytycznej Sił Zbrojnych

Rzeczypospolitej Polski. Prawdopodobnie jest to spowodowane faktem, że jednostki organizacyjne wskazują swoje priorytety w obszarze infrastruktury zapewnieniem bezpieczeństwa w zakresie własnego sektora infrastruktury. Potwierdza to też tezę, że jednostki organizacyjne podległe Ministrowi Obrony Narodowej rozpatrują i postrzegają bardzo wyraźnie Infrastrukturę Krytyczną Sił Zbrojnych Rzeczypospolitej Polski w sposób wyrywkowy i wręcz fragmentaryczny. Koncentrują one, swoje działania przede wszystkim na swoich podstawowych zadaniach, nie traktując infrastruktury jako jednego z podstawowych elementów bezpieczeństwa państwa.

Jednostki organizacyjne w sposób bardzo wyraźny koncentrują tylko swoje działania na zapewnieniu niezakłóconego i sprawnego funkcjonowania dowództw jednostek i samej jednostki organizacyjnej, pomijając inne bardzo ważne aspekty Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski pozostające w ich zakresie kompetencji.

Trzeba jasno powiedzieć że, problematyka związana z ochroną Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski zmusza w sposób znaczący do przewartościowania obecnie funkcjonujących standardów i stereotypów, dotyczących bezpieczeństwa Sił Zbrojnych, bezpieczeństwa państwa, realizacji zadań obronnych w czasie pokoju, stanów zagrożeń i wojny. Jedną z najważniejszych wad, wynikających obecnie z przyjętych zasad obowiązujących w Siłach Zbrojnych RP, jest utożsamianie wszystkich sektorów Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski z jednym tylko elementem – funkcjonowaniem Sił Zbrojnych w czasie stanów zagrożeń i wojny.

W Polsce jest brak zorganizowanej polityk bezpieczeństwa dla podmiotów odpowiedzialnych za bezpieczeństwo Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Naraża to Siły Zbrojne na bardzo duże straty oraz chaos organizacyjny w przypadku ewentualnych ataków lub zakłóceń w kluczowych węzłach sektorów infrastruktury (efekt kaskadowy) takich jak energia czy systemy i technologia teleinformatyczna oraz teleinformacyjna, łączność, ICT. Następnym niepokojącym faktem jest, brak istnienia koordynacji działań oraz współpracy między sektorami w zakresie ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.

W wyniku wyżej wymienionych problemów związanych z Infrastrukturą Krytyczną Sił Zbrojnych Rzeczypospolitej Polski należy w trybie natychmiastowym:

- utworzyć grupy eksperckie i baz danych ekspertów z zakresu poszczególnych sektorów Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.
- uruchomić prace nad szczegółowymi planami operacyjnymi w zakresie ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.
- określić w ramach Sił Zbrojnych RP priorytety działań. Propozycja podziału na takie jak:
  - ochronę bezpieczeństwa teleinformatycznego (cyberprzestrzeń) z rozróżnieniem konstruowania zabezpieczeń systemowych oraz bezpośrednim reagowaniem na „incydenty";
  - ochronę fizyczna, techniczna i osobowa infrastruktury krytycznej;
  - bezpieczeństwo funkcjonowania jednostek centralnych podległych Ministrowi Obrony Narodowej;
  - bezpieczeństwo funkcjonowania jednostek organizacyjnych podległych Ministrowi Obrony Narodowej.
- opracować program szkoleń dla jednostek centralnych i organizacyjnych podległych Ministrowi Obrony Narodowej w zakresie ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.
- zainicjować szeroko idące naukowe programy badawcze z zakresu ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.
- zbierać i udostępniać informacje o zagrożeniach i środkach ochrony.
- systematyczne gromadzić i analizować dane na temat przestępstw teleinformatycznych, włączając w to zarówno odpowiednio zmodyfikowane statystyki przestępczości, jak i również informację o sposobach działania sprawców przestępstw, dotyczące w szczególności aspektów technicznych[160].

3.4. Istota operacji informacyjnych Sił Zbrojnych Rzeczypospolitej Polski

Potrzeba opracowania „Doktryny Operacji Informacyjnych SZ RP" – dokumentu normatywnego w zakresie Operacji Informacyjnych wynikła z konieczności współdziałania naszych sił zbrojnych w ramach przyszłych działań

[160] Szerzej postulaty systemowe związane z ochroną Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski zostały zawarte w Załączniku 6 s. 33.

połączonych, a także z wypełnieniem obowiązków koalicjanta oraz potrzebą interoperacyjności w zakresie organizacji i planowania Operacji Informacyjnych[161][162].

Opracowanie dokumentu jest wynikiem prac zespołu autorskiego (Zgodnie z Programem prac normalizacyjnych MON na 2003 r., zatwierdzonym przez Sekretarza Stanu I zastępcę Ministra Obrony Narodowej), który dokonał analizy piętnastu dokumentów normatywnych narodowych i sojuszniczych[163].

Celem pracy analityczno badawczej było:

- identyfikacja stanu aktualnego polskiej teorii i praktyki w dziedzinie Operacji Informacyjnych oraz stwierdzenie stopnia jego wystarczalności i adekwatności w aspekcie członkostwa w NATO;
- określenie stopnia zgodności i niezgodności postanowień doktrynalnych Sojuszu w obszarze Operacji Informacyjnych z istniejącym w Siłach Zbrojnych Rzeczypospolitej Polski stanem prawnym w tym zakresie;
- ustalenie potrzeby opracowania narodowej doktryny Operacji Informacyjnych.

Po analizie dokumentów, autorzy opracowania przedstawili wnioski, które zamieszczone są w Rozdziale 6. Wnioski te, stanowią podstawę do opracowania projektu dokumentu narodowego, którego projekt przedstawiono w Rozdziale 7.

Jak przedstawiono w Doktrynie, prowadzenie Operacji Informacyjnych i uzyskanie dominacji informatycznej staje się warunkiem wstępnym do podejmowania jakichkolwiek innych działań przez Siły Zbrojne Rzeczypospolitej

---

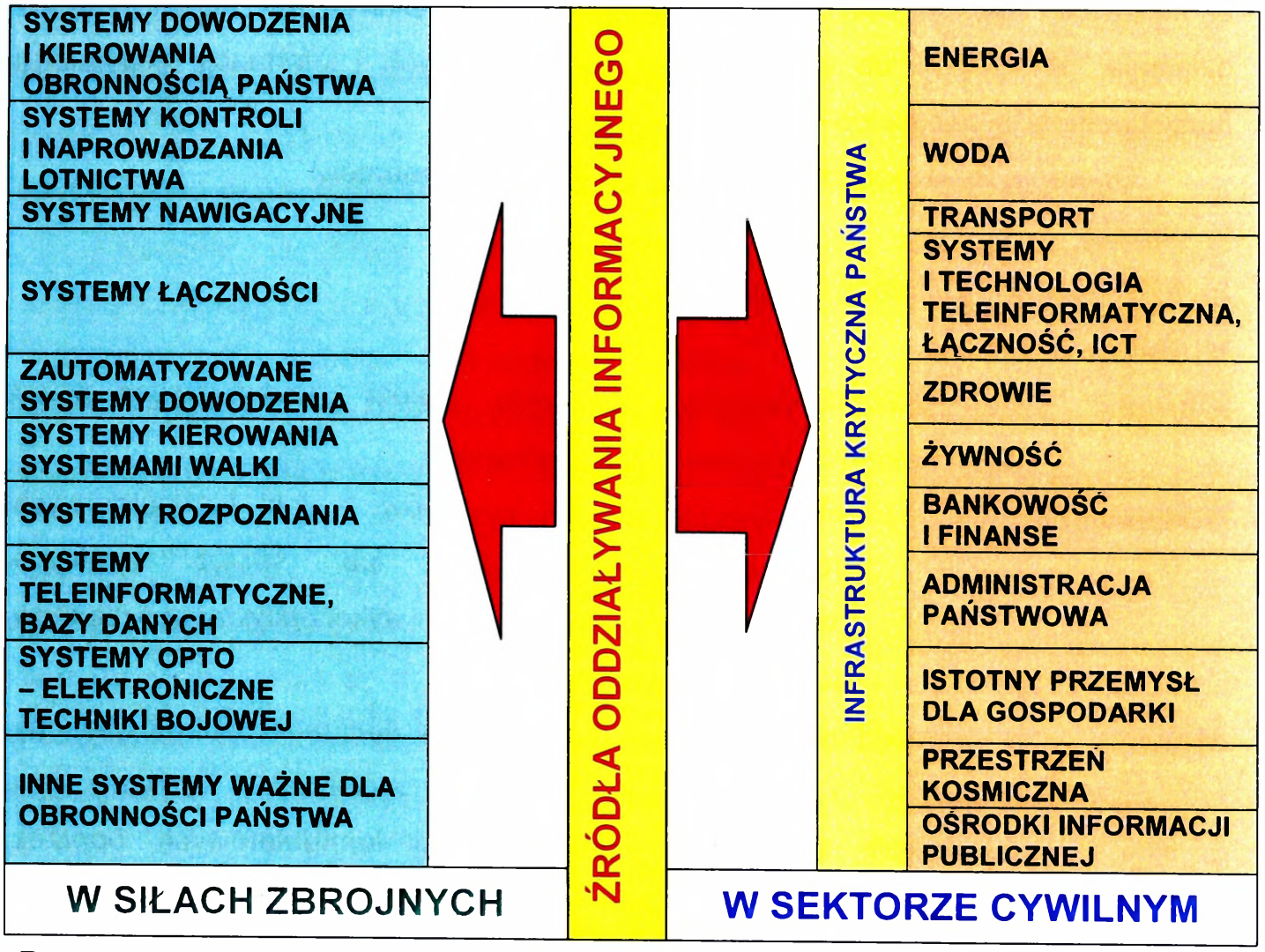
[161] *Doktryna Operacji Informacyjnych SZ RP*, Praca analityczno – badawcza – AB (temat nr 02 – 095), MON, Warszawa, 2003 r., s. 76.

[162] **Operacja Informacyjna** – działania podejmowane w celu uzyskania wpływu na proces podejmowania decyzji, informacje i systemy informacyjne przeciwnika, chroniąc jednocześnie własne informacje i systemy informacyjne – Źródło: *Doktryna operacji informacyjnych SZ RP*, Praca analityczno – badawcza – AB (temat nr 02 – 095), MON, Warszawa, 2003 r.
Operacja Informacyjna - to przedsięwzięcia mające wpływ na podejmowanie decyzji politycznych i wojskowych poprzez oddziaływanie na informację, podstawowe procesy informacyjne oraz systemy dowodzenia, kierowania, łączności i informatyki przeciwnika, a także chroniące własne informacje, procesy i systemy informacyjne – Źródło: *Doktryna Narodowa Operacji Połączonych OP/01*, MON Sztab Generalny WP, Warszawa, 2002 r.

[163] Są to następujące dokumenty normatywne sojusznicze i narodowe:
Normatywne dokumenty sojusznicze:
MC – 64 Walka elektroniczna; MC – 348 Polityka NATO w zakresie walki przeciw systemom dowodzenia i kierowania przeciwnika (C2W); MC - 400/2 Wytyczne Komitetu Wojskowego NATO w sprawie implementacji Koncepcji Strategicznej sojuszu w części wojskowej; MC – 422/1 Polityka NATO w zakresie Operacji Informacyjnych; MC – 457 polityka NATO w zakresie Informowania Publicznego; AJP – 01(B) Połączona Doktryna Sojuszu; AJP – 3.10 Doktryna Operacji Informacyjnych w Operacjach Połączonych – projekt; AJP – 3 operacje Połączone Sojuszu (STANAG – 2490 ED.1).
Normatywne dokumenty narodowe:
Doktryna Narodowa – Operacje Połączone OP/01; Walka Elektroniczna. Szt. Gen. 1549/2003; Operacje Psychologiczne. Szt. Gen. 1544/2003; Ustawa „O dostępie do informacji publicznej" z dnia 06 września 2001 r.; Ustawa „Prawo prasowe" z dnia 26 stycznia 1984 r.; Zarządzenie Nr 5/MON Ministra Obrony Narodowej z dnia 20 lutego 2002 r. „W sprawie regulaminu organizacyjnego Ministerstwa Obrony Narodowej"; Instrukcja o maskowaniu wojsk cz. II Zasady maskowania operacyjnego. Szt. Gen. 785/76.

Polskiej. Znaczenie informacji we współcześnie prowadzonych operacjach militarnych ma bardzo duże znaczenie. Osiągnięcie dominacji informacyjnej poprzez stosowanie nowoczesnych technologii, manipulację mediami i sterowanie informacjami pozwala na postrzeganie rzeczywistości w „pożądanym wymiarze".

W dokumencie przedstawiono po raz pierwszy potencjalne cele Operacji Informacyjnych (Rys. 3.7).



Rysunek 3.7. Potencjalne cele Operacji Informacyjnych.
Źródło: opracowanie własne.

Warto również zauważyć, że po raz pierwszy w Doktrynie – dokumencie normatywnym Sił Zbrojnych Rzeczypospolitej Polski pojawiło się pojęcie - definicja, charakteryzująca Operacje Cybernetyczne, które są składowymi zasadniczymi obszaru Operacji Informacyjnych[164].

---

[164] Wyróżniamy następujące obszary Operacji Informacyjnych:
Obszary zasadnicze: maskowanie, niszczenie fizyczne, walka elektroniczna, operacje psychologiczne, mylenie, operacje cybernetyczne.
Obszary związane: współpraca cywilno – wojskowa, informowanie opinii publicznej – bezpieczeństwo operacji.

„Operacje Cybernetyczne obejmują obronę (ochronę) własnych systemów i sieci przed penetracją, przed niepowołanym wykorzystaniem i destrukcją. Powinny być traktowane przede wszystkim jako działania obronne. Zdolności ofensywne mogą być wymagane dla nabywania wiedzy w zakresie przedsięwzięć obronnych lub akcji odwetowych przeciwko Operacjom Cybernetycznym przeciwnika. Może to również obejmować penetracje oprogramowania i sprzętu informatycznego (software or hardware) wrogich sieci komputerowych celem ich zniszczenia, uniemożliwienia działania, manipulacji lub uzyskania dostępu do danych i informacji, manipulacji funkcjonalnością całości lub części systemu.

Operacje Cybernetyczne składają się z trzech elementów:

- obrony;
- wykorzystania systemów przeciwnika;
- ataku.

Obrona – zabezpieczenie własnych systemów i sieci komputerowych przed nieuprawnionym dostępem lub włamaniom.

Wykorzystywanie - włamywanie się do systemów i sieci komputerowych poprzez oprogramowanie lub sprzęt (*software or hardware*) w celu dostępu i wykorzystywania systemów do celów wywiadowczych.

Atak - w zależności od narodowych uwarunkowań, atak może być prowadzony w oparciu o indywidualne narodowe możliwości. Atakiem jest włamywanie się do systemów i sieci komputerowych poprzez oprogramowanie lub sprzęt (*software or hardware*) w celu ich niszczenia, uniemożliwienia działania, modyfikacji lub manipulacji danymi, informacją lub funkcjonalnością systemu lub sieci w całości lub części. Atak obejmuje również fizyczne niszczenie komponentów powodowane przez manipulację lub modyfikację oprogramowania[165].”

W opracowaniu zauważono również że, Operacje Cybernetyczne mogą wnosić istotny wkład w osiąganie wszystkich celi Operacji Informacyjnych. Przeprowadzenie „ataku” jest trudne do osiągnięcia i będzie wymagało pomocy ze strony „wyspecjalizowanych komórek” Służb Ochrony Państwa.

---

[165] *Doktryna Operacji Informacyjnych SZ RP…*, op. cit., s. 54 – 55.

Uważa się, że prowadzenie Operacji Informacyjnych powinno być przygotowane i koordynowane na wszystkich poziomach kierowania i dowodzenia. Celowym jest również stworzenie odpowiedniej korelacji pomiędzy obszarami będącymi składowymi Operacji Informacyjnych w kontekście państwa i sił zbrojnych. Nieodzowne staje się stworzenie wzajemnie skoordynowanego krajowego systemu cywilno – wojskowego z udziałem administracji rządowej, mediów oraz służby ochrony państwa, jednostek do walki elektronicznej i operacji specjalnych – celem przygotowania tych elementów do prowadzenia wspólnych Operacji Informacyjnych.

W zakresie Informowania Opinii Publicznej, ogromne możliwości drzemią w wykorzystaniu Internetu. Jest to narzędzie, które w sposób efektywny i skuteczny kształtuje opinię publiczną[166][167].

Obecnie w Siłach Zbrojnych Rzeczypospolitej Polski w większości zautomatyzowanych systemach dowodzenia (ZSyD), zautomatyzowanych systemach dowodzenia i kierowania walką (ZSyDiKW) oraz systemach informatycznych i łączności działanie oparte jest ich na wykorzystywaniu łączy internetowych i ethernetowych[168], stwarza to dodatkową groźbę ingerencji osób

---

[166] Doktryna operacji informacyjnych SZ RP, Praca analityczno – badawcza – AB (temat nr 02 – 095), MON, Warszawa, 2003 r., s. 76.

[167] Rolę Operacji Informacyjnych oraz potrzebę wdrożenia „Doktryny Operacji Informacyjnych SZ RP" zauważył również Dowódca V Zmiany PKW w Iraku gen. dyw. Piotr Czerwiński. W artykule zamieszczonym w miesięczniku „Raport" 05/2006 stwierdził:
„W obecnych strukturach sztabów nie posiadamy żadnych komórek do spraw działalności informacyjnej. Na wzór armii innych państw NATO należałoby utworzyć etatowe komórki działań informacyjnych (od szczebla ZT). [.....] Kolejnym problemem jest brak oficjalnych (narodowych) dokumentów dotyczących działalności informacyjnych (INFO OPS). Należałoby stworzyć zespół do spraw opracowania narodowego (zgodnie z wymogami NATO) dokumentu normatywnego dotyczącego działań informacyjnych."

[168] W Siłach Zbrojnych Rzeczypospolitej Polski są wykorzystywane następujące zautomatyzowane systemy dowodzenia, zautomatyzowane systemy dowodzenia i kierowania walką oraz systemy informatyczne i łączności:
- ZSyD SZRP KOLORADO;
- ZSyD COP DUNAJ;
- ZSyD COM: ŁEBA - 2, PŁATKONOG – ŁEBA – 3;
- ZSyD SZAFRAN;
- system zintegrowanego węzła teleinformatycznego KTSAwp JAŚMIN;
- system rozpoznania SŁUŻBA;
- SKSW: ŁOWCZA - 3, REGA, TOPAZ, AZALIA, PODBIAŁ, PSTROKOSZ, PRZELOT;
- system LINK – 11 oraz LINK – 16;
- morski system dowodzenia MCCIS;
- sieć wymiany informacji MON: MIL – WAN oraz SEC – WAN;
- sieć wymiany informacji NATO: NOAN;
- bazy systemu C4ISR;
- wojskowy system łączności satelitarnej WSŁS;
- szerokopasmowy system łączności Wojsk Lądowych KROKUS 2000;
- system łączności Cygnus Tytanium Plus;
- systemy łączności cyfrowej: PCŁU SZRP STORCZYK oraz PNCŁU TCE 500B.

Ogółem na 195 (inne źródła resortowe podają 225 lub 239) systemów teleinformatycznych funkcjonujących w resorcie obrony narodowej 46 to zautomatyzowane systemy dowodzenia

nieuprawnionych do obsługi i korzystania z owych systemów. Dlatego też wykorzystanie łączy teleinformatycznych wiązać się będzie z koniecznością zastosowania odpowiedniej ochrony teleinformatycznej i teleinformacyjnej oraz stosownej w danej sytuacji ochrony fizycznej.

3.5. Prawne regulacje polityki bezpieczeństwa informacyjnego Polski

Prace nad nową Strategią Bezpieczeństwa Narodowego Rzeczypospolitej Polski zaczęto na początku 2007 r. na skutek konstatacji, iż dotychczasowa Strategia z 8 września 2003 r. straciła aktualność. Jest ona wyrazem nowego podejścia do sprawy bezpieczeństwa narodowego. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polski określa interesy narodowe i formułuje cele strategiczne w zgodzie z aktem rangi najwyższej, jakim jest Konstytucja RP[169].

W dniu 13 listopada 2007 r. Prezydent Rzeczypospolitej Polski zatwierdził, na wniosek Prezesa Rady Ministrów Strategię Bezpieczeństwa Narodowego Rzeczypospolitej Polski. Dokument ten został wydany w oparciu o Art. 4a ust. 1 pkt. 1 Ustawy z dnia 21 listopada 1967 r. „O powszechnym obowiązku obrony Rzeczypospolitej Polski".

Dokument ten jest więc dokumentem politycznym, wyrażającym uzgodnione poglądy naczelnych organów państwa odpowiedzialnych za bezpieczeństwo kraju. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, skorelowana ze strategiami sojuszniczymi – Koncepcją Strategiczną NATO i Europejską Strategią Bezpieczeństwa, stanowi podstawę do opracowania wykonawczych dyrektyw strategicznych, a w szczególności Polityczno – Strategicznej Dyrektywy Obronnej RP, strategii poszczególnych dziedzin bezpieczeństwa narodowego[170], strategicznych planów reagowania obronnego i zarządzania kryzysowego oraz wieloletnich programów transformacji systemu bezpieczeństwa państwa, w tym

---

oraz kierowania systemami walki, 36 systemów dla logistyki, 22 dla finansów oraz 15 dla kadr. Pozostałe 76 to programy typowo niszowe na przykład do obsługi bibliotek czy techniki wojskowej w parkach wozów. Stan na dzień 28.12.2007 r.

[169] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa, 2007 r. s., 3.

[170] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polski stanowi podstawę i punkt wyjścia do opracowania poszczególnych strategii sektorowych państwa (sektorów Infrastruktury Krytycznej Państwa) w dziedzinach mających podstawowe znaczenie dla bezpieczeństwa.

programów pozamilitarnych przygotowań obronnych i programów rozwoju Sił Zbrojnych Rzeczypospolitej Polski.

Polityka bezpieczeństwa narodowego wolnej i demokratycznej Polski cechuje niezmienność celów i zasad. Zapewniła wyjątkowy w naszej historii poziom bezpieczeństwa oparty między innymi na gwarancjach Sojuszu Północnoatlantyckiego. Wyrazem ciągłości dążeń państwa w tym względzie były Strategie Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej przyjęte w 1992 r., 2000 r. oraz 2003 r.[171].

Najpoważniejsze niebezpieczeństwo wśród nowych zagrożeń dla systemu międzynarodowego i bezpieczeństwa poszczególnych państw, w tym Polski, stwarza zorganizowany terroryzm międzynarodowy, aczkolwiek stopień zagrożenia terroryzmem dla poszczególnych państw jest różny. Jego działania wymierzone są między innymi w wartości, instytucje i interesy państw strefy euroatlantyckiej. Działania te przygotowuje się z użyciem nowoczesnych technik komunikacyjnych, wykorzystując łatwość przemieszczania się i prowadzenia operacji finansowych. Mają one bezwzględny charakter i obliczone są na maksimum destrukcji.

Innym zagrożeniem może być działanie w cyberprzestrzeni, skierowane w systemy teleinformatyczne i teleinformacyjne Infrastruktury Krytycznej Państwa. Skutkiem takich działań mogą być zarówno straty materialne, jak i sparaliżowanie istotnych sfer życia publicznego. Wzrasta potencjalne zagrożenie, że obce służby specjalne, a także ugrupowania terrorystyczne, ekstremistyczne oraz zorganizowane grupy przestępcze mogą podejmować próby uzyskania nieuprawnionego dostępu do informacji niejawnych, w tym wymienionych w ramach współpracy sojuszniczej. Coraz bardziej realne stają się dla Polski zagrożenia w sferze teleinformatycznej. Rośnie zagrożenie operacjami mającymi na celu dezorganizację kluczowych systemów informacyjnych instytucji rządowych oraz niektórych sfer sektora prywatnego, oddziałujących na system bezpieczeństwa państwa, a także operacjami związanymi z penetracją baz danych i prowadzenia działań dezinformacyjnych.

Nowe wyzwania dyktują potrzebę utworzenia państwowego kompleksowego systemu zarządzania i reagowania kryzysowego, odpowiadającego na współczesne zagrożenia bezpieczeństwa zarówno międzynarodowego, jak i wewnętrznego. Odpowiednie instytucje państwowe będą prowadzić działania zmierzające

---

[171] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* [URL – http://iniejawna.pl/przepisy/różne/strategia_bnrp.html] 24.01.2005 r. oraz *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa, 2007 r.

do powołania zintegrowanego systemu zarządzania i reagowania na wypadek kryzysu. Niezbędne staje się spójne uregulowanie zadań i kompetencji organów i instytucji państwowych, a także organizacji społecznych działających na rzecz bezpieczeństwa państwa.

Zintensyfikowania wymaga również budowa systemu łączności specjalnej (utajnionej) niezbędnej dla skutecznego funkcjonowania systemu zarządzania i reagowania kryzysowego. Należy kontynuować rozwój nowoczesnej, zintegrowanej struktury łączności elektronicznej (teleinformatycznej), która byłaby odporna na awarie i potencjalne ataki przestępczości cybernetycznej. Będzie to wymagać należytego współdziałania właściwych resortów i agent, a także podmiotów prywatnych[172].

Wejście do Unii Europejskiej[173] wzmocni to nasze zdolności do wykonywania zadań bezpieczeństwa wewnętrznego, związanych zwłaszcza z mechanizmami współpracy w sprawach wewnętrznych i sądownictwa, walki z przestępczością zorganizowaną, terroryzmem, narkobiznesem i innymi zagrożeniami nowego typu[174].

Ochrona infrastruktury teleinformatycznej i zwalczanie zagrożeń dla rządowych systemów teleinformatycznych należy to kompetencji wyspecjalizowanych komórek cywilnych[175] i wojskowych służb państwowych[176]. Ich zadaniem jest zwalczanie przestępczości komputerowej wymierzonej w rządową i samorządową infrastrukturę telekomunikacyjną, w tym przeciwdziałanie atakom na jej elementy.

Do zapewnienia należytej ochrony tej infrastruktury niezbędny jest rozwój i utrzymanie zdolności do zapobiegania wszelkim zakłóceniom, jakie mogą wystąpić w tej sferze, a także zdolności do koordynacji procesów dochodzeniowych w ramach instytucji posiadających elementy rządowej infrastruktury teleinformatycznej. Wyznaczone służby będą podejmować odpowiednie działania samodzielnie lub wspólnie z analogicznymi strukturami w innych państwach, zwłaszcza krajach członkowskich NATO i UE, a także producentami i dostawcami urządzeń oraz oprogramowania informatycznego, krajowymi operatorami telekomunikacyjnymi i dostawcami usług internetowych, ośrodkami badawczymi i szkoleniowymi. Aby podejmowane działania w tej dziedzinie były skuteczne, należy w sposób

---

[172] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa, 2007 r. s., 19.
[173] Polska wstąpiła do Unii Europejskiej 01 czerwca 2004 r.
[174] Zagrożeniem nowego typu jest także szeroko rozumiany cyberterroryzm.
[175] Agencja Bezpieczeństwa Wewnętrznego i Agencja Wywiadu (ABW i AW).
[176] Służba Wywiadu Wojskowego i Służba Kontrwywiadu Wojskowego (SWW i SKW).

priorytetowy podejść do rozwoju i wdrażania rodzimej kryptografii[177] oraz dostosować przepisy prawa telekomunikacyjnego, które wraz z szybkim postępem technologiczny mogą się okazać niewystarczające do zapewnienia bezpieczeństwa chronionej infrastrukturze teleinformacyjnej[178].

Polska powinna w pełnym możliwym wymiarze uczestniczyć w pracach NATO nad przeciwdziałaniem próbom destrukcji Krytycznej Infrastruktury Teleinformatycznej.

Podjęte zostaną wysiłki wymagające współdziałania odpowiednich resortów i agend na rzecz rozwoju nowoczesnej łączności, w tym sprawnej i bezpiecznej strategicznej infrastruktury teleinformatycznej oraz zapewnienie warunków budowy społeczeństwa informacyjnego.

Państwo polskie powinno jak najszybciej zbudować własny system łączności satelitarnej, wykorzystując w tym celu przyznane geostacjonarne pozycje orbitalne[179].

3.6. Przestępstwa cybernetyczne w prawie polskim

W ściganiu przestępczości cybernetycznej przeszkadza nie tylko ciągły postęp technologiczny. Utrudnia i to w sposób bardzo duży również nieprecyzyjne prawo, które cyberprzestępcy na dzień dzisiejszy z łatwością omijają. Ataki crakerów na serwery instytucji związanych z infrastrukturą krytyczną państwa, czy też włamania do komputerów osobistych to nie jedyny problem, z którym coraz trudniej radzą sobie organy ścigania oraz służba ochrony państwa.

Polska pod względem liczby zakazów karnych konstytuujących przestępstwa komputerowe w ustawodawstwie wewnętrznym, zajmuje w porównaniach międzynarodowych stosunkowo wysoką lokatę i zaliczana jest do grupy państw, które w znacznym stopniu dostosowały swój system prawny do standardów normatywnych w tej dziedzinie[180].

---

[177] Bezpieczeństwo teleinformacyjne.

[178] Najważniejsze regulacje prawne które normalizują politykę bezpieczeństwa informacyjnego Polski, zostały zamieszczone w Załączniku 3 niniejszej rozprawy doktorskiej. Przedstawione w nim **„wytłuszczonym"** drukiem, dokumenty i regulacje prawne, mają zasadniczy wpływ dla bezpieczeństwa informacyjnego systemów teleinformatycznych wykorzystywanych w Siłach Zbrojnych Rzeczypospolitej Polski.

[179] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa, 2007 r. s., 21.

[180] [URL – http://mcconnellinternational.com.html].12.12.2000 r. 12.30.

W znowelizowanym kodeksie karnym, są zapisy umożliwiające ściganie najbardziej klasycznych zamachów na bezpieczeństwo elektroniczne przetwarzanej informacji a także innych przestępstw komputerowych. Poświęcono w nim kilka artykułów dotyczących przestępstwom komputerowym.

W pierwszej kolejności omawia się przypadek odpowiedzialności karnej sprawcy ataku typu DOS (*denial of service attaca).* Przez atak DOS rozumie się różnego typu ataki na systemy komputerowe, mające na celu utrudnienie lub uniemożliwienie funkcjonowania danego urządzenia albo części sieci teleinformatycznej. Działania tego typu stanowią naruszenie jednego z katalogu praw człowieka – prawa do komunikowania się[181]. Działania takie uznaje się przy tym za sprzeczne z art. 49 Konstytucji Rzeczypospolitej Polski, w którym „zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony"[182].

W rozdziale XXXIII kodeksu karnego[183] zatytułowanym „Przestępstwa przeciwko ochronie informacji" znalazły się normy umożliwiające pociągnięcie do odpowiedzialności karnej sprawców najbardziej klasycznych zamachów na bezpieczeństwo danych i systemów komputerowych, takich jak:

- hacking (art. 267 § 1);
- podsłuch (art. 267 § 2);
- ujawnienie informacji (art. 266);
- naruszenie integralności komputerowego zapisu informacji (art. 268 § 2);
- rozpowszechnianie złośliwych programów (art. 268 § 2 lub art. 269);
- sabotaż komputerowy (art. 269 § 1 i art. 269 § 2).

Do innych przepisów kodeksu karnego, który przewiduje możliwość popełnienia przestępstwa przy użyciu komputera należy zaliczyć:

- nielegalne uzyskanie programu komputerowego (art. 278 § 2);
- kradzież kart zabezpieczających (art. 278 § 5);
- paserstwo programu komputerowego (art. 293 § 1 i art. 293 § 2);
- oszustwo komputerowe (art. 287);
- oszustwo telekomunikacyjne (art. 285);

---

[181] A. Bógdał – Brzezińska, M. F. Gawrycki, *Cyberterroryzm i problemy*..., op.cit., s. 292.
[182] *Konstytucja Rzeczypospolitej Polski* z dnia 2 kwietnia 1997 r.
[183] *Kodeks Karny* Dz. U. Nr 88 poz. 553 (Dz. U. 97.88.553) z dnia 2 sierpnia 1997 r. wraz z późniejszymi zmianami (03.05.2006 r.)

- inne, na przykład w związku z rozpowszechnianiem definicji dokumentu na „zapis na komputerowym nośniku informacji", pedofilia, pornografia[184].

W rozdziale XX kodeksu karnego[185] dotyczącym „Przestępstwa przeciwko bezpieczeństwu powszechnemu" – zakłócając, uniemożliwiając lub w inny sposób wpływając na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych (art. 165 § 1 pkt. 4).

Komputerowym przestępstwem przeciwko Rzeczypospolitej Polskiej (Rozdział XVII „Przestępstwa przeciwko Rzeczypospolitej Polskiej") jest uprzywilejowana postać szpiegostwa: kto, w celu udzielenia obcemu wywiadowi wiadomości określonych w § 2 ("wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej"), gromadzi je lub przechowuje, wchodzi do systemu informatycznego w celu ich uzyskania albo zgłasza gotowość działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej (art. 130 § 2 i art. 130 § 3)[186].

W kodeksie karnym najważniejszy w tym przypadku wydaje się art. 268 § 2 i art. 268 § 3. Analizując skutki popełnionego przestępstwa, ustawodawca stanowi wysokość kary od 3 miesięcy do 5 lat w przypadku wystąpienia „znacznej szkody majątkowej". Zastrzega się przy tym, że musi mieć ono charakter umyślny i nie może wynikać na przykład z awarii sprzętu (awarii sprzętu teleinformatycznego).

Poniżej przedstawiam Tabelę 3.6., która charakteryzuje niektóre rodzaje przestępstw komputerowych i wysokości kar za ich popełnienie.

---

[184] Mejssner. B., *Sherlock Holmes w firmowych komputerach*, „Rzeczypospolita" 08 września 2006 r. wydanie 749/210 /7504/, s. dF 4.

[185] *Kodeks Karny* Dz. U. Nr 88 poz. 553 (Dz. U. 97.88.553) z dnia 2 sierpnia 1997 r. wraz z późniejszymi zmianami (03.05.2006 r.)

[186] [URL – http://asp.digikom.pl/kara.htm] 17.01.2005 r. 14.30.

Tabela 3.6. Niektóre rodzaje przestępstw komputerowych i wysokości kar za ich popełnienie

Rodzaj przestępstwa komputerowego	Wysokość kary
Przestępstwa przeciwko ochronie informacji	
Hacking	do 2 lat
Podsłuch i inwigilacja	do 2 lat
Naruszenie integralności komputerowego zapisu informacji	od 2 do 3 lat
Sabotaż komputerowy	od 6 miesięcy do 8 lat
Przestępstwa przeciwko wiarygodności dokumentów, obrotowi gospodarczemu i pieniężnemu	
Fałszerstwo komputerowego zapisu informacji stanowiącej dokument	od 6 miesięcy do 5 lat
Zniszczenie lub pozbawienie mocy dowodowej dokumentu elektronicznego	do 2 lat
Nierzetelne prowadzenie dokumentacji działalności gospodarczej	od 3 miesięcy do 5 lat
Fałszerstwo kart płatniczych	od 5 do 25 lat
Przestępstwa przeciwko mieniu	
Nielegalne używanie programu komputerowego	od 3 miesięcy do 5 lat
Paserstwo programu komputerowego	od 3 miesięcy do 5 lat
Oszustwo komputerowe	od 3 miesięcy do 5 lat
Oszustwo telekomunikacyjne	do 3 lat
Inne rodzaje przestępstw	
Szpiegostwo komputerowe	do 25 lat
Sprowadzenie niebezpieczeństwa powszechnego	do 12 lat
Przestępstwa przeciwko danym osobowym	
Naruszenie warunków dopuszczalności przetwarzania danych	do 3 lat
Udostępnienie danych osobowych osobom nieuprawnionym	do 2 lat
Naruszenie obowiązku zabezpieczenia danych osobowych	do 1 roku
Nie zgłoszenie zbioru danych osobowych do rejestracji	do 1 roku
Naruszenie praw osoby zarejestrowanej	do 1 roku

Źródło: Opracowanie własne na podstawie *Kodeksu Karnego* oraz *Aspekt prawny. Przestępstwa komputerowe a prawo karne* [URL – http://bezpieczeństwoit.website.pl/aspekt_prawny.htm] 03.05.2008 r. 13.00.

Rozważając kwestie zapewnienia bezpieczeństwa danych należy mieć zawsze świadomość o istniejących zagrożeniach, o zabezpieczeniach, a także w szczególności prawa odnoszącego się do ochrony bezpieczeństwa informacji (bezpieczeństwa teleinformatycznego).

Znajomość odpowiednich przepisów prawa ma znaczenie zarówno dla instytucji rządowych i poza rządowych, w celu sprawnego dochodzenia swoich praw w przypadku utraty bezpieczeństwa teleinformatycznego, jak i dla pojedynczych

użytkowników, jako przestroga przed nieuprawnionym działaniem. Osoba atakująca bezpieczeństwo teleinformatyczne instytucji naraża siebie nie tylko na sankcje cywilnoprawne, lecz także na szereg kar wynikających z postępowania karnego, z karą więzienia włącznie[187].

3.7. Wnioski końcowe

1. Przy obecnym wzroście gospodarczym i polityce rządu w zakresie ICT, Polska będzie przez następną dekadę w drugiej grupie krajów europejskich o średnim wskaźniku osieciowania i rozwoju teleinformatycznym.
2. Liczba osób, które napotkała jakiekolwiek problemy dotyczące bezpieczeństwa teleinformatycznego w sieci, będzie rósł dużo wolniej niż przybywać będzie użytkowników Internetu.
3. Najczęściej występującym problemem dotyczącym bezpieczeństwa sieci i danych teleinformatycznych będzie zawirusowanie komputerów powodujące utratę danych.
4. W Polsce[188] tak jak i w Siłach Zbrojnych Rzeczypospolitej Polski do dnia dzisiejszego nie ma zdefiniowanej Infrastruktury Krytycznej a tym samym Krytycznej Infrastruktury Teleinformatycznej.
5. Złożona problematyka bezpieczeństwa i ochrony Infrastruktury Krytycznej Państwa musi wymusić zmiany w poglądach dotyczących: bezpieczeństwa narodowego, ochrony obywateli, realizacji zadań obronnych w czasie pokoju i w czasie zagrożenia. Ministerstwa nie mają opracowanych kompleksowych planów ochrony odpowiednich sektorów Infrastruktury Krytycznej Państwa. Nie mają także żadnych wytycznych w tym zakresie. Poszczególne ministerstwa powinny przyjąć na siebie rolę inspiratora działań, zmierzających do opracowania szczególnych programów ochrony Krytycznej Infrastruktury Państwa, a także do monitorowania stanu bezpieczeństwa we właściwych dla siebie sektorach infrastruktury krytycznej.

---

[187] *Przestępstwa komputerowe w kodeksie karnym*. [URL – gazeta – it.pl/prawo/przestępstwa_komputerowe.html] 03.05.2006 r. 12.50.

[188] Pierwsza próba zdefiniowania Infrastruktury Krytycznej Państwa została podjęta w Ustawie *O zarządzaniu kryzysowym* Dz. U. Nr 89 poz. 590 (Dz. U. 07.89.590) z dnia 21 maja 2007 r. Nie ma podziału infrastruktury wg. hierarchi: żywotne, krytyczne, wrażliwe i podstawowe. Podczas pisania niniejszej pracy, nie spotkałem się z żadnym opracowaniem dotyczącym Infrastruktury Krytycznej w Siłach Zbrojnych Rzeczypospolitej Polski.

6. Dotychczasowy brak kontroli monitorowania i funkcjonowania podmiotów odpowiedzialnych za bezpieczeństwo Infrastruktury Krytycznej w Polsce naraża i będzie narażać nasze państwo, gospodarkę narodową oraz Siły Zbrojne Rzeczypospolitej Polski na duże straty oraz chaos organizacyjny w przypadku ewentualnych ataków cyberterrorystycznych lub zakłóceń w kluczowych sektorów infrastruktury, skutkujących tak zwanym „efektem kaskadowym".
7. Stałe i stabilne funkcjonowanie wszystkich wymienionych sektorów Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski, jest uzależnione przede wszystkim od sektora energetycznego oraz od systemów i technologii teleinformatycznej i łączność czyli od Krytycznej Infrastruktury Teleinformacyjnej Sił Zbrojnych RP.
8. Prowadzenie Operacji Informacyjnych i uzyskanie dominacji informatycznej staje się warunkiem wstępnym do podejmowania jakichkolwiek innych działań przez Siły Zbrojne. Osiągnięcie dominacji informacyjnej poprzez stosowanie nowoczesnych technologii, manipulację mediami i sterowanie informacjami pozwala na postrzeganie rzeczywistości w „pożądanym wymiarze".
9. Prowadzenie Operacji Informacyjnych powinno być przygotowane i koordynowane na wszystkich poziomach kierowania i dowodzenia. Celowym jest stworzenie odpowiedniej korelacji pomiędzy obszarami będącymi składowymi Operacji Informacyjnych w kontekście państwa i Sił Zbrojnych Rzeczypospolitej Polski. Na wzór armii innych państw NATO należałoby utworzyć etatowe komórki działań informacyjnych od szczebla Związku Taktycznego.
10. Polska pod względem liczby regulacji prawnych dotyczących bezpieczeństwa teleinformacyjnego i zakazów karnych konstytuujących przestępstwa komputerowe w ustawodawstwie wewnętrznym, zajmuje w porównaniach międzynarodowych stosunkowo wysoką lokatę i zaliczana jest do grupy państw, które w znacznym stopniu dostosowały swój system prawny do standardów normatywnych w tej dziedzinie.

ROZDZIAŁ IV

MODEL SYSTEMU ZARZĄDZANIA KRYZYSOWEGO W SIŁACH ZBROJNYCH RZECZYPOSPOLITEJ POLSKI W WARUNKACH ZAGROŻEŃ CYBERTERRORYZMU

4.1. Cele i zadania

Przy dążeniu w XXI wieku do nasycenia różnymi systemami teleinformatycznymi Sił Zbrojnych Rzeczypospolitej Polski ich ochrona staje się na dzień dzisiejszy sprawą priorytetową. Podstawowy zasób informacyjny Sił Zbrojnych jak już określiłem w niniejszej rozprawie doktorskiej[189] znajduje się w Infrastrukturze Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Narzuca to konieczność ochrony fizycznej, elektromagnetycznej i osobowej w sposób adekwatny do obecnych zagrożeń. Obecnie głównym celem w wymiarze długoterminowym powinno być opracowanie Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski, widzianego jako system „docelowy".

Docelowy Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski należy rozumieć jako: **system organizacyjno – funkcjonalny, wykorzystujący systemy teleinformatyczne, które w sposób automatyczny zbierają, przetwarzają i magazynują informację oraz alarmują o zaistniałych lub przewidywanych zagrożeniach.**

System Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski w podstawowym swoim założeniu powinien być zgodny z założeniami NATO CIRC (NATO *Computer Incydent Response Capability*).

Główne założenia dla System Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski są następujące:

---

[189] Rozdział III, podrozdział 3.3.

1. System powinien wskazywać działania w zakresie bezpieczeństwa teleinformatycznego. Umożliwi to szybkie i skuteczne reagowanie na zagrożenia w systemach teleinformatycznych.
2. System powinien być rozszerzeniem procesu planowania, utrzymania ciągłości działania oraz gotowości do reagowania na incydenty kiedy one występują.
3. Musi on być zadaniem realizowanym na szczeblu centralnym Ministerstwa Obrony Narodowej.
4. System powinien skoncentrować w celu uniknięcia dublowania działań obsługę incydentów w jeden scentralizowany i skoordynowany sposób.
5. System Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski wymaga współpracy wszystkich jednostek organizacyjnych podległych Ministrowi Obrony Narodowej oraz resortów cywilnych uczestniczących w systemie ochrony państwa[190] (Infrastruktura Krytyczna w Siłach Zbrojnych Rzeczypospolitej Polski).
6. System powinien obejmować działania mające na celu ograniczenie poziomu ryzyka dla Krytycznej Infrastruktury Teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polski (Infrastruktura Krytyczna w Siłach Zbrojnych Rzeczypospolitej Polski). System Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski powinien podejmować między innymi niżej wymienione działania:
   - prowadzenie oceny podatności na zagrożenia systemów teleinformatycznych;
   - prowadzenie testów penetracyjnych;
   - prowadzenie szkoleń specjalistycznych;
   - opracowywanie i wydawanie materiałów szkoleniowych;
   - analizowanie i opracowywanie urządzeń ochrony teleinformatycznej dla administratorów systemów w celu prawidłowego i właściwego zapobiegania i wykrywania incydentów;
   - sprawne prowadzenie analizy systemowej;
   - projektowanie złożonych systemów organizacyjno – funkcjonalnych;
   - prowadzenie prac badawczych związanych z bezpieczeństwem teleinformatycznym (incydenty w cyberprzestrzeni).

Główne cele i zadania dla System Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski na dzień dzisiejszy przedstawiają się następująco:

---

[190] Ministerstwa i organizacje rządowe oraz pozarządowe.

1. Scentralizowanie zgłaszania incydentów (cyberataków) – **statystyki**.
2. Skoordynowanie reagowania na wybrane typy incydentów lub incydenty mające wpływ na wybraną technologię teleinformatyczną i teleinformacyjną – **wirusy**.
3. Udzielanie bezpośredniej pomocy technicznej na żądanie lub potrzebę – **zakres pomocy dla jednostek centralnych MON i jednostek organizacyjnych podległych Ministrowi Obrony Narodowej**.
4. Umożliwienie weryfikacji informacji związanych z bezpieczeństwem teleinformatycznym – **na przykład fałszywe sygnały dotyczące cyberataków i wirusów**.
5. Dostarczenie danych i wskazówek dla procesu planowania ciągłości działania – **informacje o możliwościach centrów danych i ofertach outsourcingu**.
6. Wykonywanie funkcji elementu łączności z zagranicznymi strukturami reagowania kryzysowego (np. NATO CIRC).
7. Zachęcanie wytwórców sprzętu ochrony kryptograficznej do reagowania na problemy bezpieczeństwa teleinformatycznego.
8. Wykonywanie funkcji łącznika z wojskowymi i cywilnymi organami ścigania.

Osiągnięcie i realizacja wyżej wymienionych celów Systemowi Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski umożliwi:

1. Udzielenie pomocy zaatakowanym elementom Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski w zakresie bezpiecznego, szybkiego i efektywnego usuwaniu skutków incydentów;
2. Minimalizowanie wpływu z powodu utraty lub kradzieży informacji (jawnych i niejawnych) lub zakłóceń w usługach i zasobach Krytycznej Infrastruktury Teleinformatycznej na skutek wystąpienia incydentu;
3. Systematyczne reagowanie na podstawie sprawdzonych procedur co spowoduje obniżenie ryzyka związanego z możliwością ponownego wystąpienia incydentu.

4.2. Wymagania i ograniczenia systemowe

Jednostki organizacyjne podległe Ministrowi Obrony Narodowej[191] prowadzą swoją działalność służbową również poprzez ciągłą wymianę informacji w systemach teleinformatycznych (Krytyczna Infrastruktura Teleinformatyczna Sił Zbrojnych Rzeczypospolitej Polski) połączonych w sieciach WAN, MAN i LAN[192]. Jednocześnie wyżej wymienione jednostki korzystają z globalnej sieci Internet w celu pozyskania informacji ze źródeł publicznych, wymiany jawnej informacji[193] oraz informacji związanej z projektami istotnymi dla realizacji zadania służbowych. W obecnych czasach informacja nabrała strategicznego znaczenia, co wymaga szerokich zabezpieczeń zgodnie z obowiązującymi dokumentami normatywnymi[194]. Zdolność do działania oraz wydajność wojskowych i cywilnych resortów w XXI wieku jest prawie całkowicie zależna od poprawności działania systemów teleinformatycznych, przetwarzających i przesyłających informacje. Skuteczność i efektywność tych systemów, będzie wyznacznikiem: **czy priorytet informacji może być na odpowiednim poziomie osiągnięty i utrzymany.**

W celu zapewnienia skuteczności działania systemów teleinformatycznych, urządzenia i materiały ochrony kryptograficznej muszą być jednolicie wdrożone do eksploatacji w celu zabezpieczenia ochrony teleinformatycznej[195]. System Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski ma bardzo duże znaczenie dla jednolitej implementacji urządzeń ochrony kryptograficznej niezbędnych do zapewnienia wymagań prawidłowe ochrony informacji oraz bezpieczeństwa teleinformatycznego.

Jednolita ochrona poufności, integralności i zapewnionej dostępności do informacji[196] Sił Zbrojnych Rzeczypospolitej Polski oraz do systemów teleinformatycznych stanowią główne czynniki dla potrzeby posiadania przez Siły Zbrojne Systemu Zarządzania Kryzysowego. Zdolność ta uważana jest za krytyczną względem prawidłowego zabezpieczenia ochrony teleinformatycznej.

---

[191] Mówimy tu o jednostkach administracyjnych i resortach zarówno wojskowych jak i cywilnych.
[192] WAN (*Wide Area Network*) – sieć rozległa, łącząca ze sobą sieci; MAN (*Metropolitan Area Network*)
i LAN (*Local Area Network*).
[193] Mówimy tu o informacji nieklasyfikowej, która nie jest pod żadnym względem informacją służbową.
[194] Wszystkie dokumenty normatywne zostały zawarte w Załączniku 3.
[195] Ochrona systemów teleinformatycznych i teleinformacyjnych stanowiących Krytyczną Infrastrukturę Teleinformatyczna Sił Zbrojnych Rzeczypospolitej Polski.
[196] W literaturze tematu są wymieniane następujące atrybuty które określają nam stan bezpieczeństwa teleinformatycznego i teleinformacyjnego: poufność, autentyczność, dostępność, integralność danych, integralność systemu, integralność, rozliczalność, niezawodność.

W tym kontekście oraz jako podstawowe wymaganie, wsparcie Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski musi być dostępne dla wszystkich systemów teleinformatycznych Sił Zbrojnych jako gwarancja priorytetów operacyjności niżej wymienionych systemów:

- narodowe systemy teleinformatyczne;
- sojusznicze systemy teleinformatyczne (NATO *Network Backbone Systems and WAN*);
- Zautomatyzowane Systemy Dowodzenia;
- Zautomatyzowane Systemy Dowodzenia i Kierowania Walką;
- Systemy Kierowania Systemami Walki;
- systemy teleinformatyczne Sił Zbrojnych w jednostkach i instytucjach cywilnych podległych Ministrowi Obrony Narodowej;
- globalna sieć Internet – we wszystkich jednostkach organizacyjnych (wojskowych i cywilnych) podległych Ministrowi Obrony Narodowej.

Minimalne wsparcie przez System Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski musi obejmować następujące elementy:

- wykrycie, śledzenie i znalezienie działań intruza we wszystkich systemach teleinformatycznych Sił Zbrojnych;
- pomoc w oszacowaniu słabych punktów oraz nie zabezpieczonych przed atakami miejsc w systemach teleinformatycznych a dokładnie prowadzenie oceny podatności na zagrożenia (VAAT - *Vulnerability Assessment & Assistance Team*);
- przeprowadzenie okresowych sprawdzeń bezpieczeństwa teleinformatycznego czyli prowadzenie testów penetracyjnych (IAA - *Information Assurance Assessment*);
- scentralizowane reagowanie na incydenty związane z bezpieczeństwem teleinformatycznym oraz składanie meldunków;
- scentralizowane kontakty z krajowymi[197] i sojuszniczymi systemami reagowania na incydenty komputerowe[198];
- dystrybucja poradników[199];
- prewencja w zakresie złośliwych kodów;

---

[197] W tym wchodzą również nie rządowe instytucje.
[198] Narodowe CERT krajów będących członkami Sojuszu Paktu Północnoatlantyckiego.
[199] Na przykład poradniki dotyczące bezpieczeństwa teleinformatycznego i ostrzeżeń przed incydentami komputerowymi w Siłach Zbrojnych RP.

- prowadzenie szkoleń w zakresie bezpieczeństwa teleinformatycznego z żołnierzami zawodowymi oraz pracownikami cywilnymi wojska;
- audyty bezpieczeństwa i testy penetracyjne systemów teleinformatycznych;
- generacja raportów technicznych odnoszących się do złośliwych kodów.

Reasumując System Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski powinien:

- wpierać wszystkie systemy teleinformatyczne Sił Zbrojnych RP;
- reagować w porę wspierając wszystkie instytucje podległe Ministrowi Obrony Narodowej, szczególnie w przypadku wystąpienia naruszeń bezpieczeństwa teleinformatycznego;
- współpracować z odpowiednią krajową władzą bezpieczeństwa;
- współpracować z NATO CIRC;
- zapewnić odpowiednie wsparcie kiedy jest to wymagane[200];
- działać przy ciągłej współpracy z Służbami Ochrony Państwa[201] oraz władzami operacyjnymi systemów teleinformatycznych.

Jeżeli wyżej wymienione wymagania, nie zostaną zrealizowane, to w miarę „rozrastania się" systemów teleinformatycznych będą one bardziej podatne na nie wykryte naruszenia polityki bezpieczeństwa. Zdolność Sił Zbrojnych do osiągnięcia wojskowych i politycznych celów będzie zagrożona z powodu stale rosnącego uzależnienia od systemów teleinformatycznych Sił Zbrojnych, których integralność, poufność, niezawodność, autentyczność i dostępność nie będzie już w sposób prawidłowy zapewniona. Jednocześnie zasoby Sił Zbrojnych będą wykorzystywane niewydolnie z powodu braku zcentralizowanego wsparcia poprzez System Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski oraz braku konsolidacji indywidualnego rozmieszczenia zasobów teleinformatycznych.

---

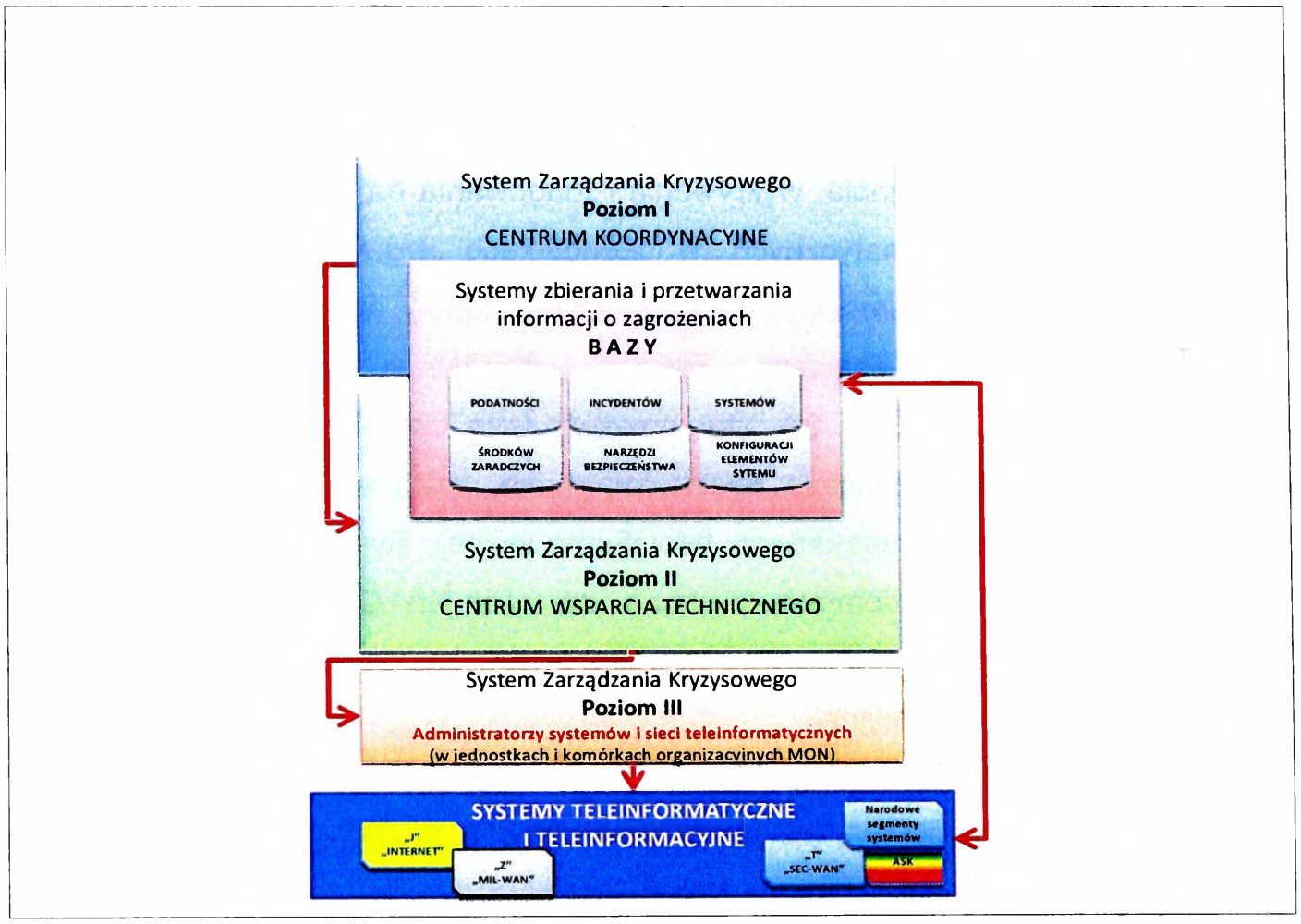
[200] Podczas ćwiczeń, codziennej pracy i kryzysu.
[201] Akredytacja oraz certyfikacja systemów przez JC SKW niejawnych systemów teleinformatycznych

4.3. Koncepcja funkcjonowania Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski - struktura Systemu Zarządzania Kryzysowego

System Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski zapewni proces zapobiegania, wykrywania i reagowania na incydenty komputerowe w systemach teleinformatycznych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej. Organizacja tego systemu na obszarze Rzeczypospolitej w znaczny sposób poprawi zdolność reagowania na incydenty komputerowe, tak aby możliwe było natychmiastowe i efektywne reagowanie na bezpieczeństwo teleinformatyczne, mające miejsce w narodowej wojskowej i cywilnej infrastrukturze teleinformatycznej. System ten, powinien być zorganizowany w trzypoziomową strukturę (na wzór NATO CIRC), w skład której wchodzą następujące komórki organizacyjne:

1. Centrum Koordynacyjne.
2. Centrum Wsparcia Technicznego.
3. Administratorzy systemów teleinformatycznych w jednostkach i komórkach podległych Ministrowi Obrony Narodowej.

Nadzór i kontrolę nad Systemem Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski powinien sprawować Dyrektor Wojskowego Biura Bezpieczeństwa Łączności i Informatyki lub Dyrektor Departamentu Informatyki i Telekomunikacji MON



Rysunek 4.1. Koncepcja funkcjonowania trójszczeblowego Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski

Źródło: Opracowanie własne.

POZIOM I - Centrum Koordynacyjne.

Realizowane zadania:

- analizowanie informacji o zdarzeniach oraz tworzenie na ich bazie opracowań okresowych (raportów) o stanie bezpieczeństwa i teleinformatycznego oraz publikowanie podręczników wspólnie z resortami cywilnymi;
- nadzór nad realizacją zadań przez Centrum Wsparcia Technicznego. Koordynacja, opracowywanie i utrzymanie „Programu Pracy" dla Centrum Wsparcia Technicznego.
- określenie zasad funkcjonowania Systemu Zarządzania Kryzysowego;
- prowadzenie działań pro aktywnych, polegających na analizie infrastruktury teleinformatycznej i opracowywaniu zaleceń zapobiegających wystąpieniu incydentów;

- współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:
  - Departamentem Ochrony Informacji Niejawnych MON;
  - Służbą Kontrwywiadu Wojskowego (Jednostka Certyfikująca SKW oraz Biuro Bezpieczeństwa Teleinformatycznego);
  - Żandarmerią Wojskową;
  - Agencją Bezpieczeństwa Wewnętrznego (Rządowy Zespół Reagowania na Incydenty Komputerowe – CERT.GOV.PL);
  - z krajowymi i międzynarodowymi organami koordynującymi System Reagowania Kryzysowego (np. NATO CIRC);
  - gestorem;
  - organizatorem systemu;
  - dostawcą usług;
  - z pionami ochrony informacji niejawnych właściwych jednostek organizacyjnych podległych Ministrowi Obrony Narodowej;
- występowanie w roli punktu kontaktowego do współpracy w ramach NATO CIRC. Udział w pracach grup roboczych oraz reprezentowanie resortu obrony narodowej w kontaktach z organizacjami spoza resortu obrony narodowej;
- występowanie w roli punktu kontaktowego do spraw odbierania, oceny i dystrybucji informacji związanych z zagrożeniem oraz utrzymywanie stosownej bazy danych dotyczących wyżej wymienionych zagadnień;
- utrzymywanie (prowadzenie) bazy danych o dochodzeniach związanych z incydentami oraz bazy danych narzędzi dotyczących bezpieczeństwa Systemu Zarządzania Kryzysowego;
- współudział w programie edukacyjnym i implementacyjnym dotyczącym szerzenia świadomości technicznej;
- meldunki, raporty do właściwych władz o trendach związanych z incydentami oraz składanie propozycji rewizji (przeglądu) polityki bezpieczeństwa teleinformatycznego;
- prowadzenie portali informacyjnych (oddzielnie dla jawnych i niejawnych systemów teleinformatycznych) na potrzeby obsługi incydentów komputerowych;
- prowadzenie wykazu osób funkcyjnych odpowiedzialnych za System Zarządzania Kryzysowego i osób współpracujących w tym zakresie;
- koordynacja działań związanych z oceną zagrożeń oraz testów penetracyjnych.

POZIOM II – Centrum Wsparcia Technicznego (Praca w trybie 24 godzinnym, 7 dni w tygodniu).

Realizowane zadania:

- prowadzenie bazy danych wskazówek - porad, informacji technicznych zawierających ostrzeżenia oraz informacje dotyczące bieżących napraw;
- składanie meldunków o incydentach i podatnościach na zagrożenia do Centrum Koordynacyjnego;
- udostępnianie ogólnych informacji związanych z incydentami władzom operacyjnym systemów teleinformatycznych;
- współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:
  - Centrum Technicznym NATO CIRC;
  - Systemem Wsparcia Eksploatacji;
  - krajowymi i międzynarodowymi zespołami reagowania na incydenty komputerowe;
  - pionami ochrony informacji niejawnych właściwych jednostek organizacyjnych podległych Ministrowi Obrony Narodowej;
- wykonywanie czynności typu: reagowanie na incydenty, odzyskiwanie i generowanie raportów, zgodnie z potrzebą lub żądaniem władz operacyjnych, koordynowanych przez Centrum Koordynacyjne;
- utrzymywanie bazy danych o incydentach, prowadzanie analiz dotyczących trendów z nimi związanych dla Centrum Koordynacyjnego. Prowadzenie bazy danych dotyczącej zagrożeń technicznych;
- monitorowanie w trybie ciągłym stanu bezpieczeństwa systemów teleinformatycznych;
- zbieranie informacji o zdarzeniach oraz tworzenie na ich bazie raportów o stanie bezpieczeństwa nadzorowanych systemach teleinformatycznych;
- bezpośrednia obsługa incydentów w systemach teleinformatycznych;
- wnioskowanie do właściwych pionów ochrony informacji niejawnych w sprawie czasowego wyłączenia lub zaniechania przetwarzania informacji w systemach w których stwierdzono wystąpienie incydentów komputerowych;
- prowadzenie strony www. zawierającej stosowne informacje (np. wskazówki, porady, narzędzia bezpieczeństwa, informacje techniczne zawierające ostrzeżenia oraz informacje, dyrektywy, wytyczne);

- wstępny wybór i ocena narzędzi bezpieczeństwa dotyczących wykrywania incydentów, oceny zagrożeń oraz realizacja czynności związanych z zapobieganiem i wykrywaniem kodów złośliwych;
- utrzymywanie bazy danych o narzędziach bezpieczeństwa (np. narzędzia zarządzania bezpieczeństwem, narzędzia służące do wykrywania kodów złośliwych), łącznie z warunkami ich pracy i możliwością zastosowania w środowisku eksploatowanych systemów;
- zapewnienie władzom operacyjnym systemów, na ich wniosek lub zgodnie z potrzebą wsparcia technicznego i pomocy w zakresie wtargnięć i zabezpieczenia przed kodami złośliwymi. Udzielenie pomocy administratorom w trakcie obsługi incydentów oraz przywracanie funkcjonowania systemów teleinformacyjnych i teleinformatycznych;
- opracowywanie i uaktualnianie materiałów dotyczących konfiguracji systemów operacyjnych i aplikacji związanych z bezpieczeństwem;
- prowadzenie oceny zagrożeń systemów na poziomie makro pod kątem architektury i projektu systemu. Prowadzenie w porozumieniu z właściwymi pionami ochrony informacji niejawnych kontroli konfiguracji systemów teleinformatycznych, w celu ustalenia aktualnego stanu zabezpieczenia tych systemów;
- wspomaganie szczegółowej oceny technicznej zagrożeń, testów penetracyjnych zgodnie z ustaleniami dokonanymi z Centrum Koordynacyjnym;
- zapewnienie wsparcia technicznego podczas dochodzeń prawnych;
- udział w pracach grup roboczych w ramach NATO w zakresie reagowania na incydenty komputerowe;
- wsparcie warsztatów technicznych lub sesji szkoleniowych dotyczących bezpieczeństwa teleinformacyjnego i teleinformatycznego;
- opracowywanie materiałów szkoleniowych przeznaczonych do dystrybucji;
- prowadzenie ewidencji administratorów systemów teleinformatycznych zawierających dane personalne, numer telefonu, nazwę komórki organizacyjnej każdej osoby wyznaczonej do pełnienia funkcji administratorów systemu.

POZIOM III – Administratorzy systemów teleinformatycznych i teleinformacyjnych w jednostkach i komórkach podległych Ministrowi Obrony Narodowej - Władze operacyjne.

Realizowane zadania:

- wykonywanie czynności związanych z przeciwdziałaniem wystąpieniu i właściwym reagowaniem na incydenty oraz odtwarzaniem systemu przy współpracy z Centrum Wsparcia Technicznego Systemu Zarządzania Kryzysowego. Wykrywanie wtargnięć w czasie rzeczywistym, wspomagane przez Centrum Koordynacji poprzez Centrum Wsparcia Technicznego Systemu Zarządzania Kryzysowego;
- przestrzeganie obowiązujących dokumentów normatywnych i zaleceń w zakresie polityki bezpieczeństwa teleinformatycznego;
- nadzorowanie użytkowników administrowanych przez nich systemów teleinformatycznych i teleinformacyjnych w zakresie przestrzegania ustalonych procedur bezpieczeństwa;
- ścisła współpraca w zakresie zabezpieczenia śladów i ustaleń przyczyn wystąpienia incydentu komputerowego z: Departamentem Ochrony Informacji Niejawnych MON i RSZ, Służbą Kontrwywiadu Wojskowego oraz Żandarmerią Wojskową;
- składanie do Centrum Koordynacyjnego oraz Centrum Wsparcia Technicznego meldunków o wykryciu zdarzeń, incydentów i zagrożeń mających wpływ na naruszenie bezpieczeństwa teleinformatycznego w administrowanych przez nich systemach teleinformatycznych;
- zapewnienie właściwym osobom wchodzącym w skład władzy operacyjnej wskazówek - porad, informacji technicznych zawierających ostrzeżenia oraz informacji dotyczących naprawy bieżącej;
- prowadzenie dokumentacji zawierającej informacje związane z konfiguracją systemów przez nich kontrolowanych;
- informowanie Centrum Wsparcia Technicznego Systemu Zarządzania Kryzysowego o zmianach personalnych administratorów oraz zmianach w konfiguracji systemów teleinformatycznych i teleinformacyjnych mogących mieć wpływ na ich bezpieczeństwo.

Służba Kontrwywiadu Wojskowego

Realizowane zadania:

- rozpoznanie, zapobieganie oraz wykrywanie popełnionych przez żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy SKW i SWW oraz pracowników cywilnych Sił Zbrojnych Rzeczypospolitej Polskiej i innych jednostek organizacyjnych MON, przestępstw:

  - przeciwko ochronie informacji określonych w rozdziale XXXIII ustawy z dnia 06 czerwca 1997 r. – Kodeks karny;

  - przeciwko Rzeczypospolitej Polskiej określonych w rozdziale XVII ustawy z dnia 06 czerwca 1997 r. – Kodeks karny;

  - związanych z działalnością terrorystyczną godzącą w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw które zapewniają wzajemność;
- współdziałanie z Żandarmerią Wojskowa do ścigania przestępstw;
- prowadzenie kontrwywiadu radioelektronicznego oraz przedsięwzięć z zakresu ochrony teleinformatycznej;
- realizowanie, w granicach swojej właściwości, zadań służbowych ochrony państwa określonych w ustawie z dnia 22 stycznia 1999 r. „O ochronie informacji niejawnych" Tekst ujednolicony po zmianach z dnia 15 kwietnia 2005 r. Dz. U. 1999.11.95; Tekst ujednolicony Dz. U. 2005.196.1631 - akty zmieniające[202][203].

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:

- producentem;
- organizatorem systemu;
- Systemem Wsparcia Projektowania Systemów Teleinformatycznych i Teleinformacyjnych;
- Żandarmerią Wojskową poprzez Centrum Koordynacyjne lub bezpośrednio w sytuacjach szczególnych;

---

[202] Opracowano na podstawie: Ustawa z dnia 09 czerwca 2006 r. *O Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* Dz. U. z 2006 r., Nr 104, poz. 709, Nr 218, poz. 1592, z 2007 r., Nr 25, poz. 162.

[203] W szczególności Ustawę z dnia 22 stycznia 1999 r. *O ochronie informacji niejawnych* Tekst ujednolicony po zmianach z dnia 15 kwietnia 2005 r. Dz. U. 1999.11.95; Tekst ujednolicony Dz. U. 2005.196.1631 - akty zmieniające – Rozdział 10 *Bezpieczeństwo systemów i sieci teleinformatycznych.*

- Centrum Koordynacyjnym.

Jednostka Certyfikująca Służby Kontrwywiadu Wojskowego

Realizowane zadania:

- przeprowadzenie oceny urządzeń realizujące zabezpieczenia teleinformatyczne oraz systemów przetwarzających informację niejawne. Certyfikacja wyrobów produkowanych w kraju oraz importowanych wyłącznie na potrzeby obronności i bezpieczeństwa państwa służące do ochrony informacji niejawnych w ramach resortu obrony narodowej;
- wydawanie certyfikatów potwierdzających zapewnienie odpowiedniego poziomu bezpieczeństwa teleinformatycznego przetwarzanym informacjom niejawnym;
- sprawuje nadzór nad certyfikowanym wyrobem w okresie ważności certyfikatu i może w dowolnym momencie cofnąć wydany przez siebie certyfikat jeżeli uzna, że wyrób przestał zapewniać odpowiedni poziom bezpieczeństwa przetwarzanym informacjom niejawnym;

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:

- producentem;
- organizatorem systemu;
- Systemem Wsparcia Projektowania Systemów Teleinformatycznych i Teleinformacyjnych;
- Centrum Koordynacyjnym.

Biuro Bezpieczeństwa Teleinformatycznego Służby Kontrwywiadu Wojskowego

Realizowane zadania:

- certyfikacja wyrobów służących ochronie informacji niejawnych – działając z upoważnienia Szefa SKW;
- akredytacja narodowym systemów i sieci teleinformatycznych przetwarzających informację niejawne;
- akredytacja sojuszniczych (np. NATO, UE) systemów i sieci teleinformatycznych przetwarzających informację niejawne;
- wyznaczane poziomów zabezpieczenia miejsca;

- akredytacja bezpieczeństwa fizycznego, elektromagnetycznego i technicznego pomieszczeń specjalnych.

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:

- producentem;
- organizatorem systemu;
- Systemem Wsparcia Projektowania Systemów Teleinformatycznych i Teleinformacyjnych;
- Centrum Koordynacyjnym.

Producent

Realizowane zadania:

- prowadzenie badań naukowych i prac rozwojowych w zakresie systemów i oprogramowania bezpieczeństwa teleinformatycznego;
- projektowanie systemów bezpieczeństwa teleinformatycznego;
- wdrażanie w praktyce oprogramowania oraz wyżej wymienionych systemów bezpieczeństwa.

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego i teleinformacyjnego z:

- gestorem;
- Systemem Wsparcia i Projektowania Systemów Teleinformatycznych i Teleinformacyjnych;
- Służbą Kontrwywiadu Wojskowego (Jednostka Certyfikująca SKW oraz Biuro Bezpieczeństwa Teleinformatycznego).

Gestor

Realizowane zadania:

- wykazanie potrzeb dotyczących nowych systemów bezpieczeństwa teleinformatycznego;
- opracowanie koncepcji systemu bezpieczeństwa teleinformatycznego;
- podanie dokładnej specyfikacji wyżej wymienionych systemów bezpieczeństwa;
- zaprojektowanie architektury systemów;

- kontrola i nadzór prac wykonywanych przez realizatorów (producentów) systemów bezpieczeństwa teleinformatycznego.

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:

- producentem;
- Centrum Koordynacyjnym.

Organizator systemu (instytucja wojskowa lub osoba funkcyjna)

Realizowane zadania:

- odpowiedzialność za tworzenie, rozwój i funkcjonowanie systemu bezpieczeństwa teleinformatycznego..

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:

- Służbą Kontrwywiadu Wojskowego (Jednostka Certyfikująca SKW oraz Biuro Bezpieczeństwa Teleinformatycznego);
- Centrum Koordynacyjnym.

Dostawca usługi

Realizowane zadania:

- świadczenie usług związanych z dostępem do sieci teleinformatycznej;
- administrowanie zgodnie z obowiązującymi zasadami bezpieczeństwa.

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:

- Systemem Wsparcia Eksploatacji;
- Centrum Koordynacyjnym.

System Wsparcia Eksploatacji

Realizowane zadania:

- wspieranie eksploatacji systemów bezpieczeństwa teleinformatycznego;
- wymiana podzespołów sieci i systemów bezpieczeństwa teleinformatycznego;
- wsparcie logistyczne zgodnie z obowiązującymi zasadami bezpieczeństwa i ochroną informacji niejawnych.

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:

- dostawcą usługi;
- Systemem Wsparcia Projektowania Systemów Teleinformatycznych i Teleinformacyjnych;
- Centrum Wsparcia Technicznego;
- systemami zbierania i przetwarzania informacji o zagrożeniach.

System Wsparcia Projektowania Systemów Teleinformatycznych i Teleinformatycznych

Realizowane zadania:

- analiza i projektowanie systemu bezpieczeństwa teleinformatycznego zgodnie ze standardami bezpieczeństwa i ochroną informacji niejawnych;
- integracja z różnymi systemami bezpieczeństwa teleinformatycznego;
- analiza przedwdrożeniowa i wdrożeniowa.

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:

- producentem;
- Systemem Wsparcia Eksploatacji;
- Służbą Kontrwywiadu Wojskowego (Jednostka Certyfikująca SKW oraz Biuro Bezpieczeństwa Teleinformatycznego);
- systemami zbierania i przetwarzania informacji o zagrożeniach.

System Wsparcia Wycofania

Realizowane zadania:

- wycofanie systemu bezpieczeństwa teleinformatycznego zgodnie z obowiązującymi przepisami i ochroną informacji niejawnych;
- niszczenie wstępne i końcowe zgodnie z obowiązującymi zasadami bezpieczeństwa teleinformatycznego.

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:

- Systemem Zarządzania Kryzysowego;
- systemami zbierania i przetwarzania informacji o zagrożeniach.

CERT GOV.PL – RZĄDOWY ZESPÓŁ REAGOWANIA NA INCYDENTY KOMPUTEROWE[204]

Realizowane zadania:

- kreowanie polityki w zakresie ochrony przed cyberzagrożeniami;
- koordynowanie przepływu informacji pomiędzy podmiotami;
- wykrywanie, rozpoznanie i przeciwdziałanie cyberzagrożeniom;
- reprezentacja Rzeczypospolitej Polskiej w kontaktach zagranicznych (tylko w zakresie współpracy cywilnej)[205];
- gromadzenie wiedzy dotyczącej stanu bezpieczeństwa i zagrożeń dla krytycznej infrastruktury teleinformacyjnej;
- reagowanie na incydenty bezpieczeństwa teleinformatycznego ze szczególnym uwzględnieniem krytycznej infrastruktury teleinformatycznej państwa;
- prowadzenie analiz po włamaniowych;
- tworzenie polityki ochrony systemów i sieci teleinformatycznych;
- szkolenie i podnoszenie świadomości odnośnie cyberzagrożeń;
- przygotowywanie okresowych raportów w zakresie bezpieczeństwa teleinformatycznego państwa[206];
- konsulting i doradztwo w zakresie cyberbezpieczeństwa.

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:

- Centrum Koordynacyjnym;
- innymi podmiotami (resortami cywilnymi)[207].

Inne podmioty (resorty cywilne)

Do innych podmiotów zaliczamy następujące instytucję sfery cywilnej, a mianowicie: Agencja Bezpieczeństwa Wewnętrznego, Ministerstwo Spraw Zagranicznych, Ministerstwo Sprawiedliwości, Ministerstwo Edukacji Narodowej, Urząd Komunikacji Elektronicznej, Ministerstwo Spraw Wewnętrznych i Administracji,

---

[204] CERT.GOV.PL został powołany w lutym 2008 r. w strukturze Departamentu Bezpieczeństwa Teleinformatycznego (DBTI) ABW.
[205] W zakresie współpracy wojskowej odpowiedzialny jest System Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski.
[206] Odnosi się tylko sfery cywilnej.
[207] Inne podmioty (resorty cywilne) – zostały szczegółowo wymienione w Podrozdziale 4.4. niniejszej rozprawy doktorskiej.

CERT/NASK POLSKA (*Computer Emergency Response* Team/Naukowa i Akademicka Sieć Komputerowa POLSKA), IPC (*Information Protection Center*), Straż Graniczna, Policja, Prokuratura, Biuro Układu z Schengen, operatorzy telekomunikacyjni (Telekomunikacja Polska S.A., UPC, Polkomtel etc) oraz dostawcy usług internetowych.

Realizowane zadania przez wyżej wymienione instytucję zostały przedstawione przez autora w Podrozdziale 4.4.

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:

- CERT GOV.PL;
- Centrum Koordynacyjnym.

Departament Ochrony Informacji Niejawnych Ministerstwa Obrony Narodowej

Realizowane zadania:

- koordynuje i nadzoruje realizację zadań dotyczących ochrony informacji niejawnych oraz ochrony obiektów przez piony ochrony jednostek organizacyjnych podległych Ministrowi Obrony Narodowej;
- sprawuje funkcję kontrolne w zakresie przestrzegania przepisów o ochronie informacji niejawnych oraz obiektów wojskowych;
- określa generalne, organizacyjne i techniczne wymagania dla systemów służących do ochrony informacji niejawnych oraz ochrony obiektów jednostek organizacyjnych podległych Ministrowi Obrony Narodowej.

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego i teleinformacyjnego z:

- Centrum Koordynacyjnym;
- Żandarmerią Wojskową;
- NATO CIRC.

Żandarmeria Wojskowa

Realizowane zadania:

- ochranianie porządku na terenach obiektach jednostek wojskowych (jednostek administracyjnych podległych Ministrowi Obrony Narodowej);
- ochranianie życia oraz mienia wojskowego przed zamachami naruszającymi te dobra;
- ściganie osób, w stosunku do których Żandarmeria Wojskowa jest właściwa oraz ujawnianie i zabezpieczanie dowodów tych przestępstw i wykroczeń;
- zapobieganiu popełnianiu przestępstw i wykroczeń przez osoby w stosunku do których jest właściwa;
- wykonywanie czynności operacyjno – rozpoznawczych;
- wykonywanie czynności procesowych w zakresie i na zasadach przewidzianych w przepisach o postępowaniu karnym;
- poszukiwanie sprawców przestępstw i wykroczeń oraz materiałów zawierających informację niejawną;
- zabezpieczenie śladów i dowodów popełnienia przestępstw i wykroczeń oraz sporządzanie ekspertyz i opinii kryminalistycznych[208].

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:

- Centrum Koordynacyjnym;
- Departamentem Ochrony Informacji Niejawnych.

NATO CIRC

Realizowane zdania:

- udzielenie pomocy zaatakowanym elementom struktur wojskowych oraz cywilnych wojskowych państw członkowskich NATO w bezpiecznym, szybkim i efektywnym usuwaniu skutków incydentów w zakresie zabezpieczeń;
- minimalizowanie wpływu z powodu utraty lub kradzieży informacji (jawnych i niejawnych) lub zakłóceń w usługach i zasobach krytycznych systemów na skutek wystąpienia incydentu;

---

[208] Opracowano na podstawie: [URL - www.zw.wp.mil.pl/index.php?go=zadania] g. 13.30 29.06.2009 r.

- systematyczne reagowanie na podstawie sprawdzonych procedur co spowoduje obniżenie ryzyka związanego z możliwością ponownego wystąpienia incydentu;
- prowadzenie polityki bezpieczeństwa teleinformatycznego. Wydawanie dyrektyw, wytycznych, zaleceń, procedur oraz prowadzenie szkolenia.

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:

- Centrum Koordynacyjnym;
- Centrum Wsparcia Technicznego.

Pion Ochrony Informacji Niejawnych

Realizowane zadania:

- zapewnia przestrzeganie zasad ochrony informacji niejawnych przetwarzanych, przechowywanych i przesyłanych w systemie lub sieci teleinformatycznej, w tym za właściwy obieg dokumentów (wchodzących, wychodzących i nośników informacji);
- zapewnienie bezpieczeństwa fizycznego obszaru, w którym usytuowany jest system;
- zapewnienie dostępu do systemu wyłącznie osobom mającym odpowiednie poświadczenie bezpieczeństwa osobowego;
- organizację szkolenia użytkowników na temat ochrony informacji niejawnych przetwarzanych, przechowywanych i przesyłanych w systemach i sieciach teleinformatycznych;
- przedstawianie kierownikowi jednostki organizacyjnej wniosków i propozycji wynikających z oceny bezpieczeństwa systemów teleinformatycznych przetwarzających informację niejawne.

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego i teleinformacyjnego z:

- Centrum Wsparcia Technicznego.

Inspektor Bezpieczeństwa Teleinformatycznego

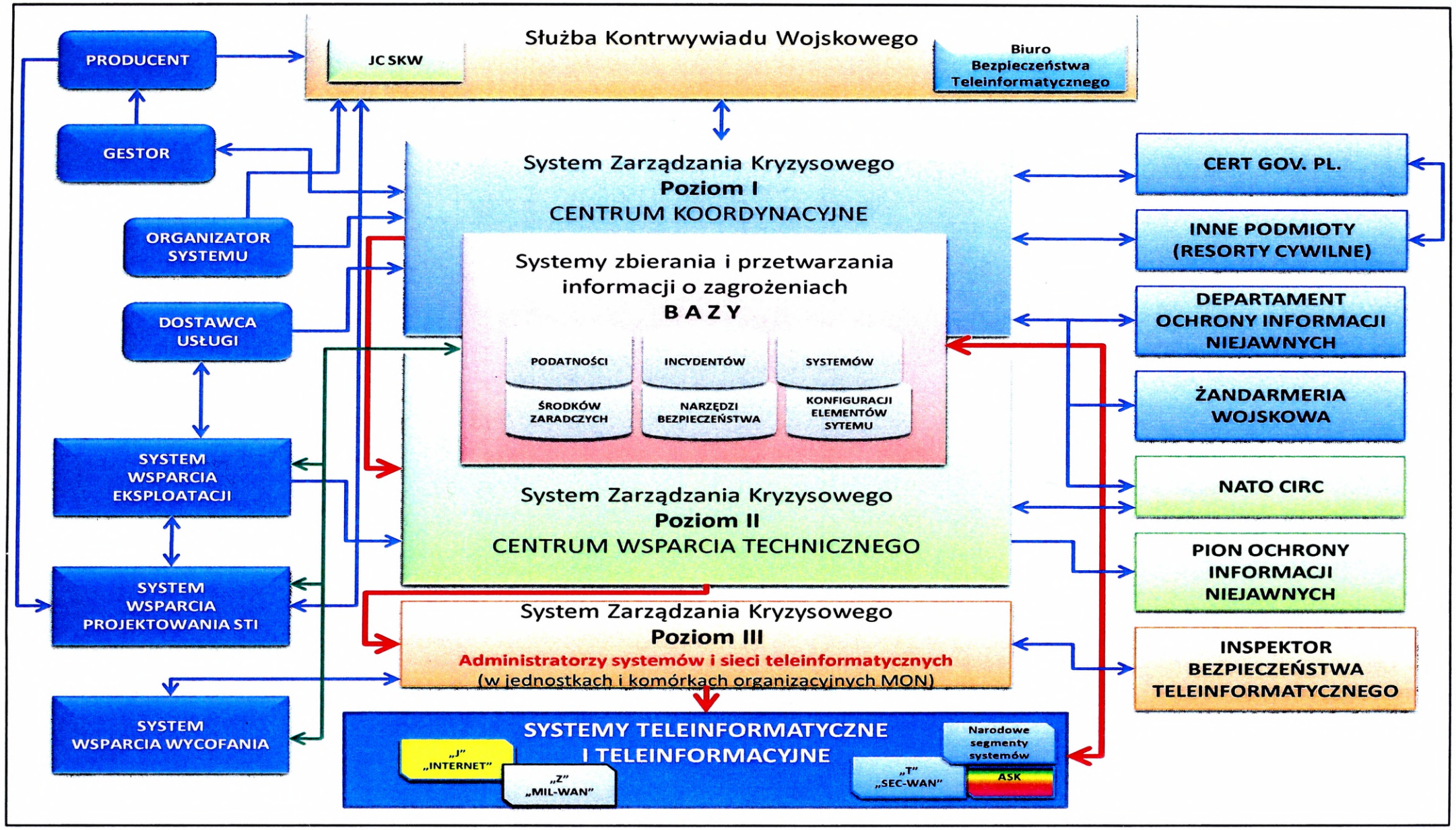
Realizowane zadania:

- uczestniczy w opracowywaniu szczególnych wymagań bezpieczeństwa i procedur bezpieczeństwa (SWB PBE);
- nadzoruje i kontroluje konfigurację systemu, przemieszczenie sprzętu oraz prowadzenie jego ewidencji;
- kontroluje znajomość procedur bezpieczeństwa przez wszystkich użytkowników systemu lub sieci teleinformatycznej;
- prowadzi bieżącą kontrolę zabezpieczeń oraz zgodności funkcjonowania systemu ze SWB PBE;
- prowadzi szkolenia z zakresu bezpieczeństwa teleinformatycznego dla pracowników jednostki organizacyjnej.

Współpraca w zakresie reagowania na incydenty komputerowe i bezpieczeństwa teleinformatycznego z:

- administratorami systemów i sieci teleinformatycznych i teleinformacyjnych w jednostkach i komórkach organizacyjnych Ministra Obrony Narodowej.

Od władz operacyjnych systemów teleinformatycznych wymaga się posiadania odpowiednich zasobów niezbędnych do realizacji powyższych funkcji oraz codziennego funkcjonowania systemu i funkcji zarządzania bezpieczeństwem teleinformatycznym.



Rysunek 4.2. Model trójszczeblowego Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski
Źródło: Opracowanie własne.

4.4. Współpraca z resortami cywilnymi

W instytucjach cywilnych tak jak w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej systemy teleinformatyczne w dobie e - government stale podlegają rozbudowie wraz z ich połączeniami wewnętrznymi (Intranet, Ethernet) i zewnętrznymi. Instytucje te, podczas wypełniania swych zdań statutowych, są coraz bardziej zależne od systemów teleinformatycznych i nie mogą pozwolić sobie na odmowę dostępu do tej usługi. Jak już wspominałem w niniejszej rozprawie doktorskiej, jednym z podstawowych celów Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski jest reagowanie na „incydenty komputerowe" i łagodzenie potencjalnych poważnych skutków związanych z bezpieczeństwem teleinformatycznym. Osiągnięcie tego celu wymaga, aby System Zarządzania Kryzysowego został również skierowany na zaangażowanie oraz ścisłą współprace z wszystkimi resortami cywilnymi uczestniczącymi w systemie obrony państwa[209].

W ramach Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski szeroko idąca współpraca z cywilnymi instytucjami powinna opierać się na bieżącej działalności z niżej wymienionymi podmiotami:

1. Agencja Bezpieczeństwa Wewnętrznego[210].
2. Ministerstwo Spraw Zagranicznych.
3. Ministerstwo Sprawiedliwości.
4. Ministerstwo Edukacji Narodowej.
5. Urząd Komunikacji Elektronicznej.
6. Ministerstwo Spraw Wewnętrznych i Administracji.
7. CERT/NASK POLSKA (*Computer Emergency Response Team*/Naukowa i Akademicka Sieć Komputerowa POLSKA).
8. IPC (*Information Protection Center*).
9. Straż Graniczna.
10. Policja.
11. Prokuratura.
12. Biuro Układu z Schengen.

---

[209] W strukturach Agencji Bezpieczeństwa Wewnętrznego powołano Rządowy Zespół Reagowania na Incydenty Komputerowe – CERT.GOV.PL.

[210] Dokładnie chodzi o: Departament Bezpieczeństwa Teleinformacyjnego Agencji Bezpieczeństwa Wewnętrznego.

13. Operatorzy telekomunikacyjni (Telekomunikacja Polska S.A., UPC, Polkomtel etc).
14. Dostawcy usług internetowych.

Współpraca Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski z wyżej wymienionymi ministerstwami i organizacjami rządowymi oraz pozarządowymi powinna obejmować niżej wymienione obszary działalności:

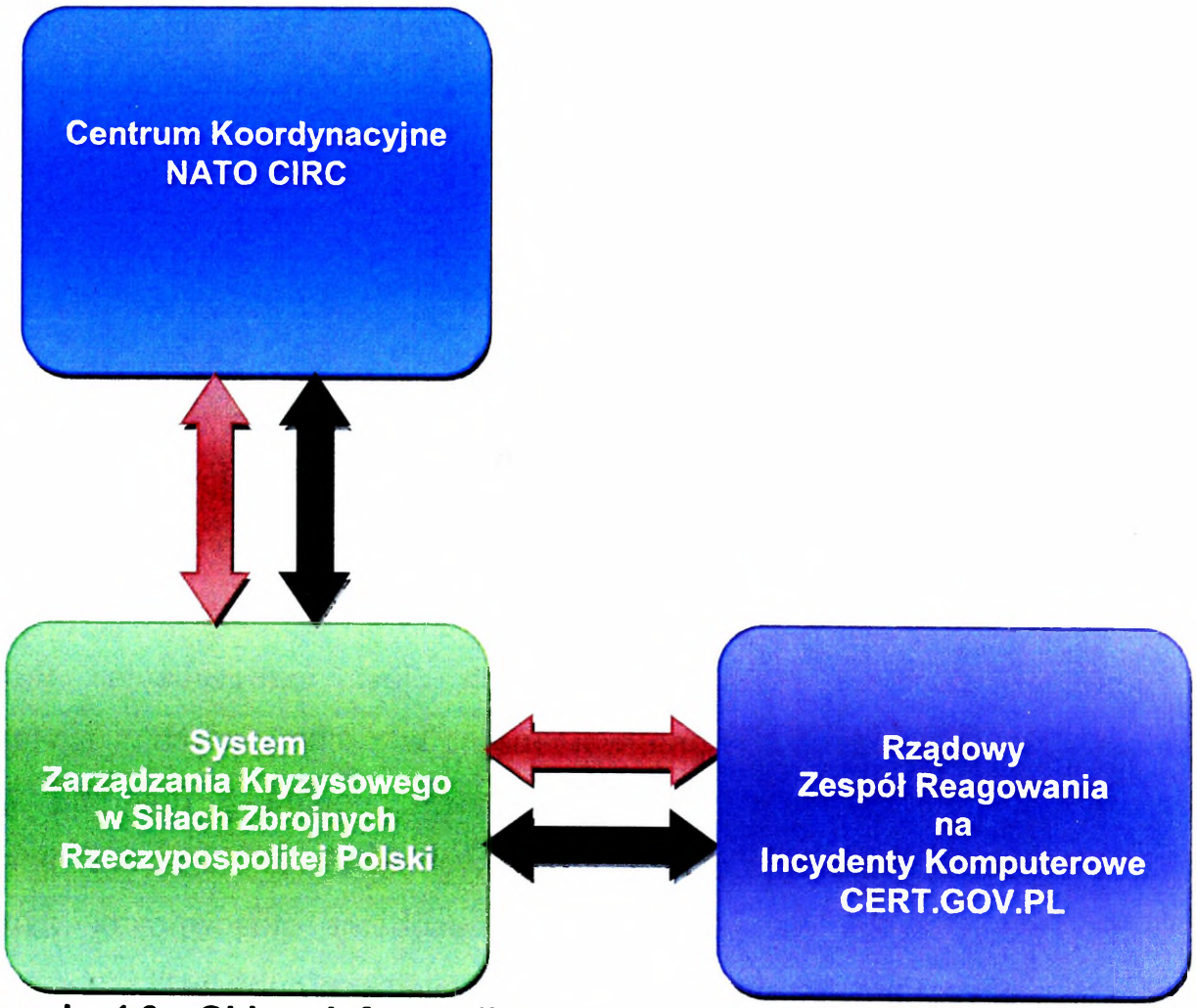
1. Analiza eksploatowanych systemów teleinformatycznych [211] w aspekcie zagrożeń incydentami komputerowymi.
2. Zgłaszanie przypadków wystąpienia incydentów naruszających bezpieczeństwo w systemach teleinformatycznych.
3. Wczesne ostrzeganie o przewidywanych lub zaistniałych zagrożeniach dla Krytycznej Infrastruktury Teleinformatycznej, a także prewencję przeciw ich powstaniu.
4. Identyfikację krytycznych elementów infrastruktury teleinformatycznej, mających wpływ na funkcjonowanie systemów o szczególnym ważnym znaczeniu.
5. Projektowanie i wdrażanie technologii informatycznych służących do zapobiegania powstania incydentów oraz ich wykrywania szkód w infrastrukturze teleinformatycznej po wystąpieniu incydentów.
6. Współdziałanie w wypracowaniu jednolitych metod klasyfikowania incydentów, rejestracji i reagowania w przypadku ich wystąpień.
7. Współdziałanie w opracowaniu zaleceń dotyczących popraw poziomu bezpieczeństwa teleinformatycznego, mających wpływ na funkcjonowanie systemów o szczególnie ważnym znaczeniu.
8. Opracowanie koncepcji możliwości reagowania na incydenty komputerowe w odniesieniu do systemów teleinformatycznych i teleinformacyjnych.
9. Udział w opracowywaniu koncepcji działań oraz projektu podręcznika „Systemu reagowania na incydenty komputerowe".
10. Udostępnianie i wymiana komputerowych baz danych dotyczących incydentów komputerowych.

Poniżej przedstawiam Rysunek 4.3., który przedstawia obieg informacji pomiędzy instytucjami cywilnymi w ramach Systemu Zarządzania Kryzysowego

---

[211] Wymiana informacji jest tu rozumiana bardzo szeroko i obejmuje systemy teleinformatyczne jawne i niejawne w połączeniu z systemami łączności.

w Siłach Zbrojnych Rzeczypospolitej Polski a Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.GOV.PL.



Rysunek 4.3. Obieg informacji jawnej i niejawnej pomiędzy instytucjami cywilnymi w ramach Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski a Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.GOV.PL.

Źródło: Opracowanie własne.

Łączność z ministerstwami i organizacjami rządowymi i pozarządowymi[212] stanowi istotną część Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski. Każda z wymienionych instytucja musi mieć sprawną i szybką łączność[213], umożliwiającą prowadzenie scentralizowanego systemu meldunkowego o incydentach oraz wnioskowania i zapewniania pomocy i informacji o aspektach odnoszących się do zagadnień bezpieczeństwa.

Podczas analizowania dokumentów źródłowych stwierdzam, że zadania Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski pokrywają się z zadaniem realizowanym przez Agencję Bezpieczeństwa

[212] Instytucje te znajdują się przy Rządowym Zespole Reagowania na Incydenty Komputerowe.
[213] Zapewnienie niejawnych (bezpiecznych) środków łączności i przesyłania danych.

Wewnętrznego. Utworzenie Rządowego Zespołu Reagowania na Incydenty Komputerowe – CERT.GOV.PL, będącego platformą wymiany doświadczeń oraz formalnych działań prowadzanych przez Agencję Bezpieczeństwa Wewnętrznego i Policję przy współpracy CERT/NASK POLSKA, operatorów telekomunikacyjnych i dostawców usług internetowych[214]. Stąd też nieodzownym staje się wspólne działanie na płaszczyźnie wojskowo - cywilnej. Powinno one w istotnym stopniu ograniczyć wszelkiego rodzaju „cyberataki"[215], czy też umyśle fałszowanie i blokowanie informacji.

4.5. Teleinformatyczna i teleinformacyjna infrastruktura Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski

Zadaniem środków teleinformatycznych jest zapewnienie tajności, integralności i dostępności przetwarzanej w chronionych systemach teleinformatycznych i teleinformacyjnych informacji, ponieważ ma ona wpływ na przebieg procesu dowodzenia w Siłach Zbrojnych RP. Zagrożenia dla informacji mogą wykorzystać podatności związane z zasobami stosowanymi zarówno w procesach przetwarzania informacji, jak i w procesach ochronnych[216].

Zdolność prawidłowej, niezawodnej i bezpiecznej łączności z jednostkami organizacyjnymi podległymi Ministrowi Obrony Narodowej, cywilnymi instytucjami oraz organizacjami łącznie z sojuszniczymi NATO CERT, stanowi istotną część Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski. Każda instytucja cywilna i jednostka wojskowa potrzebuje sprawnej, szybkiej i bezpiecznej łączności z Systemem Zarządzania Kryzysowego Sił Zbrojnych Rzeczypospolitej Polski by prowadzić scentralizowany system meldunkowy dotyczący incydentów oraz zapewniania pomocy i informacji o aspektach odnoszących się do bezpieczeństwa teleinformatycznego. Z uwagi na charakter informacji[217], łączność będzie wymagała zapewnienia bezpiecznych środków łączności i przesyłania danych, czyli urządzeń ochrony kryptograficznej

---

[214] CERT.GOV.PL ściśle współpracuje z: ABW, MSWiA, WBBŁiI oraz CERT Polska.
[215] Chodzi tu o ataki cyberterrorystyczne, hackerskie i crackerskie.
[216] Liderman K., *Analiza ryzyka i ochrona…, op.cit.*, s. 183.
[217] Informacja związana z incydentami, jest informacją wrażliwa stanowiąca tajemnice służbową i państwową.

zapewniających utajnienie informacji do klauzuli ŚCISLE TAJNE (NATO COSMIC TOP SECRET).

Zorganizowana infrastruktura teleinformatyczna powinna funkcjonować bez obawy utraty informacji. Obecnie w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej wykorzystywany jest nie wszędzie nowy sprzęt teleinformatyczny.. Kierownicy jednostek organizacyjnych nie tylko swoje możliwości ale również przepisy związane z bezpieczeństwem informacji[218].

Zorganizowana infrastruktura teleinformatyczna na potrzeby Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski wymaga ochrony w zakresie organizacyjnym jak i technicznym. Urządzeniom technicznym przekazującym informację stawiane są wymagania dotyczące zabezpieczenia przekazywanych za ich pomocą informacji. Urządzenia zastosowane w sieciach teleinformatycznych, przez które przekazywane są wiadomości, muszą mieć zabezpieczenia uniemożliwiające zdobycie tych wiadomości przez osoby niedopuszczone i nieuprawnione. Odpowiedni sposób przekazywania informacji, identyfikacja urządzeń teleinformatycznych, identyfikacja połączeń oraz zabezpieczenia techniczne użytkowanego sprzętu powoduje stworzenie przeszkód dla osób nieuprawnionych i niedopuszczonych, skutecznie i trwale ochraniając informację.

4.5.1. Systemy teleinformatyczne

ARAKIS – GOV (AgRegacja Analiza i Klasyfikacja Incydentów Sieciowych)[219] - jest systemem wczesnego ostrzegania o zagrożeniach sieciowych w oparciu o monitorowany ruch w sieci oraz informacje ze źródeł zewnętrznych. Jego funkcjonalność to przede wszystkim:

- stworzenie rozproszonego systemu wykrywania zagrożeń obejmującego swym zasięgiem sieci WAN;
- stworzenie unikalnego obrazu stanu bezpieczeństwa teleinformatycznego polskich zasobów sieci Internet;

---

[218] Frączek M., *Uwarunkowania techniczne bezpieczeństwa informacji w środowisku sieciocentrycznym*, Zeszyty Naukowe Nr 3 (68)A, AON, Warszawa 2007 r.

[219] System jest rozmieszczony w 50 jednostkach organizacyjnych administracji publicznej. Należy nadmienić, że sonda systemu nie jest jeszcze zamontowana w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej.

- wykrywanie i informowanie o nowych zagrożeniach w sieci, które nie posiadają jeszcze swoich charakterystycznych wzorców;
- opis zagrożeń w formie sygnatur, zapewniający środek ochronny który może być wykorzystany w systemach wykrywania – prewencji włamań;
- analiza trendów związanych z zagrożeniami;
- korelacja informacji dotyczących zdarzeń z różnych typów źródeł systemowych i sieciowych oraz rożnych instytucji uczestniczących w systemie[220].

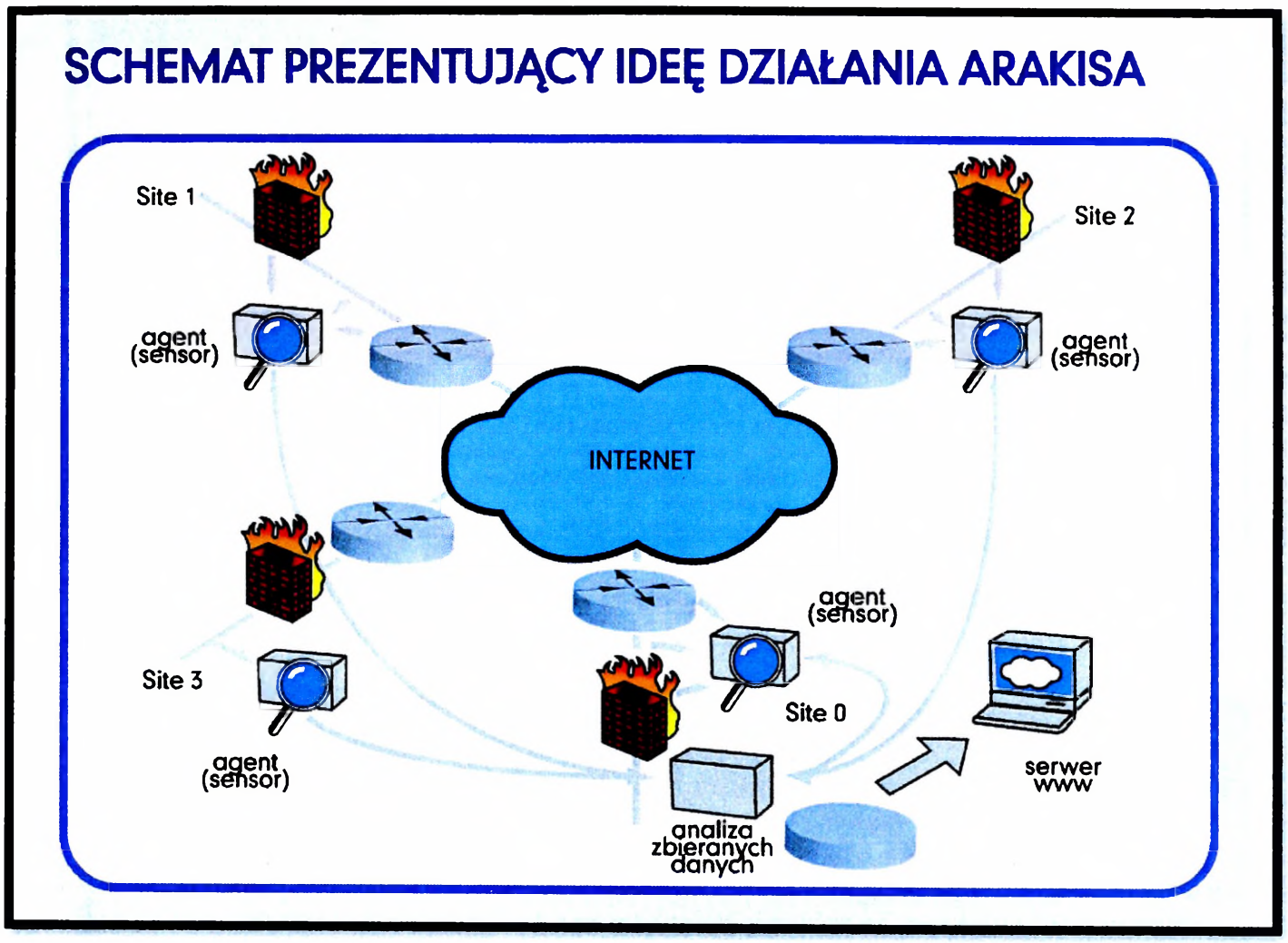
System obecnie jest w stanie wykrywać i opisywać zagrożenia, które cechują się skanowaniem jako metodą wyboru celu. Dwa podstawowe problemy, które system musi uwzględnić w przyszłości to ataki polimorficzne[221] oraz fakt, że zarówno obecny jak i w przyszłości wiele zagrożeń propagować się będzie w sposób pasywny (np. przez przeglądarki), stąd konieczność aby system sam wyszukiwał zagrożenia (np. emulując przeglądarki) a nie czekał, aż zagrożenie same przyjdą do niego. Obecnie ataki polimorficzne mogą być wykryte przez system ale nie w pełni opisane. Celem kolejnego etapu projektu jest dodanie do systemu możliwości wykrywania obydwu powyższych nowych zagrożeń[222].

---

[220] W systemie w chwili obecnej jest 50 instytucji związanych z Infrastrukturą Krytyczną Państwa. Kolejnych 25 instytucji jest przygotowanych do instalacji w tym roku (2009 r.), przy czym nie dotyczy to Ministerstwa Obrony Narodowej.

[221] Atak polimorficzny (ang. *polymorphic shellcode exploit attaca*)- złośliwy program tego rodzaju stosuje szyfrowanie – zazwyczaj jest to szyfrowanie samego złośliwego programu za pomocą procedury szyfrującej, a następnie zmienianie klucza deszyfracji przy każdej mutacji. Tak więc, aby uniknąć wykrycia, wirusy polimorficzne wykorzystują nieograniczoną liczbę procedur szyfrujących. Przy replikacji następuje zmiana fragmentu kodu szyfrującego. Ładunek oraz inne działania złośliwe mogą korzystać z szyfrowania, bądź nie – zależy to od złośliwego kodu. Zazwyczaj występuje tu silnik mutacji, samodzielny składnik programu szyfrującego, który generuje losowe procedury szyfrujące. Zarówno ów silnik, jak i złośliwy program są następnie szyfrowane, zaś nowy klucz deszyfracji przekazywany jest wraz z nimi dalej.

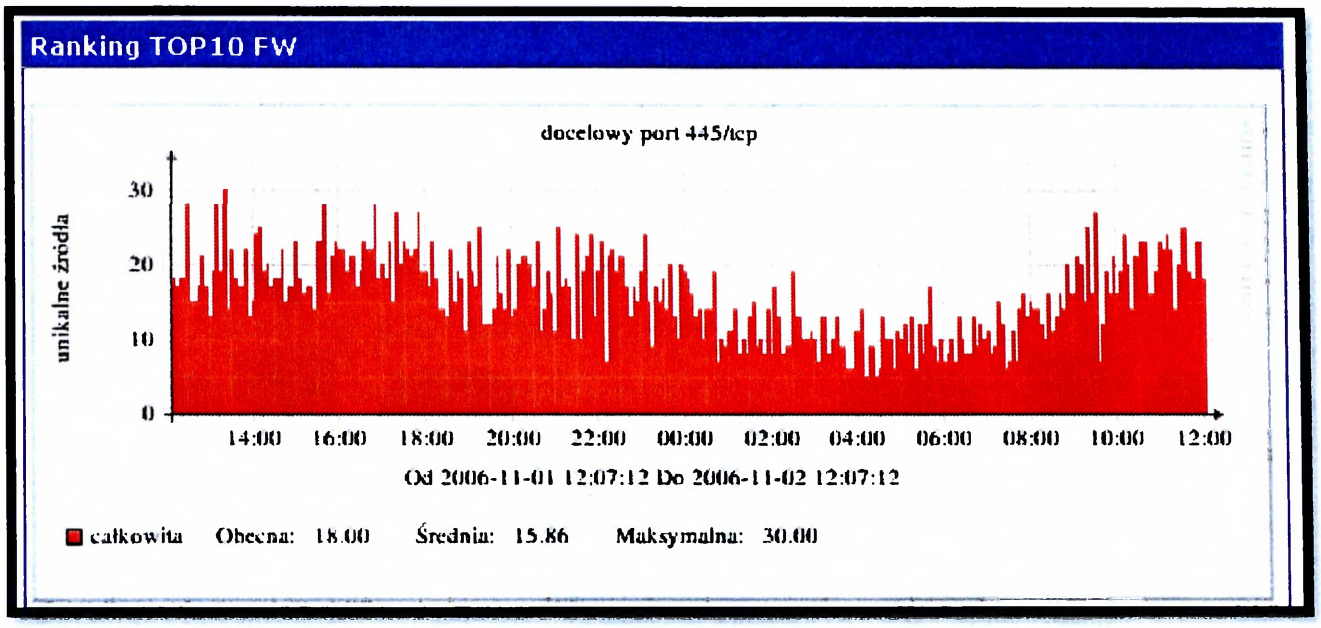
[222] NASK, Zespól CERT Polska – Materiał reklamowy projektu ARAKIS.



Rysunek 4.4. Schemat prezentujący ideę działania systemu ARAKIS
Opracowanie na podstawie: NASK, Zespól CERT Polska – Materiał reklamowy projektu ARAKIS.

Działanie systemy ma umożliwić zwiększenie kompetencji wiedzy w zakresie zagrożeń sieciowych oraz polepszenie trafności wyboru środków ochrony sieci w instytucjach rządowych. Korelacja informacji pozwala na uzyskanie unikatowej wiedzy, wynikającej z możliwości porównania sytuacji lokalnej z globalną sytuacja z sieci. Dodatkowo, gromadzone informacje mogą być wykorzystane do i grupowania źródeł ataku oraz do wspomagania analizy po włamaniowej sieci, rozszerzając przez to możliwości wczesnego ostrzegania.

Chociaż system ma na celu wykrywanie zagrożeń w sposób automatyzowany, umożliwiając także wykonanie ręcznej analizy danego zagrożenia przez użytkownika systemu, poprzez prezentacje w formie wykresów, map i tabel różnorodnych informacji związanych ze zdarzeniami w sieci.

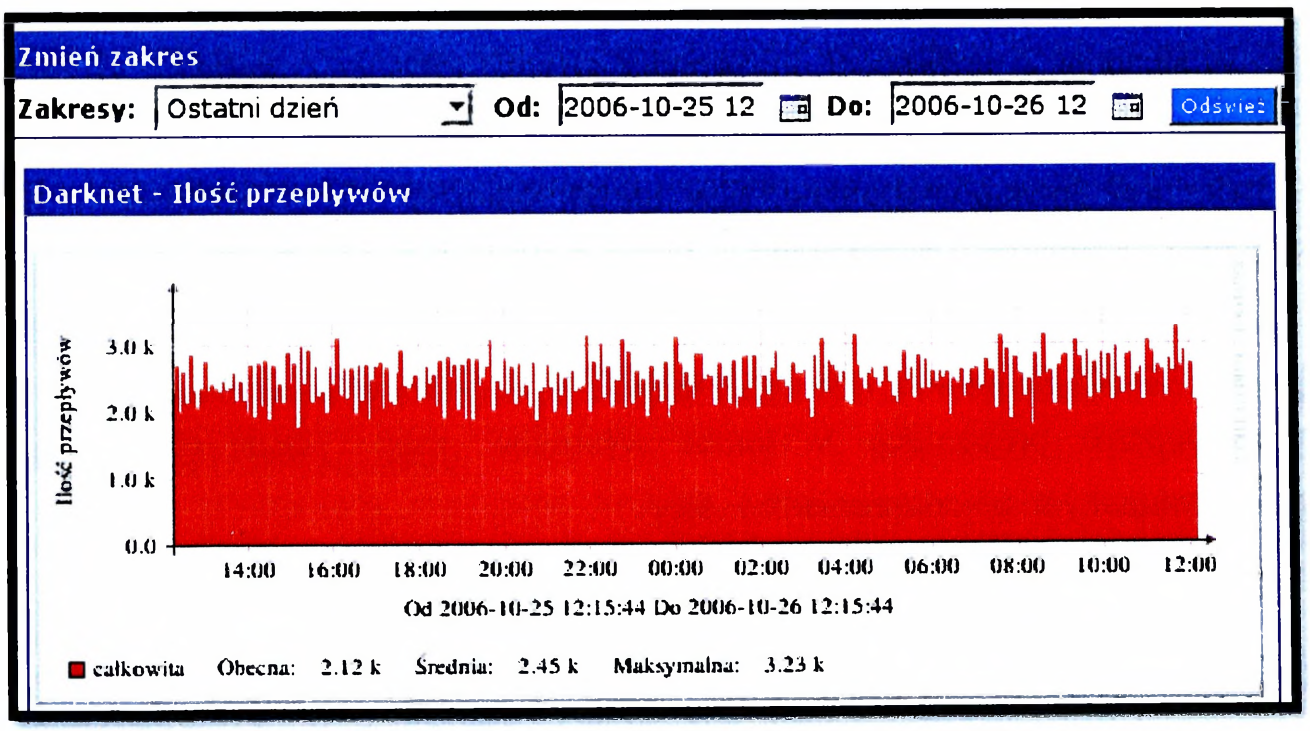


Rysunek 4.5. Ranking TOP10 dla firewalli w systemie ARAKIS
Opracowanie na podstawie: NASK, Zespól CERT Polska – Materiał reklamowy projektu ARAKIS.

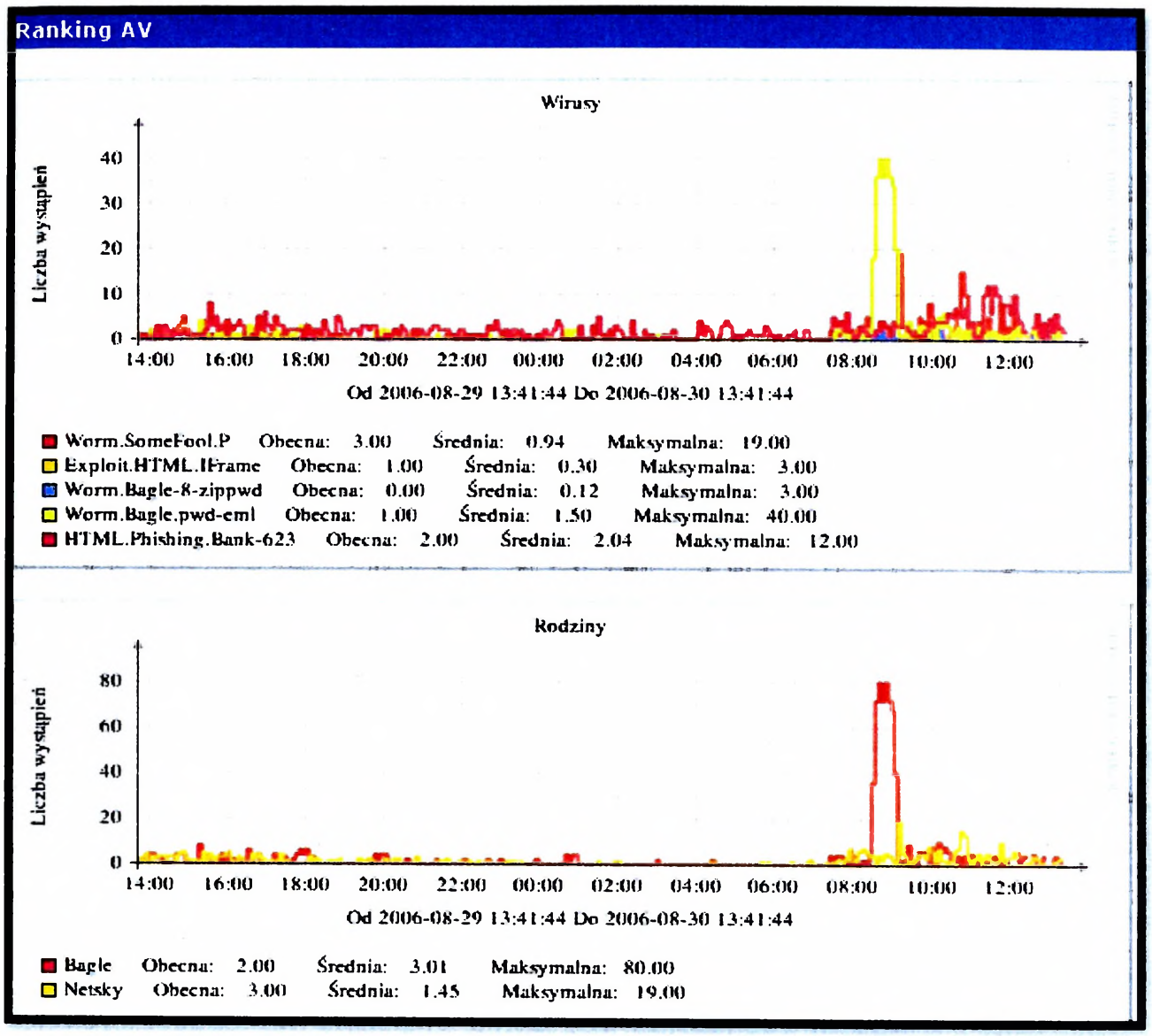
Przeplywy Wszystkich: 100

Data	Adres źródła	Port źr.	Adres celu	Port d.	Protokół	Sensor	System operacyjny
2006-08-29 13:34:43	62.64.120.197	1437	XXX.XXX.245.14	53	udp	XXX.XXX.243.230	
2006-08-29 13:34:43	153.19.178.10	32780	XXX.XXX.245.14	53	udp	XXX.XXX.243.230	
2006-08-29 13:34:46	213.199.204.4	4649	XXX.XXX.245.14	53	udp	XXX.XXX.243.230	
2006-08-29 13:34:47	194.204.152.32	32768	XXX.XXX.245.13	53	udp	XXX.XXX.243.230	
2006-08-29 13:34:48	213.199.204.50	2336	XXX.XXX.245.14	53	udp	XXX.XXX.243.230	
2006-08-29 13:34:49	195.150.20.131	3353	XXX.XXX.245.14	53	udp	XXX.XXX.243.230	
2006-08-29 13:34:51	153.19.178.10	32772	XXX.XXX.245.14	53	udp	XXX.XXX.243.230	
2006-08-29 13:34:51	213.199.204.50	2336	XXX.XXX.245.13	53	udp	XXX.XXX.243.230	

Rysunek 4.6. Przepływy w systemie ARAKIS.
Opracowanie na podstawie: NASK, Zespól CERT Polska – Materiał reklamowy projektu ARAKIS.



Rysunek 4.7. Ilości przepływu w systemie ARAKIS.
Opracowanie na podstawie: NASK, Zespól CERT Polska – Materiał reklamowy projektu ARAKIS.



Rysunek 4.8. Wykres wirusów w systemie ARAKIS.
Opracowanie na podstawie: NASK, Zespól CERT Polska – Materiał reklamowy projektu ARAKIS.

Kontynuując proces wdrażania kolejnych sond systemu ARAKIS – GOV, a także rozwoju i zwiększania funkcjonalności tego systemu, w celu jak najszerszego wykorzystania potencjału systemu ARAKIS – GOV, w latach 2009 – 2009 r. programem objęte zostaną wszystkie elementy krytycznej infrastruktury teleinformatycznej w administracji publicznej i sieci wchodzącej w skład krytycznej infrastruktury teleinformatycznej państwa poza administracją publiczną[223].

[223] *Rządowy program ochrony cyberprzestrzeni RP na lata 2009 – 2011*, Założenia, Warszawa, marzec 2009 r. s. 20.

4.5.2. Ochrona kryptograficzna Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski

W każdym systemie teleinformatycznym, wojskowym czy cywilnym należy szczególną uwagę zwrócić na bezpieczeństwo i ochronę informacji. Kryptografia jest nauką zajmującą się metodami utajniania informacji, czyli jej szyfrowania i odszyfrowywania (ochrona kryptograficzna). Stosowanie w systemie ochrony kryptograficznej pozwoli na zabezpieczenie w sposób należyty ochrony informacji jak i całego systemu.

Ochrona kryptograficzna[224] jest dziedziną informacji która nie powinna być udostępniana dla każdego i dlatego z uwagi na charakter oraz klauzulę rozprawy doktorskiej podrozdział ten zostanie potraktowany w formie informacyjnej. W przypadku Sił Zbrojnych Rzeczypospolitej Polskiej oraz Systemu Zarządzania Kryzysowego w SZ RP znaczenie kryptografii jest bardzo ważne i trudne do wyobrażenia, dlatego zarówno obecnie jak i w latach przyszłych będzie wzrastała liczba urządzeń ochrony kryptograficznej które zabezpieczą prawidłowy obieg informacji w sposób niemożliwy lub wielce utrudniony do rozszyfrowania przez osoby nie uprawnione do zapoznawania się z daną informacją.

Czynnikiem mającym zasadnicze znaczenie powinien być czas żywotności danej informacji, co odnosi się do odpowiedzi na pytanie: po jakim czasie może uznać, iż informacja odczytana przez osoby nieuprawnione może wpłynąć na nasze działanie. Jest to nieodzownie związane z mocą kryptograficzną danego urządzenia ochrony kryptograficznej. W Systemie Zrządzenia Kryzysowego do przesyłania informacji w relacjach narodowych i sojuszniczych powinny być zamontowane urządzenia ochrony kryptograficznej o minimalnej mocy kryptograficznej POUFNE (NATO CONFIDENTIAL), a preferowane będą urządzenia ochrony kryptograficznej klauzuli ŚCISLE TAJNE (NATO COSMIC TOP SECRET).

Należy nadmienić, że obecnie w Siłach Zbrojnych RP jest brak wystarczającej ilości urządzeń ochrony kryptograficznej do prawidłowej ochrony informacji powyżej klauzuli ZASTRZEŻONE (NATO RESTRICTED). Ten niedobór techniczny nadrabiany jest odpowiednią stroną organizacyjną.

Jednocześnie, trzeba podkreślić jak już zostało przedstawione w Rozdziale III niniejszej rozprawy, powinna nastąpić standaryzacja w zakresie bezpieczeństwa

---

[224] Z ochroną kryptograficzną nieodłącznie związane jest bezpieczeństwo teleinformatyczne.

teleinformatycznego (ochrony kryptograficznej) pomiędzy Służbą Kontrwywiadu Wojskowego a Agencją Bezpieczeństwa Wewnętrznego.

4.6. Kierunki rozwoju systemu zarządzania kryzysowego

Do głównych kierunków rozwoju Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski należy zaliczyć:

1. Zdefiniowanie szczegółowo Infrastruktury Krytycznej w Siłach Zbrojnych Rzeczypospolitej Polski według hierarchii:
   - żywotne;
   - krytyczne;
   - wrażliwe;
   - podstawowe.
2. Określenie w ramach Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski priorytetów działania. Można podzielić priorytety działania na[225]:
   - ochronę bezpieczeństwa teleinformatycznego cyberprzestrzeń), z rozróżnieniem konstruowania zabezpieczeń systemowych oraz bezpośrednim reagowaniem na „incydenty";
   - ochronę fizyczną Infrastruktury Krytycznej;
   - ochronę techniczną i elektromagnetyczną Infrastruktury Krytycznej;
   - ochronę osobową Infrastruktury Krytycznej;
   - bezpieczeństwo funkcjonowania jednostek organizacyjnych podległych Ministrowi Obrony Narodowej.
3. Ciągłe i systematyczne zbieranie i udostępnianie informacji o zagrożeniach i środach ochrony dotyczących Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski.
4. Budowa systemów łączności jawnych i niejawnych[226] pomiędzy Systemem Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski a ministerstwami i organizacjami rządowymi i pozarządowymi[227].

---

[225] Jest to oczywiście propozycja podziału priorytetów.
[226] Chodzi tu o systemy teleinformatyczne systemy łączności radiowej i satelitarnej.
[227] Nazywanych czasami jako „infostrady rządowe".

5. Większa dostępność środków ochrony bezpieczeństwa teleinformatycznego (badania i certyfikacja wyrobów w instytucjach odpowiedzialnych za certyfikację wyrobów)[228] dla wszystkich podmiotów uczestniczących w Systemie Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski.
6. Budowa ośrodków zapasowych i outsourcing (bazy danych dla systemów teleinformatycznych).
7. Zdefiniowanie kategorii incydentów[229].
8. Ustalenie procedur zgłaszania incydentów przez podmioty (ministerstwa i organizacje rządowe oraz pozarządowe) do Systemu Zarządzania Kryzysowego Sił Zbrojnych Rzeczypospolitej Polski i odwrotnie.
9. Utworzenie grup eksperckich i baz danych ekspertów z zakresu poszczególnych sektorów Infrastruktury Krytycznej w Siłach Zbrojnych Rzeczypospolitej Polski.
10. Uruchomienie prac nad szczegółowymi planami operacyjnymi w zakresie ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.
11. Szkolenie i uświadamianie młodzieży - bezpieczeństwo teleinformatyczne w programach szkół ponadpodstawowych.
12. Systematyczne gromadzenie i analizowanie danych na temat przestępstw związanych z używaniem komputerów, włączając w to zarówno odpowiednio zmodyfikowane statystyki „cyber przestępczości", jak również informacje o sposobach działania sprawców przestępstw, dotyczące w szczególności aspektów technicznych. Istotne znaczenie będą miały dane wywiadowcze na temat grup terrorystycznych (przestępczych) i przygotowywanych przez nich zamachów na Infrastrukturę Krytyczną w Siłach Zbrojnych Rzeczypospolitej Polski i Infrastrukturę Krytyczną Państwa.
13. Opracowanie programów szkolenia dla jednostek organizacyjnych podległych Ministrowi Obrony Narodowej w zakresie ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Szkolenie żołnierzy zawodowych i pracowników cywilnych wojska z zakresu ochrony bezpieczeństwa teleinformatycznego.
14. Realizacja programów szkoleń pracowników organów ścigania i wymiaru sprawiedliwości w celu podnoszenia poziomu wiedzy funkcjonariuszy policji,

---

[228] W myśl Ustawy z dnia 22 stycznia 1999 r. *O ochronie informacji niejawnych* Tekst ujednolicony po zmianach z dnia 15 kwietnia 2005 r. Dz. U. 1999.11.95; Tekst ujednolicony Dz. U. 2005.196.1631 – akty zmieniające; Art. 60 – odpowiedzialne za certyfikacje są odpowiednie Służby Ochrony Państwa (Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego).

[229] Można to dokonać na podstawie NATO CIRC.

żandarmerii wojskowej, prokuratorów i sędziów na temat technik ścigania przestępstw komputerowych, metod gromadzenia dowodów elektronicznych tych przestępstw oraz ich procesowego wykorzystania.

15. Zainicjowanie szeroko idących naukowych programów badawczych z zakresu ochrony Infrastruktury Krytycznej w Siłach Zbrojnych Rzeczypospolitej Polski.

4.7. Wnioski

1. System Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski powinien być zgodny z założeniami NATO CIRC (NATO Computer Incydent Response Capability). Powinien być zorganizowany w trzypoziomową strukturę (na wzór NATO CIRC).
2. System Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski wymaga współpracy wszystkich jednostek organizacyjnych podległych Ministrowi Obrony Narodowej oraz resortów cywilnych uczestniczących w systemie ochrony państwa.
3. Jednolita ochrona poufności, integralności i zapewnionej dostępności do informacji, stanowią główne czynniki dla potrzeby posiadania przez Siły Zbrojne RP Systemu Zarządzania Kryzysowego.
4. System Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski musi wpierać wszystkie systemy teleinformatyczne Sił Zbrojnych RP oraz reagować w porę wspierając wszystkie instytucje podległe Ministrowi Obrony Narodowej.
5. W ramach Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski współpraca z resortami cywilnymi musi opierać się na niezakłóconej bieżącej działalności.
6. W Systemie Zrządzenia Kryzysowego z uwagi na charakter informacji, do przesyłania danych w relacjach narodowych i sojuszniczych powinny być zamontowane urządzenia ochrony kryptograficznej o minimalnej mocy kryptograficznej POUFNE (NATO CONFIDENTIAL), a preferowane będą urządzenia ochrony kryptograficznej klauzuli ŚCISLE TAJNE (NATO COSMIC TOP SECRET).
7. Uruchomienie prac nad szczegółowymi planami operacyjnymi w zakresie ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.

8. Zainicjowanie szeroko idących naukowych programów badawczych z zakresu ochrony Infrastruktury Krytycznej w Siłach Zbrojnych Rzeczypospolitej Polski.

ZAKOŃCZENIE

W celu uzyskania pełnego obrazu bezpieczeństwa informacyjnego w warunkach zagrożeń cyberterrorystycznych dla Sił Zbrojnych Rzeczypospolitej Polski w XXI wieku, niezbędna jest refleksja dotycząca kilku kwestii zasadniczych, wobec Sił Zbrojnych RP. Wśród wielu wyzwań, za najważniejsze dla Sił Zbrojnych RP należy uznać:

1. Eskalację nacjonalizmu i fundamentalizmu religijnego, zjawiska szczególnie niepokojące w krajach o wysokim odsetku ludności pochodzenia islamskiego.
2. Nasilający się terroryzm międzynarodowy o nieobliczalnych skutkach, wpływający bezpośrednio i pośrednio na kształt stosunków międzynarodowych i spójność sojuszniczą. Istotną grupę przeciwników stanowić będą nowe jakościowo grupy terrorystyczne i przestępcze. Dzięki postępowi w zakresie technologii informacyjnych, otwarciu granic, swobodniejszemu przepływowi kapitału oraz postępowi w dziedzinie komunikacji i transportu, grupy te zyskają zupełnie nowe możliwości działania (ataki cyberterrorystyczne) oraz międzynarodowe znaczenie.
3. Wzrost przestępczości w cyberprzestrzeni, przeradzającej się w cyberterroryzm, przełamujący dotychczasowe „tradycyjne" incydenty komputerowe w kierunku zsynchronizowanych uderzeń na systemy teleinformatyczne i teleinformacyjne przy jednoczesnym zróżnicowaniu typów i metod ataków. W przeciwieństwie do ataków konwencjonalna ataki cyberterrorystyczne (cyberataki) mogą być przeprowadzone z odległości tysięcy kilometrów, co minimalizuje ryzyko przyłapania sprawców.
4. Zwiększającą się rolę technologii teleinformatycznych, globalizację systemów informacyjnych, która sprawia, ze informacja staje się jednym z zasadniczych zasobów strategicznych, a jej właściwe wykorzystanie niesie szansę rozwiązania niektórych dylematów związanych z bezpieczeństwem informacyjnym.
5. Przygotowanie systemu dowodzenia i systemu wsparcia dowodzenia do działania w warunkach wrogich działań w cyberprzestrzeni. Doświadczenia

Estonii i Gruzji świadczą o tym, że to nie jest już futurologia. Sprostanie nowym wyzwaniom w zakresie przebudowy systemu dowodzenia wymaga zmiany mentalności dowódców i sztabowców oraz mocnego zainwestowania w systemy teleinformatyczne i teleinformacyjne. Era odrębnych systemów dowodzenia, rozpoznania, obserwacji i kierowania uzbrojeniem przechodzi do historii, ustępując miejsca zintegrowanemu systemowi gwarantującemu jednoczesne pozyskiwanie i zobrazowanie informacji w czasie rzeczywistym, wysoce zautomatyzowane wspomaganie procesu podejmowania decyzji, identyfikację przynależności wykrytych obiektów, wybór celów i sposobu ich niszczenia, sterowanie systemami uzbrojenia i wreszcie sprawdzenie wyników działania. System dowodzenia przyszłości to system sieciocentryczny.

Każda rewolucja techniczna wywołuje unowocześnienie instytucji militarnych. Informacja stała się zasobem strategicznym i musi być przedmiotem szczególnej ochrony, zwłaszcza, że liczba rzeczywistych i potencjalnych zagrożeń, jak wykazano w rozprawie, jest znaczna (Rozdział 2).

Przedstawione w niniejszej pracy uwarunkowania dotyczące ochrony bezpieczeństwa teleinformatycznego i teleinformacyjnego przedstawiają obecny stan bezpieczeństwa informacyjnego Sił Zbrojnych Rzeczypospolitej Polski.

Wzrost liczby ataków cyberterrorystycznych połączonych z coraz szerszą inwigilacją dziedzin życia społecznego, wynika z gwałtownego rozwoju systemów teleinformatycznych. Istotną cechą zjawiska cyberterroryzmu jest to, że dla sprawcy nie istnieją granice geograficzne ani polityczne, łatwiej jest zachować anonimowość i zatrzeć ślady działalności.

Tak, jak wielkie są szanse rozwoju „infosfery" i różne nadzieje ludzkości w tej dziedzinie, tak wielkie też wydają się i zagrożenia. Te z nich, które można z dużym prawdopodobieństwem przewidzieć, scharakteryzowano w niniejszej pracy. Najważniejsze jest wdrożenie metod i środków zabezpieczenia, które mogą zwiększyć stopień bezpieczeństwa systemów teleinformatycznych zapewniających prawidłową integrację i niezawodne działanie. Należy unikać szablonowego podejścia do wdrażania architektury bezpieczeństwa teleinformatycznego, przewidywać nieznane obecnie możliwości uzyskiwania dostępu do informacji stanowiących tajemnicę służbową czy państwową. Skuteczność nawet najlepiej zaprojektowanych zabezpieczeń zależy zawsze od czynnika ludzkiego. Potrzeba ochrony informacji w Siłach Zbrojnych Rzeczypospolitej Polski jest uzasadniona

żywotnymi interesami państwa. Dotyczy to przede wszystkim informacji dotyczących najważniejszych dziedzin działalności Sił Zbrojnych Rzeczypospolitej Polski, takich jak:

- rozpoznawanie zagrożeń dla bezpieczeństwa informacyjnego Sił Zbrojnych Rzeczypospolitej Polski;
- funkcjonowanie zintegrowanych systemów kierowania, dowodzenia i wspomagania dowodzenia;
- funkcjonowanie systemu obronnego i organizacji Sił Zbrojnych - elementów stanowiących tajemnicę służbową i państwową.

Nadal, pomimo różnych, przewidzianych stosownymi przepisami bezpieczeństwa, zabezpieczeń dla bezpieczeństwa informacyjnego, najważniejszym czynnikiem pozostaje człowiek, jako wytwórca, użytkownik i odbiorca informacji. To, że strony człowieka istnieje największe zagrożenie dla właściwej ochrony bezpieczeństwa informacyjnego i informacji, zarówno stanowiących tajemnicę państwową jak i służbową.

Również od czynnika ludzkiego zależy właściwa realizacja wdrażania procedur bezpieczeństwa, analizy zagrożeń i zarządzania ryzykiem informacyjnym.

W niniejszej rozprawie, sformułowano hipotezy dotyczące stanu i perspektyw bezpieczeństwa teleinformatycznego Sił Zbrojnych Rzeczypospolitej Polski. Podzielono je na następujące grupy:

1. Hipotezy dotyczące słabych stron polskiego systemu bezpieczeństwa informacyjnego.
2. Hipotezy dotyczące możliwości wdrożenia narzędzi wspomagających politykę bezpieczeństwa informacyjnego państwa.
3. Hipotezy dotyczące zakresu i sposobu realizacji przedsięwzięć zapewniających bezpieczeństwo informacyjne państwa.

Celem weryfikacji przyjętych założeń autor rozprawy przeanalizował przyjęte zmienne, mające wpływ na potwierdzenie lub podważenie hipotez:

Zmienne zależne:

- wartość informacji;
- jakość metod analizy bezpieczeństwa teleinformatycznego;
- jakość metod szkolenia w zakresie bezpieczeństwa teleinformatycznego;
- nakłady na bezpieczeństwo teleinformatyczne.

Zmienne niezależne:

- stan prawny w zakresie bezpieczeństwa teleinformatycznego;
- normy narodowe w zakresie bezpieczeństwa teleinformatycznego;
- kryteria i atrybuty bezpieczeństwa;
- dostosowanie standardów bezpieczeństwa teleinformatycznego Sił Zbrojnych Rzeczypospolitej Polski do wymogów NATO.

Analizując zmienne zależne można wykazać, że w rozprawie przeprowadzono, wywód o determinującej roli informacji na współczesnym polu walki, zarówno pod kątem doboru środków (sensorów) walki informacyjnej, jak efektywności informacji w przebiegu działań bojowych. Jednocześnie zweryfikowano pozytywnie hipotezę o wpływie wykorzystywania narzędzi bezpieczeństwa informacyjnego na realizację zasady uzyskiwania przewagi informacyjnej (dominacji), przy spełnieniu warunku zapewnienia wysokiej jakości wykorzystywanym narzędziom analitycznym i nadaniu wysokiej rangi procesom szkolenia w zakresie bezpieczeństwa informacyjnego. Tym samym potwierdzono hipotezę o potrzebie upowszechnienia nowoczesnych metod analizy zagrożeń bezpieczeństwa informacyjnego jako warunku zapewnienia bezpieczeństwa teleinformatycznego i teleinformacyjnego Sił Zbrojnych Rzeczypospolitej Polski.

Biorąc pod uwagę przyjęte zmienne niezależne wykazano, że legislacyjna strona bezpieczeństwa informacyjnego Sił Zbrojnych Rzeczypospolitej Polski wymaga dalszego dostosowania do odpowiednich wymogów bezpieczeństwa teleinformacyjnego. Uzupełniając aspekt prawny bezpieczeństwa informacyjnego o informacje dotyczące naruszeń bezpieczeństwa i występujących zagrożeń dla systemów teleinformatycznych.

Intensywny rozwój technik teleinformatycznej, dający coraz większe możliwości w zakresie wytwarzania, przetwarzania, niszczenia, przesyłania

i przechowywania informacji – a szczególnie dokumentów niejawnych, nie może się odbywać bez równoległego poszukiwania nowych i bezpiecznych form ochrony systemów teleinformatycznych. Podrozdziały 4.3. i 4.4., potwierdzają potrzebę korelowania rozwoju systemów teleinformatycznych i teleinformacyjnych z procesami zapewnianiającymi ich bezpieczeństwo, co stanowi przesłankę interoperacyjnego związania narodowego systemu bezpieczeństwa informacyjnego[1] z sojuszniczymi.

Formułując wnioski z przeprowadzonych badań związanych z Infrastrukturą Krytyczną w Siłach Zbrojnych Rzeczypospolitej Polskiej i zamieszczonych w niniejszej rozprawie doktorskiej (Załącznik 6), należy stwierdzić, że analiza zagrożeń i zarządzanie ryzykiem stanowią istotne elementy w tworzeniu szczególnych wymagań bezpieczeństwa systemu teleinformatycznych. Otrzymana w wyniku przeprowadzenia tego procesu wiedza umożliwia dobór koniecznych środków ochrony, optymalny zarówno ze względu na wymagania bezpieczeństwa dla informacji niejawnych przetwarzanych w systemie, jak i ze względu na konieczne nakłady finansowe w Infrastrukturze Krytycznej, a dokładniej w Krytycznej Infrastrukturze Teleinformatycznej.

Należy jednak mieć świadomość, że zagrożenia można oszacować i zredukować, ale nie da się go wyeliminować całkowicie.

Biorąc pod uwagę wszelkie możliwe zagrożenia dla bezpieczeństwa informacyjnego (teleinformatycznego) Sił Zbrojnych Rzeczypospolitej Polski można przyjąć, że osiągnięcie całkowitego bezpieczeństwa nie jest możliwe, lecz analiza przewidywanych zagrożeń, przez System Zarządzania Kryzysowego, pozwala przedstawić w sposób kompleksowy zagrożenia dla informacji i określić czynności związane z ich neutralizacją.

Większość zagrożeń pochodzi z niezamierzonych lub celowych działań wewnętrznych, jest wynikiem braku wiedzy i praktyki lub braku świadomości zagrożeń na poziomie użytkownika lub administratora systemu teleinformatycznego.

Korzyścią z zastosowania Systemu Zarządzania Kryzysowego jest wzrost świadomości zagrożeń na wszystkich poziomach jednostek organizacyjnych podległych Ministerstwu Obrony Narodowej, od kierownictwa jednostek organizacyjnych odpowiedzialnych za bezpieczeństwo teleinformatyczne do użytkowników i personelu pomocniczego użytkującego systemy teleinformatyczne. Wzrost świadomości zagrożeń

[1] Mówimy tu o cywilnych i wojskowych systemach teleinformatycznych.

jakie obecnie występują w cyberprzestrzeni wzmacnia bezpieczeństwo informacyjne poszczególnego obiektu, systemu teleinformatycznego i teleinformacyjnego, Sił Zbrojnych Rzeczypospolitej Polski a przede wszystkim państwa.

Należy nadmienić, że wysiłek i wiedza ekspercka, zaangażowane w wykonanie analizy zagrożeń i w zarządzanie ryzykiem informacyjnym (teleinformatycznym) powinny i muszą być postrzegane zawsze równolegle i równoważnie z procesami tworzenia infrastruktury teleinformatycznej i teleinformacyjnej w Siłach Zbrojnych Rzeczypospolitej Polski.

Jeżeli niniejsza rozprawa przyczyni się do wzrostu świadomości roli bezpieczeństwa informacyjnego w systemie bezpieczeństwa Sił Zbrojnych Rzeczypospolitej Polski przy występujących coraz częściej zagrożeniach w cyberprzestrzeni oraz poszerzy wiedzę z przedstawionej tematyki – jej cel zostanie osiągnięty.

BIBLIOGRAFIA

KSIĄŻKI

1. Adamski J., *Nowe technologie w służbie terrorystów*, Collegium Civitas TRIO, Warszawa 2007 r.
2. Aleksandrowicz T., *Terroryzm międzynarodowy*, Wydawnictwa Akademickie i profesjonalne, Warszawa 2008 r.
3. Andrzejewska A., Bednarek J., Sarzała D., *Cyberprzestrzeń – szanse, zagrożenia, uzależnienia*, Fundacja PEDAGOGIUM, Warszawa 2007 r.
4. Apanowicz J., *Metodologia nauk*, Toruń 2003 r.
5. Barber B. R., *Imperium strachu, Wojna, terroryzm i demokracja*, Warszawa 2005 r.
6. Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa 2006 r.
7. Białek T., *Terroryzm manipulacja strachem*, Warszawa 2005 r.
8. Bógdał – Brzezińska A., Gawrycki M. F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, ASPRA - JR, Warszawa 2003 r.
9. Ciborowski L., *Walka informacyjna*, ECE, Toruń, 1999 r.
10. Cieślarczyk M, *Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich*, AON, Warszawa 2006 r.
11. Czaputowicz J., *System czy nieład? Bezpieczeństwo europejskie u progu XXI wieku*, Warszawa 1998 r.
12. Denning D. E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002 r.
13. Dyrcz C., *Terroryzm początku XXI wieku jako zagrożenie bezpieczeństwa międzynarodowego i narodowego*, DMW RP, Gdynia 2005 r.
14. Frączek M., *Uwarunkowania techniczne bezpieczeństwa informacji w środowisku sieciocentrycznym*, Zeszyty Naukowe Nr 3 (68)A, AON, Warszawa 2007 r.
15. Gasparski W., *Projektowanie i systemy*, PAN, Warszawa, 1991 r.
16. Gawliczek P., Pawłowski J., *Zagrożenia asymetryczne*, AON, Warszawa 2003 r.
17. Huhtinen A., *Rantapelkonen J., Imagewars. Beyond the Mask of Information Warfare*, Saarijärvi 2001 r.
18. Janczak J., Świdzikowski G., *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*, AON, Warszawa 2004 r.
19. Jemioło T., *Globalizacja szanse i zagrożenia*, AON, Warszawa 2000 r.
20. Jemioło T., Kisielnicki J., Rajchel K., *Cyberterroryzm nowe wyzwania XXI wieku*, Wyższa Szkoła Policji, Warszawa 2009 r.

21. Jemioło T., Dawidczyk A., *Wprowadzenie do metodologii badań bezpieczeństwa*, AON, Warszawa 2008 r.
22. Kolman R., *Poradnik dla doktorantów i habilitantów*, Bydgoszcz 1996 r.
23. Konieczny J., *Zarządzanie w sytuacjach kryzysowych, wypadkach i katastrofach*, Poznań – Warszawa 2001 r.
24. Konieczny J., *Inżynieria systemów działania*, WNT, Warszawa 1983 r.
25. Koziej S., *Koncepcja wspólnego bezpieczeństwa w Europie a obronność Polski*, Wystarczalność Obronna, Warszawa 1996 r.
26. Koźmiński A. K., *Analiza systemowa organizacji*, WP, Warszawa 1976 r.
27. Kręcikij J., *Działania sieciocentryczne. Wybrane problemy*, AON, Warszawa 2008 r.
28. Krysiak K., *Sieci komputerowe. Kompendium*, HELION, Gliwice 2005 r.
29. Kubiak K., *Wojny konflikty zbrojne i punkty zapalne na świecie*, Warszawa 2005 r.
30. Kubiak K., Makowski A., Mickiewicz P., *Polska wobec zagrożenia terroryzmem morskim*, Warszawa 2005 r.
31. Lehtinen R., Russell D., *Podstawy ochrony komputerów*, HELION, Gliwice 2007 r.
32. Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008 r.
33. Liderman K., *Bezpieczeństwo teleinformatyczne*, IAiR WAT, Warszawa 2001 r.
34. Liderman K., *Podręcznik Administratora bezpieczeństwa teleinformatycznego*, MIKOM, Warszawa 2003 r.
35. Liedel K., *Bezpieczeństwo informacji w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Adam Marszałek, Toruń 2005 r.
36. Liedel K., Piasecka P., *Jak przetrwać w dobie zagrożeń terrorystycznych. Elementy edukacji antyterrorystycznej*, Trio, Warszawa 2007 r.
37. Luis A., *Sieć Al.-Kaida*, Wydawnictwo Wołoszański, Warszawa 2008 r.
38. Łobocki M., *Metody badań pedagogicznych*, PWN, Warszawa 1978 r.
39. Magdi A, *Kamikadze made in Europe Czy zachodowi uda się pokonać islamskich terrorystów?*, UNIVERSITAS, Kraków 2008 r.
40. Majewski T., *Ankieta i wywiad w badaniach wojskowych*, AON, Warszawa 2002 r.
41. Malinowski M. J., Ożarowski R., Grabowski W., *Ewolucja terroryzmu na przełomie XX i XXI wieku*, Wydawnictwo Uniwersytetu Gdańskiego, Gdański 2009 r.
42. McNamara J., *Arkana szpiegostwa komputerowego*, HELION, Gliwice 2004 r.
43. Mitnick K. D., Simon W. L., *Sztuka infiltracji. Czym jak włamywać się do sieci komputerowych. Biblia hakerów*, ALBATROS, Warszawa 2006 r.
44. Mitnick K. D., Simon W. L., *Sztuka podstępu*, HELION, Gliwice 2003 r.
45. Molski M., Łacheta M., *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007 r.
46. Mroziewicz K., *Moc, niemoc i przemoc*, Bydgoszcz – Warszawa 2005 r.
47. Nowacki T., *Metodologia pedagogiki pracy*, WSiP, Warszawa 1978 r.
48. Nowakowski Z., Szafran H., Szafran R., *Bezpieczeństwo w XXI wieku. Strategia bezpieczeństwa narodowego Polski i wybranych państw*, RS DRUK, Rzeszów 2009 r.
49. Osuchowska B., *Poradnik autora, tłumacza i redaktora*, Warszawa 2005 r.

50. Parzymies A., *Islam a terroryzm*, Wydawnictwo Akademickie DIALOG, Warszawa 2003 r.
51. Piątek Z., *Procedury i przedsięwzięcia systemu reagowania kryzysowego*, AON, Warszawa 2005 r.
52. Pieter J., *Praca naukowa*, Śląsk, Katowice 1960 r.
53. Polaczek T., *Audyt bezpieczeństwa informacji*, HELION, Gliwice 2006 r.
54. Posobiec J., *Organizacja dowodzenia w środowisku sieciocentrycznym*, AON, Warszawa 2008 r.
55. Rattray G. J., *Wojna strategiczna w cyberprzestrzeni*, WNT, Warszawa 2004 r.
56. Rokiciński K., *Zagrożenia asymetryczne w rejonie Bałtyckim*, BELSTUDIO, Warszawa 2006 r.
57. Shinder D. L., Tittel E., *Cyber przestępczość. Jak walczyć z łamaniem prawa w sieci*, HELION, Gliwice 2004 r.
58. *Sieci teleinformatyczne w działaniach sieciocentrycznych, Materiały z międzynarodowej konferencji naukowej*, AON, Warszawa 2007 r.
59. Sienkiewicz P., Błażejczyk W., Lichocki E., Jóźwiak M., Świeboda H., *Analiza systemowa cyberterroryzmu zagrożenie dla bezpieczeństwa państwa. Analiza systemowa zagrożeń informatycznych w środowisku bezpieczeństwa państwa,* Wydział Strategiczno – Obronny, AON, Warszawa 2006 r.
60. Sienkiewicz P., Świeboda H., Lichocki E., *Analiza systemowa zjawiska cyberterroryzmu*, Zeszyty Naukowe Nr 2 (63), AON, Warszawa 2006 r.
61. Sienkiewicz P., Mąka D., *Sieciocentryczna infrastruktura procesów decyzyjnych*, Zeszyty Naukowe, Nr 4 (74), AON, Warszawa 2008 r.
62. Sienkiewicz P., *Cykl wykładów: Metodologia badań naukowych*, ASG (AON), Warszawa 1992 r.
63. Sienkiewicz P., *Analiza systemowa. Podstawy i zastosowania*, Warszawa 1994 r.
64. Sienkiewicz P., *Inżynieria systemowa*, Warszawa 1983 r.
65. Sienkiewicz P., *10 wykładów*, AON, Warszawa 2005 r.
66. *Słownik Języka Polskiego*, PWN, Warszawa 1996 r.
67. *Słownik Języka Polskiego*, PWN, Warszawa 2000 r.
68. Soroko P., *Polistrategia bezpieczeństwa zewnętrznego Polski. Ujęcie normatywne*, Warszawa 2005 r.
69. Stachowiak Z., *Metodyka i metodologia pisania prac kwalifikacyjnych*, AON, Warszawa 2001 r.
70. Strebe M., *Podstawy bezpieczeństwa sieci*, MIKOM, Warszawa 2005 r.
71. Sutton R. J., *Bezpieczeństwo telekomunikacji*, WKŁ, Warszawa 2004 r.
72. Szmit M., Tomaszewski M., Lisiak D., Politowska I., *13 najpopularniejszych sieciowych ataków na twój komputer, wykrywanie, usuwanie skutków i zapobieganie*, Helion, Gliwice 2008 r.
73. Szpyra R., *Militarne operacje informacyjne,* AON, Warszawa 2003 r.
74. Szpyra R., *Operacje informacyjne państwa W działaniach sił powietrznych,* Rozprawa habilitacyjna, AON, Warszawa 2002 r.
75. Swiderski F., Synder W., *Modelowanie zagrożeń*, Microsoft, Warszawa 2005 r.
76. *Terroryzm i zamachy samobójcze. Muzułmański punkt widzenia*, praca zbiorowa pod red. Capana Erguna, Wydawnictwo Akademickie DIALOG, Warszawa 2007 r.

77. Verton D., Black Ice – *Niewidzialna groźba cyberterroryzmu*, Gliwice 2004 r.
78. Virilio P., *Bomba informacyjna*, Warszawa 2006 r.
79. Waltz E., *Information Warfare. Principles and Operations*, Boston – London 1998 r.
80. Wojtowicz W., *Bezpieczeństwo infrastruktury krytycznej*, MON DPO, Warszawa 2006 r.
81. Yourdon E., *Wojna na bity*, WNT, Warszawa 2004 r.
82. Żaczyński W., *Praca badawcza nauczyciela*, Warszawa 1995 r.

DOKUMENTY, PUBLIKACJE I OPRACOWANIA

1. Abele – Wigert I., Dunn M., *An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies*, International CIIP Handbook 2006, Vol. I, Center for Security Studies, Swiss Federal Institute of Technology, ETH Zurich.
2. Berkieta P., *Rola i zadania Departamentu Bezpieczeństwa Teleinformacyjnego ABW w kreowaniu polityki ochrony informacji niejawnych*, AON, Warszawa, 04 luty 2005 r.
3. *Cyber Security Dimensions of Critikal Infrastructure Protection*, George C. Marshall European Center For Security Studies, Munich Germany, 25 – 28 October 2005 r.
4. Czerwiński P., *Doświadczenia V Zmiany PKW w Iraku*, „Raport" 2006, nr 05.
5. *Diagnoza społeczna 2005*, praca zbiorowa pod red. Czapiński J., Panek T., Wyższa Szkoła Finansowa i Zarządzania w Warszawie, Warszawa, 10 styczeń 2006 r.
6. *Doktryna Narodowa Operacji Połączonych OP/01*, MON, Sztab Generalny WP, Warszawa, 2002 r.
7. *Doktryna Operacji Informacyjnych SZ RP*, Praca analityczno – badawcza – AB (temat nr 02 – 095), MON, Warszawa, 2003 r.
8. Dyrcz C., *Wybrane problemy terroryzmu XXI WIEKU (2),* „Przegląd Morski" 2005, nr 11.
9. Główny Urząd Statystyczny, *Wykorzystanie technologii informacyjno - telekomunikacyjnych w 2005 r.*, Warszawa, 22 grudzień 2005 r.
10. Główny Urząd Statystyczny, *Wykorzystanie technologii informacyjno - telekomunikacyjnych w 2006 r.*, Warszawa, 17 listopad 2006 r.
11. Główny Urząd Statystyczny, Wykorzystanie technologii informacyjno – telekomunikacyjnych w przedsiębiorstwach, gospodarstwach domowych i przez osoby prywatne w 2008 r., Warszawa, 2009 r.
12. Główny Urząd Statystyczny, Mały rocznik statystyczny Polski 2009, Warszawa 2009 r.
13. Hołdanowicz G., *Stokrotka i NCW*, „Raport" 2005, nr 12.
14. Kiński A., *Nowości Stokrotki 05,* „Nowa Technika Wojskowa" 2005, nr 12.
15. *Kodeks Karny z dnia 2 sierpień 1997 r.*
16. *Konstytucja Rzeczypospolitej Polski z dnia 2 kwiecień 1997 r.*

17. Kośla R., *Reagowanie na incydenty w zakresie zabezpieczeń w systemach teleinformatycznych NATO i administracji publicznej RP,* SECURE 2001, Warszawa, 07 listopad 2001 r.
18. Kośla R., *Ochrona infrastruktury krytycznej w Polsce – aktualny stan prac,* SECURE 2002, Warszawa, 26 listopad 2002 r.
19. Kośla R., *Cyberbezpieczeństwo w infrastrukturze krytycznej – podsumowanie mijającego roku*, Warszawa, 05 listopad 2003 r.
20. Kośla R., *Ochrona krytycznej infrastruktury teleinformatycznej w Polsce – wstęp do dyskusji,* Warszawa, 17 listopad 2004 r.
21. Lichocki E., *Zagrożenie cyberterroryzmem w polityce bezpieczeństwa informacyjnego Polski*, Praca podyplomowa, AON, Warszawa 2005 r.
22. Mejssner B., *Sherlock Holmes w firmowych komputerach*, „Rzeczypospolita" 08 września 2006 r. wydanie 749/210 /7504/, s. dF 4.
23. Ministerstwo Gospodarki, *ePolska. Plan działania na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001 – 2006*, Warszawa, czerwiec 2001 r.
24. Ministerstwo nauki i informatyzacji, *Strategia informatyzacji Rzeczypospolitej Polskiej ePolska na lata 2004 – 2006*, Warszawa, grudzień 2003 r.
25. Ministerstwo Spraw Wewnętrznych i Administracji. Departament Bezpieczeństwa Powszechnego, *Infrastruktura krytyczna w Polsce* – Raport z badań, Warszawa, wrzesień 2002 r.
26. *Modelowanie procesów walki informacyjnej. Model „cyberwar"*, praca zbiorowa pod red. M. Kinasiewicz, AON, Warszawa, 2006 r.
27. *NATO Computer Incident Response Capability (DCI-CC5)*, Annex 1, AC/322-WP/0223- Rev 1.
28. *NATO Computer Incident Response Capability,* Annex 1, AC/322-N/0648.
29. *NATO Computer Incident Response Capability*, Annex 1, AC/322-N/0197 CONOPs.
30. PN – I – 02000: *Zabezpieczenia w systemach informatycznych – Terminologia,* PKN, Warszawa, 1998 r.
31. Podolski A., *Polska Strategia Bezpieczeństwa Narodowego jako praktyczna implementacja Europejskiej Strategii Bezpieczeństwa – między teorią a praktyką, Raporty i Analizy 1/05*, Centrum Stosunków Międzynarodowych, Warszawa, 2005 r.
32. *Progress and Challenges In Securing the Nation's Cyberspace*, Department of Homeland Security Office of Inspector General, Washington DC, July 2004 r.
33. *Przestępczość teleinformatyczna*. Materiały seminaryjne, pod red. A. Misiuka, J. Konińskiego, P. Ciszka, Szczytno, 2003 r.
34. *Przestępczość teleinformatyczna*. Materiały seminaryjne, pod red. J. Konińskiego, Szczytno, 2004 r.
35. *Regulamin działań Wojsk Lądowych (DD/3.2)* - tymczasowy, MON, Sztab Generalny WP, Warszawa, 2006 r.
36. Rotfeld A. D., *Strategia Bezpieczeństwa Narodowego RP w nowych warunkach międzynarodowych: nowe wyzwania, nowe zadania* – przemówienie

na inauguracje roku akademickiego w Akademii Obrony Narodowej, Warszawa, 01 październik 2003 r.
37. *Rządowy program ochrony cyberprzestrzeni RP na lata 2009 – 2011*, Założenia, Warszawa, marzec 2009 r.
38. Sienkiewicz P., *Współczesne koncepcje walki informacyjnej,* AON, Warszawa, 23 styczeń 2003 r.
39. Siwek J., *Zdolność reagowania na incydenty komputerowe Sił Zbrojnych jako forma walki z cyberterroryzmem,* SECURE 2004, Warszawa, 20 październik 2004 r.
40. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej,* Warszawa, 2007 r.
41. Szymański T., *Zagrożenie atakami cyberterrorystycznymi w rejonie nadmorskim Morza Bałtyckiego,* Gdynia, AMW, 2005 r.
42. *The Political – Military Dimensions of Cyber Security*, George C. Marshall European Center For Security Studies, Munich Germany, 15 – 17 March 2004 r.
43. *Trusted Information Sharing Network for Critical Infrastructure Protection, National Counter* – Terrorism Committee, Critical Infrastructure Protection in Australia, Australia 25 March 2003 r.
44. Lt. Gen. Wallace W. S., *Network-Enabled Battle Command, Royal United Services Institute*, Winter 2004/2005 r.
45. *Zielona księga w sprawie europejskiego programu ochrony infrastruktury krytycznej, COM /2005/ 576 końcowy,* Bruksela 17 listopad 2005 r.

REGULACJE PRAWNE

1. Ustawa z dnia 22 stycznia 1999 r. „O ochronie informacji niejawnych" Tekst ujednolicony po zmianach z dnia 15 kwietnia 2005 r. Dz. U. 1999.11.95; Tekst ujednolicony Dz. U. 2005.196.1631 - akty zmieniające;
2. Ustawa z dnia 13 kwietnia 2007 r. „O kompatybilności elektromagnetycznej" Dz. U. 2007.82.556;
3. Ustawa z dnia 16 lipca 2004 r. „Prawo telekomunikacyjne" Dz. U. 2004.171.1800;
4. Ustawa z dnia 18 lipca 2002 r. „O świadczeniu usług drogą elektroniczną" Dz. U. 2002.144.1204;
5. Ustawa z dnia 18 września 2001 r. „O podpisie elektronicznym" Dz. U. 2001.130.1450;
6. Ustawa z dnia 27 lipca 2001 r. „O ochronie baz danych" Dz. U. 2001.128.1402;
7. Ustawa z dnia 6 czerwca 19997 r. „KK/Przestępstwa przeciwko ochronie informacji" Dz. U. 1997.88.553;
8. Rozporządzenie Prezesa Rady Ministrów z dnia 05 października 2005 r. „W sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności a także zmiany nadanej klauzuli tajności" Dz. U. 2005.205.1696;

9. Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. „W sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego" Dz. U. 2005.171.1433;
10. Rozporządzenie Rady Ministrów z dnia 18 października 2005 r. „W sprawie organizacji i funkcjonowania kancelarii tajnych" Dz. U. 2005.208.1741;
11. Rozporządzenie Ministra Obrony Narodowej z dnia 21 czerwca 2007 r. „W sprawie szczegółowych zadań pełnomocników ochrony oraz szczególnych wymagań w zakresie ochrony fizycznej informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych" Dz. U. 2007.126.876;
12. Zarządzenie Nr 25/MON Ministra Obrony Narodowej z dnia 17 listopada 2005 r. „W sprawie szczególnego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, stosowania środków ochrony fizycznej oraz obieg informacji niejawnych";
13. Decyzja Nr 122/MON z dnia 18 marca 2008 r. „W sprawie powoływania w resorcie obrony narodowej pełnomocników i zastępców pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów oraz inspektorów bezpieczeństwa teleinformatycznego";
14. Decyzja Nr 498/MON z dnia 2 listopada 2007 r. „W sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej";
15. Decyzja Nr 485/MON z dnia 29 października 2007 r. „W szczególnej ochrony materiałów kryptograficznych w komórkach organizacyjnych Ministerstwa Obrony Narodowej";
16. Decyzja Nr 448/MON z dnia 4 października 2007 r. „W sprawie trybu akredytacji bezpieczeństwa fizycznego i technicznego pomieszczeń specjalnych";
17. Decyzja Nr 488/MON z dnia 30 listopada 2006 r. „W sprawie wprowadzenia do użytku w resorcie obrony narodowej „Tymczasowej instrukcji organizacji obiegu informacji niejawnych o klauzuli zastrzeżone w resortowej sieci teleinformatycznej MIL-WAN";
18. Decyzja Nr 390/MON z dnia 28 września 2006 r. „W sprawie ograniczeń w używaniu urządzeń do rejestracji, kopiowania lub transmisji obrazu i dźwięku w komórkach i jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych";
19. Decyzja Nr 20/MON z dnia 31 stycznia 2006 r. „W sprawie powoływania pełnomocników, zastępców pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów i sieci teleinformatycznych oraz inspektorów bezpieczeństwa teleinformatycznego w Ministerstwie Obrony Narodowej oraz w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych";
20. Decyzja Nr 21/MON z dnia 31 stycznia 2006 r. „W sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej";
21. Decyzja Nr 22/MON z dnia 31 stycznia 2006 r. „W sprawie szczegółowych zasad i trybu prowadzenia i dokumentowania postępowań sprawdzających oraz wydawania poświadczeń i certyfikatów bezpieczeństwa";

22. Decyzja Nr 23/MON z dnia 31 stycznia 2006 r. „W sprawie szkolenia w zakresie ochrony informacji niejawnych";
23. Decyzja Nr 24/MON z dnia 31 stycznia 2006 r. „W sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej";
24. Decyzja Nr 25/MON z dnia 31 stycznia 2006 r. „W sprawie trybu certyfikacji, recertyfikacji oraz kontroli kancelarii zagranicznych, punktów obsługi dokumentów zagranicznych, kancelarii kryptograficznych, stacji łączności kryptograficznej, kabin kryptograficznych oraz pomieszczeń wydzielonych organizowanych lub funkcjonujących w jednostkach i komórkach organizacyjnych resortu obrony narodowej";
25. Wytyczne Ministra Obrony Narodowej z dnia 23 stycznia 2007 r. „W sprawie ochrony informacji niejawnych oraz obiektów wojskowych w jednostkach organizacyjnych podporządkowanych Ministrowi Obrony Narodowej lub przez niego nadzorowanych w 2007 r.";
26. Instrukcja organizacji prowadzenia gospodarki materiałowo - technicznej sprzętu i oprogramowania informatycznego w resorcie obrony narodowej Sygn. Łączn. 1012/2004;
27. Zarządzenie Szefa Sztabu Generalnego WP z dnia 26 stycznia 2000 r. „W sprawie opracowywania Szczególnych Wymagań Bezpieczeństwa";
28. „Metodyka opracowywania szczególnych wymagań bezpieczeństwa dla systemów lub sieci teleinformatycznych" - wprowadzona zarządzeniem Szefa Sztabu Generalnego WP z dnia 26 stycznia 2000 r.
29. „Zalecenia w sprawie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych" – BTPO – 701B;
30. „Zalecenia w zakresie stosowania przełączników KVN" – DBBT – 803A;
31. „Zalecenia w zakresie bezpieczeństwa autonomicznych stacji roboczych oraz sieci lokalnych przetwarzających informacje niejawne" – DBBT – 803;
32. „Zalecenia dotyczące urządzeń i narzędzi kryptograficznych przeznaczonych do ochrony informacji niejawnych" – DBBT – 602A;
33. „Zalecenia Służby Kontrwywiadu Wojskowego w zakresie bezpieczeństwa teleinformatycznego" – DBBT – 801B;
34. „Ustawienia zabezpieczeń Windows NT 4.0 w systemach przetwarzających informacje niejawne" – DBBT - 802A;
35. „Zalecenia w zakresie deklasyfikacji i niszczenia informatycznych nośników danych" – DBBT – 810;
36. „Wytyczne w zakresie postępowania ze środkami i materiałami kryptograficznymi" – BTPO – 601C;
37. „Zalecenia dotyczące ustawiania zabezpieczeń systemu Windows 2000 w systemach i sieciach przetwarzających informacje niejawne";
38. „Ustawienia zabezpieczeń Windows XP w autonomicznych systemach teleinformatycznych przetwarzających informacje niejawne";
39. „Zalecenia w zakresie ochrony fizycznej i technicznej pomieszczeń systemów i sieci teleinformatycznych"– DBBT – 301C;

40. „Instruction for the Control and Safe Guarding of NATO Crypto Material" - SDIP 293.

STRONY INTERNETOWE

- Aspekt prawny. Przestępstwa komputerowe a prawo karne [URL – http://bezpieczeństwoit.website.pl/aspekt_prawny.htm] 03.05.2006 r. 13.00.
- CERT Polska – Raport 2003 [URL – http://cert.pl/index3.html] 09.02.2005 r.
- CERT Polska – Raport 2004 [URL – http://cert.pl.html] 13.02.2005 r.
- CERT Polska – Raport 2005 [URL – http://cert.pl.html] 14.04.2007 r. 13.20.
- CERT Polska – Raport 2006 [URL – http://cert.pl.html] 14.04.2007 r. 13.23.
- Cyberterroryzm [URL – http://prowincja.ostrodaonline.pl/numer2.html] 30.10.2004 r.
- Infrastruktura Krytyczna Państwa [URL – http://prawo.vagla.pl/node/7204html] 10.05.2007 r. 20.45.
- NASK [URL – www.nask.pl.html] 23.02.2005 r.
- Polityka onet pl – Sieć ponad wszystko [URL – http://czytelnia.onet.pl/0,1100435,5,do_czytania.html] 30.01.2005 r.
- Przestępstwa komputerowe w kodeksie karnym [URL – http://asp.digikom.pl/kara.htm] 17.01.2005 r.
- Przestępstwa komputerowe w kodeksie karnym [URL – gazeta – it.pl/prawo /przestępstwa_komputerowe.html] 03.05.2006 r. 12.50.
- Seminarium „Infrastruktura krytyczna w Polsce" w Pałacu Prezydenckim [URL – http://www.prezydent.pl/ser/index.php3?tem_ID=4703&kategoria=] 27.11.2004 r.
- Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej [URL – http://iniejawna.pl/przepisy/rozne/strategia_bnrp.html] 24.01.2005 r.
- Uwagi do projektu dokumentu „ePolska – Strategia rozwoju społeczeństwa Informacyjnego w Polsce na lata 2001 – 2006" [URL – http://www.infoport.pl /kontent/?.html] 21.04.2007 r. 13.22.
- www.eng.kavkaz.memo.ru/news/
- www.cdi.org/terrorism
- www.cert.org
- www.cia.go/terrorism/index.html
- www.cry.ru
- www.fbi.gov/publications/terror/

- www.fsb.ru
- www.gazeta.ru
- www.hipakistan.com
- www.islam.org.au
- www.marshallcenter.org
- www.policja.pl
- www.prawo.lex.pl/czasopisma/
- www.rand.org/terrorism_area

SPIS TABEL, RYSUNKÓW I UJĘĆ GRAFICZNYCH.

Tabela 1.1. Powody, które skłaniają terrorystów do ataku w cyberprzestrzeni **15**
Tabela 2.1. Definicje walki informacyjnej **40**
Tabela 2.2. Definicje cyberterroryzmu **54**
Tabela 2.3. Typologia metod ataków na systemy i obiekty informatyczne **62**
Tabela 2.4. Określenia atrybutów bezpieczeństwa, właściwości bezpieczeństwa **67**
Tabela 3.1. Popularność technologii informacyjno – teleinformatycznych i komunikacyjnych w Polsce **94**
Tabela 3.2. Stan bezpieczeństwa teleinformatycznego w Polsce w 2007 r. **97**
Tabela 3.3. Statystyka przestępczości komputerowej w Polsce **97**
Tabela 3.4. Lista sektorów Infrastruktury Krytycznej **105**
Tabela 3.5. Lista sektorów Infrastruktury Krytycznej w Siłach Zbrojnych Rzeczypospolitej Polski **118**
Tabela 3.6. Niektóre rodzaje przestępstw komputerowych i wysokości kar za ich popełnienie **134**

Rysunek 1.1. Relacje przy doborze metod naukowych i określeniu przedmiotu badań **19**
Rysunek 1.2. Klasyfikacja metod badawczych **30**
Rysunek 2.1. Przestrzeń zagrożeń bezpieczeństwa w społeczeństwie informacyjnym **53**
Rysunek 2.2. Przykładowa skuteczność narzędzi do cyberataku, przy jednoczesnym zmniejszeniu się wiedzy potrzebnej do jego dokonania **57**
Rysunek 2.3. Typologia zagrożeń dla bezpieczeństwa **59**
Rysunek 2.4. Model cyberataku na obiekty teleinformatyczne **61**
Rysunek 2.5. Globalna sieć informacyjna na potrzeby działań sieciocentrycznych **79**
Rysunek 3.1. Korzystanie z nowych technologii **96**
Rysunek 3.2. Odsetek osób korzystających regularnie z komputera i Internetu w latach 2004 – 2006 **96**
Rysunek 3.3. Odsetek przedsiębiorstw stosujących zabezpieczenia informatyczne w 2007 r. według rodzajów zabezpieczeń lub metod uwierzytelnienia **98**
Rysunek 3.4. Liczba zarejestrowanych incydentów komputerowych **99**

Rysunek 3.5. Strefy współzależności sektorów Infrastruktury Krytycznej Państwa 108
Rysunek 3.6. Strefy współzależności sektorów Infrastruktury Krytycznej Sił Zbrojnych RP 120
Rysunek 3.7. Potencjalne cele Operacji Informacyjnych 125
Rysunek 4.1. Koncepcja funkcjonowania trójszczeblowego Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski 144
Rysunek 4.2. Model trójszczeblowego Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski 159
Rysunek 4.3. Obieg informacji jawnej i niejawnej pomiędzy instytucjami cywilnymi w ramach Systemu Zarządzania Kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski a Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.GOV.PL. 163
Rysunek 4.4. Schemat prezentujący ideę działania systemu ARAKIS 167
Rysunek 4.5. Ranking TOP10 dla firewalli w systemie ARAKIS 168
Rysunek 4.6. Przepływy w systemie ARAKIS 168
Rysunek 4.7. Ilości przepływu w systemie ARAKIS 168
Rysunek 4.8. Wykres wirusów w systemie ARAKIS 169

ZAŁĄCZNIKI

1. Broń elektromagnetyczna 195
2. Wybrane przykłady ataków cyberterrorystycznych na świecie 205
3. Regulacje prawne normalizujące politykę bezpieczeństwa informacyjnego Polski 215
4. Sektory oraz składniki sektorów Infrastruktury Krytycznej w wybranych państwach na świecie 225
5. Kwestionariusz ankiety do rozprawy doktorskiej 227
6. Raport z badań przeprowadzonych w okresie 22.02. – 01.06.2007 r. 245
7. Spis systemów teleinformatycznych w resorcie obrony narodowej 279

UWAGA

Wszystkie tabele, wykresy i rysunki zamieszczone w poniższych załącznikach są pracowaniem własnym autora.

ZAŁĄCZNIK 1

BROŃ ELEKTROMAGNETYCZNA[1].

Bomba E, to w teorii urządzenie wysyłające bardzo silny krótkotrwały impuls o ogromnej mocy, powodujący całkowite zniszczenie wszelkich elektronicznych systemów teleinformatycznych i teleinformacyjnych oraz łączności. Bomba E potrafi uczynić ze sprzętu elektronicznego, całkowicie bezużytecznym przedmiotem. Uniemożliwi pracę systemów dowodzenia, systemów wsparcia dowodzenia i elektroniki zamontowanej w sprzęcie bojowym. Jest to broń doskonała. Nie będzie żadnych odłamków, gruzu, ognia, rannych. Nie padnie żaden strzał, nie pęknie żadna szyba, nie przeleje się nawet kropla krwi. A i tak efekty będą zatrważające. W ciągu sekundy przyniesie ciemność, chaos, bezsilność i zdumienie.

Taka broń nie wymaga bezpośredniego trafienia w cel, co często bywa trudne. Zapewne największa zaletą tej broni jest to, że nosi ona etykietkę "nie zabójczej". Nie trzeba niszczyć wszystkiego. Stosownie do ocen niektórych specjalistów koncentrator strumieniowy zdetonowany na wysokości kilkuset metrów nad ziemią jest w stanie unieszkodliwić urządzenia elektroniczne w promieniu 500 metrów. Specjaliści twierdzą, że można zbudować kompresor strumienia, który zmieści się w zwykłej teczce. Niedostatkiem jest to, że trudno mieć gwarancję, że elektromagnetyczna broń spełniła swoje zadanie. Nie można przewidzieć, jakie zniszczenia taka broń spowoduje. Idea zastosowania podobnej broni podczas wojny jest wystarczająco niepokojąca, ale co będzie, jeśli wpadnie ona w ręce terrorystów? Przecież broń mikrofalową można sklecić kupując w sklepie elektronicznym detale za kilkaset lub kilka tysięcy dolarów co dla zorganizowanej grupy terrorystycznej nie stanowi to żadnej przeszkody.

---

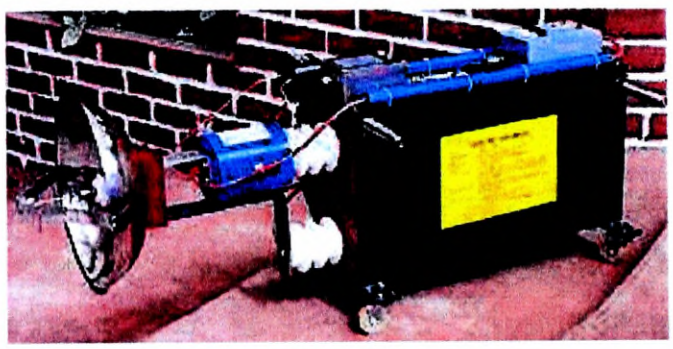
[1] Opracowano na podstawie: Szymański T., Zagrożenie atakami cyberterrorystycznymi w rejonie nadmorskim Morza Bałtyckiego, Gdynia, AMW, 2005 r.



Rysunek 1. Prototyp przenośnego emitera EMP.
Źródło: http://www.amazing1.com/

Urządzenie (Rys. 1.), zwane „Ray - Gun" może z kilku metrów zniszczyć komputer, unieruchomić samochód czy unieszkodliwić system alarmowy. Możliwości przenośnego emitera EMP zaprezentował na konferencji w Waszyngtonie w 1999 r. Winn Schwartau – ekspert od bezpieczeństwa sieci.

Generator impulsu elekromagnetycznego (Rys. 2.) można nabyć przez Internet.



Rysunek 2. Generator impulsu elektromagnetycznego.
Źródło: http://www.amazing1.com/

Specjaliści Interpolu twierdzą, że przestępcy już korzystali z broni mikrofalowej. Doniesienia z Rosji sugerują, że tego rodzaju urządzenia były użyte do unieszkodliwiania systemów zabezpieczających w bankach oraz do przerywania łączności policyjnej. Inny raport podaje, że celem takiego ataku był również pewien Londyński bank. Specjaliści ze zdziwieniem stwierdzili, że współczesne maszyny znacznie łatwiej uszkodzić, aniżeli starsze modele. Nowoczesne komputery są delikatniejsze aniżeli stare. Sprzyja temu choćby na przykład obniżanie roboczych napięć mikroprocesorów i zwiększanie ich szybkości oraz plastikowe obudowy, zamiast szczelnych blaszanych pudeł. Niezależnie od tego czy tego rodzaju broń została już użyta, czy też nie widzimy jak bardzo nasze uzależnienie od elektroniki staje się jednocześnie naszą piętą Achillesową.

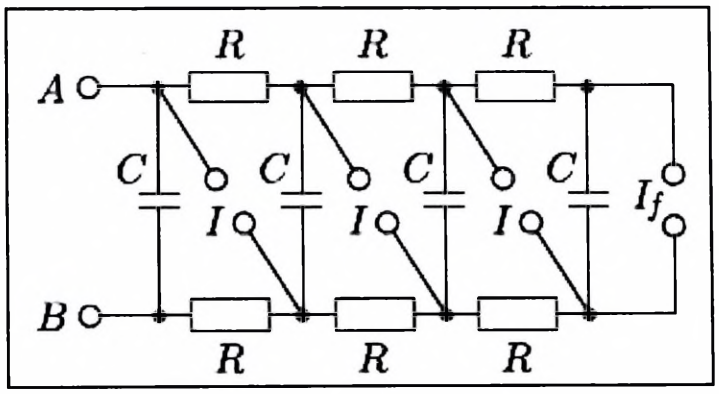
Niszczące działanie Bomby E polega na tym, że wysyła ona przez bardzo krótki czas, nie przekraczający milionowych części sekundy, niezwykle silną falę elektromagnetyczną, której moc osiąga miliardy watów. Długość tej fali wynosi od kilkudziesięciu centymetrów do ułamków milimetra, a więc jest to fala należąca do zakresu mikrofalowego. Wysłana fala rozchodzi się w otaczającej przestrzeni i dociera do wszelkiego rodzaju urządzeń elektronicznych. Zmienne pola elektryczne i magnetyczne, stanowiące tę falę, indukują zmiany napięcia w obwodach wspomnianych urządzeń, powodując ich zniszczenie lub poważne zakłócenia pracy. Jednocześnie okazuje się, że taka fala elektromagnetyczna jest praktycznie nieszkodliwa dla ludzi i innych organizmów żywych. Dlatego też bomba E nazywana jest często bronią humanitarną.

Pomysł wykorzystania fal elektromagnetycznych do zakłócania pracy urządzeń elektronicznych nie jest nowy. Już w czasie drugiej wojny światowej, a więc około sześćdziesięciu lat temu, stosowane były nadajniki skutecznie zakłócające pracę radarów. Podczas próbnych wybuchów bomb jądrowych w drugiej połowie lat czterdziestych ubiegłego wieku zauważono powstawanie tzw. burzy elektromagnetycznej, uniemożliwiającej nawet przez kilkadziesiąt minut prowadzenie łączności radiowej i funkcjonowanie urządzeń elektronicznych. Przyczyną tego zjawiska było wytworzenie w momencie wybuchu dużej liczby szybkich elektronów, kwantów promieniowania γ i zjonizowanych atomów. Elektrony, oddziałując z kwantami γ, ulegały rozproszeniu Comptona. Z kolei zjonizowane atomy ponownie przyłączały elektrony, ulegając rekombinacji. W wyniku tych efektów oddawana była energia w postaci fal elektromagnetycznych powodujących zakłócenia.

Zainteresowanie bombą E gwałtownie wzrosło w ostatnich latach. Przyczyny tego to zwiększenie liczby i znaczenia wszelkiego rodzaju urządzeń elektronicznych, wykorzystujących elementy półprzewodnikowe, które są bardzo podatne na uszkodzenia przez nawet niewielkie skoki napięcia - w granicach 1 - 2V oraz opracowanie metod wytwarzania impulsów promieniowania elektromagnetycznego o bardzo dużej mocy. Procesory stosowane we współczesnych komputerach zasilane są napięciem wynoszącym 1,4 - 1,6V. Zwiększenie tego napięcia nawet o 1V prowadzi zwykle do zniszczenia procesora. Dla porównania, stosowane dawniej lampy elektronowe wymagały napięcia anodowego 200 - 300V i wytrzymywały jego zmiany wynoszące 40 - 50V. Niewielkie zmiany napięcia, powodujące zniszczenie

elementów półprzewodnikowych, mogą być indukowane właśnie przez silne i szybkozmienne pole elektromagnetyczne, które wytwarza bomba E.

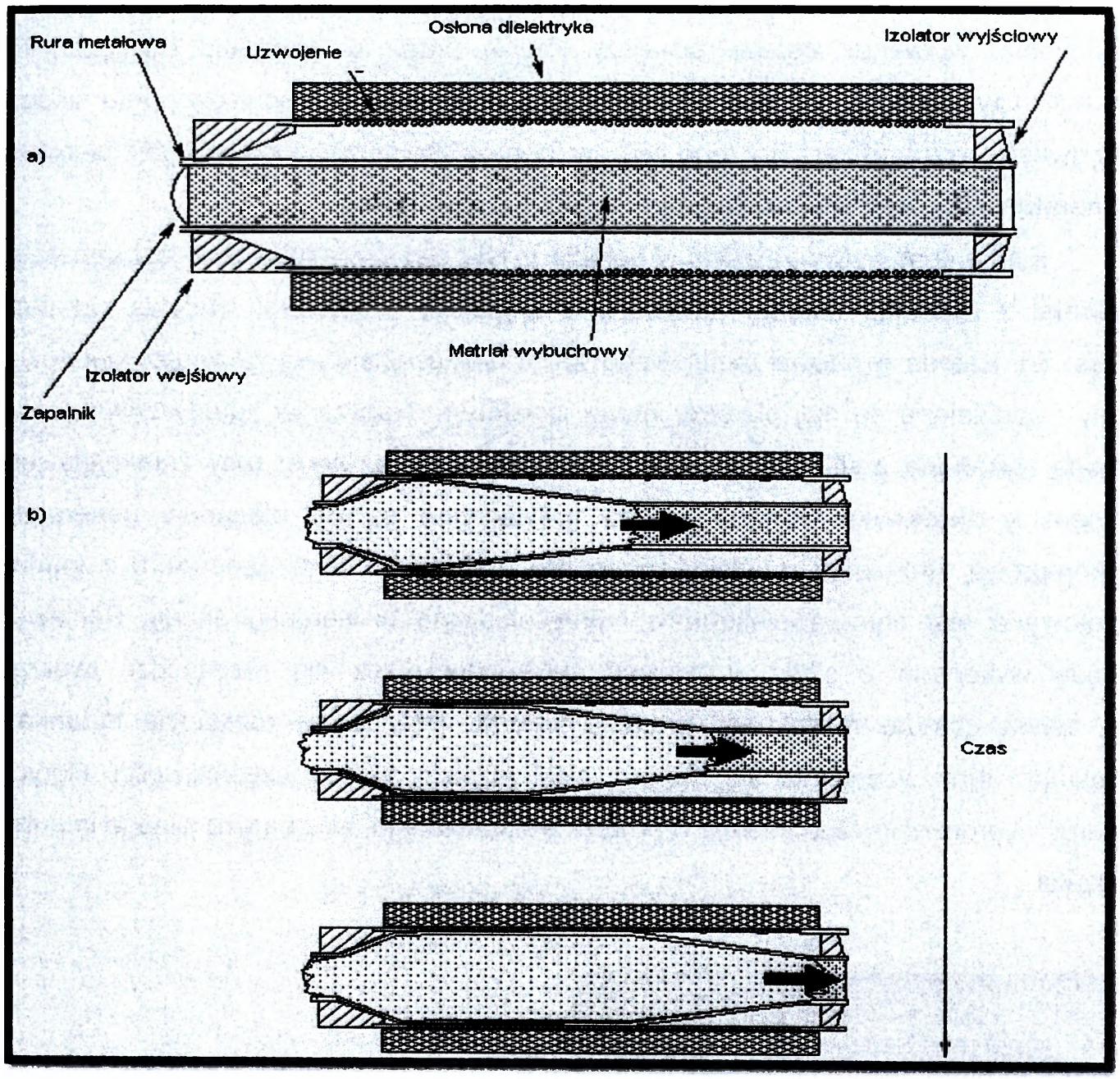
Pierwszym etapem, prowadzącym do wytworzenia takiego pola elektromagnetycznego, jest przepływ impulsu prądu o bardzo dużym natężeniu. Impuls ten uzyskuje się przez rozładowanie specjalnego układu kondensatorów, którego schemat przedstawia Rysunek 3.



Rysunek 3. Schemat generatora Marxa.
Źródło: Bednarek St., *Czy Bomba E zniszczy nasze komputery?*
[URL - www.mimuw.edu.pl/delta/artykuly/delta0604/bomba.pdf] z dnia 10.04.2005 r.

Oprócz tego, do sąsiednich kondensatorów przyłączone są iskierniki I, a do końcowego kondensatora iskiernik główny I_f. Każdy iskiernik składa się z dwóch rozsuniętych na odpowiednio dobraną odległość metalowych kulek i stanowi przerwę w obwodzie elektrycznym. Po naładowaniu kondensatorów do dostatecznie wysokiego napięcia między kulkami iskierników wytwarza się łuk elektryczny. Iskierniki zaczynają przewodzić i zmieniają początkowo równoległe połączenie kondensatorów na szeregowe, w którym napięcia na poszczególnych kondensatorach sumują się. Dzięki temu uzyskuje się zwielokrotnienie napięcia zasilacza, co powoduje przepływ bardzo silnego prądu podczas rozładowania wszystkich kondensatorów przez iskiernik główny.

Uzyskany z generatora Marxa impuls prądu zasila z kolei uzwojenie wytwarzające silne pole magnetyczne. Wewnątrz tego uzwojenia (Rys. 4), na dwóch pierścieniowych izolatorach, umieszczona jest metalowa rura wypełniona materiałem wybuchowym. W momencie, gdy natężenie prądu zasilającego osiąga wartość maksymalną, zostaje uruchomiony zapalnik znajdujący się na końcu rury. Na skutek tego rozpoczyna się wybuch, któremu towarzyszy wydzielanie dużej ilości gazów.

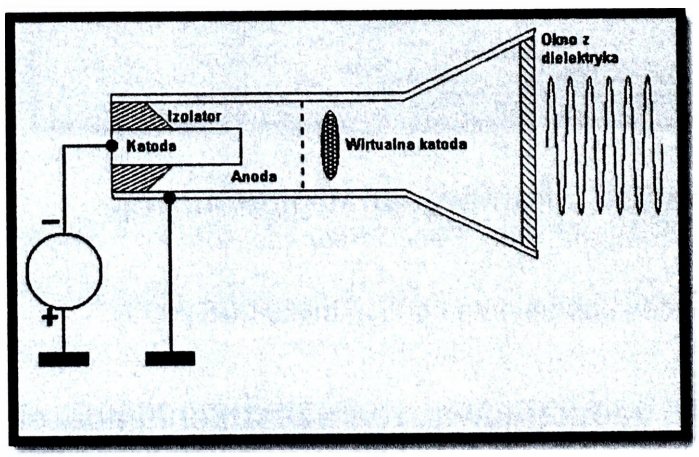


Rysunek 4. Uproszczony schemat generatora z kompresją strumieniową.
Źródło: Kopp Carlo – Defence Analist Melbourne, Australia, *The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction*
[URL - http://www.airpower.maxwell.af.mil/airchronicles/kopp/apjemp.html] z dnia 01.05.2005 r.

Wydzielające się gazy tworzą falę uderzeniową, rozprzestrzeniającą się wzdłuż rury i powodującą jej rozepchnięcie aż do wypełnienia wnętrza uzwojenia. Początkowo cała przestrzeń między rurą a uzwojeniem wypełniona jest polem magnetycznym, któremu przypisać można pewien strumień magnetyczny. Wartość tego strumienia pozostaje w rozważanym układzie stała. Poruszające się ścianki rury powodują wypchnięcie strumienia na zewnątrz w kierunku uzwojenia. Ponieważ wartość strumienia nie zmienia się, jest on przez to ściskany między rurą i uzwojeniem, a pole magnetyczne, przenikające uzwojenie, staje się przez to silniejsze. Zwiększające się pole magnetyczne indukuje w uzwojeniu dodatkowy prąd elektryczny, wzmacniający początkowy impuls prądu wytworzony

przez generator Marxa. W rezultacie urządzenie to, zwane generatorem z kompresją strumienia, wytwarza jeszcze silniejszy impuls prądu o natężeniu dochodzącym do milionów amperów. W celu uzyskania jeszcze silniejszych impulsów prądu stosuje się dwustopniowe generatory tego typu, w których impuls wytworzony przez pierwszy generator służy do zasilania drugiego, większego generatora.

Elementem wytwarzającym w bombie E fale elektromagnetyczne jest generator mikrofal z wirtualną katodą, nazywany z angielska virkatorem. Budowę virkatora (Rys. 5.). Katoda w postaci metalowego walca umieszczona jest wewnątrz metalowej tuby i oddzielona od niej pierścieniowym izolatorem. Naprzeciw katody znajduje się anoda wykonana z siatki metalowej i połączona z tubą. Wylot tuby zamknięty jest oknem z dielektryka. Katoda i tuba przyłączone są do biegunów generatora z kompresją strumienia magnetycznego. Po zadziałaniu tego generatora z katody emitowana jest chmura elektronów i przyspieszana w kierunku anody. Ponieważ anodę wykonano z siatki, większość elektronów przez nią przechodzi, tworząc za anodą chmurę nazywaną wirtualną katodą. Przy takim rozkładzie ładunków wewnątrz tuby wzbudzają się drgania elektryczne o wielkiej częstotliwości, których energii wypromieniowana zostaje w postaci krótkotrwałego, lecz bardzo silnego impulsu mikrofal.



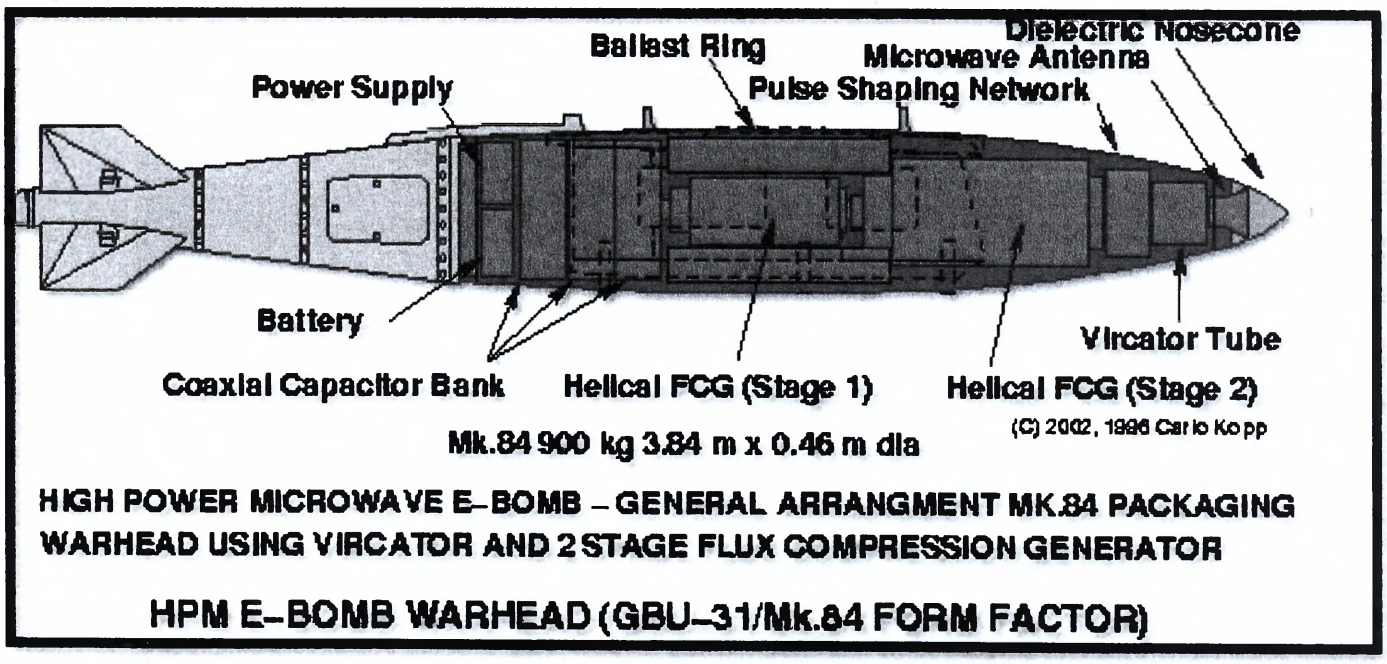
Rysunek 5. Budowa VIRKATORA.
Źródło: Kopp Carlo – Defence Analist Melbourne, Australia, *The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction*
[URL - http://www.airpower.maxwell.af.mil/airchronicles/kopp/apjemp.html] z dnia 01.05.2005 r.

Budową bomby E zainteresowane są niektóre kraje, a szczególnie Stany Zjednoczone.

CBS NEWS w wiadomościach z dnia 25.03.2003 r., doniosło o użyciu w Bagdadzie przez U.S Air Force eksperymentalnej broni wykorzystującej impuls

elektromagnetyczny, zwanej „Bombą-E” [2].

Badania nad źródłami wysyłającymi impulsy mikrofal o bardzo dużej mocy prowadzi się w stanie Nowy Meksyk. Ze względów oczywistych, szczegóły techniczne dotyczące konstrukcji podzespołów takiej bomby objęte są ścisłą tajemnicą. Domniemaną budowę jednego z rodzajów bomby E (HPM - High Power Microwave E - BOMB) przedstawia schematycznie (Rys. 6). Jest to bomba wysyłająca ukierunkowaną wiązkę mikrofal o wąskim przedziale częstotliwości. Bomba ta, oznaczona symbolem Mk.84, ma masę około 900 kg, długość 3,84 m i maksymalną średnicę 0,46 m. Zawiera 2 kg materiału wybuchowego i potrafi zniszczyć lub uszkodzić urządzenia elektroniczne na obszarze o promieniu około 1 km.



Rysunek 6. Budowa bomby GBU – 31 Mk. 84 HPM E – BOMB.
Źródło: Kopp Carlo – Defence Analist Melbourne, Australia, *The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction*
[URL - http://www.airpower.maxwell.af.mil/airchronicles/kopp/apjemp.html] z dnia 01.05.2005 r.

[2] U.S.Drops “E-Bomb” on Iraqi TV [URL-http://www.cbsnews.com/stories/2003/03/25/iraq/main546081.shtml?CMP=ILC-SearchStories] z dnia 14.03.2005 r.



Fot. 1. Uzbrajanie samolotów F/A – 18C HORNET w bomby GBU – 31 Mk. 84 na lotniskowcu amerykańskim.
Źródło: US Navy [URL - http://www.usnavy.com] z dnia 24.07.2009 r.



Fot. 2. Samolot F/A – 18 HORNET z bombą GDU – 31.
Źródło: US Navy [URL - http://www.usnavy.com] z dnia 24.07.2009 r.



Fot. 3. Podwieszanie bomby GBU – 31 Mk. 84 pod samolot.
Źródło: US Navy [URL - http://www.usnavy.com] z dnia 24.07.2009 r.

Budowane są również bomby E nie mające wirkatora i emitujące jedynie impuls promieniowania elektromagnetycznego wytworzony przez dwustopniowy generator kompresyjny. Impuls taki charakteryzuje się większą głębokością wnikania w elementy przewodzące niż mikrofale. W celu uzyskania jeszcze większych natężeń prądu i silniejszych pól elektromagnetycznych rozważa się również zastosowanie w bombie E elementów wykonanych z nadprzewodników.

Ewentualne użycie bomby E może, ale nie musi zagrozić naszym komputerom i urządzeniom elektronicznym. Jest tak, dlatego, ponieważ mikrofale, trafiając na powierzchnię przewodnika, wnikają do niego tylko na pewną głębokość, która jest tym mniejsza, im mniejsza jest długość mikrofal oraz im większa przewodność właściwa i przenikalność magnetyczna przewodnika. Ponadto, natężenie mikrofal w dobrym przewodniku bardzo szybko maleje wraz z odległością od jego powierzchni. Dla przykładu, na głębokości równej długości mikrofali natężenie to wynosi już tylko 0,05% natężenia mikrofali padającej. Ograniczone wnikanie mikrofal do przewodnika spowodowane jest indukowaniem w nich prądów elektrycznych przez zmienne pola magnetyczne i elektryczne. W wyniku tego mikrofale ulegają częściowemu pochłonięciu i odbiciu od powierzchni przewodnika, nie wnikając do jego wnętrza. Umożliwia to budowę osłon, zwanych też ekranami, zabezpieczających urządzenia elektroniczne. Łatwo, więc

wyobrazić sobie osłonę w kształcie szczelnego pudełka wykonanego z przewodnika o odpowiednich właściwościach i grubości, zabezpieczającą na przykład nasze urządzenie teleinformatyczne (np. komputer osobisty czy kalkulator). Niestety, stosowane obecnie obudowy komputerów stacjonarnych są tylko częściowo wykonane z blachy i ponadto zbyt cienkie, natomiast obudowy komputerów przenośnych wytwarza się zwykle z tworzyw sztucznych. Z kolei wszelkie anteny, np. urządzeń radiokomunikacyjnych czy radarów, należy wyposażyć w bardzo szybkie wyłączniki przepięciowe odłączające je w przypadku pojawienia się zbyt silnego sygnału. Wynika stąd, że zabezpieczenie urządzeń elektronicznych przed skutkami ewentualnego użycia bomby E jest możliwe, choć zapewne związane ze zwiększeniem ich ceny i masy. Już obecnie spotykamy urządzenia teleinformatyczne przeznaczone dla wojska, których cena trzykrotnie przewyższa cenę ich „cywilnych" wersji.

ZAŁĄCZNIK 2

WYBRANE PRZYKŁADY ATAKÓW CYBERTERRORYSTYCZNYCH NA ŚWIECIE.

Lp.	Data ataku (przybliżona data)	Cel ataku	Sprawca ataku	Opis wydarzenia
1.	Kwiecień 1990 r. – maj 1991 r.	Stany Zjednoczone	Hakerzy (Holandia)	Hakerzy włamali się do 34 komputerów należących do Departamentu Obrony. Podczas penetracji zasobów, zdobyli informacje na temat lokalizacji amerykańskich jednostek wojskowych, informacje o typach broni, które te jednostki posiadały, o możliwościach pocisków PATRIOT oraz o ruchach amerykańskich okrętów w rejonie Zatoki Perskiej. Po zdobyciu danych usunęli oni wszystkie ślady swojej działalności. Chcieli oni sprzedać zdobyte informacje Saddamowi Husajnowi za milion dolarów, ale myślał on, że to pułapka zastawiona przez CIA i nie skorzystał z bardzo „interesującej" oferty[1].
2.	08 styczeń 1991 r.	Irak	Stany Zjednoczone	Podczas pierwszej wojny w Zatoce Perskiej, dzięki wirusowi komputerowemu AF/91 (April Fools), podrzuconemu Irakijczykom w układach scalonych drukarek, udało się sparaliżować podczas pierwszych ataków system teleinformacyjny armii Saddama Husajna[2]. Inni autorzy podają inna wersję wydarzeń. Podobno pół roku przez działaniami bojowymi w Zatoce Perskiej, Amerykanie sprzedali do Iraku drukarki komputerowe, wewnątrz których zamontowali specjalne mikronadajniki, które codziennie podawały swoją pozycję do satelitów wywiadowczych. Wywiad wiedział, że są one w centrach dowodzenia armii irackiej. Amerykanie w ten

[1] *US General Accounting Office, Information Security: Computer Attacks at Departament of Defense Pose Increasing Risk*, GAO/AIMD-96-84, Washington, maj 1996 r.
[2] Schwartau W., *Information Warfare. Chaos on the Electronic Superhighway*, New York, 1995 r., s. 168.

Lp.	Data ataku (przybliżona data)	Cel ataku	Sprawca ataku	Opis wydarzenia
				sposób mieli pełny obraz rozmieszczenia celów do uderzeń lotniczych wojsk sprzymierzonych w pierwszym etapie operacji[3].
3.	1995 r.	Rosja	Kaukascy hakerzy (Czeczenia)	Hakerzy dokonali ataków w rosyjskim systemie finansowym, uszczuplając jego zasoby o około 300 mln dolarów. Z tego powodu nastąpiło zachwianie równowagi systemu bankowego Federacji Rosyjskiej.
4.	1998 r.	Sri Lanka – serwery ambasad	Separatyści tamilscy	Przez około dwa tygodnie separatyści tamilscy wysyłali dziennie ponad 1 tysiąc e-maili (*Flooding*) z oświadczeniem w kwestii roszczeń niepodległościowych, zakończonym informacją wskazującą na zorganizowane i celowe działanie przeciw systemom informacyjnym. Atak całkowicie sparaliżował komputerowy system łączności MSZ Sri Lanki oraz systemy informatyczne kilku ambasad tego państwa[4].
5.	1998 r.	Meksyk	Partyzanci zapatystowscy (Meksyk)	Blokowanie serwerów rządowych przez e-mail bombing. Zwrócenie uwagi opinii publicznej na działalność partyzantów zapatystowskich w stanie Chiapas.
6.	Od 1998 r.	Konflikt indyjsko - pakistański		W 2000 r., trzech członków grupy *Milworm* (pakistańscy hakerzy) dostało się do komputerów *Bhabha Atomic Research Center* (BARC) i uzyskało wiele cennych informacji dotyczących prób z bronią nuklearną (ukradli 5 magabajtów tajnych informacji). Atakowane także były strony kancelarii premiera, parlamentu, mediów oraz Ministerstwa Technologii Informacyjnej. Stosowane były różne metody ataków: rozsyłanie wirusów, ataki typu DDoS, włamania, *e-mail bombing* itd. Internet w tym konflikcie służy i nadal służy także do szeroko rozumianej propagandy. Na „zdobytych" stronach umieszczane są na przykład zdjęcia świadczące o brutalności indyjskich wojsk w Kaszmirze.
7.	Od 1999 r.	Konflikt izraelsko - arabski		Konflikt izraelsko – arabski w cyberprzestrzeni rozpoczął się od 1999 r. Po porwaniu w październiku

[3] Kwećka R., *Informacja w walce zbrojnej*, Warszawa 2001 r. s. 80.
[4] Adamski J., *Nowe technologie w służbie terrorystów*, Trio, Warszawa 2007 r. s. 105.

Lp.	Data ataku (przybliżona data)	Cel ataku	Sprawca ataku	Opis wydarzenia
				2000 r. 3 żołnierzy izraelskich przez Hezbollach gwałtownie się nasilił. Wtedy hakerzy izraelscy włamali się na strony tej organizacji. Później zostały zablokowane palestyńskie strony rządowe oraz strony organizacji terrorystycznych. W odpowiedzi pro palestyńscy hakerzy przeprowadzili *e-mail bom bing* na strony Knesetu, które w wyniku ataku zostały zablokowane. Podobny atak przeprowadzono na strony Ministerstwa Spraw Zagranicznych, Kancelarii Prezesa Rady Ministrów oraz Ministerstwa Obrony. Obie strony konfliktu prowadzą bardzo intensywną wojnę propagandową. Podczas każdych działań zbrojnych prowadzonych przez Izrael występuje intensywna wojna w cyberprzestrzeni. Jesienią 2000 r. hakerzy palestyńscy przeprowadzili ataki DoS przeciw serwerom firmy Netvision, największego dostawcy usług internetowych w Izraelu, dezorganizując przejściowo jego funkcjonowanie.
8.	Marzec – maj 1999 r.	Konflikt w Kosowie		W czasie konfliktu w Kosowie użyto całego wachlarza środków. Wykorzystano Internet do propagandy, komunikowania się, demonizowania przeciwnika (dezinformacja), atakowania za pomocą wirusów, DoS, DDoS, e-mail bombingu, włamywania się na strony internetowe itd[5]. 07 maja 1999 r. Amerykańskie samoloty przez „pomyłkę" bombardują chińską ambasadę w Belgradzie. Następują konsekwencje dyplomatyczne – Pekin zawiesza kontakty wojskowe z Waszyngtonem. Do akcji ruszają chińscy hakerzy, włamują się między innymi do systemów komputerowych Lockheed Martin i NASA. Chińscy hakerzy włamali się także kilka amerykańskich stron rządowych, między innymi Białego Domu, Departamentu Energetyki. W sumie, podczas działań bojowych zostało zaatakowanych około 100 serwerów należących do NATO.
9.	Sierpień 1999 r.	Konflikt chińsko - tajwański		11 sierpnia 1999 r. chińscy hakerzy uderzyli na kilka tajwańskich stron

[5] Bógdał – Brzezińska A., Gawrycki M. F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, ASPRA-JR, Warszawa 2003 r. s. 166.

Lp.	Data ataku (przybliżona data)	Cel ataku	Sprawca ataku	Opis wydarzenia
				rządowych. Zostały zaatakowane strony Kongresu, blokując całkowicie ich działanie i kasując dane. W odpowiedzi tajwańscy hakerzy „zdobyli" stronę Ministerstwa Kolejnictwa. Do września 1999 r. chińscy hakerzy włamali się 165 razy na tajwańskie strony, Pekin swoich danych nie udostępnił. Obie strony konflikty stosowały różne techniki do atakowania stron internetowych przeciwnika. Owa walka doprowadziła do pogorszenia stosunków tajwańsko – chińskich na szczeblu dyplomatycznym oraz do dużych strat finansowych.
10.	2000 r.	Stany Zjednoczone	Chiny	Chińscy hakerzy byli o krok od włamania się do komputerów zarządzających siecią energetyczną stanu Kolorado.
11.	01 kwietnia 2001 r.	Stany Zjednoczone	Chiny	Amerykański samolot zwiadowczy EP-3 zostaje przechwycony przez 2 chińskie myśliwce. Niedaleko wyspy Hainan dochodzi do kolizji. Samolot EP-3 musi awaryjnie lądować na południu Chin. Napięcie we wzajemnych stosunkach trwało 11 dni. Chińczycy 3 miesiące trzymają uszkodzony samolot, po czym go rozmontowują i w kawałkach odsyłają do Stanów Zjednoczonych. Wydarzenie to stało się pretekstem do wybuchu kolejnej wojny internetowej. Pierwsi zaatakowali amerykańscy hakerzy. Na stronach chińskich firm i instytucji pojawiły się pornograficzne zdjęcia i obraźliwe hasła. W ciągu kilkunastu dni dokonano kilkuset ataków, między innymi na *China Telecom, China Nuclear Information Center* oraz strony rządowe[6]. Chińscy hakerzy uderzyli między innymi na Biały Dom, Departament Pracy, Departament Zdrowia, Departament Energetyki, Departament Spraw Wewnętrznych, Izbę Reprezentantów i Dowództwo Marynarki Wojennej. Atakowano także małe amerykańskie firmy. W wyniku działań w cyberprzestrzeni zdobyto 1500 stron amerykańskich oraz 300 chińskich. Chińscy hakerzy w tym konflikcie udoskonalili metodę DDoS, która okazała się bardzo

[6] Gawrycka I., *Cyberporachunki*, „Życie Warszawy", 18-19.sierpnia 2001 r.

Lp.	Data ataku (przybliżona data)	Cel ataku	Sprawca ataku	Opis wydarzenia
				skuteczna.
12.	11 wrzesień 2001 r.	Stany Zjednoczone	Al. Kaida	Zostały częściowo uszkodzone przez terrorystów systemy identyfikacji samolotów porwanych i użytych podczas zamachów[7]. Zakłócono czasowo również pracę cywilnego systemu kontroli lotów w zakresie identyfikacji statków powietrznych i kierowania ruchem lotniczym (IFF). Według nieoficjalnych informacji w tym samym czasie czasowo sparaliżowano również system łączności satelitarnej NASA.
13.	Wrzesień 2001 r.	Stany Zjednoczone	Haker	Gary McKinnon, włamał się do 97 komputerów należących do NASA, Pentagonu, Sił Powietrznych i Marynarki Wojennej oraz centrum kosmicznego w Houston. Instalował na nich swoje oprogramowanie, skasował tysiące plików i zyskał dostęp do informacji stanowiących tajemnicę służbową i państwową. Według władz w Waszyngtonie włamania McKinnona były najpoważniejszym atakiem na wojskowe sieci teleinformatyczne w historii, a naprawienie ich skutków zajęło dużo czasu i kosztowało amerykańskich podatników około miliona dolarów
14.	Marzec 2003 r.	Irak	Stany Zjednoczone	Podczas drugiej wojny w Zatoce Perskiej wojska amerykańskie użyły broń elektromagnetyczna[8]. CBS NEWS w wiadomościach z dnia 25 marca 2003 r. doniosło o użyciu w Bagdadzie przez U.S Air Force eksperymentalnej broni wykorzystującej impuls elektromagnetyczny, zwanej „Bombą-E"[9].
15.	Listopad 2006 r.	Stany Zjednoczone	Chiny	Chińscy hakerzy skutecznie zablokowali strony amerykańskiej Akademii Marynarki Wojennej (*Naval War College*). Awaria sieci teleinformatycznej w Akademii trwała kilka tygodni.
16.	Grudzień 2006 r.	Stany Zjednoczone	Chiny	Chińscy hakerzy włamali się do Departamentu Stanu i wykradli poufne informacje. Pozostawili oni

[7] Adamski J., *Nowe technologie w służbie terrorystów*, Trio, Warszawa 2007 r. s. 100.
[8] Chodzi tu prawdopodobnie o bombę wysyłająca ukierunkowaną wiązkę mikrofal o wąskim przedziale częstotliwości. Bomba ta, oznaczona symbolem Mk.84, ma masę około 900 kg, długość 3,84 m i maksymalną średnicę 0,46 m. Zawiera 2 kg materiału wybuchowego i potrafi zniszczyć lub uszkodzić urządzenia elektroniczne na obszarze o promieniu około 1 km.
[9] U.S. Drops *E-Bomb" on Iraqi TV* [URL-http://www.cbsnews.com/stories/2003/03/25/iraq/main546081.shtml?CMP=ILC-SearchStories] z dnia 14.03.2005 r.

Lp.	Data ataku (przybliżona data)	Cel ataku	Sprawca ataku	Opis wydarzenia
				po sobie robaki umożliwiające dalsze włamania.
17.	Styczeń 2007 r.	Internet	Brak danych (prawdopodobnie Korea Południowa)	Została unieruchomiona część serwerów pośrednicząca w wymianie danych w Internecie. Motyw działania hakerów jest nieznany. Nie wiadomo kto i dlaczego atakował. Hakerzy przeprowadzili atak metodą *denial-of-service*. Na cel wzięto 3 spośród 13 komputerów, które przechowują i udostępniają informacje o innych serwerach w Internecie[10]. Unieruchomiono serwery zarządzane przez amerykański Departament Obrony, instytucję zarządzającą internetowymi adresami ICANN oraz firmę ULTRA DNS administrującą między innymi serwerami z nazwą kończącą się: .org.
18.	17 styczeń 2007 r. oraz 01 marzec 2007 r.	Polska (Ministerstwo Obrony Narodowej)	Polska grupa Hacking.pl (Polska)	Zostały zaatakowane internetowe witryny Ministerstwa Obrony Narodowej, (serwery: Dowództwa Operacyjnego, Departamentu Kadr MON). Sprawca posługiwał się nickiem „Słowik".
19.	26 kwiecień – czerwiec 2007 r.	Estonia	Rosja	Na kilka tygodni poprzez atak DDoS zostały zablokowane internetowe strony władz Estonii (prezydenta i parlamentu), partii politycznych, wszystkich ministerstw, mediów (czołowe gazety) i banków (2 największe banki). Po pierwszej fali ataku zostały zablokowane kolejno strony firm komunikacyjnych i przedsiębiorstw transportowych. Cyberatak spowodował paraliż kraju. Zostały uszkodzone łącza teleinformatyczne z Unią Europejską i NATO. Straty, wynikłe z zakłócenia działalności tych instytucji, szacuje się na miliony euro.
20.	18 maja 2007 r.	Polska (Policja)	Hakerzy	Hakerzy zaatakowali publiczny serwer Policji. Został on zatkany i strona policji na pewien czas zniknęła z sieci Internet (atak DDoS).
21.	Lipiec 2007 r.	Stany Zjednoczone	Chiny	Cybernetyczna inwazja zmusiła Departament Obrony do zawieszenia na tydzień działania części sieci teleinformatycznej.
22.	Sierpień 2007 r.	Niemcy	Chiny	Zmasowany atak „szpiegów" chińskiej armii (hakerzy pracujący dla chińskiej armii) na rządowe komputery w Niemczech. Niemieckim specjalistom udało się

[10] Serwery DNS kierują ruchem w całej sieci Internet.

Lp.	Data ataku (przybliżona data)	Cel ataku	Sprawca ataku	Opis wydarzenia
				zapobiec kradzieży 160 gigabajtów danych z komputerów Urzędu Kanclerskiego oraz trzech ważnych ministerstw: spraw zagranicznych, gospodarki i badań naukowych. Obiektem pożądania Chińczyków były tajemnice gospodarcze, nowe technologie i dane marketingowe.
23.	Styczeń 2008 r.	Internet	Brak danych (prawdopodobnie celowe działanie amerykańskiego okrętu podwodnego SSN – 23 USS „Jimmy Carter")[11]	Uszkodzenie czterech podmorskich kabli w zaledwie pięć dni (dwa kable FLAG i SEA-ME-WE 4 uszkodzone około 8 km od Aleksandrii, kabel QTEL między wyspami Halul i Das oraz kabel FALCON łączący ZEA i Oman przerwany około 56 km od Dubaju). W tym przypadku przecięte zostały również kable zapasowe. Największy problem z łącznością wystąpił w krajach arabskich. Awaria dotknęła przede wszystkim Egipt i Indie, a także Zjednoczone Emiraty Arabskie, Arabię Saudyjską, Kuwejt, Katar, Iran i Bahrajn. Według oficjalnych danych operatorów w Indiach i Egipcie, kraje te miały przepustowość sieci ograniczoną o mniej więcej połowę.
24.	16 – 18 kwiecień 2008 r.	Polska (Kancelaria Premiera, Ministerstwo Pracy)	Hakerzy	Po raz pierwszy hakerzy dali o sobie znać 16 kwietnia atakując oficjalną stronę Ministerstwa Pracy. 18 kwietnia „Internetowi włamywacze" weszli w nocy na stronę Kancelarii Premiera. Włamanie nastąpiło poprzez serwer zagraniczny. Hakerzy zaatakowali ogółem 6 stron urzędów centralnych. ABW oświadczyła, że atak nie naruszył wewnętrznych sieci teleinformatycznych urzędów centralnych oraz zapewniła, że hakerzy nie weszli w posiadanie dokumentów stanowiących tajemnice służbową i państwową.
25.	Lipiec 2008 r.	Sztaby wyborcze Baracka Obamy i McCaina	Hakerzy lub atak „obcego rządu lub organizacji"	Podczas kompanii wyborczej komputery w sztabach obu kandydatów atakowali hakerzy. Chcieli oni zdobyć informacje dotyczące polityki przyszłego prezydenta.
26.	Lipiec – sierpień 2008 r.	Gruzja	Rosja	Kilka tygodni przed wybuchem konfliktu serwery rządowe w Gruzji zostały „zalane" wiadomościami zawierającymi frazę „win+love+in+Russia". Równolegle

[11] Jest to okręt podwodny przystosowany do operacji szpiegowskich. Został wyposażony w sprzęt umożliwiający między innymi zakładanie podsłuchów na podmorskich kablach telekomunikacyjnych.

Lp.	Data ataku (przybliżona data)	Cel ataku	Sprawca ataku	Opis wydarzenia
				zastosowano analogiczny do użytego w Estonii typowy cyberatak typu DDoS. Serwery gruzińskie zostały zaatakowane milionami próśb o różnorodne trywialne informacje. Dotknęło to także serwery obsługujące Kancelarie Prezydenta Gruzji. Prezydencką stronę internetową i stronę najpopularniejszej stacji telewizyjnej przeniesiono na serwer znajdujący się w Stanach Zjednoczonych. W późniejszym okresie nastąpiły cyberataki powiązane z rzeczywistymi działaniami wojennymi. Po rozpoczęciu działań wojennych, podmieniona została strona prezydenta Gruzji. Następnie ta i wiele innych oficjalnych gruzińskich stron rządowych, policji, agencji prasowych, stacji telewizyjnych, a nawet najpopularniejsze gruzińskie forum hakerskie, zostały sparaliżowane atakami DDoS. Atakujący użyli wersji rosyjskiego szkodliwego kodu z rodziny *Pinch*, a do koordynowania ataku wykorzystano serwery w Turcji. Specjaliści przypuszczają, że za atak jest odpowiedzialna sieć RNB (*Russian Business Network*), znana z rozsyłania spamu i szkodliwych programów.
27.	28 listopad 2008 r.	System komputerowy Ministerstwa Obrony USA	Hakerzy (prawdopodobnie z Rosji)	Według wysokich urzędników Pentagonu, atak uderzył w komputerowe systemy dowodzenia, które są odpowiedzialne za działalność wojskową sił zbrojnych USA w Afganistanie i Iraku. Atak również „przeniknął" do tajnych informacji znajdujących się w systemach teleinformatycznych i teleinformacyjnych.
28.	Kwiecień 2009 r.	Stany Zjednoczone	Hakerzy	Hakerom udało się włamać do najkosztowniejszego i najbardziej zaawansowanego programu zbrojeniowego realizowanego przez Pentagon, czyli projektu samolotu F – 35 (*Joint Strike Fighter*). Intruzi zdołali przekopiować i wyprowadzić dane na temat systemów elektronicznych. Nie jest znana tożsamość hakerów, a także rozmiar szkód zadanych amerykańskiemu systemowi obrony, zarówno w wymiarze finansowym, jak i kwestii bezpieczeństwa. Według

Lp.	Data ataku (przybliżona data)	Cel ataku	Sprawca ataku	Opis wydarzenia
				informatorów dziennika, ataki mogły mieć swoje źródło w Chinach.
29.	Czerwiec 2009 r.	Korea Południowa	Chiny Korea Północna	Hakerzy z Chin i Korei Północnej atakują sieci komputerowe Korei Południowej. Według Seulu każdego dnia ma miejsce aż 95 000 ataków na sieci komputerowe kraju. 10 450 włamań polegało na próbach dostania się do zabezpieczonych baz danych. 81 700 przypadków to próby wpuszczenia wirusów do komputerów południowokoreańskich agencji rządowych. Aż 11% wszystkich ataków dokonywano na serwery wojskowe.
30.	Lipiec 2009 r.	Korea Południowa	Brak danych (prawdopodobnie Korea Północna)	Według państwowej Koreańskiej Agencji do spraw Bezpieczeństwa Informacji strony internetowe pałacu prezydenckiego, ministerstwa obrony, parlamentu, banków Shinhan i Korea Exchange Bank, a także najpopularniejszej wyszukiwarki internetowej naver.com.
31.	Lipiec 2009 r.	Stany Zjednoczone	Korea Północna	Na niektóre amerykańskie agencje rządowe został przeprowadzono rozległy cyberatak. Wcześniej informowano o podobnym ataku na Koreę Południową. Zaatakowano: Departament Stanu, Departament Skarbu, Pentagon, Secret Service, Krajową Komisję Handlu i Departament Transportu. Zaatakowane były również portale „The Washington Post" i nowojorskiej giełdy. Atak rozpoczęto 4 lipca, w dniu święta narodowego USA. Amerykańskie władze nie ujawniły szczegółów ani skali ataku. Ataki na Koreę Południową wydają się być połączone z atakami na USA. Według wywiadu południowokoreańskiego, za atakami może stać Korea Północna. Atak spowodował spowolnienie działania serwisów rządowych, a w niektórych przypadkach ich zamknięcie na kilka godzin, w tym strony prezydenta kraju.

Do sporządzenia załącznika wykorzystano również materiały zamieszczone w:
Rzeczpospolita 03 lipca 2007 r., s. B4, Rzeczpospolita 26 marca 2007 r. s. A5, Rzeczpospolita 10-11 lutego 2007 r. s. A18, Rzeczpospolita 17 października 2006 r. s. A7, Rzeczpospolita 28 sierpnia 2007 r. s. A7, Rzeczpospolita 05 września 2007 r. s. A8, Rzeczpospolita 19 września 2007 r. s. A6, Rzeczypospolita 05 lutego 2008 r. s. A22, Rzeczypospolita 02 września 2008 r. s. A15, Rzeczypospolita 8-9 listopada 2008 r. s. A10, Rzeczypospolita 1-2 sierpnia 2008 r. s. A12, Newsweek 02 września 2007 r. s. 32, Przekrój 09 września 2007 r. s. 37, Polska Dziennik Bałtycki 18 czerwca 2009 r. s. 15, Bógdał – Brzezińska A., Gawrycki M. F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, ASPRA-JR, Warszawa 2003 r. s. 77, 79, 165-176.

ZAŁĄCZNIK 3

REGULACJE PRAWNE NORMALIZUJĄCE POLITYKE BEZPIECZEŃSTWA INFORMACYJNEGO POLSKI.

Do najważniejszych regulacji prawnych, związanych z polityką bezpieczeństwa informacyjnego Polski, należą niżej wymienione dokumenty:[1]

- **Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polski, Warszawa 2007 r.;**

- **Ustawa z dnia 22 stycznia 1999 r. „O ochronie informacji niejawnych" Tekst ujednolicony po zmianach z dnia 15 kwietnia 2005 r. Dz. U. 1999.11.95; Tekst ujednolicony Dz. U. 2005.196.1631 - akty zmieniające;**

- Ustawa z dnia 13 kwietnia 2007 r. „O kompatybilności elektromagnetycznej" Dz. U. 2007.82.556;
- Ustawa z dnia 16 lipca 2004 r. „Prawo telekomunikacyjne" Dz. U. 2004.171.1800;
- Ustawa z dnia 18 lipca 2002 r. „O świadczeniu usług drogą elektroniczną" Dz. U. 2002.144.1204;
- Ustawa z dnia 18 września 2001 r. „O podpisie elektronicznym" Dz. U. 2001.130.1450;
- Ustawa z dnia 27 lipca 2001 r. „O ochronie baz danych" Dz. U. 2001.128.1402;
- Ustawa z dnia 14 lipca 1983 r. „O narodowym zasobie archiwalnym i archiwach" Dz. U. 2002.171.1396;
- Ustawa z dnia 6 czerwca 19997 r. „KK/Przestępstwa przeciwko ochronie informacji" Dz. U. 1997.88.553;

- **Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzona w Brukseli dnia 6 marca 1997 r.**

---

[1] Przedstawiony stan regulacji prawnych jest aktualny na dzień 01.06.2009 r.

- Dyrektywa PARLAMENTU EUROPEJSKIEGO I RADY z dnia 13 grudnia 1999 r. „W sprawie ramowych warunków Wspólnoty dla podpisu elektronicznego" /99/93/WE/;

- Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 2 listopada 2007 r. „W sprawie systemów teleinformatycznych stosowanych do realizacji zadań w zakresie świadczeń rodzinnych w urzędach administracji publicznej" Dz. U. 2007.216.1610;
- Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 2 listopada 2007 r. „W sprawie systemów teleinformatycznych stosowanych w jednostkach organizacyjnych pomocy społecznej" Dz. U. 2007.216.1609;
- Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 2 listopada 2007 r. „W sprawie systemów teleinformatycznych stosowanych w publicznych służbach zatrudnienia" Dz. U. 2007.212.1566;
- Rozporządzenie Prezesa Rady Ministrów z dnia 19 września 2007 r. „W sprawie sposobów postępowania w przypadku stwierdzenia, że urządzenie wytwarzające pole elektromagnetyczne powoduje zakłócenia pracy innego urządzenia" Dz. U. 2007.175.1227;
- Rozporządzenie Ministra spraw Wewnętrznych i Administracji z dnia 24 lipca 2007 r. „W sprawie warunków udostępniania formularzy i wzorów dokumentów w postaci elektronicznej" Dz. U. 2007.151.1078;
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 26.06.2007 r. „W sprawie wzorów kart rejestracyjnych oraz sposobu ich wypełniania" D. U. 2007.127.881;
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. „W sprawie Biuletynu Informacji Publicznej" Dz. U. 2007.10.68;
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 listopada 2006 r. „W sprawie sporządzania i doręczania pism w formie dokumentu elektronicznego" Dz. U. 2006.227.1664;
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 02 listopada 2006 r. „W sprawie wymagań technicznych formatów zapisu i informatycznych nośników danych, na których utrwalono materiały archiwalne przekazywane do archiwów państwowych" Dz. U. 2006.206.1519;

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. „W sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi" Dz. U. 2006.206.1518;
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. „W sprawie niezbędnych elementów struktury dokumentów elektronicznych" Dz. U. 2006.206.1517;
- Rozporządzenie Ministra Finansów z dnia 02 grudnia 2005 r. „W sprawie postępowania z dokumentami związanymi z dokonywaniem niektórych czynności regulowanych ustawą o obrocie instrumentami finansowymi" Dz. U. 2005.242.2041;
- **Rozporządzenie Prezesa Rady Ministrów z dnia 05 października 2005 r. „W sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności a także zmiany nadanej klauzuli tajności" Dz. U. 2005.205.1696;**
- Rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 r. „W sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne" Dz. U. 2005.200.1650;
- Rozporządzenie Prezesa Rady Ministrów z dnia 27 września 2005 r. „W sprawie sposobów, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym" Dz. U. 2005.205.1692;
- Rozporządzenie Prezesa Rady Ministrów z dnia 30 września 2005 r. „W sprawie wysokości opłat za przeprowadzenie przez służbę ochrony państwa czynności z zakresu bezpieczeństwa teleinformatycznego" Dz. U. 2005.200.1652;
- Rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 r. „W sprawie warunków organizacyjno – technicznych doręczania dokumentów elektronicznych podmiotom publicznym" Dz. U. 2005.200. 1651;
- **Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. „W sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego" Dz. U. 2005.171.1433;**
- Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. „W sprawie szczegółowego trybu przygotowania i prowadzenia przez służby ochrony państwa kontroli w zakresie ochrony informacji niejawnych" Dz. U. 2005.171.1431;
- Rozporządzenie Ministra Infrastruktury z dnia 16 czerwca 2005 r. „ W sprawie planu działania przedsiębiorcy telekomunikacyjnego w sytuacji szczególnych zagrożeń" Dz. U. 2005.122.1029;

- Rozporządzenie Ministra Infrastruktury z dnia 11 sierpnia 2005 r. „W sprawie szczegółowych wymagań związanych z połączeniem sieci telekomunikacyjnych" Dz. U. 2005.160.1349;
- **Rozporządzenie Rady Ministrów z dnia 18 października 2005 r. „W sprawie organizacji i funkcjonowania kancelarii tajnych" Dz. U. 2005.208.1741;**
- Rozporządzenie Rady Ministrów z dnia 13 września 2005 r. „W sprawie wypełniania przez przedsiębiorców telekomunikacyjnych zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego" Dz. U. 2005.187.1568;
- Rozporządzenie Ministra Gospodarki i Pracy z dnia 30 sierpnia 2004 r. „W sprawie homologacji systemów informatycznych stosowanych w urzędach pracy" Dz. U. 2004.204.2085;
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 25.10.2004 r. „W sprawie wzoru karty zapytania oraz sposobu jej wypełnienia" Dz. U. 2004.242.2425;
- Rozporządzenie Rady Ministrów z dnia 03 sierpnia 2004 r. „W sprawie przygotowań i wykorzystania systemów łączności na potrzeby obronne państwa" Dz. U. 2004.180.1855;
- Rozporządzenie Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 29 kwietnia 2004 r. „W sprawie homologacji systemów informatycznych stosowanych w urzędach administracji publicznej realizujących zadania w zakresie świadczeń rodzinnych" Dz. U. 2004.127.1323;
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. „W sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych" Dz. U. 2004.100.1024;
- Rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. „ W sprawie sposobów technicznego przygotowania systemów i sieci służących do przekazywania informacji do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych" Dz. U. 2004.100.1023;

- Rozporządzenie Ministra Finansów z dnia 31 października 2003 r. „W sprawie szczegółowych zasad tworzenia , utrwalania, przechowywania i zabezpieczenia dokumentów związanych z zawieraniem i wykonywaniem umów ubezpieczenia" Dz. U. 2003.193.1889;
- Rozporządzenie Rady Ministrów z dnia 25 lutego 2003 r. 'W sprawie zasad tworzenia, utrwalania, przechowywania i zabezpieczenia, w tym przy zastosowaniu podpisu elektronicznego, dokumentów bankowych sporządzonych na elektronicznych nośnikach informacji" Dz. U. 2003.51.442;
- Rozporządzenie Ministra Infrastruktury dnia 24 stycznia 2003 r. „W sprawie wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego" Dz. U. 2003.19.166;
- Rozporządzenie Ministra Gospodarki z dnia 09 sierpnia 2002 r. „W sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym" Dz. U. 2002.128.1101;
- Rozporządzenie Ministra Gospodarki z dnia 06 sierpnia 2002 r. „W sprawie określenia zasad wynagradzania za przeprowadzenie kontroli podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym" Dz. U. 2002.128.1100;
- Rozporządzenie Ministra Gospodarki z dnia 06 sierpnia 2002 r. „W sprawie sposobu prowadzenia rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne związane z podpisem elektronicznym, wzoru tego rejestru oraz szczegółowego trybu postępowania w sprawach o wpis do rejestru" Dz. U. 2002.128.1099;
- Rozporządzenie Ministra Gospodarki z dnia 06 sierpnia 2002 r. „W sprawie wysokości opłaty za rozpatrzenie wniosku o wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym" Dz. U. 2002.128.1098;
- Rozporządzenie Ministra Gospodarki z dnia 06 sierpnia 2002 r. „W sprawie wzoru i szczegółowego zakresu wniosku o dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym" Dz. U. 2002.128.1097;
- Rozporządzenie Ministra Finansów z dnia 08 sierpnia 2002 r. „W sprawie sposobu i szczegółowych warunków spełnienia obowiązku ubezpieczenia odpowiedzialności cywilnej przez kwalifikowany podmiot" Dz. U. 2002.128.1096;

- Rozporządzenie Rady Ministrów z dnia 07 sierpnia 2002 r. „W sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego" Dz. U. 2002.128.1094;

- **Rozporządzenie Ministra Obrony Narodowej z dnia 21 czerwca 2007 r. „W sprawie szczegółowych zadań pełnomocników ochrony oraz szczególnych wymagań w zakresie ochrony fizycznej informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych" Dz. U. 2007.126.876;**
- Rozporządzenie Ministra Obrony Narodowej z dnia 12 października 2005 r. „W sprawie szczegółowych warunków wykonywania działalności telekomunikacyjnej" Dz. U. 2005.206.1736;

- **Zarządzenie Nr 25/MON Ministra Obrony Narodowej z dnia 17 listopada 2005 r. „W sprawie szczególnego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, stosowania środków ochrony fizycznej oraz obieg informacji niejawnych";**

- **Decyzja Nr 122/MON z dnia 18 marca 2008 r. „W sprawie powoływania w resorcie obrony narodowej pełnomocników i zastępców pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów oraz inspektorów bezpieczeństwa teleinformatycznego";**
- **Decyzja Nr 498/MON z dnia 2 listopada 2007 r. „W sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej";**
- **Decyzja Nr 485/MON z dnia 29 października 2007 r. „W szczególnej ochrony materiałów kryptograficznych w komórkach organizacyjnych Ministerstwa Obrony Narodowej";**
- **Decyzja Nr 448/MON z dnia 4 października 2007 r. „W sprawie trybu akredytacji bezpieczeństwa fizycznego i technicznego pomieszczeń specjalnych";**

- **Decyzja Nr 488/MON z dnia 30 listopada 2006 r. „W sprawie wprowadzenia do użytku w resorcie obrony narodowej „Tymczasowej instrukcji organizacji obiegu informacji niejawnych o klauzuli zastrzeżone w resortowej sieci teleinformatycznej MIL-WAN";**
- **Decyzja Nr 390/MON z dnia 28 września 2006 r. „W sprawie ograniczeń w używaniu urządzeń do rejestracji, kopiowania lub transmisji obrazu i dźwięku w komórkach i jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych";**
- **Decyzja Nr 20/MON z dnia 31 stycznia 2006 r. „W sprawie powoływania pełnomocników, zastępców pełnomocników do spraw ochrony informacji niejawnych, administratorów systemów i sieci teleinformatycznych oraz inspektorów bezpieczeństwa teleinformatycznego w Ministerstwie Obrony Narodowej oraz w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych";**
- **Decyzja Nr 21/MON z dnia 31 stycznia 2006 r. „W sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej";**
- **Decyzja Nr 22/MON z dnia 31 stycznia 2006 r. „W sprawie szczegółowych zasad i trybu prowadzenia i dokumentowania postępowań sprawdzających oraz wydawania poświadczeń i certyfikatów bezpieczeństwa";**
- **Decyzja Nr 23/MON z dnia 31 stycznia 2006 r. „W sprawie szkolenia w zakresie ochrony informacji niejawnych";**
- **Decyzja Nr 24/MON z dnia 31 stycznia 2006 r. „W sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej";**
- **Decyzja Nr 25/MON z dnia 31 stycznia 2006 r. „W sprawie trybu certyfikacji, recertyfikacji oraz kontroli kancelarii zagranicznych, punktów obsługi dokumentów zagranicznych, kancelarii kryptograficznych, stacji łączności kryptograficznej, kabin kryptograficznych oraz pomieszczeń wydzielonych organizowanych lub funkcjonujących w jednostkach i komórkach organizacyjnych resortu obrony narodowej";**
- Decyzja Nr 41/MON Ministra Obrony Narodowej z dnia 26 stycznia 2007 r. „W sprawie działalności kontrolnej w resorcie obrony narodowej";
- Decyzja Nr 326/MON z dnia 25 października 2004 r. „W sprawie udzielania w resorcie obrony narodowej zamówień odjętych tajemnicą państwową oraz jeżeli wymaga tego istotny interes bezpieczeństwa państwa";

- Decyzja Nr 100/MON z dnia 06 czerwca 2000 r. „W sprawie jednostki certyfikującej właściwej w Ministerstwie Obrony Narodowej do certyfikacji wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych";

- **Wytyczne Ministra Obrony Narodowej z dnia 23 stycznia 2007 r. „W sprawie ochrony informacji niejawnych oraz obiektów wojskowych w jednostkach organizacyjnych podporządkowanych Ministrowi Obrony Narodowej lub przez niego nadzorowanych w 2007 r.";**

- **Instrukcja organizacji prowadzenia gospodarki materiałowo - technicznej sprzętu i oprogramowania informatycznego w resorcie obrony narodowej Sygn. Łączn. 1012/2004;**
- **Zarządzenie Szefa Sztabu Generalnego WP z dnia 26 stycznia 2000 r. „W sprawie opracowywania Szczególnych Wymagań Bezpieczeństwa";**
- **„Metodyka opracowywania szczególnych wymagań bezpieczeństwa dla systemów lub sieci teleinformatycznych" - wprowadzona zarządzeniem Szefa Sztabu Generalnego WP z dnia 26 stycznia 2000 r.**
- **„Zalecenia w sprawie instalacji urządzeń przeznaczonych do przetwarzania informacji niejawnych" – BTPO – 701B;**
- **„Zalecenia w zakresie stosowania przełączników KVN" – DBBT – 803A;**
- **„Zalecenia w zakresie bezpieczeństwa autonomicznych stacji roboczych oraz sieci lokalnych przetwarzających informacje niejawne" – DBBT – 803;**
- **„Zalecenia dotyczące urządzeń i narzędzi kryptograficznych przeznaczonych do ochrony informacji niejawnych" – DBBT – 602A;**
- **„Zalecenia Służby Kontrwywiadu Wojskowego w zakresie bezpieczeństwa teleinformatycznego" – DBBT – 801B;**
- **„Ustawienia zabezpieczeń Windows NT 4.0 w systemach przetwarzających informacje niejawne" – DBBT - 802A;**
- **„Zalecenia w zakresie deklasyfikacji i niszczenia informatycznych nośników danych" – DBBT – 810;**
- **„Wytyczne w zakresie postępowania ze środkami i materiałami kryptograficznymi" – BTPO – 601C;**

- **„Zalecenia dotyczące ustawiania zabezpieczeń systemu Windows 2000 w systemach i sieciach przetwarzających informacje niejawne";**
- **„Ustwawienia zabezpieczeń Windows XP w autonomicznych systemach teleinformatycznych przetwarzających informacje niejawne";**
- **„Zalecenia w zakresie ochrony fizycznej i technicznej pomieszczeń systemów i sieci teleinformatycznych"– DBBT – 301C;**
- **„Instruction for the Control and Safe Guarding of NATO Crypto Material" - SDIP 293.**

Przedstawione powyżej, **„wytłuszczonym"** drukiem, dokumenty i regulacje prawne, mają zasadniczy wpływ dla bezpieczeństwa informacyjnego systemów teleinformatycznych i teleinformacyjnych wykorzystywanych w Siłach Zbrojnych Rzeczypospolitej Polski.

ZAŁĄCZNIK 4

SEKTORY ORAZ SKŁADNIKI SEKTORÓW INFRASTRUKTURY KRYTYCZNEJ W WYBRANYCH PAŃSTWACH NA ŚWIECIE - ZESTAWIENIE TABELARYCZNE.

Kraje / Sektory/składniki sektorów	AUS	A	CAN	F	FIN	GER	IND	IT	JAP	KOR	MAL	NL	NO	NZ	RU	SE	SING	SWIT	UK	USA	Suma
System kontroli ruchu lotniczego																■					1
Przestrzeń kosmiczna																■					1
Bankowość i finanse	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	20
Przemysł chemiczny i jądrowy												■									1
Administracja państwowa	■		■			■			■	■	■	■	■	■		■			■	■	12
Obrona cywilna																		■			1
Telekomunikacja, ICT	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	20
Tamy wodne																				■	1
Szkolnictwo wyższe																				■	1
Energia/Elektryczność	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	20
Służby ratunkowe	■	■	■			■		■		■	■		■	■				■	■	■	12
Żywność/Rolnictwo	■		■		■	■						■							■	■	7
Materiały niebezpieczne (CBRN)			■																■	■	3
Służba zdrowia	■	■	■	■	■	■		■	■		■	■	■				■	■	■	■	15
Przemysł obronny, istotny przemysł dla gospodarki	■		■	■	■						■				■			■		■	8
Media	■	■	■		■					■	■	■			■	■		■	■		11
Ubezpieczenia	■					■	■													■	4

Kraje / Sektory/składniki sektorów	AUS	A	CAN	F	FIN	GER	IND	IT	JAP	KOR	MAL	NL	NO	NZ	RU	SE	SING	SWIT	UK	USA	Suma
Wymiar sprawiedliwości						■	■					■		■					■	■	6
Obrona militarna, Siły Zbrojne, instalacje wojskowe	■	■				■	■			■	■	■	■		■						9
Narodowe pomniki i pamiątki	■		■																	■	3
Elektrownie jądrowe				■		■														■	3
Dostawy gazu i ropy	■		■			■	■	■	■	■		■	■	■	■				■	■	13
Policja	■	■	■										■						■		5
Poczta i spedycja		■																		■	2
Znane miejsca publiczne (Prominent public places, high profile events)																	■				1
Administracja publiczna		■			■	■		■				■						■	■	■	8
Bezpieczeństwo i porządek publiczny				■				■				■							■		4
Gospodarka odpadami	■		■					■			■		■						■		6
Bezpieczeństwo socjalne		■											■	■							3
Transport, logistyka, dystrybucja	■	■	■	■	■		■	■	■	■	■	■	■	■	■		■	■	■	■	18
Usługi komunalne	■	■			■	■							■								5
Dostawy wody	■	■	■	■	■	■		■	■		■	■	■				■	■	■	■	15
Woda, gospodarka wodna												■									1
Suma	18	14	16	9	11	15	8	11	8	9	12	16	14	9	8	6	7	11	17	20	

Źródło: Opracowanie własne na podstawie Abele – Wigert I., Dunn M., *An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies*, International CIIP Handbook 2006, Vol. I, Center for Security Studies, Swiss Federal Institute of Technology, ETH Zurich oraz Wojtowicz W., *Bezpieczeństwo infrastruktury krytycznej*, MON DPO, Warszawa 2006 r.

ZAŁĄCZNIK 5

KWESTIONARIUSZ ANKIETY DO ROZPRAWY DOKTORSKIEJ.

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ STRATEGICZNO – OBRONNY

Nr .....

227

KWESTIONARIUSZ ANKIETY
DO ROZPRAWY DOKTORSKIEJ NA TEMAT

„MODEL SYSTEMU ZARZĄDZANIA KRYZYSOWEGO W WARUNKACH ZAGROŻEŃ CYBERTERRORYSTYCZNYCH DLA BEZPIECZEŃSTWA INFORMACYJNEGO SIŁ ZBROJNYCH RZECZYPOSPOLITEJ POLSKIEJ"

Opracował

kmdr ppor. mgr inż.
Ernest LICHOCKI

Promotor rozprawy doktorskiej

prof. dr hab. inż.
Piotr SIENKIEWICZ

WARSZAWA **2007**

CZĘŚĆ WSTĘPNA

Głównym celem badań, które są integralną częścią rozprawy doktorskiego na temat „Model systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informacyjnego Sił Zbrojnych Rzeczypospolitej Polski" jest przeprowadzenie diagnozy i zgromadzenie niezbędnych danych dotyczących Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski, a mianowicie:

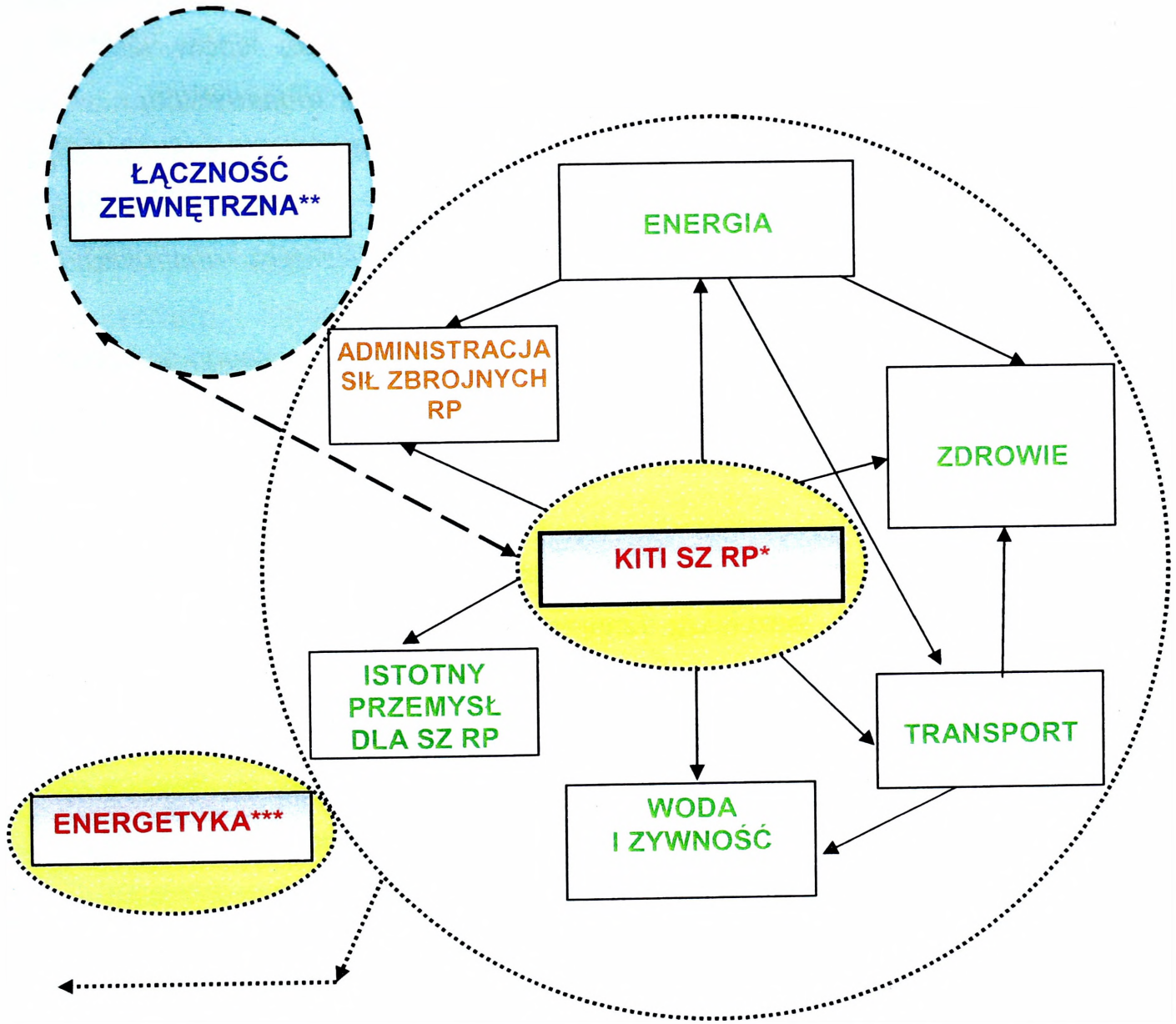
1. Uzyskanie danych, które na podstawie przeprowadzonej analizy mogą być wykorzystywane w procesie tworzenia baz danych dotyczących Infrastruktury Krytycznej. Bazy te będą w przyszłości narzędziem wykorzystywanym przez CIRC Sił Zbrojnych RP (Centrum Koordynacyjne Sił Zbrojnych RP).
2. Identyfikacja punktów kontaktowych w zakresie Infrastruktury Krytycznej w Ministerstwie Obrony Narodowej, Sztabie Generalnym WP, w poszczególnych Rodzajach Sił Zbrojnych oraz jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej.
3. Zgromadzenie informacji na temat rozwiązań prawnych i organizacyjnych w zakresie ochrony infrastruktury krytycznej. W kwestionariuszu zostanie zadane pytanie dotyczące struktur zarządzania w sytuacjach kryzysowych, kompetencji podmiotów w zakresie infrastruktury krytycznej, nadzorowania, kierowania, koordynacji, kontroli koncesjonowania bądź egzekwowania w innej formie norm bezpieczeństwa.
4. Poznanie technologicznych aspektów funkcjonowania Infrastruktury Krytycznej. Uzyskanie informacji o bazach danych, zautomatyzowanych systemach dowodzenia, sposobach ich zabezpieczenia przed zniszczeniem, zasobach map cyfrowych, aplikacjach służących wspomaganiu procesu podejmowania decyzji i dokonywania analiz, obiektach, budowlach i systemach wymagających szczególnej ochrony, wykorzystywaniu technik satelitarnych do ochrony Infrastruktury Krytycznej.
5. Analiza sposobów zabezpieczenia Infrastruktury Krytycznej przed nielegalną ingerencją w systemy teleinformatyczne i łączności.

6. Zbadanie oddziaływania czynników zewnętrznych takich jak: destabilizacja organizacyjna i ekonomiczna. Przedmiotem zainteresowania są także plany operacyjne i procedury na wypadek zagrożenia i zniszczenia Infrastruktury Krytycznej.
7. Określenie możliwości zdolności odbudowy Infrastruktury Krytycznej. Szczegółowy zakres zagadnień dotyczy planów odbudowy Infrastruktury Krytycznej, sposobów utrzymania zasadniczych funkcji Infrastruktury Krytycznej, a także możliwości odbudowy systemów teleinformatycznych i łączności służących do ochrony Infrastruktury Krytycznej.
8. Z uwagi na międzynarodowy, transgraniczny charakter zagrożeń dla Infrastruktury Krytycznej, zostanie przeanalizowana współpraca zagraniczna w zakresie ochrony Infrastruktury Krytycznej, uczestnictwo w jej instytucjonalnych formach, wykorzystanie międzynarodowych baz danych i prowadzenie bieżącej wymiany informacji z partnerami zagranicznymi.
9. Ponieważ samo pojęcie Infrastruktury Krytycznej (Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski) funkcjonuje w Polsce od niedawna, określenie które z sektorów zaproponowanej definicji są najbardziej istotne i na które elementy należy zwrócić największą uwagę.

Dla celów badań, przyjęto następującą definicję Infrastruktury Krytycznej Sił Zbrojnych RP, której niezdolność do działania znacznie obniża sprawność działania i obrony Sił Zbrojnych:

Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski to fizyczne i wirtualne sektory i systemy (systemy teleinformatyczne i teleinformacyjne) o zasadniczym znaczeniu dla minimalnego funkcjonowania Sił Zbrojnych. Niezdolność do działania infrastruktury krytycznej znacznie obniża sprawność działania i funkcjonowania Sił Zbrojnych.

Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski składa się z następujących infrastruktur - sektorów krytycznych: energia, woda, transport, systemy i technologia telekomunikacyjna, teleinformatyczna i teleinformacyjna - Krytyczna Infrastruktura Teleinformatyczna Sił Zbrojnych RP, zdrowie, żywność, administracja Sił Zbrojnych RP oraz istotny przemysł dla Sił Zbrojnych RP.



* **KITI SZ RP** – Krytyczna Infrastruktura Teleinformatyczna Sił Zbrojnych RP czyli *systemy i technologia telekomunikacyjna, teleinformatyczna i teleinformacyjna - Krytyczna Infrastruktura Teleinformatyczna Sił Zbrojnych RP.*

** **ŁĄCZNOŚĆ ZEWNĘTRZNA** – czyli: systemu dowodzenia i kierowania obronnością Sił Zbrojnych narodowe i sojusznicze, systemy łączności radiowej narodowe i sojusznicze, systemy łączności cyfrowej, systemy łączności satelitarnej narodowe i sojusznicze, zautomatyzowane systemy dowodzenia narodowe i sojusznicze, systemy teleinformatyczne narodowe i sojusznicze, systemy powiadamiania (Broadcasting).

*** **ENERGETYKA** – jeden z najważniejszych sektorów Infrastruktury Krytycznej Sił Zbrojnych RP. Jeżeli sektor ten będzie miał zakłócenia, to pozostałe sektory nie będą prawidłowo funkcjonować a w szczególności KITI SZ RP. Trzeba zawsze pamiętać o zapasowych źródłach zasilania (agregaty prądotwórcze).

Rysunek 1. Strefy współzależności sektorów Infrastruktury Krytycznej Sił Zbrojnych RP.
Źródło: opracowanie własne.

Poniżej zacytowana została inna definicja Infrastruktury Krytycznej, która została oparta na zapisie zawartym w kwestionariuszu przygotowanym przez grupę studyjną Wysokiego Komitetu ds. Planowania Cywilnego w Sytuacjach Zagrożeń NATO i rozesłana do wszystkich krajów uczestniczących w pracach Euro – Atlantyckiej Rady Partnerstwa.

Infrastruktura krytyczna oznacza obiekty (budynki i budowle) i urządzenia, służby odpowiedzialne za obsługę tych obiektów i urządzeń, komputerowe systemy informatyczne istotne dla bezpieczeństwa i ekonomicznego dobrobytu państwa oraz jego efektywnego funkcjonowania obejmując: systemy energetyczne, telekomunikacyjne, finansowe i bankowe, zarządzania zasobami wodnymi, dostaw żywności i wody, opieki zdrowotnej, transportu, usługi w zakresie bezpieczeństwa powszechnego i porządku publicznego oraz zapewnienie prawidłowego funkcjonowania najważniejszych struktur administracji publicznej w sytuacjach nadzwyczajnych zagrożeń (w tym centra zarządzania kryzysowego i stanowiska kierowania) oraz ochrony przemysłu o strategicznym znaczeniu, w tym obronnego.

Tabela 1. Lista sektorów infrastruktury krytycznej.

Sektor	Składniki sektorów
I. Energia.	1. Gaz, ropa naftowa, paliwa płynne. 2. Urządzenia do wydobywania, przetwarzania i przechowywania gazu, ropy naftowej i paliw płynnych. 3. Elektrownie. 4. Energetyczne sieci transmisyjne i dystrybucyjne dostarczające elektryczność, gaz, ropę naftową oraz paliwa płynne do użytkowników końcowych, m.in. do domów, agencji rządowych i różnego rodzaju firm.
II. Woda.	5. Zasoby wodne, rezerwuary i zbiorniki wodne. 6. Systemy transportowania i dostarczania wody do domów i do celów przemysłowych. 7. Urządzenia do filtrowania i uzdatniania wody oraz system kontroli jakości wody. 8. System odbioru wody zużytej wraz z oczyszczalniami ścieków. 9. System dostarczania wody do instalacji przeciwpożarowych.

Sektor	Składniki sektorów
III. Transport.	10. Transport drogowy wraz z drogami, autostradami, ciężarówkami i samochodami osobowymi. 11. Transport kolejowy wraz z siecią połączeń kolejowych, stacje kolejowe i tabor kolejowy. 12. Transport lotniczy wraz z siecią połączeń lotniczych z liniami lotniczymi, lotniska i samoloty. 13. Transport wodny – śródlądowy wraz z flotą handlową portami i drogami wodnymi. 14. Transport wodny – morski i oceaniczny wraz z flotą handlową portami i drogami wodnymi. 15. System dystrybucji towarów krytycznie ważnych dla bezpieczeństwa i stabilności gospodarki wraz z infrastrukturą.
IV. Systemy i technologia teleinformatyczna, łączność, ICT.	16. Sieci teleinformatyczne, oprogramowanie, procesy i ludzie dbające o prawidłowe działanie i bezpieczeństwo. 17. Systemy automatyki i kontroli (SCADA itd.). 18. Internet. 19. Stacjonarne systemy telekomunikacyjne. 20. Mobilne systemy telekomunikacyjne (telefonia komórkowa). 21. Łączność i nawigacja radiowa. 22. Łączność i nawigacja satelitarna. 23. Systemy powiadamiania (Broadcasting).
V. Zdrowie.	24. Szpitale. 25. Zdrowie publiczne. 26. Laboratoria i instytucje badawcze. 27. Przemysł farmaceutyczny.
VI. Żywność.	28. Produkcja żywności. 29. Magazynowanie i dystrybucja żywności.
VII. Bankowość i finanse.	30. Banki i bankowość. 31. Ubezpieczenia. 32. Giełda. 33. System rezerw finansowych.
VIII. Administracja państwowa.	34. Ministerstwo Obrony. 35. Służba Ochrony Państwa. 36. Parlament (Sejm i Senat).

Sektor	Składniki sektorów
	37. Kluczowe ministerstwa państwowe gwarantujące ciągłość działań rządu. 38. Służby ratunkowe /pogotowie ratunkowe, straż pożarna, policja, wszystkie systemy ratownictwa. 39. Elektrownie jądrowe. 40. Usługi doręczycielskie, poczta i spedycja.
IX. Narodowe pomniki i pamiątki.	41. Budynki, pomniki, muzea, obiekty sportowe;
X. Istotny przemysł dla gospodarki.	42. Przemysł zbrojeniowy. 43. Przemysł ciężki. 44. Produkcja i magazynowanie substancji niebezpiecznych (chemiczne, biologiczne i jądrowe). 45. Składowanie odpadów niebezpiecznych.
XI. Wymiar sprawiedliwości.	46. Sądownictwo i wymiar sprawiedliwości.
XII. Przestrzeń kosmiczna, eksploracja kosmosu	47. Przestrzeń kosmiczna. 48. Prowadzenie prac badawczych i wprowadzanie nowych technologii w przestrzeni kosmicznej.

Źródło: Opracowanie własne na podstawie Trusted Information Sharing Network for Critical Infrastructure Protection, National Counter – Terrorism Committee, Critical Infrastructure Protection in Australia, Australia 25 March 2003 r. i Zielona księga w sprawie europejskiego programu ochrony infrastruktury krytycznej, COM /2005/ 576 końcowy, Bruksela 17.11 2005 r.

Adres korespondencyjny

kmdr ppor. mgr inż. Ernest LICHOCKI
Akademia Marynarki Wojennej
ul. Śmidowicza 69
81 – 103 Gdynia
Tel.: 26 29 47
Tel. kom. 606 22 86 60
e- mail: comsec@onet.eu

CZĘŚĆ ZASADNICZA

Uwaga
Prawidłową odpowiedź zaznacz symbolem „X".

Lp.	Pytanie ankietowe	Odpowiedź		
		Tak	Nie	Nie wiem
1.	Wskaż które z sektorów krytycznych Infrastruktury Krytycznej Państwa należą do Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski:			
	I. Energia.			
	II. Woda.			
	III. Transport.			
	IV. Systemy i technologia teleinformatyczna, łączność, ICT.			
	V. Zdrowie.			
	VI. Żywność.			
	VII. Bankowość i finanse.			
	VIII. Administracja państwowa.			
	IX. Narodowe pomniki i pamiątki.			
	X. Istotny przemysł dla gospodarki.			
	XI. Wymiar sprawiedliwości.			
	XII. Przestrzeń kosmiczna, eksploracja kosmosu.			
2.	Wskaż które z sektorów Infrastruktury Krytycznej Państwa pozostają w zakresie kompetencji Panów jednostek organizacyjnych.			
	I. Energia.			
	II. Woda.			
	III. Transport.			
	IV. Systemy i technologia teleinformatyczna, łączność, ICT.			
	V. Zdrowie.			
	VI. Żywność.			
	VII. Bankowość i finanse.			

Lp.	Pytanie ankietowe	Odpowiedź		
		Tak	Nie	Nie wiem
	VIII. Administracja państwowa.			
	IX. Narodowe pomniki i pamiątki.			
	X. Istotny przemysł dla gospodarki.			
	XI. Wymiar sprawiedliwości.			
	XII. Przestrzeń kosmiczna, eksploracja kosmosu.			
3.	Czy w jednostce organizacyjnej są teleinformatyczne bazy danych.			
4.	Czy w jednostce organizacyjnej są bazy danych dotyczące Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.			
5.	Czy w jednostce organizacyjnej są bazy danych.			
6.	Czy w jednostce organizacyjnej są Zautomatyzowane Systemy Dowodzenia.			
7.	Czy w jednostce organizacyjnej są Zautomatyzowane Systemy Dowodzenia i Kierowania Walką.			
8.	Czy w jednostce organizacyjnej są systemy teleinformatyczne i łączności.			
9.	Czy w jednostce organizacyjnej są zautomatyzowane systemy zarządzania, monitorowania i sterowania Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski.			
10.	Czy w jednostce organizacyjnej są wykorzystywane mapy cyfrowe.			
11.	Czy w jednostce organizacyjnej są wykorzystywane aplikacje wspomagające proces podejmowania decyzji.			
12.	Czy w jednostce organizacyjnej jest wykorzystywana publiczna łączność jawna.			
13.	Czy w jednostce organizacyjnej jest wykorzystywana służbowa łączność jawna.			
14.	Czy w jednostce organizacyjnej jest wykorzystywana łączność niejawna.			
15.	Czy w jednostce organizacyjnej jest wykorzystywana łączność satelitarna.			
16.	Czy w jednostce organizacyjnej jest wykorzystywana łączność wewnętrzna.			
17.	Czy w jednostce organizacyjnej są wykorzystywane systemy teleinformatyczne na potrzeby Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski.			
18.	Czy w jednostce organizacyjnej są wykorzystywane wewnętrzne systemy			

Lp.	Pytanie ankietowe	Odpowiedź		
		Tak	Nie	Nie wiem
	teleinformatyczne.			
19.	Czy w jednostce organizacyjnej są wykorzystywane zewnętrzne systemy teleinformatyczne.			
20.	Czy w jednostce organizacyjnej są wykorzystywane niejawne systemy teleinformatyczne.			
21.	Czy w jednostce organizacyjnej są nadzorowane w fazie projektu i budowy systemy teleinformatyczne.			
22.	Czy w jednostce organizacyjnej wykorzystywana jest do ochrony Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski łączność satelitarna.			
23.	Czy w jednostce organizacyjnej wykorzystywana jest do ochrony Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski niejawna łączność satelitarna.			
24.	Czy w jednostce organizacyjnej są wykorzystywane specjalistyczne aplikacje teleinformatyczne wspomagające funkcjonowanie Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski.			
25.	Czy w jednostce organizacyjnej są wykorzystywane specjalistyczne aplikacje teleinformatyczne do zarządzania bazami danych.			
26.	Czy w jednostce organizacyjnej są wykorzystywane specjalistyczne aplikacje i urządzenia teleinformatyczne wspomagające bezpieczeństwo teleinformatyczne.			
27.	Czy w jednostce organizacyjnej są wykorzystywane specjalistyczne aplikacje i urządzenia teleinformacyjne wspomagające bezpieczeństwo łączności.			
28.	Czy w jednostce organizacyjnej są wykorzystywane aplikacje monitorujące Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski.			
29.	Czy w jednostce organizacyjnej są urządzenia i systemy które chronią Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski przed zniszczeniem wskutek działań fizycznych.			
30.	Czy w jednostce organizacyjnej są plany i procedury na wypadek zagrożeń i zniszczenia Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski.			
31.	Czy w jednostce organizacyjnej są plany odbudowy Infrastruktura Krytyczna			

Lp.	Pytanie ankietowe	Odpowiedź		
		Tak	Nie	Nie wiem
	Sił Zbrojnych Rzeczypospolitej Polski.			
32.	Czy w jednostce organizacyjnej są możliwości utrzymania podstawowych funkcji Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski w przypadku powstania poważnych zagrożeń, zakłóceń lub zniszczeń.			
33.	Czy w jednostce organizacyjnej jest możliwość odbudowy systemów teleinformatycznych.			
34.	Czy w jednostce organizacyjnej jest możliwość odbudowy systemów łączności niejawnej.			
35.	Czy w jednostce organizacyjnej jest możliwość odbudowy systemów łączności wewnętrznej.			
36.	Czy w jednostce organizacyjnej jest możliwość odbudowy systemów łączności zewnętrznej.			
37.	Czy jednostka organizacyjna współpracuje z innymi instytucjami w zakresie działań wewnątrz i między sektorowe w celu ochrony infrastruktury krytycznej.			
38.	Czy jednostka organizacyjna współpracuje z instytucjami międzynarodowymi w zakresie ochrony infrastruktury krytycznej.			
39.	Czy jednostka organizacyjna współpracuje na bieżąco z instytucjami międzynarodowymi w zakresie ochrony infrastruktury krytycznej w celu wymiany informacji.			
40.	Czy jednostka organizacyjna korzysta z międzynarodowych baz danych i zasobów w celu ochrony infrastruktury krytycznej.			
41.	Czy w jednostce organizacyjnej są zastosowane urządzenia i systemy które chronią Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski przed zniszczeniem wskutek działań fizycznych.			

Proszę o wskazanie najbardziej istotnych segmentów Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski według podanych poniżej pytań.

1. Uporządkuj według istotności elementy definicji Infrastruktury Krytycznej

1.	Energia.	
2.	Woda.	
3.	Transport.	
4.	Systemy i technologia teleinformatyczna, łączność, ICT.	
5.	Zdrowie.	
6.	Żywność.	
7.	Bankowość i finanse.	
8.	Administracja państwowa.	
9.	Narodowe pomniki i pamiątki.	
10.	Istotny przemysł dla gospodarki.	
11.	Wymiar sprawiedliwości.	
12.	Przestrzeń kosmiczna, eksploracja kosmosu.	

2. Przypisz wartość od 1 do 10 gdzie 1 oznacza najbardziej istotny a 10 najmniej istotny, elementom definicji Infrastruktury Krytycznej.

1.	Energia.	
2.	Woda.	
3.	Transport.	
4.	Systemy i technologia teleinformatyczna, łączność, ICT.	
5.	Zdrowie.	
6.	Żywność.	
7.	Bankowość i finanse.	
8.	Administracja państwowa.	
9.	Narodowe pomniki i pamiątki.	
10.	Istotny przemysł dla gospodarki.	
11.	Wymiar sprawiedliwości.	
12.	Przestrzeń kosmiczna, eksploracja kosmosu.	

3. Proszę o określenie się jakimi kryteriami Panowie kierowali się przy wypełnianiu podanych powyżej dwóch ostatnich pytań

1.	Z punktu podmiotu wypełniającego ankietę.	
2.	Bezpieczeństwa obywateli.	
3.	Ochrony środowiska życia ludzkiego.	
4.	Bezpieczeństwa struktur państwa.	
5.	Bezpieczeństwa narodowego.	
6.	Bezpieczeństwa jednostki organizacyjnej.	

CZĘŚĆ KOŃCOWA

Proszę o udzielenie odpowiedzi na podane poniżej pytania:

1. Wymień zakres teleinformatycznych baz danych. Jakiej tematyki dotyczą bazy danych.

2. Wymień Zautomatyzowane Systemy Dowodzenia, Zautomatyzowane Systemy Dowodzenia i Kierowania Walką oraz systemy teleinformatyczne i łączności.

3. Wymień zautomatyzowane systemy zarządzania, monitorowania i sterowania Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski.

4. Wymień jawne i niejawne systemy teleinformatyczne wykorzystywane na potrzeby Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski.

5. Jakiego rodzaju łączność niejawna wykorzystywana jest w jednostce organizacyjnej.

6. Wymień systemy teleinformatyczne wykorzystywane na potrzeby Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski.

7. Wymień wykorzystywane w jednostce organizacyjnej wewnętrzne i zewnętrzne oraz niejawne systemy teleinformatyczne.

8. Jakiego rodzaju zastosowane są specjalistyczne aplikacje teleinformatyczne, monitorujące i zapewniające ochronę łączności które wspomagają funkcjonowanie Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski.

9. Jakiego rodzaju są zastosowane urządzenia i systemy które chronią Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski przed zniszczeniem wskutek działań fizycznych.

METRYKA ANKIETY

Lp.	*Nazwa cechy respondenta*	*Odpowiedź*	*Uwagi*
1.	Wiek.		
2.	Płeć.		
3.	Stanowisko pracy.		
4.	Wykształcenie.		
5.	Staż zawodowy.		
6.	Specjalność wojskowa.		
7.	Doświadczenie zawodowe.		

ZAŁĄCZNIK 6

RAPORT Z BADAŃ PRZEPROWADZONYCH W OKRESIE 22.02. – 01.06.2007 r.

WSTĘP

W celu określenia na potrzeby rozprawy doktorskiej Infrastruktury Krytycznej w Siłach Zbrojnych Rzeczypospolitej Polskiej, rozesłano kwestionariusz ankiety do 41 jednostek organizacyjnych podległych Ministrowi Obrony Narodowej. W sumie otrzymano i poddano analizie 23 odpowiedzi, w tym 2 z Centrum Operacyjnych, 7 z Wojsk Lądowych, 7 z Sił Powietrznych i 7 z Marynarki Wojennej[1].

Odpowiedzi na pytania zawarte w ankiecie nadesłały następujące jednostki organizacyjne:

Centrum Operacji Połączonych;

Centrum Operacji Morskich;

Dowództwo Wojsk Lądowych;

Dowództwo 2 Korpusu Zmechanizowanego;

Dowództwo Pomorskiego Okręgu Wojskowego;

12 Dywizja Zmechanizowana;

16 Dywizja Zmechanizowana;

6 Brygada Desantowo – Szturmowa;

1 Brygada Logistyczna;

2 Korpus Obrony Powietrznej;

2 Brygada Radiotechniczna;

1 Brygada Lotnictwa Taktycznego;

21 Baza Lotnicza;

33 Baza Lotnicza;

3 Baza Lotnicza;

6 Baza Lotnicza;

8 Flotylla Obrony Wybrzeża.

---

[1] Wszystkie kwestionariusze ankiety nadesłane z Marynarki Wojennej, zostały wypełnione w Centrum Operacji Morskich.

Odpowiedzi nie udzieliły następujące jednostki organizacyjne:

Centrum Operacji Powietrznych;

Dowództwo Śląskiego Okręgu Wojskowego;

1 Dywizja Zmechanizowana;

11 Dywizja Kawalerii Pancernej;

25 Brygada Kawalerii Powietrznej;

49 Pułk Śmigłowców Bojowych;

56 Pułk Śmigłowców Bojowych;

4 Pułk Chemiczny;

9 Pułk Dowodzenia;

10 Brygada Logistyczna;

Dowództwo Sił Powietrznych;

3 Korpus Obrony Powietrznej;

3 Brygada Radiotechniczna;

2 Brygada Lotnictwa Taktycznego;

22 Baza Lotnicza;

12 Baza Lotnicza;

31 Baza Lotnicza;

8 Baza Lotnicza;

33 Baza Lotnicza;

23 Baza Lotnicza;

Dowództwo Marynarki Wojennej;

3 Flotylla Okrętów;

Brygada Lotnictwa Marynarki Wojennej;

Biuro Hydrograficzne Marynarki Wojennej.

CELE BADAŃ

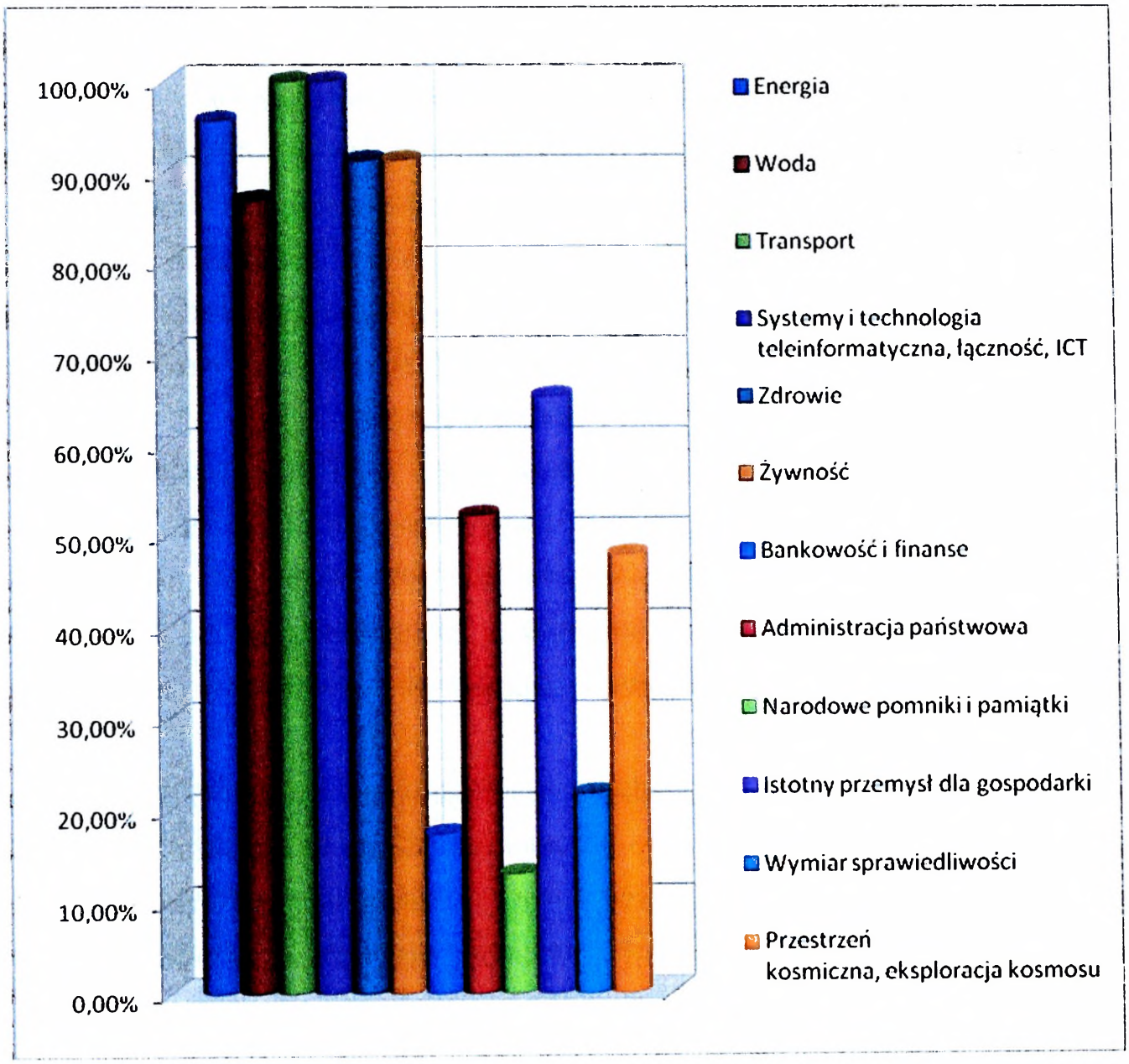
Głównym celem badań było przeprowadzenie diagnozy i zgromadzenie niezbędnych danych dotyczących Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski, a mianowicie:

1. Uzyskanie danych, które na podstawie przeprowadzonej analizy mogą być wykorzystywane w procesie tworzenia baz danych dotyczących infrastruktury krytycznej. Bazy te będą w przyszłości narzędziem wykorzystywanym przez CIRC Sił Zbrojnych RP (Centrum Koordynacyjne Sił Zbrojnych RP).

2. Identyfikacja punktów kontaktowych w zakresie infrastruktury krytycznej w Ministerstwie Obrony Narodowej, Sztabie Generalnym WP, w poszczególnych Rodzajach Sił Zbrojnych oraz jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej.
3. Zgromadzenie informacji na temat rozwiązań prawnych i organizacyjnych w zakresie ochrony infrastruktury krytycznej.
4. Poznanie technologicznych aspektów funkcjonowania infrastruktury krytycznej. Uzyskanie informacji o bazach danych, Zautomatyzowanych Systemach Dowodzenia, Zautomatyzowanych Systemach Dowodzenia i Kierowania Walką, Zautomatyzowanych Systemach Zarządzania, sposobach ich zabezpieczenia przed zniszczeniem, zasobach map cyfrowych, aplikacjach służących wspomaganiu procesu podejmowania decyzji i dokonywania analiz, obiektach, budowlach i systemach wymagających szczególnej ochrony, wykorzystywaniu technik satelitarnych do ochrony infrastruktury krytycznej.
5. Analiza sposobów zabezpieczenia infrastruktury krytycznej przed nielegalną ingerencją w systemy teleinformatyczne, teleinformacyjne i łączności.
6. Zbadanie oddziaływania czynników zewnętrznych takich jak: destabilizacja organizacyjna i ekonomiczna. Przedmiotem zainteresowania są także plany operacyjne i procedury na wypadek zagrożenia i zniszczenia infrastruktury krytycznej.
7. Określenie możliwości zdolności odbudowy infrastruktury krytycznej. Szczegółowy zakres zagadnień dotyczy planów i procedur odbudowy infrastruktury krytycznej, sposobów utrzymania zasadniczych funkcji infrastruktury krytycznej, a także możliwości odbudowy systemów teleinformatycznych, teleinformacyjnych i łączności służących do ochrony infrastruktury krytycznej.
8. Zbadanie współpracy zagranicznej w zakresie ochrony infrastruktury krytycznej, uczestnictwo w jej instytucjonalnych formach, wykorzystanie międzynarodowych baz danych i prowadzenie bieżącej wymiany informacji z partnerami zagranicznymi.
9. Ponieważ samo pojęcie infrastruktury krytycznej a w szczególności Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski funkcjonuje w Polsce od niedawna, określenie które z sektorów zaproponowanej definicji są najbardziej istotne i na które elementy należy zwrócić największą uwagę.

OPIS WYNIKÓW I INTERPRETACJA

W tej części raportu przedstawiam najbardziej interesujące moim zdaniem wyniki badań. Każdy z przedstawionych poniżej wykresów obrazuje zbiorcze zestawienie odpowiedzi na jedno poszczególne pytanie kwestionariusza ankiety do rozprawy doktorskiej. Cyfry w opisie i w tytule wykresu oznaczają odpowiednio numer pytania z kwestionariusza ankiety.

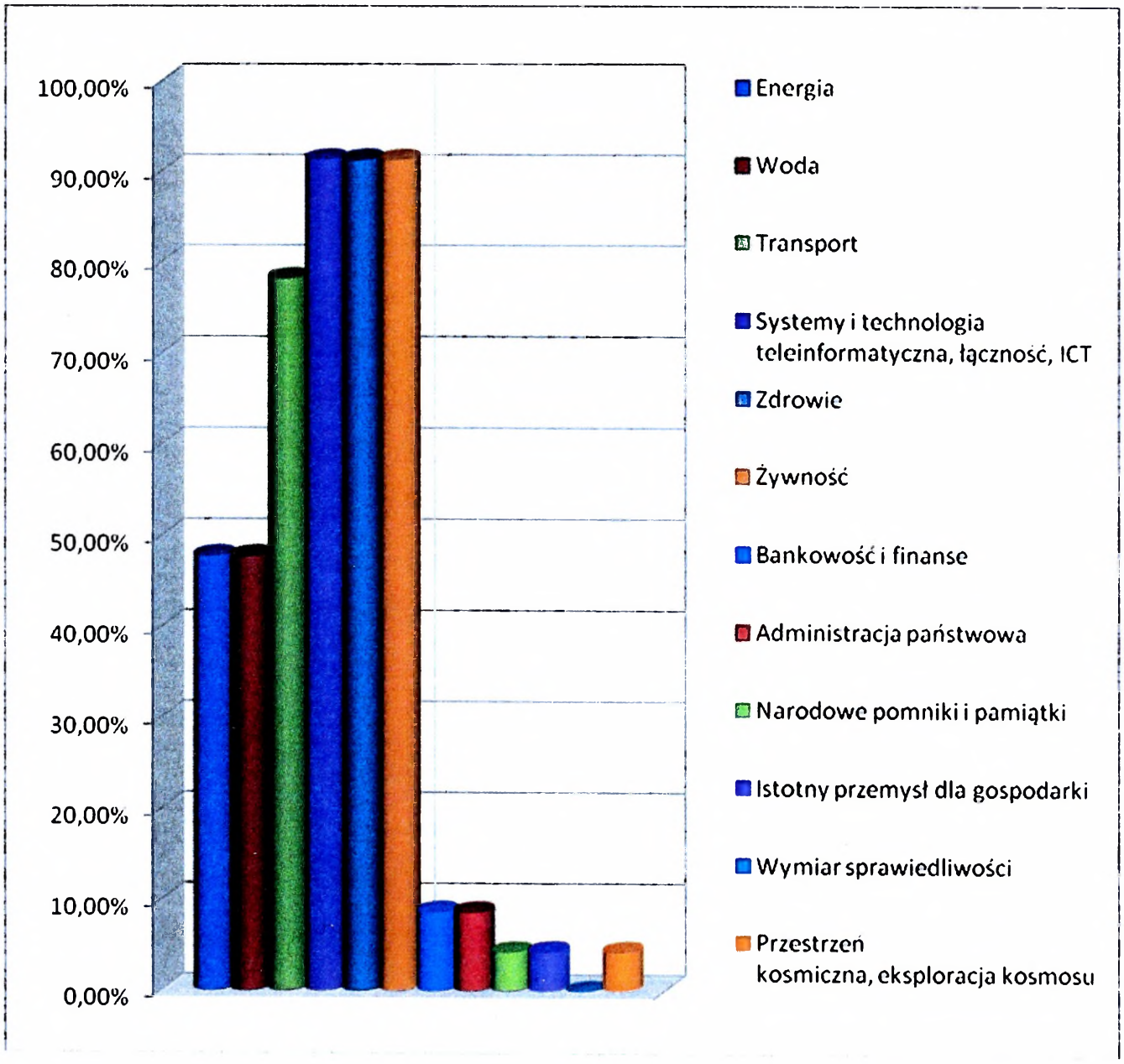


Wykres 1. Sektory krytyczne Infrastruktury Krytycznej Państwa należące do Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski

Wykres 1 opisuje sposób postrzegania sektorów krytycznych Infrastruktury Krytycznej Państwa właściwych (zgodnie z definicją podaną w kwestionariuszu ankiety) dla jednostek organizacyjnych podległych Ministrowi Obrony Narodowej wypełniających kwestionariusz ankiety. Od 86,95% do 100% wypełniających wskazało następujące sektory krytyczne Infrastruktury Krytycznej Państwa należące do Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski:

- Energia;
- Woda;
- Transport;
- Systemy i technologia teleinformatyczna, łączność, ICT;
- Zdrowie;
- Żywność.

Wartości 52,17% otrzymał tak ważne sektory dla Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski, jak sektor administracji publicznej a sektor istotny przemysł dla gospodarki otrzymał 65,21%.



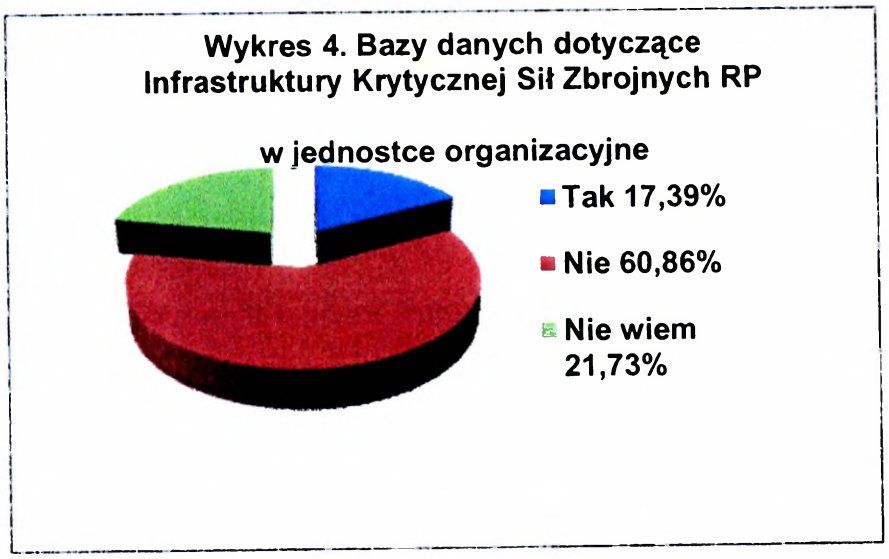
Wykres 2. Sektory krytyczne Infrastruktury Krytycznej Państwa pozostające w zakresie kompetencji jednostek organizacyjnych podległych Ministrowi Obrony Narodowej

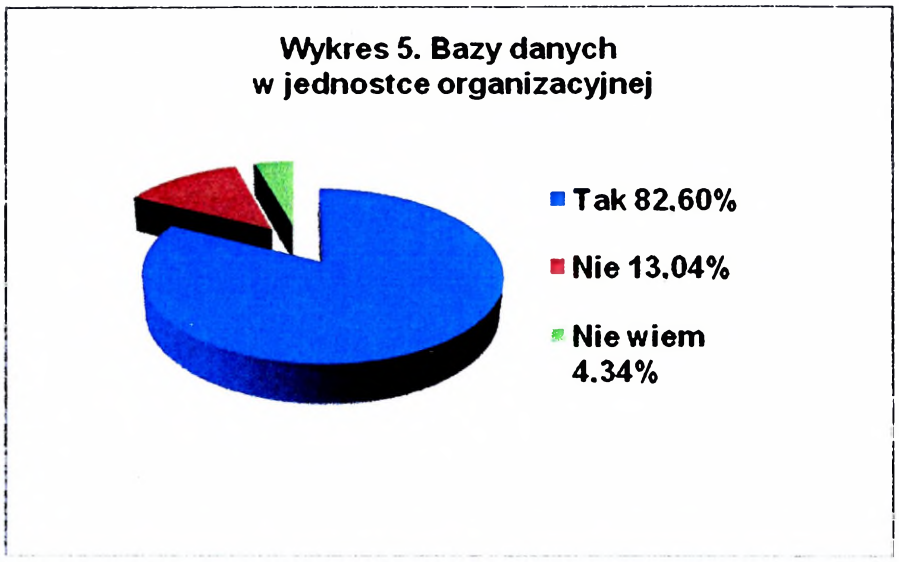
Wykres 2 przedstawia jak jednostki organizacyjne podległe Ministrowi Obrony Narodowej klasyfikują pozostające w ich zakresie kompetencji Infrastrukturę Krytyczną Państwa. Ponad 90% jednostek organizacyjnych wskazało jedynie na takie sektory jak:

- Systemy i technologia teleinformatyczna, łączność, ICT;
- Zdrowie;
- Żywność.

Analizując Wykresy 1 i 2 należy zwrócić uwagę, iż w znacznej większości jednostki administracyjne podległe Ministrowi Obrony Narodowej, zawężają pojęcie Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski do posiadanych przez siebie zasobów (segmenty stanowiące zakres właściwy dla nich kompetencji). Takie podejście ma zasadnicze znaczenie dla dalszych wyników prowadzonej analizy kwestionariusza ankiety.





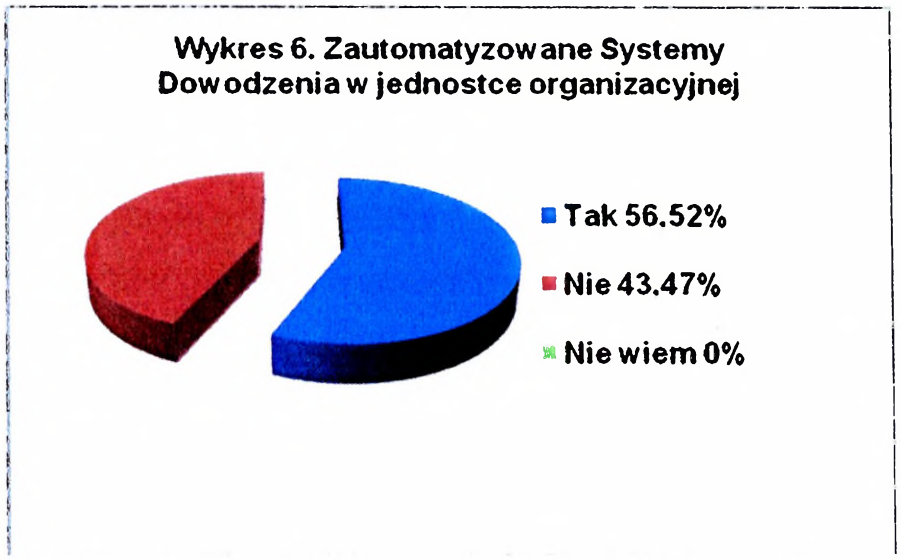


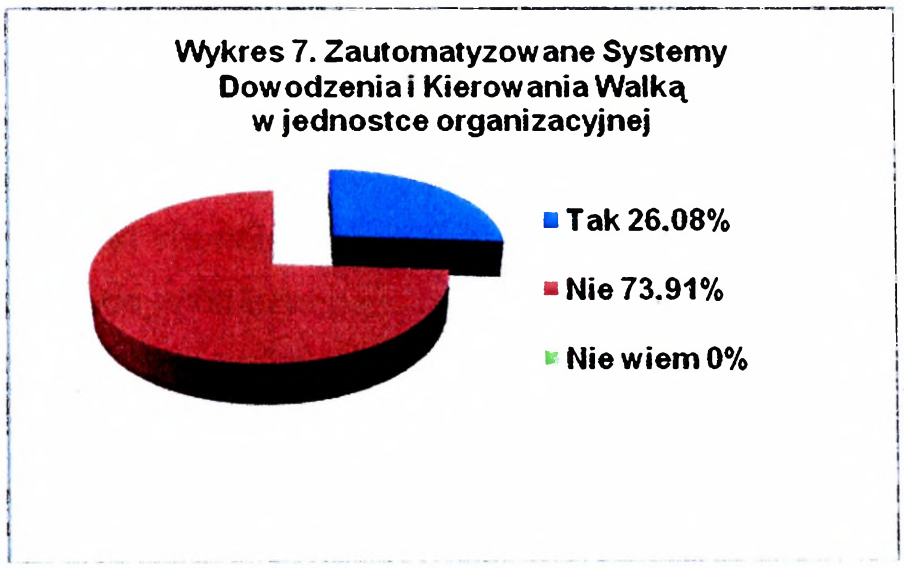
Wykresy 3,4 i 5 przedstawiają aktualny stan teleinformatycznych baz danych, baz danych oraz baz danych dotyczących Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Większość ankietowanych posiada bazy danych (82,60%) oraz teleinformatyczne bazy danych (86,95%), co pokazuje, że ponad 80% jednostek organizacyjnych podległych Ministrowi Obrony Narodowej posiada bazy danych. Tylko 17,39% ankietowanych posiada bazy danych dotyczące Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. 13,04% respondentów nie posiada żadnych baz danych, a 60,86% nie posiada baz danych dotyczących Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski, natomiast 21,73% nie wykazało informacji na temat czy posiada bazy danych dotyczące Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Większość ankietowanych posiada zabezpieczenia baz danych, zgodnie z obowiązującymi dokumentami i wytycznymi wyższych przełożonych.

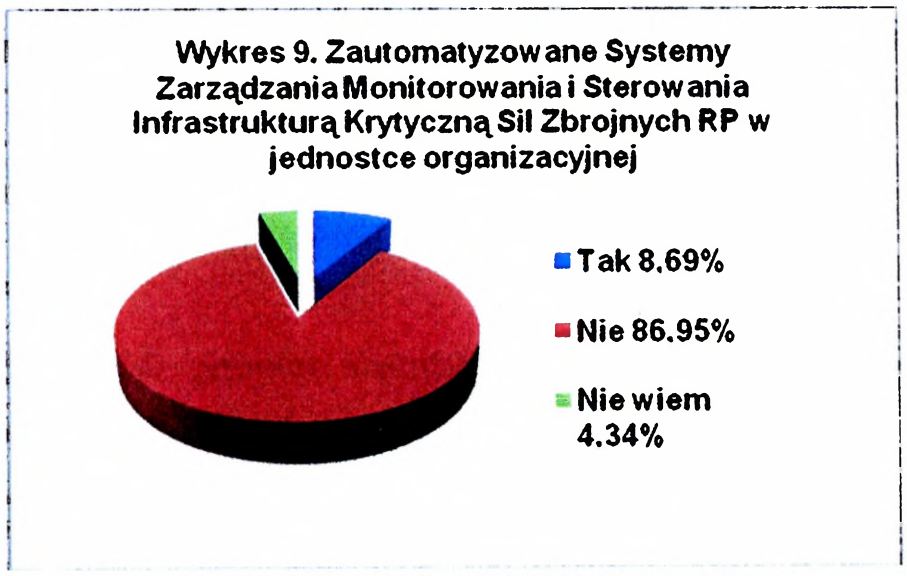
Bazy danych, zgodnie z wynikami kwestionariusza ankiety, są bardzo ważnym i istotnym elementem Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Bazy danych mogą również być jako autonomiczne narzędzie potrzebne jej funkcjonowaniu i ochronie. Wyniki przedstawione na wyżej wymienionych wykresach, nie pozwalają rozróżnić stopnia złożoności i zakresu baz danych. Najczęściej wymieniane przez jednostki organizacyjne bazy danych dotyczą:

- ***Logistycznego wsparcia działań;***
- ***Ewidencji kadr i pracowników wojska;***
- ***Gotowości bojowej.***

Zakres wyżej wymienione bazy danych, dotyczy tylko obsługi bieżącej samych jednostek organizacyjnych podległych Ministrowi Obrony Narodowej.







Wykresy 6,7 i 9 pokazują ile jednostek organizacyjnych podległych Ministrowi Obrony Narodowej posiada: Zautomatyzowane Systemy Dowodzenia, Zautomatyzowane Systemy Dowodzenia i Kierowania Walką oraz Zautomatyzowane Systemy Zarządzania, Monitorowania i Sterowania Infrastrukturą Krytyczną Sił Zbrojnych Rzeczypospolitej Polski. 56,52% jednostek posiada Zautomatyzowane Systemy Dowodzenia, a 26,08% ma Zautomatyzowane Systemy Dowodzenia

i Kierowania Walką. Jak wynika z wykresu 6 i 7 około połowa podmiotów nie posiada żadnych zautomatyzowanych systemów. Wykres 9 pokazuje szczegółowo ilość posiadanych przez jednostki Zautomatyzowane Systemy Zarządzania, Monitorowania i Sterowania Infrastrukturą Krytyczną Sił Zbrojnych Rzeczypospolitej Polski. Jedynie 8,69%[2] wykazało posiadanie takich systemów.

Zautomatyzowane Systemy Zarządzania, Monitorowania i Sterowania Infrastrukturą Krytyczną Sił Zbrojnych Rzeczypospolitej Polski wykorzystywane są obecnie wyłącznie przez jednostki organizacyjne podległe bezpośrednio „urzędom centralnym" Ministra Obrony Narodowej. Jak wynika z analizy kwestionariusza ankiety żadna jednostka organizacyjna od Dowództw Rodzajów Sił Zbrojnych nie posiada takich systemów w odniesieniu do sektorów Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski posiadających w zakresie kompetencji tych jednostek.

Wykres 10. Wykorzystywanie map cyfrowych w jednostce organizacyjnej



Wykres 10 pokazuje w jakim stopniu jednostki organizacyjne wykorzystują mapy cyfrowe. 73,91% ankietowanych posiada mapy cyfrowe, a 21,73% nie wykorzystuje żadnych map cyfrowych dla swoich potrzeb.

Mapa cyfrowa jest jednym z podstawowych aplikacji, które wykorzystuje się dla potrzeb Zautomatyzowanych Systemów Dowodzenia, Zautomatyzowanych Systemów Dowodzenia i Kierowania Walką oraz Zautomatyzowanych Systemów Zarządzania, Monitorowania i Sterowania Infrastrukturą Krytyczną Sił Zbrojnych Rzeczypospolitej Polski. Z wyników kwestionariusza ankiety wynika, że aplikacja ta, jest szeroko wykorzystywana

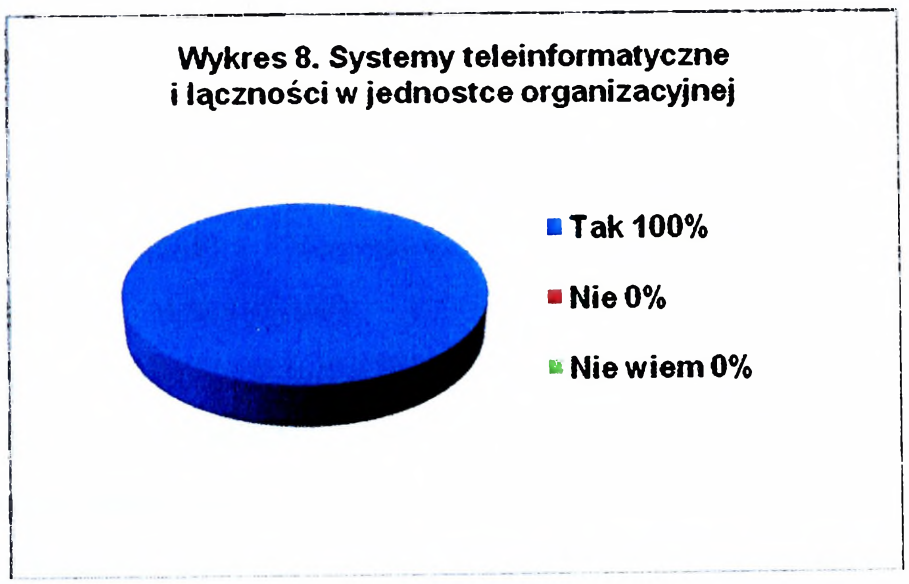
[2] Wartość 8,69% przedstawia dokładnie dwa ankietowane podmioty podległe Ministrowi Obrony Narodowej.

w Siłach Zbrojnych (73,91%), szczególnie przez sztaby jednostek organizacyjnych podległych Ministrowi Obrony Narodowej.

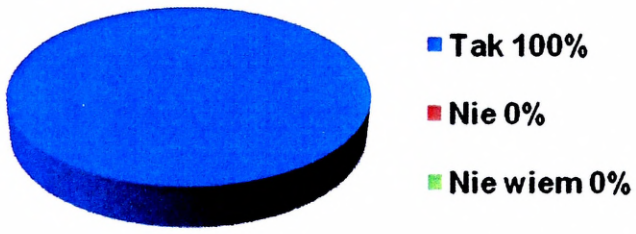


Wykres 11 przedstawia w jakim zakresie wykorzystywane są teleinformatyczne aplikacje wspomagające proces podejmowanie decyzji w jednostkach organizacyjnych. Wyżej wymienione aplikacje posiada niespełna 56,52% ankietowanych podmiotów.

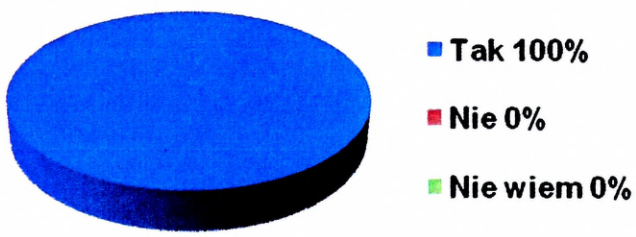
Dogłębna analiza danych zawarta w kwestionariuszu ankiety pokazuje, iż w posiadaniu jednostek organizacyjnych podległych Ministrowi Obrony znajdują się aplikacje, wykorzystywane tylko dla potrzeb sprawnego funkcjonowania samej jednostki organizacyjnej, nie zaś Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Narzędzia te posiadają jedynie podmioty podległe bezpośrednio „urzędom centralnym" Ministra Obrony Narodowej.



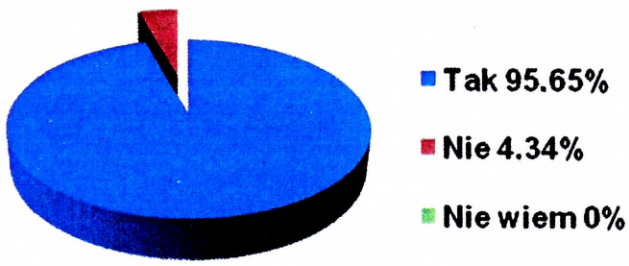
Wykres 12. Wykorzystywanie publicznej łączności jawnej w jednostce organizacyjnej



Wykres 13. Wykorzystywanie służbowej łączności jawnej w jednostce organizacyjnej



Wykres 14. Wykorzystywanie łączności niejawnej w jednostce organizacyjnej





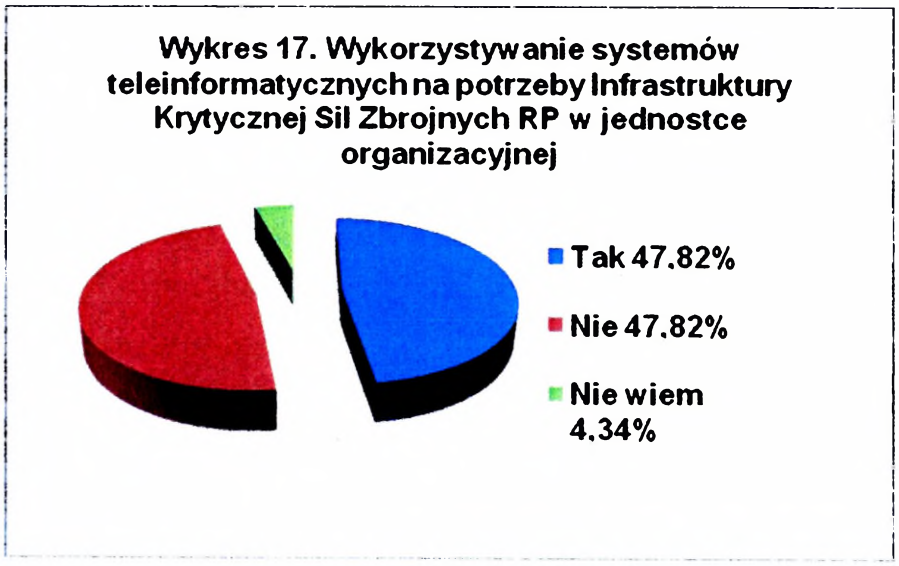


Wykresy 8,12,13,14,15 oraz 16 pokazują wykorzystanie systemów łączności jawnych i niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony. 100% podmiotów wykorzystuje: publiczną łączność jawną, służbową łączność jawną. Prawie 100% ankietowanych wykorzystuje łączność niejawną. Tylko 4,34% podmiotów nie wykorzystuje tego rodzaju łączności. Jest to spowodowane prawdopodobnie, brakiem odpowiednich systemów łączności w ankietowanej jednostce organizacyjnej. Ponad 50% jednostek organizacyjnych wykorzystuje łączność satelitarna. Powodem jest obecną sytuacją polityczno – militarną, która zaistniała po wydarzeniach 11 września 2001 r.[3]. 86,95% ankietowanych wskazało że, w jednostkach organizacyjnych wykorzystuje łączność wewnętrzną do prawidłowego funkcjonowania poszczególnych komórek organizacyjnych.

W codziennej działalności systemy i środki łączności są powszechnie wykorzystywane przez jednostki organizacyjne podległe Ministrowi Obrony

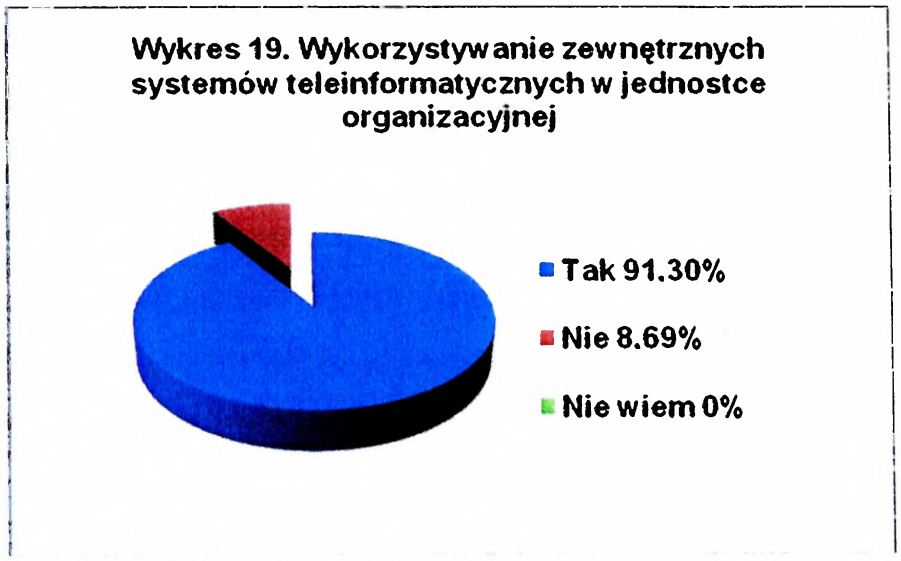
[3] Nasze wojska pełnią obecnie służbę w Iraku, Afganistanie, Syrii, Kosowie oraz wielu innych regionach zapalnych. Łączność satelitarna jest obecnie szybkim i bezpiecznym militarnym medium do przekazywania informacji pomiędzy poszczególnymi jednostkami organizacyjnymi. System łączności satelitarnej umożliwia łączność telefoniczną i transmisję danych prawie na całym świecie.

Narodowej, jedynie różni rodzaj dostępnej łączności. Do przekazywania informacji jawnych wykorzystywana jest służbowa i publiczna łączność jawna. Jeżeli jest informacja klasyfikowana to wykorzystywana jest łączność niejawna. Do prawidłowego zabezpieczenia łączności wykorzystywane jest całe spektrum technologiczne (telefony stacjonarne, faxy, telefony komórkowe, radiolinie, radiostacje zakresu VHF/UHF/HF oraz systemy łączności satelitarnej). Trzeba zaznaczyć że, coraz częściej wykorzystywane są satelitarne systemy łączności.



Wykres 17 przedstawia posiadane przez ankietowane jednostki organizacyjne systemy teleinformatyczne wykorzystywane na potrzeby Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. 47,82% ankietowanych podmiotów posiada takie systemy, natomiast 47,82% nie posiada ich. 4,34% odpowiedzi to odpowiedź „Nie wiem".

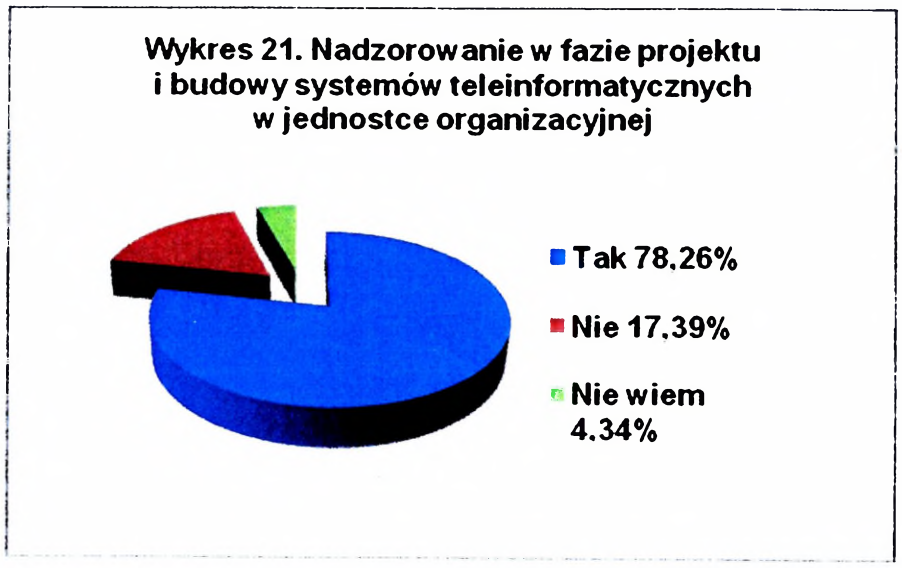






Wykresy 18,19 i 20 pokazują posiadane i nadzorowane przez jednostki organizacyjne podległe Ministrowi Obrony Narodowej jawne i niejawne systemy teleinformatyczne. Ponad 90% ankietowanych podmiotów wykorzystuje systemy teleinformatyczne do zabezpieczenia prawidłowej łączności pomiędzy poszczególnymi komórkami organizacyjnymi Ministerstwa Obrony Narodowej.

Trzeba zauważyć że, 82,60% ankietowanych jednostek organizacyjnych wykorzystuje niejawne systemy teleinformatyczne na potrzeby zapewnienia prawidłowej wymiany danych, jako istotnego elementu podtrzymującego funkcjonowanie tego bardzo ważnego i specyficznego sektora Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.



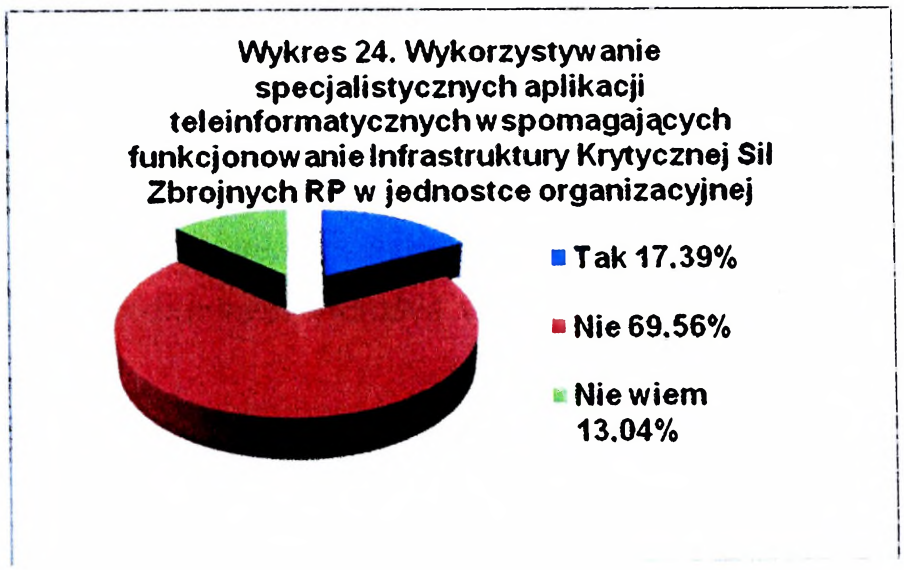
Wykres 21 przedstawia, ile ankietowanych podmiotów nadzoruje i posiada w fazie projektu systemy teleinformatyczne które wymagają szczególnej ochrony. 78,26% nadzoruje i posiada w fazie projektu i budowy systemy teleinformatyczne, a 17,39% ich nie posiada.





Powyższe dwa Wykresy 22 i 23 pokazują wykorzystanie jawnej i niejawnej łączności satelitarnej do ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.

Z przedstawionych danych wynika że, tylko 17,39% ankietowanych jednostek organizacyjnych wykorzystuje szeroko rozumianą łączność satelitarną do ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.



Wykres 24 przedstawia wykorzystanie przez ankietowane jednostki organizacyjne specjalistycznych aplikacji (programów) teleinformatycznych wspomagających funkcjonowanie Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Tylko 17,39% podmiotów posiada wyżej wymienione oprogramowanie, a 69,56% nie posiada.

Analiza kwestionariusza ankiety wskazuje, iż tylko jedynie około 17% jednostek organizacyjnych wykorzystuje specjalistyczne oprogramowanie do wspomagania i prawidłowego funkcjonowania Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.



Wykres 25 przedstawia stopień wykorzystania przez ankietowane jednostki organizacyjne, specjalistycznego oprogramowania do zarządzania bazami danych. 34,78% ankietowanych wykazało że, posiada takie oprogramowanie. 65,21% jednostek organizacyjnych odpowiedziało że, nie dysponuje takim oprogramowaniem.

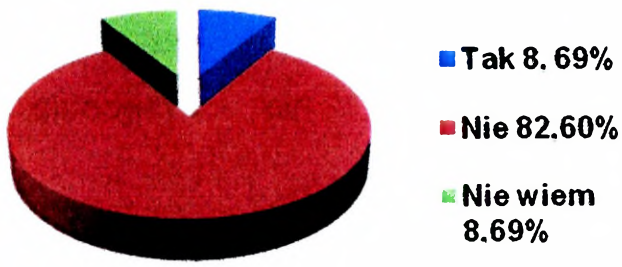
Aplikacje teleinformatyczne do zarządzania bazami danych w jednostkach organizacyjnych, są wykorzystywane w małym zakresie i głównie dla potrzeb odpowiedniego zabezpieczenia tych baz. W odpowiedziach kwestionariusza ankiety nie podano przykładów aplikacji teleinformatycznych umożliwiających zobrazowanie zasobów tych baz danych.



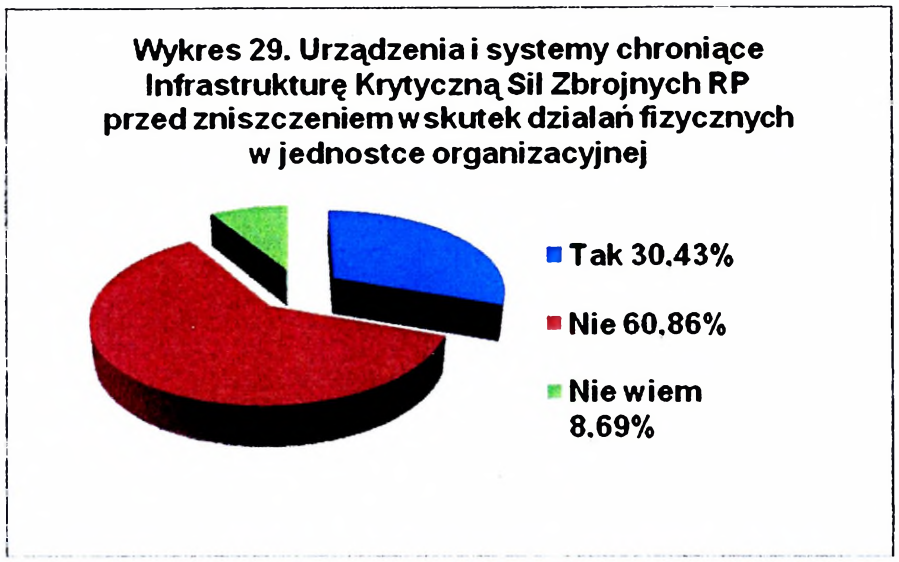
Wykres 27. Wykorzystywanie specjalistycznych aplikacji i urządzeń teleinformatycznych wspomagających bezpieczeństwo łączności w jednostce organizacyjnej



Wykres 28. Wykorzystywanie aplikacji monitorujących Infrastrukturę Krytyczną Sił Zbrojnych RP w jednostce organizacyjnej



Wykresy 26, 27 i 28 pokazują ile podmiotów ankietowanych monitoruje zagrożenie związane z bezpieczeństwem teleinformatycznym i bezpieczeństwem łączności, a w szczególności aplikacji monitorujących Infrastrukturę Krytyczną Sił Zbrojnych Rzeczypospolitej Polski. Około 80% jednostek organizacyjnych posiada specjalistyczne aplikacje i urządzenia teleinformatyczne wspomagające bezpieczeństwo teleinformatyczne i teleinformacyjne. Jedynie 8,69% posiada odpowiednie „oprzyrządowanie" do monitorowania Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.



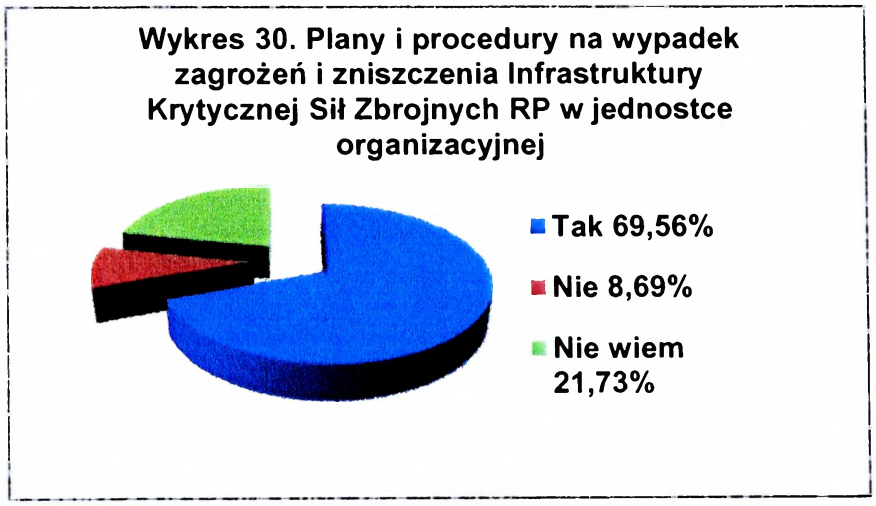
Wykres 29 pokazuje zabezpieczenia (urządzenia i systemy), Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski przed zniszczeniem wskutek działań fizycznych. Tylko 30,43% jednostek organizacyjnych posiada odpowiednie zabezpieczenia infrastruktury krytycznej. 60,86% badanych podmiotów nie jest w posiadaniu, pozostałe 8,69% odpowiedziało „Nie wiem".

Stosunek liczby jednostek organizacyjnych podległych Ministrowi Obrony Narodowej, które posiadają urządzenia i systemy chroniące Infrastrukturę Krytyczną Sił Zbrojnych Rzeczypospolitej Polski przed zniszczeniem wskutek działań fizycznych do liczby podmiotów wskazujących na brak takich zabezpieczeń można określić jako niezadawalający. Problematyczne są dwa zagadnienia:

- ***Poziom i jakość zabezpieczeń realizowanych przez poszczególne jednostki organizacyjne;***
- ***Bardzo duża liczna jednostek organizacyjnych wskazująca, że nie ma odpowiednich zabezpieczeń.***

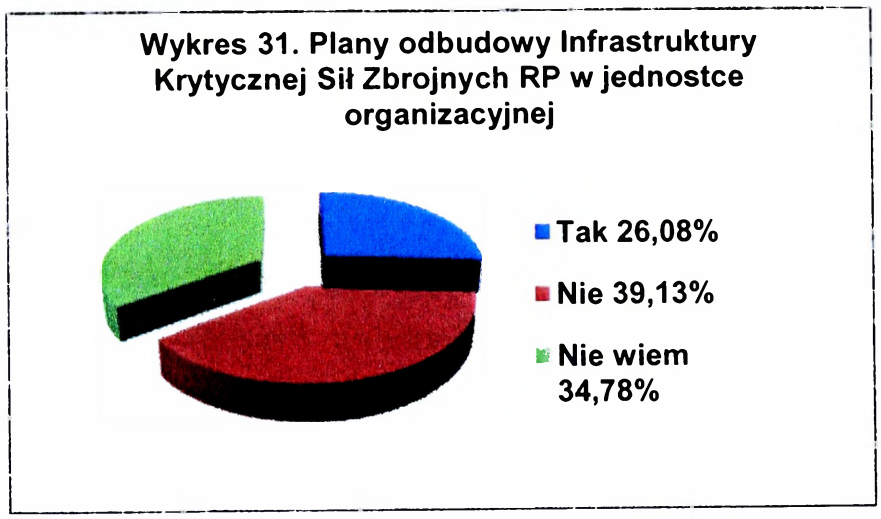
Można przypuszczać, że w bardzo dużej ilość ankietowanych podmiotów poziom zabezpieczenia ogranicza się do podstawowej fizycznej ochrony obiektów administracyjnych. Sytuacja taka dotyczy przede wszystkim podmiotów, które postrzegają swoje zadania z zakresu ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski, jako ochrony własnych obiektów znajdujących się w strefie administracyjnej i strefach bezpieczeństwa (Wykres 1 i 2). Bardzo istotne znaczenie ma fakt wskazania: 60,86% badanych podmiotów nie jest w posiadaniu, 8,69% odpowiedziało „Nie wiem". Biorąc pod uwagę znaczenie Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski, a także obecność jej i powiązania niemal w każdym sektorze

administracji, brak „zainteresowania" tym zagadnieniem przez jednostki organizacyjne stanowi zaniepokojenie.



Wykres 30 przedstawia ile ankietowanych jednostek organizacyjnych podległych Ministrowi Obrony posiada plany i procedury operacyjne na wypadek zagrożeń i zniszczenia Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. 69,56% posiada plany i procedury operacyjne, 8,69% nie posiada żadnych planów i procedur. Pozostałe 21,73% odpowiedziało „Nie wiem".

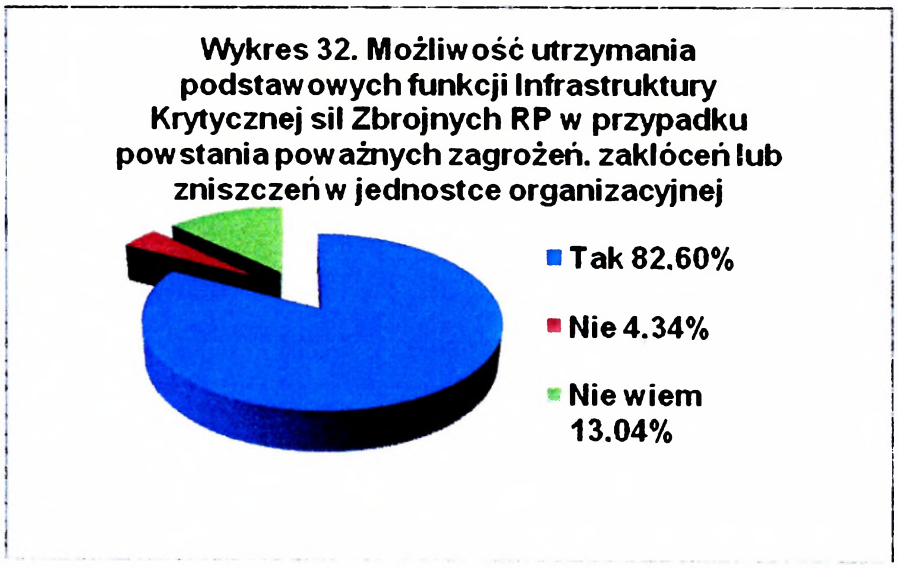
Odsetek ankietowanych jednostek organizacyjnych posiadających plany i procedury operacyjne jest wyższa niż jednostek dysponujących odpowiednimi zabezpieczeniami zwiększającymi bezpieczeństwo fizyczne.



Wykres 31 przedstawia odsetek jednostek organizacyjnych podległych Ministrowi Obrony Narodowej posiadających plany odbudowy Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. 26,08% ankietowanych jednostek

posiada takie plany. Następne 39,13% jednostek nie posiada żadnych planów. Pozostałe 34,78% odpowiedziało „Nie wiem".

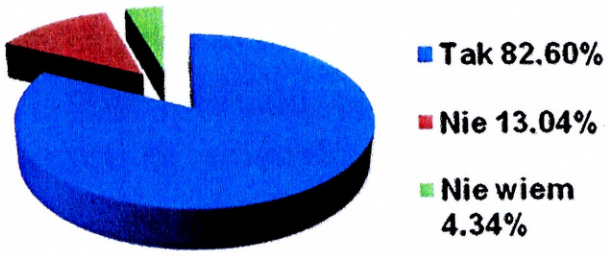
Udzielając odpowiedzi na pytanie ogólne, dotyczące planów i procedur operacyjnych na wypadek zagrożeń i zniszczenia Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski, jednostki organizacyjne deklarują w kwestionariuszu ankiety posiadanie większych zasobów. W wypadku pytań szczegółowych zasoby te okazują się znacznie mniejsze. Prawdopodobnie powodem tym jest, że przy opracowywaniu planów i procedur operacyjnych, jednostki organizacyjne nie uwzględniają konieczności odbudowy i podtrzymania podstawowych funkcji Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.



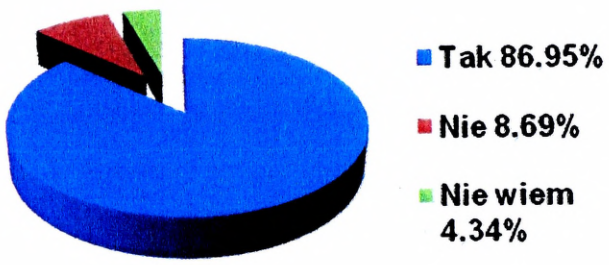
Wykres 32 prezentuje jak jednostki organizacyjne podległe Ministrowi Obrony Narodowej posiadają możliwości utrzymania podstawowych funkcji Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski w przypadku powstania poważnych zagrożeń, zakłóceń lub zniszczeń. 82,60% ankietowanych jednostek organizacyjnych jest w stanie zapewnić funkcjonowanie Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. 4,34% badanych nie jest w stanie utrzymać podstawowych funkcji a 13,04% odpowiedziało „Nie wiem".

82,60% pozytywnych odpowiedzi należy ocenić jako wynik zadawalający. Wynik ten budzi poważne zastrzeżenia wynikające z analizy Wykresu 31. Pod wielkim znakiem zapytania stoi zdolność utrzymania podstawowych funkcji Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski w przypadku powstania poważnych zagrożeń, zakłóceń lub zniszczeń przy braku jakichkolwiek planów jej odbudowy.

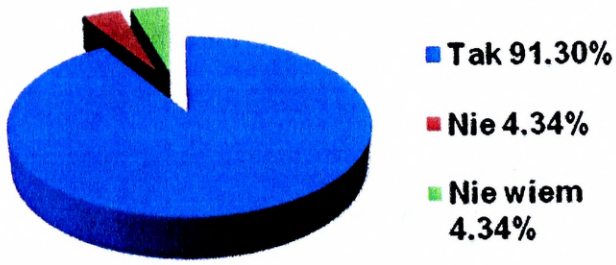
Wykres 33. Możliwość odbudowy systemów teleinformatycznych w jednostce organizacyjnej

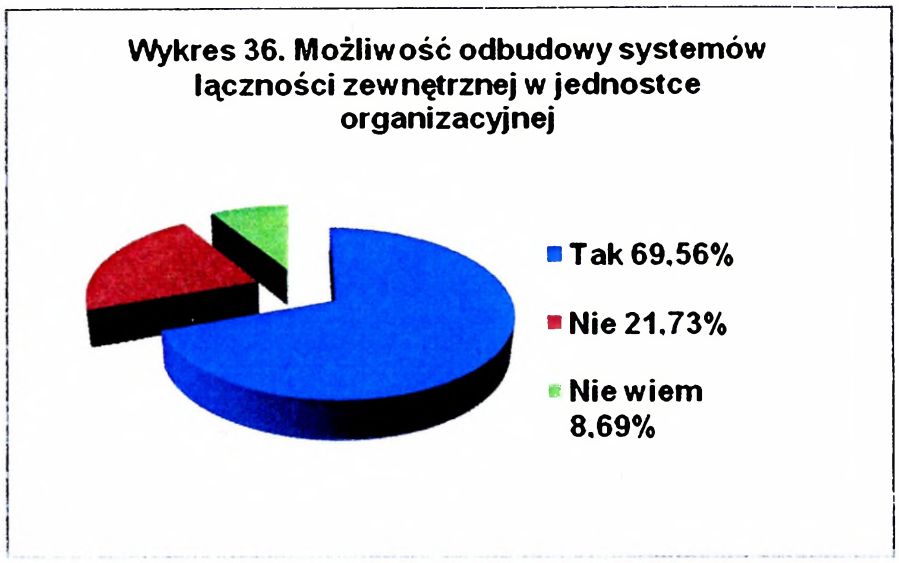


Wykres 34. Możliwość odbudowy systemów łączności niejawnej w jednostce organizacyjnej



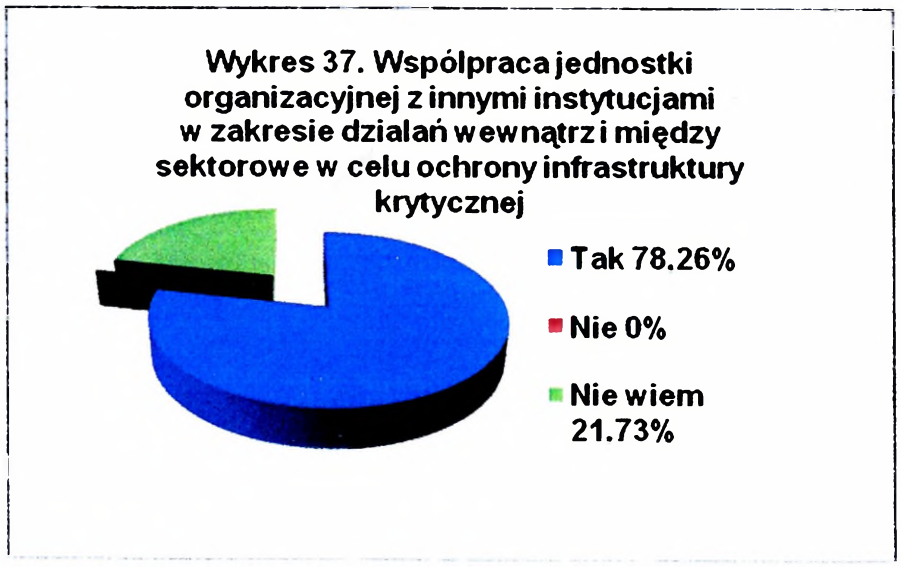
Wykres 35. Możliwość odbudowy systemów łączności wewnętrznej w jednostce organizacyjnej





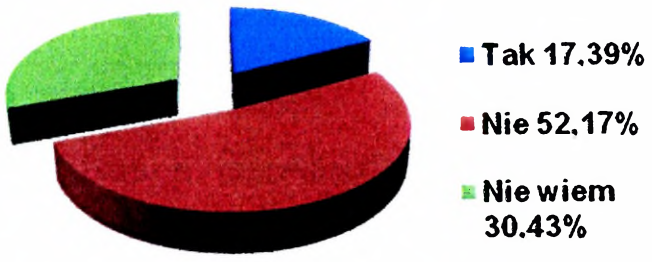
Wykresy 33, 34, 35 oraz 36 przedstawiają możliwości a ankietowanych jednostek organizacyjnych podległych Ministrowi Obrony Narodowej w zakresie odbudowy systemów teleinformatycznych, systemów łączności jawnej i niejawnej oraz systemów łączności wewnętrznej i systemów łączności zewnętrznej. Ponad 70% ankietowanych podmiotów posiada możliwości odbudowy wyżej wymienionych systemów.

Podobnie jak w wypadku poprzednich danych, procent pozytywnych odpowiedzi na pytania szczegółowe: Odbudowa systemów teleinformatycznych, systemów łączności jawnej i niejawnej oraz systemów łączności wewnętrznej i systemów łączności zewnętrznej, jest znacznie większy od procentu pozytywnych odpowiedzi na pytanie bardziej ogólne dotyczące planów odbudowy Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Stawia to pod znakiem zapytania wiarygodność odpowiedzi w kwestionariuszu ankiety.

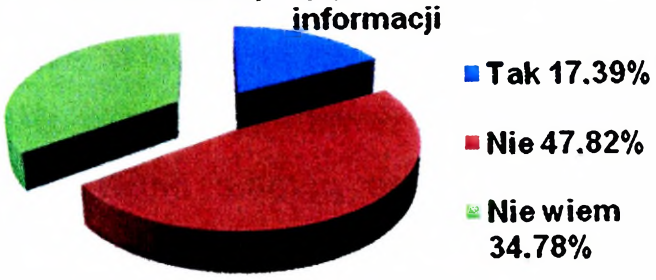


Wykres 37 przedstawia możliwości współpracy jednostek organizacyjnych podległych Ministrowi Obrony Narodowej z innymi instytucjami w zakresie wewnątrz i między sektorowe w celu ochrony Infrastruktury Krytycznej. 78,26% ankietowanych podmiotów wskazało na prowadzenie takiej współpracy.

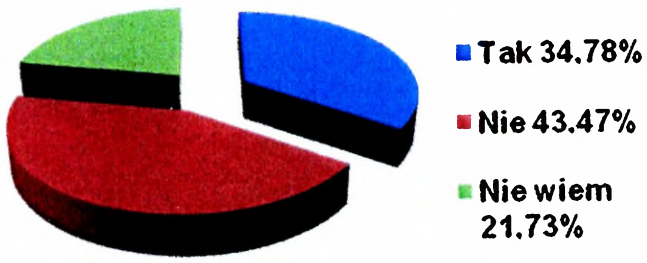
Wykres 38. Współpraca jednostki organizacyjnej z instytucjami międzynarodowymi w zakresie ochrony infrastruktury krytycznej



Wykres 39. Współpraca jednostki organizacyjnej na bieżąco z instytucjami międzynarodowymi w zakresie ochrony infrastruktury krytycznej w celu wymiany informacji



Wykres 40. Korzystanie przez jednostke organizacyjną z międzynarodowych baz danych i zasobów w celu ochrony infrastruktury krytrycznej



Wykres 38, 39 i 40 obrazuje współprace międzynarodową jednostek organizacyjnych podległych Ministrowi Obrony Narodowej w zakresie ochrony Infrastruktury Krytycznej oraz z korzystania z międzynarodowych baz danych i zasobów w celu ochrony Infrastruktury Krytycznej. 17,39% ankietowanych wskazało na prowadzenie współpracy, a 34,78% że korzysta z międzynarodowych baz danych.

Bardzo mały odsetek ankietowanych jednostek organizacyjnych prowadzi współprace międzynarodową w zakresie ochrony Infrastruktury Krytycznej, uczestniczy w instytucjonalnych formach współpracy, korzysta z międzynarodowych baz danych, prowadząc na bieżąco wymianę informacji z zagranicznymi partnerami (NATO CIRC) – wynika prawdopodobnie z faktu, że problematyka Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski jest nową i nie wszystkie jednostki organizacyjne zdążyły nawiązać odpowiednią współprace w tym zakresie.

Wykres 41. Zastosowanie w jednostce organizacyjnej urządzeń i systemów które chronią Infrastrukturę Krytyczną Sil Zbrojnych RP przed zniszczeniem w skutek działań fizycznych



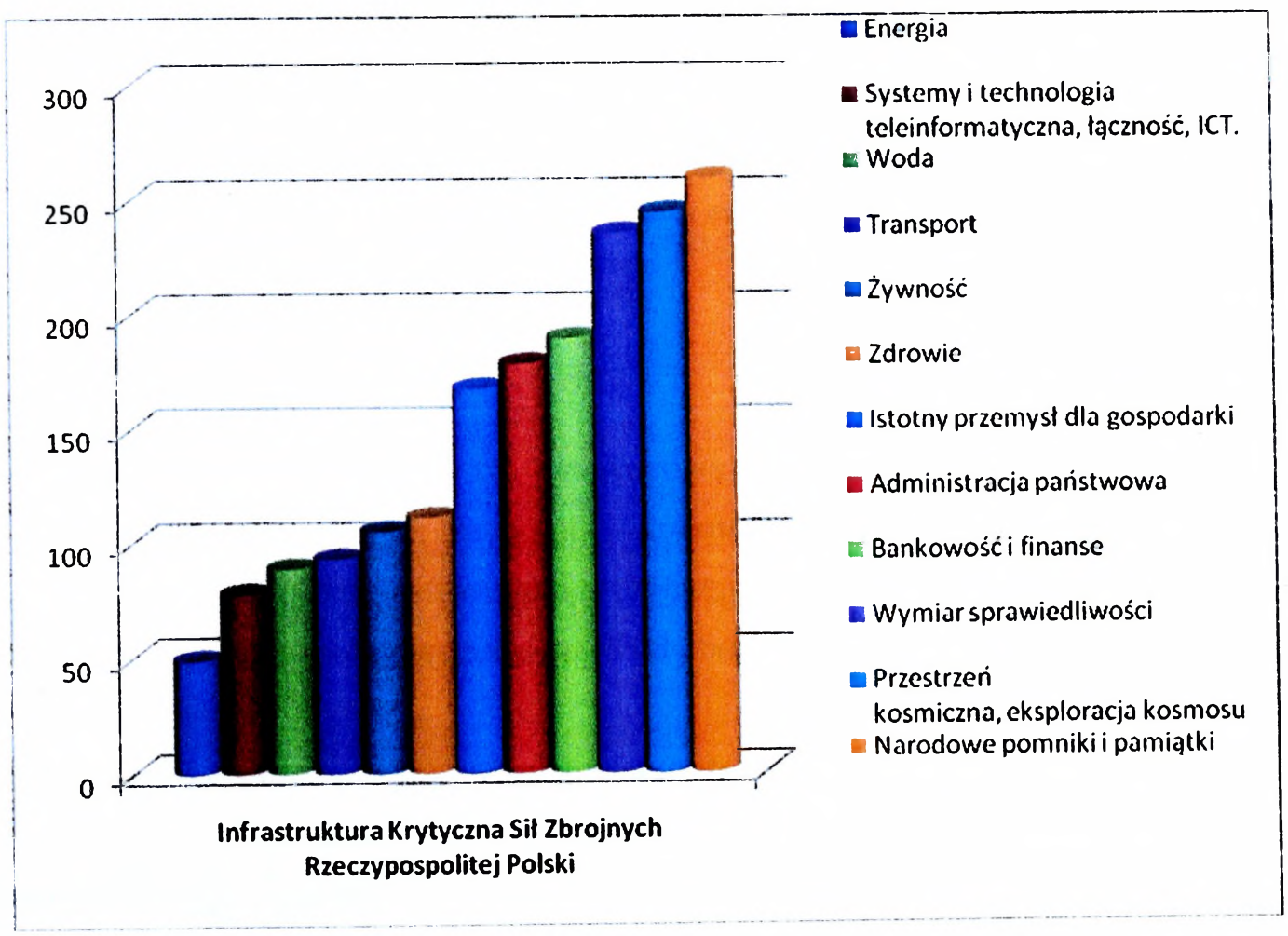
Wykres 41 przedstawia zastosowanie w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej urządzeń i systemów które chronią Infrastrukturę Krytyczną Sił Zbrojnych Rzeczypospolitej Polski przed zniszczeniem wskutek działań fizycznych. Ponad 60% ankietowanych podmiotów wskazało pozytywną odpowiedź.

W wypadku poprzednich danych (Wykres 29), procent pozytywnych odpowiedzi na pytanie: Czy w jednostce organizacyjnej są urządzenia i systemy które chronią Infrastruktura Krytyczna Sił Zbrojnych Rzeczypospolitej Polski przed zniszczeniem wskutek działań fizycznych, jest znacznie mniejszy od procentu pozytywnych odpowiedzi na pytanie

zamieszczone powyżej. Stawia to znowu pod znakiem zapytania wiarygodność odpowiedzi w kwestionariuszu ankiety.

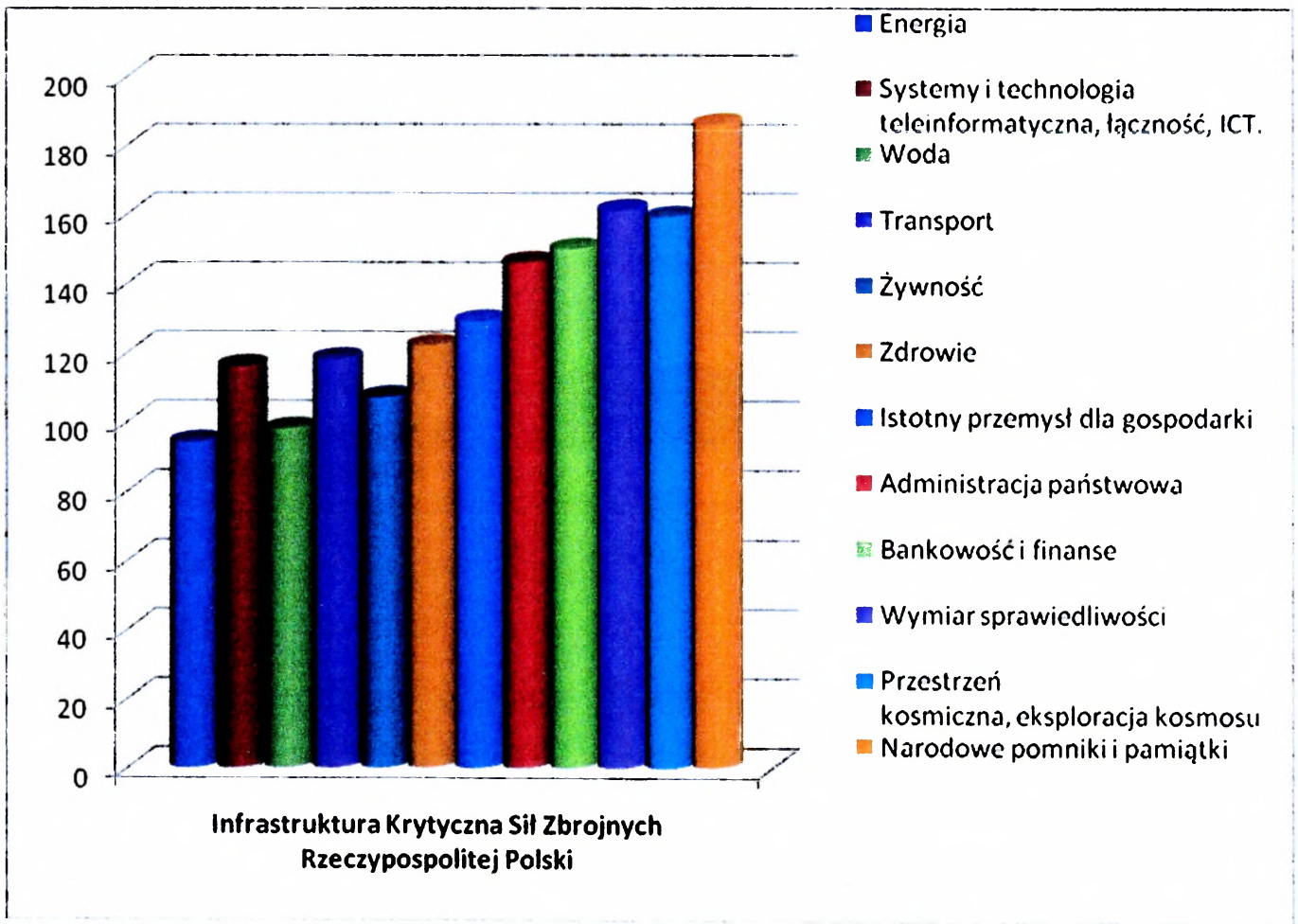
W końcowej partii, zasadniczej części kwestionariusza ankiety, jednostki organizacyjne podległe Ministrowi Obrony Narodowej zostały poproszone o wskazanie najbardziej istotnych sektorów Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Ankietowanym przedstawiono trzy pytania. Pierwsze dwa pytania miały na celu uzyskanie informacji o sposobie postrzegania najważniejszych sektorów definicji Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski zaproponowanej w kwestionariuszu ankiety. Udzielając odpowiedzi na trzecie pytanie ankietowani mieli wskazać kryteria, jakimi kierowali się przepisując ważność poszczególnych sektorów Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.

W pytaniu pierwszym należało uporządkować według istotności elementy definicji Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Poniżej przedstawiam wyniki:



Energia, systemy i technologia teleinformatyczna, łączność, ICT oraz woda zostały przez jednostki organizacyjne podległe Ministrowi Obrony Narodowej wskazane jako najbardziej istotne dla Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. W celu poprawnego i lepszego zobrazowania danych, wyniki zostały przetworzone i przedstawione w taki sposób, aby mogły być porównywalne z wykresem zamieszczonym poniżej.

W pytaniu drugim poproszono o przypisanie wartości od 1 do 10 (gdzie 1 oznacza najbardziej istotny a 10 najmniej istotny) sektorom definicji Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Poniżej przedstawiam wyniki:

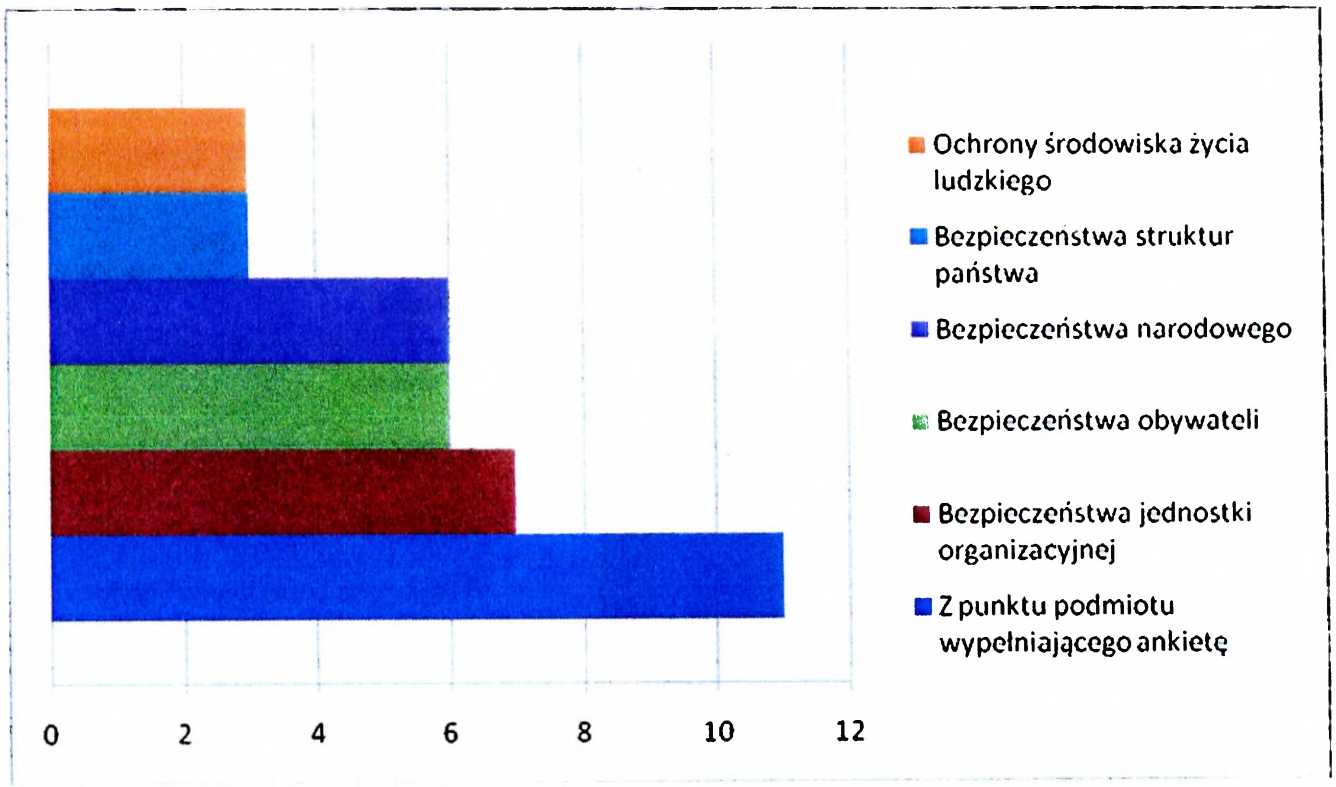


Sektory definicji Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski, które uzyskały bardzo wysokie wskazania (energia, woda, żywność oraz systemy i technologia teleinformatyczna, łączność, ICT) bardzo często otrzymywały wartości „jeden", „dwa" lub „trzy".

Jak wynika z wykresów przedstawionych powyżej, jednostki organizacyjne podległe Ministrowi Obrony Narodowej najczęściej podawały: energie, wodę, żywność, transport oraz systemy i technologia teleinformatyczna, łączność, ICT jako najbardziej istotne sektory Infrastruktury

Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Wyżej wymienione sektory stanowią najbardziej potrzebne i powszechne usługi wykorzystywane przez jednostki organizacyjne. Dlatego też, ich wysoka pozycja w kwestionariuszu ankiety nie powinna dziwić.

W ostatnim pytaniu jednostki organizacyjne miały określić kryteria, jakimi kierowały się podczas wypełniania tej części kwestionariusza ankiety. Poniżej przedstawiam wyniki:



Głównymi kryteriami, według których jednostki organizacyjne wskazywały priorytety w obszarze Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski, było zapewnienie podstawowego bezpieczeństwa w zakresie własnego sektora infrastruktury.

Wynik ostatniego pytania potwierdza tezę, że jednostki organizacyjne podległe Ministrowi Obrony Narodowej rozpatrują i postrzegają bardzo wyraźnie infrastrukturę krytyczną w sposób wyrywkowy i fragmentaryczny. Koncentrują one, swoje działania przede wszystkim na swoich podstawowych zadaniach, nie traktując Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski jako jednego z podstawowych elementów bezpieczeństwa państwa. Przykładem takiego myślenia jest fakt, iż jednostki organizacyjne w sposób bardzo wyraźny koncentrują swoje działania na zapewnieniu niezakłóconego i sprawnego funkcjonowania dowództw jednostek i samej jednostki organizacyjnej, pomijając inne bardzo ważne aspekty Infrastruktury

Krytycznej Sił Zbrojnych Rzeczypospolitej Polski pozostające w ich zakresie kompetencji.

WNIOSKI

WSTĘP

1. Raport z badań przeprowadzonych w okresie 22.02. – 01.06.2007 r., stanowi pierwszą próbę kompleksowego określenia i spojrzenia na ochronę Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Zaproponowana definicja Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski oraz szeroko rozumiana terminologia używana w kwestionariuszu ankiety stanowi nowość dla większości jednostek organizacyjnych podległych Ministrowi Obrony Narodowej[4]. Problematyka związana z ochroną infrastruktury krytycznej zmusza w sposób znaczący do przewartościowania obecnie funkcjonujących standardów i stereotypów, dotyczących bezpieczeństwa Sił Zbrojnych, bezpieczeństwa państwa, realizacji zadań obronnych w czasie pokoju, stanów zagrożeń i wojny.
2. Kwestionariusz ankiety opracowany prze ze mnie, stanowi adaptację do warunków i potrzeb rozprawy doktorskiej stosownego dokumentu NATO i kwestionariusza opracowanego przez Departament Bezpieczeństwa Powszechnego Ministerstwa Spraw Wewnętrznych i Administracji[5]. Osobiście jestem świadomy na dzień dzisiejszy „niedoskonałości" kwestionariusza. Jest to spowodowane otwartym charakterem, wynikającym z potrzeby pozyskania informacji od możliwie jak największej liczby jednostek organizacyjnych podległych Ministrowi Obrony Narodowej, różniących się bardzo zakresem obowiązków i działania w tematyce ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.
3. Kilkanaście jednostek organizacyjnych podległych Ministrowi Obrony Narodowej[6], nie udzieliło odpowiedzi, pomimo wcześniej zgłoszonych telefonicznie deklaracji.
4. Pojęcia związane z infrastrukturą krytyczna przedstawione w kwestionariuszu ankiety moim zdaniem nie powinny sprawiać żadnych trudności w przedstawieniu stanu ochrony sektorów infrastruktury krytycznej. Uważam, że zniekształcenie

---

[4] Podczas analizy kwestionariusza ankiety było to bardzo widoczne.

[5] Ministerstwo Spraw Wewnętrznych i Administracji. Departament Bezpieczeństwa Powszechnego, Infrastruktura krytyczna w Polsce – *Raport z badań*, Warszawa, wrzesień 2002 r.

[6] Dokładnie 24 jednostki organizacyjne podległe Ministrowi Obrony Narodowej nie udzieliły odpowiedzi. Jest to spowodowane brakiem odpowiednio przygotowanego personelu, który mógłby szerzej spojrzeć się na ochronę Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski oraz prawdopodobnie błędnym rozumowaniem ochrony informacji niejawnych.

(w niektórych przypadkach) wyników ankiety, spowodowane jest brakiem odpowiednio przygotowanego personelu, który mógłby szerzej spojrzeć się na ochronę Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.

5. Jedną z najważniejszych wad, wynikających obecnie z przyjętych zasad obowiązujących w Siłach Zbrojnych RP, jest utożsamianie wszystkich sektorów Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski z jednym tylko elementem – funkcjonowaniem Sił Zbrojnych w czasie stanów zagrożeń i wojny.

DIAGNOZA

1. Wyniki kwestionariusza ankiety pokazują brak zrozumienia jednostek organizacyjnych w realizacji zadań związanych z polityką bezpieczeństwa państwa.
2. Wyniki kwestionariusza ankiety pokazują, że jednostki organizacyjne podległe Ministrowi Obrony Narodowej nie mają opracowanych kompleksowych planów ochrony sektorów Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Prawdopodobnie nie opracowały także odpowiednich wytycznych w tym zakresie.
3. Brak zorganizowanej polityk bezpieczeństwa dla podmiotów odpowiedzialnych za bezpieczeństwo Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski naraża Siły Zbrojne na bardzo duże straty oraz chaos organizacyjny w przypadku ewentualnych ataków lub zakłóceń w kluczowych węzłach sektorów infrastruktury (efekt kaskadowy).
4. Wyniki kwestionariusza ankiety nie wykazały w żadnym stopniu istnienia koordynacji działań oraz współpracy między sektorami w zakresie ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.

ZREALIZOWANE CELE

1. Wyniki i dane zgromadzone w kwestionariuszu ankiety, nie pozbawione błędów merytorycznych, ilustrują w sposób wyraźny funkcjonowanie obecnie istniejących struktur Sił Zbrojnych (jednostek organizacyjnych podległych Ministrowi Obrony Narodowej), które są odpowiedzialne za bezpieczeństwo Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.
2. Bardzo dużą wartością samą w sobie są materiały nadesłane w kwestionariuszach ankiety, które mogą stać się punktem wyjścia dla przyszłych badań w zakresie ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski oraz Infrastruktury Krytycznej Państwa.

3. Najbardziej wrażliwymi sektorami Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski okazały się: energia, woda, żywność, transport oraz systemy i technologia teleinformatyczna, łączność, ICT. Jest to bardzo prawidłowy trend, który w pełni oddaje poczucie nowych zagrożeń asymetrycznych, które uwydatniły się po atakach na World Trade Center (WTC) 11 września 2001 r[7]. Coraz większe znaczenie nabiera bezpieczeństwo sektora: systemy i technologia teleinformatyczna, łączność, ICT[8]. W rozwiązaniach przyjętych w Stanach Zjednoczonych, Kanadzie, Wielkiej Brytanii, Finlandii oraz Niemczech główny nacisk kładzie się na bezpieczeństwo w „cyberprzestrzeni". Również w Siłach Zbrojnych i administracji państwowej stanie się to istotnym wyzwaniem , zwłaszcza po przyjęciu wszystkich ustaw związanych z przetwarzaniem informacji w systemach teleinformatycznych i teleinformacyjnych[9]. Coraz częściej technologia teleinformatyczna i teleinformacyjna umożliwiać będzie w niektórych segmentach „usług administracyjnych" a w szczególności w Siłach Zbrojnych bezpośrednie komunikowanie się i przesyłanie danych służbowych jawnych i niejawnych. Stąd problematyka bezpieczeństwa teleinformatycznego i teleinformacyjnego zasługuje na szczególną uwagę w dalszych pracach badawczych.
4. Wartością przeprowadzonego kwestionariusza ankiety jest także rozpoczęcie procesu tworzenia metodologii z zakresu ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.
5. Podjęcie badań z zakresu Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski ma również walor edukacyjny. Przyczynia się do upowszechniania tej problematyki w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej.

---

[7] W Raporcie z badań Departamentu Bezpieczeństwa Powszechnego Ministerstwa Spraw Wewnętrznych i Administracji z września 2002 r., „zwycięzcami rankingu" na wytypowanie najbardziej wrażliwych sektorów (segmentów) infrastruktury krytycznej okazały się: energetyka, bezpieczeństwo powszechne i telekomunikacja.

[8] Chodzi tu głownie o bezpieczeństwo teleinformatyczne.

[9] Po wdrożeniu Ustaw z dnia 18 lipca 2002 r. *O świadczeniu usług drogą elektroniczną* Dz. U. 2002.144.1204; z dnia 18 września 2001 r. *O podpisie elektronicznym* Dz. U. 2001.130.1450; z dnia 27 lipca 2001 r. *O ochronie baz danych* Dz. U. 2001.128.1402.

POSTULATY SYSTEMOWE – NASTĘPNE KROKI

1. Stworzenie powszechnie akceptowanych definicji i opracowanie wspólnej terminologii na potrzeby ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. W oparciu o ujednolicony semantycznie „słownik", w ramach tzw. pierwszego kroku, należałoby przydzielić zgodnie z obowiązującymi aktami prawnymi - poszczególne sektory infrastruktury krytycznej opiece poszczególnych resortów Ministerstwa Obrony Narodowej.
2. Zdefiniowanie Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski według hierarchii: żywotne, krytyczne, wrażliwe i podstawowe.
3. Niezwłoczne zakończenie prac nad CIRC Sił Zbrojnych RP (Centrum Koordynacyjne Sił Zbrojnych RP).
4. Określenie w ramach CIRC Sił Zbrojnych RP priorytetów działania. Propozycja podziału na:
   - ochronę bezpieczeństwa teleinformatycznego i teleinformacyjnego (cyberprzestrzeń) z rozróżnieniem konstruowania zabezpieczeń systemowych oraz bezpośrednim reagowaniem na „incydenty";
   - fizyczna i techniczna ochrona infrastruktury krytycznej;
   - bezpieczeństwo osobowe infrastruktury krytycznej;
   - bezpieczeństwo funkcjonowania jednostek centralnych Ministerstwa Obrony Narodowej;
   - bezpieczeństwa funkcjonowania jednostek organizacyjnych podległych Ministrowi Obrony Narodowej.

   Podział ten można oprzeć także w oparciu o Rodzaje Sił Zbrojnych.
5. Zbieranie i udostępnianie informacji o zagrożeniach i środkach ochrony. Większa dostępność środków ochrony teleinformatycznej i teleinformacyjnej (badania i certyfikacja urządzeń ochrony teleinformatycznej i teleinformacyjnej w instytucjach odpowiedzialnych za certyfikacje)[10].
6. Utworzenie grup eksperckich i baz danych ekspertów z zakresu poszczególnych sektorów Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Uruchomienie prac nad szczegółowymi planami operacyjnymi w zakresie ochrony infrastruktury krytycznej.

---

[10] W myśl Ustawy z dnia 22 stycznia 1999 r. *O ochronie informacji niejawnych* Tekst ujednolicony po zmianach z dnia 15 kwietnia 2005 r. Dz. U. 1999.11.95; Tekst ujednolicony Dz. U. 2005.196.1631 - akty zmieniające Art. 60 – odpowiedzialne za certyfikację są odpowiednie służby ochrony państwa (Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego).

7. Opracowanie programów szkoleń dla jednostek centralnych i organizacyjnych podległym Ministrowi Obrony Narodowej w zakresie ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski. Szkolenie i uświadamianie żołnierzy zawodowych i pracowników cywilnych wojska – bezpieczeństwo teleinformatyczne i teleinformacyjne w programach szkolenia.
8. Zainicjowanie szeroko idących naukowych programów badawczych z zakresu ochrony Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski.
9. Systematyczne gromadzenie i analizowanie danych na temat przestępstw teleinformatycznych, włączając w to zarówno odpowiednio zmodyfikowane statystyki przestępczości, jak i również informację o sposobach działania sprawców przestępstw, dotyczące w szczególności aspektów technicznych. Istotne znaczenie będą miały dane wywiadowcze na temat grup przestępczych (terrorystycznych) i przygotowywanych przez nich zamachów na Infrastrukturę Krytyczną Sił Zbrojnych Rzeczypospolitej Polski i Infrastrukturę Krytyczną Państwa.

ZAŁĄCZNIK 7

SPIS SYSTEMÓW TELEINFORMATYCZNYCH W RESORCIE OBRONY NARODOWEJ[1].

1. ABRACJA
2. AIS
3. ALASKA
4. ALBATROS
5. ALIS
6. ARCHIWUM
7. ARCUS – MON
8. ARKA 2000
9. ARNET
10. AZALIA
11. BAZA
12. BEŁTWA
13. BFEM
14. BLMW
15. BLUSZCZ – TELE
16. BLUSZCZ – H/METEO
17. BLUSZCZ – H/RL
18. BREŃ
19. BROADCAST
20. CaS
21. CASTRO
22. CBD HNS
23. CBD OPT
24. CYRANKA
25. DDM 9000
26. DDM
27. DRMM
28. DUNAJ
29. EDYTOR ZNAKÓW
30. ERC
31. ESTER
32. ETAT
33. EWIDENT P
34. EW PB
35. EXPERT
36. FALA – 25
37. FALA – 26
38. FALA – 31
39. FALA – 56
40. FALA – 57
41. FALA – 60M
42. FALA – 63
43. FALA – 75
44. FALA - 76
45. FALA – 77
46. FALA – 90M
47. FALA – 91
48. FALA – 92
49. FALA – 93
50. FALA – 94
51. FALA – 95
52. FALA – 96
53. FALA – 98
54. GALA – GOM
55. FORMULARZE
56. GBIM
57. GEOSERWER
58. GIPSÓWKA
59. GORYCZNIK
60. GRAF – WŁ
61. GRAF – ET/A
62. GURU
63. HOMAR
64. ICC
65. IETM
66. IKO3
67. ILOCZYN W1
68. INFOWSPARCIE
69. ITOD
70. JAŚMIN

[1] Stan na dzień 19.09.2007 r. Z uwagi na ochronę informacji niejawnych, przedstawione są tylko nazwy systemów teleinformatycznych w Siłach Zbrojnych RP.

71. JEDNOLITY INDEKS MATERIALOWY
72. JTLS
73. KAKTUS
74. KARMIN – PC/MOB/VIII
75. KARMIN MOB
76. KARTUS
77. KASJER
78. KELIN
79. KIM – R
80. KOLORADO
81. KONSOLA ROZPOZNAWCZA
82. KONSUMENT
83. KONTROLER
84. KROKUS – 2000
85. KRYL
86. KULA
87. KWISA – 1
88. KWISA – 2
89. KWISA
90. LEGALIS
91. LEX OMEGA
92. LINK – 11
93. LINK - 16
94. LIR – DSO
95. LOARA
96. LOGIS – MSM
97. LOGIS – ZSMM
98. LOGIS – A
99. LOGIS – BIK
100. LOGIS – BIS
101. LOGIS – BTS/TN
102. LOGIS – E
103. LOGIS – EWI
104. LOGIS – IBI
105. LOGIS – ISK
106. LOGIS – KOL
107. LOGIS – MGL
108. LOGIS – MOW
109. LOGIS – NET OG
110. LOGIS – NET WSPARCIE
111. LOGIS – R
112. LOGIS – XX
113. LOGIS – Z
114. LOGIS – ZSMP
115. LOGIS – ZŚB
116. LUZ
117. ŁEBA
118. ŁOWCZA – 3KS
119. MAG – MAT
120. MCCIS
121. MCM EXPERT
122. MIKOŁAJEK – CBH/RBM
123. MIKOŁAJEK – ODDZ
124. MIKOŁAJEK – RL
125. MIS – UMOWY
126. MNOŻNIK 95
127. MOSZIR
128. MOSZIR – R
129. NBP HEART
130. NDPASS
131. NEFRYT
132. NEURON
133. NFZ
134. NORMA – PRO
135. OBSZAR - POW
136. OGNIWO
137. ORBAT – NATO
138. ORCHIDEA
139. ORZYC DL 15
140. ORZYC TU – 20L
141. PATROL
142. PAX
143. PCŁU SZRP STORCZYK
144. PERSONEL
145. PERON
146. PGO
147. PIAST
148. PILAWA
149. PŁATKONÓG
150. PŁATNIK
151. PNCŁU TCE 500B
152. PODATEK
153. PODATEK – E
154. PODBIAŁ
155. POBRZEŻKA
156. POLIP
157. PROCES 1
158. PROCES 3
159. PROGNOZA 6S

160. PROMIEŃ
161. PROPLAN
162. PROSTA – C
163. PROSTA – K
164. PROSTA – N
165. PRZEBIŚNIEG
166. PRZELOT – WOC
167. PRZEMYSŁAW
168. PRZYLASZCZKA
169. PSTROKOSZ
170. RADAR 2000
171. RAMZES
172. REGA – 2
173. REJESTR – 2 PC
174. RODON
175. ROMB
176. ROZWÓJ
177. RUDNIA
178. SAMANTA BIS
179. SAN
180. SFINKS – 2
181. SFINKS – BILANS
182. SFINKS BUDZET
183. SFINKS RB – 30
184. SFINKS RB – 31
185. SFINKS RB – 70
186. SIGMAT – SMT
187. SIGMAT – MPS
188. SIGMAT – RBM
189. SIGMAT – TSM
190. SIGMAT – ZSM
191. SIGMAT – ZŚB
192. SIK
193. SIWOSZ
194. SKALAR KT
195. SKALAR SAO
196. SKARGA
197. SŁUŻBA
198. SOWA
199. SPIRALA K1
200. SPIRALA – MU
201. SPIRALA – MU/IS
202. SPIRALA – MU/IS/K
203. SIRALA – ZINT
204. SP – OG
205. SR – TR
206. SUPRAŚL
207. SZAFRAN – ZT
208. SZYK – 2M
209. SZYK (MEK)
210. ŚLEPOWRON
211. ŚREDNIA – K(RAB)
212. ŚR – TR
213. TACTICOS
214. TADIL
215. TADPOLE
216. TAMIZA
217. TER
218. TERMIN
219. TIEREK
220. TOPAZ
221. TRANS
222. TROP
223. TUBIS
224. TURAWA
225. UHLA
226. UZUP
227. VALLOR
228. VAT
229. VIDEOTEL
230. VINSON
231. WACŁAW
232. WBE _ STATYSTYKA
233. WOŁCZENICA
234. WYKŁADNIA
235. ZASOBY
236. ZENIT – 40
237. ZŁOCIEŃ
238. ZOL
239. ZUZANNA – T
240. ZUZIA
241. ZBIK

STRESZCZENIE

Słowa kluczowe: *cyberterroryzm, bezpieczeństwo teleinformatyczne, Krytyczna Infrastruktura Teleinformatyczna, Siły Zbrojne Rzeczypospolitej Polskiej, zarządzanie bezpieczeństwem informacji, analiza systemowa, model.*

Praca poświęcona jest aktualnej problematyce bezpieczeństwa informacyjnego (bezpieczeństwa teleinformatycznego). Autor szeroko przedstawia zjawisko cyberterroryzmu jako zagrożenia dla bezpieczeństwa teleinformatycznego Sił Zbrojnych Rzeczypospolitej Polski. W pracy przedstawiono istotę cyberterroryzmu, na tle zagrożeń bezpieczeństwa teleinformatycznego. Cyberterroryzm zaklasyfikowana jako jedno z najważniejszych zagrożeń.

W części metodologicznej zaprezentowano proces badań cyberterroryzmu oparty na analizie systemowej jako metametodzie. Poświęcona jest współczesnym zagrożeniom bezpieczeństwa teleinformatycznego: ich istocie, źródłom i przyczynom. Dokonano analizy identyfikacji podstawowych źródeł zagrożeń (rodzaj, typ, przewidywane skutki dla wybranych sektorów Krytycznej Infrastruktury Państwa) o istotnym znaczeniu dla bezpieczeństwa narodowego i Sił Zbrojnych Rzeczypospolitej Polskiej.

W części empirycznej zawarto wyniki z przeprowadzonych badań nad bezpieczeństwem Infrastruktury Krytycznej Sił Zbrojnych RP. Zawiera ona analizę polityki bezpieczeństwa informacyjnego Sił Zbrojnych Rzeczypospolitej Polskiej. Opisano Infrastrukturę Krytyczną oraz pokazano (na podstawie badań przeprowadzonych w 2007 r.) Infrastrukturę Krytyczną w Siłach Zbrojnych RP jako obiekt zagrożeń. Zaproponowano model funkcjonowania systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych. Cele i zadania systemu, wymagania i ograniczania systemowe oraz koncepcję funkcjonowania systemu zarządzania kryzysowego w Siłach Zbrojnych Rzeczypospolitej Polski. Dla modelu bardzo szczegółowo określono zadania poszczególnych elementów trójszczeblowego systemu zarządzania kryzysowego. Model opisuje najbardziej skomplikowane relacje wymiany informacji zachodzące w poszczególnych elementach składowych systemu.

System zarządzania kryzysowego w warunkach zagrożeń cybernetycznych traktowany jest jako jeden z istotnych podsystemów systemu zarządzania bezpieczeństwem Sił Zbrojnych Rzeczypospolitej Polski (Infrastruktury Krytycznej Sił Zbrojnych Rzeczypospolitej Polski). Opracowano ogólny model tego systemu, który jest wyrazem przyjętej w rozprawie metodologii badań nad zagrożeniami bezpieczeństwa teleinformatycznego dla bezpieczeństwa Sil Zbrojnych RP. Ze względu na złożony, niepewny i dynamiczny charakter badanych zjawisk, wykorzystano ogólne zasady metodologii badań systemowych, a w szczególności posłużono się analizą systemową.

Rozprawa składa się z czterech rozdziałów oraz wstępu i zakończenia. Bibliografia, spis tabel, rysunków i ujęć graficznych oraz załączniki są zamieszczone w części pozamerytorycznej.

SUMMARY

MODEL OF SYSTEM OF CRISIS MANAGEMENT IN CONDITIONS OF CYBERTERRORISM THREATS FOR INFORMATION SAFETY OF THE ARMED FORCES OF THE REPUBLIC OF POLAND

Key words: *cyberterrorism, teleinformation security, Critical Teleinformatic Infrastructure, Armed Forces of the Republic of Poland, information security management, comprehensive analysis, model.*

The dissertation is devoted to the current information security problems (teleinformatic security). The author widely discusses the phenomenon of cyberterrorism in the context of the teleinformatic security threats. Cyberterrorism is classified as on of the major threats.

The overall research process over cyberterrorism was based on the comprehensive analysis as the metamethod and is presented in the methodological chapter which is devoted to the definition of basic sources of the information threats (their kinds, frequency, predicted effects on the chosen sectors of the state critical infrastructure) of the key importance to the national security and the security of the Armed Forces of The Republic of Poland.

The experimental part of the dissertation comprises of the results from the research conducted on the Polish Armed Forces (PAF) critical infrastructure security. It consists of the PAF's information security analysis. It also describes the critical infrastructure and shows (on the basis of research conducted in 2007) the PAF's critical infrastructure as the object to threats. The crisis management model in the cyberterrorist threat environment has been hereby elaborated. Together with the aims and tasks of the system, requirements and limitations as well as the PAF's crisis management system operating concept. The tasks devoted to particular elements of the three-level system were defined in a very detailed way. The model describes the most complicated links of information exchange which occur in and between the particular elements constituting the system.

The crisis management system in the cyber threat environment is treated as one of the crucial subsystems of the state security management system (Polish Armed Forces critical infrastructure). In this dissertation the general models of such systems have been elaborated and they are the expression of the methodology concerning research of information threats to the national security. Due to the fact that the phenomena examined are characterized with high level of complexity, uncertainty and dynamics, the general comprehensive research methodology was utilized, with special regard to the comprehensive analysis.

The dissertation is comprised of four chapters, introduction and conclusion. Bibliography, chart, picture and graphics index as well as the annexes are placed beyond the content-related sections.

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 75501
Akademii Obrony Narodowej

S/7596
Cutt. Resp. ...dict