AKADEMIA OBRONY NARODOWEJ
WYDZIAŁ ZARZĄDZANIA I DOWODZENIA

ZARZĄDZANIE BEZPIECZEŃSTWEM MILITARNYM W UJĘCIU NARODOWYM I SOJUSZNICZYM

Praca naukowo - badawcza

Kryptonim „BEZPMIL"

Kod pracy: II.2.16.2.0

WARSZAWA

AKADEMIA OBRONY NARODOWEJ
WYDZIAŁ ZARZĄDZANIA I DOWODZENIA

ZARZĄDZANIE BEZPIECZEŃSTWEM MILITARNYM W UJĘCIU NARODOWYM I SOJUSZNICZYM

Praca naukowo - badawcza

Kryptonim „BEZPMIL"

Kod pracy: II.2.16.2.0

WARSZAWA

AKADEMIA OBRONY NARODOWEJ
WYDZIAŁ ZARZĄDZANIA I DOWODZENIA

ZARZĄDZANIE BEZPIECZEŃSTWEM MILITARNYM W UJĘCIU NARODOWYM I SOJUSZNICZYM

Praca naukowo - badawcza

Kryptonim „BEZPMIL"

Kod pracy: II.2.16.2.0

WARSZAWA **2008**

	1	2	3	
				A

4

Tytuł.: Zarządzanie bezpieczeństwem militarnym w ujęciu narodowym i sojuszniczym.

5	6	7
Rozpoczęto: 06.05.2008 Zakończono: 14.11.2008	kart: 167	

8	9

Dyrektor Biblioteki Głównej AON

dr. inż. Jerzy KOZIOŁ

Recenzent pracy: prof. dr hab. Leopold CIBOROWSKI

ZESPÓŁ AUTORSKI:

1. **Prof. dr hab. Michał HUZARSKI – kierownik zespołu**: *wstęp, rozdział pierwszy oraz zakończenie*;
2. **Płk dr hab. Grzegorz SOBOLEWSKI:** *rozdział 4 oraz załączniki nr* 4-9;
3. **Płk dr inż. Andrzej NOWAK**: *rozdział 2 oraz załączniki nr 1-3;*
4.: **Ppłk dr inż. Marek KUBIŃSKI**: *rozdział 3 oraz załączniki nr 10-13.*

SPIS TREŚCI

WSTĘP

Niniejsza praca naukowo – badawcza jest wykonana w ramach realizacji planu badań naukowych Wydziału Wojsk Lądowych na 2008 rok. Jest ona finansowana z dotacji na działalność statutową AON, w grupie zadań nowych. Mieści się ona w zadaniu numer 16 p.t. „Kierunki ewolucji sztuki wojennej w świetle założeń współczesnej teorii organizacji i zarządzania".

Temat pracy nakreśla obszar problemowy, który w swej istocie jest obecnie aktualny i ważny dla specjalistów zajmujących się kwestiami zarządzania bezpieczeństwem militarnym w ujęciu narodowym i sojuszniczym. Dostrzegamy tu wiele istotnych zmian, zarówno w postanowieniach teoretyczno - normatywnych, jak i w koncepcjach zarządzania tym bezpieczeństwem. Było to przyczyną i potrzebą podjęcia stosownych wysiłków celem identyfikacji problemu i na tej podstawie wypracowania elementów projektowych. Powyższe treści uznano jako element sytuacji problemowej ukazujący zasadność podjęcia badań i zaprezentowania uzyskanych rezultatów.

Główny problem badawczy wyrażono w następującym pytaniu:

Jak zarządzać bezpieczeństwem militarnym, aby zapewnić wymagany (oczekiwany) jego poziom, zarówno w wymiarze narodowym, jak i sojuszniczym?

Uzyskanie odpowiedzi na to pytanie wymagało rozwiązania kilku następujących problemów cząstkowych:

- Jakie są podstawy teoretyczno – normatywne zarządzania bezpieczeństwem militarnym?

- Jakie jest znaczenie i jakie są potrzeby w zakresie wykorzystywania zasobów informacyjnych w zarządzaniu bezpieczeństwem militarnym?
- Jaki jest zakres narodowego zarządzania bezpieczeństwem militarnym?
- Jakie aspekty sojusznicze stanowią o potrzebie podejmowania wysiłków na rzecz bezpieczeństwa militarnego?

***Celem poznawczym** pracy jest dokonanie identyfikacji problemu i określenie istoty zarządzania bezpieczeństwem militarnym, przez co wzbogacenie teorii organizacji i zarządzania bezpieczeństwem we wskazanym zakresie.*

***Celem pragmatycznym** jest wykorzystanie rezultatów badań w pracach projektowych nad podwyższaniem poziomu bezpieczeństwa militarnego, a także w procesie dydaktycznym WZ i D AON na kierunku – zarządzanie.*

W przewidywaniach hipotetycznych Zespół dostrzega wiele obszarów problemowych związanych z istotą i relacjami miedzy bezpieczeństwem w ujęciu narodowym i sojuszniczym, które wymagają zbadania celem ich aktualizacji i na tej podstawie zaprojektowania racjonalnych rozwiązań organizacyjno – funkcjonalnych w obszarze przedmiotu badań. Istnieje też potrzeba uaktualnienia i uzupełnienia podstaw teoretycznych i normatywnych w przedmiotowym zakresie wiedzy, która stworzy stosowną płaszczyznę do racjonalnych analiz i ocen podporządkowanych wzmacnianiu bezpieczeństwa militarnego.

Do przeprowadzenia badań zaprojektowano klasyczną procedurę, w tym głównie teoretyczne metody badawcze. Z metod empirycznych możliwe do zastosowania obecnie było badanie opinii techniką wywiadów eksperckich, zwłaszcza ze specjalistami – teoretykami i praktykami

zajmującymi się zagadnieniami bezpieczeństwa militarnego, w kontekście szeroko rozumianego bezpieczeństwa.

W zamyśle autorów było poznanie istoty przedmiotowej problematyki oraz dotarcie do dostępnych i aktualnych źródeł wiedzy w interesującym nas zakresie. Uznano, że wymaganą płaszczyzną do rozwiązywania problemów szczegółowych związanych z kształtowaniem bezpieczeństwa militarnego będzie szeroka problematyka bezpieczeństwa, a niej bezpieczeństwa narodowego.

W nakreślonym przedmiocie badań, mimo wielu szczegółowych opracowań, zarówno w obszarze zarządzania, jak i bezpieczeństwa militarnego, nie dokonano jeszcze uogólnionego określenia ich istoty i wzajemnych relacji. Wskazana jest wiec weryfikacja teoretyczno – pragmatyczna zaprezentowanych rezultatów badań, w kontekście wpływu zmiennych zagrożeń i uwarunkowań, zarówno narodowych, jaki sojuszniczych. Takie podejście było uwzględniane przez zespół autorski w zaprojektowanych założeniach metodologicznych

1. PODSTAWY ZARZĄDZANIA BEZPIECZEŃSTWEM MILITARNYM

1.1. Kwestie terminologiczne i typologiczne związane z zarządzaniem i bezpieczeństwem militarnym

Na temat zarządzania napisano wiele dzieł i różnych opracowań. Jest ono obecnie przedmiotem szczególnego zainteresowania szerokiego spektrum organizacji zhierarchizowanych. Przez efektywne zarządzanie gremia kierownicze organizacji dążą do osiągania zamierzonych celów. Wedle takiego projektu funkcjonalnego powinno być także zarządzane bezpieczeństwo militarne.

W odniesieniu do zarządzania i jego relacji z kierowaniem i dowodzeniem pojawiło się obecnie wiele poglądów i definicji. W tym opracowaniu przyjmujemy, że ***zarządzanie jest zespołem działań lub procesów mających na celu koordynację i integrację użytkowania zasobów dla osiągnięcia celu organizacyjnego przez ludzi przy użyciu techniki i informacji w zorganizowanych strukturach.***[1]

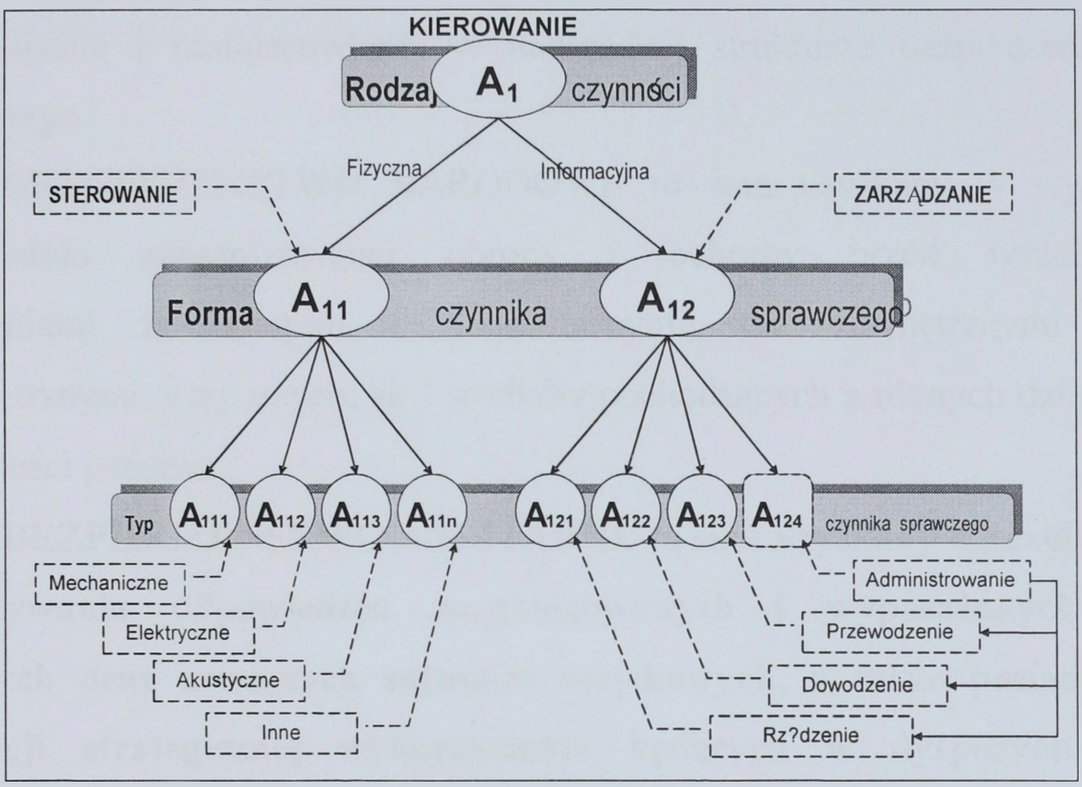
Według J. Kurnala, teoria zarządzania obejmuje wiedzę o organizowaniu zbiorowej działalności ludzkiej. Identyfikuje i wyjaśnia zależności występujące w procesach działań skupionych wokół wytyczonych celów i podejmowania wysiłków zmierzających do ich realizacji.

Spotykamy też interpretację traktowania zamiennie kierowania i zarządzania.[2] Z kolei ***Dowodzenie*** *jest podstawową formą kierowania wojskami, oparta na uprawnieniu do kompleksowego kształtowania wszystkich elementów gotowości i zdolności bojowej w odniesieniu do bezpośrednio i pośrednio odległych żołnierzy, a więc wszechstronnego*

---

[1] A. K. Koźmiński, Współczesne koncepcje zarządzania, Warszawa 1987, s. 352.
[2] Słownik terminów z zakresu bezpieczeństwa narodowego, Warszawa 2002, s. 169.

przygotowania ich w czasie pokoju do wszelkiego rodzaju działań i kierowania nimi podczas ich realizacji w okresie pokoju kryzysu i wojny.[3]



Rys. 1.1. Relacje między kierowaniem, zarządzaniem, sterowaniem i dowodzeniem (w dendrycie struktury kierowania)

Źródło: E. Skrzypek (red.), Jakość kształcenia w społeczeństwie wiedzy, UMCS, Lublin 2006,s.295; R. Polko, Rozprawa doktorska, Zarządzanie i dowodzenie wojskową formacją specjalną Grom, AON, Warszawa 2008, s. 16.

Wskazane jest mieć na uwadze wykładnię **istoty dowodzenia**, która akcentuje zapewnienie przewagi w systemach dowodzenia, łączności i informatyki oraz sprawnego obiegu informacji, także sprzężenie informacyjne pomiędzy elementami struktur dowodzenia, co zapewnia wymianę informacji i reagowanie na zmiany sytuacyjne podczas wykonywania zadań. Do priorytetów w tym obszarze zaliczmy: dostosowanie struktur i procedur dowodzenia do obowiązujących wymagań, zwłaszcza sojuszniczych; automatyzację procesów dowodzenia; rozwój mobilnych

[3] J. Michniak, Dowodzenie w teorii i praktyce wojsk, Warszawa 2003, s. 17.

systemów łączności; kompatybilność sprzętu i rozbudowę infrastruktury dowodzenia.[4]

W badanej problematyce bezpieczeństwa militarnego istotne jest jego zdefiniowanie i umiejscowienie w nadrzędnej strukturze bezpieczeństwa narodowego.

BEZPIECZEŃSTWO NARODOWE to stan uzyskany w wyniku odpowiednio zorganizowanej obrony i ochrony przed wszelkimi zagrożeniami **militarnymi** i niemilitarnymi, tak zewnętrznymi jak i wewnętrznymi, przy użyciu sił i środków pochodzących z różnych dziedzin działalności państwa.[5]

BEZPIECZEŃSTWO MILITARNE to stan uzyskany w rezultacie utrzymywania odpowiednio zorganizowanych i wyposażonych sił zbrojnych oraz zawartych sojuszów wojskowych, a także posiadania koncepcji strategicznej wykorzystania będących w dyspozycji sił, stosownie do zaistniałej sytuacji[6].

Ze względu na wagę znaczenia terminu „bezpieczeństwo militarne" w tym opracowaniu, uznano za celowe dokonanie oceny treści słownikowej definicji. Dostrzec można, iż termin „potencjał militarny" jest szerszy od „sił zbrojnych", i oprócz sojuszów wojskowych zawieramy także umowy polityczno - militarne w ramach Organizacji Narodów Zjednoczonych, Unii Europejskiej, czy też partnerskiej współpracy z innymi państwami, zwłaszcza z sąsiadami. Istotna jest tu także kwestia znaczenia pojawiających się zagrożeń. Można zatem zaproponować pewne zmiany w cytowanej wcześniej definicji i nadać jej następujące brzmienie:

BEZPIECZEŃSTWO MILITARNE to stan uzyskany w rezultacie utrzymywania na wymaganym poziomie potencjału militarnego oraz

---

[4] Strategia wojskowa..., wyd. cyt. s. 25.
[5] Słownik terminów z zakresu bezpieczeństwa narodowego, AON, Warszawa 2002, s. 16.
[6] Tamże, s. 16.

zawartych sojuszów wojskowych i umów polityczno – militarnych, a także posiadania koncepcji strategicznej, operacyjnej i taktycznej wykorzystania tego potencjału, stosownie do zaistniałej sytuacji i ocenianych zagrożeń wymagający użycia siły militarnej.

W przedstawionej wyżej definicji wyróżnić możemy trzy części o wyraźnej tożsamości:

- potencjał militarny – siły zbrojne;
- sojusze wojskowe i umowy polityczno – militarne;
- koncepcje strategiczne, operacyjne i taktyczne, wykorzystania potencjału militarnego.

Przy takim zdefiniowaniu bezpieczeństwa militarnego wskazane jest jego umiejscowienie klasyfikacyjne. Na najwyższym poziomie jest **bezpieczeństwo**, w którym ze względu na zasięg możemy wyróżnić: bezpieczeństwo globalne, regionalne i narodowe. W odniesieniu do bezpieczeństwa narodowego, przyjmując kryterium zakresu odpowiedzialności, podzielić je możemy na bezpieczeństwo: **militarne,** polityczne, społeczne. Przy kryterium podmiotowości podzielić je możemy na bezpieczeństwo: fizyczne, psychiczne, socjalne, strukturalne i personalne. W każdym z wymienionych elementów dostrzegamy związki z bezpieczeństwem militarnym.

Z analizy treści definiowanych wcześniej terminów wynika podrzędność bezpieczeństwa militarnego w stosunku do bezpieczeństwa narodowego, przy jednoczesnym priorytetowym jego znaczeniu w ramach tego bezpieczeństwa. Ponadto, w literaturze przedmiotu dostrzegamy także możliwość zamiennego użycia terminów **„bezpieczeństwo militarne”** i **„bezpieczeństwo wojskowe”**.. Jednak w kolejnych sekwencjach tej pracy używany będzie terminu „bezpieczeństwo militarne”, bowiem bardziej oddaje

on istotę problemu w obecnych, narodowych i sojuszniczych uwarunkowaniach.

1.2. Zakres problemowy bezpieczeństwa militarnego

Powyższe treści, a także analizy i oceny przedstawionych definicji oraz obecnych poglądów dotyczących szeroko rozumianego bezpieczeństwa pozwalają nakreślić obszar zainteresowania (przedmiot badań) **bezpieczeństwa militarnego**, który może obejmować:

- **podstawy normatywne i teoretyczne**;
- **zagrożenia militarne;**
- **aspekt naukowy bezpieczeństwa militarnego;**
- **potencjał militarny i koncepcja strategiczna jego wykorzystania;**
- **sojusze militarne;**
- **operacje militarne, reagowania kryzysowego i wsparcia pokoju;**
- **kierowanie bezpieczeństwem militarnym;**
- **prognostyczne kierunki zmian w bezpieczeństwie militarnym.**

U podstaw nakreślonego zakresu problemowego bezpieczeństwa militarnego legło wiele różnych przesłanek. Zaliczyć do nich należy przede wszystkim wykazanie jego istoty, jak również potrzebę uporządkowania tej niewątpliwie ważnej i rozległej problematyki, przy uwzględnianiu zmian uwarunkowań wpływających na kwestie bezpieczeństwa.

Nawiązując do definicji bezpieczeństwa militarnego i nakreślonego jego zakresu, ze względu na różnice w interpretacji, wskazane jest podkreślenie znaczenia podstawowego kryterium, którym jest przewidywany **udział sił militarnych** w zapewnianiu bezpieczeństwa. Podkreślenie „**militarnych**" wynika z jego szerszego znaczenia od **„wojskowych**",

używanych często zamiennie. Mamy na uwadze wszystkie formacje o charakterze militarnym (paramilitarnym), posiadające w dyspozycji uzbrojenie i stosowne prawo do użycia broni. Wymienić tu można, oprócz wojskowych sił zbrojnych (armii), także formacje policyjne (np. antyterrorystyczne), czy Straż Graniczną.

1.3. Naukowy aspekt bezpieczeństwa militarnego

W wyniku prowadzonych badań powstaje **wiedza naukowa**, którą tworzą twierdzenia uzasadnione i sprawdzone. Badaniami samej nauki zajmuje się **naukoznawstwo,** gdzie nadrzędne miejsce zajmuje filozofia. Znawcy przedmiotu twierdzą, iż w literaturze przedmiotu znaleźć można ponad sto różnych definicji **nauki.** Do dalszych rozważań w tym opracowaniu proponuje się przyjąć, za S. Kamińskim, iż: **NAUKA** to proces, a zarazem obiektywny rezultat twórczego poznania; to proces nauczania a zarazem uczenia się; to proces planowego dochodzenia do nowego i twórczo osiągniętego poznania.

Ponadto wskazane jest także mieć na uwadze pogląd R. Wróblewskiego, który dostrzega powszechne przyjmowanie nauki jako społecznie zorganizowanej działalności nastawionej na wytwarzanie informacji (badania) oraz rezultaty tej działalności (teorie).

Zgodnie z Obwieszczeniem Centralnej Komisji do spraw tytułu Naukowego i Stopni Naukowych z 1992 roku nauka składa się z następujących **dziedzin nauki:** biologiczne; chemiczne; ekonomiczne; farmaceutyczne; fizyczne; humanistyczne; leśne; matematyczne; medyczne; o kulturze fizycznej; o ziemi; prawne; rolnicze; techniczne; teologiczne; weterynaryjne; **wojskowe.**

Większość z wymienionych dziedzin naukowych dzielimy na dyscypliny i specjalności naukowe. Interesujące nas **nauki wojskowe** mają

zatem określone miejsce w podziale nauki, który można postrzegać także jako system nauk.

NAUKI WOJSKOWE stanowią zbiór dyscyplin (specjalności) naukowych badających istotę walki zbrojnej i jej rolę w rozstrzyganiu sporów między państwami (koalicjami państw), procesy tworzenia potencjału wojskowego i jego wykorzystania w okresie pokoju kryzysu i wojny.[7]

Dokonując porównania definicji bezpieczeństwa militarnego i nauk wojskowych dostrzec można ich spójność i stosowne relacje i zależności. Przede wszystkim ich obszary zainteresowania i przedmiot badań wykazują wzajemna korespondencję. Obecnie w środowisku akademickim prowadzona jest dyskusja celem wypracowania stanowiska w odniesieniu do proponowanych dyscyplin w naukach wojskowych (obecnie ich nie ma), a także możliwej zmiany ich nazwy, czy też wprowadzenia nowej dziedziny naukowej nazwanej „nauki o bezpieczeństwie narodowym". Potrzeba taka istnieje, gdyż obecnie w AON badania naukowe wychodzą poza zakres nauk wojskowych i obejmują problematykę bezpieczeństwa narodowego (bezpieczeństwo polityczne, ekonomiczne).

Istnieją podstawy do przeprowadzenia realnych zmian w zasygnalizowanym zakresie, bowiem takie są obecne i przyszłe potrzeby badań naukowych, a także koresponduje to z zamiarami centralizowania struktur wyższego szkolnictwa wojskowego otwartego na inne resorty zajmujące się bezpieczeństwem państwa. Wskazane jest przy tym zaznaczyć, że nauki wojskowe mają charakter interdyscyplinarny i eklektyczny, mają wiec podstawy do twórczej współpracy z innymi, pokrewnymi dziedzinami naukowymi, dzielenia się osiągnięciami twórczymi, ale także korzystania z dorobku innych ośrodków naukowo badawczych i dydaktycznych. Z definicji bezpieczeństwa militarnego, nauk wojskowych i zamiarów

[7] Słownik terminów ..., wyd. cyt., s. 76.

dokonywania stosownych zmian wnioskować można, iż istotną rolę odgrywają wspomniane relacje miedzy nimi, w kontekście potrzeb efektywnego zarządzania.

1.4. Koncepcje wykorzystania potencjału militarnego

Zarówno w bezpieczeństwie militarnym, jak i naukach wojskowych, jedną z podstawowych kwestii jest koncepcja wykorzystania dyspozycyjnego potencjału militarnego z wyeksponowaniem znaczenia strategii. To podkreślenie wynika z szerokiego znaczenia terminu „strategia". Jednak podstawowe jej odniesienie to strategia militarna. Gdyby poprzestać na koncepcjach strategicznych wykorzystania potencjału militarnego ich obraz byłby niepełny. Dlatego też wskazane jest pewne uszczegółowienie o poziomy operacyjne i taktyczne, bowiem one stanowią dopełnienie całości przy uwzględnieniu kwestii wsparcia i zabezpieczenia działań. Warto tu przywołać pogląd klasyka wojskowości C. v Clausewitza, który określał strategię jako sumę zwycięstw taktycznych. Przywołajmy zatem aktualne definicje interesujących nas terminów.

Strategia militarna obejmuje problematykę tworzenia i wykorzystania sił zbrojnych państwa w okresie pokoju, kryzysu i wojny w sposób zapewniający osiągnięcie celów nakreślonych przez politykę.[8]

Operacje militarne to działania militarne jednej ze stron, skoordynowane czasowo i przestrzennie, ukierunkowane na wspólny cel. Obejmują one okresy przed, w czasie i po działaniach, aż do osiągnięcia celu końcowego – zamierzonego wyniku działań militarnych.[9]

---

[8] Por. R. Wróblewski, Wprowadzenie do strategii wojskowej, Warszawa 1998, s. 30-31; Słownik terminów...,wyd. cyt., s. 134.

[9] Por. J. Pawłowski, Istota operacji połączonych, [w:] Działania (operacje) połączone, Materiały z konferencji naukowej, tezy, referaty, głosy w dyskusji, Warszawa 2002, s. 18; M. Kozub, Lotnictwo wojsk lądowych w operacjach połączonych, Warszawa 2002, s. 8.

Taktyka militarna obejmuje taktyki rodzajów sił zbrojnych (wojsk lądowych, sił powietrznych i marynarki wojennej), które zajmują się przygotowaniem i prowadzeniem działań taktycznych.[10]

Przedstawione wyżej definicje mają charakter ogólny i eksponują jedynie istotne kwestie zaproponowanych części składowych bezpieczeństwa militarnego.

Wymieniona na pierwszym miejscu **strategia militarna**, związana jest bezpośrednio z terminem „strategia", o której napisano wiele dzieł i opracowań. Początkowe, militarne znaczenie strategii, w wyniku rozwoju społeczeństw, zmieniło się i poszerzyło o inne obszary rządzenia państwem. Wymienić tu można m.in. kwestie polityczne, ekonomiczne czy też społeczne. Jest to bardzo szeroki obszar problemowy, którym zajmuje się także szerokie grono specjalistów wojskowych i cywilnych. W wyniku podejmowanych prac koncepcyjnych powstają m.in. strategie: narodowe, bezpieczeństwa narodowego, polityki zagranicznej, czy też w zakresie ekonomii.

W nawiązaniu do **operacji militarnych** wskazane jest wyjaśnienie, iż jeden z podziałów jest adekwatny do rodzajów sił zbrojnych. Stąd zrodziły się operacje **lądowe, morskie i powietrzne**. Uściślenie podkreślające militarny charakter operacji wynika z wieloaspektowego używania terminu „operacja".

Obecnie, ze względu na dynamiczny rozwój działań operacyjnych równolegle w różnych środowiskach, zaistniała potrzeba łączenia wysiłków. Dało to początek **operacjom połączonym**, których istota wyraża się w synchronizacji wysiłków wojsk i środków rodzajów sił zbrojnych, co znacząco podwyższa skuteczność w osiąganiu celów. Przyjmując kryterium charakteru zadań i środowiska, operacje połączone można podzielić na: operacje powietrzno-lądowe, lądowo- morskie, powietrzno-morskie i inne.

---

[10] M. Huzarski (red.), Taktyka ogólna wojsk lądowych, Warszawa 2001, s. 6.

Zależnie od doboru komponentów rozróżniamy następujące rodzaje operacji połączonych:

1. **Operacje połączone**, w których biorą udział narodowe komponenty sił zbrojnych.
2. **Operacje sojusznicze** prowadzone wspólnie przez wojska dwóch lub więcej państw.
3. **Sojusznicze operacje połączone**, w których udział biorą komponenty co najmniej dwóch rodzajów sił zbrojnych z co najmniej dwóch państw.

Z powyższych wyjaśnień dotyczących istoty współczesnych operacji wnioskujemy, iż nie można obecnie wyodrębniać operacji prowadzonej przez jeden rodzaj sił zbrojnych. Natomiast sam charakter operacji połączonych staje się naturalną konsekwencją ich dostosowania do istniejących uwarunkowań i wymagań operacyjno-strategicznych.

Operacje połączone w takim ujęciu obejmują:

- planowanie i przygotowanie;
- przegrupowanie i rozwinięcie wojsk;
- zakończenie konfliktu, przegrupowanie do rejonów wyjściowych;
- odtworzenie stanu wyjściowego.[11]

W powyższym ujęciu dostrzec można całościowe ujęcie zamierzeń operacyjnych, zwłaszcza z doprowadzeniem do zamierzonego zakończenia działań. Niewątpliwie, ze względu na potencjał i przeznaczenie, najszerszy zakres zadań przewidywany jest dla wojsk lądowych. Dotyczy to przede wszystkim podstawowych operacji o charakterze militarnym, zwłaszcza, gdy ich celem jest opanowanie i utrzymanie określonego obszaru.[12]

---

[11] K. M. Hofeditz, Zasady prowadzenia operacji, Myśl Wojskowa 1998, nr 5, s. 88.

[12] A. Tomaszewski, Wojska lądowe w operacjach połączonych, [w:] Działania (operacje) połączone, wyd. cyt., s. 34.

Kolejne wyjaśnienia odnoszą się do **taktyki militarnej.** Akcent militarny wynika z potrzeby podkreślenia odrębności specjalistycznej. Bowiem sam termin **„taktyka"** jest używany także w różnych kontekstach, nie tylko związanych z bezpieczeństwem.[13] Klasyfikacja taktyki ujmowana w dokumentach normatywnych i opracowaniach teoretycznych dotyczących rodzajów sił zbrojnych jest w swym ogólnym podziale tożsama i dzieli się na:

- **taktykę wojsk lądowych;**
- **taktykę sił powietrznych;**
- **taktykę marynarki wojennej;**
- **taktykę sił specjalnych.**

Wcześniej dzielono je na **taktykę ogólną i taktykę rodzajów wojsk**. Jednak zaistniałe uwarunkowania, zwłaszcza zaś potrzeby dostosowania się do wymagań sojuszniczych, przyczyniły się do wprowadzania określonych zmian. Dotyczą one wszystkich rodzajów sił zbrojnych i obejmują:

- **teoretyczne podstawy taktyki;**
- **taktykę działań w stanach – pokoju, kryzysu i wojny;**
- **wsparcie działań.**

Dostrzegamy, iż zrezygnowano z dotychczasowego podziału na dwa komponenty taktyki. Wprowadzono natomiast podział w dowiązaniu do pokoju, kryzysu i wojny, z uwzględnieniem wyodrębnienia **wsparcia działań,** które obecnie obejmuje *wsparcie ogniowe i zabezpieczenie*, tak na poziomie taktycznym jak i operacyjnym. Przy pewnej odrębności organizacyjno-funkcjonalnej wsparcia działań, powinno być wykonywane przede wszystkim na korzyść wojsk wykonujących zadania o charakterze rozstrzygającym. Wymaga to jednak stosownych **uzgodnień koordynacyjnych**. Przedmiotem uzgodnień stają się kwestie ogniowe i zabezpieczenia w dowiązaniu do *zadań, czasu, terenu i obiektów*, natomiast

[13] Szerzej o klasyfikacji i terminologii taktyki [w:] M. Huzarski, Wpływ nowych wyzwań i zagrożeń na zmiany w taktyce wojsk lądowych, Warszawa 2002, s. 17-22. W kolejnych treściach obejmujących bezpieczeństwo militarne, przymiotnik ten będzie pomijany.

szczegółowe wykonawstwo realizowane powinno być zgodnie z zasadami specjalistycznymi rodzajów wojsk.

1.5. Sojusze polityczno – militarne

W treści definicji bezpieczeństwa militarnego eksponowane są sojusze. Wskazane jest wiec przywołanie definicji **sojuszu,** który rozumiany jest jako „traktat wiążący dwa lub więcej niepodległych państw przyrzeczeniem przyjścia jedno drugiemu z pomocą zbrojną w okolicznościach wyspecyfikowanych w traktacie",[14] natomiast **sojusz polityczno – militarny** to „przyrzeczenie (obietnica) wzajemnej pomocy militarnej między dwoma lub więcej suwerennymi państwami".[15]

Od 12 marca 1999 roku Polska jest członkiem NATO[16]. Ta obecność w Sojuszu poprzedzona była wieloletnimi staraniami i dużym wysiłkiem, którego celem było dostosowanie naszych sił zbrojnych do określonych standardów.

Problematyka naszego funkcjonowania w NATO jest bardzo obszerna i została ona opisana w wielu opracowaniach. Nas, przede wszystkim interesują zobowiązania sojusznicze dotyczące podjęcia określonych działań, którym poświecone są artykuły III, IV i V Traktatu Waszyngtońskiego. Zaliczamy do nich:

- utrzymywanie i rozwijanie indywidualnej i zbiorowej zdolności do odparcia napaści (art. III);
- podejmowanie konsultacji w razie zagrożenia integralności terytorialnej, niezależności politycznej lub bezpieczeństwa którejkolwiek ze stron (art. V);

---

[14] B. Balcerowicz, Siły zbrojne w państwie i stosunkach międzynarodowych, Scholar, Warszawa 2006, s. 73.
[15] Tamże, s. 73.
[16] Pod wspólnymi sztandarami, Droga Polski do NATO, AON, Warszawa 1999, s. 5.

- **udzielanie pomocy, podjęcia solidarnej akcji (nie wyłączając użycia siły zbrojnej) w razie napaści na któregokolwiek z członków Sojuszu (art. V).**[17]

Dotrzymywanie tych ogólnych zobowiązań wymaga realizacji zamiarów o charakterze szczegółowym, które wynikają z postanowień podejmowanych na kolejnych Szczytach NATO i podczas bieżącej działalności organów Sojuszu. Wymienić tu można np. decyzje o powołaniu Sił Odpowiedzi na Szczycie NATO w Pradze w 2002 roku.

Od 1 maja 2004 roku Polska jest członkiem Unii Europejskiej. Na 27 państw zajmuje 6 miejsce pod względem obszaru i ludności. UE jest gospodarczo – politycznym związkiem państw. Ma ona także swe ambicje samodzielności militarnej. W Deklaracji Petersberskiej przyjętej na spotkaniu Rady Ministrów UZE 19 czerwca 1992 roku postanowiono, że jednostki wojskowe państw członków UZE mogą być wykorzystywane do:

- zadań humanitarnych i ratowniczych;
- prowadzenia operacji pokojowych;
- zadań jednostek bojowych przy opanowywaniu sytuacji kryzysowych, kryzysowych tym przywracania pokoju.[18]

Do wykonywania tych zadań powołano stosowne organy UE, a mianowicie: Komitet Polityczny i Bezpieczeństwa, Komitet Wojskowy oraz Sztab Wojskowy. Potwierdzono, że UE powinna być gotowa do prowadzenia operacji siłami jednego korpusu [19]. Rzeczywista realizacja zamierzeń UE o charakterze militarnym przebiega różnie, co wymaga kontynuacji uzgodnień.

Dobrym początkiem jest realne tworzenie Grup Bojowych UE, których koncepcję przyjęto na posiedzeniu Rady UE w maju 2004 roku.

---

[17] B. Balcerowicz, Siły…., wyd. cyt., s. 83.
[18] A. Ciupiński, Rozwój sytuacji reagowania kryzysowego Unii Europejskiej, [w:] Podział odpowiedzialności za bezpieczeństwo Europy pomiędzy NATO a Unię Europejską, Materiały z sympozjum, AON, Warszawa 2006, s. 59.
[19] Tamże, s. 62.

Polska ma uczestniczyć w tworzeniu trzech grup, w tym w jednej jako państwo ramowe.

Zamiary UE w obszarze bezpieczeństwa i udziału sił militarnych w operacjach prewencyjnych i reagowania kryzysowego uznać można jako działania o charakterze sojuszniczym. Przyjmujemy określone zobowiązania militarne w imię utrzymania wspólnego bezpieczeństwa.

Wiele przesłanek pozwala stwierdzić, że nasz udział w sojuszach wojskowych i polityczno – militarnych znacząco wpływa na kształt bezpieczeństwa militarnego. Wymaga to określonego wysiłku i efektywnego zarządzania tym bezpieczeństwem, przez co podwyższany jest poziom naszego bezpieczeństwa, co skutkuje wysoką pozycją wśród krajów europejskich.

Wnioski

Z przedstawionych definicji i podziałów typologicznych związanych z bezpieczeństwem militarnym wynika, iż istniała potrzeba ich przywołania, wyjaśnienia istoty i wskazania na zachodzące relacje miedzy nimi. Wskazane też było określenie akceptowanych poglądów na zasadnicze kwestie zarządzania, które miały zastosowanie w odniesieniu do bezpieczeństwa militarnego.

Rozwinięciem zaproponowanej definicji bezpieczeństwa militarnego było określenie jego zakresu problemowego. Stworzyło to czytelną płaszczyznę do analiz i ocen związanych z zarządzaniem tym bezpieczeństwem.

Istotną pozycję w badanej problematyce ma wzrastający potencjał militarny. Koncepcje jego wykorzystania wskazane jest łączyć z wiedzą o strategii, operacjami i taktyką w ujęciu militarnym. Terminy te mają różne

znaczenia, w zależności od zakresu badań. Podkreślenie militarnego ich charakteru uściśla nasze zainteresowania poznawcze.

Potwierdzony został rosnący wpływ sojuszy polityczno – militarnych na przedmiotowe bezpieczeństwo, zwłaszcza na kwestie zwiększania mocy potencjałów militarnych, które przez połączenie wysiłków pozwalają uzyskać efekt synergii w osiąganiu zamierzonych, sojuszniczych celów obronnych.

W uogólnieniu stwierdzić można, iż przedstawione, wybrane elementy podstaw zarządzania bezpieczeństwem militarnym, stwarzają czytelną płaszczyznę do badania i prezentacji uzyskanych wyników stanowiących rozwiązania problemów szczegółowych.

2. INFORMACJA W ZARZĄDZANIU BEZPIECZEŃSTWEM MILITARNYM

Bezpieczeństwo a szczególnie „bezpieczeństwo militarne" poddawane jest analizie i opisywane w ramach różnorodnych typologii. Jedną z podstawowych jest podział bezpieczeństwa narodowego odnoszący się do kryterium przedmiotowego: bezpieczeństwo militarne, ekonomiczne, polityczne, społeczne, czy wreszcie - bezpieczeństwo informacyjne[20].

Analiza założeń teoretycznych oraz wnioski i doświadczenia z wojen i konfliktów lokalnych skłaniają do wniosku, że czynnik militarny przez wieki odgrywał kluczową rolę w stosunkach między państwami. Do tego stopnia, iż można było utożsamiać bezpieczeństwo z brakiem bezpośredniego zagrożenia militarnego. Obecnie, wobec zwiększającego się znaczenia pozostałych czynników, nie odgrywa już tak absolutnej roli jak w przeszłości.

Nie można jednak postawić tezy, iż bezpieczeństwo militarne utraciło całe znaczenie. Jakkolwiek prawne możliwości prowadzenia wojny zostały w XX w. mocno ograniczone przyjętym prawem międzynarodowym, świat nie został uwolniony od tego zjawiska. Według Sztokholmskiego Międzynarodowego Instytutu do spraw Badania Pokoju (SIPRI) w latach 1945 - 1993 na świecie odnotowano ok. 200, tzw. większych konfliktów zbrojnych[21].

W przedstawionej definicji „bezpieczeństwa militarnego[22]" przyjęto, że bezpieczeństwo to jest obszarem (dziedziną) charakteryzującym się wielopłaszczyznowością, rozległością oraz złożoną praktyką, które trwają

---

[20] Zobacz, rozdział pierwszy.

[21] G. Michałowska (red.), Mały słownik stosunków międzynarodowych, Warszawa 1997, s. 98. Konflikt „większy" to, wg terminologii SIPRI konflikt w którym „przez dłuższy czas walczą z sobą oddziały wojskowe podlegające dwóm albo więcej rządom lub jednemu rządowi i co najmniej jednej uzbrojonej organizacji, i w którego wyniku zginęło co najmniej 1000 osób".

[22] Zobacz, rozdział pierwszy.

w sposób ciągły, dopóki istnieje państwo i środowisko międzynarodowe. Ponadto założono, że bezpieczeństwo militarne postrzegane może być jako dziedzina wiedzy i praktyki czyli może być rozpatrywane jako zjawisko, system lub proces[23].

Do dalszych rozważań w tym rozdziale przyjęto percypować **bezpieczeństwo militarne jako system który należy postrzegać jako złożoną organizację**, której zasadniczym elementem składowym są siły militarne odpowiednio powiązane relacjami wewnętrznymi z pozostałymi jego elementami potencjału obronnego (gospodarką, społeczeństwem) państwa oraz relacjami zewnętrznymi (w postaci sojuszów wojskowych, politycznych i gospodarczych) z innymi państwami[24].

Nie ulega dziś wątpliwości, że „bezpieczeństwo" rozumiane jako gwarancja prawidłowego (bez zakłóceń) funkcjonowania określonego podmiotu, jest agregatem wielu obszarów cząstkowego bezpieczeństwa. Jego globalny (kompleksowy) poziom zależy oczywiście od poziomu poszczególnych obszarów bezpieczeństwa cząstkowego (dziedzinowego) – jest więc funkcją wielkości jego poziomów cząstkowych. Zarządzanie bezpieczeństwem w warstwie najbardziej ogólnej polega zatem na zagwarantowaniu odpowiednich poziomów bezpieczeństwa cząstkowego. Zadanie to można sprowadzić do zadania alokacji łącznych środków przeznaczonych na bezpieczeństwo, w stosunku do poszczególnych jego obszarów.

Potwierdzeniem tej tezy jest fakt, że czynnik technologiczny odgrywający znaczącą rolę w gospodarce, zdobywa coraz większe znaczenie także w dziedzinie militarnej. Innowacyjność produktu, oszczędność materiału i energii pozwala zdobywać nowe rynki i wypierać starsze produkty. Również, w dziedzinie militarnej przewaga technologiczna coraz

---

[23] Por. E. Nowak, Zarządzanie bezpieczeństwem militarnym RP, ZN AON nr 4/2007, s. 8.
[24] Tamże, s. 8.

częściej zastępuje przewagę liczebną[25]. Należy zwrócić także uwagę na fakt, że trendy w badaniach nad „bezpieczeństwem militarnym" wskazują, że rozwój technologii informacyjnych prowadząc do rozwoju społeczeństw może również prowadzić do powstawania nowych zagrożeń. Zagrożenia te mogą powstawać w newralgicznych punktach infrastruktury informacyjnej, a także w związku z uzależnieniem współczesnego społeczeństwa od natychmiastowego i niezakłóconego przepływu informacji.

W odniesieniu do całości problemu, czynnik informacyjny nabiera na znaczeniu wraz z rozpowszechnianiem się powszechnego dostępu do źródeł informacji, takich jak media, czy Internet. Środki masowego przekazu pozwalają obecnie na manipulowanie informacją w skali całego globu. Masowy przepływ informacji odbywa się również ponad państwem. Z tego powodu państwa muszą przywiązywać coraz większą wagę do kontrolowania tego zjawiska i odcinania obywateli od informacji niepożądanych z punktu widzenia państwa.

Wyniki badań skłaniają do wniosku, że w miarę intelektualnego rozwoju i politechnizacji życia, informacje zaczęły nabierać coraz większych wartości. Ich posiadanie stało się warunkiem lepszej i bezpieczniejszej egzystencji. Na tym też tle pojawiła się konkurencja. Informację zaczęto coraz bardziej chronić jako dobro materialne. Jednocześnie, chęć stworzenia sobie podobnych do innych lub lepszych warunków życia zidentyfikowano potrzebę posiadania informacji[26].

Przedstawione propozycje można odnosić do różnych obszarów bezpieczeństwa, jak również do różnych podmiotów bezpieczeństwa, np. bezpieczeństwa narodowego, regionalnego, czy też absolutnie lokalnego. Nie bez znaczenia jest tu również aspekt synergii poziomów bezpieczeństwa

---

[25] Zobacz: M. Lisowski, Gdy silny atakuje słabego, RAPORT-wto 2003, nr 5.

[26] Por. Wykaz obowiązujących standardów technologii informatycznych do stosowania w resorcie obrony narodowej na lata 2007-2008, Departament Informatyki i Telekomunikacji MON, Warszawa 2007.

cząstkowego, co powoduje, że poziom bezpieczeństwa ogólnie nie jest prostą sumą poziomów bezpieczeństwa cząstkowego.

Celem rozdziału jest zaprezentowanie wyników badań z zakresu znaczenia informacji w procesach zarządzania bezpieczeństwem militarnym.

Wysiłek zespołu badawczego ukierunkowany został na zidentyfikowanie informacyjnego wymiaru bezpieczeństwa militarnego, określono potrzeby w zakresie wykorzystania zasobów informacyjnych w zarządzaniu bezpieczeństwem militarnym oraz wskazano na główne obszary ochrony informacji w bezpieczeństwie militarnym.

2.1. Informacyjny wymiar bezpieczeństwa militarnego

Terminem „informacja" posługujemy się powszechnie, a jego znaczenie pozornie nie budzi żadnych wątpliwości. Jednakże pomimo powszechności używania zdefiniowanie go sprawia liczne trudności. Przez wielu teoretyków informacja uznawana za pojęcie pierwotne, nie doczekała się jednoznacznej definicji. W wielu publikacjach, rezygnuje się nawet z jej definiowania poprzestając na intuicyjnym potocznym rozumieniu. Rozwiązania problemu poszukuje się zazwyczaj poprzez rozpatrywanie treści informacji, cech źródeł jej pochodzenia i obszarów wykorzystania lub jej wartości praktycznych i teoretycznych.

2.1.1. Interpretacja pojęcia informacja

Potocznie informacja jest definiowana w powiązaniu z przedmiotami myślowymi, które odzwierciedlają różnorodne postacie wiadomości, wieści czy też wiedzy o aktualnych zdarzeniach[27]. W *Encyklopedii popularnej* pojęcie to interpretowane jest jako czynnik, dzięki któremu człowiek lub

[27] W. Kopaliński, Słownik Wyrazów Obcych, Wiedza Powszechna 1980, s. 429.

urządzenie automatyczne mogą przeprowadzić bardziej sprawne, celowe działanie[28].

W znaczącej liczbie opracowań, informację utożsamia się z wiedzą i wiadomością podkreślając zarazem jej powszechność, indywidualność i ścisły związek ze świadomością nie tylko żywego organizmu, ale również automatu (komputera), któremu człowiek nadał taką zdolność percepcji informacji[29].

Uzyskiwanie, posiadanie i przetwarzanie informacji towarzyszy niezmiennie człowiekowi we wszelkich procesach poznawczych. Rezultatem poznawczym tych procesów jest wiedza[30], którą dysponujemy. Człowiek otoczony hipermedialnymi[31] środkami przekazu „zalewany" jest strumieniami informacji o faktach, które miały miejsce w ciągu ostatnich kilku godzin czy dni. Transformacja informacji w wiedzę, z jej pozytywnymi lub negatywnymi skutkami, następuje w sposób niemalże niezauważalny.

W bezpieczeństwie militarnym informacja odgrywa rolę szczególną, jest siłą sprawczą łączącą ogół działań, czas przygotowania oraz czas realizacji celów działań w jedną spójną całość. Systemy istniejące w obszarze bezpieczeństwa militarnego muszą dysponować określonymi informacjami, których analiza stanowi podstawę działania. Nie ma tu miejsca na dowolność w interpretacji „zdobytej wiedzy", każda decyzja kryje w sobie działania ludzi, wymaga więc precyzji i rozwagi. Strony biorące udział w walce informacyjnej[32] starają się maksymalnie zakłócić procesy zdobywania

---

[28] Encyklopedia popularna PWN, Warszawa 1982, s. 294.

[29] U. Świętochowska, Informacja w przemianach cywilizacji przełomu XX i XXI wieku, Zeszyty Naukowe Uniwersytetu Gdańskiego, nr 4, Wyd. Adam Marszałek, Toruń, s. 90.

[30] S. Kamiński, Nauka i metoda. Pojęcie nauki i klasyfikacja nauk, Towarzystwo Naukowe KUL, Lublin 1992, s. 24.

[31] Hipermedia - to użyte w jednym kanale informacyjnym różnorodne formy sygnału, stanowiące przekaz faktów lub rzeczywistości wirtualnej, służące do wielokierunkowego, interakcyjnego oddziaływania na podmiot przekazu (R. Kwećka, Wykorzystanie techniki komputerowej w kształceniu oficerów, AON, Warszawa 2000, s. 19).

[32] Zob. L. Ciborowski, Walka Informacyjna, Europejskie Centrum Edukacyjne, Toruń 1999, s. 47.

informacji. Równolegle prowadzą działania mające na celu pogłębienie własnej wiedzy.

Najstarszych, zapisanych treści na ten temat można doszukać się już w VI wieku przed naszą erą. Chiński filozof, Sun Tzu spisał je w traktacie *Sztuka wojny*[33]. Wskazywał tam potrzebę posiadania informacji, choć przy eksponowaniu jej roli stosował inne określenia typu: wykryj, ustal, dowiedz się, zdobądź itp.

Na stronach wspomnianego traktatu formułuje na przykład maksymę: *„Jeśli wiem, że moje oddziały mogą uderzyć na wroga, lecz nie wiem, czy wróg jest przygotowany do odparcia, to szansa przegranej i wygranej jest jeden do jednego. Tak samo, jeśli wiem, że wróg nie jest przygotowany na atak, lecz nie wiem, czy moje oddziały są gotowe do uderzenia, szansa zwycięstwa i porażki jest jak jeden do jednego. Jeśli wiem, że moje oddziały mogą uderzyć i wróg nie jest przygotowany na atak, lecz nie rozpoznałem dobrze ułożenia terenu bitwy, szansa zwycięstwa i porażki jest jak jeden do jednego. Dlatego też twierdzę: Poznaj siebie i poznaj wroga, dopiero wtedy twoje zwycięstwo nie będzie zagrożone. Poznaj warunki terenu i pogody, wtedy twoje zwycięstwo będzie całkowite"*[34] . Jak widać sukces zbrojny Sun Tzu warunkuje wcześniejszym powodzeniem osiągniętym dzięki informacji i wszelkim procesom związanym z jej zdobywaniem. Używa przy tym bardzo obrazowych i jednoznacznych pojęć do eksponowania wynikających z tego konsekwencji.

Znaczenie informacji doceniali również i inni, a w szczególności teoretycy sztuki wojennej. Na szczególną rolę informacji zwraca uwagę w swym dziele „O Wojnie" Carl von Clausewitz interpretując informację „jako całą wiedzę posiadaną o przeciwniku i jego kraju, a więc podstawę

---

[33] Zob. Sun Tzu, Sztuka wojny, wyd. Przedświt Warszawa 1994 r.
[34] Tamże s. 71.

wszelkich własnych idei i działań"[35]. Twierdzi, iż w czasie działań wojennych wiadomości o przeciwniku, jego siłach zbrojnych i możliwościach są najważniejsze. *„Wiele wiadomości jest tu sprzecznych, jeszcze więcej fałszywych, a najwięcej - niepewnych. Wymaga to od oficera pewności w ich rozróżnianiu, jaką mu dać może znajomość rzeczy i ludzi, jak też zdolność osądzania"*[36] Zatem z mnogości informacji dowódca musi wykazać się krytyczną oceną niepewnych danych i wyboru właściwego rozwiązania.

S. Koziej określa informację jako *„niematerialny czynnik zespalający pozostałe czynniki walki zbrojnej w zharmonizowaną całość starcia zbrojnego"*[37].

Z kolei L. Ciborowski określa informację jako *„bodziec oddziałujący na układ recepcyjny człowieka, powodujący wytwarzanie w jego wyobraźni przedmiotu myślowego, odzwierciedlającego obraz rzeczy materialnej lub abstrakcyjnej, [...] który w jego przekonaniu (świadomości) kojarzy się jakoś z tym bodźcem. Oznacza to, że informacje to tylko te doznania, które inspirują umysł ludzki do pewnej wyobraźni. Jej istnienie jest relatywnie związane z istnieniem człowieka i jego umysłu"*[38] .

Indukując treści przytoczonych definicji, zgodzić się należy z przyjętą opinią, że wszystkie dotychczasowe próby definiowania *informacji* są niewystarczające, co najwyżej ukazujące tylko niektóre jej aspekty. Niemniej jednak we wszystkich, chociaż z różną mocą akcentowanych, można zauważyć elementy wspólne. Mianowicie informacja zawsze ma związek ze zdarzeniami istniejącymi w obiektywnej rzeczywistości. Zdarzenia, fakty czy zjawiska stają się informacją po ich dostrzeżeniu i wyjaśnieniu. Dlatego też można założyć, że informacja jest zjawiskiem abstrakcyjnym, rezultatem percepcji i interpretacji. Stąd informacjami można by nazywać tylko te

---

[35] Carl von Clausewitz, O wojnie, Test, Lublin 1945, s. 94.
[36] Tamże, s. 116.
[37] S. Koziej, czynniki walki zbrojnej, Zeszyty Naukowe AON, Warszawa 1993, nr 4, s. 38.
[38] L. Ciborowski, Walka Informacyjna..., wyd. cyt., s. 185.

doznania, które są możliwe do rejestrowania zmysłami ludzkimi, bo tylko one inspirują umysł człowieka do kojarzenia transformowanych doznań w rzeczywiste i abstrakcyjne wyobrażenia o jego otoczeniu. W związku z tym, należy zgodzić się z prof. Ciborowskim, który twierdzi, iż „informacja to bodziec oddziałujący na układ recepcyjny człowieka..." Oznacza to, że **informacje to tylko te doznania, które inspirują umysł ludzki do pewnej wyobraźni**. Ich istnienie jest związane z istnieniem człowieka i jego umysłem.

Interpretując pojęcie informacji, na podstawie definicji prof. Ciborowskiego można więc przyjąć, iż stanowią ją przetworzone widane zgrupowane według określonych kryteriów. Dalsze opracowywanie informacji prowadzi do powstania wiadomości, rozumianych jako przetworzone (opracowane) informacje powiadamiające odbiorcę o sytuacji.

2.1.2. Desygnaty bezpieczeństwa informacyjnego

Przez praktyków, bardzo często bezpieczeństwo informacyjne rozumiane jest jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania. Środki bezpieczeństwa podejmowane są w celu zapewnienia poufności, integralności i dostępności informacji. Ich celem jest wyeliminowanie zagrożenia dla informacji. Wskazuje to, że przytoczone wyżej pojęcie bezpieczeństwa informacyjnego sformułowane zostało w ujęciu negatywnym. W miarę intelektualnego rozwoju i politechnizacji życia informacje zaczęły nabierać coraz większych wartości. Ich posiadanie stało się warunkiem lepszej i bezpieczniejszej egzystencji. Na tym też tle pojawiła się konkurencja. Informacje zaczęto coraz bardziej chronić jako dobro materialne. Chęć stworzenia sobie podobnych do innych lub lepszych warunków życia stworzyła potrzebę zdobywania informacji. Zrodził się zatem swoisty rodzaj rywalizacji - jedni, możliwymi dla siebie

sposobami, dążą do zdobycia informacji, a drudzy - z podobnym zaangażowaniem - starają się im to udaremnić. W postępowaniu takim występuje sprzeczność celów i działań, czyli najbardziej dystynktywnych cech, które kojarzą się z desygnatem pojęcia „walka". Można by powiedzieć, że przedmiotem tej walki stała się informacja, a narzędziami - wszelkie środki dostosowane do jej zdobywania, zakłócania i obrony.

Wobec wzrostu znaczenia informacji ujęcie negatywne bezpieczeństwa informacyjnego jest niewystarczające dla zapewnienia bezpieczeństwa militarnego. Każda płaszczyzna bezpieczeństwa militarnego staje się coraz bardziej zależna od swobodnego przepływu informacji i od zachowania systemów bazujących na informacjach. Wojsko, gospodarka, energetyka, media, systemy finansowe i transportowe są szczególnie uzależnione od systemów informatycznych. Już dziś stanowią one kluczowe elementy procesu podejmowania decyzji w wielu organizacjach cywilnych i wojskowych. Ich dotychczasowy rozwój i zakresy wdrożeń pozwalają prognozować, że obszary zastosowań informatycznych będą obejmować coraz większe przestrzenie funkcjonalne. Teoretycznie został stworzony niemalże nieograniczony dostęp do ogromnych zbiorów informacji, a w tym: finansowych, przemysłowych, marketingowych, technologicznych, wojskowych i innych. Dlatego, niezbędne dla bezpieczeństwa militarnego staje się wprowadzenie polityki bezpieczeństwa informacyjnego zapewniającej ochronę istniejących systemów, ale również gwarantującej państwu i podmiotom, które chroni, posiadanie, przetrwanie i swobodę rozwoju „społeczeństwa informacyjnego". Takie ujęcie bezpieczeństwa informacyjnego ma charakter pozytywny.

Nie wdając się w bardziej szczegółowe rozważania, można zatem założyć, iż środki polityki bezpieczeństwa informacyjnego budowane w oparciu o ujęcie pozytywne muszą uwzględniać, że:

- informacja stanowi zasób strategiczny;

- informacja i wynikająca z niej wiedza oraz technologie informatyczne staną się podstawowym czynnikiem militarnym;
- procesy decyzyjne uzależnione będą od systemów przetwarzania i przesyłania informacji;
- zakłócenie prawidłowości działania systemów informacyjno - sterujących nie wymaga wysokich nakładów materialnych;
- rywalizacja pomiędzy przeciwnikami przeniesie się na płaszczyznę walki informacyjnej.

Wszystko wskazuje na to, że potrzebę wypracowania skutecznych środków polityki bezpieczeństwa informacyjnego wymusza wzrastająca informatyzacja sił militarnych, zwiększające się ciągle możliwości systemów informatycznych, ze wzrastającym nasyceniem wojsk nowymi technikami walki - w tym szczególnie bronią precyzyjnego rażenia. Z badań wynika, że zarówno na Zachodzie jak i Wschodzie współczesna walka informacyjna najbardziej łączona jest z walką zbrojną. Wyrażane są nawet poglądy – z czym trzeba się zgodzić - że w przyszłości ta forma zmagań stać się może ekwiwalentem innych rodzajów walk, w tym i walki zbrojnej. Można więc przewidywać, że obserwowany w tym zakresie wyścig może doprowadzić w przyszłości do tego, że walka informacyjna stanie się nawet substytutem wojny. Umiejętnie prowadzona, jest z pewnością w stanie naruszać szeroko rozumiane proporcje strategiczne i kształtować sceny polityczne, tak w aspekcie międzynarodowym, jak i wewnętrznym.

W odniesieniu do całości problemu, należy stwierdzić, że współczesność wchłonęła też w sferę walki informacyjnej media, które w sposób dla siebie nieświadomy mogą być wykorzystywane przez przeciwnika jako narzędzia skutecznego zakłócania informacyjnego. Szczególnie dogodne do tego warunki istnieją w państwach demokratycznych, gdzie wolna prasa, goniąc za sensacjami dnia codziennego, jest niezwykle podatna na dezinformowanie i błyskawiczne

rozprzestrzenianie wszelkich informacji, które mogą przynosić korzyści określonemu przeciwnikowi[39]. Z tych samych powodów może stać się niepostrzeżenie źródłem upływności informacyjnej. Współczesne środki walki informacyjnej są dostosowane do zdobywania informacji przeróżnymi metodami i technikami. Nawet wśród zaprzyjaźnionych państw trwa w tym zakresie ciągła konkurencja i sądzić należy, że nigdy nie zostanie zaniechana. Uzyskana w tym zakresie przewaga spełniać może nie tylko funkcje wspomagające walkę zbrojną, ale może również spełniać funkcje odstraszania przez unaocznianie przeciwnikowi braku realnych perspektyw do osiągnięcia łatwych korzyści. Już dziś bardzo skutecznymi środkami walki informacyjnej stać się mogą wszystkie te, które dostosowane są do zdalnego wprowadzania wirusów komputerowych do sieci informacyjnych, dostosowanych programowo do samopowielania się i szybkiego rozprzestrzeniania. Ogromne znaczenie mogą mieć również tak zwane bomby logiczne, które jako odpowiednio opracowane aplikacje programowe, będą dostosowane do uaktywniania się na określone wcześniej sygnały lub według zaprogramowanych reżimów czasowych. Skutecznym przedsięwzięciem może być także blokowanie wymiany informacji i szerzenie dezinformacji w torach transmisyjnych za nieświadomym pośrednictwem środków masowego przekazu. Współczesne narzędzia walki informacyjnej stwarzają możliwości podejmowania skutecznej działalności ukierunkowanej na sterowanie procesami decyzyjnymi przeciwnika, nawet w skali państwowej. Wprowadzenie do publicznego i utajonego systemu informacyjnego danego państwa złożonych zbiorów precyzyjnie dobranych prawdziwych i sfałszowanych danych może tworzyć z góry zaplanowane nastroje społeczne i klimat polityczny, które w efekcie spowodują podejmowanie decyzji zgodnych z oczekiwaniami sprawcy tych manipulacji. Współczesne środki walki informacyjnej wskazują, jak nigdy dotąd, na konieczność

[39] Np. wykorzystanie mediów przez Al-kaidę

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

Na podstawie dostępnych materiałów należy stwierdzić, że wysiłki walki informacyjnej mogą być ukierunkowane na podrywanie autorytetu zaatakowanego państwa na arenie międzynarodowej, czy też podrywanie jego zaufania sojuszniczego. W szerokim zakresie może być włączana do tego dyplomacja, handel zagraniczny i media. Na oddziaływanie takie szczególnie jest podatna sfera ekonomiczna, polityczna, polityczna i społeczna. W działaniach tych mogą być również prowokowane incydenty międzypaństwowe, powodujące napięcia społeczne w stosunkach dobrosąsiedzkich.

Dotychczasowe doświadczenia wskazują, że wojna informacyjna w ścisłym rozumieniu tego słowa wymaga znacznie mniejszych nakładów środków niż klasyczne kampanie wojenne. Atak na gospodarkę informacyjną wymaga jedynie ograniczenie przepływu informacji - jest to z całą pewnością

mniej kosztowne niż przeprowadzanie fizycznego ataku na jego infrastrukturę[40].

W odniesieniu do całości problemu, zgodnie z realistyczną teorią bezpieczeństwa narodowego utrzymanie bezpieczeństwa militarnego w aspekcie informacyjnym powinno być oparte na następujących przesłankach:

- zwiększanie ochrony własnych systemów informacyjnych;
- stała ocena słabości systemów informacyjnych potencjalnych przeciwników, w tym takie działania, jak tworzenie możliwości wtargnięcia do ich systemów;
- przygotowanie możliwych form odpowiedzi na atak, w tym z wykorzystaniem informacyjnych, jak i konwencjonalnych wojskowych środków rażenia;
- rozwijanie metod szacowania poniesionych i/lub zadanych zniszczeń (strat informacyjnych).

Natomiast, w wypadku zastosowania teorii liberalnej bezpieczeństwa militarnego ochrona systemów informacyjnych będzie polegała przede wszystkim na:

- zwiększaniu poziomu powiązań i współzależności systemów informacyjnych różnych państw w celu przeciwdziałania zagrożeniom;
- tworzenie globalnych instytucji i porozumień zapobiegających wojnie informacyjnej.

2.2. Wykorzystanie informacji w zarządzaniu bezpieczeństwem militarnym

Informację, w zarządzaniu bezpieczeństwem militarnym, rozpatrywać można zarówno statycznie jak i dynamicznie. W pierwszym wypadku

---

[40] Por. Białas A. , „Bezpieczeństwo informacji i usług w nowej instytucji i firmie", Wydawnictwo WNT, Warszawa 2006, s. 79.

koncentracja uwagi kierowana będzie na treść informacji istniejącej w danym momencie. Natomiast w ujęciu dynamicznym zwracamy uwagę na przekaz informacji. Przekaz ten występuje między jej nadawcą i odbiorcą, stąd informacja przekazywana może być między maszynami, między człowiekiem i maszyną, maszyną i człowiekiem oraz między ludźmi. Natomiast, rozpatrując informacje z punktu widzenia czynnika czasu, informacja dotyczyć może przeszłości (informacja retrospektywna), stanu bieżącego (informacja bieżąca) lub okresów przyszłych (informacja prospektywna).

Na podstawie dostępnych materiałów ocenia się, że informacja jest podstawowym instrumentem opisu „wejścia" (WE), „wyjścia" (WY) oraz „czasu" (T) w każdej organizacji w tym też w bezpieczeństwie militarnym. Stanowi ona podzbiór informacji znakowych, typowych dla danego języka, w którym jest wyrażana. Są nimi litery, cyfry i znaki specjalne, występujące w danym języku etnicznym lub maszynowym, a także zbiory punktów, tworzących linie proste lub krzywe - w języku obrazów oraz mowa i dźwięki - w języku dźwięków itd[41]..

Wyniki badań dowodzą, że w ramach bezpieczeństwa militarnego, informacje spełniają następujące główne funkcje: informacyjną (powiadamiającą), decyzyjną, sterującą oraz tworzącą modele:

- **funkcja informacyjna** - informacja może wystąpić w formie potencjalnej lub użytecznej. Każda informacja użyteczna jest jednocześnie informacją potencjalną, lecz nie każda informacja potencjalna ma jednocześnie cechę użyteczności. Każda z nich, zarówno prawdziwa jak i fałszywa, spełnia funkcję informacji potencjalnej. Aby informacja potencjalna mogła spełniać funkcję informacji użytecznej, zakłada się, że muszą być spełnione następujące założenia:

[41] Zob. J. Stokłosa, T. Bilski, T. Pankowski, Bezpieczeństwo danych w systemach informatycznych. Warszawa 2001, s. 120-148.

- należy zdefiniować odbiorcę informacji (informacja użyteczna jest zawsze użyteczna dla kogoś, a niekoniecznie dla wszystkich);
- informacja użyteczna występuje tylko wtedy, gdy powiększa zasób wiedzy jej odbiorcy. Z tego powodu dostarczanie informacji użytecznej wymaga:
    - rozpoznania aktualnych zasobów wiedzy odbiorcy;
    - rozpoznania potrzeb informacyjnych odbiorcy;
    - identyfikacji języka, którym posługuje się odbiorca;
    - identyfikacji formy przekazu informacji (np. opis, tabela, wykres itp.) oraz częstotliwości jej pojawiania;

- **funkcja decyzyjna -** informacji polega na tym, że decyzja jest jedną z form informacji (informacja tworzy decyzję) oraz na tym, że dostarcza informacji niezbędnych do podjęcia decyzji. W tym ostatnim wypadku, zakłada się, że informacja dotyczy zarówno samego problemu decyzyjnego, jak i procedur, możliwych do wykorzystania przy podejmowaniu decyzji;
- **funkcja sterująca -** informacji polega na tym, że przekazujący informację chce wywołać zamierzoną reakcję na nią u jej odbiorcy. Inaczej mówiąc nadawca informacji stara się (z różną siłą i często z różnym skutkiem) wpłynąć na stanowisko (poglądy, działania) innej osoby lub osób czy też organizacji. Szczególnie odnosi się to do decyzji kierowniczych, podejmowanych w ramach zarządzania bezpieczeństwem militarnym;
- **funkcja modelowania -** jest konsekwencją tego, że bezpieczeństwo militarne jest także systemem informacyjnym, a więc systemem, którego sposób funkcjonowania można ująć informacyjnie, jak i tego, że należy do systemów skrajnie złożonych, czyli takich, którego sposób funkcjonowania nie może być rozpoznany w pełni, co prowadzi do jego modelowania.

Ostatnia z form funkcjonowania bezpieczeństwa militarnego to zarządzanie,[42] obejmuje ono dwie części. Pierwszą z nich jest kierowanie w szerszym sensie, czyli część regulująco-sterująca, a drugą - część społeczno-polityczna, dotycząca:

- norm społeczno-militarnych i politycznych, charakterystycznych dla ustroju państwa, obowiązującego w danym okresie;
- stopnia centralizacji decyzji, określającego czego te decyzje dotyczą i gdzie są zlokalizowane;
- stopnia swobody decyzyjnej różnego rodzaju bezpieczeństwa.

Konkludując, należy zwrócić uwagę, że zarządzanie w bezpieczeństwie militarnym może być rozpatrywane z instytucjonalnego, funkcjonalnego oraz informacyjnego punktu widzenia. Dostępne materiały określają, że pod pojęciem **zarządzania w ujęciu instytucjonalnym** rozumiemy określoną liczbę osób, którym przyznano uprawnienia do wydawania poleceń i podejmowania decyzji militarnych. Natomiast, **zarządzanie** w **ujęciu funkcjonalnym można** odnosić - niezależnie od stanowisk i szczebli kierowniczych - do tych działań, które służą kierowaniu procesami. Natomiast, punktem wyjścia w określeniu **zarządzania** w **ujęciu informacyjnym** jest fakt, że zarządzanie stanowi sobą określony podzbiór procesów intelektualnych (myślowych), nakierowany na działania regulacyjno-sterujące. Stąd jakość takich działań zależeć będzie głównie od:

- rozmiaru i struktury dostępnych informacji, a jednocześnie w maksymalnym stopniu istotnych dla realizacji celów bezpieczeństwa militarnego;
- nastawień, motywacji, poglądów, a szerzej mówiąc - od uwarunkowań psychologicznych i socjologicznych osób, włączonych w różnym stopniu i zakresie w procesy zarządzania w bezpieczeństwie militarnym.

---

[42] W. Falkiewicz, Systemy informacyjne w zarządzaniu. Warszawa 2002, s. 24.

W odniesieniu do całości problemu, jest to o tyle istotne, gdyż człowiek także w bezpieczeństwie militarnym - po pierwsze - jest kreatorem informacji, tzn. tworzy ją oraz wprowadza w obieg, - po drugie - jest jednocześnie analizatorem funkcjonujących informacji ze względu na ich przydatność, użyteczność, kompletność, wystarczalność, aktualność itp. własności.

Wynik powyższej analizy można sprowadzić do następującego wniosku: jeśli wyodrębnimy w bezpieczeństwie militarnym **podsystem zarządzania,** odpowiedzialny za całościowe sterowanie jego działalnością, jak też za działalność jego części (podsystemów) oraz **podsystem działalności podstawowej**, to podsystem informacyjny, spełniał będzie funkcje usługowe na rzecz obu ww. podsystemów.

2.2.1. Umiejscowienie informacji według funkcji zarządzania

Różnorodność działań podejmowanych w bezpieczeństwie militarnym i związana z tym różnorodność modeli informacyjnych strukturalizuje popyt na informacje, wykazujące specyficzne swe własności i charakterystyki. Aby ustalić te charakterystyki, należy ustalić kryteria, wg których można wyodrębnić określone zbiory informacji charakteryzujące się podobieństwem ich cech. Z przeprowadzonej analizy wynika, że kryteria te dotyczą: 1) typowych funkcji zarządzania, 2) głównych dziedzin zarządzania, 3) głównych strumieni informacji, 4) głównych poziomów zarządzania[43].

Jeśli przyjąć za punkt wyjścia podejście funkcjonalne do problematyki zarządzania w bezpieczeństwie militarnym, wtedy w zbiorze różnorodnych działań wyodrębnić możemy funkcje, czyli określone jednorodne tematycznie i stale realizowane grupy działań, wywodzące się z zasady podziału

[43] W. Falkiewicz, Systemy informacyjne w zarządzaniu. Warszawa 2002, s. 48.

czynności. Dostępne materiały wyróżniają następujące, główne funkcje zarządzania w bezpieczeństwie militarnym:

- **planowanie (P)** - czyli ustalanie celów, które zamierza się osiągnąć w danym czasie i w danym obszarze tematycznym oraz ustalanie zadań, realizacja których zapewnić może wykonanie tych celów. Czynnik czasu może tu dotyczyć okresów o różnej rozpiętości, od dni do przedziałów wieloletnich. Obszary tematyczne mogą obejmować cele i zadania stojące przed bezpieczeństwem militarnym, traktowanym jako całość, jak też dotyczyć mogą określonych fragmentów jego części składowych;
- **organizowanie** - czyli **pozyskiwanie i alokacja zasobów (O),** a więc środków niezbędnych do realizacji celów i zadań. Zasoby potrzebne do prowadzenia własnej działalności podzielić można na zasoby zewnętrzne i własne. Do pierwszej grupy należą zasoby ludzkie, materialne oraz finansowe. Podfunkcja ich pozyskiwania następuje w drodze penetracji odpowiednich obszarów oraz ilości i jakości możliwych do pozyskania zasobów. Zasoby własne dotyczą zasobów informacyjnych;
- **motywowanie (M)** - czyli tworzenie warunków do sprawnej, wydajnej i efektywnej pracy osób, w świetle stojących do wykonania celów i zadań oraz posiadanych środków. Funkcja ta realizowana będzie głównie przez politykę kadrową oraz płacową w organizacji bezpieczeństwa militarnego;
- **kontrolowanie (K)** - jest to funkcja polegająca na okresowym porównywaniu osiąganych, rzeczywistych efektów i wyników z zakładanymi celami i zadaniami. Podstawą do porównania będą meldunki zwrotne z realizacji zadań i stosowne analizy badające przyczyny i skutki zaistniałych zjawisk, stanów i procesów w bezpieczeństwie militarnym;

- **koordynowanie (KO)** - funkcja ta polega na zapewnieniu harmonijnego współdziałania ze sobą wszystkich, wyżej wymienionych funkcji (P, O, M i K). W praktyce zachodzi bowiem często konieczność równoczesnego włączania się wielu działań, zależnych od różnych funkcji;
- **decydowanie (D)** - jest to szczególna funkcja, różniąca się od pozostałych tym, że jest funkcją przekrojową, tzn. przebiegającą przez wszystkie, wcześniej wymienione funkcje. Możemy więc mówić o decyzjach planistycznych, organizacyjnych, motywacyjnych, kontrolnych i koordynacyjnych. Wszystkie wymienione wyżej funkcje mają zwykle swą wewnętrzną, wielopoziomową strukturę, opartą na wyodrębnionych podfunkcjach cząstkowych w bezpieczeństwie militarnym.

Każda z wymienionych funkcji posiada swe własne potrzeby informacyjne w bezpieczeństwie militarnym. Należy jednak podkreślić, że poszczególne informacje mogą obsługiwać potrzeby zgłaszane przez wiele funkcji zarządzania. Stąd łączne zapotrzebowanie na informacje, zgłaszane przez poszczególne funkcje w bezpieczeństwie militarnym stanowi sumę logiczną (a nie arytmetyczną) informacji niezbędnych dla ich prawidłowego działania[44].

W odniesieniu do całości problemu zarządzania bezpieczeństwem militarnym, można zaobserwować powstanie czwartego poziomu zarządzania, zwanego w literaturze **poziomem wiedzy i danych** *(data and knowledge level of management).*

Ten czwarty poziom zarządzania bezpieczeństwem militarnym powstał na tle pogłębiającej się złożoności potrzeb informacyjnych, związanych z odczuwaną luką, której wypełnienia nie gwarantowała uzyskiwana z posiadanych informacji wiedza standardowa, zarówno prosta,

---

[44] Tamże, s. 149.

jak i złożona. Zaistniała zatem konieczność wydobywania wiedzy niestandardowej, która mogła wyjść na przeciw tym nowym potrzebom informacyjny, angażując w tym celu najnowocześniejsze technologie informacyjne. Ponadto, istotność bardzo złożonych potrzeb informacyjnych spowodowała, że samo wydobywanie wiedzy oparte o przygotowywanie odpowiednich modeli informacyjnych, stało się niewystarczające. W związku z tym założono, że należy taką wiedzą również zarządzać, co wymaga m.in.:

- zbierania informacji, intuicji i doświadczeń;
- zbierania informacji o „intelektualnym kapitale" (wiedza, dokumenty, raporty badawcze itp.) ich gromadzenia (banki danych, macierze dyskowe itp.) w systemach informatycznych,
- gromadzenia informacji o umiejętnościach i procedurach działania poszczególnych osób, głównie wywodzących się z kadry decyzyjnej.

Jednocześnie zakłada się, że spełnienie tych wymagań musi być jednocześnie wspierane przez specyficzne technologie informacyjne takich organizacji. Poza tym, możliwość spełnienia zadań stawianych przed poziomem danych i informacji wymaga zatrudnienia wysoko wyspecjalizowanego personelu, pracującego w tym obszarze. Z przeprowadzonych badań wynika, że należy tu wyodrębnić dwie grupy specjalistów zarządzających bezpieczeństwem militarnym: zajmujących się wiedzą oraz zajmujących się danymi. Przed pracownikami zajmującymi się wiedzą *(knowledge workers)* należy postawić zadania, polegające głównie na:

- tworzeniu oraz dostarczaniu w zintegrowany sposób nowej, niestandardowej wiedzy;
- spełnianiu przez te osoby funkcji wewnętrznych konsultantów i ekspertów zarówno w zakresie wiedzy aktualnie, jak i w zakresie kierunkowania nowych badań w dostosowaniu do aktualnych i dających się przewidzieć potrzeb informacyjnych, związanych z opisem, analizą zjawisk czy z decyzjami, które należy podjąć;

- funkcji kreatorów zmian w sposobach działania[45].

Uogólniając można stwierdzić, aby spełnić wymienione zadania, osoby pracujące w obszarze wiedzy powinny legitymować się bardzo wysokimi kwalifikacjami zawodowymi (inżynierowie, ekonomiści, analitycy, projektanci itp.) a jednocześnie znawstwem nowoczesnych technologii informacyjnych i umiejętnościami posługiwania się nimi. Dostarczana przez nich wiedza powinna być wyrażona w języku zrozumiałym przez kadrę kierowniczą. Osoby te powinny pracować na rzecz wszystkich poziomów, funkcji i dziedzin zarządzania oraz mieć dostęp do wszystkich zbiorów, baz danych i informacji.

Druga grupa osób to ci, którzy zajmują się danymi *(data workers).* Celem tej grupy będzie zapewnienie najbardziej sprawnej obsługi oraz transferu informacji (głównie między decydentami, specjalistami oraz osobami zajmującymi się wiedzą, bez względu na lokalizację ich miejsc pracy). Będą to osoby o niższych kwalifikacjach zawodowych, niż pracownicy zajmujący się wiedzą (np. sekretarki, osoby zajmujące się obsługą i konserwacją sieci komputerowych itp.). Osoby te będą obsługiwać wszystkie poziomy, funkcje i dziedziny zarządzania oraz zaznajomione będą z technologiami przygotowywania i przesyłania informacji.

Z rozważań wynika, że rozwój tego poziomu zarządzania będzie ściśle powiązany ze stosowaniem nowoczesnych technologii informacyjnych, wymagających znacznego zaawansowania kapitałowego, w zakresie zakupu odpowiedniego sprzętu, oprogramowania oraz rozwoju sieci komputerowych. Z tego też powodu, tempo organizacji poziomu danych i wiedzy będzie różne. Zróżnicowany będzie również jego zasięg oddziaływania.

---

[45] Por. CSO - Magazyn zarządzających bezpieczeństwem 3/2006, s. 34.

2.2.2. Zarządzanie zasobami informatycznymi w bezpieczeństwie militarnym

Zarządzanie zasobami informatycznymi jako jedna z funkcji bezpieczeństwa militarnego jest koniecznością i odpowiedzią na wyzwanie, które niesie społeczeństwo informacyjne. Warunkiem istnienia na rynku i rozwoju każdej organizacji - w tym bezpieczeństwa militarnego - jest pożądane kształtowanie określonych zasobów informatycznych rozpatrywanych w kategoriach zasobów strategicznych[46].

Na podstawie dostępnych materiałów zespół autorski założył, że pod pojęciem **zasobu informatycznego należy rozumieć zasoby rzeczowe, informacyjne i ludzkie**. Do zasobów rzeczowych należał będzie sprzęt komputerowy wraz z wszelkimi urządzeniami wprowadzania i wyprowadzania informacji, nośniki danych, urządzenia telekomunikacyjne. Zasoby informacyjne stanowić będą informacje przetwarzane w systemach informacyjnych bezpieczeństwa militarnego lub w otoczeniu, istotne dla prowadzenia działalności oraz oprogramowanie użytkowe i systemowe. Zasoby ludzkie natomiast to wiedza, umiejętności, doświadczenia użytkowników i administratorów informacyjnych systemów zarządzania.

Należy zwrócić uwagę także, że zarządzanie wszelkimi zasobami, w tym także zasobami informatycznymi wiąże się z koniecznością sterowania procesami:

- zdobywania i pozyskiwania zasobów;
- gromadzenia, przechowywania i ochrony zasobów, alokacji i dystrybucji zasobów;
- przetwarzania i eksploatacji zasobów.

Ogólnie można przyjąć, że działalność ta jest dalece różnorodna, nawet w tak wąskiej dziedzinie, jaką jest zastosowanie informatyki

---

[46] M. Pańkowska, Zarządzanie zasobami informacyjnymi, Delfin 2001, s. 59.

w zarządzaniu bezpieczeństwem militarnym. Nie ulega dziś wątpliwości, że dysponent zmuszony będzie widzieć problemy całościowo w powiązaniu z innymi, jak też fragmentarycznie, cząstkowo w różnych aspektach. Czynność ta poddana będzie konieczności ciągłego dopasowywania do nowych sytuacji międzynarodowych, a rządzona będzie w dużym stopniu zdarzeniami, nad którymi trudno jest mieć stałą kontrolę.

W odniesieniu do wytworzonej sytuacji, najważniejszym celem zarządzania zasobami informatycznymi w bezpieczeństwie militarnym jest lepsze informowanie i większa decyzyjność informacji. Pod tym pojęciem należy rozumieć skuteczne i racjonalne wykorzystanie informacji do podejmowania decyzji.

Ponadto, wyniki badań skłaniają do wnioski, że w bezpieczeństwie militarnym - podobnie jak w innych organizacjach - problem zarządzania techniką informatyczną sprowadza się do implementacji systemu administrowania wewnętrzną siecią komputerową. Inne podejście jest o tyle trudne, że brak jest możliwych do naśladowania, dobrze przygotowanych metod zarządzania techniką informatyczną, jak i powszechnie dostępnych narzędzi automatyzacji administrowania systemami informacyjnymi, narzędzi monitoringu wykonania zadań i pracy systemów informacyjnych, narzędzi analizy potencjalnych użyteczności techniki informatycznej w organizacji. Pożądane rozwiązania muszą rozpoznać i akceptować różnorodność systemów komputerowych i oprogramowania użytkowego. Ponadto należy zauważyć, że wprowadzenie techniki informatycznej do organizacji zawsze jest zmianą i im bardziej nowoczesny sprzęt i oprogramowanie, tym zmiana odczuwana jest jako bardziej radykalna i trudna do akceptacji przez użytkowników. Zatem dla zarządzania zasobami informatycznymi wskazane byłoby przyjęcie podejścia Hammera i Champy'ego radykalnej przebudowy

procesów organizacyjnych[47]. Hammer i Champy w swojej pracy przedstawili szereg założeń istotnych dla skutecznej implementacji techniki informatycznej w organizacji, którą by można zaadoptować w bezpieczeństwie militarnym m.in. zalecają organizować przedsięwzięcia informatyzacji na podstawie prognoz użyteczności efektów, a nie tylko w oparciu o specyfikację zadań automatycznego przetwarzania, traktować geograficznie rozproszone zasoby informatyczne jak scentralizowane, ustalać odpowiedzialność i przywileje podejmowania decyzji na poziomie bezpośredniego wykonawcy procesu.

Dość istotny jest również fakt, że rozwój techniki informatycznej spowodował, że sprzęt komputerowy i oprogramowanie stały się obecne na każdym stanowisku pracy, rozwinęły się sieci łączące ze sobą społeczności, siły militarne, członków sojuszów, aplikacje programowe tworzone są przez specjalistyczne firmy, ośrodki informatyczne w dużych instytucjach, jak i przez użytkowników końcowych. To nowe środowisko przetwarzania i przesyłania informacji zrodziło nowe wyzwania dla informatyków, pracowników różnych działów bezpieczeństwa militarnego. Główną potrzebą stała się konieczność uporządkowania zagadnień racjonalnej i efektywnej eksploatacji zasobów w zarządzaniu bezpieczeństwem militarnym.

Z militarnego punktu widzenia decydent musi dostrzegać różnice między zarządzaniem na podstawie informacji i zarządzaniem informacją. Z badań wynika, że analiza zarządzania informacją i pozostałymi zasobami informatycznymi w bezpieczeństwie militarnym jest sposobem ustalania wartości informacji. Analiza prowadzi do przekonania, że jeśli decydent lepiej rozumie znaczenie i rolę zasobu informacyjnego, może doskonalić zarządzanie tym krytycznym zasobem.

---

[47] M. Hammer, J. Champy, Reengineering w przedsiębiorstwie. Neumann 96, s. 37.

Powyższe założenia prowadzi do postawienia tezy, że zasoby informacyjne w zarządzaniu bezpieczeństwem militarnym można analizować w czterech aspektach:

- aspekt rzeczowy - dotyczy on treści i jest nierozerwalnie związany z pozostałymi aspektami, mimo że najlepiej funkcjonowałby w oderwaniu od pozostałych;
- aspekt autoprezentacji - każdy zasób informacyjny oprócz treści zawierał będzie prezentacje nadawcy i rzucał światło na percepcję aspektu rzeczowego, wyraża np. niechęć, entuzjazm;
- aspekt relacji – zasób informacyjny będzie nawiązaniem kontaktu nadawcy i odbiorcy. Nieważne, czy któryś z nich zareaguje, czy milczy. Aspekt relacji pozostanie w cieniu treści przekazu. Dla kształtu relacji niezależnie od treści zasobu informacji ważne będzie wzajemne nastawienie nadawcy i odbiorcy;
- aspekt apelu - każda komunikacja ma swój cel, wywiera wpływ na odbiorcę, ma skłonić go do zrobienia czegoś. Często nadając apel nadawca nie zdaje sobie sprawy, że odbiorca jest przeczulony na apele i natychmiast reaguje działaniem.

W odniesieniu do całości problemu, wartość zasobów informacyjnych wynikać będzie z korzyści, jakie zapewnia użytkownikowi. Im bardziej zadowalające są konsekwencje decyzji podjętej na podstawie informacji, tym wyższa wartość informacji i zasobów informacyjnych. Problem wartości zasobów informacyjnych w zarządzaniu bezpieczeństwem militarnym jest często ignorowany ze względu na swój subiektywizm. Jednakże subiektywna ocena wartości zasobów informacyjnych jest lepsza niż żadna i jakość oraz koszt systemu informacji może pozostawać pod wpływem tych ocen. Przy braku ocen wartości zasobów informacyjnych, organizacja jaką jest bezpieczeństwo militarne może zignorować problem ich ochrony, albo w takim samym stopniu chronić wszelkie zasoby informacyjne w obrębie

organizacji lub zapewnić częściową ochronę zasobów informacyjnych w obrębie granic i otoczenia bezpieczeństwa militarnego. Wszystkie trzy podejścia są wadliwe, pierwsze grozi utratą wartościowej zasobów informacyjnych, drugie jest kosztowo nieefektywne, a trzecie prowadzi do ochrony zasobów informacyjnych niskiej wartości przy braku ochrony zasobów informacyjnych wysokiej wartości, do kreowania sposobności wykorzystania słabości ochrony, przecieku informacji lub ataku w innym niechronionym miejscu[48].

Nietrudno dostrzec w naszych dotychczasowych rozważaniach, że wartość zasobów informacyjnych może być wyrażona także przez jej jakość. Jakość - można definiować - jako ogół cech i właściwości wyrobu lub usługi decydujących o zdolności wyrobu lub usługi do zaspokojenia stwierdzonych lub przewidywanych potrzeb[49]. Natomiast, jakość zasobów informacyjnych nie będzie określana bezpośrednio, lecz za pośrednictwem innych zmiennych. Należą do nich – między innymi - miary jakości zasobów informacyjnych:

- miary jakości definiowania: zgodność z istotnymi standardami i wytycznymi, zgodność wzajemna wielu nazw, jasność, precyzja, kompletność, konsensus (uzgodnienie opinii), unikatowość, wyjątkowość określeń, poprawność;
- miary jakości treści: kompletność zarówno w odniesieniu do rodzaju, jak i wartości, ważność, użyteczność dla decyzji, aktualność stwierdzona w drodze pomiaru na próbie losowej, precyzja pomiaru kosztów, brak zbędnej duplikacji wystąpień, zgodność replikowanych, dystrybuowanych, redundantnych lub pochodnych.

Wśród innych własności zasobów informacyjnych determinujących ich jakość wymienić należy:

---

[48] M. Pańkowska, Zarządzanie zasobami informacyjnymi, Delfin 2001, s. 136.
[49] Słownik Języka Polskiego, T. I, PWN, Warszawa 2002, s. 769.

- istotność: tylko informacja potrzebna w danej sytuacji jest otrzymywana, istotność eliminuje nadmiar informacji;
- kompletność: wszelka informacja odpowiednia dla danej sytuacji jest otrzymywana, kompletność eliminuje niedomiar informacji;
- aktualność: wszelka niezbędna informacja jest otrzymywana dokładnie na czas. Aktualność eliminuje sytuację, gdy informację otrzymujemy za późno lub za wcześnie;
- zwięzłość, treściwość: wszelka niezbędna informacja jest otrzymywana w zrozumiałej i możliwej do natychmiastowego użycia postaci;
- użyteczność: informacja jest niezbędna i przydatna dla podejmowania decyzji.

Reasumując wnioski z przeprowadzonej analizy, należy stwierdzić że zarządzanie zasobami informacyjnymi w bezpieczeństwie militarnym obejmuje identyfikację i analizę dostępnej i koniecznej informacji i procesów jej przetwarzania, a następnie planowanie i kontrolę działań dla rozwoju tych zasobów i procesów przetwarzania dla osiągnięcia celów bezpieczeństwa militarnego.

Zarządzanie wymaga spełnienia następujących warunków:

- powinno być zintegrowane;
- powinno być niezależne od jakiejś szczególnej aplikacji;
- powinno być dostępne wielu użytkowników jednocześnie, zalecane jest scentralizowane zarządzanie.

Zasoby informatyczne są narzędziem, które zwiększa wartość bezpieczeństwa militarnego, buduje przewagę konkurencyjną i wspomaga zarządzanie.

2.3. Ochrona informacji w bezpieczeństwie militarnym

Współczesna ochrona informacji stanowi problem techniczno - organizacyjny. Głównym celem bezpieczeństwa jest kontrolowanie dostępu do danych (informacji), zasobów informacyjnych. Obserwowane zagrożenia i dokonane przestępstwa związane z informacją czy tez zasobami informacyjnymi stały się podstawą sformułowania pytań: co, jak, kiedy, przed kim i za jaką cenę chcemy chronić[50].

Podstawowa zasada w ochronie informacji czy tez zasobów informacyjnych stanowi, że jedynie osoba o prawidłowo sprecyzowanych uprawnieniach może mieć możliwość przeglądania, kreowania, usuwania lub modyfikowania informacji.

Przy wyborze rozwiązań ochrony informacji (zasobów informacyjnych) w zarządzaniu bezpieczeństwem militarnym należy uwzględnić techniczne trendy i dążenia występujące przy projektowaniu systemu zarządzania bezpieczeństwem informacyjnym. Występujące tam założenia to:

- przesłanie jak najwięcej danych (czyli zwiększenie pojemności systemu);
- przesłanie danych z każdego miejsca i do każdego miejsca (czyli upowszechnienie dostępu do systemu);
- utrzymanie kontroli (czyli zapewnienie rzetelności działania systemu i usług w nim dostarczanych);
- osiągnięcie zamierzonych i wyżej wymienionych celów jak najtaniej.

Z przeprowadzonych badań wynika, że dzisiejsze pojęcie bezpieczeństwa systemów komputerowych to nie tylko środki techniczne i programowe systemów ochrony, ale i zarządzanie zasobami oraz informacją,

---

[50] Zob. PN-EN ISO 10011 Wytyczne dotyczące audytowania systemów zarządzania jakości i/lub zarządzania środowiskowego, PKN, Warszawa 2003, s. 7.

które jest w gruncie rzeczy pochodną dobrej organizacji jaką jest bezpieczeństwo militarne.

Sieci korporacyjne zmieniają się nieustannie i ktokolwiek planuje dzisiaj zarządzanie i ochronę bezpieczeństwa militarnego, musi być świadom konieczności zaakceptowania pewnego „obszaru wiedzy" co do przyszłej topologii sieci i systemu. Na domiar złego typowe duże sieci (systemy) są geograficznie rozległe, fizycznie heterogeniczne, a logicznie bardzo złożone.

Doświadczeni administratorzy sieci i systemów uważają, że w pierwszej kolejności należy wprowadzić właściwą politykę ochrony na najwyższych szczeblach. Problem ochrony sieci bezpieczeństwa militarnego należy postawić na wszystkich poziomach struktur organizacyjnych systemu sterowania i zarządzania w bezpieczeństwie militarnym, nie wyłączając z tego ścisłego kierownictwa, czyli najwyższej warstwy systemu[51].

Sprawdzianem przygotowania i sprawności systemu zarządzanie bezpieczeństwem informacyjnym będzie ochrona danych i oraz identyfikacja kategorii zagrożeń systemów komputerowych a w tym:

- utrzymywania poufnych danych, ważnych dla działalności bezpieczeństwa militarnego i danych personalnych;
- utrzymywania integralności i dokładności danych, zapamiętywanych w systemie komputerowym;
- zapewniania upoważnionym użytkownikom stałego dostępu do danych;
- upewnienia się, że prowadzone działania są zgodne z prawem, etyką, zawartymi umowami międzynarodowymi, podpisanymi umowami np. licencyjnymi.

Jednak, istnieje wiele różnych czynników, które mogą powodować, że niektórych z wyżej wymienionych celów nie można osiągnąć. Nie oznacza to

---

[51] Zob. Wykaz obowiązujących standardów technologii informatycznych do stosowania w resorcie obrony narodowej na lata 2007-2008, Departament Informatyki i Telekomunikacji MON, Warszawa 2007.

jednak, że należy zaniechać wysiłków. Polityka bezpieczeństwa[52] to działanie długofalowe, nie jednorazowy wysiłek czyniony po ujawnionej próbie włamania się do systemu lub na skutek konieczności odzyskania utraconych plików.

Dość istotny jest również fakt, że istnieje kilka kategorii zagrożeń systemu informatycznego, z którymi osoba odpowiedzialna za bezpieczeństwo powinna sobie radzić.

A. Zagrożenia fizyczne:

- kradzież sprzętu, plików lub danych;
- celowe zniszczenie (sabotaż);
- bezmyślne zniszczenie danych lub programów (wandalizm).

B. Siły wyższe (powódź, piorun, pożar) i inne katastrofy:

B.1. Użytkownicy:

- pomyłki i nieuwaga;
- celowe działania na szkodę firmy;
- wykorzystanie służbowego sprzętu i oprogramowania (nielegalne kopiowanie) do celów niezgodnych z przeznaczeniem.

B.2. Technologia:

- awarie sprzętowe;
- awarie systemowe i błędy programów;
- wirusy i bomby logiczne w programach.

B.3. Komunikacja:

- zdalny dostęp do sieci dla legalnych użytkowników;
- nielegalny dostęp do sieci (hakerzy);
- celowe podsłuchiwanie komunikacji.

---

[52] Zob. PN ISO/IEC 17799:2007 –Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, Warszawa 2007, s. 68.

Ponadto, uwzględniając zasady określone w normie (PN-EN ISO 19011), ochrona informacji w systemach związana jest z następującymi usługami powiązanymi zarówno z komunikacją jak i z przetwarzaniem danych:

- kontrola dostępu (access control) - ochrona przed nieuprawnionym dostępem do zasobów;
- integralność dostępu (data integrity) - gwarancja spójności danych; ochrona przed modyfikacją, wtrąceniem, wymazaniem danych;
- uwierzytelnienia (authentication) - informacja i kontrola tożsamości stron lub danych wymienianych pomiędzy nimi podczas danej sesji komunikacyjnej,
- niezaprzeczalność (non-repudation) - metody rozstrzygnięcia ewentualnego sporu pomiędzy nadawcą, a odbiorcą dotyczącego zarówno faktu nadania i odbioru informacji jak i jej treści;
- poufność danych (confidentiality) - ochrona danych przed nieuprawnionym uzyskaniem informacji przez strony niepowołane.

Kontrola dostępu (czyli tzw. autoryzacja) jest usługą dzięki, której tylko uprzywilejowane podmioty mogą otrzymać dostęp do zasobów. Podmiotem może być zarówno człowiek jak i proces, a zasobem - proces, bądź system sieciowy[53].

W literaturze przedmiotu zwraca się szczególna uwagę na fakt, że kontrola dostępu jest pierwotna względem pozostałych usług i realizuje się ją przed wykorzystaniem zasobów.

Natomiast, usługa integralności zapewnia ochronę przed zmianą porządku (kolejności) w danych, wtrąceniem lub modyfikacją oraz skasowaniem.

---

[53] Por. PN-I-13335-1 Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, Warszawa 1999, s 19.

Uwierzytelnienie definiowane jest jako mechanizmy umożliwiające weryfikację tożsamości podmiotu przez inny podmiot lub weryfikację źródła danych.

Istnieją dwa stopnie uwierzytelniania (ISO 9594-8):

- proste uwierzytelnianie - polega ono na identyfikatorze i haśle podawanym przez nadawcę, które jest weryfikowane przez odbiorcę.
- silne uwierzytelnianie - wymaga zastosowania technik kryptograficznych, chroniących wymieniane informacje uwierzytelniające.

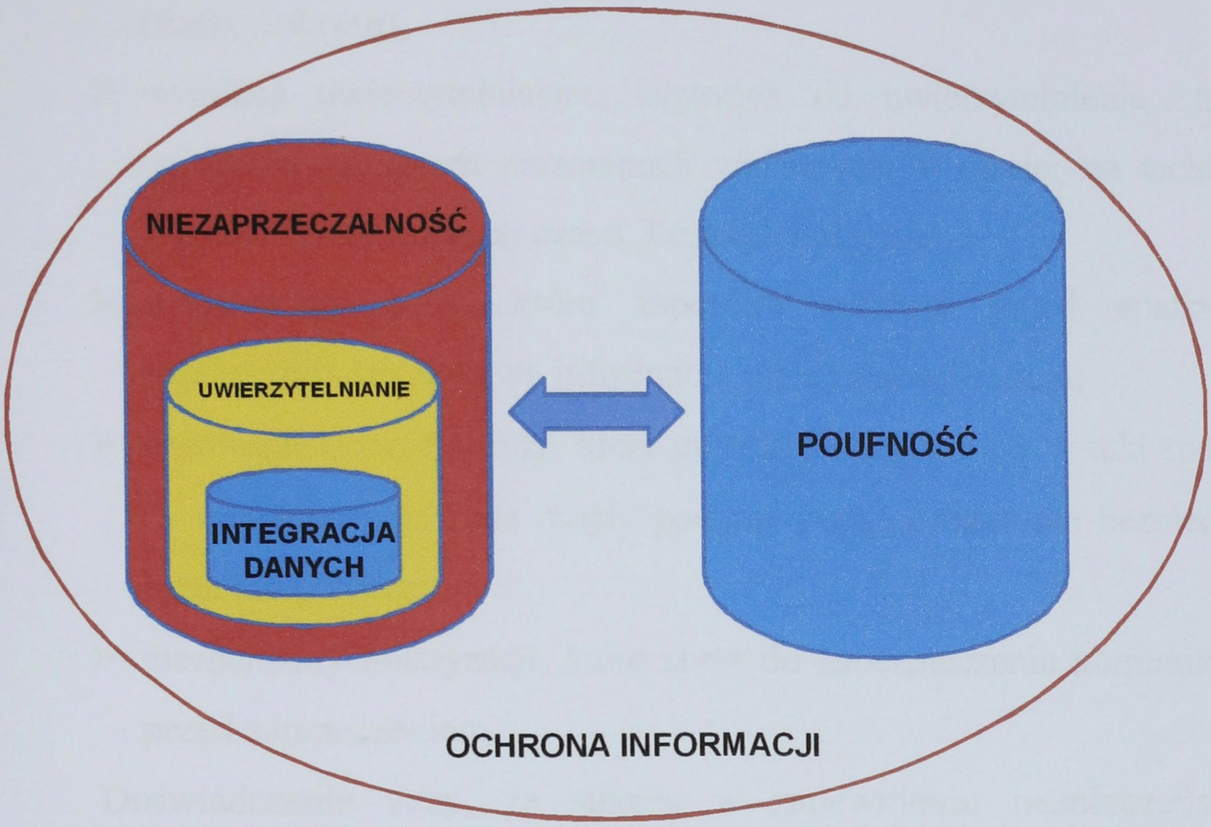
Poza tym, niezaprzeczalność to usługa o dwóch odmianach:

- niezaprzeczalność z wykazaniem odbiorcy - odbiorca nie jest w stanie wyprzeć się faktu uczestnictwa w sesji jak i jej treści;
- niezaprzeczalność z wykazaniem nadawcy - nadawca nie będzie w stanie wyprzeć się zarówno uczestnictwa jak i treści sesji.

Zakłada się, że w usłudze niezaprzeczalności obok nadawcy i odbiorcy może wystąpić trzecia strona tzw. „sędzia" rozstrzygający spór pomiędzy nadawcą i odbiorcą na podstawie informacji arbitrażowych pochodzących od nadawcy, odbiorcy, „zarządu bezpieczeństwa" (trzeciej strony).

Jednocześnie, poufność może być zapewniona niezależnie od integralności, uwierzytelnienia i niezaprzeczalności. Niezaprzeczalność zawsze wiąże się z uwierzytelnieniem, natomiast uwierzytelnienie z integralnością (rys. 2.1.).

W systemach informacyjnych obok podstawowych pięciu usług wprowadza się (ISO-10181-1) usługę związaną w dużym stopniu z przetwarzaniem danych, tzn. audyt i alarmy (security audit and alarms). Jest to zbiór metod umożliwiających wgląd do systemu i ocenę poprawności jego pracy z punktu widzenia bezpieczeństwa.



Rys. 2.1. Relacje w ochronie informacji

Opracowanie własne: na podstawie normy PN-EN ISO 19011

Wymienione usługi prowadzone mogą być poprzez stosowanie określonych mechanizmów, które na podstawie normy (ISO 7498-2) można scharakteryzować następująco:

- szyfrowanie zapewniające poufność informacji lub strumienia danych; wyróżnia się dwie klasy algorytmów szyfrowych: symetryczne (tj. z kluczem tajnym) i asymetryczne (tj. z kluczem publicznym);
- podpis cyfrowy o dwóch procedurach: podpisywanie i weryfikacja; w pierwszej stosuje się informację, która jest unikalną i poufną (prywatną) własnością podpisującego, w drugiej - informację publicznie dostępną,
- mechanizmy kontroli dostępu, używane w celu określenia i przestrzegania praw dostępu do zasobów;
- mechanizmy integralności danych, używane do zachowania integralności

danych; najczęściej korzysta się z kryptograficznych sum kontrolnych (funkcji skrótu);

- wymiana uwierzytelniająca, używana do uwierzytelnienia stron; opiera się na trzech parametrach zmiennych w czasie: na technice wyzwania, znacznikach czasu, liczbach kolejnych;
- wypełnianie ruchu, które zapewnia ochronę przed analizami ruchowymi - np. ukrywa informację o aktywności źródła;
- sterowanie doborem trasy, które umożliwia dobór trasy w taki sposób by transmitowane dane mogły podążać poprzez fizycznie bezpieczne łącza lub podsieci;
- mechanizmy notaryzacji, które służą do zabezpieczenia komunikacji przed zaprzeczeniem.

Doświadczenie uczy, że sukces w zapewnieniu bezpieczeństwa informacji w zarządzaniu bezpieczeństwem militarnym często zależy od następujących, krytycznych czynników:

a. polityki bezpieczeństwa informacji, celów i działań w zakresie bezpieczeństwa informacji, które odzwierciedlają cele;
b. podejścia oraz struktury służącej wdrażaniu, utrzymaniu, monitorowaniu i doskonaleniu bezpieczeństwa informacji, które jest zgodne z kulturą organizacji;
c. widocznego wsparcia i zaangażowania na wszystkich szczeblach kierowniczych;
d. właściwego zrozumienia wymagań bezpieczeństwa informacji, szacowania ryzyka i zarządzania ryzykiem;
e. skutecznego propagowania bezpieczeństwa informacji wśród kierownictwa, pracowników i innych podmiotów, w sposób umożliwiający osiągnięcie efektu uświadomienia;
f. rozpowszechniania zaleceń dotyczących bezpieczeństwa informacji wśród kadry zarządzającej, pracowników i innych podmiotów;

g. finansowania działań związanych z zarządzaniem bezpieczeństwem informacji;
h. zapewnienia odpowiedniej świadomości, kształcenia i szkoleń;
i. ustanowienia skutecznego procesu zarządzania incydentami związanymi z bezpieczeństwem informacji;
j. wdrożenia systemu pomiaru do oceny efektywności zarządzania bezpieczeństwem informacji oraz mechanizmów sprzężenia zwrotnego służących doskonaleniu tego systemu[54].

Literatura przedmiotu zaleca, aby działania w zakresie bezpieczeństwa były koordynowane przez reprezentantów różnych części bezpieczeństwa militarnego pełniących odpowiednie role i funkcje.

Zazwyczaj koordynacja bezpieczeństwa informacji w zarządzaniu bezpieczeństwem militarnym wymaga współdziałania kierownictwa, użytkowników, administratorów, projektantów aplikacji, audytorów i pracowników działu bezpieczeństwa oraz specjalistycznych umiejętności z takich dziedzin, jak ubezpieczenia, prawo, zarządzanie zasobami ludzkimi, informatyką lub ryzykiem. Zaleca się, aby te działania:

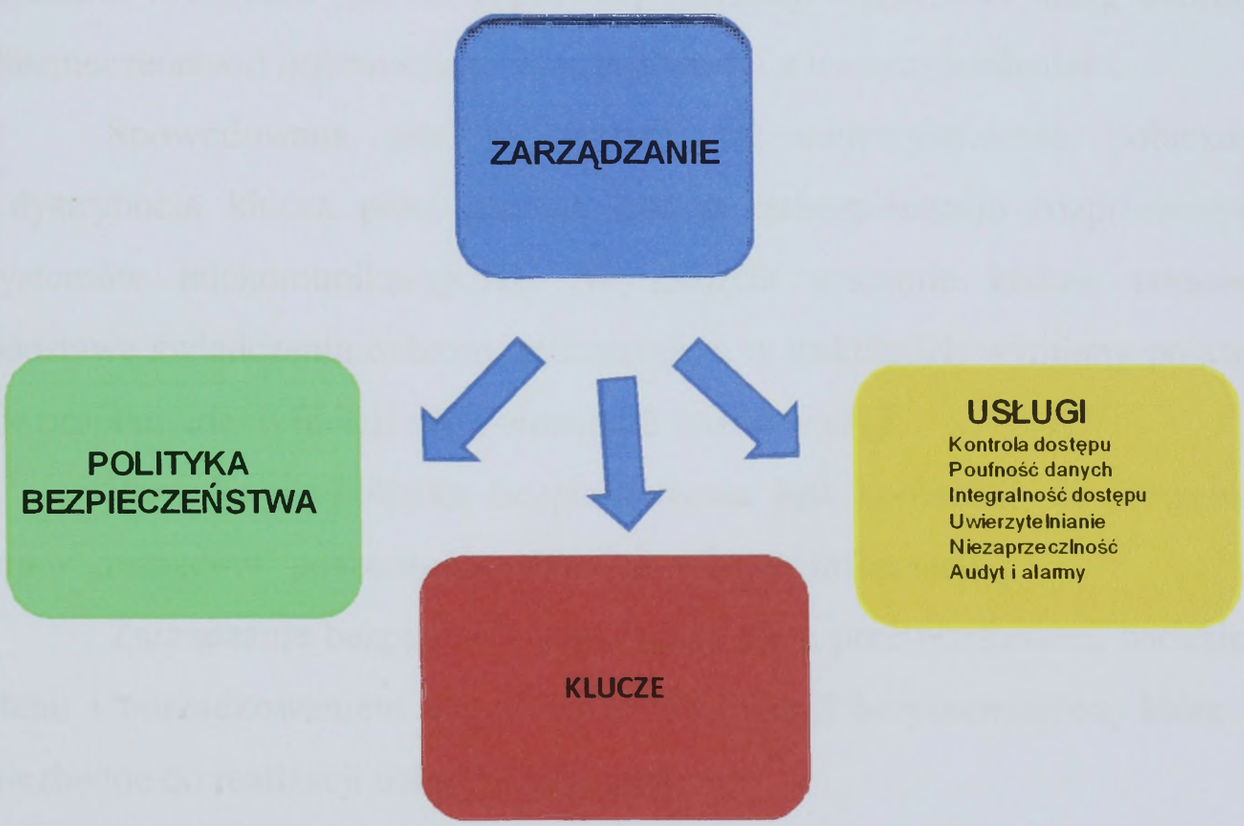
a. zapewniały, że zadania z zakresu bezpieczeństwa są realizowane zgodnie z polityką bezpieczeństwa informacji;
b. określały postępowanie z przypadkami niezgodności;
c. zatwierdzały metodykę i procesy związane z bezpieczeństwem informacji, np. klasyfikację informacji lub szacowanie ryzyka;
d. rozpoznawały znaczące zmiany zagrożeń i stopień narażenia informacji lub środków do przetwarzania informacji na zagrożenia;
e. szacowały adekwatność i koordynowały wdrożenie zabezpieczeń;
f. skutecznie promowały w organizacji kształcenie, szkolenia i uświadamianie w zakresie bezpieczeństwa informacji;

---

[54] Zob. PN-ISO/IEC 17799 Technika informatyczna. Technika bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, Warszawa 2007, s 20.

g. oceniały informacje uzyskane z monitorowania i przeglądu incydentów związanych z bezpieczeństwem informacji oraz zalecały odpowiednie działania w stosunku do zidentyfikowanych incydentów związanych z bezpieczeństwem informacji[55].

Po określeniu planu bezpieczeństwa należy zorganizować strukturę zarządzania bezpieczeństwem (rys. 2.2.), które wiąże się ze sterowaniem od strony zabezpieczeń komunikacją i przetwarzaniem danych poprzez wymianę informacji niezbędnych do przeprowadzenia tego procesu.



Rys. 2.2. Struktura zarządzania bezpieczeństwem

Źródło: opracowanie własne

Zgodnie z przedstawioną na rysunku 2.2. strukturą, ze względu na charakter zarządzanych obiektów wyróżnia się trzy obszary zarządzania:

---

[55] Tamże, s. 56.

- Zarządzanie usługami - tzn. zarządzanie:
  - ✓ kontrolą dostępu,
  - ✓ poufnością danych,
  - ✓ integralnością dostępu,
  - ✓ uwierzytelnieniem,
  - ✓ niezaprzeczalnością,
  - ✓ audytem i alarmami.
- Zarządzanie kluczami.
- Zarządzanie polityką bezpieczeństwa.

Klucz jest „parametrami - cechą szyfru" i dlatego zarządzanie kluczami niezbędne jest do poprawnej realizacji większości usług ochrony (bezpieczeństwa) informacji, a w szczególności z uwierzytelnieniem.

Spowodowane jest to faktem, iż uwierzytelnienie połączone z dystrybucją klucza pełni główną rolę w zabezpieczeniu rozproszonych systemów telekomunikacyjnych. W każdym systemie klucze stanowią podstawę świadczenia ochrony informacji, a w trakcie ich wymiany pojawia się problem identyfikacji stron biorących udział w sesji.

Zarządzanie polityką bezpieczeństwa jest konieczne do właściwej pracy „zarządów" poszczególnych usług ochrony informacji.

Zarządzanie bezpieczeństwem wiąże się z przetwarzaniem, badaniem stanu i porządkowaniem tak zwanych informacji bezpieczeństwa, które są niezbędne do realizacji usług bezpieczeństwa

Konkludując, należy stwierdzić, że istnieje kilka podejść i wiele rozwiązań tego problemu, mających wpływ na całą architekturę systemu ochrony. Żadne z nich nie jest rozwiązaniem idealnym, gdyż zwykle nie jesteśmy w stanie spełnić wszystkich wymagań, chociaż należy do tego dążyć.

Dlatego dla zapewnienia kompromisu pomiędzy kosztem zabezpieczeń zasobów informatycznych w bezpieczeństwie militarnym,

a wartością (ważnością) tych zasobów należy tworzyć i eksploatować systemy bezpieczeństwa uwzględniając następujące uwagi:

- Utrzymywać i systematycznie przeglądać log systemowy. W rejestrze tym zwracać uwagę na nietypowe próby logowania się do sieci.
- Od samego początku budować system z myślą o jej bezpieczeństwie. W szczególności - jeśli system ma łączność z Internetem - oznacza to dodanie serwera proxy i zapory firewall, oraz fizyczne odseparowanie sieci LAN od świata zewnętrznego. Celem zapory firewall jest uniemożliwienie wchodzenia z zewnątrz do sieci osobom nieuprawnionym, zaś celem serwera proxy - ukrycie wewnętrznych adresów IP w sieci (po to aby uniemożliwić włamania metodą fałszowania adresów IP).
- Zainstalować w systemie oprogramowanie antywirusowe. Idealnie powinno się mieć zainstalowany jeden pakiet antywirusowy na zaporze firewali, inny na serwerze, a jeszcze inny na poszczególnych stacjach roboczych. Ponadto powinno się ustalić żelazną regułę: żadna dyskietka z zewnątrz nie ma prawa być odczytana przed przeskanowaniem jej porządnym programem antywirusowym.
- Opracować, wdrożyć i egzekwować politykę haseł. Nowoczesne sieciowe systemy operacyjne potrafią wymusić na użytkownikach zmienianie hasła logowania nie rzadziej niż co ileś dni. Wykluczyć logowanie anonimowe.
- Poinstruować użytkowników i podległych administratorów, że haseł, identyfikatorów logowania ID i innych danych odnoszących się do bezpieczeństwa z zasady nie przekazuje się przez telefon.
- Wymusić tajność wszystkich haseł i ściśle przestrzegać tej strategii.
- Fizycznie zabezpieczyć dostęp do serwera i koncentratów. Dostęp

do konsoli serwera musi być zawsze obwarowany hasłem i wszystkie próby uzyskania dostępu do niego muszą być rejestrowane.

- Pamiętać o zwyczaju wylogowywania się po zakończeniu dnia pracy, także wtedy, gdy pozostawia się swój komputer bez nadzoru nawet tylko na kilka minut.

Chociaż będziemy przestrzegać powyższych spostrzeżeń to bezpieczeństwo informacji w zarządzaniu bezpieczeństwem militarnym będzie ciągle aktualnym procesem zmieniającym swoje struktury w miarę rozwoju systemów informatycznych.

Wnioski

Rosnące znaczenie informacji oraz stale rozbudowywane powiązanie sieciowe bezpieczeństwa militarnego rodzi nowe uzależnienia mające decydujące znaczenie dla zwycięstwa czy porażki, zwłaszcza w przypadku konfliktów zbrojnych. Strategiczne zarządzanie informacjami stało się elementarną częścią składową bezpieczeństwa militarnego.

Informacja jest żywotnie ważną częścią systemu zarządzania bezpieczeństwem militarnym. Żeby informacja mogła być użyteczna, musi być dokładna, terminowa, pełna i odpowiednia. Na zarządzanie informacją najlepiej patrzeć jako na część procesu kontroli. Systemy informacyjne zawierają pięć podstawowych składowych: urządzenie wprowadzające (wejściowe), procesor, urządzenie przechowujące informacje, urządzenie wyjściowe i system kontrolny. Choć mogą one występować w różnych formach, zarówno ręczne jak i skomputeryzowane systemy informacyjne obejmują wszystkie te składowe (zob. załącznik 1.).

Potrzeby bezpieczeństwa militarnego w zakresie zarządzania informacją są określane od strony organizacyjnej przez jej otoczenie

i wielkość, a od strony kierowniczej przez pole działania i szczebel w organizacji. Planowanie systemu informacyjnego musi uwzględnić każdy z tych czynników.

Podstawowymi rodzajami systemów informacyjnych w zarządzaniu bezpieczeństwem militarnym są systemy: przetwarzania danych transakcyjnych, podstawowych informacji kierowniczych, wspomagania decyzji oraz informacji najwyższego kierownictwa. Każdy z nich dostarcza pewnych typów informacji i ma szczególną wartość dla określonego typu odbiorców.

Zarządzanie systemami informacyjnymi obejmuje przede wszystkim decyzje o sposobie ich wprowadzania. Oczywiście, można tu wykorzystać szeroki zestaw konkretnych działań i kroków. Potem następuje integracja systemów. Wreszcie - użytkownicy powinni umieć posługiwać się systemem.

Systemy informatyczne oddziałują na zarządzanie bezpieczeństwem militarnym w rozmaity sposób. Podstawowe kierunki oddziaływań to wpływ na wyniki, na samą organizację i na zachowania jej członków. Decydenci powinni również mieć świadomość, że systemy informatyczne mają swoje ograniczenia, i nie wiązać z nimi nierealistycznych oczekiwań.

Najnowsze postępy w systemach informatycznych obejmują przełomy w telekomunikacji, wykorzystaniu sieci i systemów eksperckich. Każda z tych możliwości otwiera przed bezpieczeństwem militarnym obiecującą perspektywę bardziej skutecznego zarządzania informacją (zob. załącznik 2.).

Zarządzanie bezpieczeństwem informacyjnym w bezpieczeństwie militarnym jest nową dziedziną z pogranicza informatyki, prawa, organizacji i zarządzania, zajmująca się definiowaniem aspektów bezpieczeństwa dla instytucji i jej systemów teleinformatycznych, jego osiąganiem i utrzymywaniem (zob. załącznik 3.).

W niniejszym rozdziale wykazano, że informacja, zasoby informatyczne oraz zarządzanie informacjami, jako środek zarządzania, musi

stanowić integralną część wojskowo-politycznych percepcji i decyzji. Konieczne są do tego pewne formy organizacyjne i odpowiednia hierarchizacja procesów kierowniczych i decyzyjnych.

3. NARODOWE ASPEKTY W ZARZĄDZANIU BEZPIECZEŃSTWEM MILITARNYM

Jak wskazują wydarzenia dziejące się na świecie w ostatnich latach, a nawet miesiącach, wojsko coraz częściej angażowane jest w rozwiązywanie kryzysów i konfliktów, zwłaszcza gdy instrumenty polityczne i misje dyplomatyczne okazują się niewystarczające.

Podstawowe interesy narodowe Polski wynikają z koncepcji bezpieczeństwa państwa, uwzględniającej aspekty polityczno-militarne, ekonomiczne, społeczne i ekologiczne.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, określa, że nadrzędnym celem strategicznym RP jest zapewnienie korzystnych i bezpiecznych warunków realizacji interesów narodowych poprzez eliminację zewnętrznych i wewnętrznych zagrożeń, redukowanie ryzyka oraz odpowiednie oszacowanie podejmowanych wyzwań.

Jedną z zasadniczych przyczyn zmian w zakresie zadań Sił Zbrojnych, są nowe wyzwania[56] i zagrożenia[57]. Zagrożenia mogą pojawiać się w obszarach militarnych i niemilitarnych. Szczególną kategorią nowych zagrożeń są **działania terrorystyczne** wymuszające realizację szeregu przedsięwzięć, w których coraz częściej biorą udział komponenty wojsk lądowych.

Reakcją wojskową w powyższych sytuacjach, może być aktywne lecz z zasady nie gwałtowne zaangażowanie militarne występujące jako dopełnienie środków dyplomatycznych.

---

[56] „Wyzwanie" to działanie mające na celu skłonienie przeciwnika do podjęcia walki, Mały Słownik Języka Polskiego, PWN, Warszawa 1995, s. 1087.

[57] Leksykon Wiedzy Wojskowej MON, Warszawa 1979, s 510.

3.1. Główne założenia bezpieczeństwa militarnego w aspekcie narodowym

Przeciwdziałanie i rozwiązywanie sytuacji kryzysowych jest jednym z głównych zadań Sojuszu ujętym w nowej „Koncepcji Strategicznej", przyjętej podczas szczytu waszyngtońskiego. Przedmiotowy dokument przedstawia całe spektrum operacji reagowania kryzysowego mających na celu zapewnienie bezpieczeństwa państwom członkowskim NATO. Operacje tego typu obejmują różnorodne działania polityczne, cywilne i militarne prowadzone zgodnie z obowiązującym prawem międzynarodowym w celu zapobiegania wszelkiego typu konfliktom i ich przezwyciężania.[58]

W naszym, narodowym rozumieniu, bezpieczeństwo militarne dotyczy działań podejmowanych w razie pojawienia się zagrożeń w stosunku do państwa lub naszych sojuszników, czy też dla pokoju międzynarodowego. Pod tym pojęciem zrozumie się poczynania narodowe Sił Zbrojnych, jak i udział w wysiłkach międzynarodowych, prowadzonych w celu opanowywania kryzysu oraz zapewnienia osłony przed ich skutkami. Wreszcie są działania wojenne, które będą podejmowane w razie agresji na Polskę lub jej sojuszników. Przewidują one wykorzystanie całego lub części potencjału militarnego państwa, niezbędnego do przygotowania i przeprowadzenia operacji wojennych, mających doprowadzić do odparcia obcej napaści.

Bezpieczeństwo militarne Polski funkcjonuje w oparciu o szereg dokumentów normatywno – prawnych, w tym głównie: *Strategię Bezpieczeństwa Rzeczypospolitej Polskiej* i *Strategię Obronności Rzeczypospolitej Polskiej*.

Ponadto, zarówno Konstytucja RP z 2.04.1997 r. jak i cytowana ustawa określają misję Sił Zbrojnych RP, która polega na *obronie*

---

[58] Doktryna ...wyd. cyt., rozdział 6, pkt. 6054.

suwerenności i niepodległości Narodu Polskiego oraz jego bezpieczeństwa i pokoju.

Oznacza to, że rola Sił Zbrojnych ogranicza się do realizacji funkcji zewnętrznej, w warunkach zagrożenia militarnego i wojny. Dopiero nowelizacja ustawy w lipcu 1997 roku, podczas powodzi tysiąclecia, rozszerzyła zadania Sił Zbrojnych RP o możliwość udziału w zwalczaniu klęsk żywiołowych, nadzwyczajnych zagrożeń środowiska i likwidacji ich skutków.

W odniesieniu do możliwości udziału sił zbrojnych w zwalczaniu terroryzmu prawo międzynarodowe nie reguluje jednoznacznie, przy pomocy jakich organów i instytucji wewnętrznych państwa powinny rozwiązywać problemy związane z przeciwdziałaniem i zwalczaniem zagrożeń terrorystycznych.

Polska, jak każde państwo demokratyczne, powinna przestrzegać prawa międzynarodowego, dotyczy to również zwalczania terroryzmu. W Polskim prawodawstwie narodowym instrumenty prawne służące zapobieganiu i zwalczaniu terroryzmu należą do sfery prawa karnego oraz do sfery prawa administracyjnego[59].

W tekście *Konstytucji Rzeczypospolitej Polskiej* brak bezpośredniego zapisu o zagrożeniach terrorystycznych i przeciwdziałaniu takim zagrożeniom, jednakże treść niektórych artykułów może stanowić podstawę do działań skierowanych przeciwko terroryzmowi. Szczególne znaczenie w tej kwestii mają: art.5, art. 228 i art. 230 Konstytucji.

Zgodnie z art. 5 Konstytucji „Rzeczypospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego".

System Kierowania Reagowaniem Kryzysowym resortu Obrony Narodowej funkcjonuje w oparciu o dokumenty normatywno - prawne opracowane na szczeblu Ministerstwa Obrony Narodowej oraz dokumenty wykonawcze opracowane w Sztabie Generalnym WP. Najważniejsze z nich to: *Decyzja nr Z-7/MON Ministra Obrony Narodowej w sprawie Systemu Kierowania Reagowaniem Kryzysowym Ministerstwa Obrony Narodowej* z dnia 16 października 2000 r. (znowelizowana 16 września 2002 r.), *Decyzja nr Z-3/MON Ministra Obrony Narodowej w sprawie wprowadzenia Regulaminu Sztabu Kryzysowego MON* z dnia 25 stycznia 2002 r. oraz *Rozkaz Nr Pf - 28/DOW/P3 Szefa Sztabu Generalnego WP w sprawie wdrożenia Systemu Kierowania Reagowaniem Kryzysowym Siłach Zbrojnych RP* z dnia 31 stycznia 2001 r. Dokumenty te mają zastosowanie praktyczne i są niezbędne dla budowy i funkcjonowania resortowego systemu reagowania kryzysowego. Na ich podstawie zorganizowano System Kierowania Reagowaniem Kryzysowym resortu Obrony Narodowej oraz opracowano inne dokumenty regulujące problematykę reagowania kryzysowego na niższych szczeblach dowodzenia. Dokumenty te są na bieżąco nowelizowane, stosownie do pojawiających się potrzeb.

Na użytek systemu reagowania kryzysowego resortu ON, opracowano „*Plan użycia oddziałów i pododdziałów SZ RP w przypadku wystąpienia sytuacji kryzysowych*", który zawiera informacje pozwalające na efektywne przygotowanie i utrzymanie w stałej gotowości do użycia wydzielone siły i środki w przypadku wystąpienia sytuacji kryzysowych o charakterze pozamilitarnym - z zagrożeniami terrorystycznymi włącznie. Ponadto do „*Planu...*" załączono „*Rejestr zagrożeń oraz procedury działań podejmowanych przez Siły Zbrojne RP w przypadku wystąpienia sytuacji kryzysowych*" jako materiał pozwalający na sklasyfikowanie zagrożeń,

---

[59] Akty prawne z zakresu prawa karnego obejmują przepisy *Kodeksu karnego*, a także innych ustaw. Natomiast sfera prawa administracyjnego to przede wszystkim ustawy regulujące ustrój, kompetencje

w których żołnierze mogą nieść pomoc oraz uczestniczyć w likwidacji skutków powstałych w związku z zaistniałą sytuacją kryzysową.

Różnice pomiędzy prowadzeniem operacji z Art. 5 i spoza Art. 5 polegają m. in. na złożoności sytuacji, szerokim oddziaływaniu opinii publicznej, trudności identyfikacji przeciwnika, braku jednolitej linii frontu oraz trudności w przewidywaniu rozwoju sytuacji. Podczas prowadzenia operacji spoza Art. 5 wielokrotnie staniemy przed problemem trafnego określenia zagrożeń i sposobu działania przeciwnika. Operacje te różnić będzie również określenie punktu ciężkości. O ile dla operacji z Art. 5 określa się jeden punkt ciężkości na określonym szczeblu dowodzenia, o tyle w operacjach spoza Art. 5 konieczne będzie określenie kilku punktów ciężkości i co więcej – istotą działania nie będzie ich zniszczenie ale ich ochrona. Ponadto udział sił NATO i sił spoza Sojuszu wspólnie z organizacjami międzynarodowymi wymagał będzie ścisłej koordynacji ich działań zarówno na etapie planowania, jak i podczas realizacji zadań.[60]

W operacjach reagowania kryzysowego, działania bojowe prowadzone są w celu rozbicia przeciwnika lub obniżenia jego potencjału bojowego oraz przeciwdziałania wszelkiego typu zagrożeniom przy użyciu posiadanych środków militarnych.[61]

Decyzja o użyciu siły jest jedną z trudniejszych, jaką muszą podjąć dowódcy. Złe użycie grozi naruszeniem równowagi i zaostrzeniem kryzysu w rejonie przygranicznym.

Staje się wielce prawdopodobne, zwłaszcza obserwując różnorodność nieprzewidzianych i często niekonwencjonalnych poczynań zwaśnionych stron, że celem użycia jednostek wojsk lądowych może być wsparcie lub zastąpienie sił pokojowych ONZ (innych sił) i stabilizacja sytuacji kryzysowej, lub też, w wypadku dalszego niepomyślnego rozwoju sytuacji

---

i zadania służb, powołanych między innymi do zapobiegania terroryzmowi i jego zwalczania.

[60] Doktryna ...wyd. cyt., rozdział 6, pkt. 6058.

(przejścia w fazę konfliktu zbrojnego), stworzenie warunków do wprowadzenia niezbędnych sił w obszar objęty kryzysem.

Podstawa prawna umożliwiająca użycie sił NATO w celu wsparcia lub zastąpienia innych sił wynika z ogłoszonej w 1992 r. *„woli NATO do wspierania, zgodnie ze swymi własnymi procedurami, operacji pokojowych prowadzonych pod auspicjami ONZ, (UN – United Nations) i Konferencji Bezpieczeństwa i Współpracy w Europie (obecnie Organizacji Bezpieczeństwa i Współpracy w Europie)"*[62].

W Doktrynie Narodowej Operacji Połączonych zostało zapisane, iż: *„Wojska lądowe, w określonych uwarunkowaniach operacyjnych, mogą być zaangażowane do prowadzenie działań spoza Art. 5 – działania w ramach reagowania kryzysowego. W przypadku prowadzenia tego typu działań, wojska lądowe używają tych samych jednostek i na tych samych zasadach, co podczas prowadzenia działań w ramach konfliktu i wojny."*[63]

Wiele faktów przemawia za tym, że skuteczne może okazać się łączenie wysiłku działań wojsk operacyjnych, obrony terytorialnej, pozamilitarnych ogniw obronnych oraz całego społeczeństwa w jeden spójny system, czyniący z przeciwdziałania agresji zadanie całego narodu.

Jak pisze, W. Lidwa: *Skuteczność działań obrony powszechnej będzie wynikiem zespolenia profesjonalizmu wojsk operacyjnych wyposażonych w nowoczesne środki walki, z działaniem formacji wojsk obrony terytorialnej broniącymi wcześniej wyznaczonych rejonów odpowiedzialności, oraz z powszechnością oporu społeczeństwa wyrażającą się w masowych działaniach nieregularnych.*[64]

---

[61] Tamże, rozdział 6, pkt. 6053.
[62] Bi - MNC, Directive, NATO Doctrine for peace Support Operations, Supreme Allied Commander, Europe, SHAPE B - X7070, Belgium, 11.12.1995, s. 5.
[63] Doktryna ..., wyd. cyt., rozdział 6, pkt 6006.
[64] W. Lidwa, Współdziałanie wojsk operacyjnych z siłami obrony terytorialnej w działaniach na obszarze kraju, rozprawa habilitacyjna, AON, Warszawa 1999, s. 33.

W sytuacji bezpośredniego zagrożenia militarnego, szereg istotnych zadań przypisuje się jednostkom „obrony terytorialnej", w tym między innymi:

- prowadzenie rozpoznania terytorialnego;
- ochrona i obrona ważnych obiektów w rejonie zagrożenia;
- ewentualne zabezpieczenie przyjęcia i pobytu wojsk NATO;
- uczestniczenie w zabezpieczeniu mobilizacyjnego i operacyjnego rozwinięcia wojsk operacyjnych;
- przeciwdziałanie dywersji;
- prowadzenie rozbudowy inżynieryjnej terenu w ramach operacyjnego przygotowania obszaru kraju[65].

Zespolenie działań wojsk operacyjnych z siłami obrony terytorialnej oraz działań regularnych i nieregularnych na obszarach zajmowanych lub zajętych przez przeciwnika[66], uwiarygodnia strategię odstraszania sugerując że agresja spowoduje uwikłanie się agresora w długotrwałą, nie rokującą nadziei na szybkie zakończenie kampanii wojennej, której koszty (straty) przewyższać mogą przewidywane korzyści.[67]

W militarnej obronie kraju wojska lądowe, jako jeden z rodzajów sił zbrojnych, przeznaczone są do prowadzenia działań na lądowym teatrze działań wojennych i zdolne do utrzymania i zajęcia terenu[68]. Stanowią one trzon sił biorących udział w połączonej operacji obronnej, bez których udziału nie można osiągnąć założonych celów operacji.

---

[65] Por.: A. Tomaszewski, Wojska lądowe w systemie obronnym kraju, Warszawa 1997, s. 26; R. Jakubczak, Rola, funkcje, zadania ..., Zeszyty Naukowe AON, 1998, Nr 1(30)A, s. 43; R. Jakubczak, Organizacja i wykorzystanie wojsk obrony terytorialnej, Warszawa 1996, s. 48.

[66] J. Marczak, J. Pawłowski, O obronie militarnej Polski przełomu XX i XXI wieku, Warszawa 1995, s. 219.

[67] W. Lidwa, Współdziałanie ...wyd. cyt., s. 34.

[68] Słownik terminów z zakresu bezpieczeństwa narodowego, Warszawa 1996, s. 102.

3.2. Wybrane warianty reakcji potencjałem militarnym na obszarze kraju

Szukając rozstrzygnięcia istoty działania „Aby wyjaśnić komuś, w jaki sposób coś się robi, wystarczy odpowiedzieć na pytanie, jak się to robi"[69] – wyjaśnia T. Kotarbiński. Wykonując postawione zadania, wojska będą osiągały określone cele w konkretnych warunkach. Dlatego też ich działania będą wynikały głównie z treści zadań charakterystycznych dla okresu kryzysu i w sytuacji bezpośredniego zagrożenia militarnego kraju.

Jeśli założyć, iż podczas wykonywania zadań mogą zaistnieć różne, trudne do przewidzenia sytuacje i do działań w takich, zaskakujących okolicznościach trzeba być przygotowanym np. przez projektowanie (symulacje) wielowariantowych reakcji.

M. Huzarski podkreśla, że: *„Wariantowanie użycia pododdziałów wiąże się z rozwiązywaniem problemów o charakterze taktycznym, w wyniku których powstają koncepcje działania przetwarzane na zamiary i decyzje dowódców"*[70].

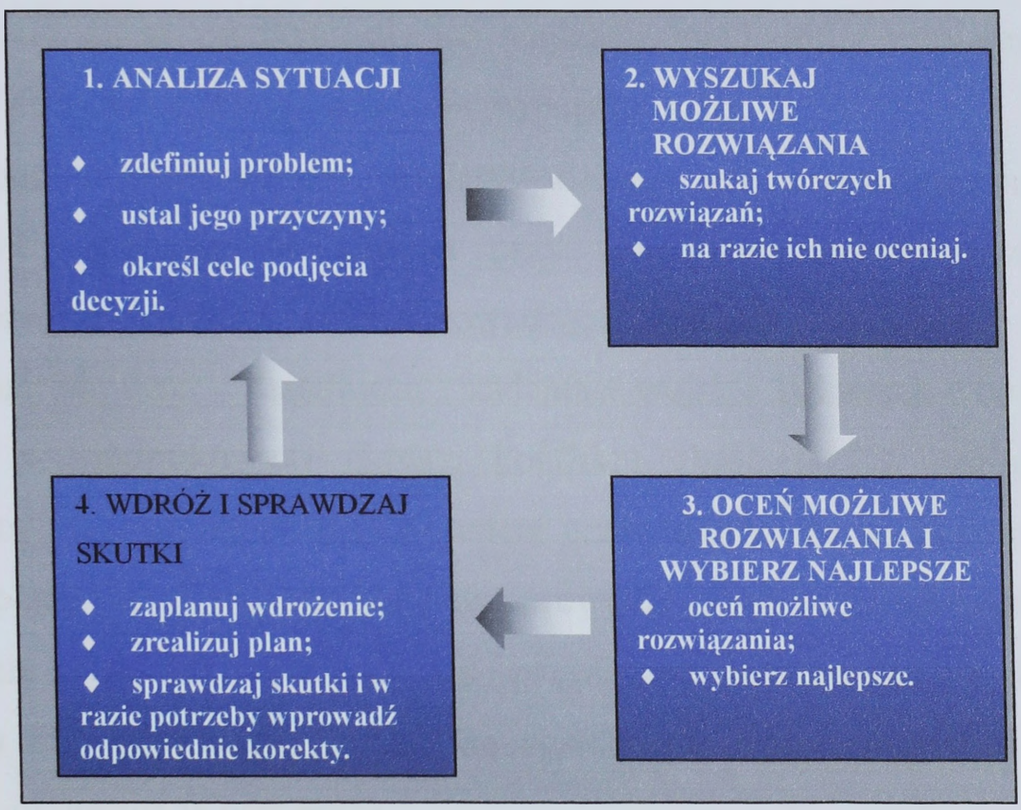
Stąd też, warianty powinny umożliwić jak najlepsze wykorzystanie potencjału intelektualnego i materialnego wojsk, zgodnie z przyjmowaną w teorii organizacji i zarządzania zasadą optymalności, której treść sprowadza się do twierdzenia, że w procesie podejmowania decyzji poszukuje się najlepszego z możliwych w danej sytuacji sposobu działania[71]. Wymaga to jednak rozważenia różnych możliwości, z których wiele wiąże się z przyszłymi wydarzeniami, często trudnymi do przewidzenia. Ocenia się je według skali rozciągającej się od pewności (pełnej możliwości przewidywania), poprzez ryzyko, do niepewności (minimalnej możliwości przewidywania)[72].

---

[69] T. Kotarbiński, Traktat o dobrej robocie, Wrocław – Warszawa – Kraków – Gdynia, 1973, s. 56.
[70] M. Huzarski, Zagadnienia ..., s. 56.
[71] Encyklopedia Organizacji i Zarządzania, Warszawa 1981, s. 614.
[72] Por. J. A. F. Stoner, C. Wankel, Kierowanie ..., s. 246-247.

W celu rozważenia możliwości i określenia optymalnego poziomu ryzyka w poszczególnych wariantach, teoria organizacji i zarządzania proponuje racjonalny model podejmowania decyzji (rys. 3.1.). Obejmuje on cztery etapy[73]:

1. Analiza sytuacji.
2. Wyszukanie możliwych rozwiązań.
3. Ocena możliwych rozwiązań i wybór najlepszego z nich.
4. Wdrażanie decyzji i śledzenie jej skutków.



Rys. 3.1. Racjonalny model podejmowania decyzji

Źródło: J.A.F. Stoner, C. Wankel, Kierowanie, Warszawa 1997, s. 249.

W aspekcie wojskowym, punktem wyjściowym wskazanego modelu jest zazwyczaj otrzymanie zadania od przełożonego, w którym określa on podwładnemu cel jaki powinien osiągnąć. Analiza sytuacji powinna zaś stworzyć warunki do sprecyzowania jak ów cel ma być osiągnięty. W trakcie jej prowadzenia należy przeanalizować zadanie oraz ocenić warunki jego

[73] Tamże, s. 249-259.

wykonania, tj. przeciwnika, wojska własne, otoczenie (warunki terenowe, atmosferyczne, itp.) oraz inne czynniki, które należy wziąć pod uwagę (np. czas).

Wyszukiwanie możliwych rozwiązań powinno bazować na założeniu, że jeżeli rozwiązanie umożliwia osiągnięcie celów organizacji, to oznacza, że jest skuteczne.[74]

W etapie oceny możliwych rozwiązań i wyboru najlepszego z nich należy dążyć do porównania wariantów, określenia wad i zalet każdego z nich w odniesieniu do: sił niezbędnych dla ich realizacji, zgodności z zamiarem przełożonego, prawdopodobnego działania przeciwnika, itp.[75].

Kryterium wyznaczającym warianty działań jest prakseologiczna reguła przygotowania się do działań przy najbardziej niekorzystnym wariancie rozwoju sytuacji[76]. Przeprowadzone badania wykazały, iż w układzie narodowym, zasadnicze zadania wojsk lądowych będą wykonywane w początkowym okresie konfliktu zbrojnego, w ramach strategicznej operacji obronnej. Należy zatem przewidywać, że jej pierwsza faza będzie połączoną operacją opóźniającą, prowadzoną siłami narodowymi, z możliwością wsparcia tych działań przez siły powietrzne państw sojuszniczych pod warunkiem jednak, że agresor nie będzie dysponował zdecydowaną przewagą w powietrzu[77].

Stąd też w niniejszym rozdziale zostały rozpatrzone warianty wykonania następujących zadań:

- *Działania osłonowe i opóźniające;*
- *Działania blokujące;*
- *Wsparcie działań antyterrorystycznych.*

---

[74] Tamże, s. 250.

[75] J. Kręcikij, Przygotowanie działań taktycznych w NATO, (Na przykładzie procedur Wojsk Lądowych Sił Zbrojnych USA), Warszawa 1996, 16.

[76] „Każdą swoją strategię oceniaj wedle najgorszej ewentualności jaka może się zdarzyć gdy ją zastosujesz". T. Kotarbiński, Arcydzieło praktyczności, Warszawa 1972, s. 23.

[77] Por. A. Tomaszewski i in., Wojska lądowe w systemie obronnym kraju pk. „Armia", Warszawa 1998, s. 53.

Z przeprowadzonych wcześniej ocen wynika, że konflikt przygraniczny o ograniczonym zasięgu jest wariantem o znacznym prawdopodobieństwie zaistnienia. Rozpocząć się może niespodziewanym uderzeniem przeciwnika, z zamiarem opanowania określonego terytorium. W wypadku zaistnienia takiego rozwoju sytuacji, siły narodowe będą dążyć, wspólnie z siłami OT i układem pozamilitarnym do powstrzymywania i opóźniania podejścia przeciwnika. Ważnym zagadnieniem wymagającym szczegółowego rozpatrzenia jest czas niezbędny na przygotowanie działań. Ponieważ w literaturze przedmiotu podaje się różne wartości liczbowe należy przypuszczać, że jest to problem nadal otwarty.

Jeśli założyć, że jednym z warunków powodzenia działań jest uzyskanie zaskoczenia przeciwnika, to planując użycie zgrupowań taktycznych, należy brać pod uwagę możliwość wykonywania przez niego zadań w nocy i w trudnych warunkach pogodowych. Warunki nocne zmniejszają aktywności skuteczność działań lotnictwa oraz zmniejszają lub wykluczają wykorzystanie wielu środków OPL, a to oznacza, iż znacznie zwiększają się szanse sił, którym prawdopodobnie przyjdzie się zmierzyć z dużo większym potencjałem przeciwnika. Ponadto, przy takim założeniu spełniona zostanie prakseologiczna reguła przygotowania się do działań przy najbardziej niekorzystnym wariancie rozwoju sytuacji.

3.2.1. Warianty działań osłonowych

Ochrona granicy państwowej pozostaje jedną z podstawowych funkcji państwa. Jej nienaruszalność jest zasadniczym czynnikiem zapewniającym byt narodu i suwerenność państwa. Powszechnie uznaje się, że *„dobrze i skutecznie strzeżona granica jest odbierana (przez społeczeństwo) jako*

świadectwo siły i sprawności państwa, jako wyraz bezpieczeństwa jego obywateli" [78].

Z drugiej zaś strony ochrona granicy jest dzisiaj jednym z instrumentów regulacji stosunków społeczno-gospodarczych z bliższym lub dalszym otoczeniem państwa.

Dlatego też ochrona granicy państwowej pojmowana jest dziś wieloaspektowo, jako *„zespół administracyjno-politycznych, celnych i sanitarnych oraz militarnych przedsięwzięć o różnym zakresie rygorów, podejmowanych przez każde suwerenne państwo w celu niedopuszczenia do nielegalnego przekraczania granicy państwowej i przewożenia bez zezwolenia określonych towarów (...), zapobiegania przenikaniu przez granicę chorób zakaźnych*" [79].

Jak twierdzi B. Balcerowicz, państwo graniczne – to nie państwo frontowe lub nie koniecznie frontowe. Z obecnego położenia Polski powinna wynikać rola nie tyle swoistego „bufora", co „pomostu" spełniającego niezwykle ważną rolę w stosunkach z sąsiadami. Determinantami działalności w nowym położeniu są: konieczność podjęcia większych wysiłków w obronie zbiorowej sojuszu, w reagowaniu kryzysowym, w prewencji, a także w budowie partnerskich stosunków z sąsiadami [80].

Istotą osłony operacyjnej granicy państwa są uzgodnione i zorganizowane działania rozpoznawcze, graniczne, pogotowie i ewentualne działania obronne Straży Granicznej, sił OT i wydzielonych jednostek wojsk operacyjnych oraz przedsięwzięcia administracyjne (rygory) realizowane przez współdziałające ogniwa niemilitarne, ukierunkowane na wykrycie symptomów bezpośredniej groźby wybuchu konfliktu zbrojnego, manifestowanie suwerenności państwowej i odparcie ewentualnej agresji [81].

---

[78] S. Ziółkowski, W ochronie granicy państwowej, „Polska Zbrojna" z 12.06.1995 r.
[79] Leksykon wiedzy wojskowej, MON, Warszawa 1979, s. 250.
[80] B. Balcerowicz, Sojusz a obrona narodowa, Bellona, Warszawa 1999, s. 141.
[81] Materiały z konferencji nt. Wykorzystanie sił Obrony Terytorialnej w osłonie granicy państwowej, Zamość 1999, s. 3.

Z reguły celem osłony podczas kryzysu militarnego będzie zapewnienie dogodnych warunków dla przeprowadzenia mobilizacji i koncentracji oraz zorganizowanego wprowadzenia zasadniczych sił do bitwy obronnej lub też ochrona skrzydeł i tyłów zgrupowania odpierającego agresję od strony granicy.

Jedną z cech osłony jest wyczekiwanie na działania przeciwnika i przeciwdziałanie im (reagowanie).

Osłona granicy w czasie kryzysu jest połączeniem:

- działań operacyjno-rozpoznawczych (tzw. wywiadu płytkiego) Straży Granicznej;
- ochrony granicy przez Straż Graniczną;
- działań osłonowych jednostek Obrony Terytorialnej;
- działań jednostek administracji państwowej;
- działań innych jednostek przewidzianych do osłony granicy, np. Policji Państwowej.

W ramach osłony w okresie kryzysu mogą być wykonywane następujące zadania:

- zapobieganie przenikaniu na obszar kraju agentury i GDR przeciwnika oraz próbom przemytu broni i środków dywersyjnych;
- rozpoznawanie symptomów bezpośredniej groźby wybuchu konfliktu zbrojnego i uprzedzenie o możliwości wtargnięcia zgrupowań uderzeniowych przeciwnika (agresji);
- rozbudowa wzdłuż granicy państwowej i w głębi pasa przesłaniania - systemu pozycji, rejonów i punktów oporu oraz zapór i przygotowanie niszczeń.

Realizując osłonę, Straż Graniczna ochrania granicę państwa prowadząc działania graniczne obejmujące działania: rozpoznawcze, pościgowe, zaporowe, likwidujące stan zagrożenia siłami odwodów.

Ważna rola w zakresie działań osłonowych przypada wojskom obrony terytorialnej, które jako część sił zbrojnych powinny stwarzać warunki do efektywnego wspierania, zabezpieczenia i uzupełniania działań prowadzonych przez Straż Graniczną w rejonach gdzie występują zagrożenia, a jednocześnie osłaniać przygotowania obronne zasadniczych sił[82].

Rola OT może polegać na uszczelnianiu granicy w celu niedopuszczenia do nielegalnego przekraczania granicy przez grupy terrorystyczne i przestępcze, a także uchodźców.

W razie eskalacji terroryzmu i zorganizowanej przestępczości mającej swoje podłoże w konfliktach lokalnych w pobliżu granicy Polski, wojska obrony terytorialnej mogą być wyznaczone do izolacji pewnych obszarów kraju w celu niedopuszczenia do rozprzestrzeniania się tych zagrożeń.

Ciekawe wnioski wynikają z wielu ćwiczeń i treningów sztabowych prowadzonych w ostatnich latach w naszych siłach zbrojnych. Dla przykładu, w dniach od 4 do 14 2002 roku w Sztabie Generalnym WP, został przeprowadzony dwuszczeblowy trening sztabowy pk. CZERWIEC, na temat: *Rozwinięcie operacyjne elementów Wojennego Systemu Dowodzenia (WSYD) w ramach osiągania wyższych stanów gotowości bojowej*. Celami szkoleniowymi treningu było między innymi sprawdzenie zasadności przyjętych rozwiązań strukturalno-funkcjonalnych Połączonego Dowództwa Operacyjnego. Powyższy cel został przyjęty z uwagi na zmiany strukturalne zachodzące w SG WP, oraz z uwagi na podział kompetencyjnego zakresu zadań i funkcji wykonawczych nowoutworzonych organów dowodzenia według nowej koncepcji Wojennego Systemu Dowodzenia, zakładający między innymi przejęcie dowodzenia nad wydzielonymi siłami przez Połączone Dowództwo Operacyjne.

---

[82] J. Marczak, R. Jakubczak, K. Gąsiorek, Obrona Terytorialna w obronie powszechnej RP, AON, Warszawa 1998, s. 49.

Na potrzeby treningu skonfigurowano aplikacyjne państwa umiejscowione na kontynencie tj. Wislandię i Dragoland pozostające w stosunku do siebie w historycznie zadawnionym konflikcie. Jako czynnik równowagi polityczno-wojskowej utworzono na Kontynencie „Sojusz Niebieskich", którego członkiem jest Wislandia, Lalandia, Turlandia, Urlandia. Jako państwa neutralne przyjęto Tabor i Witlandię.

W treningu założono ograniczonego użycia sił zbrojnych zarówno przez przeciwnika, jak i sił własnych. Założono ponadto wyrażenie zgody przez Sojusz Niebieskich do organizacji działań przez narodowe dowództwo Wislandii we własnym zakresie stosownie do skali konfliktu.

Niepokojący wzrost napięcia, narastający w stosunkach pomiędzy Dragolandem, a Wislandią postrzegany był jako kryzys, który mógł przeistoczyć się w konflikt zbrojny.

O możliwości podjęcia decyzji siłowego rozwiązania przez Dragoland zaistniałego kryzysu świadczy zakres przedsięwzięć szkoleniowych, intensywność szkoleń mobilizacyjnych i sprawdzianów z gotowości bojowej i ćwiczeń.

Przeciwnik dążąc do osiągnięcia zakładanych celów poprzez uprzedzające uderzenia, dążył do opanowania spornego obszaru w zachodniej części kraju. Pozbawienia możliwości obrony siły Niebieskich i w ciągu 4-6 dób opanować obszar na zach. od linii: Bolesławiec, Głogów, Kościan, Jarocin. Następnie w ciągu 10 -12 dni działań wojennych opanować obszar na zach. od linii: Konin, Sieradz, Wieluń.Po zrealizowaniu celu operacji przejść do obrony opanowanej rubieży lub stworzyć warunki do rozwijania operacji zaczepnej w głąb Wislandii.

Przeciwnik dokonał pełnego mobilizacyjnego rozwinięcia sił reagowania, przeprowadził rozpoznanie wzdłuż wsch. i płn. granicy z Wislandią, zintensyfikował szkolenie oraz ćwiczenia dowództw, sztabów i wojsk.

W związku z eskalacją napięcia, Wislandia podjęła działania przewidziane planem stosownie do rozwoju sytuacji kryzysowej, których celem było podwyższenie zdolności obronnych państwa. W tym celu zintensyfikowano proces szkolenia dowództw sztabów i wojsk skupiając wysiłek szkoleniowy na przygotowaniu sił zbrojnych do prowadzenia operacji obronnej.

Dla realizacji zakładanych celów obrony dowódca wojsk lądowych Wislandii zdecydował przejść dwoma związkami operacyjnymi do Strategicznej Operacji Obronnej na rubieży: Tczew, Grudziądz, Toruń, Września, Poznań, Zbąszynek, Bolesławiec, Duży Las.

W wypadku zdecydowanej przewagi przeciwnika, działaniami manewrowymi na kolejnych rubieżach obronnych dążyć do załamania jego natarcia przed linią: Konin, Jarocin, Rawicz, Legnica, stwarzając warunki do wykonania przeciwuderzenia z planowanej rubieży przez siły Sojuszu Niebieskich (zał. 4.).

W tym celu organy władzy państwowej Wislandii przystąpiły do realizacji przedsięwzięć mających na celu podwyższenie gotowości obronnej państwa, realizując fazę ostrzegania i aktywacji, w tym rozwinięto krajowy system kierowania reagowaniem kryzysowym. Wprowadzono podwyższoną gotowość bojową w 2 KZ. Rozporządzeniem Prezydenta wprowadzono częściową mobilizację SZ.

Opracowano trzy warianty prowadzenia działań osłonowych (por. zał. 4-6.) według następujących etapów[83]:

I - ostrzeganie i aktywacja;

II - rozwinięcie sił;

III - osłona i działania opóźniające;

---

[83] Warianty działania Sił Zbrojnych Wislandii w osłonie strategicznej, informacja na temat treningu sztabowego pk. CZERWIEC, Generalny Zarząd Operacyjny SG, Zespół Planowania Operacyjnego.

IV - wycofanie sił.

Zasadnicze różnice pomiędzy wariantami działania dotyczyły głównie rozmieszczenia lądowego komponentu sił osłony, głębokości ich ugrupowania oraz rejonu kluczowego obrony (por. zał. 4-6.).W etapie oceny proponowanych rozwiązań, dokonano porównania wariantów działania przyjmując następujące kryteria: uwarunkowania polityczno - militarne, wielkość zaangażowanych sił, koncentracja wysiłku, możliwość manewru, ryzyko nie osiągnięcia celu, płynność przejścia do operacji obronnej, ochrona wojsk, zabezpieczenie logistyczne, relacje dowodzenia. Wyniki porównania wariantów działania przedstawia rys. 3.2.

Rys. 3.2. Porównanie wariantów działania metodą kryteriów

Źródło: Warianty działania Sił Zbrojnych Wislandii w osłonie strategicznej, informacja na temat treningu sztabowego pk. CZERWIEC, Generalny Zarząd Operacyjny SG, Zespół Planowania Operacyjnego.

Powyższe zestawienie porównawcze wskazują na wariant trzeci jako ten, który był rekomendowany dowódcy i w efekcie końcowym stał się bazą do podjęcia decyzji. Do jego głównych atutów zaliczono między innymi niskie prawdopodobieństwo niewykonania zadania (realność wariantu). Ponadto powyższy wariant zapewniał uzyskanie odpowiedniego potencjału w wymaganym miejscu i czasie oraz dawał niezbędną swobodę manewru wojskom operacyjnym.

W dalszej części oceny zaproponowano również porównanie wariantów metodą wad i zalet (tab. 3.1.). Również ta metoda wskazała na wariant trzeci. W zaletach podkreślano ekonomię sił oraz możliwość reagowania na zmiany sytuacji operacyjno-taktycznej.

Tabela 3.1.

Porównanie wariantów działania (metoda wad i zalet)

	WARIANT I	WARIANT II	WARIANT III
ZALETY	Absorbowanie znacznych sił przeciwnika na całej długości granic. W miarę równomierne zaangażowanie sił 1 i 2 KZ. Szczelność granicy z Dragolandem.	Skupienie wysiłku na kierunkach prawdopodobnych głównych uderzeń przeciwnika- ekonomia sił. Możliwość powstrzymywania przeciwnika w czasie umożliwiającym manewr pozostałymi siłami.	Głębokie ugrupowanie bojowe. Możliwość reagowania na zagrożonych kierunkach. Łatwe przejście z osłony strategicznej do operacji obronnej. Skupienie wysiłku na kierunkach prawdopodobnych głównych uderzeń przeciwnika- ekonomia sił.
WADY	Nie uwzględnia prawdopodobnego głównego kierunku uderzenia przeciwnika. Ograniczone możliwości wykonania manewru. Płytkie ugrupowanie bojowe. Brak odwodów. Utrudniona koordynacja współdziałania (zmiana podporządkowania sił).	Płytkie ugrupowanie bojowe. Brak odwodów. Utrudniona koordynacja współdziałania (zmiana podporządkowania sił).	Nieszczelność granicy (ograniczone siły w bezpośredniej odległości od granicy państwa).

Źródło: Warianty działania Sił Zbrojnych Wislandii w osłonie strategicznej, informacja na temat treningu sztabowego pk. CZERWIEC, Generalny Zarząd Operacyjny SG, Zespół Planowania Operacyjnego.

3.2.2. Działania opóźniające

Zgodnie z klasyfikacją działań taktycznych zawartą w narodowym regulaminie, działania opóźniające są jednym z podstawowych rodzajów walki.[84] Stanowisko takie znaleźć można również w regulaminach innych armii NATO, gdzie działania opóźniające zaliczane są do podstawowych rodzajów walki.[85]

Działania opóźniające obejmują „szereg kolejnych starć o charakterze obronnym i zaczepnym,[86] szeroko stosowany manewr i działania osłabiające potencjał przeciwnika".[87]

Zatem cel główny działań opóźniających powinien być odnoszony do wymiaru czasowego, a jest nim odsunięcie w czasie dotarcie przeciwnika do określonego rejonu (rubieży), a po przez to„zyskanie czasu" na zorganizowanie innych działań.[88] Konieczność zyskania czasu na przygotowanie obrony w głębi jest szczególnie istotne w początkowym okresie konfliktu, w sytuacji, gdy agresor może uzyskać zaskoczenie, a zasadnicze siły obrońcy są w fazie osiągania gotowości do działania.

Zebrane wnioski i doświadczenia z przeprowadzonych ćwiczeń oraz wyniki analizy literatury przedmiotu wskazują, że przed wyprowadzeniem uderzeń zgrupowań lądowych, przeciwnik starał się będzie uchwycić i umocnić obiekty decydujące o powodzeniu natarcia.

Użyje w tym celu prawdopodobnie desantów i oddziałów wydzielonych (OW) które wykonując swoje zadania, wyzwolą ruch lądowych zgrupowań uderzeniowych. W razie zaistnienia takie właśnie scenariusza rozwoju wydarzeń, jednym z ważniejszych celów działania obrońcy może być

---

[84] Regulamin działań wojsk lądowych, DWL, Warszawa 1999, s. 123-131.

[85] m.in. Doktryna wojsk lądowych ATP-35(B), Regulamin walki wojsk lądowych Bundeswehry HDv 100/100, Podręcznik polowy 100-5. Działania wojsk lądowych armii Stanów Zjednoczonych, Z. Ścibiorek, Zasady prowadzenia działań opóźniających przez oddziały i pododdziały ogólnowojskowe (OPÓR I), AON, Warszawa 1996, s. 10.

[86] „Siły opóźniające muszą wykorzystywać każdą dogodną sytuację do wykonania zwrotów zaczepnych", Regulamin ..., wyd. cyt. s. 124

[87] Tamże, s. 123.

niedopuszczenie do połączenia się OW z wysadzonymi wcześniej desantami, co może w znacznym stopniu opóźnić i zdezorganizować natarcie zasadniczych sił przeciwnika.

Jak wskazują wnioski z wielu ćwiczeń[89], zadanie to może być skutecznie wykonywane przez jednostki aeromobilne lub desantowo-szturmowe, zwłaszcza te, wytypowane do sił o Wysokiej Gotowości. Wymaga jednak szczegółowego rozpatrzenia, tj. wyodrębnienia w nim zadań cząstkowych, do których można zaliczyć:

- rozpoznanie kierunków podchodzenia i składu OW;
- naprowadzenie na nie uderzeń zasadniczych sił zgrupowania;
- wykonanie zapór i niszczeń na drogach podchodzenia OW;
- obezwładnianie elementów ugrupowania OW.

Zasadnicza trudność w opóźnianiu podejścia OW polega na trafnym rozpoznaniu zamiarów przeciwnika i podjęciu stosownego przeciwdziałania. Skutecznym sposobem rozpoznania kierunków podchodzenia i składu OW jest patrolowanie ze śmigłowców. Wykorzystując właściwości maskujące terenu, powietrzne patrole rozpoznawcze wyszukują cele, określają parametry ich ruchu (prędkość, kierunek) oraz skład OW. Wskazanym jest przy tym, niepodejmowanie walki z elementami rozpoznawczymi przeciwnika, a raczej pozwolenie im na „kontrolowaną" kontynuację rozpoznania. W przeciwnym razie, zasadnicze siły OW podejmą działania w celu uniknięcia uderzeń, np. poprzez zmianę kierunku podchodzenia, czy też mylenie. Dlatego też patrole rozpoznawcze powinny dążyć do wykrycia zasadniczych sił OW przeciwnika i z chwilą ich wykrycia, ograniczyć swoje działania do nakierowania na nie uderzeń zgrupowań taktycznych.

---

[88] Taktyka ogólna wojsk lądowych, AON, Warszawa 2000, s. 104.

[89] W ćwiczeniu dowódczo-sztabowym przeprowadzonym w październiku 2000 roku 18 bdsz, działając w pasie sił przesłaniania, otrzymał zadanie opóźnić i zdezorganizować wejścia do walki oddziałów wydzielonych przeciwnika. Podobne było działanie bdsz w ćwiczeniu pk. „TATRY 96", gdzie wspólnie z innymi jednostkami opóźniał podchodzenie sił przeciwnika.

Jeżeli zaistnieją uzasadnione obawy o utracenie kontaktu z OW, np. poprzez jego wejście w duży kompleks leśny, lub możliwe podejście innych sił przeciwnika, należy przystąpić do ataku lub przygotować zasadzkę. Niezależnie od przyjętego sposobu działania, należy dążyć do rozczłonkowania kolumn przeciwnika, a następnie niszczenia ich częściami. Dodatkowo organizowane zapory i niszczenia w rejonach węzłów komunikacyjnych zmuszą przeciwnika do szukania dróg obejścia.

Wnioski z wielu ćwiczeń wskazują, że w etapie działań opóźniających jednostki aeromobilne mogą zostać użyte w dwóch zasadniczych wariantach: zaczepnym lub obronno-opóźniającym. W wariancie zaczepnym, rozważane działanie polega na atakowaniu newralgicznych obiektów w ugrupowaniu przeciwnika. Często będzie to związane z koniecznością przeniknięcia w głąb ugrupowania przeciwnika, co z kolei będzie niezmiernie trudne, mając na uwadze fakt, iż przeciwnik będzie w tym czasie realizował powietrzną operację zaczepną.

W przypadku użycia do działań opóźniających jednostek aeromobilnych, z ich składu wydziela się zazwyczaj kilka podgrup w sile np. wzmocnionej kompani szturmowej (ksz) każda oraz mobilne odwody, każdy w sile ok. plutonu. Taki podział sił umożliwia zorganizowanie: trzech pozycji opóźniania i jednej zasadzki powietrznej.

Uzyskanie wysokiej skuteczności działań w powyższym wariancie wymaga szczegółowego zaplanowania poszczególnych jego etapów, tj. zajęcia rejonu wyjściowego i przelotu oraz działań po wylądowaniu.

Zajęcie rejonu wyjściowego powinno odbyć się skrycie, wyznaczonymi zgrupowaniami, po różnych drogach i w różnym czasie. W celu sprawnego załadowania i transportu sił w rejon planowanych działań, dla każdej z podgrup wyznacza się zasadniczy oraz zapasowy rejon załadunku

o powierzchni ok. 1 km^2. Czas załadowania na śmigłowce jednej podgrupy w sile wzmocnionej ksz wynosi 25-30 min[90].

Jeśli założyć, iż w jednym z warunków powodzenia działań jest uzyskanie zaskoczenia, to należy tak zaplanować przemieszczenie, aby możliwe było dotarcie GDSz w nakazane rejony w jak najkrótszym czasie, z zachowaniem maskowania przelotu i jego bezpieczeństwa. W tym celu należy opracować między innymi: trasy przelotu do celu i z powrotem oraz tabele przegrupowania powietrznego (harmonogram czasowy przewozu poszczególnych grup, kalkulacje czasowe przelotu, procedury dotyczące kontroli przestrzeni powietrznej, zakres i sposób koordynacji działań lotnictwa wojsk lądowych z środkami obrony powietrznej, lotnictwem taktycznym i wspierającą artylerią[91].

Przy planowaniu desantowania koniecznym jest ustalenie sposobu wprowadzenie sił w rejon obiektu, miejsce, czas i kolejność lądowania i rozmieszczenia grup po opuszczeniu śmigłowców.

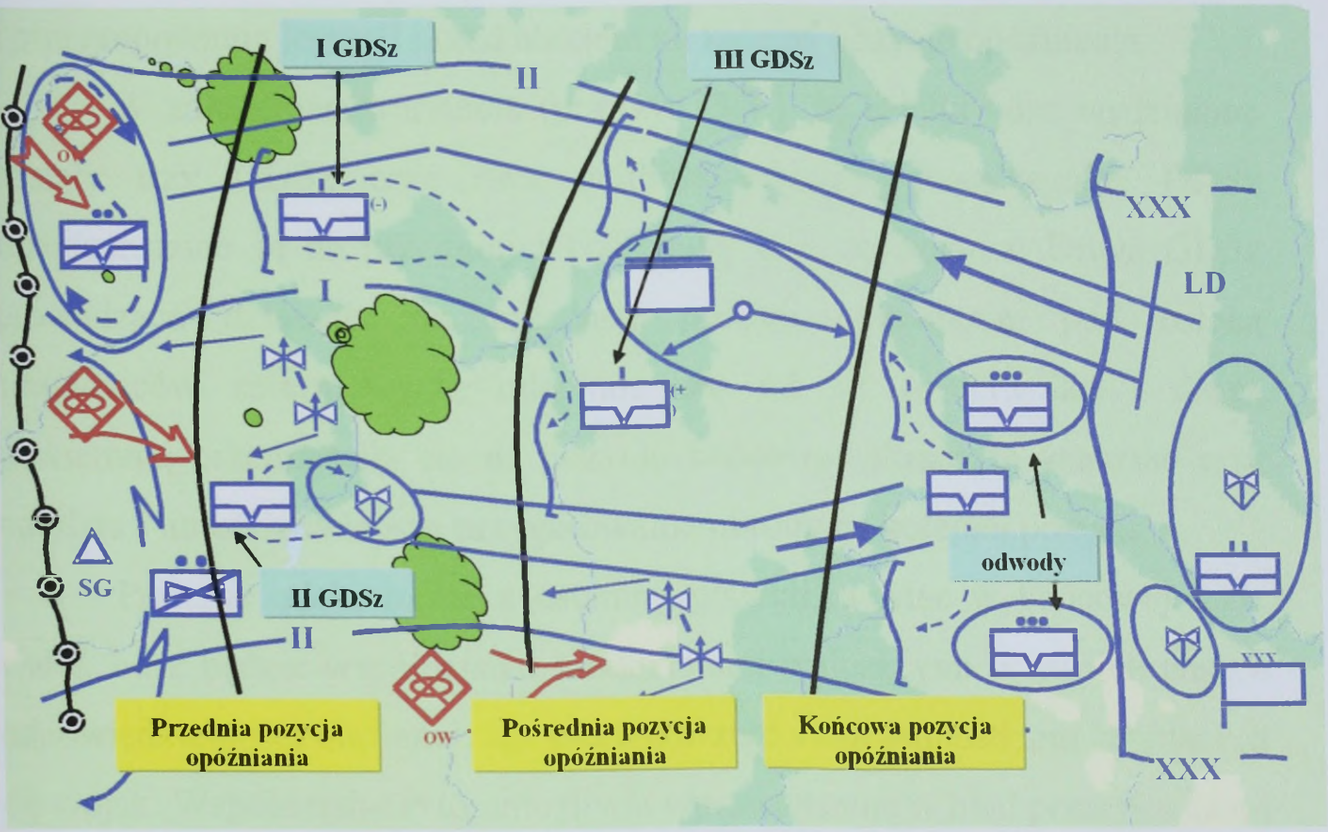
Zakładając, iż działania mogą być prowadzone w sytuacji nie do końca rozpoznanych zamiarów przeciwnika, to po desantowaniu w pierwszej kolejności należy zorganizować system rozpoznania, zwłaszcza na kierunkach prawdopodobnego podejścia przeciwnika. Umożliwi to ubezpieczenie, alarmowanie i szybką reakcję, a w konsekwencji skuteczniejsze opóźnianie jego podejścia poprzez wykonanie uderzeń na podchodzącego przeciwnika w najmniej oczekiwanej dla niego chwili.

Walka już od pierwszej pozycji opóźniania powinna być na tyle uporczywa, aby przeciwnik nie mógł jej pokonać czołowymi pododdziałami i był zmuszony do wcześniejszego rozwinięcia i wprowadzenia do walki części swoich sił głównych.

---

[90]Por. T. Sapierzyński, Co dowódca wiedzieć powinien, Kraków 1995, s. 17.
[91]T. Berezowski i zespół, Wybrane zagadnienia dowodzenia w wojskach aeromobilnychna na szczeblu taktycznym, Warszawa 2001, s. 35.

Dążyć przy tym należy do obrony najważniejszych obiektów i punktów terenowych, osłaniając ogniem luki i skrzydła. Działając z rejonów bazowych, zgrupowaniami wędrownymi lub zasadzkowymi, może natomiast prowadzić walkę na kolejnych pozycjach opóźniania.



Rys. 3.3. Prowadzenie działań opóźniających przez batalion desantowo-szturmowy (wariant)

Wnioski z ćwiczeń potwierdzają, że bdsz może prowadzić działania na dużą głębokość - do 60 km od wojsk własnych i w krótkim czasie (2 -12 godzin), umożliwiając wchodzącym do walki związkom taktycznym zorganizowanie skutecznej obrony na wyznaczonych rubieżach terenowych (por. rys. 3.3.)[92].

Istotny wpływ na sposób prowadzenia działań opóźniających mają warunki terenowe. Od nich bowiem zależy w dużej mierze wybór poszczególnych pozycji opóźnienia oraz obiektów obrony. Usytuowanie ich

---

[92] W ćwiczeniu dowódczo-sztabowym pk. „PAŹDZIERNIK", bdsz opóźniał podejście OW przeciwnika przez 6 godzin.

w rejonach przeszkód terenowych (wzgórza, rzeki, kompleksy leśne), w sposób naturalny może utrudnić działanie przeciwnika, np. dzieląc jego ugrupowanie na odizolowane części. Ważną sprawą jest także to, aby przygotowane do obrony obiekty ułatwiały skryte odejście sił, a poszczególne pozycje zmuszały przeciwnika do częstych zmian stanowisk ogniowych i przegrupowania jego sił przed atakiem na kolejną pozycję opóźniania.

W założonym wariancie (por. rys. 3.3.), ze składu bdsz wydzielone zostały trzy GDSz oraz dwa mobilne odwody. Poszczególne GDSz rozmieszczone są na przedniej i pośredniej linii opóźniania. Druga GDSz prowadząca działania na przedniej pozycji opóźniania, pod osłoną śmigłowców szturmowych, oderwała się od sił przeciwnika i drogą powietrzną przemieściła się na pozycję końcową. Skraca to znacznie czas odejścia i umożliwia lepsze przygotowanie obrony na kolejnej pozycji.

Podczas odchodzenia z ostatniej pozycji, a więc w końcowej fazie walki, bdsz będzie współdziałać z oddziałami walczącymi w swoich pasach odpowiedzialności obronnej, np. pierwszorzutowymi jednostkami broniących się wojsk. Współdziałanie to umożliwia wprowadzenie w błąd przeciwnika co do przebiegu przedniej linii obrony i „wciągniecie" go w rejon kluczowy przygotowywanej obrony.

Istotną rolę w zwalczaniu przeciwnika odgrywają śmigłowce szturmowe, wspierając walkę bdsz, mogą niszczyć jego środki pancerne i opancerzone. Natomiast śmigłowce wielozadaniowe i transportowe, w powyższym wariancie, wspierają bdsz między innymi w zakresie: rozpoznania, transportu, stawianie narzutowych zapór minowych, ewakuację rannych i chorych oraz zaopatrywanie wojsk.

Analiza tempa natarcia przeciwnika (por. zał. 7.) wskazuje, iż przez pierwsze trzy godziny walki, będzie ono bardzo niskie, gdyż nie przekroczy wartości 0,5 km/h. Tak niskie tempo będzie prawdopodobnie efektem uzyskanego przez bdsz zaskoczenia (między innymi poprzez organizację

zasadzki) i zorganizowania silnej pierwszej pozycji opóźniania. Z chwilą jej pokonania, tempo natarcia przeciwnika znacznie wzrośnie, osiągając wartość maksymalną 3,5 km/h w piątej godzinie walki.

Największe przesunięcie wojsk przeciwnika w symulowanej sytuacji, następuje od trzeciej do piątej godziny walki.

Analiza dynamiki strat wskazuje, że przeciwnik największe straty poniesie przez pierwsze dwie godziny walki (18%), jednak w każdej następnej godzinie, będzie ich ponosił coraz mniej. Bdsz najwięcej strat (ok. 10%) poniesie między drugą a trzecią godziną walki, w następnych godzinach ich dynamika będzie również coraz mniejsza. Z sumy straty bdsz poniesionych w poszczególnych godzinach walki wynika, że po ok. czterech godzinach walki będzie on na granicy utraty zdolności bojowej.

W powyższym wariancie istnieje uzasadniona konieczność zaangażowania całości lub większości sił bdsz do wykonania jednego zadania, stąd też bdsz może zostać użyty tylko jeden raz w ciągu doby, po czym powinien zostać wycofany do odwodu.

3.2.3. Działania blokujące

Konflikt może zaistnieć w bliższym, lub w dalszym otoczeniu Polski, nie będziemy stroną konfliktu, wówczas dywizja (brygada) może być użyta w ramach NATO.

Inna sytuacja, to kryzys, w którym Polska będzie stroną, wówczas ZT (oddział) może działać w układzie narodowym. W miarę oceny skali, charakteru i kierunków zagrożeń agresją militarną, celowe jest odpowiednie ukierunkowanie szkolenia w kontekście przewidywanego użycia i jak najszybsze przemieszczenie sił i środków te kierunki.

Przewidywać więc należy możliwość zwiększenia obszaru odpowiedzialności przewidzianego wojskom lądowym poprzez

uwzględnienie rejonów odpowiedzialności wojsk OT oraz wzrostu zadań związanych z dowodzeniem siłami o różnym przeznaczeniu i możliwościach. Cel działań taktycznych, jaki wynika ze wspomnianej koncepcji sprowadza się do utrzymania możliwie największej części terytorium państwa przy użyciu wszystkich dostępnych środków oraz odzyskania terenu utraconego. Wynika stąd, że w taktyce wojsk lądowych należy uwzględniać między innymi konieczność:

- prowadzenia walki przeciwdesantowej na całym obszarze objętym zwiększenia aktywności obrońców;
- działaniami, przez wszystkich uczestników walki;
- prowadzenia nowego rodzaju działań jakim są działania nieregularne;
- organizowania działań w terenie zabudowanym w skali większej niż dotychczas;
- jednoczesnego prowadzenia działań na całej głębokości ugrupowania.

Analogicznie, czas trwania walki zgrupowań taktycznych wynikać będzie z potrzeb wykonania zadań przez siły broniące się w punkcie ciężkości oraz ich możliwości bojowych, zaangażowanego potencjału przeciwnika i jego celu działania, skutecznego działania na każdym szczeblu, jak też celowości decyzji podejmowanych w toku obrony.

Dzisiejsze pole walki charakteryzuje się mobilnymi i efektywnymi środkami walki zbrojnej, szeroko stosowaną elektroniką i integralnie związane jest z systemem informacyjnym, dużą precyzją i skutecznością środków rażenia, co stawia wysokie wymagania w czasie prowadzenia działań. Wprowadzenie nowych rodzajów środków walki wskazuje na konieczność dokonania zmian w kształcie ugrupowania bojowego. Pojawienie się nowych środków walki wymusza zmiany w taktyce. Każdy nowy rodzaj

uzbrojenia wprowadzany do wojsk, czy też w wojskach przeciwnika zmusza do wprowadzenia zmian w działaniach bojowych, co rzutuje na skład i przeznaczenia elementów ugrupowania bojowego. Takim przykładem jest pojawienie się na szeroką skalę śmigłowców bojowych i postępujący wzrost ich roli i znaczenia, co umożliwia szersze ich wykorzystanie a tym samym stanowi zagrożenie dla nieodpowiednio przyjętego ugrupowania bojowego. Wprowadzenie nowych, bardziej nowoczesnych środków walki może spowodować zmniejszenie lub łączenie elementów ugrupowania bojowego. Siły o największej wartości bojowej powinny być wydzielane na kierunek największego zagrożenia.

Przy tendencjach zmierzających w kierunku zmniejszenia ilości posiadanych sił i podwyższenia ich jakości, szczególnego znaczenia nabiera racjonalne wykorzystanie posiadanego potencjału bojowego.

Istotnym czynnikiem jest wymiar powietrzno-lądowy zadań obronnych oraz potrzeba dostosowania rozwiązań koncepcyjnych do funkcjonowania praktycznych struktur organizacyjnych[93].

Wielowymiarowość operacji oraz ich nieliniowy charakter prowadzić będzie do rozdzielenie działań, to jest do powstawania uniezależnionych od siebie ognisk walki. Powstanie zatem sytuacja, w której planowanie będzie centralne, ale realizacja działań będzie zdecentralizowana. Na podstawie dotychczasowych konstatacji można z dużą dozą prawdopodobieństwa stwierdzić, że w przyszłych działaniach może dojść do rezygnacji z koncentracji sił w określonym miejscu i czasie na rzecz koncentracji wysiłków (skutków oddziaływania)[94].

Również przed brygadami pojawił się problem przygotowań do działań autonomicznych w różnych sytuacjach operacyjnych, jednak z pełną wyrazistością może on wystąpić podczas wykonywania zadań

---

[93] M. Huzarski, Obrona i natarcie dywizji, AON, Warszawa 1997, s. 75.

obronnych na samodzielnych kierunkach. Z praktyki prowadzonych ostatnio ćwiczeń wynika, iż przyjmowanie ugrupowania obronnego przez brygadę samodzielnie, wymaga utrzymywania większości sił w głębi ugrupowania, zachowując średnią proporcję miedzy pierwszym rzutem a odwodem (odwodami). Silny odwód (odwody) pozwala na zdecydowane reagowanie w rejonach i na kierunkach gdzie zarysowuje się zagrożenie. Ponadto podczas samodzielnego wykonywania zadań przez brygadę występują charakterystyczne uwarunkowania, które nakazują osłonę skrzydeł oraz utrzymywanie ciągłej gotowości do obrony okrężnej Odpowiednia głębokość ugrupowania i jego koliście rozmieszczone elementy skracają drogę manewru i sprzyjają szybkiemu reagowaniu, stosownie do zaistniałej sytuacji.

Dla przykładu, w ćwiczeniu dowódczo-sztabowym p.k. „PIERŚCIEŃ", prowadzonym w Akademii Obrony Narodowej, 7 DZ otrzymała zadanie od granicy państwowej przejąć odpowiedzialność za zwalczanie przeciwnika (por. zał. 8.). Kanalizować jego natarcie na kierunkach: Dęblin, Stoczek Łukowski, Siedlce; Biała Podlaska, Łosice, Siedlce. W pierwszym dniu walki opóźniać natarcie przeciwnika do linii żółta i w D+1 dążyć do zerwania operacji zaczepnej na linii czerwona.

Dca 7 DZ zamierzał współdziałając z siłami OT i Straży Granicznej, opóźniać i dezorganizować natarcie przeciwnika od granicy państwowej, stwarzając warunki do zerwania operacji zaczepnej przeciwnika w głębi pasa opóźniania. W przydzielonym pasie zorganizować cztery pozycje opóźniania: biała, zielona, żółta i czerwona. Działaniami na pozycji biała opóźniać natarcie przeciwnika do H+6, nie dopuścić do pokonania jej z marszu i zmusić przeciwnika do rozwinięcia sił głównych. Działaniami w głębi opóźniać natarcie przeciwnika: na pozycji zielona do H+10, na pozycji żółta

---

[94] S. Korzeniowski, A. Bujak, Działania zgrupowań kawalerii powietrznej na korzyść związku taktycznego w przyszłych operacjach pk. „RAJD", AON, Warszawa 2000, s. 83.

do H+16. Zadać przeciwnikowi maksymalne straty i kanalizować jego natarcie w nakazanych kierunkach. Brygadą odwodową przejść do obrony na linii czerwona i we współdziałaniu z częścią sił wycofanych z pierwszej pozycji opóźniania, w D+1 dążyć do zerwania operacji zaczepnej przeciwnika. Ugrupowanie bojowe w jeden rzut z odwodem: pierwszy rzut: 71 BZ, 73 BPanc, odwód: 72 BZ.

Tak sformułowane zadanie dla dywizji oraz przyjęty sposób jego wykonania wynikał ze złożoności sytuacji, gdyż dywizja przejmowała odpowiedzialność za zwalczanie przeciwnika już od granicy państwowej, opóźniała operację zaczepną przeciwnika i w efekcie końcowym dążyła do jej zerwania w kolejnych dniach operacji. Wymagało to odpowiedniego uszykowania sił dywizji, gdzie zasadnicze z nich, tj. dwie brygady w pierwszym rzucie prowadziły działania opóźniające. Natomiast brygada odwodowa organizowała obronę w głębi, a jej zadaniem było zatrzymać natarcie przeciwnika. Dodatkowym utrudnieniem w wykonaniu zadania były duże rejony i pas obrony. Wymuszało to konieczność prowadzenia działań na samodzielnych kierunkach, a tym samym organizowanie samodzielnych zgrupowań taktycznych (por. zał. 8.).

W wypadku nasilania się zagrożeń i jawnych oznak interwencji zbrojnej, szczególnie narażonymi na ataki obiektami będą prawdopodobnie lotniska oraz porty morskie. Stąd też jednym z ważniejszych przedsięwzięć obronny w ramach reagowania kryzysowego staje się przygotowanie obrony wymienionych obiektów.

Obrona portów morskich i wybrzeża jest to o tyle ważne, iż prawie cała granica morska Polski stwarza dogodne warunki do wysadzenia desantu. Dlatego siły wyznaczone do tego typu działań muszą mieć na względzie tę ewentualność i być w gotowości do szybkiej reorganizacji swoich sił i przemieszczenia ich na zagrożone kierunki.

Specyfika działań obronnych na wybrzeżu morskim wynika z charakteru przestrzeni, z której może nastąpić zagrożenie – morza. W tych warunkach z jednej strony trudno jest ocenić prawdopodobny kierunek podejścia sił przeciwnika, z drugiej zaś przeciwnik nie ma możliwości ukrycia swojego zgrupowania na morzu[95].

Obrona wybrzeża składa się z dwóch głównych składników: obrony na morzu i obrony brzegu por. załącznik 9[96].

Obrona na morzu obejmuje działania marynarki wojennej i sił powietrznych, mające na celu przeciwdziałanie zagrożeniu desantem morskim przeciwnika. Obrona prowadzona będzie przez marynarkę wojenną i siły powietrzne wsparte posiadaną artylerią[97]. Będą one obserwować działania przeciwnika i atakować jego siły, zadając maksymalne straty oraz dezorganizując ruch jego wojsk, zyskując tym samym czas na zorganizowanie obrony na brzegu na wykrytym kierunku podejścia sił desantowych. Celem tych działań jest zniszczenie zgrupowań desantowych przeciwnika, dopóki znajdują się na morzu i są wrażliwe na uderzenia.

Obrona na brzegu powinna być skupiona wokół terenu kluczowego i najbardziej prawdopodobnych miejsc desantowania z jednoczesnym dozorowaniem innych rejonów wybrzeża[98]. Jak wynika z perspektywicznych ocen, obrońca z reguły, nie będzie posiadał dostatecznych sił do zorganizowania silnej obrony wzdłuż całego wybrzeża[99]. Posiadane siły powinien więc odpowiednio ugrupować, umożliwiając podjęcie skutecznej walki na dowolnym kierunku.

Na ugrupowanie bojowe w obronie wybrzeża morskiego wpływa bezpośrednio stosunkowo szeroki pas (rejon) obrony. Tak więc by można

---

[95] Por.: W. Kaczmarek, Związek taktyczny (oddział) w obronie wybrzeża morskiego, Warszawa, AON 1997.
[96] Huzarski M. (red.), Aspekty narodowe i sojusznicze w teorii taktyki ogólnej wojsk lądowych p.k. „GARDA", AON, Warszawa 2000, s. 236.
[97] Por.: T. Gander, Szwedzkie potężne siły antyinwazyjne, Sweden's powerful anti-invasion force., Jane's Defence. Weekly, 1986, vol. 6, nr 24, s. 1458-1459.
[98] Huzarski M. (red.), Aspekty ...wyd. cyt., s. 237.
[99] Z. Bieżuński, Przeciwdesantowa obrona wybrzeża morskiego, Warszawa, AON 1991.

było mówić o skutecznej obronie więcej niż jednego odcinka desantowania przeciwnika, celowym jest podczas tworzenia ugrupowania organizowanie większej ilości odwodów. Ważnym jest również to, by planując obronę umiejętnie wykorzystać wszystkie siły znajdujące się w pasie (rejonie) obrony, np. wojsk OT.

Bardzo dużą rolę w tworzeniu wariantu ugrupowania obronnego odgrywa teren przylegający do wybrzeża morskiego. Należy dążyć by w maksymalnym stopniu go wykorzystać, a wszystkie elementy ugrupowania tak wkomponować w jego ukształtowanie, by zapewnić im odpowiednie warunki pod względem zabezpieczenia bojowego, logistycznego jak również możliwości manewru.

Siły organizujące obronę na poszczególnych kierunkach (odcinkach) powinny być zdolne do odparcia uderzenia i niszczenia desantu przeciwnika na plażach. W sytuacji, gdy nie będą posiadać dostatecznych sił do realizacji tego zadania, powinny podjąć walkę z desantem w celu zapewnienia dogodnych warunków do szybkiej koncentracji mobilnych odwodów i ich uderzenia na siły desantu zanim umocnią się na uchwyconym przyczółku.

Ponieważ obrońca musi być przygotowany na lądowanie sił desantu na całej długości rejonu odpowiedzialności, to podstawowym problemem w tych warunkach jest znalezienie odpowiedzi na pytanie, jak ugrupować siły i środki oraz gdzie podjąć rozstrzygającą walkę z desantem morskim.

Obrońca szczególną uwagę musi zwrócić na desanty przeciwnika wysadzane w głębi lądu. Jak wskazują doświadczenia, powinny one być natychmiast izolowane, pozbawione możliwości uchwycenia wzniesień, punktów kanalizujących ruch i innych kluczowych obiektów terenowych, z których mogłyby kontrolować przegrupowanie sił obrońcy i w ten sposób pozbawiać go swobody manewru. Z powyższego wynika też wniosek, że możliwe rejony wysadzenia desantu przez przeciwnika powinny być

wcześniej rozpoznane i zabezpieczone, w ich obszarze powinna zostać rozmieszczona część odwodów[100].

Do ważnych właściwości wynikających ze specyfiki terenu zaliczyć również trzeba znaczenie rozbudowy inżynieryjnej pasa nadbrzeżnego i wód do niego przyległych[101]. Bardzo istotnym jest, aby przygotowując się do obrony wybrzeża, stworzyć pas zapór przeciwdesantowych zarówno na morzu, jak i na lądzie, w portach oraz bazach morskich. Powinny one w znacznym stopniu utrudnić desantowanie sił przeciwnika.

W obronie szczególne znaczenie będzie miała trwałość obrony sił prowadzących obronę na brzegu w rejonie lądowania desantu przeciwnika i manewrowość odwodów w połączeniu z natychmiastowym przejściem do działań ofensywnych w celu zniszczenia desantowanych sił[102].

Jeżeli chodzi o artylerię część rozmieszcza się w ugrupowaniu oddziałów pierwszego rzutu, natomiast pozostałe siły umiejscawia się w głębi lądu gdzie są one w gotowości do sprawnego zajęcia stanowisk ogniowych, w sytuacji ustalenia rejonu desantowania wojsk przeciwnika. Odwody przeciwpancerne z zasady rozmieszcza się w pobliżu przedniej linii obrony w gotowości do wyjścia na rubieże ogniowe, celem wsparcia pododdziałów pierwszego rzutu.

Podsumowując dotychczasowe rozważania na temat obrony wybrzeża, można sformułować następujące wnioski:

1. Skuteczne prowadzenie obrony wybrzeża morskiego zależne jest od ścisłego współdziałania lotnictwa, sił lądowych i marynarki wojennej.
2. Wyjątkowo ważną rolę w obronie wybrzeża spełnia rozpoznanie.

---

[100] A. Bujak, Z. Śliwa, Działania bojowe związku taktycznego i oddziału w specyficznych środowiskach Warszawa, AON 1999, s. 95.

[101] Por.: J. Garstka, System zapór i niszczeń w obronie przeciwdesantowej wybrzeża morskiego, Myśl Wojskowa 1994, nr 3.

[102] Por.: M. Hewisch, Obrona wód przybrzeżny i wybrzeży, Internationale Defense Review 1986, vol. 19, nr 9, s. 1259-1262 [w:] Wojskowy Przegląd Zagraniczny 1989, nr 1, s. 48.

3. Szczególnie duże zagrożenie występuje ze strony sił aeromobilnych przeciwnika.

4. Należy wypracować koncepcję obrony, umożliwiającą zwalczanie sił przeciwnika na samym brzegu i w głębi obrony.

5. Ze względu na przewidywane szerokie pasy odpowiedzialności w obronie wybrzeża, skuteczność prowadzonej obrony będzie często zależeć od możliwości manewrowych broniących się wojsk.

3.2.4. Wsparcie działań antyterrorystycznych

Przeciwdziałanie terroryzmowi zazwyczaj postrzegane jest jako fizyczna eliminacja jego przejawów, realizowana zwykle przy pomocy jednostek antyterrorystycznych. Jednakże jest to powierzchowne i błędne pojmowanie tego zagadnienia.

Na przeciwdziałanie terroryzmowi składa się wiele różnorodnych przedsięwzięć, realizowanych przez poszczególne służby samodzielnie lub we współdziałaniu. Poddając system przeciwdziałania terroryzmowi analizie można wyróżnić następujące etapy działań:

- rozpoznanie;
- zapobieganie;
- zwalczanie;
- usuwanie skutków[103].

W Polsce odpowiedzialność za każdy z wymienionych obszarów spoczywa na innych służbach, natomiast Siły Zbrojne RP spełniają w czasie ich realizacji jedynie wspierającą rolę (z wyjątkiem zwalczania zagrożeń typu „RENEGADE[104]").

---

[103] S. Wudarski, System przeciwdziałania terroryzmowi w Polsce http://www.terroryzm.com/article/273/System-przeciwdzialania-terroryzmowi-w-Polsce.html

[104] Przez określenie „RENEGADE" należy rozumieć wykorzystanie różnego typu statków powietrznych, zarówno wojskowych jak i cywilnych, jako środków uderzeniowych na obiekty naziemne / nawodne (zał. 7.).

Rozpoznanie zagrożeń terrorystycznych – polega na monitorowaniu działalności jednostek oraz grup, mogących zastosować metody terrorystyczne[105]. Odpowiedzialność za rozpoznawanie zagrożeń terrorystycznych spoczywa przede wszystkim na: Agencji Bezpieczeństwa Wewnętrznego (ABW), Agencji Wywiadu (AW), Służby Wywiadu Wojskowego (SWW) oraz Służby Kontrwywiadu Wojskowego (SKW). Kompetencje SWW i SKW w kwestii zwalczania terroryzmu dotyczą w zasadzie przestępstw podlegających jurysdykcji sądów wojskowych.

Instytucjami wiodącymi w aspekcie rozpoznania i monitorowania zagrożeń terrorystycznych są ABW i Policja.

Poza wymienionymi powyżej elementami w skład systemu rozpoznania wchodzą placówki monitorujące skażenia (radiologiczne, chemiczne i biologiczne, mogące być wynikiem aktu terroryzmu). Jednakże odgrywają one mniejszą rolę w systemie, zważywszy na mniejsze prawdopodobieństwo zagrożenia atakami terrorystycznymi z użyciem broni masowego rażenia.

Zapobieganie aktom terrorystycznym – polega na niedopuszczeniu do ataku z wykorzystaniem metod terrorystycznych. Zapobieganie nie może być realizowane bez rozpoznania, gdyż jedynie rozpoznanie konkretnego zagrożenia może prowadzić do jego identyfikacji i podjęcia odpowiednich środków bezpieczeństwa, mających na celu nie dopuszczenie do tego zagrożenia. Zapobieganie obejmuje również działania prewencyjne. W zakresie zapobiegania można wyróżnić działania instytucji państwowych oraz organizacji pozapaństwowych. Wśród instytucji państwowych poza służbami specjalnymi (ABW, AW, SKW, SWW), znaczącą rolę odgrywają przede wszystkim Policja, Straż Graniczna oraz Biuro Ochrony Rządu.

---

[105] S. Wudarski, wyd. cyt., s. 34.

Z kolei instytucje pozapaństwowe to przede wszystkim różnego rodzaju agencje ochrony oraz służby wewnętrzne bezpośrednio zaangażowane w ochronę przed dokonaniem aktu terroryzmu.

Działania prewencyjne Policji realizowane są zgodnie z jej kompetencjami określonymi w ustawie o Policji i polegają przede wszystkim na zapewnieniu ogólnego bezpieczeństwa, poprzez zapobieganie przestępstwom, w tym również działaniom terrorystycznym. Policja może być użyta w celu niedopuszczenia do dokonania aktu terrorystycznego na podstawie informacji operacyjnych z własnych źródeł lub informacji pochodzących od służb specjalnych.

Straż Graniczna z kolei odpowiada za kontrolę granic między innymi w celu zapobiegania przedostawaniu się do kraju osób podejrzanych o działalność terrorystyczną. Natomiast Biuro Ochrony Rządu, jest organem odpowiedzialnym za bezpieczeństwo osób, wykonujących ważne funkcje publiczne, ale także polskich placówek dyplomatycznych oraz obiektów i urządzeń o szczególnym znaczeniu.

W zakresie zapobiegania bardzo ważną rolę w systemie przeciwdziałania terroryzmowi w Polsce odgrywa powołany w 2006 r. Międzyresortowy Zespół do Spraw Zagrożeń Terrorystycznych[106], który zastąpił sformowane w 2002 roku Międzyresortowe Centrum do spraw Zwalczania Przestępczości Zorganizowanej i Międzynarodowego Terroryzmu. Zespół jest organem pomocniczym Rady Ministrów zapewniającym współdziałanie administracji rządowej w zakresie rozpoznania, przeciwdziałania i zwalczania terroryzmu. W skład Zespołu wchodzą: Minister Spraw Wewnętrznych i Administracji – przewodniczący Zespołu, zastępcy przewodniczącego, którymi są Ministrowie Finansów, Obrony Narodowej, Spraw Zagranicznych oraz minister-członek Rady

[106] Zarządzenie nr 162 Prezesa Rady Ministrów z dnia 25 października 2006 r. w sprawie utworzenia Międzyresortowego Centrum do Spraw Zagrożeń Terrorystycznych.

Ministrów – Koordynator Służb Specjalnych, powoływany przez przewodniczącego sekretarz oraz członkowie: sekretarz (lub podsekretarz) stanu wskazany przez Ministra SWiA, Szef Obrony Cywilnej Kraju, Szef ABW, Szef AW, Szef BOR, Szef SWW, Szef SKW, Komendant Główny Policji, Komendant Główny Straży Granicznej, Komendant Główny Państwowej Straży Pożarnej, Komendant Główny Żandarmerii Wojskowej, Generalny Inspektor Kontroli Skarbowej, Generalny Inspektor Informacji Finansowej oraz Szef Służby Celne.

Głównymi zadaniami Zespołu w dziedzinie zapobiegania terroryzmowi są:

- monitorowanie zagrożeń terrorystycznych, dokonywanie ich analiz i ocen oraz przedstawianie opinii i wniosków;
- opracowywanie projektów standardów i procedur w zakresie zwalczania terroryzmu;
- inicjowanie, koordynowanie i monitorowanie działań w zakresie wykorzystania informacji oraz rozpoznawania, przeciwdziałania i zwalczania terroryzmu;
- organizowanie współpracy międzynarodowej w zakresie zwalczania terroryzmu;
- inicjowanie działań legislacyjnych zmierzających do usprawnienia metod i form zwalczania terroryzmu;
- inicjowanie szkoleń i konferencji dotyczących zwalczania terroryzmu.

Kolejną komórką współuczestniczącą w zapobieganiu aktom terroru jest powołane na mocy rozporządzenia Rady Ministrów z dnia 2 lipca 2002 r. – Kolegium do Spraw Służb Specjalnych. Do priorytetowych zadań Kolegium należy nadzór i koordynowanie działań służb specjalnych, opracowywanie ocen i opinii projektów aktów normatywnych i innych dokumentów rządowych dotyczących działalności służb specjalnych oraz kierunków i planów działania służb specjalnych. W ramach Kolegium działa

również Zespół ds. Koordynacji Działań Operacyjno-Rozpoznawczych w Zakresie Zwalczania Terroryzmu Politycznego[107].

Zwalczanie zagrożeń terrorystycznych – polega na likwidacji jednostek, lub też grup, stosujących metody terrorystyczne. Zwalczanie, podobnie jak zapobieganie, ściśle łączy się z rozpoznaniem, jednakże w przeciwieństwie do zapobiegania przy zwalczaniu musi dojść do aktu terroryzmu. W polskim systemie przeciwdziałania terroryzmowi jest wiele środków, które mogą być podjęte w celu zwalczania terroryzmu. Poza środkami typowo siłowymi (fizycznym zwalczaniem) są także środki formalno-prawne, które mogą być użyte na przykład w kwestii zwalczania finansowania terroryzmu. Zwalczanie aktów terroryzmu determinowane jest przez rodzaj tych ataków. W ramach zwalczania należy także zawrzeć wszystkie działania, zmierzające do schwytania i osądzenia sprawców tych aktów.

W Polsce głównymi służbami odpowiedzialnymi za zwalczanie aktów terroryzmu są: Policja (w szczególności Biuro Operacji Antyterrorystycznych i pododdziały antyterrorystyczne Policji), ABW, AW, SKW i SWW, jednostki wojsk specjalnych (poza granicami kraju, lub też po wprowadzeniu adekwatnego stanu nadzwyczajnego) oraz Siły Powietrzne (w kwestii obrony granicy państwowej w powietrzu) oraz Straż Graniczna (realizując ochronę granicy państwowej), Służba Celna i Generalny Inspektorat Informacji Finansowej.

Gdyby doszło do aktu terroryzmu na terenie kraju, śledztwo przekazane zostałoby ABW, gdyż to w jej właściwościach leży prowadzenie tego typu spraw. W tym celu ABW otrzymała stosowne uprawnienia śledcze.

Jednakże akty terroryzmu na obywatelach i obiektach polskich (budynki, statki morskie i powietrzne) mogą być dokonywane poza granicami naszego kraju, gdzie Policja oraz ABW nie mają takich uprawnień jak na

---

[107] D. Szlachter, Walka z terroryzmem w Unii Europejskiej – nowy impuls, Toruń 2007.

terenie kraju. Za zwalczanie aktów terroryzmu za granicami odpowiadają więc AW oraz SWW (w kwestiach określonych ustawami, regulującymi działanie tych służb). Poza granicami Polski zwalczanie terroryzmu realizowane jest przy wykorzystaniu jednostek wojsk specjalnych.

W przypadku, użycia samolotu, śmigłowca lub innego statku powietrznego do ataku terrorystycznego, zgodnie z wprowadzoną w dniu 2 lipca 2003 r. nowelizacją ustawy o ochronie granicy państwowej z dnia 12 października 1990 r., po spełnieniu określonych warunków, Minister Obrony Narodowej może podjąć decyzję o zestrzeleniu przechwyconego statku powietrznego – za realizację tego zadania odpowiadają Siły Powietrzne.

Usuwanie skutków ataku terrorystycznego – polega na organizacji i przeprowadzeniu akcji ratunkowej oraz na zabezpieczeniu przed powtórnym atakiem. Zagadnienia związane z usuwaniem skutków ataku terrorystycznego zostały uregulowane dopiero niedawno ustawą o zarządzaniu kryzysowym. Ustawa ta ustanawia zintegrowany system zarządzania kryzysowego, za którego funkcjonowanie odpowiadają organy administracji publicznej. Zarządzanie kryzysowe odbywa się na poziomach: krajowym, wojewódzkim, powiatowym oraz gminnym. Zarządzanie kryzysowe na poziomie krajowym sprawuje Rada Ministrów, a w sprawach nie cierpiących zwłoki minister właściwy do spraw wewnętrznych (zawiadamiając niezwłocznie o swoich działaniach Prezesa Rady Ministrów). Rada Ministrów sprawuje zarządzanie kryzysowe poprzez Rządowy Zespół Zarządzania Kryzysowego, który jest organem opiniodawczo-doradczym właściwym w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego. Przewodniczącym Rządowego Zespołu Zarządzania Kryzysowego jest Prezes Rady Ministrów. W skład zespołu wchodzą: Minister Obrony Narodowej i minister właściwy do spraw wewnętrznych (zastępcy przewodniczącego), Minister Spraw Zagranicznych oraz Minister

Koordynator Służb Specjalnych – jeżeli został powołany. Ponadto w posiedzeniach Zespołu na prawach członków biorą udział ministrowie kierujący działami administracji rządowej, istotnymi dla funkcjonowania państwa[108].

Do obsługi i zabezpieczenia prac Rządowego Zespołu Zarządzania Kryzysowego powołane zostało funkcjonujące w trybie ciągłym Rządowe Centrum Bezpieczeństwa, do którego zadań w zakresie zarządzania kryzysowego należy między innymi: planowanie cywilne, monitorowanie zagrożeń, przygotowanie uruchamiania procedur związanych z zarządzaniem kryzysowym, zapewnienie wymiany informacji i koordynacja działań między krajowymi i zagranicznymi organami i strukturami zarządzania kryzysowego[109].

Organem właściwym w sprawach zarządzania kryzysowego na terenie województwa jest wojewoda, który swoje zadania w tym zakresie realizuje przy pomocy wojewódzkiego zespołu zarządzania kryzysowego. Ponadto utworzono wojewódzkie centra zarządzania kryzysowego, działające w ramach całodobowych dyżurów, w celu zapewnienia przepływu informacji na potrzeby zarządzania kryzysowego, nadzorowania systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania ludności. Do zadań wojewódzkich centrów zarządzania kryzysowego należy ponadto współpraca i współdziałanie z organami administracji publicznej oraz podmiotami prowadzącymi akcje ratownicze, poszukiwawcze i humanitarne.

Na analogicznej zasadzie skonstruowane jest zarządzanie na szczeblu powiatu i gminy, gdzie organami pomocniczymi starosty i wójta /burmistrza/

---

[108] Członkami Zespołu są: ministrowie kierujący następującymi działami administracji rządowej: administracja publiczna, budownictwo, gospodarka przestrzenna i mieszkaniowa, finanse publiczne, gospodarka, gospodarka morska, gospodarka wodna, instytucje finansowe, informatyzacja, kultura i ochrona dziedzictwa narodowego, łączność, oświata i wychowanie, rolnictwo, sprawiedliwość, środowisko, transport, zdrowie, praca i zabezpieczenie społeczne, a ponadto: Główny Geodeta Kraju, Główny Inspektor Sanitarny, Główny Lekarz Weterynarii, Komendant Główny Państwowej Straży Pożarnej, Komendant Główny Policji, Komendant Główny Straży Granicznej, Prezes Państwowej Agencji Atomistyki, Prezes Urzędu Lotnictwa Cywilnego, Szef ABW, Szef AW, Szef Obrony Cywilnej Kraju, Szef SKW oraz Szef SWW.

[109] Art. 11 ustawy z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U.07.88.590).

prezydenta miasta są powiatowe / gminne i miejskie zespoły zarządzania kryzysowego, z zastrzeżeniem, że na szczeblu gminy i miasta nie muszą być powoływane gminne (miejskie) centra zarządzania kryzysowego.

W aspekcie przeciwdziałania aktom terroru wymienione struktury zarządzania kryzysowego mogą włączyć się we wcześniejszych etapach, jednakże biorąc pod uwagę dynamikę incydentu terrorystycznego, jego skalę i skutki, struktury te największą rolę odegrają w czasie usuwania skutków działań terrorystycznych.

Dotychczas w czasie kryzysu zazwyczaj powoływane były sztaby antykryzysowe. W ich skład wchodzili także specjaliści z konkretnych dziedzin, przydatnych w czasie rozwiązywania sytuacji kryzysowych. To właśnie w sztabach antykryzysowych podejmowane były najważniejsze decyzje polityczne w kwestii działań zmierzających do usuwania skutków ataku. W mojej ocenie, w obecnych uwarunkowaniach, przy sprawnie działających elementach zarządzania kryzysowego prawdopodobnie nie będzie zasadne powoływanie sztabów antykryzysowych organizowanych ad hoc.

Z analizy dokumentów normujących udział Sił Zbrojnych RP w realizacji przedstawionych powyżej etapów przeciwdziałania terroryzmowi wynika jednoznacznie, iż pełnią one jedynie wspierającą rolę i wykorzystywane będą w sytuacjach, kiedy zastosowanie innych środków okaże się niewystarczające.

Analizując akty prawne normujące problematykę użycia Sił Zbrojnych RP na terenie kraju, można wyróżnić cztery zasadnicze grupy zadań możliwe do realizacji przez elementy wydzielone z wojsk lądowych. Są to:

- bezpośrednie wsparcie oddziałów Policji w działaniach antyterrorystycznych;
- ochrona obiektów szczególnie ważnych dla obronności państwa;

- ochrona granicy państwowej w powietrzu;
- usuwanie skutków ataku terrorystycznego o znamionach klęsk żywiołowych i katastrof.

Wszystkie z wymienionych powyżej sytuacji znalazły odzwierciedlenie w „Planie udziału Sił Zbrojnych RP w działaniach antyterrorystycznych".

„Plan użycia oddziałów i pododdziałów SZ RP w przypadku wystąpienia sytuacji kryzysowych" przewiduje realizację zadań związanych z przeciwdziałaniem sytuacjom kryzysowym w trzech zasadniczych fazach:

Faza I – monitorowanie sytuacji w ramach działalności bieżącej.

Faza II – aktywacja sił i środków, reagowanie.

Faza III – usuwanie skutków.

Przedstawione powyżej fazy różnią się nieznacznie od etapów działań antyterrorystycznych, jednakże nie powinno to niekorzystnie wpłynąć na realizację zadań przez wojska lądowe w tym zakresie. W praktyce pierwszy etap działań antyterrorystycznych (rozpoznanie) wpisuje się w fazę I przeciwdziałania sytuacjom kryzysowym. Realizacja drugiego i trzeciego etapu działań antyterrorystycznych (zapobieganie i zwalczanie) nie jest możliwa bez wcześniejszej aktywacji sił i środków – praktycznie etapy te będą realizowane w ramach „reagowania" sił i środków SZ RP. Natomiast usuwanie skutków ataku terrorystycznego realizowane będzie w ramach fazy III przeciwdziałania sytuacjom kryzysowym.

Pododdziały i oddziały **wojsk lądowych mogą być ponadto użyte do wsparcia elementów układu pozamilitarnego w usuwaniu skutków ataku terrorystycznego o znamionach klęsk żywiołowych i katastrof,** przy założeniu, iż realizować będą zadania zgodnie z ich specjalistycznym przygotowaniem i przeznaczeniem. Jednocześnie, ich użycie w sytuacji kryzysowej nie może zagrozić ich zdolności do realizacji zadań konstytucyjnych i wynikających z ratyfikowanych umów międzynarodowych.

W takim przypadku, wydzielone z Sił Zbrojnych RP elementy realizowały będą zadania zgodnie z postanowieniami ustawy o zarządzaniu kryzysowym. Zgodnie z tą ustawą Minister Obrony Narodowej, na wniosek wojewody, może przekazać do jego dyspozycji pododdziały lub oddziały Sił Zbrojnych RP, wraz ze skierowaniem ich do wykonywania zadań z zakresu zarządzania kryzysowego[110].

Zadania możliwe do realizacji przez pododdziały lub oddziały Sił Zbrojnych RP realizowane będą zgodnie z wojewódzkim planem reagowania kryzysowego (uzgodnionym z organem wskazanym przez Ministra Obrony Narodowej) i obejmować mogą:

- współudział w monitorowaniu zagrożeń;
- wykonywanie zadań związanych z oceną skutków zjawisk zaistniałych na obszarze występowania zagrożeń;
- wykonywanie zadań poszukiwawczo-ratowniczych;
- ewakuowanie poszkodowanej ludności i mienia;
- wykonywanie zadań mających na celu przygotowanie warunków do czasowego przebywania ewakuowanej ludności w wyznaczonych miejscach;
- współudział w ochronie mienia pozostawionego na obszarze występowania zagrożeń;
- izolowanie obszaru występowania zagrożeń lub miejsca prowadzenia akcji ratowniczej;
- wykonywanie prac zabezpieczających, ratowniczych i ewakuacyjnych przy zagrożonych obiektach budowlanych i zabytkach;
- prowadzenie prac wymagających użycia specjalistycznego sprzętu technicznego lub materiałów wybuchowych będących w zasobach Sił Zbrojnych RP;
- usuwanie materiałów niebezpiecznych i ich unieszkodliwianie przy

[110] Art. 25 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U.07.87.590).

pomocy sił i środków będących na wyposażeniu wojska;

- likwidowanie skażeń chemicznych oraz skażeń i zakażeń biologicznych;
- usuwanie skażeń promieniotwórczych;
- wykonywanie zadań związanych z naprawą i odbudową infrastruktury technicznej;
- współudział w zapewnieniu przejezdności szlaków komunikacyjnych;
- udzielanie pomocy medycznej i wykonywanie zadań sanitarno-higienicznych i przeciwepidemicznych;
- wykonywanie zadań ujętych w wojewódzkim planie reagowania kryzysowego.

Zadania powyższe, pomimo braku bezpośredniej delegacji do działań antyterrorystycznych mogą być realizowane w czasie usuwania skutków ataku terrorystycznego. Pododdziały lub oddziały Sił Zbrojnych RP mogą być przekazywane do realizacji tych zadań w etatowym składzie lub jako doraźnie tworzone zgrupowania zadaniowe. Muszą być zintegrowane w jedną, jednolicie prowadzoną kampanię cywilno-wojskową, na wzór tych, które w sztuce wojennej od dłuższego czasu nazywamy operacjami połączonymi (joint operations)[111].

Dlatego też, realizacja celów długofalowej „wojny z terroryzmem" wymaga podjęcia działań wielowymiarowych, obliczonych na dłuższy czas i polegających m.in. na:

- stworzeniu trwałej międzynarodowej koalicji, obejmującej jak największą liczbę państw i akceptującej uzgodniony kodeks zasad postępowania wobec organizacji terrorystycznych;
- wewnętrznym konsensusie w krajach rozwiniętych co do stosowania ostrzejszych niż dotąd środków walki z terroryzmem, nawet jeśli to wpłynie w jakiejś mierze na zakres wolności obywatelskich;

- ewolucji nastrojów społeczeństw państw rozwiniętych w kierunku akceptacji ciężaru prowadzenia walki z terroryzmem, łącznie z akceptacją strat wojskowych i wśród ludności cywilnej.

Powinna ona objąć także, działania w następujących płaszczyznach: prawnej; ekonomicznej; instytucjonalnej; wywiadowczej; policyjno-paramilitarnej; dyplomatycznej.

O ile przy pomocy powyższych środków niemilitarnych można utrudnić organizację spektakularnych akcji terrorystycznych, o tyle nie da się ich wykorzystać do skutecznej likwidacji większych grup terrorystycznych i ich infrastruktury oraz wymusić posłuch państw popierających terroryzm. Dlatego też, perspektywa długofalowej ofensywy przeciwko międzynarodowemu terroryzmowi stawia siły zbrojne i ich akcje militarne na równi z innymi quasi-militarnymi lub niemilitarnymi formami działań.

Ocena podejmowanych przez nasz kraj działań na arenie międzynarodowej pozwala stwierdzić, iż Polska jest zagrożona atakami terrorystycznymi w podobnym stopniu jak inne państwa europejskie. Zagrożeniom tym mogą podlegać np. polskie przedstawicielstwa zagraniczne lub kontyngenty wojskowe realizujące misje poza granicami kraju. Zagrożenia związane z terroryzmem odnosi się również do terytorium Polski. Tutaj wyselekcjonować można cztery zasadnicze grupy, które będą najbardziej narażone na ataki terrorystyczne: władze rządowe; wojsko, policja, służby specjalne; przedsiębiorstwa państwowe i prywatne (sfera biznesu); ludność.[112]

Powyższe potencjalne cele ataków terrorystycznych pozwalają wnioskować, iż skuteczne zwalczanie terroryzmu wymagać będzie nowej jakościowo współpracy, prowadzącej do zaniku dotychczasowego wyraźnego podziału na cywilno- policyjne zwalczanie terroryzmu i wojskowe zwalczanie

---

[111] S. Koziej, Powrześniowe wyzwania ..., wyd. cyt., s. 75.
[112] K. Jałoszyński, Terroryzm a wojsko, „Zeszyty Naukowe" 2000 nr 2, s. 192 – 193.

powstań. Mimo przewagi środków militarnych państwo musi pokonać ogromne trudności, aby odnosić sukcesy w asymetrycznych konfliktach z niepaństwowymi przeciwnikami. Przede wszystkim w konflikcie asymetrycznym to właśnie państwo znajduje się w niedogodnej sytuacji. Brak reguł i wyraźnego rozgraniczenia wojny od pokoju rodzi sprzeczności z politycznymi i etycznymi podstawami funkcjonowania państwa, a przez to zagraża porządkowi społecznemu. Przeciwnik niepaństwowy natomiast dzięki niestosowaniu reguł, osiąga wyłącznie korzyści, zwłaszcza dużą swobodę działania. Bowiem świadomość społeczeństw demokratycznych z jednej strony narzuca państwu oraz siłom zbrojnym ograniczenia, które nie dotyczą przeciwnika w konflikcie asymetrycznym[113], natomiast z drugiej stawia określone wymogi co do porządnego poziomu bezpieczeństwa.

Istotnym staje się zatem podejmowanie przez państwo takich działań, które z jednej strony zapewniać będą sprawne funkcjonowanie struktur państwowych, natomiast z drugiej zapewniać będą maksymalne warunki przetrwania społeczeństwa w warunkach zagrożenia terroryzmem. Zestaw prognozowanych celów i działań politycznych państwa obejmować może: zapewnienie maksymalnej zdolności do ciągłego i sprawnego funkcjonowania strategicznie ważnych elementów systemu państwowego; minimalizowanie strat i szkód; samodzielne i we współpracy międzynarodowej ograniczanie swobody działania i likwidowanie organizacji terrorystycznych; podnoszenie odporności systemu państwowego i międzynarodowego na uderzenia terrorystyczne; ograniczanie i likwidowanie społecznych podstaw terroryzmu.[114]

Z powyższych celów oraz działań państwa wynikają możliwe misje, funkcje, role, cele i zadania SZ RP.[115] Do tej grupy zaliczać się będą:

---

[113] Por. M. Wiatr, Walka z terroryzmem ..., wyd. cyt., s. 93-94.
[114] Zob. C. Rutkowski, A. Kasprzewski, A. Dawidczyk, opr. pod krypt. „Adaptacja", cz. 2, AON, Warszawa 1999, s. 78.
[115] Tamże, s. 78-79.

samoochrona /samoobrona SZ; ochrona/ obrona obiektów systemu państwowego / sojuszniczego (samodzielnie lub wsparcie sił poza wojskowych); wsparcie działań poza wojskowych w rozbijaniu/likwidacji grup (organizacji) terrorystycznych; utrzymanie zdolności prewencyjnych i odwetowych; pomoc społeczeństwu w ograniczaniu społecznej bazy terroryzmu.

Do wypełniania wielu z prezentowanych powyżej misji i funkcji powinny być przygotowane wojska lądowe. Bowiem, ważnym miejscem wykorzystania i zaangażowania tego komponentu wydaje się być obszar związany z pełnieniem funkcji ochronnych i obronnych (np. strategicznie ważnych obiektów, które mogą stać się celami ataków) oraz dotyczący likwidacji grup terrorystycznych podczas uderzeń lub przed ich wykonaniem.

W pierwszym z wymienionych obszarów wojska lądowe mogą wykonywać następujące zadania:

- ochrona i obrona obiektów zagrożonych atakami grup terrorystycznych i przestępczych;
- izolowanie rejonów(obszarów), w których mogą bazować grupy terrorystyczne i przestępcze;
- blokowanie kierunków możliwego przenikania terrorystów i grup przestępczych;
- sukcesywne zdobywanie informacji o możliwych atakach z jednostek (oddziałów) wyspecjalizowanych w działaniach antyterrorystycznych.[116]

Z powyższego wynika, iż do tego typu zadań mogą być użyte jednostki, które nie są wyspecjalizowane w tego typu działaniach. Wydaje się jednak, że w szkoleniu wojsk - szczególnie wojsk zmechanizowanych - należy uwzględnić zagadnienia związane z przygotowaniem do tego typu

[116] Zob. B. Szulc, Zadania wojsk lądowych w walce z terroryzmem [w:] Operacje i zadania wojsk lądowych na obszarze kraju, pod kier. A. Tomaszewskiego, AON, Warszawa 2001, s. 142.

działań. Zauważyć należy, iż działalność terrorystyczna może nasilać się w okresie konfliktu zbrojnego. Dlatego też, do tego typu działań należy przewidywać odpowiednie dowody, składające się z dobrze wyszkolonych żołnierzy mogących szybko i skutecznie wykonać wymienione zadania.

W likwidacji grup terrorystycznych i przestępczych (drugi z wymienionych obszarów) wiodącą rolę pełnić będą wyspecjalizowane pododdziały antyterrorystyczne Policji oraz sił zbrojnych (np. GROM). Nie ulega wątpliwości jednak, że jednostki wojsk lądowych w tym wypadku wykonywać będą zadania izolująco –blokujące, które polegać będą na:

- osłonie obiektów militarnych oraz użyteczności publicznej;
- organizowaniu blokad na możliwych kierunkach podejść grup terrorystycznych i przestępczych;
- udziale w okrążeniu grup w przypadku ich lokalizacji;
- organizowaniu blokad na kierunkach wycofywania grup po wykonaniu uderzeń;
- wykonywaniu ataków na bazy terrorystów wspólnie z wyspecjalizowanymi oddziałami.[117]

W realizacji ostatniego z wymienionych zadań pododdziały wojsk lądowych mogą jednak spełniać jedynie funkcję pomocniczą. Zauważyć jednak należy, iż w przypadku konfliktu zbrojnego, przy nasileniu ataków grup tego typu, jednostki wyspecjalizowane nie będą prawdopodobnie w stanie przeciwdziałać licznym atakom. Należy zatem przypuszczać, iż wojska lądowe w obszarze swoich działań będą zmuszone do podjęcia samodzielnej walki z takimi oddziałami, stąd też pojawia się konieczność przygotowania, już na szczeblu taktycznym, pododdziałów zdolnych do podjęcia takiej walki.[118]

---

[117] Tamże, s. 143.
[118] Tamże, s. 144.

Wnioski

Ograniczenia czasowe możliwości użycia wydzielonych elementów Sił Zbrojnych do działań na obszarze kraju wynikają z szeregu różnych czynników. Jednym z nich, dotyczącym nie tylko wojsk lądowych, ale całych Sił Zbrojnych jest bardzo ograniczona możliwość przewidzenia terminu, miejsca i rodzaju sytuacji nadzwyczajnej. Aby zminimalizować czas reakcji, niezbędna jest ścisła współpraca wszystkich narodowych służb odpowiedzialnych za rozpoznawanie, zapobieganie i przeciwdziałanie rozwojowi kryzysu.

Nierównomierne rozmieszczenie na terenie kraju jednostek wojskowych, powoduje określone ograniczenia przestrzenne ich użycia. Powyższa sytuacja wymusza konieczność przemieszczenia oddziałów i pododdziałów, rozlokowanych w różnych garnizonach na terenie kraju, do rejonów gdzie wystąpi sytuacja kryzysowa. Wymusza to konieczność utrzymywania w gotowości do użycia niezbędnej liczby środków transportu. Nie stanowi to większego problemu w przypadku środków niezbędnych do transportu ludzi, gdyż jednostki wojskowe posiadają dużą autonomiczność w zakresie mobilności. Znacznie gorzej przedstawia się sytuacja w przypadku transportu sprzętu ciężkiego możliwego do wykorzystania w czasie usuwania skutków sytuacji nadzwyczajnych (pływające transportery samobieżne, spycharki gąsienicowe, wozy zabezpieczenia technicznego na gąsienicach.

Dodatkowym czynnikiem ograniczających możliwość wyboru sił i środków do działań w sytuacjach kryzysowych są nasze **zobowiązania sojusznicze** i koalicyjne, a w szczególności poziom zaangażowania wojsk lądowych w misjach poza granicami kraju. Aktualnie w różnego rodzaju misjach i operacjach poza granicami kraju uczestniczy około ok. 3,5 tys. żołnierzy, co stanowi ok. 2 % całego stanu naszej armii. Jednakże, jeżeli weźmiemy pod uwagą fakt, iż w tym samym czasie taka sama ilość żołnierzy

odtwarza zdolność bojową po udziale w misjach, a kolejne 3,5 tys. przygotowuje się do udziału w kolejnych zmianach – otrzymujemy liczbę ok. 7,5 tys. żołnierzy, czyli ok. 6% stanu Sił Zbrojnych RP częściowo wykluczonych z możliwości wykorzystania do innych działań.

Wydawać by się mogło, iż nie są to znaczące liczby w skali kraju, jednakże nabierają one innej wymowy, jeżeli uświadomimy sobie, że w operacjach poza granicami kraju biorą udział przede wszystkim najlepiej wyszkoleni żołnierze naszych elitarnych jednostek wojskowych.

4. SOJUSZNICZE ASPEKTY W ZARZĄDZANIU BEZPIECZEŃSTWEM MILITARNYM

Dokonując obserwacji w zakresie szeroko rozumianego bezpieczeństwa w obszarze narodowym, jak też międzynarodowym jesteśmy świadkami szeroko idących przemian. Zmiany, jakie dokonały się w sferze polityczno – militarnej i społecznej w Europie i na świecie na przełomie XX i XXI wieku zapoczątkowały wiele ważnych procesów. W Polsce obok gruntownych przemian w obszarze gospodarczym i społecznym rozpoczęły się zmiany związane z przebudową systemu obronnego państwa oraz dostosowanie jego kształtu i możliwości do nowych uwarunkowań i potrzeb. Wstąpienie Polski do NATO i Unii Europejskiej spowodowało przyjęcie nowej koncepcji bezpieczeństwa, opartej na siłach i środkach własnych, wzajemnych zobowiązaniach wynikających z członkostwa w NATO i Unii Europejskiej oraz dwustronnych stosunkach Polski ze Stanami Zjednoczonymi.

Polityka bezpieczeństwa militarnego Polski realizowana jest jednocześnie w kilku płaszczyznach, które obejmują: działania narodowe, działania integracyjne i współpracę w ramach NATO, UE, ONZ. Polska jako członek NATO i UE dysponująca solidnymi gwarancjami bezpieczeństwa militarnego, przyjęła kierunki polityki obronnej opartej na:

- członkostwie w Sojuszu Północnoatlantyckim;
- integracji z Unią Europejska;
- koalicji ze Stanami Zjednoczonymi Ameryki Północnej;

Mając powyższe na uwadze w rozdziale tym zaprezentowano wnioski i wyniki badań uzyskane w procesie poszukiwania odpowiedzi na kolejny problem szczegółowy wyrażający się w postaci następującego pytania: *jakie*

aspekty sojusznicze stanowią o potrzebie podejmowania wysiłków na rzecz bezpieczeństwa militarnego?

4.1. Podstawowe uwarunkowania międzynarodowego bezpieczeństwa militarnego

Obecne usytuowanie Polski na współczesnej politycznej mapie bezpieczeństwa (członkostwo w NATO, Unii Europejskiej, czy zawiązana współpraca z USA) wymaga nowego spojrzenia na system bezpieczeństwa militarnego. Jedną z podstawowych przesłanek zmian w założeniach owego systemu jest wzrastający poziom międzynarodowego zaufania i współpracy na rzecz ogólnego bezpieczeństwa. Należy jednak dostrzegać, że mimo wzrostu poziomu międzynarodowego zaufania i bezpieczeństwa, współczesny świat jest niejednorodny. Analizując współczesne zagrożenia dochodzi się do wniosku, iż nie są one przewidywalne do końca.

4.1.1. Współczesne zagrożenia w aspekcie bezpieczeństwa militarnego

Międzynarodowe środowisko bezpieczeństwa podlega ciągłej ewolucji i pojawiają się nowe zagrożenia – jakościowo i ilościowo odmienne od konwencjonalnych i tradycyjnych wyzwań XX wieku. Wobec zagrożeń, wywoływanych między innymi przez radykalny fundamentalizm, międzynarodowy terroryzm i ponadnarodowe siatki przestępcze.

Współczesne wyzwania w dziedzinie bezpieczeństwa wynikają głównie z przemian, jakie dokonały się na kontynencie europejskim w ciągu ostatnich lat. Ryzyko wojny konwencjonalnej na dużą skalę zmniejszyło się radykalnie, ale równocześnie nastąpiła znacząca dywersyfikacja i globalizacja zagrożeń. Obecnie w otoczeniu Polski nie występują zagrożenia dla jej suwerenności, stabilności wewnętrznej i pozycji międzynarodowej.

Zagrożenie militarne nie wynika tylko z faktu posiadania przez naszych sąsiadów określonego potencjału militarnego. Należy się liczyć, że w wypadku konfliktu będą oni mogli tego potencjału użyć w celu rozstrzygnięcia sporu na swoją korzyść. Analiza stanu potencjału państw sąsiadujących pozwoli na wygenerowanie wniosków o skali możliwego zagrożenia, w jakim może się znaleźć Polska. Wartości potencjałów militarnych państw sąsiadujących w odniesieniu do stanu naszego potencjału przedstawia tabela nr 4.1.

Tabela 4.1.

LIMITY CFE-1[119]

KRAJ	ŻOŁNIERZE	CZOŁGI	BWO	ARTYLERIA	SAMOLOTY	ŚMIGŁOWCE
POLSKA	234000	1730	2150	1610	460	130
BIAŁORUŚ	100000	1800	2600	1615	294	80
UKRAINA	450000	4080	5050	4040	1090	330
ROSJA*	11450000	6350	11280	6315	3416	855
NIEMCY	345000	4069	3281	2445	900	280
SŁOWACJA	46667	478	683	383	100	40
CZECHY	93333	957	1367	767	230	50

* Na terytorium objętym CFE-1

Przedstawione wyżej porównanie potencjałów rażenia nie oddaje prawdziwego obrazu sytuacji, a zwłaszcza czynnika mogącego doprowadzić do konfliktu zbrojnego. Obecnie w ocenie teoretyków wojskowych nie ma państwa lub grupy państw, które w perspektywie najbliższych lat mogłyby stanowić konwencjonalne zagrożenie dla NATO, czy UE któremu wymienione organizacje nie mógłby się skutecznie przeciwstawić. Reasumując w perspektywie krótko- i średnioterminowej prawdopodobieństwo wystąpienia konfliktu zbrojnego na dużą skalę jest znikome.

---

[119] Polska Zbrojna, nr 31/2007, s. 39.

Zmniejszeniu zagrożenia wojną globalną lub kontynentalną towarzyszy wzrost liczby kryzysów lokalnych, przeradzających się niejednokrotnie w konflikty lokalne lub regionalne. Ich źródła są różnorodne: waśnie etniczne i religijne, spory graniczne, naruszenia praw człowieka, katastrofy naturalne i wywołane działalnością człowieka, niedobór podstawowych środków do egzystencji, zapaść gospodarczo-cywilizacyjna, osłabienie lub rozpad struktur państwowych itp. Naruszając zarówno rzeczywiste, jak i subiektywne poczucie bezpieczeństwa, stanowią one poważne źródło destabilizacji.

Coraz większego znaczenia natomiast nabiera ewolucja zagrożeń – od podmiotowych do przedmiotowych. Współcześnie coraz trudniej jest określić podmioty będące źródłem zagrożeń (państwo, organizacja lub grupa społeczna), ważniejsze stają się warunki i czynniki generujące potencjalne zagrożenia oraz obszary ich występowania, np. obszar postsowiecki, Bałkany, Bliski Wschód i Afryka Północna. Poprzez coraz to szersze otwarcie granic, pojawia się olbrzymia przestrzeń, w której wewnętrzne i zewnętrzne aspekty bezpieczeństwa stały się trudne do podziału. Wśród zjawisk determinujących zmiany w środowisku bezpieczeństwa należy wymienić także zagrożenia płynące ze strony państw słabych i „państw w stanie rozkładu" oraz podmiotów pozapaństwowych.

Robert Scales w wydanej przez U.S. Army War College w Pensylwanii książce „Przyszła wojna" (Future Warfare) wyodrębnia 5 źródeł konfliktów, mających stanowić zagrożenie pokoju światowego w pierwszych dekadach XXI wieku[120]. Do źródeł tych zalicza:

- podziały biedny – bogaty;
- problemy etniczne;
- walkę o dominację;

---

[120] R.Scales, *Future warfare*, U.SS. Army War College, Carlislr Barraks 1999.

- przeciwstawne interesy ekonomiczne;
- walkę o strefy surowców naturalnych.

Współcześnie towarzyszą nam zagrożenia, które są związane, przede wszystkim z napięciami i niestabilnością wywoływanymi przez terroryzm międzynarodowy, rozprzestrzenianiem broni masowego rażenia oraz nieprzewidywalną polityką reżimów autokratycznych. Polska, jak każdy inny członek wspólnoty euroatlantyckiej, jest wystawiona na bezpośrednio związane z nimi zagrożenia. Wyzwania dla bezpieczeństwa wiążą się z opóźnieniami rozwojowymi, ubóstwem, degradacją środowiska naturalnego, chorobami, niekontrolowaną migracją, napięciami etnicznymi, kurczącymi się zasobami naturalnymi, jak również związane są z osłabieniem możliwości regulacyjnych państw i organizacji międzynarodowych z powodu pogłębiającej się polaryzacji poziomu rozwoju i życia pomiędzy krajami bogatymi a biednymi i rosnącej na tym tle frustracji i niezadowoleniem społecznym.

W obecnym stuleciu jednym z zasadniczych wyzwań dla szeregu państw oraz ich systemów bezpieczeństwa będzie skuteczne przeciwdziałanie oraz efektywna reakcja na nabierające coraz wyraźniejszych kształtów i groźniejszych form – zagrożenia asymetryczne. Rangę oraz znaczenie tych zagrożeń, a szczególnie możliwość ich potencjalnego, ale i realnego destrukcyjnego oddziaływania na państwo i jego obywateli, zaczęło dostrzegać coraz większe grono krajów i organizacji międzynarodowych.

Oceniając możliwości wystąpienia zagrożenia bezpieczeństwa międzynarodowego zasadne wydaje się potwierdzenie opinii wielu specjalistów, którzy uznają, że będą to w większości zagrożenia asymetryczne. W opinii K. Piątkowskiego do charakterystycznych cech wojny asymetrycznej należą[121]:

---

[121] K. Piątkowski, Wojna nowego typu? Polska w Europie, Warszawa 2002, s. 12.

- **cele** – prowadzący wojnę asymetryczną nie ogranicza ataku do potencjału militarnego przeciwnika, z założenia uznając za cel całość jego terytorium, społeczeństwa i zasobów. Preferowane są cele, których rażenie przyniesie największy efekt psychologiczny;
- **organizacja** - wojny asymetrycznej nie muszą prowadzić siły zbrojne. Bez względu na to, czy jest ona inspirowana, wspierana czy prowadzona przez jakieś państwo lub na jego zlecenie, wykonawcą uderzeń asymetrycznych są grupy zakonspirowane na terytorium przeciwnika;
- **technika** - bronią w wojnie asymetrycznej może być wszystko: uzbrojenie konwencjonalne (broń, materiał wybuchowy, przenośne wyrzutnie rakiet), broń masowego rażenia (ładunki jądrowe, biologiczne, chemiczne), niekonwencjonalne (samolot pasażerski, samochód-pułapka);
- **metody działania** - im dany sposób działania ma mniej wspólnego z prowadzeniem konwencjonalnych operacji wojskowych, tym większe jest prawdopodobieństwo, że zostanie wykorzystany przez podmiot prowadzący działania asymetryczne - przenikanie w struktury terytorialne społeczeństwa, stosowanie metod opartych na działaniach partyzanckich, kryminalnych itp.;
- **zasięg** - w przeciwieństwie do „zwykłych" działań terrorystycznych, wojna asymetryczna wyróżnia się skalą i zasięgiem działania. Nie jest on ograniczony geograficznie – przeciwnik jest atakowany zarówno na swoim terytorium, jak też w każdym punkcie globu, gdzie znajdują się jego obywatele lub zasoby. To samo dotyczy skali działań – z założenia mają być intensywne.

Istota zmian we współczesnym środowisku bezpieczeństwa polega, zatem na przesuwaniu się punktu ciężkości z zagrożeń klasycznych (inwazja zbrojna), których rola się zmniejsza, na zagrożenia

asymetryczne, których źródłem stają się także trudne do zidentyfikowania podmioty pozapaństwowe.

Obecnie **żadne zagrożenie nie jest czysto militarnym przedsięwzięciem i nie może być pokonane tylko przez czysto militarne środki**. Każde z tych zagrożeń wymaga, bowiem posiadania i współdziałania różnych instrumentów w skali państwa i społeczności międzynarodowej[122].

4.1.2. Strategie i koncepcje bezpieczeństwa międzynarodowego

Współcześnie bezpieczeństwo międzynarodowe i narodowe nie jest zjawiskiem statycznym. Analiza konfliktów militarnych na przełomie XX i XXI wieku wskazuje, iż jest to proces wysoce dynamiczny. Do historii można zaliczyć prosty dwubiegunowy system (okres zimnej wojny), oparty nie tyle na równowadze sił (równowagi takiej nigdy nie było), co na równowadze strachu. Bezpieczeństwo międzynarodowe odznaczało się w tym okresie znaczną stabilnością, której towarzyszyło wysokie ryzyko wybuchu wojny jądrowej. Wraz z zakończeniem zimnej wojny ten stan rzeczy należy do przeszłości.

Bezpieczeństwo międzynarodowe nie jest kategorią pojęciową dającą się jednoznacznie zdefiniować. Kiedy przyjmie się, że bezpieczeństwo sojuszu jest stanem niezagrożenia, umożliwiającym bezpieczną egzystencję i rozwój, wówczas możemy przyjąć, że zapewnienie bezpieczeństwa dotyczy ochrony (obrony) przed istniejącymi lub przewidywanymi zagrożeniami. Zadanie zapewnienia państwu, sojuszowi bezpieczeństwa oznacza w konsekwencji zapewnienie pokoju[123].

Rozpatrując kwestie bezpieczeństwa w nauce i praktyce stosunków międzynarodowych, można uznać, iż bezpieczeństwo to stan, w którym

---

[122] Por. J. Kaczmarek, Współczesne bezpieczeństwo, Warszawa 2008, s.20.
[123] Por. M. Carnovale, Partnerzy i sojusznicy NATO, Stosunki cywilno - wojskowe i demokratyczna kontrola nad armią, Bliżej NATO, zeszyt 3, Warszawa 1998, s. 18.

państwa mają poczucie pewności, że brak jest groźby ataku militarnego, politycznych presji, nacisku gospodarczego, zagrożenia ekologicznego czy utraty istotnych wartości kulturowych i tożsamości kulturowych i tożsamości narodowych, co stanowiłoby przeszkodę dla rozwoju państw, współpracy międzynarodowej i utrzymania pokoju.

Rozpatrywane kwestie związane z pojęciem zewnętrznego bezpieczeństwa państwa, stanowią kategorię zmienną w czasie, jest jednak ściśle związana ze stanem stosunków międzynarodowych oraz dominującymi w tym obszarze strategiami politycznymi zagranicznych państw. Cel działania poszczególnych państw w obszarze bezpieczeństwa powinien być ukierunkowany w głównej mierze na ochronę przed istniejącymi potencjalnymi zagrożeniami, zdolnością narodu do ochrony jego wewnętrznych wartości przed zewnętrznymi zagrożeniami.

Właściwe projektowanie polityki bezpieczeństwa międzynarodowego i narodowego, powinno uwzględniać współczesny i dający się przewidzieć w przyszłości charakter zagrożeń takowego bezpieczeństwa. Prowadzone analizy zagrożeń wskazują, że dziś jest małe prawdopodobieństwo wybuchu światowej wojny – konfliktu militarnego na szeroką skalę, czy światowej wojny nuklearnej, ale też jest bardzo niski stopień stabilności. Od wielu lat utrzymuje się stan niepewności i co gorsza – nieprzewidywalności. Wydarzenia z 11 września 2001 pogłębiły ten stan rzeczy. Dla nikogo nie powinno być tajemnicą, że w zglobalizowanym świecie, typowe zagrożenia militarne ustępują pola zagrożeniom asymetrycznym i przyrastającym na sile zagrożeniom terrorystycznym.

Poszukując odpowiedniego antidotum na dostrzeżone zagrożenia należy wyjść z generalnego założenia, iż obecnie bezpieczeństwo nie może być tylko kwestią narodową. Istnieje potrzeba globalnego podejścia do problemu i na filarach międzynarodowego systemu bezpieczeństwa można budować skuteczne narodowe systemy bezpieczeństwa. W świecie

globalnych zagrożeń współpraca międzynarodowa staje się warunkiem koniecznym zachowania pokoju, bezpieczeństwa międzynarodowego i narodowego. Klasyczny bowiem podział na wewnętrzne i zewnętrzne aspekty bezpieczeństwa dawno przeszedł do historii.

Główne założenia ONZ bezpieczeństwo międzynarodowe ukazują jako sumę i rezultat bezpieczeństwa każdego oddzielnie i wszystkich państw członkowskich razem wziętych. Przedstawiana koncepcja bezpieczeństwa międzynarodowego zbudowana jest na idei współdziałania państw współtworzących system. Fundamentem owych założeń jest zasada zbiorowej samoobrony, agresja (napad) wobec któregokolwiek z uczestników systemu uważany jest za napad na wszystkich pozostałych i zobowiązuje do przyjścia z pomocą w rozwiązaniu sytuacji kryzysowej. Koncepcja wspólnego bezpieczeństwa zakłada partnerstwo i przymus współdziałania w rozwiązywaniu sporów międzynarodowych. Wspólne bezpieczeństwo tworzy strukturę umożliwiającą zmniejszenie napięć i redukcję czynników konfliktogennych oraz groźbę wojny[124].

Koncepcja strategiczna Sojuszu NATO zakłada stałe utrzymanie zdolności użycia swoich sił w rejonie konfliktu i kryzysu. W głównych założeniach owej koncepcji zawarte jest między innymi: skuteczność działań wojskowych w każdych dających się przewidzieć okolicznościach stanowi podstawę zdolności Sojuszu do zapobiegania konfliktom, reagowania na kryzys oraz organizowania operacji reagowania kryzysowego nie ujętych w Artykule 5. Operacje te mogą stwarzać poważne wyzwania wymagające jednocześnie dużych umiejętności politycznych i wojskowych do wspólnych wielonarodowych działań[125]. W przypadku kryzysów mogących prowadzić do militarnego zagrożenia bezpieczeństwa państw NATO, siły zbrojne Sojuszu

---

[124] http://www. un.org, http://www.unic.un.org.pl

[125] NATO w systemie bezpieczeństwa euroatlantyckiego, Materiały do studiowania oprac., H. Binkowski i inni, Warszawa 2004, s. 145.

mogą uzupełnić lub wzmocnić działania polityczne w ramach szerokiego podejścia do problemu bezpieczeństwa, przyczyniając się w ten sposób do opanowania kryzysów i ich pokojowego rozwiązywania[126].

Europejska strategia bezpieczeństwa jest także ukierunkowana na zapobieganie i rozwiązywanie konfliktów. W swoich założeniach uwzględnia nie tylko uwarunkowania militarne i polityczne, ale również te o charakterze ekonomicznym, społecznym i międzykulturowym. Strategia ta odniesie sukces wyłącznie wtedy, gdy dokonana zostanie całościowa analiza zagrożeń oraz zostanie ustalona wspólna definicja. Pozwoli to na wyznaczenie strategicznych celów wspólnych dla wszystkich państw Unii (jak to zaproponował, były generał armii francuskiej w stanie spoczynku, Philipe Morillon). Wiarygodność UE będzie zależała również w znacznym stopniu od zdolności do posiadania odpowiedniego potencjału militarnego, który będzie sfinansowany z budżetu wspólnotowego.

Zapewnienie **bezpieczeństwa narodowego**, nazywanego również **bezpieczeństwem państwa**[127], jest jedną z podstawowych funkcji każdego kraju, obejmującą problematykę przeciwstawiania się wszelkim zewnętrznym oraz wewnętrznym zagrożeniom jego istnienia i rozwoju. Całość ujęcia bezpieczeństwa państwa powinno obejmować **aspekty wewnętrzne i zewnętrzne**[128]**.** Jest to uwarunkowane potrzebami bezpieczeństwa wewnątrz struktury społeczeństwa, jak również funkcjonowaniem i ewolucją środowiska międzynarodowego, w którym powstają różnorodne zagrożenia i wyzwania. Biorąc pod uwagę fakt, że powszechnie pojmowane bezpieczeństwo ma bezpośredni związek z zagrożeniami zewnętrznymi, dlatego wiodące znaczenie jest przypisywane polityce zagranicznej kraju

---

[126] J. Kaczmarek: NATO - Polska 2000, Wrocław 1999, s. 52.

[127] Do czynników wpływających na bezpieczeństwo państwa zaliczamy: położenie geopolityczne, gospodarkę, politykę, siły zbrojne, zagrożenia militarne, zagrożenia pozamilitarne, świadomość obywateli i ekologię, Por. K. Malak, Bezpieczeństwo i obronność państwa. Warszawa 1998, s. 87.

[128] L. Freedman, The Concept of Security. [w:] M. Hawkesworth, M. Kogan, Encyclopedia of Government and Politics, Vol. 2. London-New York 1992, s. 733.

w całokształcie przedsięwzięć zmierzających do ochrony jego suwerenności[129].

Z początkiem lat dziewięćdziesiątych, kiedy Polska znalazła się w zupełnie nowej sytuacji. Wokół pojawiły się nowe państwa: zjednoczone Niemcy, podzielone Czechy i Słowacja, niepodległe: Ukraina, Białoruś i Litwa oraz zmieniona ustrojowo Rosja. W tym też okresie Polska przechodziła czas transformacji politycznej, militarnej i gospodarczej. Równolegle z tymi przemianami Rzeczpospolita Polska dążyła do zapewnienia sobie bezpieczeństwa w ramach **euroatlantyckich struktur bezpieczeństwa międzynarodowego** (NATO i Unia Europejska).

Ostatnimi czasy poziom bezpieczeństwa europejskiego oparty na **Sojuszu Północnoatlantyckim**, został wzmocniony poprzez jego rozszerzenie, co zwiększyło jednocześnie obszar demokracji i stabilności na kontynencie europejskim. Należy jednak podkreślić, że wejście Polski w struktury NATO nie było celem ostatecznym. Jest etapem i jednym z zadań strategicznych na drodze do zapewnienia możliwości pewniejszego i łatwiejszego osiągnięcia celu nadrzędnego, jakim dla każdego państwa jest zagwarantowanie bezpieczeństwa narodowego, jego prawa do życia w pokoju, suwerenności, nienaruszalności terytorialnej i rozwoju ekonomicznego. Ponieważ Europa nie stoi już w obliczu niebezpieczeństwa wojny na dużą skalę, zadanie Polski polega na zbudowaniu odpowiedniego **potencjału obronnego** czasu pokoju[130].

W celu utrzymania stabilności w rejonie i zapewnienia bezpieczeństwa w różnorodnych zagrożeniach, które niespodziewanie mogą pojawić się w przyszłości, Polska musi w ramach struktur NATO, ONZ i UE utrzymać silny, odpowiednio finansowany potencjał obronny[131]. Zarówno

---

[129] J. Kukułka, R. Zięba, Polityka zagraniczna państwa, Warszawa 1992, s. 64-69.
[130] S. Kępka, Uwarunkowania i zagrożenia bezpieczeństwa państwa w świetle aktualnej sytuacji międzynarodowej, Wrocław 2004, s. 328.
[131] Polska polityka obronna oraz struktury SZ RP w warunkach rozszerzenia NATO, Warszawa 1997, s. 15.

ONZ, Sojusz Północnoatlantycki, jak i Unia Europejska realizują dwutorową strategię promocji stabilności w całym świecie (Europie) przyjmując nowych członków i oferując wieloaspektowe formy współpracy tym państwom, których członkostwo w NATO lub UE nie jest jeszcze możliwe. Przyjęta strategia odzwierciedla potrzebę kontynuacji rozszerzenia, ale bez osłabienia wewnętrznej zdolności działania instytucji.[132] Środowisko bezpieczeństwa w Europie i wokół Europy nadal ulega zmianom. Pozytywnie wpływają na nie przemiany związane z postępującą integracją europejską i euroatlantycką oraz pogłębiającą się współpracą regionalną w Europie, a także z transformacją w państwach, które rozpoczęły reformy demokratyczne i wolnorynkowe.

Głównym przesłaniem (założeniem) Strategii Bezpieczeństwa Narodowego RP z 2007 r. jest **zapewnienie bezpieczeństwa państwa w nowych warunkach międzynarodowych. Powyższe założenia wymagają zwiększonej aktywności w sferze polityki zagranicznej**[133]. W szczegółach chodzi tu o takie działania, jak[134]:

- dbanie o sprawność mechanizmów sojuszniczych (zwłaszcza o funkcjonowanie Paktu Północnoatlantyckiego, który określany jest nadal jako najważniejsza gwarancja zewnętrznego bezpieczeństwa i stabilnego rozwoju naszego kraju);
- troska o zapewnienie skuteczności instytucji międzynarodowych i prawa międzynarodowego (głównie Organizacja Narodów Zjednoczonych, Unia Europejska, Organizacja Bezpieczeństwa i Współpracy w Europie);
- zachowanie przyjaznych stosunków z krajami sąsiedzkimi (nie można bowiem – nawet w okresie funkcjonowania w „globalnej

---

[132] P. Schmidt, Rozłącznie ale nie odrębnie. [w:] Przegląd NATO, Większa sprawność i lepsza równowaga. Bruksela 2000, s. 12.
[133] http:// www.wp.mil.pl, Strategia bezpieczeństwa narodowego RP, Warszawa 2007.
[134] Tamże.

wiosce" – gubić z oczu najbliższego otoczenia) oraz partnerskimi (tu szczególna rola przypada Stanom Zjednoczonym, które zaraz po NATO wymienia się jako najważniejszego gwaranta naszego bezpieczeństwa);

- wspieranie procesów transformacji w Europie Wschodniej i Południowej;
- udział w umacnianiu mechanizmów kontrolnych w dziedzinie nieproliferacji broni masowego rażenia;
- utrzymywanie gotowości do uczestnictwa w akcjach zapobiegania konfliktom i utrzymania pokoju;
- udział w działaniach na rzecz promocji demokracji i poszanowania praw człowieka.

W interesie Polski leży współkształtowanie systemu bezpieczeństwa międzynarodowego, który będzie coraz efektywniej eliminować zagrożenia militarne i sprzyjać budowie równowagi interesów oraz współpracy międzynarodowej w rozwiązywaniu globalnych problemów i wyzwań. Podstawową zasadą polityki bezpieczeństwa naszego państwa jest traktowanie Europy i Ameryki Północnej jako jednolitego obszaru bezpieczeństwa. Tworzony żmudnie system bezpieczeństwa europejskiego może stać się w przyszłości głównym gwarantem suwerenności i niepodległości Rzeczypospolitej.

Polska będzie nadal kontynuować politykę aktywnego zaangażowania w sprawy utrzymania międzynarodowego pokoju i bezpieczeństwa zarówno w skali regionalnej, jak i globalnej. Wyrazem gotowości do odgrywania odpowiedzialnej roli międzynarodowej jest nasze duże zaangażowanie w proces stabilizacji w Iraku i Afganistanie. Podjęcie się stabilizacyjnej funkcji w Iraku i bezpośredniej walki z terroryzmem i stabilizacją sytuacji w Afganistanie podnosi pozycję międzynarodową Polski, a należyte wykonanie powierzonych zadań jest źródłem dodatkowego prestiżu, utrwala

obraz Polski jako odpowiedzialnego i solidarnego partnera na arenie międzynarodowej. Polska ma jednocześnie świadomość, że aktywna rola w koalicji antyrrorystycznej może wystawiać kraj na ryzyko ataków i wrogich akcji ze strony ugrupowań, którym społeczność międzynarodowa wydała walkę[135].

Konstatując, **założenia polityki bezpieczeństwa narodowego i międzynarodowego nakłada na nasze Siły Zbrojne RP zobowiązanie do udziału w różnego rodzaju operacjach militarnych (wojennych i poniżej progu wojny) w ramach potrzeb rozwiązania zaistniałej sytuacji kryzysowej pod egidą organizacji stojących na straży bezpieczeństwa typu ONZ, NATO, UE. Stąd też istnieje potrzeba wydzielania komponentów narodowych w różnym wymiarze ilościowo-jakościowym, w zależności od zadań i okoliczności ich realizacji.**

Obecność naszych kontyngentów w składzie wielonarodowych sił zadaniowych oraz w ramach reagowania kryzysowego, to olbrzymi narodowy wkład w utrzymanie bezpieczeństwa międzynarodowego, a tym samym bezpieczeństwa narodowego.

4.2. Sojusze polityczno-militarne w zarządzaniu bezpieczeństwem militarnym

Tworzenie koalicji, wchodzenie w sojusze, zawiązywanie aliansów i przymierzy to najstarsze metody polityki zagranicznej. To także historycznie najdawniejsze formy organizacji sceny międzynarodowej i współpracy państw. Za ich pośrednictwem państwa wzmacniały swoje możliwości i zapewniały ochronę swoich interesów[136].

Początkowo koalicje, sojusze zawiązywano na czas wojny, zaś po jej zakończeniu z reguły się rozwiązywały. Dokonujące się zmiany w obszarach

---

[135] http:// www.wp.mil.pl, Strategia bezpieczeństwa narodowego RP, Warszawa 2007.
[136] B. Balcerowicz, Siły zbrojne w państwie i stosunkach międzynarodowych, Warszawa 2006, s. 72.

polityczno-militarnych spowodowały, iż współcześnie możliwości (potencjał militarny) jednego państwa są zbyt małe, aby skutecznie przeciwdziałać jawiącym się niebezpieczeństwom (zagrożeniom). Aktualny międzynarodowy charakter możliwych zagrożeń sprawia, iż do ich neutralizacji potrzebne są siły i środki wielu państw, czyli organizacje także o charakterze międzynarodowym.

Współcześnie większość rozwiniętych państw swoje bezpieczeństwo (w tym bezpieczeństwo militarne) upatruje w przynależności do sojuszy i koalicji. O bezpieczeństwie Polski również stanowi fakt przynależności do struktur NATO i UE oraz szerokiej współpracy militarnej ze Stanami Zjednoczonymi. Kierunek takiej polityki spotyka się z ogólną aprobatą społeczeństwa, ponieważ przynależność i tylko aktywny udział w wymienionych koalicjach i sojuszach może dawać poczucie bezpieczeństwa. Rodzima polityka bezpieczeństwa akcentuje potrzebę zacieśniania współpracy międzynarodowej w zapewnieniu bezpieczeństwa także bezpieczeństwa militarnego.

4.2.1. Sojusz Północnoatlantycki NATO

Istotą Sojuszu NATO jest wspólne i równoprawne działanie państw członkowskich w celu zagwarantowania sobie, środkami politycznymi i militarnymi, bezpieczeństwa, zgodnie z zasadami Karty Narodów Zjednoczonych. Sojusz bazuje na wyznawaniu wspólnych wartości demokracji, praw człowieka i praworządności. Główną zasadą jego działania jest współpraca suwerennych państw, oparta na niepodzielności bezpieczeństwa wszystkich członków. Decyzje w NATO podejmowane są na zasadzie jednomyślności. Podstawą prawną i traktatową NATO jest Traktat Północnoatlantycki oparty na art. 51 Karty Narodów Zjednoczonych, mówiącym o niezbywalnym prawie każdego państwa do samodzielnej

i zbiorowej obrony [137]. System obrony zbiorowej opiera się na ścisłej współpracy politycznej członków oraz potencjale militarnym utrzymywanym na podstawie wspólnego planowania obronnego i zintegrowanej struktury dowodzenia. W Sojuszu Północnoatlantyckim NATO można wyróżnić trzy kategorie instytucji (zał. 10.): **polityczne organy kierowania, organy wojskowe i administrację**. Główną zasadą funkcjonowania organizacji są konsultacje, wymiana poglądów i ocena bieżąca sytuacji polityczno-militarnej. Wśród zasad, na których została skonstruowana struktura organizacyjna Sojuszu, można wymienić trzy najważniejsze[138]:

- całkowita suwerenność państw członkowskich;
- jednomyślność w podejmowaniu najważniejszych decyzji;
- oddzielne struktury polityczne od zintegrowanej struktury dowodzenia.

Głównym dokumentem funkcjonowania NATO jest **koncepcja strategiczna,** która definiuje podstawowe zadania Sojuszu w zakresie bezpieczeństwa, w kategoriach obrony zbiorowej. Opisuje nowe środowisko strategiczne i dokonuje oceny możliwych do przewidzenia wyzwań i zagrożeń dla bezpieczeństwa. Koncepcja strategiczna NATO kładzie nacisk, że Sojusz musi być zdolny do przeciwstawienia się agresji o różnej skali, a obrona kolektywna pozostaje nadal jego ważną misją. Za równie ważne uważa się posiadanie zdolności do prowadzenia pełnego spektrum operacji począwszy od wojennych poprzez reagowanie kryzysowe do pomocy humanitarnej włącznie.

Jest też dokumentem, który zawiera wymagania, jakie powinny spełniać siły zbrojne Sojuszu w zakresie struktury dowodzenia, wyposażenia, gotowości bojowej i wsparcia logistycznego. Określa ona również, w jaki

---

[137] S. Koziej, Między piekłem a rajem, szare bezpieczeństwo na progu XXI wieku, Toruń 2006, s. 106.
[138] K. Piątkowski, Jak działa NATO?, [w:] W. Feler, Współczesne bezpieczeństwo, Toruń 2003, s. 71.

sposób siły powinny być zorganizowane, aby odzwierciedlać wielonarodowy i połączony charakter misji Sojuszu.

Jak już wspomniano kraje członkowskie NATO uczestniczą w tzw. planowaniu kolektywnej obrony. Głównym celem wspólnego planowania obronnego jest stworzenie podstaw do efektywnego zharmonizowania planów narodowych z planami NATO tak, aby były one spójne z wymogami Sojuszu. Proces ten obejmuje następujące zasadnicze dziedziny planowania obronnego NATO: sił zbrojnych, uzbrojenia, logistyki, zasobów obronnych, systemów (rozpoznania, dowodzenia, kierowania, łączności i innych).

W zaleceniach dokument ten podkreśla potrzebę ciągłego rozwijania zdolności wojskowych niezbędnych do wypełniania pełnego zakresu misji Sojuszu, od obrony zbiorowej do wspierania pokoju i innych operacji kryzysowych.

Wśród zdolności, których znaczenie zostało w szczególny sposób podkreślone są: zdolność do skutecznego angażowania sił przeciwnika; zdolność do rozmieszczania i mobilność; zdolność sił i infrastruktury do przetrwania; samowystarczalność i interoperacyjność – w tym interoperacyjność z siłami państw partnerskich.

Kolejnym dokumentem regulującym działalność Sojuszu są **wytyczne Komitetu Wojskowego NATO** w sprawie implementacji strategii Sojuszu w części wojskowej – MC-400/2, które określają warunki, jakie powinny spełniać siły zbrojne państw członkowskich, aby posiadały one:

- niezbędne zdolności operacyjne;
- odpowiedni stopień ukompletowania i wyszkolenia;
- obowiązujące standardy w zakresie procedur planowania operacyjnego, dowodzenia, wyposażenia oraz logistyki.

Następnie na podstawie Wytycznych Ministerialnych[139] są tworzone **cele sił zbrojnych NATO** i są to ogólne cele, które mają być osiągnięte przez siły zbrojne NATO w sześcioletnim okresie planistycznym. Cele SZ NATO to „zobowiązania do zaangażowania" sił zbrojnych o określonych możliwościach przez dany kraj członkowski. Cele nie odzwierciedlają rzeczywistego wkładu wojskowego danego członka w zakresie sił zbrojnych i ich możliwości. Dla każdego rodzaju sił zbrojnych opracowana jest tabela sił, ustalająca realistyczny poziom sił, realistyczną strukturę sił oraz realistyczną gotowość jednostek. Powiązane z celami SZ są wymagania długoterminowe, które wybiegają poza okres sześcioletniego okresu planowania. Dotyczą one badań i rozwoju sił zbrojnych krajów członkowskich i mogą stać się celami, jeżeli są wykonalne w czasie cyklu planistycznego.

Realizacja sojuszniczych zadań w sferze militarnej zapewnia zintegrowana struktura wojskowa NATO (zał. 11) Stanowią ją wszystkie siły i środki udostępniane przez państwa do wspólnej dyspozycji. Składają się na nią dowództwa sojusznicze oraz wydzielone do ich dyspozycji siły zbrojne. Dzielą się one na **siły reagowania** (natychmiastowego i szybkiego), **główne siły obronne** oraz **siły wzmocnienia**. Większość sił NATO pozostaje cały czas pod pełnym narodowym dowództwem, dopóki nie zostaną wydzielone do Sojuszu do konkretnych działań. Wyjątkiem od tej generalnej zasady są: zintegrowane sztaby w różnych dowództwach sojuszniczych; część zintegrowanej obrony powietrznej, włączając w to powietrzne elementy wczesnego ostrzegania i dowodzenia (AWACS); jednostki łączności; tzw.,

---

[139] **Wytyczne ministerialne** opracowywane są co dwa lata i zatwierdzane przez ministrów obrony. Ustanawiają one ogólne kierunki działania w zakresie sił konwencjonalnych i nuklearnych oraz nierozprzestrzeniana broni masowego rażenia. Ponadto zawierają wytyczne w zakresie planowania dla władz wojskowych NATO oraz poszczególnych krajów członkowskich w zakresie:

- planowania sił zbrojnych i uzbrojenia;
- reagowania kryzysowego i utrzymania pokoju;
- partnerstwa dla pokoju.

stałe siły morskie oraz inne elementy sojuszniczych sił reagowania [140]. Dowodzenie zintegrowanymi siłami zbrojnymi sprawują dowódcy strategiczni (SACEUR i SACLANT)[141]. Dowództwa te zapewniają doradztwo dla Komitetu Wojskowego poprzez swoich stałych przedstawicieli w Kwaterze Głównej. Realizują planowanie wojskowe (obronne i operacyjne - zał. 12), włączając w to określenie i zapotrzebowanie sił potrzebnych do realizacji pełnego zakresu zadań stabilizacyjnych, kryzysowych i obronnych w obszarach swojej odpowiedzialności.

Nowe wyzwania sprawiły, że na szczycie NATO w Pradze w 2002 roku położono podwaliny pod gruntowną reorganizację NATO i przygotowanie Sojuszu do działań w nowych warunkach. Do najważniejszych postanowień należało zaproszenie do grona członków NATO nowych państw Europy Środkowej i Wschodniej, co ma działać stabilizacyjnie w tym regionie świata. Kolejnym zdarzeniem, które miało wpływ na kształt NATO było zadecydowanie o utworzeniu Sił Odpowiedzi NATO (NATO Response Force – NRF). Z koncepcji NRF wynika, że są to zgrane oraz dobrze wyszkolone, utrzymujące wysoką gotowość bojową siły, które mogą spełniać wymagania prowadzenia operacji określonych przez Radę Północnoatlantycką. Dokumentem bazowym stanowiącym podstawę do tworzenia sił NRF był MC 477 [142]. Zgodnie z tym dokumentem Siły Odpowiedzi były przeszkolone i są gotowe do działania jako wielonarodowe siły połączone, które posiadają możliwości prowadzenia działań zarówno samodzielnie, jak i w składzie innych większych sił. Siły Odpowiedzi NATO składają się z zaawansowanych technologicznie, elastycznie reagujących, wysoce mobilnych wojsk, w tym jednostek lądowych, morskich

---

[140] S. Koziej, Strategiczne problemy bezpieczeństwa globalnego, Warszawa 2006, s. 96.

[141] SACEUR – dowódca sojuszniczy Europy, SACLANT – dowódca sojuszniczy na Atlantyku, Dowódcom strategicznym podlegają dowództwa regionalne. W Europie są to dowództwa północnoeuropejskich sił sojuszniczych – AFNORTH i południowoeuropejskich sił sojuszniczych – AFSOUTH, S. Koziej, Strategiczne problemy ..., wyd. cyt., s. 97.

[142] Military Concept for NATO Response Force MC 477.

i powietrznych, gotowych do szybkiego przemieszczania się w miejsca, gdzie będą potrzebne, zgodnie z decyzjami Rady NATO. Poszczególne państwa członkowskie przyjęły polityczne zobowiązania polepszenia ich zdolności do obrony przed atakiem chemicznym, biologicznym, radiologicznym, nuklearnym, a także możliwości działania w różnych uwarunkowaniach środowiska. To powoduje, iż siły wyznaczone do realizacji zadań w ramach Sił Odpowiedzi oparte będą na zgrupowaniach, tworzonych w odniesieniu do charakteru zadań i warunków działań militarnych. Liczebność Sił Odpowiedzi w momencie osiągnięcia gotowości operacyjnej w październiku 2006 liczyły 21000 żołnierzy.

W przypadku prowadzenia działań samodzielnie, możliwości NRF będą w pewien sposób ograniczone, co do wielkości, składu oraz charakteru działań. Jeśli zaś będą użyte w drugim przypadku, spełniać będą funkcję sił rozwiniętych w pierwszej kolejności - IEF[143]. Z uwagi na wysoką gotowość bojową i posiadane możliwości szybkiego przemieszczenia się i rozwinięcia, będą odpowiedzialne za przygotowanie wejścia w rejon przyszłej operacji sił głównych. Siły Odpowiedzi są zdolne do prowadzenia każdej operacji prowadzonej przez Sojusz w ramach Artykułu V i poza nim. Komponent lądowy NRF składa się ze struktur pozwalających na rozwinięcie formacji szczebla brygady. Taka brygadowa grupa bojowa składa się z 2-3 taktycznych zgrupowań bojowych, dysponuje siłami zarówno ciężkimi, lekkimi i aeromobilnymi, a także elementami wsparcia bojowego - CS [144] i zabezpieczenia logistycznego działań - CSS[145] o wysokiej manewrowości.

Siły Odpowiedzi pomyślane są również jako swoisty „katalizator" transformacji zdolności i możliwości Sojuszu Północnoatlantyckiego. Siły militarne z państw członkowskich, wyznaczone do struktur Sił Odpowiedzi,

---

[143] IEF - Initial Entry Force – Siły Inicjujące.
[144] CS - Combat Support.
[145] CSS - Combat Service Support.

z odpowiednim wyprzedzeniem otrzymują wytyczne dotyczące głównego wysiłku działania. W ten sposób mają możliwość przygotować oraz spełnić określone wstępnie założenia operacyjne i interoperacyjne. Natomiast realizacja rotacji kolejnych zgrupowań, postrzeganych jako Sił Odpowiedzi, będzie sprzyjać podnoszeniu możliwości operacyjnych oraz zdobywaniu doświadczeń w prowadzeniu operacji połączonych w rozumieniu całego Sojuszu, co w konsekwencji zapewni spełnienie podstawowych wymagań sojuszniczych (CJSOR[146]) przez państwa członkowskie.

4.2.2. Unia Europejska

Unia Europejska jest to gospodarczo-polityczna wspólnota, którą tworzą państwa członkowskie (27 państw), podstawę do funkcjonowania UE stanowi traktat z Maastricht, zwany też Traktatem o Unii Europejskiej.

Główne cele Unii to: **zapewnienie bezpieczeństwa, stabilnego wzrostu gospodarczego, rozwoju społecznego oraz ochrona praw i wolności obywateli.** W jej ramach poszczególne państwa członkowskie rozwijają współpracę w takich dziedzinach, jak: gospodarka, wymiar sprawiedliwości, transport, rolnictwo, energetyka, handel, kultura, transport, czy sfera obronności i polityki zagranicznej.

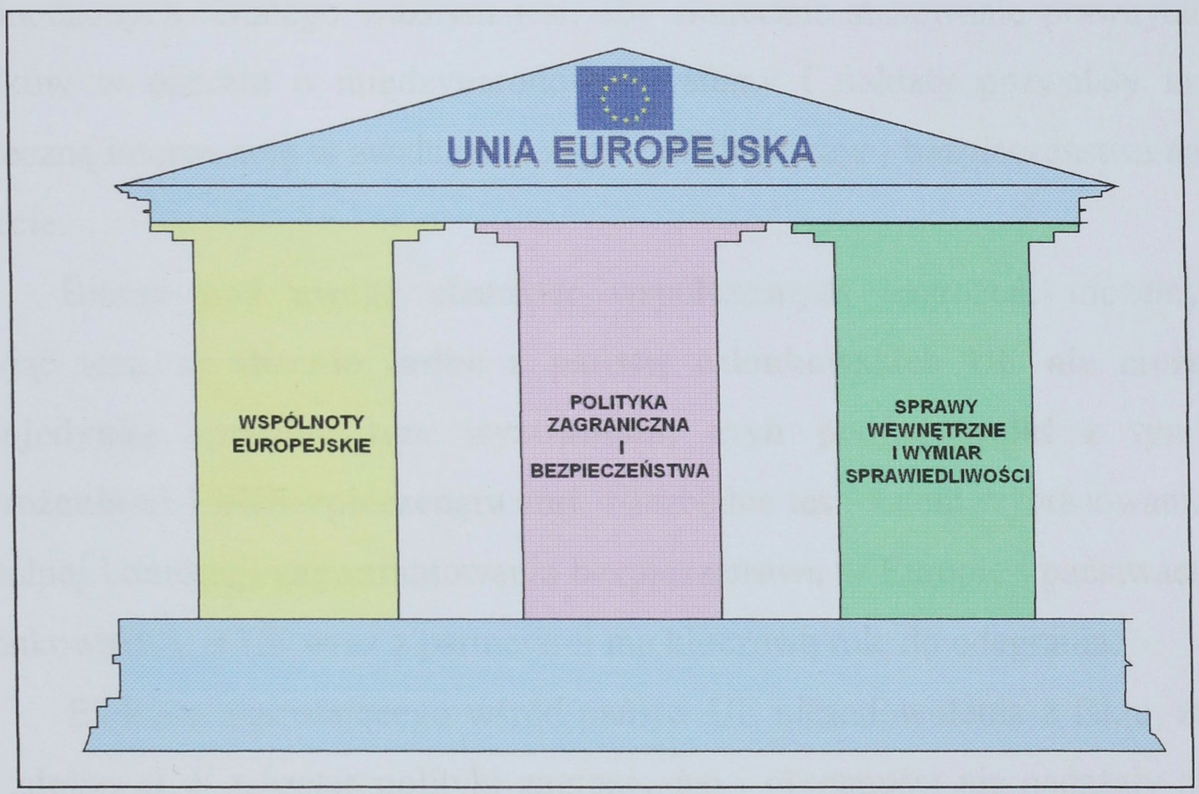
Aktualnie funkcjonowanie Unii Europejskiej koncentruje się na trzech filarach, którymi jest gospodarka - wspólnoty europejskie, polityka zagraniczna i bezpieczeństwa oraz wymiar sprawiedliwości i sprawy wewnętrzne (rys.4.2). Najważniejszymi organami UE są: **Rada Europejska, Rada UE (dawniej Rada Ministrów), Komisja Europejska (dawniej Komisja Wspólnot), Parlament Europejski, Trybunał Sprawiedliwości, Trybunał Obrachunkowy** (zał. 13.).

---

[146] CJSOR - Combined Joint Statement of Requirement

Podobnie jak w Sojuszu NATO wiodącym dokumentem w kwestii bezpieczeństwa jest **Strategia Bezpieczeństwa Europejskiego**, gdzie główny wysiłek państw wspólnoty powinien być skierowany na[147]:

po pierwsze – posiadaniu zdolności do odpowiedzi na zagrożenia. W związku z rozwojem sytuacji międzynarodowej Unia musi być zdolna na zwalczanie zagrożeń nie tylko na swoim obszarze, ale także poza swoim terytorium. Realizuje to przedsięwzięcie przy współpracy z państwami członkowskimi oraz przy współpracy transatlantyckiej przeciwdziałając terroryzmowi, rozprzestrzenianiu się broni masowego rażenia, reagowaniu na konflikty regionalne;



Rys. 4.2. Filary Unii Europejskiej

po drugie - budowaniu bezpieczeństwa w swoim bezpośrednim sąsiedztwie, zwłaszcza w kontekście rozszerzenia Unii, przez co granica przesuwana jest w stronę obszarów niestabilnych. Można realizować to na

---

[147] Strategia Bezpieczeństwa Europejskiego, Bruksela 12. 12 2003 r.

dwa sposoby: poprzez połączenie wspólnych wysiłków oraz nawiązaniu współpracy ze Stanami Zjednoczonymi, NATO, Rosją, ONZ, dzięki czemu udaje się utrzymywać pokój lub zapobiegać rozprzestrzenianiu konfliktu, na obszarach niestabilnych politycznie i gospodarczo (Bałkany, Bliski Wschód); poprzez współpracę gospodarczą i pomoc humanitarną krajom mniej rozwiniętym, dzięki czemu państwa mogą czerpać obustronne korzyści (Rosja) lub zostaje ograniczony obszar ubóstwa (Afryka);

po trzecie - kreowaniu porządku międzynarodowego. W świecie globalnych zagrożeń bezpieczeństwo może zapewnić tylko międzynarodowe wielostronne forum rozwiązywania konfliktów oparte na Karcie Narodów Zjednoczonych. Dlatego ważnym jest, aby skuteczne stosowanie prawnych środków w oparciu o międzynarodowe, systemy i traktaty pozwalały na skuteczną interwencję w zwalczaniu zagrożeń dla pokoju i bezpieczeństwa na świecie.

Biorąc pod uwagę charakter współczesnych zagrożeń, możemy przyjąć tezę, iż **obecnie żadne z państw członkowskich UE nie może w pojedynkę sprostać tym wyzwaniom, czyli podjąć walki z tymi zagrożeniami i niebezpieczeństwami.** Niezbędne jest, zatem wypracowanie wspólnej koncepcji zagwarantowania bezpieczeństwa w Europie i państwach członkowskich, a UE wraz z partnerami ma kluczową rolę do odegrania.

Efektem wzrastającego wśród państw UE niezadowolenia z faktu, że ich zdolności w zakresie polityki zagranicznej i obronności nie nadążały za wzrostem znaczenia Unii jako potęgi handlowej i gospodarczej było przyjęcie **Wspólnej Polityki Zagranicznej i Bezpieczeństwa** (WPZiB). Unia ustanowiła również **Europejską Politykę Bezpieczeństwa i Obrony** (EPBiO) określającą działania, jakie mogą podejmować siły zbrojne UE i do których należą między innymi misje humanitarne, akcje ratunkowe, operacje pokojowe, zarządzanie kryzysami, a nawet czynne przywracanie pokoju.

W dziedzinie Europejskiej Polityki Bezpieczeństwa i Obrony przełomowym wydarzeniem było posiedzenie w Helsinkach w 1999 roku, gdzie Rada Europy opowiedziała się za dalszym rozwojem swej autonomicznej zdolności do decydowania o podjęciu i prowadzeniu operacji wojskowych pod kierownictwem UE. Zapowiedziano również potrzebę utrzymania przez państwa członkowskie siły wojskowej i utworzenie nowej struktury politycznej i wojskowej w łonie Rady Europejskiej, jak też stworzenie niezbędnych warunków dla konsultacji, współpracy i pełnej przejrzystości w stosunkach między NATO i UE.

W celu sprawnego zarządzania bezpieczeństwem militarnym Rada Europy zdecydowała o powołaniu następujących organów politycznych i wojskowych[148]:

- stały Komitet Polityczny i Bezpieczeństwa, który zajmuje się wszystkimi aspektami WPZiB i EPBiO;
- Komitet Wojskowy, który będzie wyrażał opinie i formułował wnioski oraz wydawał dyrektywy sztabom;
- sztab w łonie Rady Europy, który zapewnia kierowanie operacjami mających na celu rozwiązanie kryzysów pod auspicjami UE.

Autorytet wspólnej polityki zagranicznej opiera się na istnieniu wiarygodnych środków działania. Dlatego też UE dążyła do wzmocnienia zdolności operacyjnej EPBiO, zarówno wojskowej, jak i cywilnej, a także do opracowania strategii bezpieczeństwa.

Dodatkowo kryzys iracki z jednej strony ujawnił głęboki podział wśród państw członkowskich Sojuszu, zaś z drugiej spowodował zwiększenie gotowości do nadania Unii większych zdolności reagowania siłami militarnymi w sytuacjach kryzysowych. Dlatego też Unia Europejska zdecydowała się na utworzenie własnych sił szybkiego reagowania (European

---

[148] W. Feler, Współczesne ..., wyd. cyt., s. 86.

Rapid Reaction Force -ERRF), w ramach rozwoju Wspólnej Polityki Bezpieczeństwa i Obrony UE. W maju 2004 r. ministrowie obrony Unii, dostrzegając jednak problemy z realizacją projektu ERRF, przystali na zmianę tzw. Europejskiego Celu Operacyjnego UE wg nowych zamierzeń. Założono, iż UE do 2010 r. powinna być gotowa do przeprowadzania operacji militarnych w całym spektrum działań antykryzysowych. Nowym instrumentem umożliwiającym wykonanie tych zadań mają być tzw. Grupy Bojowe (Battle Groups)

W konsekwencji tych działań na brukselskim posiedzeniu jesienią 2004 roku ministrowie obrony państw Unii Europejskiej oficjalnie zatwierdzili utworzenie 13 Grup Bojowych. Jednostki te mają być użyte wyłącznie do autonomicznych operacji wojskowych Unii. Od 2006 r. Grupy Bojowe częściowo były zdolne do ich użycia w dwóch jednocześnie przeprowadzanych operacjach militarnych. W bieżącym roku Grupy Bojowe osiągną pełną zdolność operacyjną (tzw. Full Operational Capability). Każda Grupa jest zdolna do operacji trwającej 30 dni i przy jej wzmocnieniu do 120 dni.

Mając na uwadze bezpieczeństwo narodowe i międzynarodowe Polska poparła francusko-niemiecko-brytyjską inicjatywę utworzenia Grup Bojowych, ponieważ uważała, że będzie to realny wkład w budowę rzeczywistej siły operacyjnej UE. Nie występuje tu sprzeczność między dalszym rozwojem Europejskiej Polityki Bezpieczeństwa i Obrony a stosunkami z Sojuszem. Można natomiast oczekiwać generalnego podniesienie poziomu potencjału obronnego Unii, a tym samym wzmocnienia komponentu europejskiego w NATO. Polsko-niemiecka Grupa Bojowa z udziałem Litwy, Łotwy i Słowacji rozpocznie swoją działalność począwszy od 2009 roku. Polska i Niemcy reprezentują podobne stanowisko, uważając, że Grupy Bojowe nie mogą naruszyć spójności Sił Szybkiego Reagowania NATO. Siły te mają tutaj dla obu państw priorytetowe znaczenie.

Zdolność szybkiego reagowania wymaga przyśpieszenia procesu planowania i podejmowania decyzji na szczeblu krajowym i europejskim w zakresie operacji szybkiego reagowania, przeprowadzanych przez UE.

Najważniejszym ciałem podejmującym decyzję w UE jest Rada Europejska, która w swojej kompetencji rozpatruje wnioski wpływające od Komisji Europejskieji podejmuje wiążące decyzję metodą „kwalifikowanej większości", a w sprawach EPBiO (wspólnej polityki bezpieczeństwa i obrony) i współpracy policyjnej i sądowej oraz w sprawach karnych poprzez jednomyślne głosowanie, przy czym każde państwo posiada prawo veta. Aby wniosek został przyjęty przez Radę musi otrzymać „kwalifikowaną większość[149]" głosów.

W dziedzinie WPZiB i EPBiO podejmowanie decyzji przez Radę nie wymaga użycia metody „kwalifikowanej większości", ale decyzje Rady muszą być jednomyślne, czyli mogą zostać zablokowane przez **veto każdego z krajów**. Jest to główna przeszkoda w kreowaniu wykonawczego wspólnego sposobu szybkiego działania w ramach systemu bezpieczeństwa Unii, bowiem o ile wskazanie instytucji podejmujących problematykę bezpieczeństwa w Europie nie nastręcza trudności, to określenie powiązań pomiędzy nimi oraz wyszczególnienie jednego ośrodka decyzyjnego, mogącego podjąć wiążącą decyzję nie jest takie oczywiste. Jest to spowodowane wieloma czynnikami z których najważniejszym jest trudne określenie prawnej tożsamości Europejskiej z wieloma państwami narodowościowymi. W obecnie ratyfikowanym Traktacie Reformującym, formuła podejmowania decyzji może być zmieniona[150].

---

[149] „Kwalifikowaną większość" głosów. Oznacza to, co najmniej 232 głosy ze wszystkich 321. Wniosek musi poprzeć większość państw (w niektórych przypadkach: 2/3 państw). Ponadto, każde państwo może poprosić Radę o sprawdzenie, czy liczba ludności w krajach głosujących za przyjęciem wniosku stanowi co najmniej 62% całej populacji UE - określa to Traktat Nicejski w art. 1.

[150] Stan na 12.2007.

4.3. Nowe kierunki (tendencje) rozwoju międzynarodowego bezpieczeństwa militarnego

Współcześnie NATO i Unia Europejska funkcjonują generalnie w tym samym środowisku bezpieczeństwa militarnego. Większość państw wchodzących w ich skład jest członkami obu organizacji. Naukowcy zajmujący się tą problematyką, bardzo często stawiają sobie pytanie, czy obie organizacje się nie dublują i czy państwom Europy potrzebne jest członkowstwo w NATO?

Oceny współczesnych zagrożeń bezpieczeństwa, globalny charakter owych zagrożeń powoduje, iż tylko partnerstowo wszystkich organizacji może wzmacniać stan bezpieczeństwa międzynarodowego. W świecie globalnych zagrożeń współpraca i partnerstwo jest warunkiem przetrwania w pokoju, skutecznego przeciwstawiania się możliwym zagrożeniom wojennym. Partnerstwo to taki rodzaj współdziałania, które oparte jest na równych zasadach tj., korzyści i współodpowiedzialności. Własne cele można osigać utrzymując wspólne wartości. Partnerstwo gwarantuje instytucjonalną współpracę. Należy przypuszcza, iż **współpraca dalej się będzie rozwilała, ponieważ zarówno NATO, jak i Unia Europejska nie są w stanie samodzielnie rozwiązać wszystkich problemów związanych z zapewnieniem szeroko rozumianego bezpieczeństwa**[151].

Oceniając stan bezpieczeństwa europejskiego, możemy przyjąć tezę, iż **Europie nie zagraża militarnie żadne państwo, a poziom jej bezpieczeństawa zależy przede wszystkim od działań na rzecz rozwiązywania konfliktów i kryzysów poza jej obrębem**. Zdecydowana większość kryzysów ma swoje źródła w skomplikowanej sytuacji

---

[151] NATO jest i będzie gwarantem naszego bezpieczeństwa, nie jako współzawodnik, lecz jako partner strategiczny. Jakie skutki wywiera to partnerstwo dla pokoju i stabilności widzieliśmy w praktyce na Bałkanach. Tak mówił J. Solana prezentując dokument pn.: Strategia bezpieczeństwa Unii Europejskiej. Implikacje dla Europy w zmieniającym się świecie, Berlin 2003, [w:] H. Binkowski i inni, NATO w systemie bezpieczeństwa euroatlantyckiego, Warszawa 2004, s.446.

wewnętrznej. Podłoże większości dzisiejszych konfliktów to przede wszystkim zła sytacja gospodarcza kraju połączona z problemami enicznymi i niezadowoleniem z władzy. Powoduje to narastanie nastrojów nacjonalistycznych i w konsekwencji często prowadzi do wybuchu konfliktów wewnątrzpaństwowych. Dlatego też wyzwaniem dla społeczności międzynarodowej stanowić będzie przede wszystkim dostosowanie regulacji prawnomiędzynarodowych oraz wkształcenie instrumentu reagowania w przypadku kryzysów o charakterze wewnętrznym.

Dokonując analiz kwesti zarządzania militarnego NATO i Unii Europejskiej możemy wyciągnąć wnioski, iż w obu tych organizacjach przedsięwzięcia te oparte są na podobnych zasadach. Zarwóno NATO jak i Unia Europejska w swoich założeniach przyjeły, iż głównym celem ich działalności w sytuacji powstawania sytuacji kryzysowej jest: **redukcja napięć, podejmowanie działań, które pozwolą uniknąć konfliktu, oraz odparcia ewentualnej agresji.** Zarządzanie militarne w sytuacjach kryzysowych opiera się na następujących zasadach: Rada Północnoatlantycka i Rada Europejska jest najwyższą władzą; decyzje podejmowane są poprzez konsens; stali przedstwaiciele wszystkie elementy rządów; siły zbrojne pozostają cały czas pod kontrolą polityczną i żadna decyzja o planowaniu użycia sił nie może być podjęta bez politycznego przyzwolenia. Przyjęte podobne założenia zarządzania militarnego przez obie organizacje ułatwiają współpracę i partnerstwo. Odrębną natomiast rzeczą jest proces planowania i praktyka ćwiczeniowa. W tym obszarze potrzebne są ujednolicenia, co podniesie sprawność działania w przypadku wspólnego rozwiązywania sytuacji kryzysowych.

Głównym ukierunkowaniem Uni Europejskiej, jak też NATO w zakresie bezpieczeństawa militarnego należy przypuszczać, iż będzie zwalczanie terroryzmu i kontrola zbrojeń. Aczkolwiek terroryzm nie jest nowym zjawiskiem, to na początku XXI wieku tragicznie dotknął Stany

Zjednoczone, Wielką Brytanię i Hiszpanę. Oceniając to zjawisko, należy się spodziewać w najbliższych latach jego nasilenia, ponieważ stanowi on dogodną i skuteczną formę osiągania celów politycznych.

Walka z terroryzmem staje się jednym z ważniejszych obszarów bezpieczeństwa. Z tego względu zdolność do interwencji militarnej, jako środek obrony państw i regionów jest niezbędna przede wszystkim w celu[152]:

- niedopuszczenia do prawdopodobnych konfliktów lub zakończenia już istniejących wojen, gdyż stanowią one pożywkę do powstawania i rozwoju organizacji terroystycznych;
- rozbicia fizycznego siatek terrorystycznych i ośrodków szkoleniowych;
- przeprowadzania prewencyjnych operacji, uniemożliwiających wsparcie terrorystów przez państwa i organizacje tym zainteresowane.

Dlatego zarówno NATO jak też Unia Europejska widzi potrzebę i deklaruje współpracę ze wszelkimi organizacjami w walce z terroryzmem, aby ograniczyć jego skalę. W swoich działaniach angażuje wszelkie zasoby i instrumenty cywilne i wojskowe sojusznicze i narodowe (państw członkowskich).

W zakresie bezpieczeństwa militarnego, NATO jak i Unia Europejska widzi potrzebę zwiększonego nacisku na na problem przeciwdziałania rozprzstrzenianiu się broni masowego rażenia i kontroli zbrojeń. Powstrzymywanie ambicji atomowych niektórych państw, jak też kontrola rozwoju zbrojeń, przeciwdziałanie nielegalnemu handlowi bronią może stanowić podstwę bezpieczeństwa międzynarodowego.

---

[152] J. Kaczmarek, Współczesne bezpieczeństwo, Warszawa 2008, s. 12.

Nową tendencją jest podejmowanie misji o charakterze cywilnym, policyjnym i doradczym, które mają decedujące znaczenie w fazie odbudowy życia społecznego i instytucji publicznych na zasadach demokratycznych[153].

Kolejnym takim kerunkiem (tendencją) rozwoju bezpieczeństawa międzynarodowego jest zangażownie NATO, a zwłaszcza Unii Europejskiej, poza strefą euroatlantycką. Poprzez rozwiązywanie konfliktów bezpośrednio niezagrażających Europie, czy bezpieczeństwu Sojuszu - podnosi się stan bezpieczeństwa międzynarodowego. Takie podejście wynika z nowej filozofi zakceptowanej przez NATO, jak też Unię Europejską, gdzie obie organizacje wyznają zasady:

po pierwsze – niebezpieczeństwom należy przeciwdziałać tam gdzie one powstają, neutralizować źródła powstających zagrożeń;

po drugie – większym niż dotychczas stopniu należy prowadzić działania cywilno-militarne, ale też, skuteczność owych działań należy upatrywać w tym, iż oprócz środków militarnych wykorzystwać należy szeroko środki polityczne, dyplomatyczne, ekonomiczne i inne[154].

W erze globalizacji stan midzynarodowego bezpieczeństwa militarnego w coraz większym stopniu zależy od efektywnego systemu multilaternego. Wzmacnianie społeczności międzynarodowej, rozwój dobrze funkcjonujących instytucji międzynarodowych oraz ład oparty na prawie, to cele sojuszu, zarówno NATO jak też Unii Europejskiej. Sytuacja stanu

---

[153] R. Zięba, Bezpieczeństwo międzynarodowe po zimnej wojnie, Warszawa 2008, s. 291.

[154] Aktualnie zapoczątkowany jest Wielonarodowy Eksperyment 6 (w którym uczestniczy też Polska), który obejmować będzie problematykę kompleksowego podejścia do rozwiązywania sytuacji kryzysowych. Zasadniczy wysiłek w MNE 6 skupiony zostanie na opracowaniu dokumentów (koncepcji, wytycznych, podręczników, ...) dla dowódców koalicji, prowadzących operacje w warunkach oddziaływania nieregularnego przeciwnika (irregular adversaries) oraz innych „nie współpracujących" z siłami koalicji uczestników kryzysu (non-compliance actors). Eksperyment obejmuje cztery obszary:

- **Obszar I:** synchronizacja wysiłków sił koalicji, organizacji i innych partnerów oraz pomoc państwom objętym kryzysem;
- **Obszar II**: tworzenie oraz wdrażanie wspólnej strategii informacyjnej;
- **Obszar III**: ocena postępów i efektów realizacji planu operacji przez siły koalicji razem z innymi współpracującymi siłami w celu dostosowania dalszych działań;
- **Obszar IV:** wymiana informacji pomiędzy wojskowymi i cywilnymi uczestnikami operacji.

zagrożeń wymaga koordynacji międzynarodowej pomiędzy najważniejszymi aktorami środowiska bezpieczeństwa, czyli Unii Europejskiej i Sojuszu NATO. Posiadanie przez obie organizacje sprawnych i skutecznych narzędzi w postaci Grup Bojowych i Sił Odpowiedzi mogą być dzisiaj gwarantem bezpieczeństwa militarnego.

Wnioski

Dokonując analiz stanu bezpieczeństwa, a przede wszystkim rozpoznane trendy rozwoju cywilizacyjnego wskazują, że polityka bezpieczeństwa nadal się będzie zmieniała. Przyrost naturalny ludności, zmiany środowiskowe, eskalacja zagrożeń w postaci terroryzmu oraz dalszy gwałtowny rozwój nauki, techniki i technologii sprawiają, iż pojawią się nowe scenariusze polityki bezpieczeństwa. Zmiany te dotyczyć też będą kwestii zarządzania militarnego. Dynamika zachodzących zmian i związana z nimi niepewność wymaga, by system zarządzania był sprawny i skuteczny, aby w krótkim czasie posiadał zdolność poprzez swoje instrumenty (siły zbrojne) mógł reagować na nowe formy zagrożeń i konfliktów.

Sprawność zarządzania militarnego w aspekcie obecnych sojuszy to przede wszystkim głownie siły i środki sił zbrojnych NATO i Unii Europejskiej, poprzez zdolność do szybkiego rozpoznania ognisk konfliktów, powinny mieć możliwość użycia nie tylko głównych sił na duże odległości i interweniowania w wypadku kryzysu przy małych stratach, lecz również ochrony własnych sił zbrojnych, ludności i obiektów infrastruktury krytycznej.

Uzyskane wyniki badań w zakresie sojuszniczych aspektów zarządzania militarnego pozwala wnioskować, iż istnieje potrzeba dalszych regulacji w zakresie zarządzania bezpieczeństwem, w tym bezpieczeństwem militarnym. W dniu dzisiejszym, kiedy nieprzewidywalne są zagrożenia,

a skala tych zagrożeń ma charakter globalny, żadne państwo nie jest w stanie zapewnić sobie bezpieczeństwa, a zwłaszcza bezpieczeństwa militarnego. Współcześnie bezpieczeństwo militarne Polski, Unii Europejskiej i Sojuszu NATO powinno opierać się na współpracy i partnerstwie. Dlatego potrzebne są dalsze zmiany, także w zakresie zarządzania bezpieczeństwem militarnym. Mając na uwadze międzynarodowy (sojuszniczy) aspekt zarządzania bezpieczeństwem militarnym, należy sądzić, iż filarami jego powinno być:

1. Współpraca poszczególnych państw w ramach NATO i Unii Europejskiej z wykorzystaniem swoich instytucji, jako płaszczyzny do wspólnego kreowania polityki bezpieczeństwa militarnego.

2. Wspólna polityka zagraniczna i bezpieczeństwa w tym wzajemnie uzupełnianie się: Europejskiej Polityki Bezpieczeństwa i Obrony (EPBiO), wraz z siłami wojskowymi (Grupy Bojowe) oraz Koncepcji Strategicznej NATO z siłami militarnymi (Siły Odpowiedzi NATO).

3. Współpraca z instytucjami ponadnarodowymi typu ONZ oraz zawiązywanie koalicji wielonarodowych dla wspólnego zapobiegania bądź rozwiązywania sytuacji kryzysowej.

ZAKOŃCZENIE

Przedstawione w pracy rezultaty badań obrazują realizację zamierzeń zaprojektowanych w ramach założeń metodologicznych przedstawionych we wstępie. Przy wykorzystaniu posiadanego doświadczenia naukowego i wiedzy specjalistycznej zespołu autorskiego można było, przy zastosowaniu dostępnych metod, rozwiązać problemy badawcze na wymaganym poziomie dla prac naukowo – badawczych. Sadzimy także, że osiągnięte zostały określone cele. Wniesiony został stosowny wkład do teorii zarządzania i dowodzenia, a także bezpieczeństwa, w części dotyczącej bezpieczeństwa militarnego, ze wskazaniem na elementy rozwojowe.

Uzyskane wyniki potwierdziły nakreślone przewidywania hipotetyczne, bowiem zarządzanie bezpieczeństwem militarnym wymaga ciągłych zmian podporządkowanych podwyższaniu jego skuteczności. Wynika to z potrzeby stosownych reakcji, zarówno na zmiany uwarunkowań polityczno – militarnych, jak i doskonalenia instrumentów i sposobów zarządzania.

Sądzimy, że treści merytoryczne niniejszego opracowania mogą być wykorzystane przez gremia decyzyjne w procesie projektowania i realizacji zamiarów wykonawczych procesu zarządzania przedmiotowym bezpieczeństwem. Przedstawione podstawy zarządzania bezpieczeństwem militarnym, wraz z propozycjami stosownych elementów projektowych, stworzyło określona całość podporządkowaną celowi poznawczemu pracy. Jest to problematyka trudna i wymaga kolejnych ocen i reagowania na nowe zjawiska w tym obszarze penetracji naukowej.

W pracy wykazano rosnące znaczenie informacji w zarządzaniu bezpieczeństwem, która staje się podstawą do podejmowania racjonalnych

decyzji. Potwierdzona została też zasadność oddzielnego podejścia przy badaniu narodowych i sojuszniczych aspektów bezpieczeństwa militarnego. Przy czym wykazano też potrzebę postrzegania tych aspektów we wzajemnych związkach i zależnościach.

W uogólnieniu stwierdzić można, iż przedstawione w pracy analizy, oceny, syntezy i elementy koncepcyjne dotyczące zarządzania bezpieczeństwem militarnym wygenerowano na podstawie identyfikacji problemu i obecnego stanu interesującej nas wiedzy teoretycznej z elementami prognostycznymi. Stąd przedstawione w pracy rezultaty badań mogą być w różnym stopniu wykorzystywane, zarówno w pracach projektowych w przedmiotowym zakresie, jak i w stosowaniu rozwiązań funkcjonalnych zapewniających wymagany poziom badanego bezpieczeństwa militarnego.

BIBLIOGRAFIA

1. AAP-6(U), Słownik terminów i definicji NATO, Warszawa 2005.
2. Afganistan militarny i pozamilitarny wymiar stabilizacji, materiały z konferencji AON, Warszawa 2007.
3. AJP-01(B) (1D), Allied Joint Doctrine, 12.2002.
4. AJP-3 (2D), Allied Joint Operations, 09.2002.
5. Alexander B., The Future of Warfare, W. W. Norton & Company Ltd, London.
6. Alexander S. E., Urban Warfare: U.S. Forces in Future Conflicts, Military Review, styczeń – luty 2002.
7. Awsiuk T., Tworzenie zgrupowań uderzeniowych, Myśl Wojskowa 1986, nr 4.
8. Balcerowicz B., Siły zbrojne w państwie i stosunkach międzynarodowych, Scholar, Warszawa 2006.
9. Balcerowicz B., Wybrane problemy obronności państwa, AON, Warszawa 2002.
10. Bastone J. J., Urban Operations Update, Infantry nr wiosna, Fort Benning 2002.
11. Bendyk E., Bajty w boju, Polityka nr 11 (2495), 19 marca 2005.
12. Bieniek M., Siły Odpowiedzi jako narzędzie nowych struktur dowodzenia NATO, Warszawa 2005.
13. Binkowski H., i inni NATO w systemie bezpieczeństwa euroatlantyckiego. Materiały do studiowania. Warszawa 2004.
14. Biuletyn informacyjny nr 2 (162), Sztab Gen. WP, Warszawa 1995.
15. Black W., Rozwój taktyki w ciągu wielkiej wojny, Warszawa 1921.
16. Bojko K., Polityka amerykańska wobec konfliktu na Bliskim wschodzie w świetle inicjatyw pokojowych Arabii Saudyjskiej, Egiptu i Jordanii w: Sprawy międzynarodowe nr 3 z 2002.
17. Bujak A., Sobolewski G., Teren Zabudowany środowiskiem pola walki XXI wieku, AON, Warszawa 2005.
18. Bujak A., Środowisko a działania bojowe na terytorium Polski, Wyd. A. Marszałek, Toruń 2000.
19. Carnovale M., Partnerzy i sojusznicy NATO: Stosunki cywilno - wojskowe i demokratyczna kontrola nad armią. Bliżej NATO, zeszyt 3. Warszawa 1998.
20. Ciborowski L., Organizacja rozpoznania w sztabach, AON, Warszawa 1991.
21. Ciborowski L., Walka Informacyjna, Europejskie Centrum Edukacyjne, Toruń 1999.
22. Fitas M., Siły Odpowiedzi NATO - praca studyjna. Warszawa, 2003.
23. FM 3 – 06. Urban Operations, Waszyngton 2003.
24. FM 3-07 Stability and Suport Operations,Washington, HQ Department of the Army 2003.
25. FM 3-21.31 The Stryker Brigade Combat Team, Headquarters Department Of The Army, march 2003.
26. Fryc M., Charakter przyszłych operacji wojskowych, [w:] Zeszyty naukowe Nr 1 (62), AON, Warszawa 2006.
27. Gągor F., Siły Zbrojne RP stan obecny i przyszłość, Wykład, AON, dn. 16.01.2007.
28. Grupy Bojowe w UE, Wojska lądowe nr 6(119) 15-31 marzec 2005.

29. Haliżak E., Kuźniar R., (red.), Stosunki międzynarodowe, Geneza, struktura, dynamika, WUW, Warszawa 2006.
30. Huzarski M. (red), Taktyka ogólna wojsk lądowych, Warszawa 2001.
31. Kaczmarek J., *NATO - Polska 2000*. Wrocław 1999.
32. Kaczmarek J., Współczesne bezpieczeństwo, Warszawa 2008.
33. Kępka S., Uwarunkowania i zagrożenia bezpieczeństwa państwa w świetle aktualnej sytuacji międzynarodowej, Wrocław 2004.
34. Kmiciński Z., Siły Odpowiedzi NATO a koncepcja Grup Bojowych Unii Europejskiej. Możliwości i ograniczenia wspólnych działań, Praca dyplomowa AON, Warszawa 2005.
35. Koziej S., Metropolie a wojna z terroryzmem, Zeszyt Naukowy AON nr 2(55), 2004.
36. Koziej S., Między piekłem a rajem, szare bezpieczeństwo na progu XXI wieku, Toruń 2006.
37. Koziej S., Strategiczne problemy bezpieczeństwa globalnego, Warszawa 2006.
38. Kukułka J., Bezpieczeństwo międzynarodowe w Europie środkowej po zimnej wojnie, Warszawa 1994.
39. Leksykon wiedzy wojskowej, pod red. M. Laprusa, MON, Warszawa 1979.
40. Lisiecki M., (red.) Zarządzanie bezpieczeństwem – wyzwania XXI wieku, Warszawa 2008.
41. M. Wiatr, Między strategią a taktyką, Toruń 1999.
42. MC 133/3 (F), NATO Operational Planning System, 28.08.2000.
43. MC 317/1 (Final), NATO Force Structure, 08.07.2002.
44. MC 324/1 (8 Draft), NATO Military Command Structure, 23.03.2003.
45. MC 477 (MD), The NATO Response Force Military Concept, 10.04.2003.
46. McMahon M., Aviation Restructure Initiative - corps aviation brigade, theater aviation, US Army Aviation Digest, March/April 1994.
47. Miszczak K., Battle Groups/Grupy Bojowe - Europejskie Siły Szybkiego Reagowania, Przegląd Środkowoeuropejski nr 40.
48. Mreła K., Struktury organizacji. Analiza wielowymiarowa, PWE, Warszawa 1989.
49. NATO Handbook, Brussels – Public Diplomacy Division 2006.
50. NATO Response Force 2 (NRF-2) Findings and Lessons Learned, NRDC-T, 07.2004.
51. Operacja „Iracka Wolność", materiały z konferencji naukowej, red. M. Krauze, AON, Warszawa 2003.
52. Operations, www.armyapp.dnd.ca/allc/main.asp, dn. 20 maj 2002.
53. Pawłowski J., Istota operacji połączonych, [w:] Działania (operacje) połączone, Materiały z konferencji naukowej, AON, Warszawa 2002.
54. Piątek Z., Procedury i przedsięwzięcia systemu reagowania kryzysowego, AON, Warszawa 2005.
55. Piątkowski K., Wojna nowego typu? Polska w Europie, Warszawa 2002.
56. PN-ISO/IEC 17799, Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, Warszawa 2007.
57. PN-I-13335-1, Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, Warszawa 1999.
58. PN-EN ISO 19011, Wytyczne dotyczące audytowania systemów zarządzania jakością i/lub zarządzania środowiskowego, PKN, Warszawa 2003.
59. PN-ISO/IEC 27001, technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania, PKN, Warszawa 2007.

60. Polska Zbrojna, nr 31/2007.
61. Projekt doktryny szkolenia sił zbrojnych RP DD/7, Warszawa 2004.
62. Regulamin Działań Wojsk Lądowych (DD/3.2), Szkol.809/2006, Warszawa 2006.
63. Scales R., Future warfare, U.S. Army War College, Carlislr Barraks 1999.
64. Siły Odpowiedzi NATO – kompendium „Biuletyn Informacyjny" nr 1 (173).
65. Sobolewski G., Operacje militarne wojsk lądowych w terenie zabudowanym, Zeszyty Naukowe 2(58), AON, Warszawa 2005.
66. Sobolewski G., Rola terenu zurbanizowanego we współczesnych operacjach, materiał z konferencji, Warszawa 2005.
67. Sobolewski G., Wybrane aspekty walki w mieście, Warszawa 2006.
68. Sobolewski G., Zgrupowania wojsk lądowych w terenie zabudowanym, ZN 2(63) 2006.
69. STANAG 2827: Materials Handling in the Field.
70. Stepek W., Powietrzno – lądowy wymiar działań wojsk lądowych, [w:] Sztuka wojenna we współczesnych konfliktach zbrojnych – przemiany i tendencje rozwojowe, Materiały z konferencji naukowej zorganizowanej 20 października 2006r. AON, Warszawa 2007.
71. Strategia Bezpieczeństwa Europejskiego, Bruksela 12. 12 2003.
72. The NATO Response Force (NRF) Detailed Implementation Programme, 07.05.2003.
73. Trudna stabilizacja. Doświadczenia i wnioski z sojuszniczego współdziałania pierwszej zmiany polskiego kontyngentu wojskowego w działaniach pokojowych w Iraku, materiały z konferencji, red. J. Gotowała, AON, Warszawa 2004.
74. Wykaz obowiązujących standardów, technologii informatycznych do stosowania w resorcie obrony narodowej na lata 2007-2008, Departament Informatyki i Telekomunikacji MON, Warszawa 2007.
75. Zięba R., Bezpieczeństwo międzynarodowe po zimnej wojnie, Warszawa 2008.
76. Zięba R., Instytucjonalizacja bezpieczeństwa europejskiego, Warszawa 1994.

Strony internetowe

http:// www.wp.mil.pl, *Strategia bezpieczeństwa narodowego RP*, Warszawa 2007.
http://europa.eu/index_pl.htm
http://www. un.org
http://www.nato.int
http://www.unic.un.org.pl
http://europa.eu/institutions/inst/comm/index_pl.htm

ZAŁĄCZNIKI

1. Architektura systemów informatycznych
2. Prognoza standardów technicznych
3. Architektura resortowych systemów informatycznych
4. Wariant działania Sił Zbrojnych Wislandii w osłonie strategicznej (Wariant 1)
5. Wariant działania Sił Zbrojnych Wislandii w osłonie strategicznej (Wariant 2)
6. Wariant działania Sił Zbrojnych Wislandii w osłonie strategicznej (Wariant 3)
7. Wyniki symulacji działań
8. Schemat działania 7 DZ w ćwiczeniu dowódczo-sztabowym p.k. „PIERŚCIEŃ"
9. Brygada zmechanizowana w obronie wybrzeża (wariant)
10. Struktura i zadania podstawowych komórek organizacyjnych NATO
11. Struktury cywilno-wojskowe zarządzania bezpieczeństwem militarnym NATO
12. Kategorie planowania NATO
13. Struktura i zadania podstawowych komórek organizacyjnych UE

Załącznik 1.

ARCHITEKTURA SYSTEMÓW INFORMATYCZNYCH

Produkty perspektywy technicznej powinny być zgodne ze specyfikacją zawartą w *NATO C3 Technical Architecture (NC3TA)* w wersji 7.0.

NC3TA definiuje NATO Common Operating Environment (NCOE), które określa usługi jakie powinny być dostępne na różnego typu komputerach w ramach systemu informatycznego. Usługi te podzielone są na następujące kategorie:

- aplikacje specyficzne dla misji (ang. specific mission applications);
- usługi aplikacji powszechnego zastosowania (ang. Common Support Application;
- Services;
- usługi infrastruktury (ang. infrastructure services);
- usługi jądra (ang. kernel services);
- usługi sieci (ang. network services).

NSV-9 - Prognoza technologii dla systemu

W poniższej tabeli przedstawiono obecnie używane lub wyłaniające się technologie informatyczne.

Lp.	Grupa technologii	Produkt (standard)
1.	Bezpieczeństwo	Secure HTTP (HTTPS) Secure Sockets Layer (SSL) Secure Network Communication (SNC) X.509
2.	Bazy danych	Oracle 10g Microsoft SQL Server MySQL x
3.	Formaty danych	XML, EDI, Java Business Integration (JSR-208)
4.	Komunikacja	JI NI
5.	Platformy aplikacyjne	JavaServer Faces (JSF) Java 2 Enterprise Edition (J2EE) Enterprise Generation Language (EGL) Eclipse Java 2 Standard Edition (J2SE) ASP .NET C# PHP5
CD	Architektura ukierunkowana na usługi	Simple Object Access Protocol (SOAP) Web Services Definition Language (WSDL) Reusable Asset Specification (RAS) Universal Description, Discovery and Integration (UDDI) eXtensible Markup Language (XML) Service Data Objects (SDOs) Business Process Execution Language (BPEL)

Źródło: Wykaz obowiązujących standardów technologii informatycznych do stosowania w resorcie obrony narodowej na lata 2007-2008, s. 6.

Załącznik 2.

Prognoza standardów technicznych

W poniższej tabeli zebrano pojawiające się standardy techniczne i normy:

Klasa usług:	Standardy i normy:
INTERFEJS UZYTKOWNIKA	
graficzny interfejs użytkownika	X Window System 11 R6.6
wygląd elementów interfejsu (ang.	CDE2.1
	Motif/CDE Style Guide Rev2.1
zestaw elementów interfejsu (ang. Toolkit)	**Motif 2.1**
ZARZĄDZANIE DANYMI	
obiektowy system zarządzania bazą danych	ODMG 3.0:2000
zdalny dostęp do danych	JDBC
	SQL CLI (ISO/IEC 9075-3:2003)
replikacja bazy danych	mechanizm replikacji ATCCIS
wspólny schemat danych NATO	NATO Corporate Data Model wersja 2 (ADatP-32)
	ISO 19107:2003
	ISO 19109:2003
WYMIANA DANYCH	
obrazy graficzne	WebCGM, W3C REC 20011217, 2001
	SVG Tiny oraz SVG Basic, W3C REC 20030114,2003
	JPEG 2000 (ISO/IEC 15444-1:2001)
	JPEG LS (ISO/IEC 14495:1999)
	BIIF (ISO 12087-5:1998)
wideo/audio	MPEG-4 (ISO/IEC 14496:2001)
komutacja ka ałów (ang.	Differential PCM (ITU-T G.726:1990)
	STANAG 4444 edycja 1
	MELP (STANAG 4591 edycja 0)
	STANAG 4421 edycja 1
	STANAG 4479 edycja 1
formaty symboliki (ang.	BIIF (ISO 12087-5:1998)
	NPIF (STANAG 7023 edycja 3)
	AR-TRI (STANAG 7024 edycja 2)
linki taktyczne (ang. Tactical Digital Information Links)	Link-22 (STANAG 5522 edycja 1, J-Series)
dane geograficzne	DIGEST wersja 2.1
	GML wersja 3.0:2004, OGC Ref. 02-023r4
	Geographic Information Metadata (ISO 19115:2003)
	WECDIS (STANAG 4564 edycja 1)
	SEDRIS (ISO/IEC CD 18023-1:2004)
	EDCS (ISO/IEC FCD 18025:2003)
	SRM (ISO/IEC CD 18026:2003)
opis stron dokumentów	DOM Level 3
	formaty Office XP
	XHTML 1.0:2002 (W3C)
	XML 1.0 edycja 3 :2004, W3C
	Link 1.0:2001, W3C
	XPointer 1.0:2001, W3C
	Relax NG (ISO/IEC 19757-2:2003)
	XMLInfoset:2001, W3C
	XSL Associaton:1999, W3C
	xml-names-19 990114:1999
	XSLT 1.0:1999
	XSL 1.0:2001

	XML Schema część 0-2:2001
	WML 2.0:2001
kompresja i archiwizacja	UNIX 98 (compress/uncompress, tar)
symbolika wojskowa	opis ISO/DIS 19117
	IHOS-52

usługi sieciowe	• ISO/DIS 19128 Web Map Service
	• Web Feature Service 1.0 (OGC Ref. 02-058)
	• Web Coverage Service 1.0 (OGC Ref. 03-065r6)
	• Web Registry Service 0.0.2 (OGC Ref. 01-024r1)
	• Catalog Interface 1.1.1 (OGC Ref. 02-087r3)
zestawy znaków	• ISO/IEC 15417:2000
	• ISO/IEC 15416:2000
kodowanie danych	• S/MIME ESS (RFC 2632:1999, 2633:1999)
• GRAFIKA	
projektowanie grafiki	• OpenGL wersja 2.0:2004
modelowanie grafiki	• UML 1.5:2003 (OMG)
• KOMUNIKACJA	
• warstwa aplikacji modelu ISO	
przesyłanie wiadomości	• eSMTP (RFC 1985:1996, 2034:1996, 2554:1999, 2920:2000, 3207:2002, 3461:2003)
	• ACP 145
	• IMAP4 (RFC 3501:2003)
katalog (ang. Directory)	• ACP 133C
	• DOP(ITU-TX.500:2001)
nazwy i adresowanie	• STANAG 4250 część 3
telekonferencje audio/wideo	• ACP 220:2003
warstwa sieci modelu OSI	•
rozwiązania internetowe	• IPv6 (RFC 2460:1998, 2461:1998, 2462:1998, 2463:1998, 2464:1998, 2375:1998, 2710:1999 uaktualnione przez 3590:2003, 3513:2003, 3587:2003)
	• IGMP wersja 3 (RFC 3376:2002)
	• Differentiated Services Field (RFC 2474:1998 uaktualnione przez 3168:2001, 3260:2002)
	• OSPF dla IPv6 (RFC 2740:1999)
	• RIPng dla IPv6 (RFC 2080:1997)
	• rozszerzenia BGP-4 (RFC 2858:2000, 2545:1999)
	• PIM-DM
	• NAT-PT (RFC 2766:2000 uaktualnione przez 3596:2003)
	• Mobile IPv6 (RFC 3775:2004)
	• IPSec i Mobile IPv6 (RFC 3776:2004)
	• Policy-based Network Management-General (RFC 1104, 2753, 3198, 3334)
	• Policy-based Network Management -DiffServ (RFC 2963, 2998, 3086, 3260, 3287, 3289, 3290, 3308, 3496)
	• Policy-based Network Management-IntServ (RFC 2205-2210, 2370, 2380, 2382, 2430, 2490, 2745 - 2747, 2749, 2750, 2755, 2814, 2872, 2961, 2996, 3097, 3175, 3181, 3182, 3209, 3210, 3468, 3473, 3474, 3476, 3477)
WAN na łączach komutowanych (ang. Circuit switched WAN)	• EDSTG (STANAG 4578 edycja 1)
morska sieć taktyczna WAN (ang	• IPv6 over PPP (RFC 2472:1998)
	• UNI wersja 4.1:2002 (af-sig-0061.0001)
	• PNNI wersja 1.1:2002 (af-pn i-0055.0001)
linki taktyczne	• STANAG 4444 edycja 1
warstwa łącza danych / fizyczna modelu OSI	•
łączność satelitarna	• STANAG 4271 edycja 0
	• STANAG 4492 edycja 1
	• STANAG 4505 edycja 0
	• STANAG 4577 edycja 0
	• STANAG 4606 edycja 0

	• STANAG 4622 edycja 0
łączność radiowa	• STANAG 4444 edycja 1
	• STANAG 4538 edycja 1
	• STANAG 4539 edycja 1
• SYSTEMY OPERACYJNE	
systemy czasu rzeczywistego	• Linux Standard Base Spec. 1.3 (Free Standards Group), 2002
• systemy inne niż czasu rzeczywistego	• Linux Standard Base Spec. 1.3 (Free Standards Group), 2002
•	• MS Windows XP (oraz 2003 Server)
• ZARZĄDZANIE SYSTEMAMI	
• Zarządzanie siecią LAN	• SNMPv3 (RFC 3413:2002)
•	• Message Processing and Dispatching for SNMP (RFC 3412:2002)
•	• USM for SNMPv3 (RFC 3414:2002)
•	• VACM for SNMP (RFC 3415:2002)
•	• RFC 3411:2002
•	• RMON 2 MIB (RFC 2021:1997)
• Zarządzanie siecią WAN	• CIM
• BEZPIECZEŃSTWO	
• uwierzytelnianie	• Single Sign On (The Open Group)
• poufność	• TLS (RFC 2246:1999 uaktualnione przez RFC 3546:2003)
•	• IP ESP (RFC 2401:1998-2412:1998 uaktualnione przez RFC 3168:2001)
• karty identyfikacyj e	• ISO/IEC 7810:2003
•	• ISO 7812:2000
•	• ISO/IEC 7816:1999
•	• specyfikacja PC/SC wersja 1.0
•	• JAVACard
•	• ISO/IEC 144443:2000
• poufność treści wiadomości	• ESS (RFC 2632:1999, 2633:1999)
• etykietowanie wiadomości	• X.411:1999
• PRZETWARZANIE ROZPROSZONE	
• środowisko rozproszone	• DCE 1.1
•	• ONC 1.1 (The Open Group)
• procesy	• DCERPC1.1
•	• MS-RPC - jako część interfejsu MS Windows 2000
• pliki	• DCEDFS1.1
•	• XNFS 3W (The Open Group)
• drukowanie	• MS-SMB -jako część MS Windows 2000
• czas	• DCEDTS 1.1
• obiekty	• CORBA/IIOP2.2
•	• MS DCOM/ActiveX-jako część interfejsu MS Windows 2000
•	• SOAP 1.2, W3C
• symulacje	• HLA(IEEE 1516:2000)
• usługi	• UDDI 3.0, W3C
•	• WSDL 1.1:2001, W3C
•	• XPath 2.0:2003, W3C
•	• WS-I Web Service Basic Profile 1.1:2004
•	• WS-I Simple SOAP Binding Profile 1.0:2004
•	• WS-I Attachments Profile 1.0:2004
• INŻYNIERIA OPROGRAMOWANIA	
• języki programowania	• Java (ISO JSG)
•	• C#
• metodyki	• IEEE/EIA 12207:1996
•	• EIAIS640
•	• UML 2.0:2003 (OMG)

Źródło: Wykaz obowiązujących standardów technologii informatycznych do stosowania w resorcie obrony narodowej na lata 2007-2008, s. 14.

Załącznik 3.

ARCHITEKTURA RESORTOWYCH SYSTEMÓW INFORMATYCZNYCH

Specyfikacja standardów w układzie dziedzinowym:

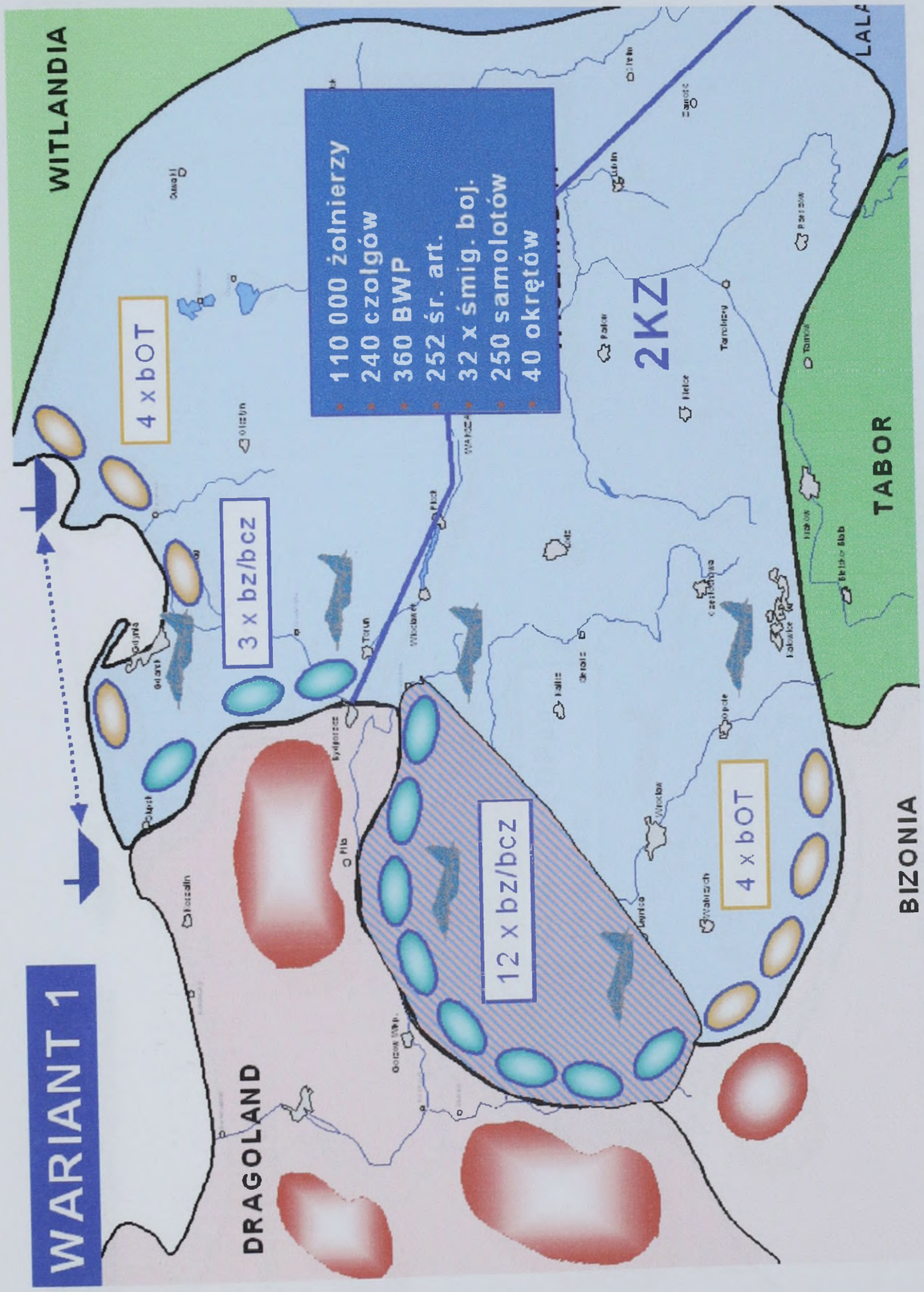
- wdrożenie do eksploatacji użytkowej efektywnych technologii informatycznych nowych;
- generacji;
- budowę i wdrożenie zintegrowanych i kompleksowych stacjonarnych systemów;
- informatycznych; automatyzację i integrację procesów dowodzenia i kierowania środkami;
- walki;
- budowę i wdrożenie sieci komputerowych;
- zapewnienie bezpieczeństwa i ochrony systemów;
- budowę i wdrożenie systemów zarządzania zasobami teleinformatycznymi w resorcie;
- obrony narodowej.

obowiązujące i dopuszczalne standardy w zakresie oprogramowania, z podziałem na poszczególne dziedziny usług programowo-systemowych, tj.:

1) Systemy operacyjne.
2) Języki programowania.
3) Narzędzia CASE (komputerowe wspomaganie inżynierii oprogramowania).
4) Interfejs użytkownika.
5) Zarządzanie bazami danych.
6) Poczta elektroniczna i praca grupowa.
7) Grafika operacyjna.
8) Usługi sieciowe.
9) Zarządzanie zasobami teleinformatycznymi.
10) Usługi biurowe.
11) Oprogramowanie antywirusowe.
12) Oprogramowanie specjalistyczne.
13) Oprogramowanie do projektowania sieci teleinformatycznych.

Źródło: Wykaz obowiązujących standardów technologii informatycznych do stosowania w resorcie obrony narodowej na lata 2007-2008, s. 18.

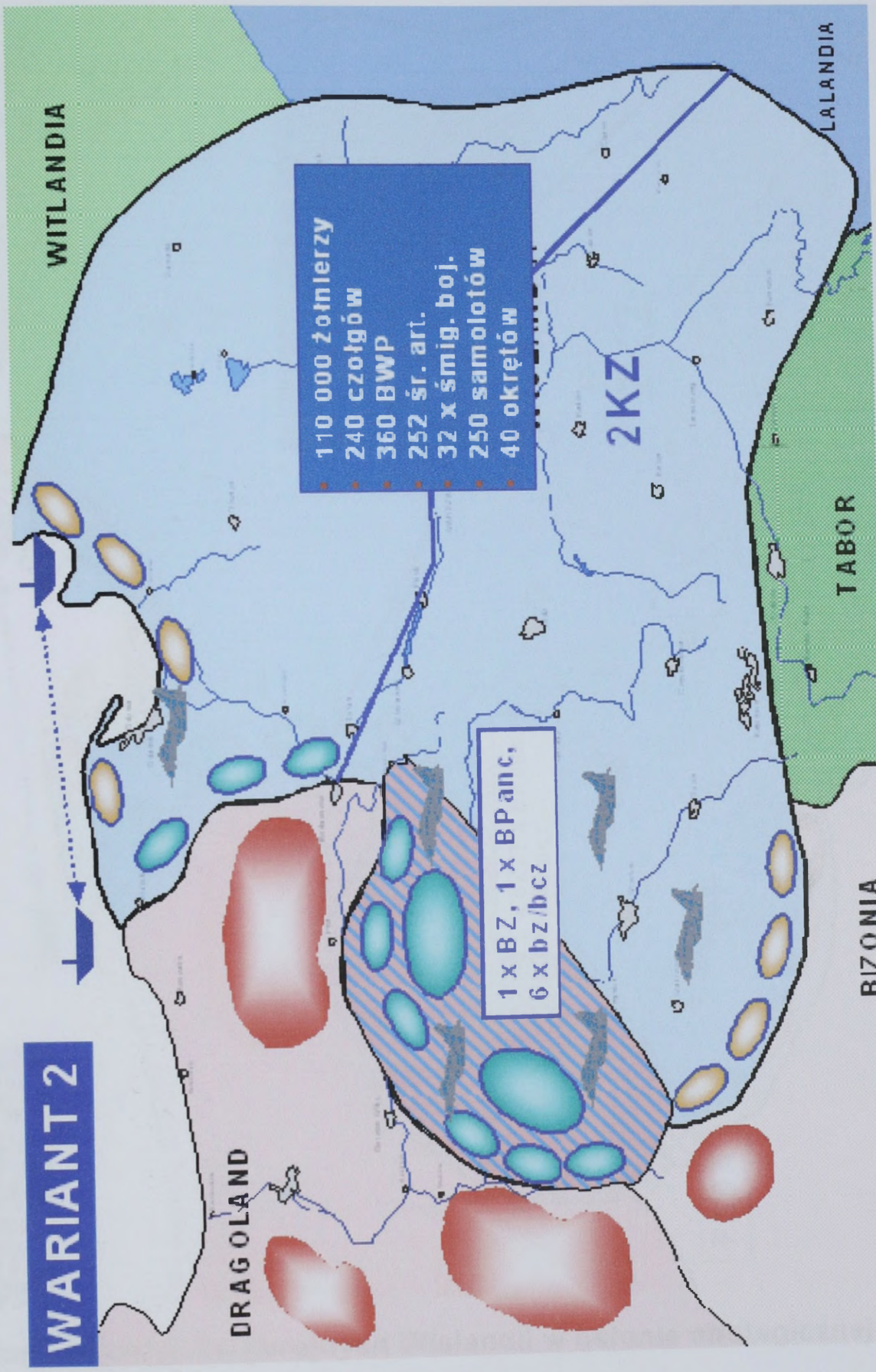
Załącznik 4.



Wariant działania Sił Zbrojnych Wislandii w osłonie strategicznej

Źródło: trening sztabowy pk. CZERWIEC, Generalny Zarząd Operacyjny SG, Zespół Planowania Operacyjnego

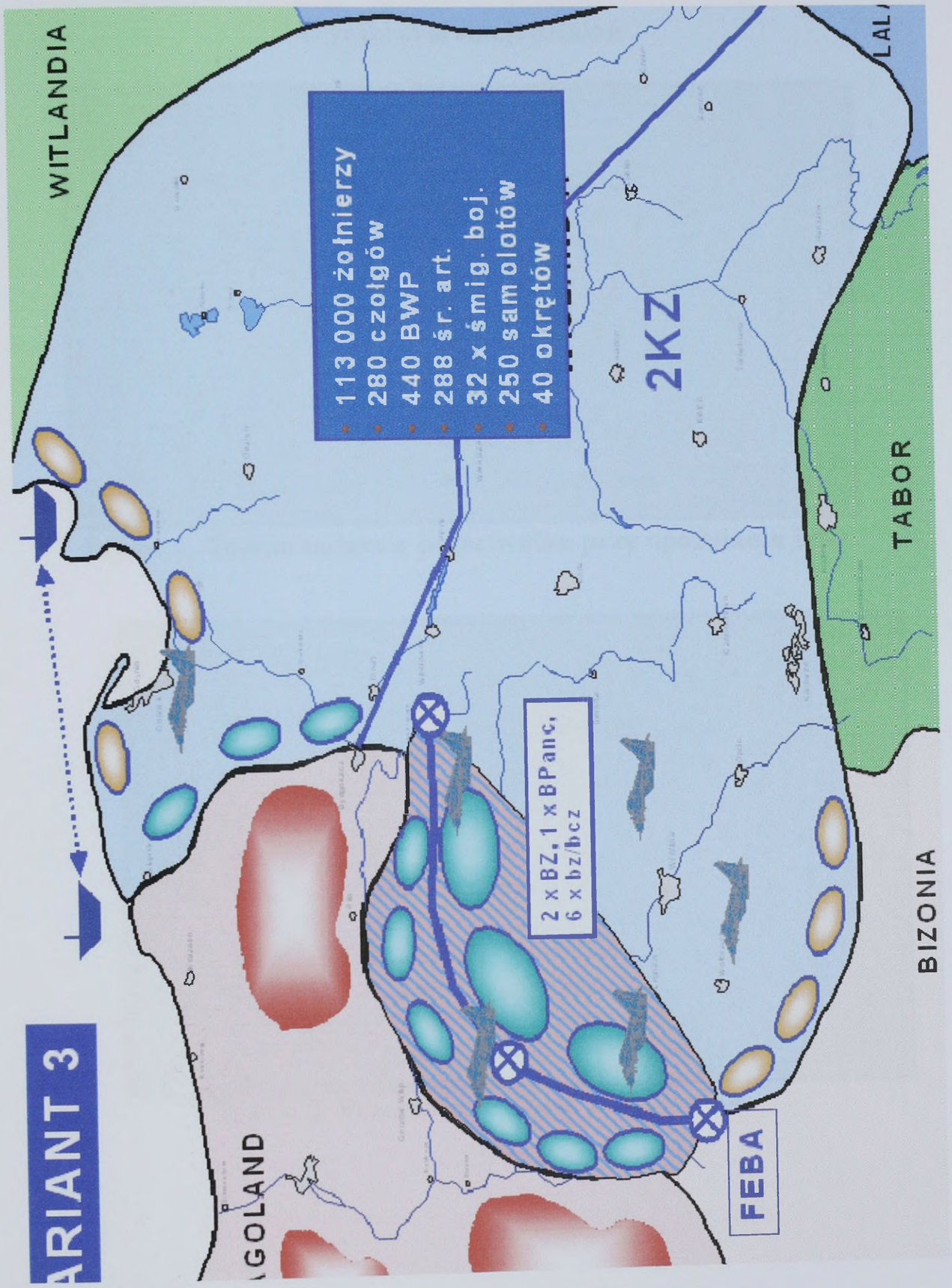
Załącznik 5.



Wariant działania Sił Zbrojnych Wislandii w osłonie strategicznej.

Źródło: trening sztabowy pk. CZERWIEC, Generalny Zarząd Operacyjny SG, Zespół Planowania Operacyjnego.

Załącznik 6.

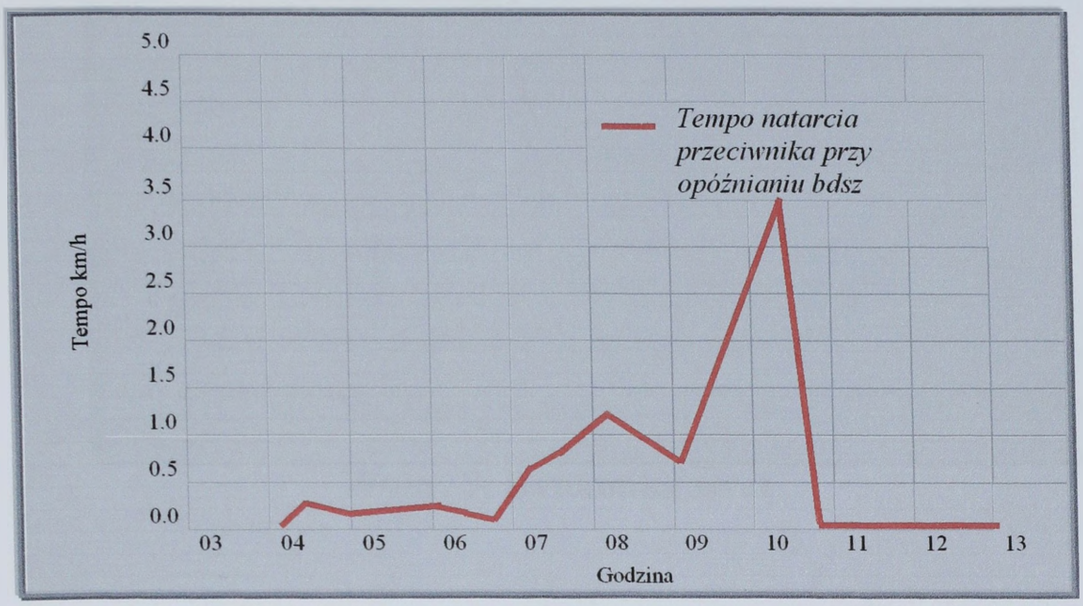


Wariant działania Sił Zbrojnych Wislandii w osłonie strategicznej

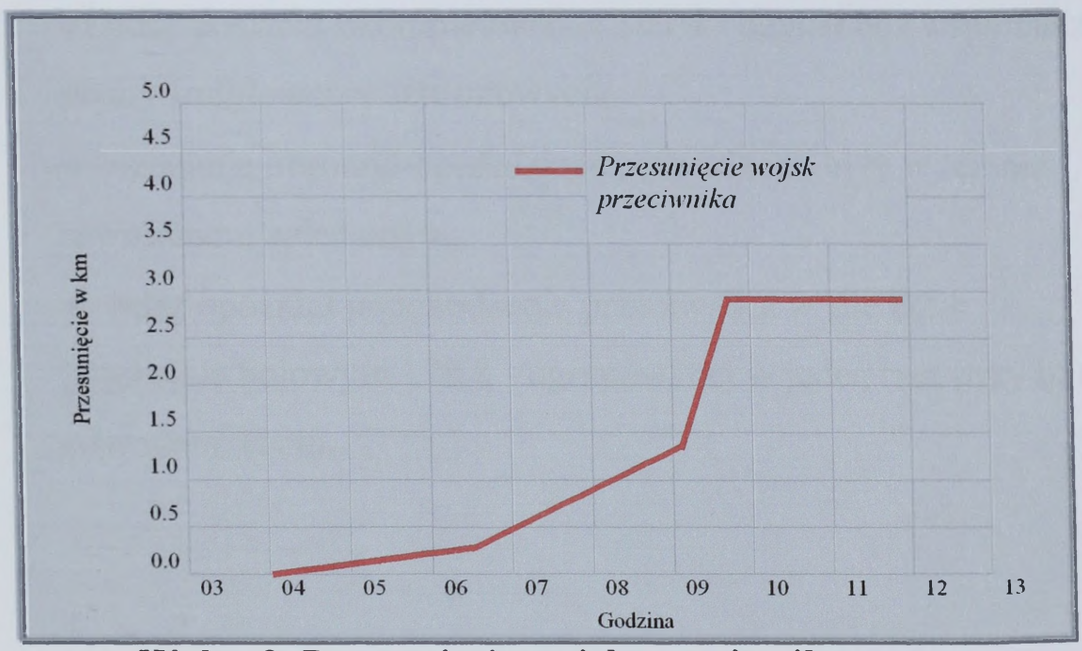
Źródło: trening sztabowy pk. CZERWIEC, Generalny Zarząd Operacyjny SG, Zespół Planowania Operacyjnego.

Załącznik 7.

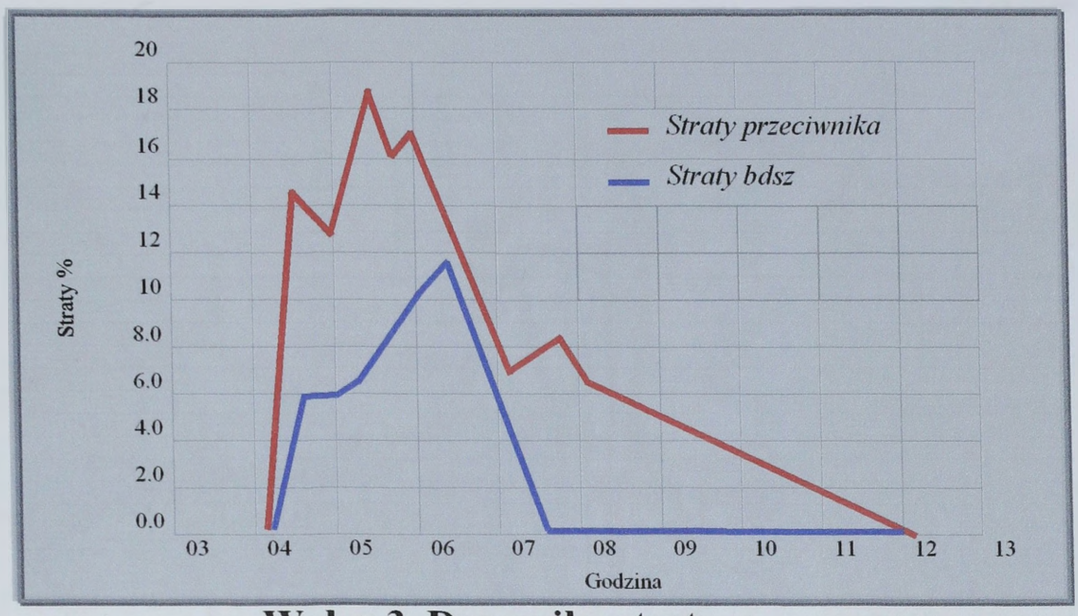
Wyniki symulacji działań



Wykr. 1. Tempo natarcia przeciwnika przy opóźnianiu bdsz



Wykr. 2. Przesunięcie wojsk przeciwnika



Wykr. 3. Dynamika strat

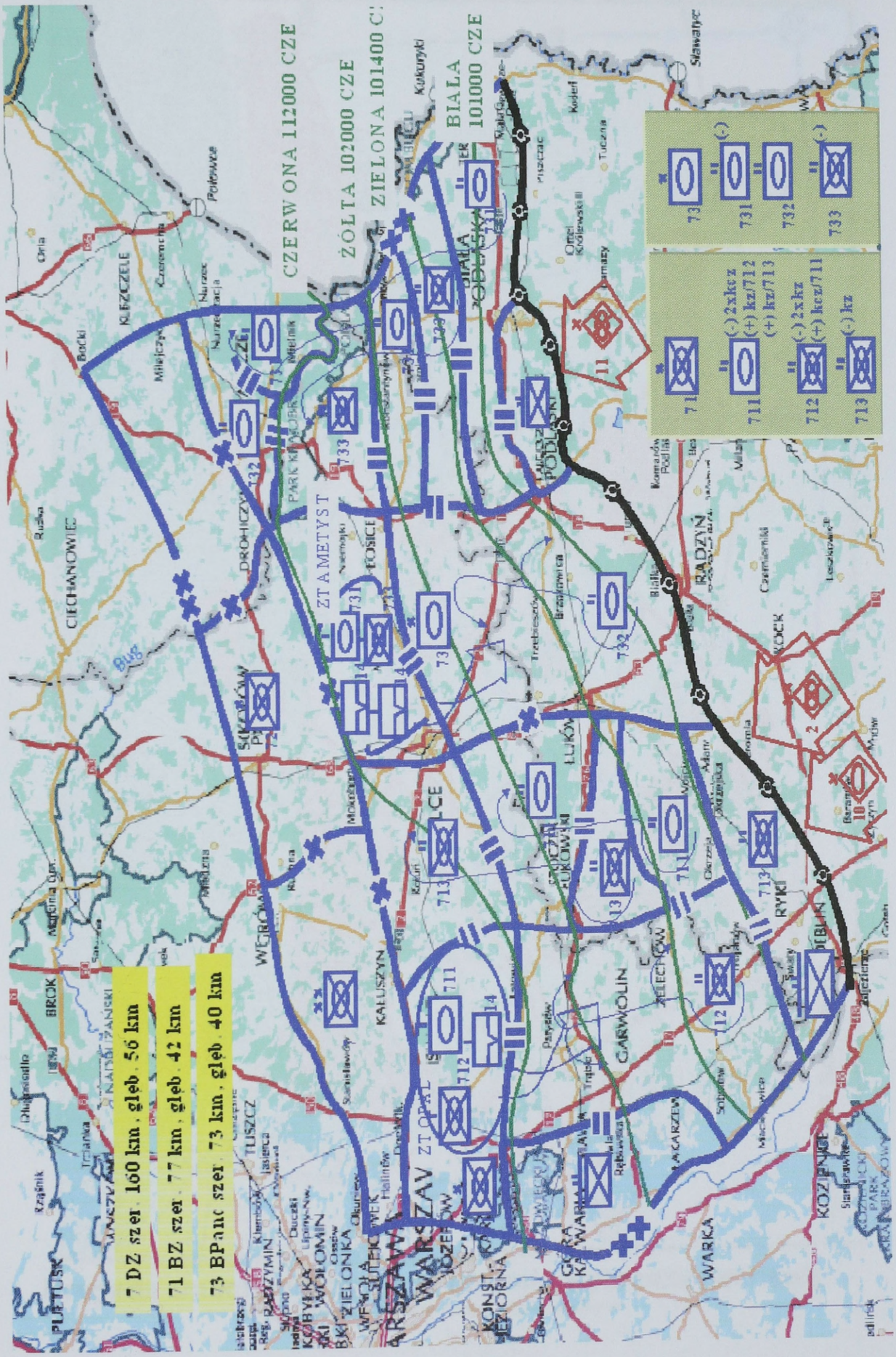
Założone warunki symulacji działań[1]

W wariancie, założono następujące warunki działania:

- bdsz posiadał ukompletowanie 100% i działał bez wsparcia ze strony śmigłowców szturmowych;
- działania obronno-opóźniające prowadzone były w terenie równinnym, zalesionym;
- bdsz opóźniał podchodzenie przeciwnika w sile BZ o potencjale bojowym 178,8 - ugrupowanej w jeden rzut (trzy bz) z odwodem (bcz).

[1] Symulacji dokonano przy użyciu programu komputerowego MODEL 96. Z powodu braku w bazie danych programu symulacyjnego, bdsz o strukturze i wyposażeniu jak proponowany w rozdziale IV jego perspektywiczny model, dla potrzeb symulacji wzmocniono go odpowiednimi siłami i środkami w celu uzyskania wymaganych możliwości bojowych.

Załącznik 8.



Schemat działania 7 DZ w ćwiczeniu dowódczo-sztabowym p.k. „PIERŚCIEŃ”

Załącznik 9.

Brygada zmechanizowana w obronie wybrzeża (wariant)

Źródło: materiały Zakładu Taktyki Wojsk Lądowych

Załącznik 10.

STRUKTURA I ZADANIA PODSTAWOWYCH KOMÓREK ORGANIZACYJNYCH NATO[1]

Rada Północnoatlantycka (North Atlantic Council - NAC) jest to podstawowy organ decyzyjny NATO. W jej skład wchodzą przedstawiciele państw członkowskich w randze ambasadorów; jest organem plenarnym, wyposażonym w prawo powoływania innych organów NATO. Obraduje ona na posiedzeniach odbywających się na następujących szczeblach:

- szefów państw i rządów; są to tzw. szczyty NATO, zwoływane okazjonalnie;
- ministerialnym; spotykają się ministrowie państw członkowskich, co najmniej dwa razy na rok;
- stałych przedstawicieli; spotykają się regularnie, co najmniej raz w tygodniu przedstawiciele państw członkowskich. Mają oni rangę ambasadorów. Stali przedstawiciele tworzą Radę Stałych Przedstawicieli.

Rada Północnoatlantycka jest zwoływana na żądanie swego przewodniczącego lub któregokolwiek państwa członkowskiego. Przy podejmowaniu decyzji obowiązuje zasada jednomyślności - consensusu. Podejmowane przez Radę zalecenia nie mają charakteru wiążącego, bez względu na to, na jakim zapadły szczeblu.

Do najważniejszych zadań Rady należą:

- konsultacje polityczne pomiędzy członkami;
- wyznaczanie dyrektyw dla władz wojskowych;
- obrona cywilna;
- ustalanie wysiłku zbrojeniowego państw członkowskich.

Komitet Planowania Obrony (Defence Planning Committee - DPC), jest to organ, który podejmuje zasadnicze decyzje w kwestii planowania obronnego Sojuszu. Składa się z przedstawicieli państw członkowskich. Jego posiedzenia odbywają się na dwóch szczeblach:

- ministerialnym; tu obradują dwa razy w roku ministrowie obrony państw członkowskich;
- stałych przedstawicieli.

Grupa Planowania Nuklearnego (Nuclear Planning Group - NPG), zajmuje się planowaniem potencjału nuklearnego NATO i doktryną jego użycia. Zajmuje się ona oceną polityki nuklearnej przeciwników, bada kryteria i rozmieszczenie broni itp. Stanowi ona najważniejsze forum konsultacyjne we wszystkich sprawach związanych z rolą sił jądrowych w polityce wojskowej NATO.

System ciał kolegialnych uzupełniają liczne komitety specjalistyczne, które działają na mocy mandatu przyznanego im przez Radę Północnoatlantycką (państwa członkowskie reprezentowane są w nich przez przedstawicieli delegacji narodowych), podejmują szczegółowe decyzje merytoryczne w poszczególnych dziedzinach funkcjonowania Sojuszu oraz nadzorują ich wykonanie.

---

[1] Na podstawie: *Vademecum NATO*, Warszawa 2001; www.nato.int.; S. Koziej, *Między piekłem a rajem, szare bezpieczeństwo na progu XXI wieku*, Toruń 2006; W. Feler, *Współczesne bezpieczeństwo*, Toruń 2003.

Sekretariat Międzynarodowy składa się z Sekretarza Generalnego, jego zastępcy oraz asystentów.
Sekretarz Generalny pełni funkcje:

- przewodniczenia - przewodniczy m.in. posiedzeniom Rady Północnoatlantyckiej, Komitetu Planowania Obrony;
- nadzorcze - sprawuje nadzór nad wykonywaniem uchwał organów NATO, opracowywaniem raportów itp.

Zintegrowana Struktura Wojskowa (Integrated Military Structure) stanowi właściwą militarną część Sojuszu. Składa się ona z systemu funkcjonujących permanentnie połączonych dowództw i sztabów oraz kontyngentów sił zbrojnych, wydzielonych przez państwa członkowskie do operowania w ramach połączonych zgrupowań strategicznych i operacyjnych w czasie konfliktu zbrojnego lub innej operacji wojskowej.
Nastawiona jest ona na realizację planów nakreślonych przez strukturę polityczną Sojuszu oraz zgłaszanie ewentualnych uwag i wniosków dotyczących następnych okresów planistycznych.

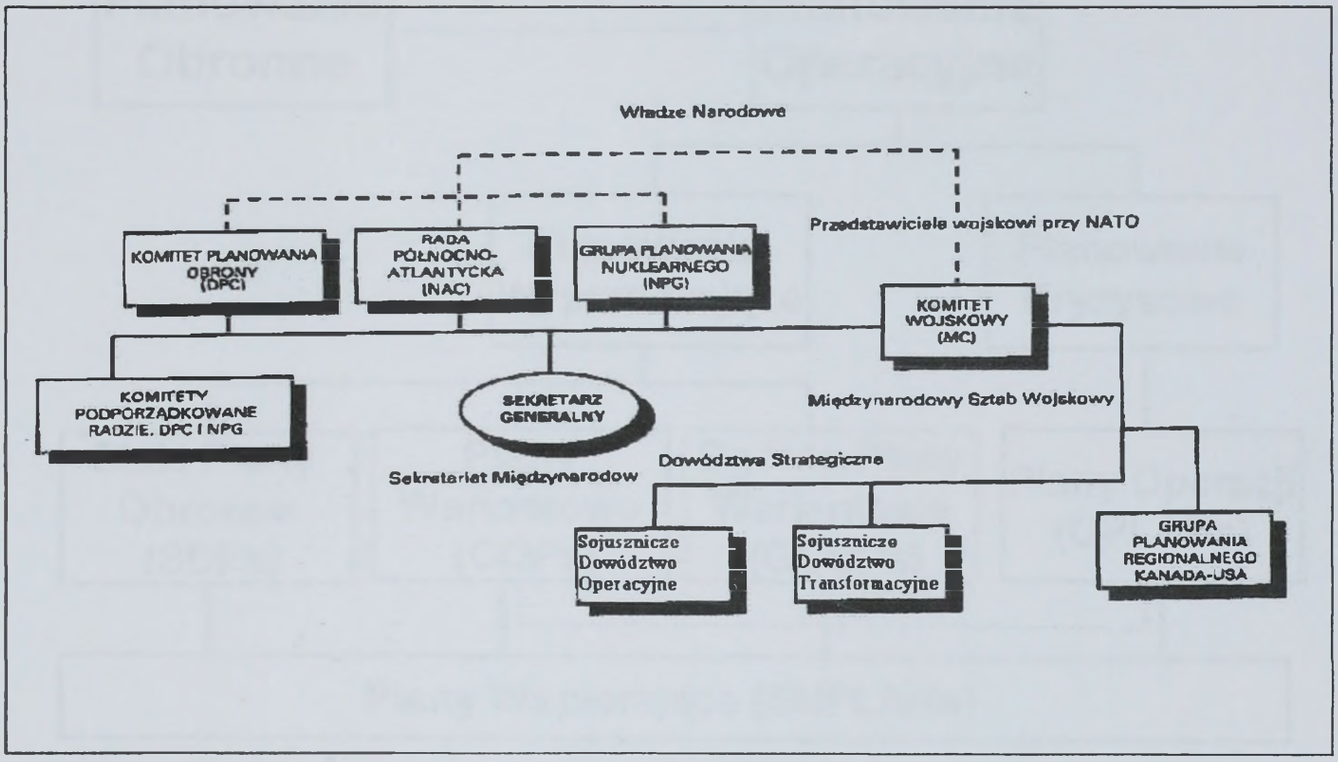
Komitet Wojskowy jest najwyższym ciałem konsultacyjnym i doradczym Rady Północnoatlantyckiej w dziedzinie wojskowej. Jest to najwyższy organ decyzyjny w sprawach wojskowych NATO. Podlega on cywilnemu Komitetowi Planowania Obrony. Składa się on z narodowych reprezentantów wojskowych, będący stałymi przedstawicielami szefów sztabów sił zbrojnych państw członkowskich. Obsługę prac Komitetu Wojskowego NATO zapewnia Międzynarodowy Sztab Wojskowy (IMS), który obok Sekretarza Generalnego i podległych mu biur (Sekretariat Wykonawczy, Biuro Prasy i Informacji, Biuro Bezpieczeństwa NATO) oraz Sztabu Międzynarodowego (IS) stanowi centralny organ wykonawczy Sojuszu.
Komitet Wojskowy jest organem kierowniczym - wobec Dowództw regionalnych i innych organów wojskowych, i opiniującym - wobec Komitetu Planowania Obrony i Grupy Planowania Nuklearnego.
Komitet Wojskowy obraduje na:

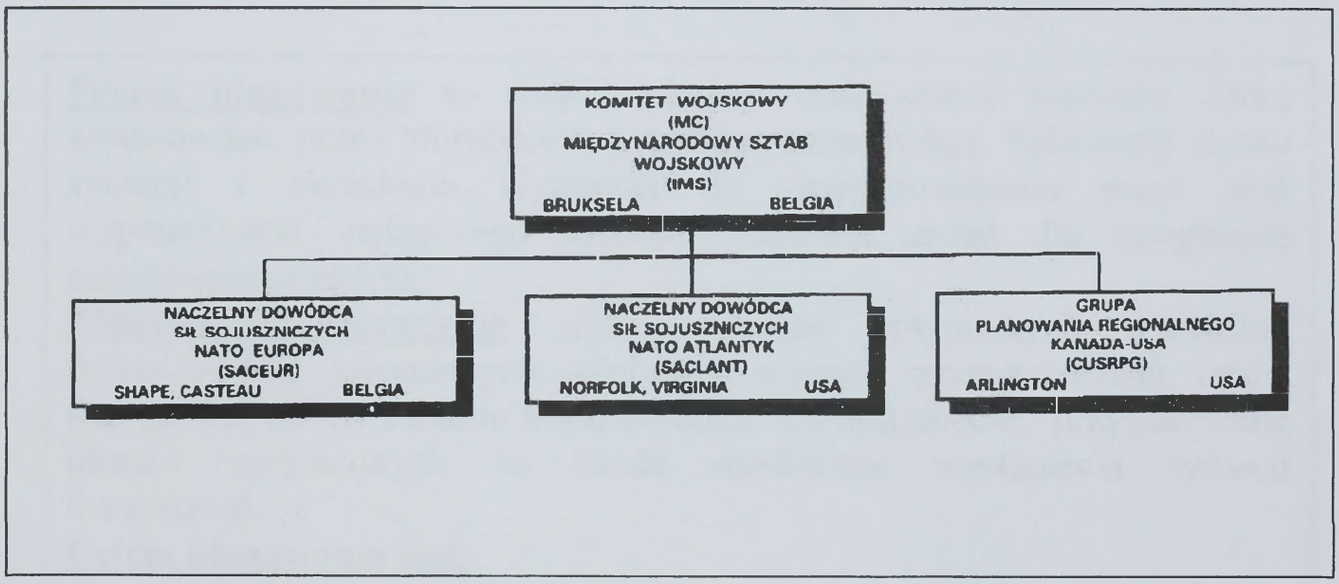
- szczeblu szefów sztabów generalnych poszczególnych państw członkowskich (oprócz Islandii, która nie ma sił zbrojnych i Francji, chyba, że jej Prezydent wyrazi indywidualną zgodę);
- szczeblu przedstawicieli sztabów generalnych - w formie Stałego Komitetu Wojskowego.

Międzynarodowy Sztab Wojskowy jest organem pomocniczym i wykonawczym w stosunku do Komitetu Wojskowego. Wykonuje jego decyzje wydawane w formie rozkazów dla dowództw regionalnych. Ponadto Międzynarodowy Sztab Wojskowy przygotowuje plany, inicjuje studia nad problematyką wojskową, utrzymuje kontakty z Sekretarzem Generalnym oraz Komitetami.

Załącznik 11.

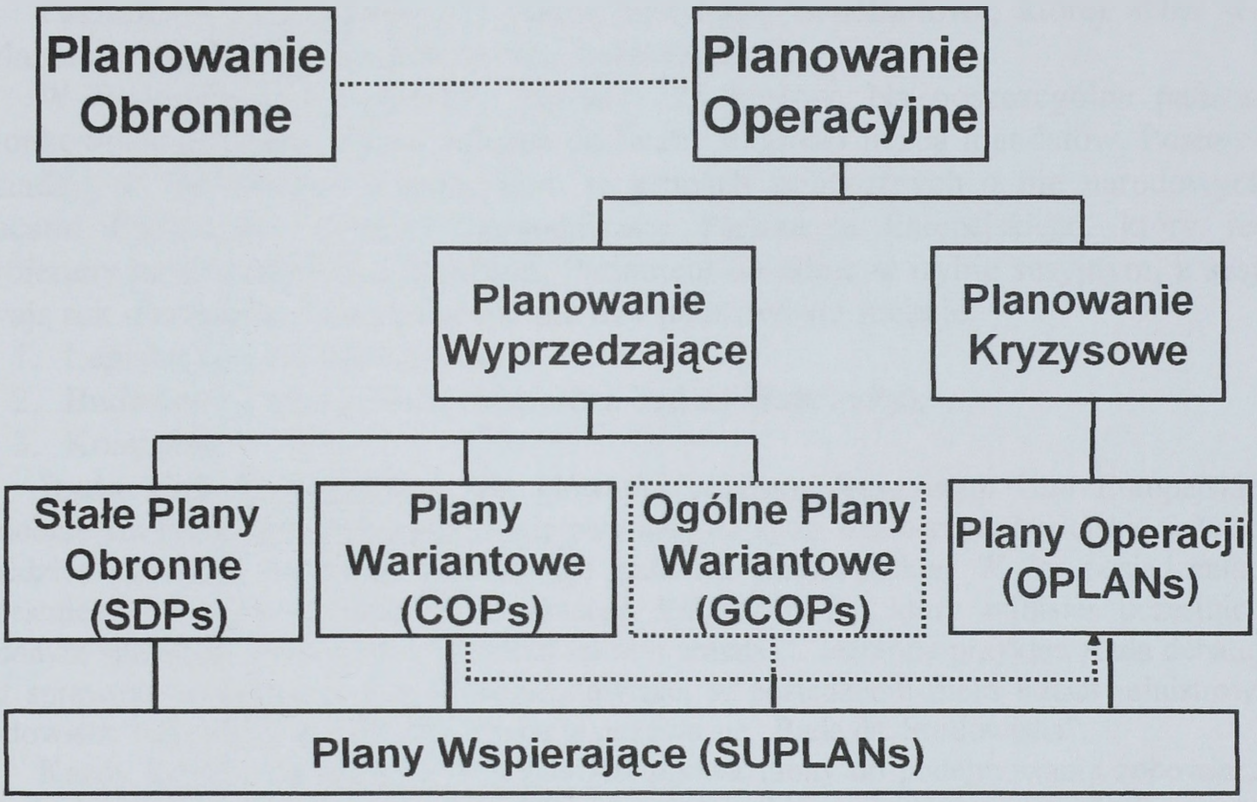
STRUKTURY CYWILNO-WOJSKOWE ZARZĄDZANIA BEZPIECZEŃSTWEM MILITARNYM NATO





Załącznik 12.

KATEGORIE PLANOWANIA NATO



Proces planowania to zespół zdarzeń oraz zestaw procedur, które zastosowane przez dowódców i sztaby umożliwiają dokonanie oceny sytuacji i określenia wymagań do przeprowadzenia misji oraz wypracowania najlepszego sposobu realizacji zadań dla osiągnięcia oczekiwanego efektu.

Planowanie operacyjne służy wyborze optymalnych rozwiązań wykorzystania posiadanych zdolności sojuszu; przekształceniu celów strategicznych w zadania umożliwiające ich osiągnięcie; przygotowanie planów operacyjnych na każdą możliwość wystąpienia sytuacji kryzysowej.

Celem planowania jest:

- przygotowanie planów prowadzenia przyszłych operacji sojuszu;
- umożliwienie sprawnego pozyskania sił do operacji i ich rozwinięcia w rejonie operacji;
- stworzenie warunków do osiągnięcia celów operacji oraz pożądanego stanu końcowego zgodnie z wytycznymi przełożonych;
- utrzymywanie uaktualnionych planów operacji w celu szybkiej odpowiedzi na pojawiające się zagrożenie.

Załącznik 13.

STRUKTURA I ZADANIA PODSTAWOWYCH KOMÓREK ORGANIZACYJNYCH UE[1]

Parlament Europejski jest jedyną instytucją wspólnotową, której skład jest wyłaniany w wyborach powszechnych i bezpośrednich.

W Parlamencie Europejskim zasiada 723 posłów. Na poszczególne państwa członkowskie przypada różna, zależna od liczby ludności liczba mandatów. Posłowie zasiadają w Parlamencie Europejskim w grupach politycznych a nie narodowych. Pracami Parlamentu kieruje Przewodniczący Parlamentu Europejskiego, który jest wybierany na posiedzeniu plenarnym. Parlament obraduje w trybie sesyjnym, a sesje trwają rok. Parlament Europejski spełnia trzy podstawowe funkcje:

1. Legislacyjną (wespół z Radą).
2. Budżetową (wraz z Radą zatwierdza budżet Wspólnoty).
3. Kontrolną.

Rada Unii Europejskiej jest głównym organem decyzyjnym Unii Europejskiej. Podobnie jak Parlament Europejski, Radę powołały do życia traktaty założycielskie w latach pięćdziesiątych XX w. Rada reprezentuje państwa członkowskie. W jej posiedzeniach uczestniczy po jednym ministrze z każdego kraju Unii.To, który minister uczestniczy w danym spotkaniu, zależy od poruszanej na nim tematyki. Jeżeli na przykład Rada debatuje nad sprawami związanymi z ochroną środowiska, w posiedzeniu biorą udział ministrowie środowiska wszystkich państw UE, a radę tę nazywa się „Radą ds. Środowiska".

Każdy minister zasiadający w radzie jest upoważniony do podejmowania zobowiązań w imieniu swojego rządu. Innymi słowy, podpis takiego ministra jest równoznaczny z podpisem całego rządu. Ponadto każdy minister w Radzie odpowiada przed parlamentem swojego kraju oraz przed reprezentowanymi przezeń obywatelami. To właśnie stanowi umocowanie demokratyczne decyzji Rady.

Maksymalnie cztery razy do roku prezydenci lub premierzy państw członkowskich wraz z przewodniczącym Komisji Europejskiej spotykają się jako Rada Europejska. Podczas tych „szczytów UE" wyznaczane są ogólne kierunki polityki Unii i rozwiązywane problemy, których nie można było rozwiązać na niższym szczeblu (tzn. na szczeblu ministrów w ramach zwykłych posiedzeń Rady). Debaty Rady Europejskiej ze względu na ważkość tematyki często przedłużają się do późnych godzin nocnych i przyciągają sporą uwagę mediów.

Komisja Europejska jest niezależna od rządów krajowych. Jej zadaniem jest reprezentowanie i ochrona wspólnych interesów całej Unii Europejskiej. Komisja przygotowuje wnioski dotyczące nowych aktów prawa europejskiego, które następnie przedkłada do zatwierdzenia Parlamentowi i Radzie. Jest również organem wykonawczym Unii – a więc odpowiada za wprowadzanie w życie decyzji Parlamentu i Rady. Oznacza to zarządzanie bieżącymi sprawami Unii Europejskiej, wdrażanie jej polityk, prowadzenie jej programów i dysponowanie jej środkami finansowymi.

Podobnie jak Parlament Europejski i Radę, Komisję powołały do życia traktaty założycielskie UE w latach pięćdziesiątych XX w.

[1] http://europa.eu/index_pl.htm; http://europa.eu/institutions/inst/comm/index_pl.htm; S. Koziej, *Między piekłem a rajem, szare bezpieczeństwo na progu XXI wieku*, Toruń 2006; W. Feler, *Współczesne bezpieczeństwo*, Toruń 2003. R. Zięba, Bezpieczeństwo międzynarodowe po zimnej wojnie, Warszawa 2008.