* 55

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH
INSTYTUT ZARZĄDZANIA I DOWODZENIA
ZAKŁAD ROZPOZNANIA I WALKI ELEKTRONICZNEJ

ROZPOZNANIE W DZIAŁANIACH ASYMETRYCZNYCH

Praca naukowo-badawcza
Kryptonim „NEFRYT-2"
Kod pracy II.2.2.3.0

PAN B

WARSZAWA

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH
INSTYTUT ZARZĄDZANIA I DOWODZENIA
ZAKŁAD ROZPOZNANIA I WALKI ELEKTRONICZNEJ

ROZPOZNANIE W DZIAŁANIACH ASYMETRYCZNYCH

Praca naukowo-badawcza
Kryptonim „NEFRYT-2"
Kod pracy II.2.2.3.0

WARSZAWA

AKADEMIA OBRONY NARODOWEJ
WYDZIAŁ WOJSK LĄDOWYCH
INSTYTUT ZARZĄDZANIA I DOWODZENIA
ZAKŁAD ROZPOZNANIA I WALKI ELEKTRONICZNEJ

ROZPOZNANIE W DZIAŁANIACH ASYMETRYCZNYCH

Praca naukowo - badawcza

Kryptonim „NEFRYT-2"

kod pracy: II.2.2.3.0

WARSZAWA 2006

Recenzent pracy: **płk dr hab. Józef JANCZAK**

Kierownik zdania naukowego: prof. dr hab. inż. Józef MICHNIAK

Zespół autorski:

1.	Płk dr inż. Marek WRZOSEK (kierownik tematu)	- wstęp; - rozdział 1, 2; 6; - zakończenie; oraz załączniki 1,2,3,4,5,7,8,9.
2.	Ppłk dr inż. Andrzej NOWAK	- rozdział 3;
4.	Ppłk dr inż. Grzegorz ROSŁAN	- rozdział 4; oraz załącznik 6;
5.	Ppłk dr inż. Waldemar SCHEFFS	- rozdział 5;

3

Spis treści

WSTĘP

Koniec zimnej wojny nie spowodował końca wewnętrznych lub regionalnych źródeł konfliktu i długo oczekiwanego pokoju. Dzisiaj, w ocenie ekspertów wiele krajów międzynarodowej społeczności staje w obliczu jednej z wielu odmian działań militarnych. Powstania zbrojne, wewnętrzne wojny i inne odmiany konfliktów w małej skali (*small-scale conflict*), które choć jeszcze nie są dominujące to wkrótce będą najprawdopodobniej częstym typem konfliktu w nowym światowym porządku. Jest bardzo prawdopodobne, że wcześniej lub później, liczne państwa zostaną uwikłane, bezpośrednio albo pośrednio, w odmiany różnego typu konfliktów militarnych. Pewne wydaje się także, iż zróżnicowane doświadczenia wyniesione z walk z przeciwnikiem nieokreślonym, pozbawionym jasnych struktur organizacyjnych i standardowej taktyki (np.: walki w Wietnamie, Algierii, Jugosławii, Somalii, Afganistanie, Iraku) zmieniają sposób myślenia o prowadzeniu regularnych działań zbrojnych. Jako efekt minionych wydarzeń w wielu armiach świata prowadzi się szerokie studia na poziomie strategicznym zarówno doświadczeń wyniesionych z małych, lokalnych konfliktów, które przez lata miały miejsce w przeszłości, jak również wielonarodowych operacji początku XXI wieku.

Na podstawie zgromadzonych doświadczeń można wnioskować, że zagrożenie nieregularne, a więc asymetryczne stwarza najczęściej strona, która dążąc do konfrontacji (zbrojnej lub niezbrojnej), nie jest zdolna przeciwstawić się agresorowi w sposób symetryczny (regularny), z użyciem tych samych lub zbliżonych potencjałem środków walki (np.: wojna partyzancka armii fińskiej przeciwko wojskom radzieckim, ruch oporu w latach drugiej wojny światowej skierowany przeciw niemieckiemu agresorowi). W opinii ekspertów przeważa pogląd, że w takiej sytuacji strona „A" hipotetycznego konfliktu opierająca się na działaniach asymetrycznych stara się tak wybrać taki obszar konfrontacji, aby maksymalnie ograniczyć możliwość wykorzystania przez stronę przeciwną „B" jej przeważającego potencjału bojowego lub gospodarczego. Ponadto jak wskazują doświadczenia, działania asymetryczne w wymiarze militarnym są prowadzone wówczas, kiedy jedna ze stron konfliktu dokona przełomu technicznego lub technologicznego, zmieniającego możliwości i zdolność bojową sił zbrojnych. Przykładem potwierdzającym powyższą tezę jest fakt wyprodukowania i użycia przez USA broni jądrowej przeciwko Japonii oraz utrzymujące się

do dziś zagrożenie wykorzystania środków masowego rażenia (np.:Iran, Korea). W tej sytuacji dysponowanie jedynie przez jedną ze stron konfliktu odmiennymi środkami walki prowadzi do asymetrii działań.

Ponadto w opinii ekspertów, należy dostrzegać fakt, że nowe środki oddziaływania, bazujące zarówno na zjawiskach znanych, ale dotychczas niewykorzystywanych jako środki walki, jak i na zjawiskach nowo poznanych, umożliwiły wyprodukowanie broni porównywalnej do klasycznych środków walki (np.: broń precyzyjnego rażenia) oraz opracowanie zupełnie nowych środków (bronie niezabijające – *non lenthal weapons*), będących produktem wykorzystywania szczególnie zawansowanych technik i technologii (np.: inżynieria genetyczna, informatyka).

Na podstawie wyników analizy literatury można także wnioskować, że rola i wzrastające znaczenie problematyki zagrożeń asymetrycznych zostały dostrzeżone już we wczesnych latach dziewięćdziesiątych[1], głównie w kontekście przyczyn ich powstawania, a także potencjalnego ryzyka generowania konfliktów. Zagrożenia asymetryczne były przedmiotem zainteresowania w aspekcie zarówno krótko- i długoterminowych prognoz ich występowania, a także, co szczególnie istotne z punktu widzenia systemu rozpoznania, oceny ewentualnych skutków w wymiarze lokalnym, regionalnym i globalnym. W ciągu ostatnich lat bardzo uważnie ośrodki studiów strategicznych wielu krajów analizowały przyczyny i przebieg działań w Wietnamie, Algierii, na Bliskim Wschodzie, zmagania z organizacjami terrorystycznymi, przestępczością zorganizowaną, nielegalnym handlem.

W związku z nową sytuacją w dziedzinie zagrożeń międzynarodowego pokoju także w ramach NATO dostrzeżono konieczność przeprowadzenia szerszych analiz tego nowego zjawiska. Dlatego powołano do życia różne struktury (komitety, zespoły i sekcje) oraz zaproszono ekspertów do realizacji szeregu przedsięwzięć programowych i badawczych, których efektem stały się aktualne analizy, opracowania, a nawet dokumenty normatywne, zatwierdzane następnie przez zwierzchnie organy Sojuszu[2].

W założeniach doktrynalnych Sojuszu przyjmuje się, że państwa NATO, zgodnie z obowiązującą strategią, muszą być przygotowane do prowadzenia wielu, często równoległych operacji wojskowych o zróżnicowanym stopniu intensywności, w różnych miejscach świata. Z tego powodu powstały między innymi siły zadaniowe (CJTF) oraz poszczególne dowództwa. Ponadto wojska NATO w myśl stosownych zapisów powinny być

---

[1] M. G. Manwaring, *Studies in asymmetry*, US Army War Collage, Strategic Studies Institute, 2001.

[2] Najważniejsze z nich to plan działania dla państw SEEGROUP (South-East Europe Security Cooperation Steermg Group) oraz dokumenty Komitetu Politycznego i Komitetu Wojskowego NATO, zob. P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*, Warszawa 2003, s. 21.

zdolne do realizowania zadań we wszystkich warunkach, także wobec stosowania przez przeciwnika asymetrycznych sposobów walki, m.in. użycia broni masowego rażenia[3] oraz terroryzmu[4]. Biorąc pod uwagę powyższe uwarunkowania, zakłada się, że w warunkach zdecydowanej przewagi wojskowej państw NATO, potencjalni przeciwnicy (strony konfliktu) w celu uzyskania pożądanych rezultatów polityczno-militarnych będą stosowali niekonwencjonalne, nieregularne, asymetryczne sposoby walki, obejmujące nietypową strategię (np.: długotrwałe walki partyzanckie) i taktykę działania oraz czego nie należy wykluczać – nowoczesną technikę i informatykę.

Rozwojowi złożonych procesów cywilizacyjnych towarzyszy zazwyczaj dynamiczny postęp w zakresie zdolności tworzenia i wytwarzania[5] . W opinii ekspertów, powoduje to określone zmiany odniesień pomiędzy podmiotami wielowymiarowego układu (państwa, organizacje, korporacje przemysłowe), opisującego całokształt zjawisk społecznych i cywilizacyjnych oraz ich wzajemnych związków i relacji. Czynniki określające występowanie określonych relacji pomiędzy podmiotami, a także wielkość ich udziału w procesie powstawania asymetrii są zatem zmienne[6]. Zgromadzone fakty wskazują, że w odniesieniu do wielu konfliktów można określić czynniki demograficzne, gospodarcze czy militarne wpływające na genezę i przebieg działań. Pozostaje jednak zawsze element niepewności spowodowany intensywnością wpływu poszczególnych czynników na przebieg obserwowanego zjawiska i sposobem pomiaru mocy ich oddziaływania.

Dokonując analizy konfliktów zbrojnych w aspekcie historycznym można wnioskować, że pomimo przejawów i krótkotrwałego wpływu uwarunkowań jakościowych[7], przeważał zdecydowanie czynnik ilościowy[8]. Ekspansja i podboje strony dominującej były najczęściej konsekwencją zgromadzenia większych potencjałów militarnych i występowania asymetrii powodowanej narastaniem zróżnicowania ilościowego, w mniejszym stopniu - jakościowego. Szczególnie wiek XX, a zwłaszcza jego druga połowa, stał się okresem przewartościowań jakościowych na niespotykaną dotychczas skalę[9], zmieniających stosunki sił przeciwstawnych stron, a co się z tym wiąże generowaniu nowych zagrożeń i działań

---

[3] Zagrożenie w początkowym okresie konfliktu w Zatoce Perskiej.
[4] Np: NATO Response Force.
[5] A., H., Toffler, *Wojna i antywojna*. Warszawa 1997 oraz A. Toffler, *Trzecia fala*, Warszawa 1986.
[6] Zob. szerzej S. Humington, *Zderzenia cywilizacji*, Warszawa 1998.
[7] Wprowadzenie do uzbrojenia: karabinów maszynowych, czołgów, samolotów, broni atomowej.
[8] Dla przykładu – uderzenie wojsk niemieckich na Polskę w 1939 roku, Bitwa o Falklandy – Malwiny, Operacja Pustynna Burza 1991.
[9] Automatyzacja procesów kierowania środkami rażenia, zwiększenie zasięgu oddziaływania, precyzja uderzenia.

asymetrycznych. W ostatniej dekadzie XX wieku nastąpiły ogromne zmiany cywilizacyjne[10], technologiczne[11], polityczne[12], społeczne i kulturowe[13]. Postęp w technice, procesach wytwarzania, przetwarzania i przekazywania informacji dokonał się w bardzo krótkim czasie, w opinii specjalistów niemal w okresie jednego pokolenia, przez co umożliwił budowanie zupełnie nowej jakości warunków funkcjonowania krajów i organizacji.

Nie bez znaczenia w kontekście zagrożeń asymetrycznych jest fakt, iż z postępu technicznego i technologicznego oraz wymiany informacji o zasięgu światowym zaczęły czerpać korzyści kraje, które dotychczas nie dysponowały dostępem do najnowszych osiągnięć w dziedzinie zaawansowanej techniki, w tym szczególnie techniki bojowej[14]. Powoduje to określone następstwa i zmiany poziomu bezpieczeństwa[15], a ponadto wymaga właściwego ich rozpoznawania oraz rozumienia powstających na tym tle zagrożeń, tak by można było podejmować szybkie decyzje i przeciwdziałać adekwatnie do poziomu powstających zagrożeń. Mając na uwadze obszar zagrożeń asymetrycznych, należy się także liczyć z możliwością wystąpienia nagłej sytuacji kryzysowej związanej z użyciem i dalszym rozprzestrzenianiem się broni masowego rażenia i środków jej przenoszenia. Trzeba też podkreślić, że coraz liczniejsza jest grupa państw (w tym prowadzących politykę konfrontacyjną – np.: Iran, Korea) bliskich wejścia w jej posiadanie. Jeżeli uwzględnić fakt, że do dysponowania tego rodzaju bronią dążą również skrajne ugrupowania polityczne, religijne, a nawet organizacje przestępcze, to możliwość jej użycia wykracza już poza obszar militarnych ocen rozpoznawczych.

W odniesieniu do kontekstu prowadzonych badań – rozpoznanie w działaniach asymetrycznych – celowym jest jednoznaczne wskazanie na fakt, że zagrożenia militarne przybierają charakter zarówno pozapaństwowy jak i asymetryczny. Obserwacja współczesnych stosunków międzynarodowych wskazuje, że coraz częściej już nie tylko określone państwa zagrażają swoim sąsiadom, lecz procesy i zjawiska, jakie występują w zmieniających się społeczeństwach generują nowe zagrożenia[16]. Dlatego w opiniach

---

[10] Zwiększenie obszarów zurbanizowanych, rozwój przemysłu i informatyki.
[11] Miniaturyzacja urządzeń, automatyzacja procesów produkcyjnych, wprowadzenie do powszechnego użytku osiągnięć w dziedzinie informatyzacji i telekomunikacji.
[12] Powstanie nowych państw, rozpad bloków polityczno-militarnych.
[13] Standaryzacja warunków życia, handlu i wypoczynku, upowszechnienie wzorców zachowań.
[14] Eksport broni i dotychczas zastrzeżonych technologii.
[15] Następstwem braku kontroli eksportu broni był długotrwały konflikt zbrojny na terenach byłej Jugosławii. Pomimo powszechnego embarga na dostawy broni strony konfliktu były zaopatrywane w amunicję i środki walki.
[16] Przykładem jest Francja gdzie dysproporcje w rozwoju społecznym spowodowały rozruchy i zamieszki w wielu miastach. Tego rodzaju działania przez nieliczne grono ekspertów określane zostały jako początek trzeciej wojny światowej.

ekspertów pojawiają się tezy, że biedne społeczeństwa występują przeciwko bogatym, a totalitarne systemy państwowe przeciwko zasadom demokracji[17]. Jest to przejaw coraz widoczniej rysującego się nowego elementu rozwoju społecznego, który w sensie globalnym wyraża się w dysproporcjach międzypaństwowych, międzyregionalnych czy wręcz coraz bardziej powszechnej asymetrii rozwojowej świata.

[17] Większość ekspertów zgadza się, że wydarzenia z 11 września 2001 roku należą do przełomowych w historii i są zaliczane do pierwszej bitwy wojny asymetrycznej.

1. PROBLEMATYKA PRACY I PROCEDURA BADAWCZA

Potrzeba uporządkowanych badań w obszarze rozpoznania w działaniach asymetrycznych wojsk lądowych narastała stopniowo w toku pracy naukowej i dydaktycznej. Pierwsze oznaki braku pełnej wiedzy o tym zjawisku w siłach zbrojnych zidentyfikowano jeszcze w czasie działań wojsk w misjach pokojowych, a następnie operacji stabilizacyjnych sił wielonarodowych. Wówczas to właśnie przeprowadzono cykl badań wstępnych zmierzających do wyjaśnienia problematyki zagrożeń asymetrycznych w czasie konfliktu zbrojnego o niskiej intensywności.

Można przyjąć, z bardzo dużym prawdopodobieństwem, za prawdziwą tezę, że w tym okresie rozpoczęto pierwsze prace w ramach wspomnianej problematyki będącej obecnie przedmiotem tematu badawczego. Jedną z konsekwencji wspomnianej naukowej penetracji był cykl badań poświęconych zagrożeniom w nowych uwarunkowaniach (organizacyjnych i strukturalnych) prowadzony w Akademii Obrony Narodowej[1]. Uzyskany we wspomnianych latach materiał porównawczy pozwolił na wykorzystanie otrzymanych wyników i kontynuację dalszych badań aż do opracowania niniejszej pracy naukowo-badawczej.

Ze sfery rzeczywistości, w miarę integrowania systemu rozpoznania ze standardami Sojuszu, indukowano kolejne problemy wymagające rozwiązania przez teorię naukową. Po ich rozwiązaniu dokonywano systematycznie dwóch czynności - weryfikacji w toku ćwiczeń grupowych ze studentami (np.: zagrożenie w tyłowej strefie działań) i dowódczo-sztabowych w wojskach operacyjnych[2], a następnie w postaci finalnej wdrażano do praktyki dydaktycznej, formułując określone wytyczne do zmian w procesie kształcenia[3].

---

[1] *Ocena warunków środowiska i przeciwnika*, pod red. M. Wrzosek, Warszawa 2003, *Planowanie, organizowanie i prowadzenie działań rozpoznawczych*, pod red. A. Nowak, Warszawa 2003, *Rozpoznawcze przygotowanie pola walki*, pod red. M. Wrzosek, Warszawa 2004,

[2] Zagrożenie stery tyłowej, np.: ćwiczenia: *Granica – 04*, *Capable Warrior -04*, *Orzeł-06*.

[3] Wprowadzenie do programu kształcenia uzupełniających studiów magisterskich tematyki zagrożenia terrorystycznego, bezpieczeństwa wojsk w operacjach pokojowych i stabilizacyjnych.

Pierwsze potrzeby poszerzenia i pogłębienia rozwiązań problemów zawartych obszarze zagrożeń asymetrycznych, zidentyfikowane podczas badań wstępnych posłużyły do opracowania zasadniczych założeń pracy.

Ponadto konstatację, że brakuje dostatecznej wiedzy z zakresu zagrożeń asymetrycznych, potwierdziły napływające z wojsk operacyjnych wnioski opracowywane po ćwiczeniach oraz potrzeby zgłaszane przez studentów w czasie ćwiczeń prowadzonych w AON. Potrzeba wyodrębnienia zagrożeń asymetrycznych z całej problematyki informacyjnego przygotowania pola walki wypływała także z konieczności rozdzielenia treści informacyjnych będących efektem pracy poszczególnych oficerów rozpoznania w różnych strefach odpowiedzialności (działania głębokie, bezpośrednie, tyłowe). Częściowych rozwiązań w tym obszarze niewiedzy dostarczyła także ogólna identyfikacja problemów, jakie występują w czasie bezpośredniego działania wojsk w rejonach konfliktów.

W kolejnym etapie pracy prowadzonej w ramach zadania badawczego dotyczącego rozpoznania w działaniach asymetrycznych wiedzę w tym obszarze, poszerzyła analiza literatury oraz wnioski wynikające z ćwiczeń a także konfliktów zbrojnych, szczególnie zaś wojen w Zatoce Perskiej[4] i na terenach byłej Jugosławii[5]. Literatura dostarczyła wielu przykładów różnych interpretacji zakresu badanego zjawiska w działaniach taktycznych i operacyjnych oraz wskazała szereg uwarunkowań organizacyjnych. Bazując na wspomnianych przykładach można wnioskować, że działania asymetryczne stanowią wysiłek podejmowany przez przeciwnika w celu uderzenia w najsłabsze punkty systemu wojsk własnych.

Cennym i ważnym źródłem wiedzy był udział autorów pracy w konferencjach naukowych i seminariach. Warto wymienić między innymi:

1) konferencję na temat: „Bezpieczne niebo, zorganizowaną 10 września 2002 roku w Akademii Obrony Narodowej, pod patronatem Biura Bezpieczeństwa Narodowego oraz Ministerstwa Obrony Narodowej;

2) seminarium na temat: „Prognozowanie zagrożenia w nowych uwarunkowaniach międzynarodowych", zorganizowaną w dniu 5 kwietnia 2006 przez Zakład Rozpoznania Wojskowego i Walki Elektronicznej, Instytutu Zarządzania i Dowodzenia na Wydziale Wojsk Lądowych AON z udziałem oficerów dowództw rodzajów sił zbrojnych i Sztabu Generalnego Wojska Polskiego;

---

[4] Konflikt zbrojny o wysokiej intensywności.
[5] Konflikt zbrojny o niskiej intensywności i operacje pokojowe ONZ.

3) seminarium na temat: „Siły zadaniowe w działaniach taktycznych", zorganizowaną 16 listopada 2006 przez Katedrę Sztuki Operacyjnej i Taktyki, Wydziału Wojsk Lądowych AON.

Pozyskane tą drogą zasoby informacyjne stanowiły właściwą bazę do porządkowania przedmiotowego zjawiska. W rezultacie powstał zbiór twierdzeń, definicji, sądów (opinii) klasyfikujących fakty, który pozwolił na pełną identyfikację poznawczą przedmiotu badań.

Powszechnie uznanym w nauce wyznacznikiem zorganizowanych badań naukowych jest ich cel. Celem niniejszej pracy jest określenie możliwości i wskazanie potrzeb w zakresie rozpoznawania i identyfikacji zagrożeń asymetrycznych? W związku z tak postawionym problemem konieczne było uzyskanie odpowiedzi na pytania szczegółowe:

1) Jak identyfikować działania asymetryczne?
2) Jakie są możliwości rozpoznawania zagrożeń asymetrycznych w tyłowej strefie działań wojsk własnych?
3) Jaki są potrzeby w zakresie przygotowania systemu rozpoznania do realizacji zadań rozpoznawczych w systemie globalnego bezpieczeństwa?
4) Jak rozpoznawać zagrożenia asymetryczne spowodowane intensywnym rozwojem środków zdobywania, przetwarzania i dystrybucji informacji?

Analiza pojęcia zagrożenia asymetrycznego, jego porządkowanie i rozwijanie drogą formułowania uniwersalnego, względnie spójnego terminu, wymagała specyficznego podejścia metodologicznego. Poszukiwanie takiego podejścia ułatwiła analiza zależności występujących w ogólnym procesie zagrożenia, uwzględniającym aspekty militarne i niemilitarne. Za najważniejsze uznano fakt, że zespół rozpoznania opracowuje prawdopodobny wariant działania, a dowódca podejmuje decyzje w warunkach niepewności przy niepełnych zbiorach informacyjnych. Wobec powyższego określenie funkcji i procesów metodami analizy strukturalnej, dobrane zostało jako sposób postępowania dogodny i adekwatny dla nauk wojskowych. Specyfikacja zagrożeń asymetrycznych okazała się właściwa dla nowo tworzonych i usprawnianych elementów[6] systemu rozpoznania, definiowało niezbędne wymagania informacyjne i funkcjonalne, jednocześnie czyniąc system otwartym na obecne

[6] Np. zespoły analizy, oceny i prognozy zagrożenia tworzone w wielonarodowych związkach taktycznych.

i przyszłe potrzeby (operacje stabilizujące i wspierające[7], działania humanitarne) zarówno dowódców wojsk lądowych, jak i wymagania techniczne systemów dowodzenia wprowadzanych do wojsk lądowych (np.: Szafran).

Nauki wojskowe należą do grupy nauk empirycznych, a zatem postępowanie badawcze w generalnym kształcie jest takie, jakie jest stosowane w naukach indukcyjnych. Tymczasem brak w naukach wojskowych dostępu do fragmentu rzeczywistości, który należy wykorzystać do badań empirycznych. Stosuje się, dość powszechnie „praktykę naukową", weryfikując uzyskane wyniki badań paraempirycznie (ćwiczenia w oparciu o umowne struktury i wyposażenie wojsk). Realizm w badaniach próbowano, zatem osiągnąć, traktując zagrożenia asymetryczne jako fragment rzeczywistości w walce zbrojnej. Szukano i eksponowano w przedmiocie poznania najważniejsze elementy składowe, ich cechy własne oraz relacje między tymi cechami (np.: działania w strefie tyłowej, przemyt broni i narkotyków, rozprzestrzenianie broni masowego rażenia, walka w infosferze).

Poruszając się w obszarze ustalonych faktów, stosowano dwie podstawowe metody rozumowania: wyjaśnienie oraz uzasadnienie badanego zjawiska. W tym etapie badań szeroko stosowano indukcje. Pozyskane na drodze indukcji fakty traktowano jako aksjomaty rzeczywistości. Następnie fakty gromadzone w zbiorze przesłanek, stanowiły wystarczający do sformułowania logicznego wniosku wyjaśniającego fragment zagrożeń asymetrycznych (np.: normy taktyczne dla formacji przeciwnika działającego w strefie tyłowej – siły specjalne, organizacje paramilitrane).

Na podstawie literatury przedmiotu wyróżniono dwie podstawowe odmiany uzasadnienia w nauce[8]: sprawdzanie (weryfikacja) empiryczne oraz dowodzenie. Dowodzenie wiążę z tą częścią wyjaśniania przedmiotowego zjawiska, w której fakty naukowe (aksjomaty rzeczywistości) stanowią rację, do której można odwołać się, twierdząc coś o zagrożeniach asymetrycznych.

Założony i zrealizowany proces badań zjawiska zagrożeń asymetrycznych wymagał doboru, przestudiowania i wykorzystania w działalności badawczej szerokiej, interdyscyplinarnej, często obcojęzycznej literatury przedmiotu badań. Główne sposoby podejścia do realizowanych problemów badawczych poszukiwano w opracowaniach autorów z obszaru nauk wojskowych. Wymagania wynikające z potrzeby zastosowania

---

[7] Zob. *Stability operations and support operations (SOSO)*, US Army Training and Doctrine Command TRADOC, Fort Leavenworth 2003.

[8] Naukom wojskowym przypisuje się głównie weryfikację hipotez na drodze sprawdzania (empiria), w prowadzonych badaniach posługiwano się także prowadzeniem logicznego wywodu - dowodzeniem.

interdyscyplinarnego podejścia w praktyce, skierowały zespół do pozycji klasyków naukoznawstwa[9], teorii czynu skutecznego[10], zarządzania organizacjami[11], nauki i sztuki wojennej[12], jak i najnowszych opracowań we wskazanych obszarach wiedzy naukowej. Dobór i studiowanie kolejnych pozycji literatury tematycznej (rozpoznanie wojskowe, sztuka operacyjna, strategia wojskowa) to w znacznej mierze logiczna konsekwencja wniosków wyciągniętych z lektury wydawnictw dotychczas publikowanych szczególnie nakładem AON jak i na łamach periodyków resortowych. Najistotniejszy wpływ na sprecyzowanie uwarunkowań badanego problemu miały poglądy pracowników naukowo-dydaktycznych AON oraz opinie wąskiego grona ekspertów z zakresu bezpieczeństwa międzynarodowego wyrażane w szeregu publikacjach.

Szczególnie istotne w procesie poszerzania i porządkowania wiedzy o przedmiotowym zjawisku dotyczącej teorii i praktyki działania wojsk, znalazły się także w licznych artykułach naukowych i popularnonaukowych[13]. Artykuły te przybliżają zasadnicze kwestie w kategoriach teoretycznych i empirycznych, zwiastują konieczność zastosowania jednakowego aparatu pojęciowego w badanym zjawisku oraz ukazują wzrost znaczenia zagrożeń asymetrycznych we współczesnych konfliktach.

Obok literatury specjalistycznej wykorzystywano, ze względu na złożoność procesu badawczego i jego interdyscyplinarność szereg innych publikacji dotyczących teorii konfliktów zbrojnych.

Przyjęta w jednej z teorii teza (S. Huntington), u której podstaw tkwi założenie o zaostrzających się konfliktach międzycywilizacyjnych, wydaje się trafna ze względu na potwierdzające ją liczne obserwowane współcześnie i nasilające się konflikty, których podłoże stanowią sprzeczności pojawiające się wzdłuż „linii tektonicznych" dzielących nie tylko narody i państwa, lecz całe cywilizacje[14]. Autor zauważa, że to kultura i tożsamość kulturowa, będąca w szerokim pojęciu tożsamością cywilizacji, będą kształtować wzorce spójności, dezintegracji i konfliktów w przyszłym świecie.

---

[9] S. Kamiński, *Nauka i metoda, Lublin*, Towarzystwo Naukowe Katolickiego Uniwersytetu Lubelskiego 1992.
[10] J. Kurnal (red.), *Teoria organizacji i zarządzania*, Warszawa, PWE 1979.
[11] Stoner J, Wankel Ch., *Kierowanie*, Warszawa, PWE 1996.
[12] Szulc B. (red.), *Przemiany w teorii sztuki wojennej lat dziewięćdziesiątych*, Warszawa, 1997, Wiatr M., *Między strategią a taktyką*, Toruń 1999.
[13] B.Balcerowicz, *Wojny współczesne. Wojny przyszłe*, Myśl Wojskowa nr 5/2003, M. Kozub, *Charakter zagrożeń oraz konfliktów zbrojnych w pierwszych dekadach XXI wieku*, Myśl Wojskowa nr 1/2006.
[14] Zob. S. Huntington, *Zderzenia cywilizacji*, Warszawa 1998.

Ideę nasilających się konfliktów i niestabilności o różnej skali przedstawia również Z. Brzeziński, który prezentuje „teorię pola gry". Autor prezentuje Eurazję jako gigantyczną szachownicę, na której w przyszłości będzie rozgrywała się rywalizacja o światową hegemonię. Wybór tego kontynentu jako miejsca walki głównych graczy geostrategicznych nie jest, jak się ocenia, przypadkowy. Teza ta wynika z faktu, że Eurazja jest kontynentem, na którym znajduje się większość najbardziej ekspansywnych i dynamicznych politycznie państw świata[15]. Południowy wschód kontynentu zajmują rosnące w siłę i wyrastające na mocarstwo Chiny, których dążenia do sprawowania władzy, co najmniej regionalnej, nie podlegają dyskusji. Strefę południową wreszcie zajmuje ogarnięty eksplozją demograficzną, anarchiczny pod względem politycznym, lecz bogaty w surowce energetyczne, region państw arabskich o potencjalnie dużym znaczeniu zarówno dla państw położonych na zachodzie, jak i na wschodzie.

W każdym z wymienionych obszarów występują i w opinii ekspertów z całą odpowiedzialnością można stwierdzić, że w dalszym ciągu będą występować zjawiska i zdarzenia, których zaistnienie lub przebieg mogą w nadchodzącym czasie kształtować sytuację geopolityczną i geostrategiczną zarówno na kontynencie eurazjatyckim, jak i na całym świecie.

Spośród innych teorii geopolitycznych w opinii ekspertów, na uwagę zasługuje spojrzenie A. Tofflera, którego istotę stanowi trójpodział cywilizacyjny, oparty na sposobach pozyskiwania dóbr. Cywilizację pierwszego typu mają stanowić państwa wiążące swoją koncepcję rozwojową z erą informacyjną. Produkowane przez nią dobra to w przeważającej większości informacje, stanowiące w równym stopniu narzędzie pozyskiwania dóbr, jak i zyskiwania przewagi. Cywilizacje drugiego typu charakteryzuje sposób pozyskiwania dóbr oparty na tradycyjnej produkcji przemysłowej. Cywilizacje te, zwane industrialnymi, powinny pozostawać w wyraźnej opozycji do cywilizacji pierwszego typu, głównie ze względu na znacznie ograniczone możliwości kształtowania przewagi w otoczeniu. Sytuacja ta, jak się ocenia, będzie się bezpośrednio wiązała z malejącym zapotrzebowaniem na oferowane produkty, postępującym spadkiem możliwości finansowych, a co za tym idzie - pozyskiwaniem zasobów niezbędnych do utrzymania i stosowania narzędzi kontroli. Trzeci typ cywilizacji będą tworzyć państwa zwane agrarnymi, to jest takie, w których podstawowym źródłem pozyskiwania dóbr materialnych będzie produkcja rolna. Nie

---

[15] Zob. Z. Brzeziński, *Wielka szachownica*, Warszawa 1998.

można jednak założyć, że na terenie tych państw nie będzie dochodziło nie tylko do konfliktów, ale również i wojen[16].

W podsumowaniu wybranych teorii opisujących prognostyczny kształt rodzącego się ładu światowego, zasadne wydaje się przedstawienie następującego uogólnienia - świat w dalszym ciągu będzie areną złożonych i skomplikowanych stosunków politycznych, ekonomicznych, religijnych, kulturowych, społecznych i co za tym idzie – militarnych.

W aspekcie zagrożeń asymetrycznych, uwieńczeniem pionierskiego etapu badań prowadzonych pod kierownictwem J. Pawłowskiego, *Pojęcie, istota oraz tendencje zagrożeń asymetrycznych*[17]. Praca zawierała szerokie wyjaśnienie zagadnień dotyczących zagrożeń asymetrycznych według poglądów amerykańskich, brytyjskich i niemieckich. Prezentowany materiał odzwierciedlał istniejący stan rzeczy, jaki autorzy uzyskali poprzez przetłumaczenie tekstów oryginalnych zawartych w publikacjach zagranicznych.

W Stanach Zjednoczonych pojęcie „asymetria", w kontekście zaangażowania militarnego sił zbrojnych USA, pojawiło się oficjalnie w 1995 roku w publikacji doktrynalnej „Walka połączona sił zbrojnych USA" (*Joint Warfare oft he Armed Forces of ihe United States - Joint Publication 1*). Było definiowane jako starcie między sobą różnych rodzajów sił zbrojnych, na przykład sił powietrznych z siłami lądowymi czy też siłami morskimi. Mieliśmy do czynienia z wąskim pojęciem koncepcji asymetrii. Zjawisko to w szerszym wymiarze zostało opisane w tym samym roku w Narodowej Strategii Wojskowej (*National Military Strategy*). Wskazano na takie zagrożenia asymetryczne, jak: terroryzm, wykorzystanie (lub sama groźba użycia) broni masowego rażenia i walka informacyjna.

W miarę upływu czasu zagrożenia asymetryczne zaczęły skupiać coraz większą uwagę analityków i ekspertów. W 1997 roku w raporcie Czteroletniego Przeglądu Obronnego (*Quadrennial Defence Review - QDR*) stwierdzono, że (...) dominacja Sianów Zjednoczonych w dziedzinie uzbrojenia konwencjonalnego może zachęcić przeciwnika do wykorzystania środków asymetrycznych w celu zaatakowania sił amerykańskich stacjonujących za granicą lub Amerykanów w ich kraju[18].

---

[16] Zob. A.Toffler *Trzecia fala*, Warszawa 1986 oraz A., H., Toffler *Wojna i antywojna*, Warszawa 1997

[17] *Pojęcie, istota oraz tendencje zagrożeń asymetrycznych*, pod kier J. Pawłowskiego, Warszawa 2002.

[18] *Quadrennial Defense Review Report*, Department of Defense, 30 September 2001.

W raporcie przedłożonym w tym samym roku przez Narodowy Panel Obronny (National Defence Panel), w którego skład wchodzili eksperci powołani przez Kongres, stwierdzono: (...) można założyć, że nasi przyszli przeciwnicy wyciągnęli wnioski z wojny w Zatoce Perskiej. Nie jest prawdopodobne, aby stawili nam czoła, wykorzystując formacje pancerne, siły powietrzne czy też zespoły okrętów, to znaczy na płaszczyznach, na których USA posiadają miażdżącą przewagę. Zamiast tego mogą przyjąć nowe sposoby do zaatakowania naszych interesów, sił i obywateli[19]

W raporcie zwrócono szczególną uwagę na możliwość:

- dużych strat, jakie mogą być zadane przez broń masowego rażenia, jednocześnie skutkującymi trudnościami lub opóźnieniem dostępu sił USA do rejonu działań;
- uderzeń na amerykańskie systemy informacyjne;
- wykorzystania min i pocisków rakietowych w rejonach cieśnin oraz podejść do wybrzeża;
- działań terrorystycznych.

Reakcją amerykańskich kręgów polityczno-wojskowych na powyższy dokument było szczegółowe zajęcie się asymetrią oraz jej potencjalnymi skutkami. Problemowi temu poświęcono doroczną konferencję strategiczną, zorganizowaną w 1998 roku w Akademii Wojennej Sił Lądowych USA. Temat konferencji brzmiał: „Zagrożenia symetryczne i asymetryczne Stanów Zjednoczonych. Czy Ameryka może zostać pokonana?". W wymiarze merytorycznym skupiono uwagę na ocenie możliwości i odpowiedzi na pytanie, czy USA mogą zostać zwyciężone uderzeniem środkami asymetrycznymi w najsłabsze ogniwo sił zbrojnych bądź, w większości niechronione, kluczowe ośrodki infrastruktury cywilnej. Z przeprowadzonej dyskusji wynikała następująca konstatacja: USA nie mogą zostać pokonane w wyniku ataku symetrycznego, mogą być natomiast pokonane w wyniku ataku asymetrycznego.

Należy zauważyć, że w trakcie dyskusji zostały podważone treści opracowania „Wspólna wizja 2010" (*Joint Vision 2010*[20]), opublikowanego w 1997 roku przez przewodniczącego Kolegium Połączonych Sztabów i przedstawiającego zadania, strukturę i sposoby działania sił zbrojnych USA w perspektywie roku 2010. Konkluzją dyskusji było również to, że administracja amerykańska nie jest właściwie

[19] *Transforming Defence. National Security in the 21 st Cenury, National Defence Panel*, Washington, December 1997.
[20] *Joint Vision 2010,* Chairman of the Joint Chiefsof Staff, Washington 1997.

przygotowana, wyposażona i zorganizowana do sprostania wszystkim typom zagrożeń. Konieczne jest zatem opracowanie koncepcji, doktryn oraz zasad organizacyjnych dotyczących współpracy wykraczającej poza granice kulturowe, prawne i budżetowe.

Jak wynikało z podsumowania konferencji, jej uczestnicy byli zgodni co to tego, że dotarcie do umysłów nieprzyjaciela jest ważniejsze od dotarcia do jego bitów. Podkreślono także, że dysponowanie nowoczesnymi technologiami może stanowić w sytuacjach walki asymetrycznej poważną słabość. Sposobem odniesienia sukcesu jest zrozumienie istoty zagrożeń, a przez to uzyskanie zdolności zapobiegania im w takim czasie, aby nie doszło do rozwoju konfliktu.

Można przypuszczać, że druzgocąca krytyka, jakiej zostało poddane opracowanie „Wspólna wizja 2010", stanowiła przyczynę opublikowania już w 2000 roku przez przewodniczącego Kolegium Połączonych Sztabów kolejnego dokumentu o podobnym tytule „Wspólna wizja 2020" (*Joint Vision 2020*), z tą jednak różnicą, że konieczność sprostania zagrożeniom asymetrycznym została przedstawiona jako jedno z wiodących wyzwań przyszłości dla sił zbrojnych USA.

We wstępie stwierdzono między innymi, że tylko osoby w pełni zaangażowane oraz innowacyjne organizacje mogą przekształcić siły połączone zgodnie z potrzebami XXI wieku. Wskazano, że siły zbrojne powinny:

- być wiarygodne w okresie pokoju,
- odgrywać kluczową rolę w okresie wojny,
- być niezrównane w każdej formie konfliktu.

Reasumując zatem, autorzy uważają, że siły zbrojne mają być zdolne do osiągnięcia dominacji w pełnym zakresie. Koncepcja operacyjna, która stanowiła podstawę opracowania założeń do„Wspólnej wizji 2020", dotyczyła dominacji, będącej pochodną następujących cech:

- dominujący manewr,
- precyzyjne działania bojowe,
- zogniskowana logistyka,
- ochrona w pełnym zakresie.

Ponadto w opracowaniu został przedstawiony zakres spodziewanych operacji (działań) sił zbrojnych Stanów Zjednoczonych w perspektywie 2020 roku.

Niezbędnej wiedzy merytorycznej w identyfikacji problemu badawczego, dostarczyła analiza publikacji pod tytułem Zagrożenia asymetryczne[21] gdzie wskazano zarówno zasadnicze definicje, jak i syntetyczne konteksty spojrzenia na problematykę przez wybrane państwa sojuszu.

W toku całych badań konieczną wiedzę w obszarze problemowym dostarczyły encyklopedie i słowniki. Ogólną poprawność językową pracy autorzy uzyskali mając ciągły dostęp do słowników języka polskiego, natomiast w aspekcie nauk wojskowych pomocne były wydawnictwa takie jak: *Leksykon wiedzy wojskowej* (1979 r). oraz Słownik *podstawowych terminów wojskowych* (1977 r) a także *Słownik podstawowych terminów rozpoznawczych*[22]. Leksykalny punkt odniesienia do terminologii sojuszniczej był możliwy, między innymi dzięki wykorzystaniu AAP-6PL, *Słownik terminów i definicji NATO.*

W przedstawionym przeglądzie stanu wiedzy zawartej w literaturze przedmiotu badań, z jakiej korzystano zarówno w procesie badawczym, jak i w toku pisarskiego opracowania wyników uzyskanych badań, skupiono uwagę na publikacjach, które w ocenie zespołu autorskiego wywarły największy wpływ na kształt niniejszej pracy.

W toku badań korzystano także z innych źródeł informacji, np. dokumentacja licznych ćwiczeń akademickich i wojsk operacyjnych, opis wyników czynionych obserwacji znalazł swoje odzwierciedlenie w treści pracy[23].

W prowadzonych badaniach wykorzystywano różne techniki badań. Przyjęto, że techniki badań[24] to zbiór sposobów gromadzenia materiału naukowego (danych) opartych na wytycznych prakseologicznych. Są to konkretne czynności i wskazówki posługiwania się określonymi środkami badawczymi. Wiele z nich może znaleźć zastosowanie w różnych metodach. Można, zatem stwierdzić, że techniki badań to rodzaj wytycznych (instrukcji), które określają np. jak prowadzić ankietowanie, wywiad, testowanie itp., a więc są to sposoby zdobywania szczegółowych informacji o przedmiocie badań. W związku z powyższym zastosowano technikę analizy dokumentów, techniki obserwacyjne oraz techniki oparte na wzajemnym komunikowaniu się badacza z respondentami.

---

[21] P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*, AON, Warszawa 2003.

[22] M. Tęgos, M. Górecki, M. Łokociejewski, *Słownik podstawowych terminów rozpoznawczych*, Warszawa ASG WP 1988.

[23] Autorzy brali udział w szeregu ćwiczeniach między innymi.: *Granica 2003*, *Cannon Cloud 2003*, *Capable Warrior 2004*, *Orzeł -06*.

[24] C. Lewicki, *Zbiór zadań ze statystyki dla pedagogów*, Rzeszów 1996, s. 139.

W grupie narzędzi badawczych rozumianych jako różnorodne środki techniczne i dokumenty stosowane w badaniach wykorzystano kwestionariusz ankiety, arkusz obserwacji i notatki z obserwacji.

Zaprezentowane wcześniej treści głównego i szczegółowych problemów badawczych, a także założone cele do osiągnięcia, wskazywały na potrzebę zastosowania wielu, zarówno teoretycznych jak i empirycznych metod badawczych.

Metody empiryczne posłużyły do zgromadzenia danych w postaci materiału faktograficznego. Najszerzej wykorzystywano obserwację – stosując zarówno technikę uczestniczącą jak i nieuczestniczącą oraz standaryzowaną i niestandaryzowaną[25]. Stosowana była w ramach działalności służbowej zespołu autorskiego, umożliwiając dostrzeganie wielu faktów, zdarzeń i zjawisk. Obserwacja (zewnętrzna – nieuczestnicząca i wewnętrzna – uczestnicząca) prowadzona była w trakcie szeregu ćwiczeń organizowanych zarówno w AON jak i w wojskach operacyjnych. Zaobserwowane, istotne dla problematyki badawczej fakty (wyniki obserwacji) zarejestrowano w postaci notatek.

W celu zebrania doświadczeń wielu specjalistów rozpoznania wojskowego, zarówno z jednostek wojskowych, jak i Dowództwa Wojsk Lądowych (Zarząd Rozpoznania) oraz środowiska naukowego wykorzystano metody sondażu diagnostycznego – w badaniach zastosowano technikę wywiadu oraz technikę ankiety. W badaniu opinii na szeroką skalę wykorzystywano ankietowanie, którego celem było uzyskanie empirycznego materiału faktograficznego dotyczącego poglądów respondentów w zakresie przedmiotu badań. W zbieraniu informacji metodą ankietowania, wykorzystano kwestionariusz ankiety (kwestionariusz przedstawiono w załącznikach). Natomiast kwestionariusz wywiadu przygotowano dla grupy oficerów rozpoznania, zajmujących różne stanowiska służbowe w systemie rozpoznania wojsk lądowych.

Wśród metod teoretycznych dominowała analiza, która umożliwiła określenie cech, związków i zależności badanych elementów zagrożeń asymetrycznych, ze szczególnym uwzględnieniem oddziaływania wyników końcowych na rezultat prowadzonych działań. Analizę stosowano zarówno jako proces myślowy oraz jako metodę badawczą. Analiza literatury przedmiotu oraz dokumentów normatywnych umożliwiła pogłębienie wiedzy zespołu autorskiego w obszarze założonej problematyki

---

[25] Podział przyjęto za: L. Sołoma, *Metody i techniki badań socjologicznych, wybrane zagadnienia*, Olsztyn, WSP 1995, s. 52–60.

badawczej, pozwoliła przedstawić i uzasadnić ważność i aktualność sprecyzowanych problemów naukowych. Uzyskany tą metodą materiał wykorzystano jako podbudowę opracowania wniosków końcowych.

Metodą, która posłużyła ustaleniu podobieństw i różnic między badanymi przedmiotami było porównanie. Zastosowanie tej metody pozwoliło na wyodrębnienie cech wspólnych (np.: w obszarze definicji działań asymetrycznych), różnic (np.: pomiędzy techniką walki terrorystów a partyzantów) i cech charakterystycznych w procesach zachodzących w obiekcie badań. Metodę tę wykorzystano również w czasie interpretacji teoretycznej nowych faktów przez odwołanie się do wiedzy o faktach znanych (teorii), czyli przez konfrontację wiedzy nowej (powstałej z empirii – badanie opinii) z wiedzą istniejącą.

Metoda indukcyjna pozwoliła na wyprowadzenie uogólnień z faktów jednostkowych (od szczegółu do ogółu, zwłaszcza w odniesieniu do poszczególnych przykładów działań asymetrycznych w konfliktach zbrojnych, operacjach pokojowych i misjach stabilizacyjnych). Stanowiła podstawę przy formułowaniu i weryfikacji hipotez roboczych, a w konsekwencji umożliwiła opracowanie wniosków końcowych. W badaniach zastosowano indukcję enumeryczną niezupełną, gdzie wnioskowanie przebiega w relacji przesłanka-wniosek. Metoda redukcji natomiast polega na tym, że badacz zna wniosek, a zastanawia się, co było przyczyną danego zjawiska. Wnioskowanie w tej metodzie przebiega w relacji wniosek-przesłanka. Uwzględniono przy tym, że metody indukcji i redukcji nie zapewniają 100-procentowej pewności wnioskowania, dają natomiast wystarczające prawdopodobieństwo.

Abstrahowanie pozwoliło na usunięcie z obszaru badań cech i zależności mało istotnych (np.: jak poszczególne zagrożenia asymetryczne wpływają na ogólny poziom bezpieczeństwa wojsk?) oraz uwzględnienie tych, które były najważniejsze w aspekcie badanego problemu (np.: rodzaje zagrożeń asymetrycznych, sposoby ich rozpoznania i przeciwdziałanie zagrożeniu).

Uogólnienie – wiążące się ściśle ze wskazanymi powyżej metodami – pozwoliło na sformułowanie wniosków wyższego rzędu, wniosków ogólnych, co szczególnie ujawniło się w części pa cy dotyczącej określenia wyników końcowych (rozdział – Efekty poznawcze).

Prezentując wyniki badań zespół autorski uznał, że pracę powinna rozpoczynać wszechstronna, głęboka i kompletna identyfikacja terminu zagrożenia asymetryczne. Stąd też, po wprowadzeniu w genezę przedmiotowego procesu nastąpiła analiza

struktury poszczególnych elementów składowych. Logicznym następstwem w dalszej części pracy jest przedstawienie zagrożeń asymetrycznych w tyłowej strefie walki (rozdział trzeci) oraz w aspekcie rozprzestrzeniania broni masowego rażenia (rozdział czwarty) a także w odniesieniu do wybranych zagadnień walki informacyjnej (rozdział piąty). Dopełnieniem przedstawionych rozwiązań są wnioski ogólne prezentujące wyniki badań.

2. IDENTYFIKACJA ZAGROŻEŃ ASYMETRYCZNYCH

Terminy „asymetria", „asymetryczność", „przeciwsymetria", „działania asymetryczne", „podejście asymetryczne", „opcje asymetryczne" pojawiają się na łamach wydawnictw wojskowych przede wszystkim w kontekście rozważań nad nowymi zagrożeniami. Wyniki analizy literatury przedmiotu pozwalają na stwierdzenie, że istnieją duże rozbieżności interpretacyjne definicji asymetrii w odniesieniu do środowiska bezpieczeństwa.

Wnioskując z treści różnych zdefiniowanych pojęć tego terminu, przez asymetrię rozumie się między innymi:

- odmienną taktykę walki,
- oddziaływanie na wrażliwe punkty w systemie walki strony przeciwnej,
- walkę informacyjną,
- zmagania informacyjne w sferze opinii publicznej[1],
- groźbę lub wykorzystanie broni masowego rażenia.

Reasumując zatem należy wnioskować, że „asymetria i asymetryczność" są pojęciami określającymi różnorodne formy dysproporcji, zróżnicowania i dysharmonii, które w sposób naturalny lub zamierzony występują w otoczeniu przeciwstawianych sobie rzeczywistości. Dotyczą one zarówno ich sfery materialnej, to jest gospodarczej, ekonomicznej, naukowej, technicznej, informacyjnej i militarnej, jak i sfery duchowej - obejmującej aspekty kulturowe, religijne, etyczne i inne. Wzajemna symetria czynników opisujących wielowymiarowy układ porównywanych z sobą zależności minimalizuje, w określonym przedziale możliwości generowania zagrożeń oraz stabilizuje względnie trwałą równowagę ich zmian. Znamiennym przykładem jest w tym przypadku równowaga sił jądrowych pomiędzy NATO a Układem Warszawskim gwarantująca stabilizację na świecie[2].

W tym kontekście oznacza to, że „asymetryczność" jest antonimem hipotetycznego stanu „symetrycznej" równowagi, odnoszącego się do całokształtu zjawisk społecznych i cywilizacyjnych oraz ich wzajemnych związków, relacji i oddziaływań. Symetria wydaje się więc determinantą trwałości i stabilności zmian zachodzących w całym systemie procesów ewolucyjnych.

---

[1] Jako zespół przedsięwzięć realizowanych w ramach działań informacyjnych.
[2] Por. J. Pawłowski, P. Gawliczek, *Zagrożenia asymetryczne*, Warszawa 2003.

Czynniki warunkujące powstawanie asymetryczności pomiędzy zantagonizowanymi stronami stają się, po przekroczeniu określonego poziomu ryzyka, stymulatorami realnych zagrożeń, które w dalszym etapie ich narastania prowadzą do konfliktów i konfrontacji. Polem konfrontacji staje się nieuchronnie obszar występowania czynnika asymetryczności, na którego wykorzystanie decyduje się zwykle strona agresywna, zdesperowana bądź nieobliczalna. W sferze materialnej może się to przejawiać w formie:

-walki zbrojnej - w której zamiarem strony dominującej jest dążenie do inwazji terytorialnej, okupacji i całkowitego podporządkowania sobie przeciwnika[3];

-wojny gospodarczej - niszczącej i bezwzględnie uzależniającej gospodarkę słabszego od dominującej i ekspansywnej gospodarki silniejszego[4];

-wojny ekonomicznej - niszczącej bazę ekonomiczną słabszego, bądź jako element wojny gospodarczej, podporządkowującej ją bazie ekonomicznej silniejszego[5];

- walki informacyjnej - obejmującej wszelkie działania informacyjne[6] w odniesieniu do przeciwnika, prowadzone z zamiarem promowania określonego celu politycznego, gospodarczego lub wojskowego, przy równoczesnym zapewnieniu odpowiedniej ochrony własnym systemom informacyjnym;

- konfrontacji naukowej - obejmującej działania zmierzające do zniszczenia samodzielności naukowej przeciwnika, do degradacji jego bazy naukowej, zwłaszcza ośrodków akademickich i placówek naukowo-badawczych (zarówno wojskowych, jak i cywilnych)[7];

- konfrontacji technicznej - zmierzającej do uzyskania nad przeciwnikiem bezwzględnej (asymetrycznej) przewagi technicznej i technologicznej, która po przez dokonania rewolucjonizujące zdolność bojową sił zbrojnych jednej ze stron odbiera drugiej możliwość skutecznego przeciwstawienia się, czy nawet zabezpieczenia przed skutkami oddziaływania stosowanych środków rażenia.

Z kolei w sferze duchowej może się to przejawiać w formie:

-wojny kulturowej - zmierzającej do narzucenia przeciwnikowi własnych wzorców kulturowych i zwyczajów, zdecydowanie wypierających dotychczasowe oraz

---

[3] Asymetria potencjału bojowego stron konfliktu.

[4] Uzależnienie Afganistanu od dostaw z byłego ZSRR, a w sytuacji próby pozyskania innych rynków interwencja zbrojna.

[5] Ekspansja gospodarki chińskiej na światowe rynki.

[6] Także jako element przedsięwzięć prowadzonych w ramach działań psychologicznych.

[7] Między innymi: przejmowanie pracowników naukowych, zakup technologii, stypendia i staże naukowe.

zacierających tożsamość narodową i więzi społeczne[8] wśród ludności strony przeciwnej;

-wojny religijnej - polegającej na narzucaniu społeczeństwu strony przeciwnej dogmatów religijnych głoszonych przez stronę ekspansywną, w tym norm, zwyczajów i obrzędów, która jest prowadzona z zastosowaniem wszelkich dostępnych środków, przy jednoczesnym, bezwzględnym zwalczaniu innych form i przejawów kultu religijnego[9];

-konfrontacji etycznej - zmierzającej do narzucenia grupom społecznym i środowiskowym przeciwnika, a docelowo całości jego społeczeństwa, obcych mu zasad i wzorców, degradujących obowiązujące wartości moralne, wprowadzających zamęt, niestabilność nastrojów i nieprzewidywalność zachowań; konfrontacji tej towarzyszy zwykle rozwój patologii społecznych w postaci upowszechniania narkomanii, alkoholizmu, pornografii, przemocy oraz innych tego typu zjawisk[10].

Względna asymetryczność zantagonizowanych stron, zarówno w sferze materialnej, jak i duchowej, oraz wynikające z niej zagrożenia są z zasady warunkowane łącznym wpływem czynników ilościowych i jakościowych, tworzących wypadkową udziału i jednych, i drugich. W opinii grona ekspertów Akademii Obrony Narodowej klasyczne już uwarunkowania ilościowe powodują, że bazą dla asymetrycznej przewagi jednej ze stron jest jej dominująca przewaga ilościowa[11]. Może to mieć odniesienie do liczebności wojsk, ilości posiadanych środków rażenia (broni), wielkości wytwarzanych dóbr czy też innych czynników wpływających bezpośrednio na przebieg konfrontacji i decydujących o jej powodzeniu.

Uwarunkowania jakościowe charakteryzują się natomiast znacznie większym udziałem czynników wpływających na postęp i rozwój cywilizacyjny[12]. Ich obecność powoduje, że nawet przy zbliżonych i porównywalnych potencjałach ilościowych występuje asymetria jakościowa dająca przewagę jednej ze stron. Oznacza to najczęściej większą

---

[8] Zarówno etniczne, grupowe (klanowe), rodzinne, jak i jednostkowe.
[9] Fundamentalizm islamski, szkoły koraniczne.
[10] Kraje ameryki południowej.
[11] Zob. J. Pawłowski (red.) *Pojęcie, istota oraz tendencje zagrożeń asymetrycznych*, Warszawa 2002 oraz C. Rutkowski (red.) *Zarządzanie bezpieczeństwem jako problem nauki i dydaktyki szkoły wyższej*, Warszawa 2003, a także M. Kozub, *Charakter zagrożeń oraz konfliktów zbrojnych w pierwszych dekadach XXI wieku*, Myśl Wojskowa nr 1/2006.
[12] Określanych także w literaturze przedmiotu mianem „skoku cywilizacyjnego".

skuteczność i efektywność wykorzystania będących w jej posiadaniu środków, decydujących o szybkim uzyskaniu przewagi na polu konfrontacji[13].

W kontekście rozważań o asymetryczności ważną rolę zaczęła odgrywać szeroko pojęta problematyka proliferacji, odnosząca się zwłaszcza do broni masowego rażenia i problemów związanych z upowszechnianiem (udostępnianiem) najnowszej techniki bojowej oraz sposobów i metod jej wytwarzania. Problematyka proliferacji broni masowego rażenia ma odniesienie zarówno do pojedynczych państw, jak i ich grup, powiązanych na przykład porozumieniami politycznymi, gospodarczymi i militarnymi, a ostatnio również do tzw. organizacji pozapaństwowych (*non-state actors*).

Ostatnie dekady minionego wieku umożliwiły wykreowanie nowych form i sposobów działań proliferacyjnych, określanych specyficznymi terminami: „technologie nieuchwytne" (*intangible technology*) oraz „nieuchwytny transfer" (*intangible transfer*)[14]. Pierwszy z nich odnosi się do technik i technologii z grupy tzw. środków podwójnego zastosowania (*dual using*), a więc takich, które w całości lub w formie komponentów mogą znaleźć zastosowanie wojskowe bądź też pozamilitarne, np. w chemii, farmacji, bio- i nanotechnologiach czy elektronice. Drugi ma natomiast związek z coraz łatwiejszym i powszechniejszym dostępem do najnowszych systemów komunikacyjnych i wymiany informacji (np. Internetu, sieci lokalnych - LAN i rozległych - WAN) oraz środków umożliwiających skryte porozumiewanie się, także z użyciem najnowocześniejszych systemów kryptografii. Pozwala to na niekontrolowany przekaz informacji, w tym również dokumentów objętych reżimami międzynarodowej kontroli (np.: patenty, technologie).

Z powyższego wynika, że w działaniach asymetrycznych szczególne znaczenie ma walka informacyjna, rozumiana jako zdobywanie i ochrona informacji. Przyjmuje się, że wkrótce walka informacyjna może być podstawową składową działań asymetrycznych, przenikającą wszystkie pozostałe czynniki dotyczące tego typu działań. Ponadto należy wskazać na fakt, że w związku z gwałtownym rozwojem technologii informacyjnych następuje dynamiczny rozwój nowej, samoistnej formy wielowymiarowego odwzorowania obszaru walki - cybernetycznej przestrzeni działań militarnych.

Obecnie daje się zauważyć wiele różnych sposobów podejścia do kwestii definiowania zagrożeń asymetrycznych. Podstawowe różnice wyrażane przez głównych animatorów Sojuszu Północnoatlantyckiego (Stany Zjednoczone, Wielką Brytanię, Niemcy

---

[13] Często przytaczanym przykładem jest niemiecki Blilzkrieg z okresu II wojny światowej oraz użycie broni jądrowej w 1945 r., a obecnie możliwość zastosowania broni precyzyjnego rażenia lub opartych na wykorzystaniu nowych technologii (*no lenthal weapons*).

[14] Zob. J. Pawłowski, P. Gawliczek, *Zagrożenia asymetryczne*, Warszawa 2003, s. 14.

i Francję) dotyczą kwestii oceniania udziału nowych technologii i sposobów walki w osiąganiu celów strategicznych oraz znaczenia występowania w nich czynnika psychologicznego. Są one istotne zwłaszcza dla rozważań o tym, jak *„asymetryczni aktorzy"* zamierzają osiągać swoje cele, które (czy to zrealizowane, czy nie) są przez jednych uznawane za przedsięwzięcia o charakterze strategicznym, a przez innych (jak Stany Zjednoczone) za taktyczne lub co najwyżej operacyjne. Nie zmienia to jednak faktu, iż zagrożenia asymetryczne istniały i wciąż istnieją na wszystkich możliwych poziomach konfrontacji, w odniesieniu do wszystkich sfer życia i działalności, szczebli dowodzenia i rodzajów sił zbrojnych, a związani z nimi „aktorzy" (*state* – państwa oraz *non-state actors* – organizacje niepaństwowe) będą je wykorzystywali zarówno do działań dyplomatycznych, jak i do bezpośrednich zmagań w tym także walki. Na podstawie szeregu faktów można stwierdzić, że przez asymetrię należy rozumieć umiejętność wykorzystania wszelkiego rodzaju różnic w szeroko pojmowanych potencjałach stron - od strony materialnej po psychologiczną - zarówno przed, jak i w toku prowadzenia działań, w celu osiągnięcia przewagi nad przeciwnikiem.

W literaturze przedmiotu spotykane są także definicje bardziej precyzyjne. Eksponuje się w nich, że przez asymetrię w sferze bezpieczeństwa i strategii należy rozumieć myślenie i działanie odmienne od przeciwnika, w celu maksymalizowania własnej przewagi, wykorzystania jego słabości, a także zdobycia inicjatywy lub uzyskania większej swobody operacyjnej. Poziom rozważań, ocen i działań dotyczy każdej sfery, w tym także zmagań w sferze polityczno-militarnej[15].

Reasumując zatem powyższe treści można wnioskować, że na obecnym etapie wiedzy z zakresu sztuki wojennej i bezpieczeństwa państwa nie opracowano jednolitej i uznanej przez wszystkich definicji zagrożeń asymetrycznych, a większość terminów została sformułowana przez teoretyków wojskowych z samodzielnych (narodowych) ośrodków badawczych. Ponadto na podstawie wniosków z analizy dokumentów normatywnych można stwierdzić, że trwają również uzgodnienia oraz próby wypracowania jednoznacznej definicji zagrożeń asymetrycznych w ramach Sojuszu Północnoatlantyckiego.

Z tego powodu na obecnym etapie uzgodnień i prób wypracowania definicji w NATO odnośnie zagrożeń asymetrycznych przyjmuje się, że powstają one w wyniku obniżenia siły przeciwnika poprzez wykorzystanie jego słabych stron i przy użyciu metod

[15] Por. J. Pawłowski, P. Gawliczek, *Zagrożenia asymetryczne*, Warszawa 2003, s. 18.

różniących się w sposób istotny od standardowych procedur działania oraz zastosowanych środków.

Współcześnie można zaobserwować, że asymetria, a zwłaszcza zagrożenia asymetryczne bardzo często polegają na zastosowaniu środków pozamilitarnych do zdobycia przewagi militarnej. Tak więc połączenie zagrożeń w sferze środków militarnych i pozamilitarnych powoduje, że asymetria staje się integralną częścią zagrożeń bezpieczeństwa i rzutuje na ich nieprzewidywalność. Takie podejście do zagrożeń asymetrycznych wskazuje, że stają się one coraz bardziej powszechne, a niekiedy są kluczowym czynnikiem sukcesu.

Z powyższych rozważań wynika, że zagrożenia asymetryczne dotyczą zarówno sfery militarnej, jak i pozamilitarnej. Obejmują myślenie, organizowanie i działanie odmienne od przeciwnika, w tym wykorzystywanie wszelkiego rodzaju różnic w szeroko pojmowanych potencjałach stron. Dlatego wydaje się, że celem działania asymetrycznego jest maksymalizowanie własnej przewagi, wykorzystywanie słabości przeciwnika dla uzyskania dominacji nad nim oraz zapewnienia wojskom własnym większej swobody operacyjnej.

2.1. Współczesne zagrożenia

Zmiany w charakterze zagrożeń bezpieczeństwa państw, organizacji i sojuszy międzynarodowych zapoczątkowane wraz z zakończeniem zimnej wojny wyraźnie uwidoczniły się wraz z atakami terrorystycznymi przeciwko USA w 2001 roku. Znalazło to swoje odzwierciedlenie w przyjmowanych oficjalnie i stanowiących fundament długofalowych planów rozwoju sił zbrojnych założeniach strategicznych prognozujących środowisko bezpieczeństwa w perspektywie najbliższych 15-20 lat.

W podstawowych założeniach „*Strategii bezpieczeństwa RP*" przyjmuje się, że sytuacja międzynarodowa stała się mniej stabilna i przewidywalna. Ocenia się, że lokalne napięcia i konflikty na tle ekonomicznym, politycznym, kulturowym, religijnym, a także ideologicznym mogą stanowić źródło wielu zagrożeń, w tym przede wszystkim terroryzmu międzynarodowego i sprzyjać zorganizowanej przestępczości[16]. W polskiej strategii bezpieczeństwa podkreśla się, że konflikty i kryzysy regionalne związane ze zjawiskiem „państw w stanie rozkładu", nędzą, fiaskiem reform ustrojowych i ekonomicznych, migracjami i klęskami żywiołowymi mogą oddziaływać poza granice swego występowania,

[16] Zob. *Strategia bezpieczeństwa narodowego RP*, www.bbn.gov.pl/dokument/strategiabezpieczeństwa.html

stwarzając różnorodne zagrożenia, nawet dla regionów odległych geograficznie, w tym także dla regionu środkowoeuropejskiego. Wzrasta też zagrożenie proliferacją broni masowego rażenia (BMR) i środków jej przenoszenia oraz możliwością jej użycia nie tylko przez państwa posiadające taką broń, ale również organizacje niepaństwowe, zwłaszcza międzynarodowe grupy terrorystyczne. Polskie oceny zagrożeń bezpieczeństwa podkreślają radykalnie zmniejszone ryzyko wojny konwencjonalnej na dużą skalę w Europie przy równoczesnej dywersyfikacji i globalizacji zagrożeń. Głównym zagrożeniem jest zorganizowany terroryzm międzynarodowy, stanowiący obecnie największe zagrożenie dla bezpieczeństwa globalnego. Terroryzm zmienił swój charakter, a ugrupowania terrorystyczne przyjęły nowe, dotychczas niespotykane metody działania i formy organizacyjne. Dążąc do osiągnięcia swoich celów, grupy takie rozwijają koncepcję ataków na wielką skalę, które skierowane są przeciwko instytucjom międzynarodowym, państwom i ludności cywilnej. Jasno określonym celem działania dla wielu istniejących ugrupowań terrorystycznych jest uzyskanie dostępu do broni masowego rażenia, która może być użyta lub stanowić instrument politycznego szantażu. Z ocen zawartych w „Strategii bezpieczeństwa narodowego RP" wynika, że w odleglejszej perspektywie czasowej realnym zagrożeniem dla interesów Polski mogą stać się państwa prowadzące własne, sprzeczne z przyjętymi porozumieniami międzynarodowymi, programy produkcji BMR i środków jej przenoszenia, zwłaszcza rakiet balistycznych. Ten rodzaj zagrożenia ze względu na wrogość lub nieprzewidywalność polityki władz krajów rozwijających BMR oraz brak możliwości egzekwowania międzynarodowego reżimu kontroli arsenałów tej broni, może wymusić konieczność podejmowania antyproliferacyjnych działań wojskowych w ramach koalicji międzynarodowych[17]. Rozwój sytuacji w państwach powstałych po rozpadzie Jugosławii, przede wszystkim w Serbii, ze względu na sytuację w Kosowie, wciąż wskazuje na możliwość powrotu do otwartych konfliktów na Bałkanach. Takie konflikty mogą zwiększać zagrożenie związane z napływem dużej liczby uchodźców, traktujących Polskę jako kraj tranzytowy lub docelowy. Niestabilność regionu i słabość struktur państwowych na Bałkanach sprzyja rozwojowi przestępczości zorganizowanej, która współpracuje z formacjami paramilitarnymi i partyzanckimi. Zagrożenia bezpieczeństwa mogą również tworzyć wyzwania związane głównie z masową migracją, zorganizowaną przestępczością, radykalizacją ruchów antyglobalistycznych, handlem narkotykami, rosnącą dysproporcją

[17] Tamże.

między poziomem rozwoju państw bogatych i ubogich oraz problemem upadających reżimów autorytarnych.

Nowe podejście do zagrożeń bezpieczeństwa zawierają dokumenty Sojuszu Północnoatlantyckiego. NATO ocenia zagrożenia swojego bezpieczeństwa w bardziej zachowawczy sposób niż czyni to Polska. W koncepcji strategicznej przyjmuje się, że w obecnej chwili agresja na pełną skalę środkami konwencjonalnymi przeciwko Sojuszowi jest wysoce nieprawdopodobna, jedynie w dalszej perspektywie możliwość zaistnienia takiej groźby wciąż istnieje. Jako zagrożenie postrzegana jest niestabilność wewnątrz i wokół obszaru euroatlantyckiego, możliwość wystąpienia, gwałtownie rozwijających się, regionalnych kryzysów na peryferiach terytorium sojuszu. Zagrożenie mogą generować też państwa borykające się z dużymi problemami o charakterze ekonomicznym, społecznym i politycznym. Ocenia się, że rywalizacja na tle religijnym lub etnicznym, konflikty terytorialne, nieodpowiednie lub zaniechane reformy, naruszanie praw człowieka oraz rozpad państwa prowadzić mogą do kryzysów zagrażających stabilizacji obszaru euroatlantyckiego, a nawet do zbrojnych konfliktów. Takie konflikty, poprzez rozszerzenie się na kraje sąsiadujące z Sojuszem lub nawet państwa członkowskie, mogą zagrozić jego bezpieczeństwu lub w inny sposób zagrozić bezpieczeństwu innych państw[18].

Dużą wagę w ocenie zagrożeń bezpieczeństwa NATO przewiązuje się do zagrożeń bronią masowego rażenia. Proliferacja broni masowego rażenia może wystąpić pomimo wysiłków skierowanych na jej zapobieganie, co może spowodować bezpośrednie zagrożenie wojskowe dla terytorium, ludności i sił zbrojnych sojuszu. Zagrożenie uważane jest za realne, gdyż niektóre państwa, również te sąsiadujące z terytorium sojuszu, sprzedają bądź kupują lub próbują zakupić broń masowego rażenia i jej środki przenoszenia. Istotnym prolemem jest to, że materiały oraz technologia, które mogą być zastosowane do budowy takiej broni i środków jej przenoszenia stają się coraz bardziej dostępne, podczas gdy wykrywanie i zapobieganie nielegalnemu obrotowi tymi materiałami i technologią produkcji wciąż pozostają skomplikowane[19]. Potencjalne zainteresowanie produkcją i użytkowaniem tych broni wykazują także organizacje terrorystyczne. Już w 1999 r. koncepcja strategiczna sojuszu przyjmowała, że obok wcześniej wymienionych zagrożeń interesy Sojuszu w dziedzinie bezpieczeństwa mogą być zagrożone przez inne wyzwania o bardziej powszechnym charakterze, wliczając w to akty terroryzmu, sabotaż, przestępczość

[18] Zob. *Koncepcja Strategiczna Sojuszu Północnoatlantyckiego* 1999, pkt 20-21, www.bbn.gov.pl/pl/nato/szczyt/nsc.html
[19] Tamże.

zorganizowaną oraz zniszczenie bądź odcięcie od dopływu ważnych surowców. Niekontrolowany przepływ dużych mas ludzkich, szczególnie będący skutkiem zbrojnych konfliktów, również był uważony za zagrożenie wpływające na stabilność i bezpieczeństwo na obszarze Sojuszu Północnoatlantyckiego[20].

Ocena przez Sojusz Północnoatlantycki zagrożeń bezpieczeństwa, uległa poważnym przewartościowaniom w związku z atakami terrorystycznymi na USA w 2001 r. W trakcie szczytu praskiego w listopadzie 2001 r. odwołując się do tragicznych wydarzeń z 11 września 2001 r. oraz do decyzji o zastosowaniu art. 5 Traktatu Waszyngtońskiego, NATO przyjęło szeroki pakiet środków, wpisujący się w koncepcję strategiczną sojuszu. W kontekście takiej percepcji przyszłego środowiska bezpieczeństwa terroryzm stał się jednym z głównych, obok broni masowego rażenia, zagrożeniem bezpieczeństwa Sojuszu Północnoatlantyckiego. O ile w koncepcji strategicznej sojuszu analizowane są różnego rodzaju zagrożenia bezpieczeństwa, to analizy i oceny zagrożeń dokonywane przez dowódców strategicznych NATO ukierunkowane są na implikacje wynikające z zagrożeń dla przyszłych operacji wojskowych sił sojuszu. Stąd też odmienną w pewnym stopniu od ocen zawartych w koncepcji strategicznej sojuszu z 1999 r. analizę zagrożeń bezpieczeństwa NATO zawiera dokument koncepcyjny dowódców strategicznych NATO „*Strategic Vision: The Military Challenge*" z sierpnia 2004 r. prognozujący warunki działań i koncepcje operacyjnego użycia sił wojskowych sojuszu na najbliższe 15 lat. Zgodnie z sformułowanymi w tym dokumencie ocenami środowisko strategiczne, w jakim będzie działał sojusz będzie warunkowane poprzez szereg czynników, które mogą zagrozić interesom NATO powodując napięcia, kryzysy i konflikty. Dowódcy strategiczni zakładają, że trend gwałtownych eskalacji sytuacji kryzysowych z bardzo krótkim czasem ostrzegania będzie się utrzymywał, co najmniej, przez najbliższe 15 lat[21]. Najważniejsze czynniki stanowiące zagrożenie dla bezpieczeństwa NATO mają w przyszłości obejmować: skutki globalizacji, wzrost skuteczności działań asymetrycznych, różnice demograficzne i środowiskowe, państwa w stanie rozpadu, grupy wspierające radykalne ideologie oraz nierozwiązane konflikty.

W wizji strategicznej zagrożenia związane z globalizacją rozpatrywane są w aspekcie możliwości wykorzystania technologii informacyjnych przez grupy terrorystyczne oraz wpływ mediów na percepcję konfliktów. Dowódcy strategiczni przewidują wzrost wyrafinowania i skuteczności działań asymetrycznych spowodowany coraz szerszym dostępem do zaawansowanych technologii. Za szczególnie niebezpieczne uznawana jest

[20] Tamże.
[21] Zob. *Strategic Vision: The Military Challenge*, NATO Strategic Commanders, 2004, s. 2.

możliwość podjęcia zamachów samobójczych przez grupy terrorystyczne gotowe do użycia broni masowego rażenia. W ocenach dokonywanych przez Dowództwo Operacji i Dowództwo Transformacji NATO poważnie traktowane są rosnące różnice demograficzne pomiędzy państwami rozwiniętymi i rozwijającymi się, które mogą stać się powodem masowych migracji i przyczyniać się do wzrostu napięć na tle etnicznym. Ocenia się, że rosnące zapotrzebowanie na energię i wodę również może stać się w przyszłości przyczyną konfliktów. Analogicznie do ocen zawartych w europejskiej strategii bezpieczeństwa zagrożenia związane z państwami w stanie rozpadu utożsamiane są przez dowódców strategicznych NATO ze wzrostem zagrożenia terroryzmem i przestępczością zorganizowaną, które wykorzystują takie państwa jako bezpieczne bazy do działań w skali globalnej. Stąd też znaczenie takich państw, pomimo braku surowców naturalnych czy istotnej pozycji geostrategicznej, może być niewspółmiernie wysokie dla bezpieczeństwa NATO. Warto zauważyć, że jako potencjalne źródło terroru uważane są zdeterminowane do użycia wszelkich dostępnych środków przemocy grupy wspierające radykalne ideologie. Są one uznawane za zagrożenie interesów bezpieczeństwa sojuszu. Ocenia się, że nierozwiązane konflikty w wielu regionach świata mogą tworzyć sprzyjające warunki do wzrostu poparcia dla grup o radykalnych ideologiach. Kompleksowość nierozwiązanych problemów, jak wynika z zapisów wizji strategicznej, wymagać będzie zaangażowania w operacjach wojskowych państw członkowskich NATO współdziałających z państwami regionu, gdzie wystąpiły kryzysy i konflikty.

Zbliżone do sojuszniczych oceny w zakresie zagrożeń bezpieczeństwa państw członkowskich oraz interesów Unii Europejskiej zawiera europejska strategia bezpieczeństwa „Bezpieczna Europa w lepszym świecie" przyjęta 12 grudnia 2003 r.[22] Konkluzja w odniesieniu do kluczowych zagrożeń bezpieczeństwa UE wyklucza groźbę agresji o dużej skali przeciwko jednemu z państw członkowskich. Za najważniejsze zagrożenia Unia Europejska uznaje terroryzm, proliferację broni masowego rażenia, konflikty regionalne, zjawisko państw w stanie rozkładu oraz zorganizowana przestępczość. Terroryzm w ocenie Unii Europejskiej ma wymiar globalny i jest powiązany z radykalnym ekstremizmem religijnym. Ocenia się, że terroryzm stanowi rosnące strategiczne zagrożenie dla całej Europy i może powodować masowe ofiary. Proliferacja broni masowego rażenia postrzegana jest przez Unię Europejską jako potencjalnie największe zagrożenia bezpieczeństwa Europy. W europejskiej strategii bezpieczeństwa zauważa się, że proliferacja broni masowego rażenia

[22] Zob. J. Kaczmarek, *Strategia bezpieczeństwa Unii Europejskiej*, Zeszyty Naukowe AON nr 1 (54)/2004 oraz *A secure Europe in a better World, European Security Strategy*, Brussels 2003, s. 6.

i jej środków przenoszenia została, co prawda, spowolniona dzięki przestrzeganiu porozumień międzynarodowych oraz kontroli eksportu, ale rozpoczyna się nowy wyścig zbrojeń, w dziedzinie BMR, szczególnie na Bliskim Wschodzie. Z niepokojem obserwowany jest postęp w dziedzinie broni biologicznej oraz możliwość przeprowadzenia ataków chemicznych i z użyciem materiałów rozszczepialnych. Najbardziej groźny scenariusz rozwoju wydarzeń przewidywany w europejskiej strategii bezpieczeństwa przewiduje pozyskanie i użycie broni masowego rażenia przez grupy terrorystyczne[23]. Konflikty regionalne są postrzegane przez Unię Europejską przede wszystkim jako zagrożenia interesów europejskich, a nie jej terytorium czy obywateli. Ocenia się, że takie konflikty mogą jednakże prowadzić do rozwoju ekstremizmu oraz terroryzmu, jak również upadku państw, a w konsekwencji tworzyć warunki dla działań przestępczości zorganizowanej. Uważa się, że brak stabilności sytuacji polityczno-militarnej w wymiarze regionalnym może stać się przyczyną dążeń niektórych państw do pozyskania broni masowego rażenia jako gwarancji bezpieczeństwa. Upadek państw, w ocenie Unii Europejskiej, jest ściśle powiązany z wzrostem zagrożenia zorganizowana przestępczością oraz terroryzmem. Może powodować również ład międzynarodowy i przyczyniać się do wzrostu niestabilności sytuacji polityczno-militarnej w wymiarze regionalnym. Zorganizowana przestępczość traktowana jest przez Unię Europejską jako wewnętrzne zagrożenia bezpieczeństwa państw członkowskich Unii, przy czym nie wyklucza się związków zorganizowanych grup przestępczości kryminalnej z grupami terrorystycznymi. W strategii bezpieczeństwa europejskiego przyjmuje się, że rozmieszczenie geostrategiczne zagrożeń bezpieczeństwa Unii Europejskiej ma charakter globalny. Tym niemniej zagrożenia związane z proliferacją broni masowego rażenia umiejscawiane są według ocen zawartych w strategii bezpieczeństwa Unii Europejskiej w Korei Północnej, Azji Południowej oraz na obszarze Bliskiego Wschodu[24]. Terroryzm i zagrożenia przestępczością zorganizowaną uznawane są jako zagrożenie globalne, chociaż zjawiska tego typu w centralnej i południowo-wschodniej Azji uznawane są za bezpośrednie zagrożenia dla krajów europejskich i ich obywateli. Upadek państw i zorganizowana przestępczość wymieniane są w europejskiej strategii bezpieczeństwa jako zagrożenia wymagające wystarczająco wczesnego przeciwdziałania. Państwa Afryki Zachodniej podawane są jako przykład szczególnie jaskrawego występowania obu powyższych zjawisk.

Reasumując zebrane dotychczas fakty można stwierdzić, że analiza ocen zagrożeń bezpieczeństwa dokonanych przez Polskę, NATO i Unię Europejską wskazuje na wysoką

[23] Tamże, s. 7.
[24] Tamże, s. 8.

zbieżność i zgodność międzynarodowej percepcji charakteru i lokalizacji zagrożeń i wyzwań. Za najpoważniejsze zagrożenia bezpieczeństwa uznawane są terroryzm, proliferacja broni masowego rażenia, zorganizowana przestępczość oraz nierozwiązane konflikty lokalne Zasadniczym przewartościowaniem w stosunku do analiz prowadzonych w okresie zimnej wojny jest niemal powszechne założenie, iż w perspektywie najbliższych kilkunastu lat mało prawdopodobny jest wybuch konfliktu globalnego lub regionalnego o dużej intensywności, w który mogłyby być bezpośrednio zaangażowane państwa zachodnie. Nie oznacza to, że zagrożenie takie zupełnie wykluczono. Uznano jednak, że główne zagrożenia będą miały mniejszą skalę, ale pojawiać się będą częściej i będą trudniejsze do przewidywania.

2.2. Asymetryczne rzeciwdziałanie zagrożeniom

Operacje wielonarodowe w opinii specjalistów, będą na ogół miały miejsce w płynnej i dynamicznej sytuacji politycznej, militarnej i kulturowej. Nierozwiązane problemy polityczne, brak jasności i zgody odnośnie docelowej wizji geopolitycznej i militarnej świata, a także trudności w osiągnięciu międzynarodowego porozumienia w tych dziedzinach mogą potęgować dwuznaczność sytuacji związanej z przygotowaniem i prowadzeniem takich operacji. Wpływ sytuacji polityczno-militarnej na kreowanie zagrożeń asymetrycznych może również wynikać z wielu innych czynników:

- rozproszenia wojsk skłóconych stron konfliktu na obszarze operacji;
- trudności w identyfikacji stron konfliktu i konieczność wiarygodnego rozpoznania celów i obiektów ataku;
- braku dyscypliny wśród zwalczających się frakcji, nie uznających władzy centralnej i nie zainteresowanych osiągnięciem porozumienia;
- łamania podstawowych praw i porządku publicznego, co powoduje potrzebę siłowego ale kontrolowanego wymuszania postanowień rezolucji;
- zniszczeń infrastruktury związanej z ochroną i pomocą socjalną, oraz rozpadu administracji i instytucji cywilnych;
- zniszczeń w środowisku naturalnym;
- masowego napływu osób przesiedlonych;
- zagrożenia chorobami zakaźnymi lub epidemiami;
- działalności organizacji międzynarodowych i pozarządowych oraz przedstawicieli mediów;
- działalności terrorystycznej i kryminalnej oraz fanatyzmu religijnego.

Złożoność sytuacji geopolityczno-militarnej, w której mogą wystąpić zagrożenia asymetryczne, wymaga szczegółowego planowania oraz koordynacji działań różnych agencji i instytucji uczestniczących w operacji. W tej sytuacji przeciwdziałanie zagrożeniom asymetrycznym może być realizowane poprzez zastosowanie systemów broni obezwładniającej. Dla urzeczywistnienia powyższej tezy, należy przyjąć, że wojska koalicyjne będą przygotowane do działań prowadzonych równocześnie na wielu płaszczyznach, tzn.: politycznej (narodowe instytucje państw zaangażowanych), dyplomatycznej (akceptacja międzynarodowa), ekonomicznej (organizacje i przedsiębiorstwa w rejonie operacji, szczególnie ich systemy informacyjne) i militarnej (strony konfliktu).

W przekonaniu zespołu autorskiego, stały rozwój środków walki, w tym także systemów broni obezwładniającej w operacjach prowadzonych w środowisku wielonarodowym jest drogą do kształtowania nowego sposobu przeciwdziałania zagrożeniom asymetrycznym. Ponadto w opinii ekspertów wojskowych, zastosowanie systemów broni obezwładniającej kształtuje zaufanie do sił interwencyjnych, sprzyja propagowaniu demokratycznych ideałów, odstrasza potencjalnego agresora i likwiduje źródła niestabilności i zagrożenia jeszcze przed pojawieniem się pełnego spektrum kryzysu militarnego.

Obserwacja przebiegu zdarzeń pozwala na stwierdzenie, że w rejonie misji zagrożenia asymetryczne różnego rodzaju istnieją zawsze mimo wielu pozytywnych zmian w sytuacji międzynarodowej, w tym mimo radykalnego zmniejszenia prawdopodobieństwa konwencjonalnej agresji na dużą skalę przeciwko wojskom interwencyjnym. Na podstawie zebranych opinii można stwierdzić, że zagrożenia asymetryczne wynikają przede wszystkim z niepewności i niestabilności sytuacji zarówno w obszarze operacji, jak i wokół niego, a także z możliwości nagłego pojawienia się kryzysów o wymiarze regionalnym na peryferiach NATO.

Wyniki obserwacji środowiska euroatlantyckiego wskazują, że niektóre państwa w obszarze zainteresowania przeżywają poważne problemy ekonomiczne (np.: Ukraina), społeczne i polityczne (np.: Białoruś). Rywalizacja etniczna i religijna, spory terytorialne, nieskutecznie lub źle wprowadzane reformy, naruszanie praw człowieka, a także rozpad państw może prowadzić do destabilizacji sytuacji lokalnej, a nawet regionalnej. Wymienione źródła napięć mogą być przyczyną kryzysu, który może zagrozić euroatlantyckiej stabilności, a nawet doprowadzić do konfliktu zbrojnego. Tego typu konflikty mogą osłabiać bezpieczeństwo Sojuszu przez podziały w państwach sąsiednich, obejmujące swym zasięgiem również państwa NATO lub też w inny sposób mogą naruszać bezpieczeństwo innych

państw.[25] W kontekście przedstawionych założeń można wnioskować, że perspektywicznym kierunkiem rozwoju przeciwdziałania zagrożeniom asymetrycznym będzie budowa systemów broni obezwładniającej, a w tym urządzeń bezpośredniego oddziaływania zdolnych do spektakularnego osiągania efektów. W ten sposób potencjalny przeciwnik zanim rozpocznie działania zostanie obezwładniony przed rozpoczęciem działań falami elektromagnetycznymi, generatorami dźwięku, środkami psychotropowymi i różnymi substancjami ograniczającymi ruch i manewr wojsk.

Wskazanie kierunków rozwoju sposobów przeciwdziałania zagrożeniom asymetrycznym wymaga specyfikacji źródeł ich powstawania. Według poglądów amerykańskich ekspertów główne źródła niestabilności we współczesnym świecie to:

1. Naruszenie istniejącej równowagi sił na szczeblu państwowym, co doprowadziło do groźnych konfliktów na Bałkanach i Bliskim Wschodzie. Przyczynia się do tego zarówno proces globalizacji, jak i powstawanie potężnych, wielonarodowych korporacji, a także pojawianie się na scenie konfliktów tzw. aktorów pozapaństwowych[26]. Wszelkie zmiany równowagi sił, jak również osłabienie stabilności będą uderzać w żywotne interesy krajów demokratycznych i powodować zagrożenia dla międzynarodowego bezpieczeństwa. W tej sytuacji zastosowanie systemów broni obezwładniającej może zapobiegać naruszeniom porządku publicznego, chronić obiekty użyteczności publicznej i wspierać działania lokalnych sił porządkowych. Rozmieszczenie sił pokojowych w rejonie konfliktu z bronią obezwładniającą według opinii ekspertów, spowoduje obniżenie odporności psychologicznej potencjalnego przeciwnika, który nieświadomy specyfiki działania nowej broni nie będzie potrafił skutecznie się przeciwstawić nieznanym zagrożeniom.
2. Nacjonalizm, zwłaszcza niektóre jego formy mogące powodować konflikty wewnątrz- i międzypaństwowe. Podstawą ruchów nacjonalistycznych było przekonanie, że narody skorzystają więcej, działając samodzielnie a nie zespołowo, eksponując raczej narodowe niż międzynarodowe cele. W toku badań ustalono, że istnieje wiele form nacjonalizmu, takich jak nacjonalizm: etniczny, religijny, plemienny, historyczny i terytorialny. Ruchy te określają swoją tożsamość, bazując na ideologii. W wielu przypadkach są ściśle związane z organizacjami kryminalnymi. W ocenie ekspertów sytuacje tego rodzaju mogą

[25] A. Tyszkiewicz, *Operacje stabilizacyjne*, Warszawa 2005, s. 29.
[26] Zob. J. Flis, *Globalne zagrożenia,* Polska Zbrojna 2004 nr 27, s. 30.

powodować konflikty regionalne. Bezpośrednie oddziaływanie na członków ruchu nacjonalistycznego może być postrzegane jako prześladowanie i ograniczanie praw mniejszości. Natomiast wykorzystanie broni obezwładniającej może spowodować eliminację jedynie wybranych członków organizacji na określony czas lub pozbawić struktury organizacyjne zdolności do działania. Generowanie dźwięków wysokiej częstotliwości w trakcie zebrań i narad kluczowych osób w organizacji ekstremistycznej (terrorystycznej) może spowodować zachwianie ich równowagi psychicznej i niedyspozycyjność fizyczną. Przeprowadzone badania wskazują, że wykorzystanie syntezatorów dźwięku w celu wygenerowania głosu[27] przywódców i w ten sposób przygotowania stonowanych przemówień zapobiegających radykalnym działaniom jest skutecznym środkiem zapobiegającym eskalacji napięcia. Ponadto „spreparowane" przemówienia podważają wiarygodność przywódców organizacji nacjonalistycznych szczególnie, gdy są oni radykalni w swoich poglądach politycznych. Innym skutecznym sposobem zwalczania zagrożeń asymetrycznych może być zastosowanie broni mikrofalowej. Emituje ona ukierunkowaną wiązkę energii, która nie powoduje oparzeń, ale bolesne uczucie pieczenia[28]. W opinii ekspertów urządzenia emitujące mikrofale będą najbardziej przydatne w czasie rozpędzania manifestacji i tłumienia rozruchów społecznych spowodowanych działaniem ekstremistów.

3. Walka kultur, będąca kolejnym źródłem konfliktów, do których dochodzi, gdy państwa i narody odrzucają lub wręcz zwalczają euroatlantyckie wartości polityczne i kulturowe. W wielu przypadkach nowe kraje wykorzystują zachodnioeuropejskie i amerykańskie formy polityczno-ustrojowe jednak, gdy znajdują się pod silnym wpływem grup nacjonalistycznych, etnicznych lub religijnych, gwałtownie próbują odnaleźć lub przywrócić swoją odrębność polityczno-kulturową. Wnioski z analizy sposobów, w jaki rządy i organizacje pozarządowe ograniczały potencjalne skutki waśni religijnych wskazują, że z arsenału środków broni obezwładniającej najbardziej skuteczne było bezpośrednie oddziaływanie psychologiczne na strony konfliktu. Jednak, jak wskazują doświadczenia perswazja i negocjacje wydają się skutecznym narzędziem w początkowej fazie konfliktu. W przypadku eskalacji napięcia

[27] Zob. I. Nowak, *Broń obezwładniająca o działaniu akustycznym*, Przegląd Wojsk Lądowych nr 6/2003.
[28] Jak podają liczne źródła prace nad bronią tego rodzaju prowadzą armia amerykańska i niemiecka.

celowe wydaje się wykorzystanie do rozpędzania zgromadzeń armatek wodnych i pododdziałów wyposażonych w broń na pociski wodne. Karabiny tego rodzaju zgodnie z zamiarami konstruktorów będą już wkrótce dysponowały regulowanym poziomem ciśnienia wylotowego wody. Zatem w przypadku wzrostu agresji tłumu siły porządkowe mogą zwiększyć zasięg rażenia i siłę uderzenia pociskami wodnymi, aż do uszkodzenia ciała włącznie. Nie należy także zapominać o znanych i stosowanych pociskach gumowych i granatach z gazem łzawiącym, których skuteczność została dowiedziona w wielu akcjach bezpośrednich.

4. Czynnik demograficzny, czyli szybki wzrost liczby ludności, zwłaszcza w państwach słabo rozwiniętych. Wskazana sytuacja powoduje wyczerpanie zasobów ekonomicznych małych państw i destabilizuje ich struktury socjalne. Sytuację pogarsza fakt, że do tego typu zjawisk demograficznych dochodzi na ogół w regionach, w których najczęściej występują klęski naturalne i żywiołowe, powodujące masową migrację ludności. Nie budzi wątpliwości teza, że eliminacja całego spektrum zagrożeń asymetrycznych nie jest możliwa za pomocą broni obezwładniającej jednak istnieją sposoby ograniczenia powstałych skutków. Masowe migracje ludności mogą stanowić źródła zagrożeń wtórnych. W tłumie uciekających mogą się znajdować członkowie organizacji zbrojnych, przestępcy i terroryści, którzy korzystając z okazji będą inspirowali rozruchy i zamieszki[29]. W tej sytuacji skuteczne mogą być sieci oplatające najbardziej aktywnych uczestników zamieszek oraz kolorowe pociski z farbą do oznaczania liderów akcji lub grup chuliganów. Obserwacje ruchów migracyjnych wskazują, że ich uczestnicy nie zawsze respektują przepisy i ustalenia, co do miejsc lokalizacji obozów i rejonów odpoczynku. Ponieważ rozwiązania siłowe w zakresie wymuszenia posłuszeństwa uchodźców, mogą doprowadzić do eskalacji napięć i spowodować rozruchy, celowe wydaje się wykorzystanie w celu eliminacji zagrożenia broni obezwładniającej. Rozmieszczone w wybranych punktach generatorów ultradźwięków może zapobiegać samowolnej organizacji postojów i odpoczynków w miejscach do tego nieprzygotowanych[30]. Nie należy wykluczać także konieczności rozpylenia lub rozlania specjalnych środków chemicznych, które będą izolowały wybrane obszary od niepożądanego napływu ludności. Ten sposób działania może być także efektywnym rodzajem izolacji zwaśnionych

[29] Doświadczenia między innymi z Bośni, Iraku i Afganistanu.
[30] Zabezpieczenie pielgrzymek wiernych do miejsc kultu religijnego.

mniejszości narodowych, które na skutek kataklizmu (np.: powodzi lub trzęsienia ziemi) opuściły swoje tereny i znalazły się w sąsiadujących obozach. Przykładem ilustrującym omawiane zjawisko jest powódź w Nowym Orleanie (2005), gdy na małej powierzchni przeznaczonej dla uchodźców dochodziło do zamieszek na tle rasowym.

5. Brak zdolności wielu rządów do skutecznego rządzenia i zaspokajania potrzeb ludności. Jest to zjawisko charakterystyczne dla wielu państw świata. Globalna sytuacja gospodarcza oddziałuje na ekonomikę poszczególnych państw, będąc źródłem wielu trudności i zagrożeń, które prowadzą do nieudanych reform gospodarczych oraz utraty stabilności ekonomicznej i bezpieczeństwa. Nieumiejętne przejście od gospodarki centralnie zarządzanej do wolnorynkowej również powoduje wiele problemów, takich jak destabilizacja gospodarki, duże bezrobocie i korupcja. Źle przeprowadzona demobilizacja, swobodny dostęp obywateli do broni, wzmacnia organizacje kryminalne i komplikuje powrót do normalności po zakończeniu konfliktu. Wskazany brak zdolności do sprawowania władzy państwowej i zaspokojenia potrzeb obywateli może stanowić przesłankę do powstania niepokojów społecznych. W sytuacji, gdy każde napięcie społeczne prowadzić może do wzrostu sytuacji kryzysowej należy zakładać, że użycie broni obezwładniającej będzie argumentem niwelującym poziom zagrożenia. Na podstawie rezultatów badań można wnioskować, że szczególnie skutecznym rodzajem broni obezwładniającej są środki chemiczne o działaniu łzawiącym, drażniącym, uspokajającym i obezwładniającym. Wykorzystanie do przywrócenia porządku granatów i dymów zawierających substancje chemiczne umożliwia siłom porządkowym oddziaływanie bez wchodzenia w bezpośredni kontakt z demonstrantami lub przestępcami. Ponadto szerokie zastosowanie w działaniach w bezpośredniej styczności mają ręczne miotacze gazu. Doświadczenia państw wykorzystujących już omawiane rozwiązania wskazują, że gaz lub dym użyty w odpowiednich stężeniach potrafi wyeliminować z działania na okres około 10 minut bardzo agresywnych napastników. Czas oddziaływania zastosowanego środka umożliwia aresztowanie i ograniczenie swobody postępowania wytypowanych uczestników zajść, zamachowców, dywersantów. Szczególnym sposobem izolowania osób, którym udowodniono działalność antyrządową jest wczepianie pod skórę niewielkich nadajników elektronicznych, które w polu magnetycznym wysyłają sygnały identyfikujące właściciela. W ten sposób po

wejściu na teren objęty monitoringiem osób do tego nieuprawnionych system identyfikuje ich położenie, a personel służby bezpieczeństwa może zatrzymać wskazanych, jeśli tylko podejmą działania niezgodne z prawem.

6. Katastrofy ekologiczne, takie jak: klęski żywiołowe, zmiany klimatu, degradacja środowiska naturalnego. Wskazane zjawiska mogą prowadzić do złej sytuacji ekonomicznej państwa, do konfliktów na płaszczyźnie dostępu do surowców, a także wymuszać masowe ruchy ludności. Zanieczyszczenie środowiska naturalnego w obszarach przygranicznych może również wywoływać napięcia między regionami oraz bardziej i mniej rozwiniętymi państwami. Także kwestia naruszenia równowagi bezpieczeństwa, wynikająca z przejęcia kontroli nad obiektami infrastruktury chemicznej i nuklearnej, może być przyczyną prowadzenia operacji wojskowych, w tym np. operacji wielonarodowych[31]. Do ochrony granic i zabezpieczenia obiektów przed niepożądanym wtargnięciem osób postronnych szeroko wykorzystuje się czujniki elektroniczne i kamery obserwacyjne z laserowym oznaczeniem celu. Z chwilą przekroczenia granic strzeżonego obszaru kamery podświetlają osoby łamiące prawo, a specjalne lampy wykrywające promienie pomagają w ujęciu przemytników. Innym sposobem przeciwdziałania zagrożeniom asymetrycznym w tej sytuacji jest zastosowanie specjalnych mat i pian chemicznych. Rozmieszczone na kierunkach podejścia do chronionych obiektów (np.: elektrownie, ujęcia wody, zakłady chemiczne) stanowią bezinwazyjną metodę zatrzymania intruzów, którzy planowo lub przez pomyłkę weszli w rejon zastrzeżony. Rozmieszczone piany lub maty stanowią kompilację środków chemicznych, które aktywują swoją działalność na skutek zmiany napięcia powierzchniowego. Wykorzystując nowoczesne rozwiązania technologiczne konstruktorzy opracowali piany i maty posiadające zdolność „rozróżniania" obiektu, dzięki temu nie reagują one na zwierzęta lub spadające liście i szyszki z drzew. Ich reakcja spowodowana jest jedynie wtargnięciem ludzi lub pojazdów w zabronione rejony. Działanie i skuteczność tego rodzaju środków z arsenału broni obezwładniającej zostało sprawdzone na granicy izraelskiej oraz w górach w Afganistanie gdzie chroniono bazy sił specjalnych i posterunki kontrolne.
7. Propaganda, którą mogą wykorzystywać zarówno rządy, jak i „aktorzy

[31] Zob. Z. Ścibiorek, *Wojna czy pokój*, Wrocław 1999, s. 164.

pozapaństwowi", wywołując i potęgując zagrożenie oraz oddziałując na opinię publiczną. Należy wskazać, że dzięki zwiększonemu dostępowi do informacji powstała możliwość manipulowania mediami przez strony konfliktu (np.: Irak, była Jugosławia). Jak wskazują zgromadzone doświadczenia bardzo skuteczną bronią są środki oddziaływania psychologicznego. Dysponując mobilnymi rozgłośniami i generatorami dźwięku można emitując sygnały powodujące zmiany w organizmach uczestników manifestacji. Skutecznym instrumentem oddziaływania na opinię publiczną są stacje radiowe i telewizyjne emitujące przygotowane programy wyjaśniające zaistniałą sytuację. Szczególnie ważną rolę odgrywają środki masowego przekazu w sytuacji, gdy na skutek działań militarnych lub rozruchów i starć z siłami porządkowymi zniszczono lokalne rozgłośnie zapewniające bieżące informowanie. Właściwie przygotowane audycje i materiały filmowe potrafią wykreować pożądany obraz sytuacji w rejonie działania. Dowodem prawdziwości tej tezy są wydarzenia z byłej Jugosławii i Iraku, gdzie Taktyczne Zespoły Działań Psychologicznych informowały lokalne społeczeństwo o miejscu i czasie przybycia konwojów z pomocą humanitarną i lokalizacji punktów pomocy medycznej. Ponadto rozpowszechniano wiadomości na temat odbudowy zniszczonej infrastruktury w regionie, uruchomienia wodociągów, elektrowni, transportu i zaopatrzenia. Obserwacja skutków zastosowania broni psychologicznej wskazuje, że dzięki kreowaniu pozytywnego wizerunku sił koalicyjnych zmieniło się nastawienie miejscowej ludności do sił zbrojnych zaangażowanych w działania. Zanotowano wzrost aktywności sektora cywilnego, współpracę i koordynacje działań sprzyjających poprawie sytuacji ludności. W Iraku i w Afganistanie w wyniku ukształtowania stabilnej sytuacji możliwe było przekazanie władzy lokalnym strukturom bezpieczeństwa i redukcja zagrożeń asymetrycznych.

8. Terroryzm, którego skutki odczuwają zarówno siły zbrojne jak i organizacje cywilne, a szczególnie ludność w rejonie konfliktu. Terroryści mogą także dokonywać ataków informacyjnych za pomocą hakerów wykorzystujących przede wszystkim wirusy komputerowe. Tego typu ataki na systemy komputerowe mogą przerodzić się w terroryzm informacyjny i mieć negatywny wpływ na przygotowanie i prowadzenie operacji wielonarodowych, a nawet doprowadzić do sparaliżowania systemów informacyjnych w państwach koalicji.

Zwiększone zagrożenie terroryzmem dostrzeżono również w Sojuszu Północnoatlantyckim, który po atakach terrorystycznych z 11 września do jego zwalczania po raz pierwszy w swej historii zastosował artykuł V Traktatu Waszyngtońskiego. Natomiast w celu permanentnego przeciwdziałania atakom terroru przewiduje prowadzenie konsultacji i podejmowanie działań zgodnych z treścią traktatu.

Po atakach terrorystycznych z 11 września 2001 r. problem zwalczania międzynarodowego terroryzmu znalazł się w centrum zainteresowania struktur polityczno-militarnych i wojskowych NATO. Aby w przyszłości zapobiec podobnym zagrożeniom, dokonano wielu analiz i podjęto zdecydowane działania w sferze obronnej, a także struktur wojskowych i broni masowego rażenia oraz politycznej i cywilnej. Wiele posiedzeń kierowniczych gremiów Sojuszu ze Szczytem Praskim włącznie, poświęcono zwalczaniu terroryzmu. Zjawisko to na pierwszym miejscu wśród współczesnych zagrożeń wymieniają również autorzy dokumentów doktrynalnych wielu państw[32]. Prowadzone badania teoretyczne i empiryczne pozwalają na postawienie tezy, że intensyfikacja rozwoju systemów broni obezwładniającej nastąpiła na skutek wzrostu skali zagrożeń asymetrycznych, w tym szczególnie aktywności terrorystycznej. Niestt y zgromadzone fakty wskazują, że sektory odpowiedzialne za bezpieczeństwo preferują rozwiązania siłowe. Dlatego w przyjętych rozwiązaniach docelowych wskazuje się na konieczność natychmiastowej eliminacji zagrożenia. Drogą ku temu są rozwiązania polegające na opracowaniu amunicji gazowej, chemicznej i rażącej, która umożliwia natychmiastowe obezwładnienie atakowanego terrorysty. Szeroko zakrojone są badania nad wykorzystaniem fal dźwiękowych o działaniu destrukcyjnym. Trzeba wskazać na fakt, że rozchodzenie się fali infradźwiękowej nie jest ograniczane przez przeszkody naturalne i budowane przez człowieka. Z tego powodu są to elementy broni obezwładniającej predysponowane do wykorzystania w rejonach zurbanizowanych, gdzie szczególnie często działają terroryści. Stąd należy wnosić, że wykorzystanie przedstawionych środków oddziaływania może stanowić perspektywiczny kierunek przeciwdziałania zagrożeniom asymetrycznym.

Zasadność czynników determinujących zagrożenia oraz poprawność przyjętych na tej podstawie założeń doktrynalnych potwierdziły się podczas operacji stabilizacyjnej prowadzonej przez siły wielonarodowe między innymi w Iraku, Afganistanie, Bośni i Kosowie.

---

[32] Zob. A. Tyszkiewicz, *Operacje stabilizacyjne*, Warszawa 2005, s. 31 i dalej.

Na podstawie obserwacji przebiegu zdarzeń można stwierdzić, że głównym zagrożeniem asymetrycznym dla sił wielonarodowych w wielu miejscach świata jest ruch oporu zorganizowany przez zwolenników byłego reżimu[33]. Uzyskane wyniki analiz wskazują, że największą siłę zbrojny ruch oporu przybiera w regionach zamieszkałych przez mniejszość narodową, która w okresie sprawowania poprzedniej władzy była niezwykle uprzywilejowaną grupą[34]. Stwierdzono, że zwolennicy byłego reżimu przygotowywali się do walki z siłami wielonarodowych kontyngentów sił pokojowych lub koalicyjnych struktur CJTF jeszcze przed rozpoczęciem operacji, tworząc swą organizację zbrojną często z wykorzystaniem wsparcia wojskowego z krajów sąsiednich[35]. Jak wskazują doświadczenia, wiele organizacji zbrojnych przygotowuje specjalne magazyny, Zawczasu gromadząc broń, amunicję i lokując środki finansowe w bankach.

Wskazane zagrożenia asymetryczne ich zróżnicowanie i odmienne źródła wymagają, aby stosować zróżnicowane systemy przeciwdziałania. Niestety brak jest obecnie uogólnionych wyników prowadzonych badań. W tej sytuacji zdecydowane wskazanie konkretnego kierunku rozwoju systemów ochrony jest trudne.

Istotnym źródłem zagrożeń, w opinii uczestników wielu operacji wielonarodowych jest frustracja lokalnej ludności spowodowana szeregiem zniszczeń, brakiem perspektyw na przyszłość, katastrofalną sytuacją gospodarczą, olbrzymim bezrobociem, a także przedłużającymi się przerwami w dostawach paliw i energii oraz brakiem zaopatrzenia w podstawowe produkty codziennego użytku. W tej sytuacji w rejonie operacji błyskawicznie rozwijała się działalność kryminalna obejmująca handel bronią i narkotykami, wymuszenia, porwania dla okupu, a także niebywała korupcja wśród urzędników państwowych wszystkich szczebli. Bezpośrednia eliminacja uczestników grup przestępczych może być realizowana z wykorzystaniem pocisków bezinwazyjnych, zawierających gaz paraliżujący lub środki psychotropowe o przedłużonym działaniu. Sprawdzonym w rejonach misji sposobem zwalczania nielegalnego handlu jest fizyczna izolacja miejsc, gdzie prowadzony jest przemyt i nielegalna działalność. Wykorzystanie w tym celu systemu znaków oświetlających oraz chemicznych środków znaczących. Detekcja osób zaangażowanych w nielegalna działalność możliwa jest dzięki zastosowaniu wykrywaczy niewidzialnego dla ludzkiego oka promieniowania w świetle lamp ultrafioletowych. Innym sposobem zapobiegania działaniom przestępczym jest rozmieszczenie w rejonie zagrożenia specjalnie przygotowanych min

[33] Ruch oporu rozumiany jako działania partyzanckie, sabotaż, terroryzm, dywersja, wzniecanie niepokojów społecznych.
[34] Haiti, Irak, Rwanda.
[35] Somalia, Irak, Afganistan.

i fugasów ze środkami obezwładniającymi w postaci gazu lub proszku. Z chwilą wejścia w rejon obiektu objęty ochroną następuje naruszenie systemu bezpieczeństwa i automatycznie zostają uruchomione systemy obronne. Po zerwaniu systemu zabezpieczenia, w powietrze są wystrzelane zasobniki ze środkami chemicznymi, które eksplodują na określonej wysokości nad ziemią. Na skutek wybuchu zostaje uwolniona ich zawartość powodując paraliż osób znajdujących się w rejonie działania miny. Nowym sposobem ograniczania swobody przemieszczania osób w rejonach objętych walką są systemy elektronicznej kontroli ruchu. Rozmieszczone w ustalonych parametrami technicznymi nadajniki emitujące fale elektromagnetyczne wyznaczają granice strzeżonego rejonu. Z chwilą przekroczenia linii bezpieczeństwa system wysyła impuls ostrzegawczy do urządzeń bojowych, a te po automatycznym naprowadzeniu środków rażenia emitują ukierunkowana wiązkę energii, która powoduje obezwładnienie intruza. Innym rozwiązaniem jest zastosowanie jako środka obezwładniającego siatki oplatającej lub piany samoprzylepnej. W obu przypadkach napastnik ma ograniczoną swobodę ruchu, a im bardziej energicznie stara się wyzwolić tym efektywniej działa środek obezwładniający.

Scharakteryzowane zagrożenia zarówno natury ogólnej, jak i specyficzne, z którymi mają do czynienia siły koalicji w Iraku czy Afganistanie, będą najprawdopodobniej typowymi zagrożeniami, które należy brać pod uwagę w czasie przygotowywania i prowadzenia operacji przez wielonarodowe formacje. Dlatego wskazane sposoby wykorzystania elementów systemów broni obezwładniającej będą prawdopodobnie rozwijane i doskonalone ze względu na dużą efektywność działania i niskie koszty produkcji, a także niski poziom strat osobowych, jakie powstają w toku operacji.

2.3. Nowe wyzwania dla systemu rozpoznania w aspekcie zagrożeń asymetrycznych

Ze zgromadzonych faktów można wnioskować, że każda sytuacja zastosowania systemów broni obezwładniającej w celu eliminacji zagrożeń asymetrycznych będzie inna, niepowtarzalna. Dotyczy to również zagrożeń, które będą specyficzne dla danego rejonu działań, charakteru operacji i składu kontyngentu wojskowego. Zagrożenia te, ich rodzaj, wzajemne powiązania oraz intensywność występowania będą warunkowały w istotny sposób rodzaj wykorzystywanych systemów broni obezwładniającej. Przedstawione aspekty warunkujące użycie środków obezwładniających w aspekcie zagrożenia, nie wyczerpują całej problematyki zadań sił militarnych, nie należy zapominać o szerokim spektrum możliwości

konwencjonalnego oddziaływania, a więc na przekład elementów walki elektronicznej i zespołów działań psychologicznych.

Po szeregu zmianach politycznych i gospodarczych nowym gwarantem bezpieczeństwa Polski stało się wstąpienie do Sojuszu. W oficjalnych wystąpieniach zarówno politycy jak i wojskowi stwierdzają, że nie występuje bezpośrednie zagrożenie ze strony państw sąsiednich. Akcentują także, że wielka konfrontacja zbrojna – globalna wojna nie jest prawdopodobna w najbliższej przyszłości, ale zagrożenie stanowią różne formy konfliktów charakteryzujące się „asymetrycznością" przebiegu. To właśnie narastające konflikty, nawet te odległe, mają określony wpływ na sytuację nie tylko w Polsce, ale również na całym kontynencie europejskim. Stąd też tak wiele uwagi w aspekcie politycznym i militarnym poświęca się problemom lokalnym i regionalnym oraz udziałowi sił zbrojnych w operacjach innych niż wojna, prowadzonych w rejonach bardzo oddalonych od granic własnego państwa. Fakt interweniujących w odległych zakątkach świata jednostek wojskowych dziś już nikogo nie dziwi. Operacje w Afganistanie i Iraku rzuciły całkiem nowe światło na użycie formacji „sił interwencyjnych" (sił zadaniowych). Należy się zgodzić z opinią ekspertów wojskowych, że rola jednostek rozpoznawczych przygotowanych do realizacji odmiennych od standardowych zadań we współczesnych i przyszłych konfliktach zbrojnych na pewno wzrośnie. Zdolność do prowadzenia operacji w różnym środowisku i to zarówno terenowym jak i społecznym sprawia, że pododdziały rozpoznawcze stają się jednostkami pierwszego rzutu operacyjnego. Problem dotyczy wykorzystania wszystkich sił i środków rozpoznania, w tym także tych wysoce wyspecjalizowanych, takich jak pododdziały rozpoznania elektronicznego, specjalnego, działań psychologicznych[36].

Zapobieganie kryzysom oraz skuteczne przeciwdziałanie zagrożeniu bezpieczeństwa wymusza postępowanie prewencyjne, co w kontekście polityczno-wojskowym oznacza użycie sił zbrojnych poza obszarem kraju. Wiele publikacji ostatniego 10-lecia wskazuje, że wykorzystanie jednostek rozpoznawczych w działaniach ratunkowych, humanitarnych czy stabilizacyjnych – to realizm dzisiejszych i przyszłych operacji. Jednak już niewielu wskazuje, że do realizacji całego spektrum nowych zadań potrzebne są także nowe elementy systemu rozpoznania, które będą w stanie sprostać różnorodnym potrzebom informacyjnym w poszczególnych operacjach. Z przedstawionych powyżej faktów wynikają także nowe uwarunkowania dla systemu rozpoznania.

---

[36] Zob. M. Wrzosek, *Uwarunkowania działalności rozpoznawczej w operacjach wsparcia pokoju i stabilizacyjnych*, Przegląd Wojsk Lądowych nr 7/2005.

Nowe spojrzenie na problematykę powstawania zagrożeń asymetrycznych i sposobów ich rozwiązywania, spowodowało, że na szczycie NATO w Pradze utworzono siły odpowiedzi, czyli siły zdolne do reagowania na zaistniałe sytuacje kryzysowe w dowolnym regionie świata. Takie podejście sprawia, że sprzęt wojskowy, w tym środki rozpoznania muszą być zdolne do działań mobilnych prowadzonych w znacznym oddaleniu od macierzystych krajów. W zakresie rozpoznania wymóg ten szczególnie dotyczy środków przekazu informacji rozpoznawczych, a więc łączności satelitarnej i KF a także, co niezmiernie istotne elementów zabezpieczenia logistycznego.

Jak wskazują wyniki analizy doświadczeń operacji pokojowych będących przedmiotem badań, na wiele dni przed lądową operacją w rejonie kryzysowym elementy rozpoznawcze w tym siły specjalne, patrole dalekiego rozpoznania, zespoły działań psychologicznych penetrują i przygotowują obszar przyszłej interwencji. Organizują działania rozpoznawcze w strefie odpowiedzialności i przygotowują wsparcie polityczne. Rozpoznanie osobowe w operacjach pokojowych jest najbardziej wiarygodnym i pożądanym przez dowódców przejawem aktywności rozpoznawczej. Stąd też należy wnioskować, że udział jednostek rozpoznania osobowego w pozyskiwaniu informacji na potrzeby podejmowania decyzji w rejonie sytuacji kryzysowej pozostanie w centrum zainteresowania decydentów zarówno politycznych jak i militarnych.

Zasadniczym zadaniem rozpoznania (w tym szczególnie studyjnego) w operacjach militarnych, poza możliwie wczesnym wykryciem rejonów nowych ognisk zapalnych i ich monitorowaniem, jest informacyjne wsparcie jednostek przewidzianych do działania w rejonach zagrożenia lub wojsk już działających w wyznaczonych strefach. Stąd też w kontekście zagrożeń, jakie mogą wystąpić w sytuacji kryzysowej system rozpoznania informuje, monitoruje i ostrzega. Na podstawie szeregu publikacji i wniosków z przebiegu dotychczasowych konfliktów za najważniejsze zadanie rozpoznania w działaniach asymetrycznych można uznać informowanie organów kierowania państwem i sztabu generalnego o aktualnej sytuacji oraz prognozowanie ewentualnych zagrożeń. Natomiast w odniesieniu do jednostek przewidzianych do działania w rejonie kryzysu należy wskazać, że priorytetem być powinno opracowanie i przekazanie wszelkich dostępnych informacji o rejonie działania. Konieczne będzie również przygotowanie możliwych scenariuszy (wariantów) rozwoju sytuacji (działania stron konfliktu) i ocena związanego z tym ryzyka (poziomu zagrożenia).

Na podstawie zgromadzonych faktów można wnioskować, że w związku z koniecznością zapewnienia bezpieczeństwa jednostkom przygotowującym się do działania

lub już działającym jako kontyngenty celowe jest opracowanie zaleceń dotyczących ochrony stanu osobowego i sprzętu (bezpieczeństwo wojsk własnych). Podejmowane przedsięwzięcia powinny koncentrować się na zapewnieniu bezpieczeństwa wojskom zarówno w bazie (obozie) jak i w czasie realizacji zadań na posterunkach i patrolach[37]. Z powodu niestabilnej sytuacji polityczno-wojskowej w rejonie konfliktu, nie należy wykluczać, że problem zapewnienia bezpieczeństwa wojsk i obywateli może także wystąpić na terenie naszego kraju (zamachy terrorystyczne, napady na wartowników). Rozwiązaniu powyższych zagadnień służą podejmowane obecnie działania minimalizujące poziom zagrożenia. Opracowywaniu i doskonaleniu ulegają także procedury postępowania i zasady reagowania w przypadkach nieznanych zjawisk i zachowań. Istotnym i zupełnie nowym zadaniem wydaje się także ochrona kontyngentów przed działaniem służb wywiadowczych państw rejonu objętego kryzysem[38].

Przedstawione powyżej uwarunkowania skłaniają do wniosku, że w celu uzyskania zdolności do działań rozpoznawczych w ramach operacji pokojowych i stabilizacyjnych należy już dziś w naszym kraju rozpocząć budowę jakościową i ilościową systemu rozpoznania uwzględniającą nowe zadania[39]. Jak wskazują rezultaty obserwacji praktycznych działań w rejonach misji i konfliktów istotnym zagadnieniem analizowanego problemu jest także budowa przyszłościowych struktur organizacyjnych formacji rozpoznawczych zdolnych do samodzielnego funkcjonowania w układzie narodowym oraz koalicyjnym. W związku z szeregiem zmian organizacyjnych konieczna wydaje się również techniczna modyfikacja rozpoznania, zwłaszcza w oddziałach i pododdziałach przewidywanych do użycia w ramach operacji innych niż wojna.

Jednym z najmłodszych rodzajów rozpoznania jest rozpoznanie osobowe (HUMINT), które stanowi wartościowe dopełnienie rozpoznania prowadzonego z wykorzystaniem środków technicznych. Niestety, nie może być powszechnie stosowane w działaniach asymetrycznych ze względu na zbyt małą liczbę przygotowanego personelu. Braki występują także w zakresie znajomości języka kraju gdzie prowadzone są działania, stąd konieczne jest korzystanie z pomocy pracowników cywilnych (przykładem operacja w Iraku, gdzie brakowało specjalistów językowych). W tej sytuacji wydaje się słuszne

---

[37] Zob. Bąk T., *Doświadczenia z Kosowa*, Przegląd Wojsk Lądowych, nr 5/2001

[38] Zob. M. Dukaczewski, *Informacyjne zabezpieczenie operacji „Iracka Wolność"* [w:] Operacja „Iracka Wolność", materiały z konferencji naukowej, AON, Warszawa 2003.

[39] Planując np.: informatyczne wsparcie procesów przetwarzania danych rozpoznawczych, opracowanie geoinformacji o obszarze działania, przesłuchiwanie jeńców, zbiegów, uchodźców.

priorytetowe traktowanie rozpoznania osobowego[40]. Bowiem w sytuacji reagowania kryzysowego coraz większego znaczenia nabierają możliwości analizowania i przewidywania, a przede wszystkim zapewnienie dopływu dokładnych i aktualnych informacji z rozpoznania osobowego.

Na koniec warto wskazać, że o jakości każdej organizacji stanowią ludzie. Tak więc personel rozpoznania w działaniach asymetrycznych stanowić powinna grupa osób wybranych, sprawdzonych i doskonale wyszkolonych w specyfice działań rozpoznawczych w operacjach pokojowych i stabilizacyjnych[41]. Dlatego dotychczasowa, szczupła baza osobowa rozpoznania wojskowego wymaga nie tylko ilościowych, ale i jakościowych zmian. Nie chodzi przy tym o wprowadzenie specyficznego modelu pracy zawodowej, lecz o podniesienie poziomu profesjonalizmu kadry poprzez system kształcenia w zakresie oceny i prognozowania zagrożeń o podłożu nie tylko militarnym.

Zebrane doświadczenia wskazują, że najważniejszym elementem strukturalnym „nowego" systemu rozpoznania na potrzeby działań asymetrycznych powinno być zintegrowane centrum rozpoznania[42]. Utworzenie zintegrowanego centrum rozpoznania pozwoli na zbieranie i opracowywania informacji rozpoznawczych napływających z różnych źródeł militarnych i cywilnych. Zatem personel centrum stanowić powinni pracownicy cywilni i wojskowi po to, aby uporządkować i przekazać do dyspozycji odpowiednich organów (dowodzenia i kierowania) zebrane wiadomości. W przypadkach wątpliwych lub sprzecznych centrum może przygotować materiały do konsultacji specjalistycznych (opinie ekspertów, weryfikacja danych). Pracujące na potrzeby centrum urządzenia telekomunikacyjne oraz systemy przetwarzania informacji powinny zapewnić całodobowe opracowywanie informacji, a to z kolei umożliwi podejmowanie decyzji w celu opanowania kryzysu albo wzmocnienia działających sił stabilizacyjnych lub pokojowych. Wspólne działania w sferze rozpoznania nie będą możliwe bez dostosowania systemu łączności (procedury, częstotliwości, kodowanie) do potrzeb użytkowników narodowych przy zachowaniu zobowiązań sojuszniczych. Konieczna jest także integracja w systemach informatycznych i jednolity standard informacyjny[43]. Na podstawie sumarycznych wniosków z dotychczasowej działalności rozpoznawczej zespół autorski przewiduje, że do zasadniczych zadań Centrum należy zaliczyć:

---

[40] W armii niemieckiej i holenderskiej planuje się po jednym plutonie w każdym związku taktycznym.
[41] Konieczne wydają się kursy specjalistyczne dla oficerów rozpoznania w zakresie oceny i analizy sytuacji nie tylko militarnej.
[42] Być może taką rolę przejmie dowództwo operacyjne.
[43] Doświadczenia z Somalii, Bośni i Iraku potwierdzają słuszność prezentowanego wniosku.

- kierowanie rozpoznaniem w rejonie kryzysu (misji, operacji);
- gromadzenie informacji i zarządzanie zasobami informacyjnymi na potrzeby działalności prewencyjnej;
- opracowanie polityczno-militarnej oceny sytuacji i prognozy jej rozwoju w rejonie kryzysowym (odpowiedzialności i zainteresowania rozpoznawczego);
- przedstawianie aktualnej sytuacji i prognozowanie jej rozwoju.

Z chwilą utworzenia Dowództwa Wojska Lądowych oraz Dowództwa Operacyjnego nastąpiła koncentracja wszystkich sił i środków rozpoznania osobowego i elektronicznego. Takie rozwiązanie wpływa na większą elastyczność użycia sił i środków w rejonach odpowiedzialności oraz zwiększa zdolności przetwarzania informacji. Zapewnia także kierowanie rodzajami rozpoznania poszczególnych jednostek i koordynowanie ich działań. Zarówno w zakresie przygotowania do działania lub wydzielenia stosownych elementów na potrzeby reagowania w rejonie kryzysowym, prowadzenia operacji stabilizacyjnych i pokojowych. W ten sposób w aspekcie narodowym wydzielona komórka rozpoznania będzie dla sojuszników partnerem do wymiany informacji dotyczących sytuacji w rejonie działania. Bowiem nie należy zapominać, że poszczególne podsystemy rozpoznania wzajemnie się uzupełniają, a zdobywane informacje są wykorzystywane na bieżąco do informowania lub też gromadzone w zasobach informacyjnych na potrzeby analizy (rozpoznanie studyjne).

Dla zapewnienia wartościowych informacji konieczna jest reorganizacja dotychczasowego sposobu gromadzenia danych rozpoznawczych. W związku z tym celowym jest jasne wyodrębnienie zakresu kompetencji rozpoznawczych na potrzeby operacji wysokiej i niskiej intensywności prowadzonych działań (pokojowych i stabilizacyjnych). Oznacza to, że rozpoznanie strategiczne powinno posiadać informacje o zasięgu światowym, a więc monitorować rejony podwyższonego ryzyka. Rozpoznanie operacyjne powinno dysponować danymi o rejonach działania, w których nastąpia eskalacja zagrożenia i konieczne było rozmieszczenie sił interwencyjnych. Zatem rozpoznanie taktyczne gromadzić będzie informacje bezpośrednio ze strefy odpowiedzialności.

W projektach rozwoju systemu rozpoznania RP zakłada się, że integralną częścią rozpoznania strategicznego będą budowane elementy systemu AGS, nadzorowania sytuacji lądowej z powietrza. Zdobywane informacje muszą być uzupełnione przez polityczno-gospodarcze analizy poszczególnych rejonów kryzysowych. Bowiem jak wskazują doświadczenia zagrożenia bezpieczeństwa są rezultatem poważnych problemów gospodarczych, trudności społecznych i politycznych, z rywalizacją etniczną i sporami

terytorialnymi włącznie. Ewentualne napięcia nawet, jeżeli będą miały charakter lokalny mogą zagrażać stabilizacji regionu i w konsekwencji prowadzić do konfliktów zbrojnych[44]. Rozpoznanie operacyjne realizowane na poziomie komponentu wojsk lądowych w operacji reagowania kryzysowego dla uzyskania stosownych informacji musi dysponować całą gamą urządzeń do rozpoznania „bezinwazyjnego" to znaczy zdolnych do pozyskiwania danych rozpoznawczych za pomocą środków rozpoznania elektroniczne i bezpilotowych aparatów latających.

Uzupełnieniem rozpoznania operacyjnego winno być rozpoznanie prowadzone w rejonach działania przez siły i środki poszczególnych kontyngentów (narodowe działania rozpoznawcze). Z organizacyjnego punktu widzenia sojusz podjął stosowne działania dążąc do wyodrębnienia samodzielnych modułów rozpoznawczych (ISTAR[45]). Należy wnioskować, że moduły tworzone będą w celu integracji zadań rozpoznawczych na bazie sił i środków zarówno rozpoznania osobowego sęp jak elektronicznego. Struktura organizacyjna każdego modułu rozpoznawczego określana będzie stosownie do realizowanego zadania. Ze względu na jego specyfikę[46] i możliwości zdobywania aktualnych i szczegółowych informacji, dane te będą wykorzystywane nie tylko przez poszczególne kontyngenty, lecz będą także ważnym źródłem informacji dla komórek rozpoznawczych szczebla operacyjnego i strategicznego (w tym państwowego). Dla zapewnienia sprawności procesów informacyjnych konieczne jest dysponowanie całym spektrum środków łączności i urządzeń teleinformatycznych zapewniających bezpieczeństwo przesyłanych informacji[47].

Analiza wniosków z obserwacji przebiegu narastania i rozwoju sytuacji kryzysowych pozwala na przypuszczenie, że współdziałanie międzynarodowych zespołów rozpoznawczych musi się ogniskować na:

- systematycznym korzystaniu ze zbiorów informacyjnych;
- koordynacji działań i wzajemnym uzupełnianiu się poszczególnych podsystemów rozpoznania;
- połączeniu odpowiednich sensorów w jeden system zbierania i analizowania danych;

---

[44] Przykład byłej Jugosławii, powstanie nowych państw z byłych republik radzieckich, krach gospodarczy w Argentynie.

[45] Intelligence, Surveillance, Target Acquisition, Reconnaissance.

[46] Specjalistyczne elementy rozpoznawcze.

[47] Doświadczenia wojsk amerykańskich z wykorzystaniem grup ISR (*intelligence, Surveillance, Reconnaissance*) są potwierdzeniem słuszności prezentowanej tezy.

- bieżącym opracowywaniu wiadomości i komunikatów rozpoznawczych.

Zespół autorski zakłada, że przedstawione rozwiązania przyczynią się do poprawy działalności całego systemu rozpoznania organizowanego na potrzeby operacji prowadzonych zarówno na terenie kraju, jak i poza jego granicami oraz do efektywniejszego wykorzystania zdobytych informacji. Ponadto zdobytymi i opracowanymi informacjami w kraju będzie można wspierać jednostki działające jako kontyngenty wojskowe. Prowadzenie działań pokojowych i stabilizacyjnych w rejonach kryzysowych oraz ich wszechstronne wsparcie – to największe wyzwania w ostatnim okresie stojące przed rozpoznaniem.

Doświadczenia z minionych operacji pokojowych sprawiły, że zainteresowane państwa do oceny sytuacji w rejonach kryzysowych kierują rozpoznawcze elementy wsparcia (np. *National Intelligence Cell*). Są to specjalnie zorganizowane mobilne zespoły, zdolne do szybkiego przerzutu w rejony zagrożenia. Mogą one wspierać informacyjnie narodowe dowództwo, dowódcę kontyngentu oraz tych, którzy informacji potrzebują (np.: organizacje humanitarne, lokalna policja), jednak z zastrzeżeniem, że mają prawo je otrzymać (dostęp informacyjny). Ponadto zespoły narodowe mogą przekazywać zdobyte wiadomości jednostkom państw zaprzyjaźnionych działających w tym samym rejonie.

Rozpoznanie wojskowe jako integralna część komponentu lądowego ponosi odpowiedzialność za analizę i ocenę sytuacji oraz prognoę zagrożeń podczas działania każdego kontyngentu. Aby sprostać wymaganiom, musi uwzględniać m.in. potrzeby informacyjne kontyngentów dotyczące zagadnień: politycznych, socjologicznych, etnicznych, religijnych, gospodarczych, medycznych (sanitarnych), logistycznych i infrastruktury. Konieczne jest przy tym uwzględnianie również nowej problematyki w operacjach reagowania kryzysowego dotyczącej między innymi:

- rozprzestrzeniania broni masowego rażenia (BMR)[48];
- przestępczości zorganizowanej w rejonie kryzysu[49];
- przemytu broni i narkotyków[50];
- ruchów migracyjnych ludności[51].

Jak wskazują uzyskane wyniki badań, zasadniczo zebranie informacji na wyszczególnione powyżej zagadnienia obejmujące problematykę zagrożeń asymetrycznych wchodzi w zakres

[48] Np.: Irak, Korea.
[49] Bośnia, Chorwacja, Słowenia po rozpadzie Jugosławii.
[50] Kosowo – Polsko-Ukraiński Batalion pilnuje granicy i likwiduje przemyt miedzy innymi broni i amunicji.
[51] Powrót uchodźców do kraju, ewakuacja ludności z zagrożonych terenów w operacjach na terenie byłej Jugosławii.

kompetencji wywiadu. Zatem efektywna współpraca z wywiadem wojskowym ma dla rozpoznania szczególne znaczenie. Różne zadania, środki oraz metody działania wyraźnie rozgraniczają oba komponenty pozyskujące różne zasoby informacyjne. Decydujące znaczenie jednak to, że napływ informacji ze wszystkich źródeł służy ocenie tej samej sytuacji w regionie kryzysowym. Dane uzyskane przez różne zespoły analityczne, za pomocą odmiennych środków i metod uzupełniają się, dzięki czemu uzyskiwany jest efekt synergiczny działalności rozpoznawczej – prawdziwy obraz aktualnej sytuacji w rejonie kryzysu. Wynika z tego, że w przypadku sytuacji kryzysowej wywiad i rozpoznanie wojskowe, działając w ramach swoich kompetencji, uzupełniają się, przyczyniając się w ten sposób do zdobywania informacji niezbędnych dla właściwej oceny sytuacji.

Doświadczenia państw zachodnich wskazują, że w realizacji zadań stojących przed rozpoznaniem wojskowym w zakresie pozyskiwania informacji współuczestniczą attachaty wojskowe. Bowiem reprezentują one polityczno-militarne, militarne i obronne interesy państwa[52]. W opinii zespołu autorskiego, ze względu na ciągle zmieniającą się sytuację międzynarodową oraz zwiększający się zakres zadań rozpoznawczych nie można pominąć roli tych źródeł informacji.

Zagrożenie związane z prowadzeniem działań asymetrycznych w sytuacji kryzysowej jest realne w wielu rejonach świata. Od rozpoznania wojskowego wymaga się zatem pełnej i rzetelnej informacji zapewniającej budowę banku wiedzy oraz elastycznego doboru środków i sposobów zdobywania informacji umożliwiających nadążanie za zmianami w rejonach podwyższonego ryzyka.

Reasumując dotychczasowe ustalenia można wnioskować, że do uwarunkowań rozpoznania w kontekście zagrożeń asymetrycznych należy zaliczyć przede wszystkim:

- dynamiczne zmiany w rozmieszczeniu sił aktualnego i potencjalnego przeciwnika,
- stosunek miejscowej ludności oraz państw ościennych do sił interwencyjnych, w tym przypadku należy się liczyć z brakiem akceptacji, a nawet wrogim nastawieniem i przeciwdziałaniem mieszkańców, traktujących - z powodów politycznych, religijnych i kulturowych –wojska biorące udział w operacji jako agresora;
- funkcjonowanie ugrupowań bojowych przeciwnika, które nie zostały rozbite lub zlikwidowane oraz grup zbrojnego podziemia (dywersyjno-

[52] Zob. S. Miłosz, *Rola ataszatu wojskowego w procesie integracji Rzeczypospolitej Polskiej z państwami Sojuszu Północnoatlantyckiego*. Warszawa, AON 2001.

sabotażowych), gotowych do ewentualnych działań partyzanckich na terenach zajętych przez siły stabilizacyjne lub pokojowe;

- odmienność warunków klimatycznych, kulturowych oraz religijnych;
- możliwość kierowania w rejon operacji zbrojnej przez organizacje terrorystyczne zamachowców, w celu podjęcia działań wymierzonych w siły interwencyjne na terytorium państwa, na którym jest prowadzona operacja. Nie należy także wykluczać wsparcia udzielanego ugrupowaniom wrogim w stosunku do sił pokojowych lub stabilizacyjnych przez państwa sąsiadujące z krajem objętym działaniami interwencyjnymi;
- działalność przestępczości zorganizowanej związanej głównie z nielegalnym handlem bronią i narkotykami, czemu sprzyja - charakterystyczny dla konfliktów zbrojnych - proces ubożenia społeczeństwa oraz niski poziom sprawności lokalnych sił porządkowych;
- występowanie zjawisk kryminalnych, typowych dla kraju objętego działaniami wojennymi, w tym przede wszystkim wynikających z działalności grup przestępczych, a także - jak wskazują doświadczenia z minionych operacji - grabieży mienia prywatnego[53] i państwowego[54] dokonywanej przez miejscową ludność na terenach zajętych przez siły pokojowe lub stabilizacyjne;
- obecność na zajętym terenie służb specjalnych i lojalnych pracowników wobec dotychczasowych władz kraju, w którym prowadzona jest operacja[55];

W związku z tym, że wiele aspektów zagrożenia asymetrycznego dotyczy strefy tyłowej sił stabilizacyjnych lub pokojowych przed rozpoznaniem stoi szereg nowych wyzwań. Należą do nich ocena zagrożenia wynikająca z działań organizacji terrorystycznych mogących podejmować akcje odwetowe, rozpoznanie nastrojów społecznych, ustalenie lokalnych przywódców organizujących strajki i manifestacje oraz określenie stanu bezpieczeństwa i porządku publicznego na trasach patroli i w rejonach działania sił pokojowych lub stabilizacyjnych.

Wnioski z przebiegu operacji pokojowych i stabilizacyjnych wskazują, iż dowódca odpowiedzialny za prowadzenie działań będzie od rozpoznania nieco innych informacji rozpoznawczych niż w warunkach militarnych. Z ogólnych ustaleń wynika, że będą one

[53] Wojna w byłej Jugosławii – rozkradanie opuszczonych domów.
[54] Operacja „Iracka Wolność" – rozkradanie dzieł sztuki i zabytków.
[55] Irak, Afganistan, Bośnia.

dotyczyły:

- sytuacji politycznej, która warunkuje prowadzenia działań militarnych;
- sytuacji strategicznej w rejonie konfliktu, zwłaszcza postaw i nastrojów w państwach sąsiednich;
- podłoża historycznego, etnicznego, kulturalnego oraz prawdopodobnego wpływu tych czynników na przebieg operacji;
- oceny postaw i wpływu zewnętrznych ugrupowań politycznych, finansowych, religijnych na przebieg misji;
- zaangażowania środków masowego przekazu, określenie ich aktywności i wiarygodności informacji;
- sytuacji w obszarze spraw cywilnych (ranni, chorzy, poziom bezrobocia, przestępczość, itd.).

Sumaryczne rezultaty badań pozwalają stwierdzić, że w kontekście operacji pokojowych rozpoznanie w Wojsku Polskim stoi przed koniecznością rozwiązania dwóch problemów. Pierwszy to przystosowanie jednostek rozpoznawczych do nowych wyzwań, co oznacza, że przede wszystkim muszą być zdolne do udziału w całym spektrum reagowania kryzysowego. Pozostawać w gotowości do rozwinięcia działań rozpoznawczych w czasie bezpośredniego konfliktu i utrzymać zdolność do działania po jego [illegible]zeniu, a więc w okresie stabilizacji. Tak, więc system rozpoznania musi funkcjonować zaraz po ujawnieniu symptomów kryzysu, monitorować jego przebieg i być zdolnym do pozyskiwania i opracowywania informacji aż do czasu jego całkowitego zakończenia. Z uwagi na konieczność reagowania nawet na ograniczony kryzys system rozpoznania musi być zdolny w wymaganym stopniu do natychmiastowej reakcji oraz błyskawicznego rozwinięcia w rejonie objętym kryzysem.

Kolejnym problemem systemu rozpoznania jest sprostanie pojawiającym się wyzwaniom operacyjnym i technologicznym. Dotyczy to działania w niesprzyjającym środowisku (specyficzne warunki obszaru działania), nie zawsze przeciwko zdefiniowanemu przeciwnikowi, który dąży do narzucenia swojej woli. W czasie operacji pokojowych lub stabilizacyjnych nie należy zapominać, że działania rozpoznawcze są podejmowane lub prowadzone w ramach ograniczeń politycznych limitujących zarówno rodzaj i wielkość użytych wojsk, jak i poziom strat tolerowanych przez społeczeństwo. Sprostanie tym wyzwaniom wymaga, aby system rozpoznania stał się bardziej skuteczny (wystarczalny informacyjnie) i uniwersalny (działania militarne, u progu wojny i pokojowe). Może bowiem powstać taka sytuacja polityczno-militarna, w której część systemu rozpoznania podejmie

bezpośrednie działania rozpoznawcze w sytuacji eskalacji zagrożenia, a inne komponenty będą jedynie prowadzić rozpoznanie studyjne monitorując rozwój działań.

Wyniki przeprowadzonych badań wskazują, ze narodowe doświadczenia w zakresie prowadzenia działalności rozpoznawczej w działaniach asymetrycznych są dopiero na etapie weryfikacji. Dotychczas zgromadzone wiedza z okresu operacji reagowania kryzysowego jedynie wykazała braki w systemie rozpoznania i konieczność zmian w strukturach organizacyjnych i wyposażeniu. W efekcie pozyskanych wniosków między innymi na stałe wprowadzono do sztabu batalionu sekcję rozpoznania S-2, wyposażono transportery rozpoznawcze w mobilne radary pola walki, nowe przyrządy obserwacyjne, systemy nawigacji satelitarnej. Jednak zasadniczym obszarem sprawdzenia praktycznych rozwiązań z zakresu rozpoznania są działania stabilizacyjne w Iraku. Międzynarodowa Dywizja pod polskim dowództwem w praktyce realizuje szereg zadań rozpoznawczych w warunkach koalicyjnych w środowisku zagrożeń asymetrycznych. Dopiero teraz po zgromadzeniu i analizie wniosków oraz doświadczeń możliwe będzie opracowanie pozyskanej wiedzy. W Iraku po raz pierwszy samodzielnie przez Wojsko Polskie realizowane są działania psychologiczne, rozpoznanie osobowe, obrazowe (wykorzystanie rumuńskich systemów *Shadows*) czy wymiana informacji rozpoznawczych[56].

Nowym zagadnieniem w rozpoznaniu jest także informacyjne przygotowanie i kontrwywiadowcze zabezpieczenie realizacji projektów CIMIC. Przykładem jest tutaj odbudowa i dodanie do użytku (19 sierpnia 2005) przez specjalistów współpracy cywilno-wojskowej Polskiego Kontyngentu Wojskowego w Iraku kolejnej szkoły. Szkoła znajduje się w miejscowości Abu Gharab, na zachód od Hilli, w prowincji Babil. Prace przy jej odbudowie rozpoczęły się podczas IV zmiany PKW w Iraku. Projekt koordynowali specjaliści CIMIC (współpraca cywilno-wojskowa) 1 Brygadowej Grupy Bojowej, której jednostki stacjonują w Diwaniji i Hilli. W ramach projektu odnowiono między innymi sale lekcyjne, pomieszczenia użytkowe, węzły sanitarne, szkoła ma nowe boisko sportowe, nową elewację budynków oraz tzw. małą architekturę. W Iraku, podobnie jak w Polsce, już wkrótce rozpoczyna się rok szkolny. Do szkoły w Abu Gharaq uczęszczać będzie pół tysiąca dzieci. Od początku misji do połowy 2006 roku, Wielonarodowa Dywizja Centrum-Południe zrealizowała 477 projektów na rzecz rozwoju systemu edukacyjnego w Iraku. Pozornie tylko wydaje się, że jest to problem rozwoju systemu edukacji należy do CIMIC, tymczasem bez

[56] Zob. szerzej: *Rozpoznanie w Iraku – wyobrażenia a rzeczywistość*. Przegląd Wojsk Lądowych nr 12/2003.

udziału elementów rozpoznania osobowego[57] i działań psychologicznych[58] realizacja tego i innych projektów wymagających wielu szczegółowych informacji nie byłaby możliwa.

Przedstawione uwarunkowania są jedynie uogólnieniem wielu wniosków, jakie opracowano na podstawie doświadczeń uczestników misji pokojowych i stabilizacyjnych, dostępnych materiałów sojuszniczych i otwartych źródeł informacji. Temat jest wielowątkowy i złożony, jego kompleksowe opracowanie musi, zatem uwzględniać zróżnicowane aspekty, które ze względu na obszerność zagadnień nie mogą być przedmiotem jednej pracy.

2.4. Asymetria a bezpieczeństwo wojsk

Dla kompletności prowadzonych badań należy wskazać na fakt, że eskalacja zagrożeń asymetrycznych powoduje potrzebę wzmocnienia ochrony i bezpieczeństwa wojsk działających w obszarze operacji. Eksperci wojskowi stwierdzili, że nowe połączenie elementów zagrożenia występujących do tej pory oddzielnie stworzyć może zupełnie nową, zaskakującą swoimi możliwościami całość. W odpowiedzi na nowy typ zagrożeń, zakłada się, że powstanie sprzężony układ wielu różnych urządzeń zapewniający ochronę i przeżycie wojsk zaatakowanych na przykład bronią konwencjonalną przez przeciwnika posiadającego niżej technologicznie rozwinięty system bojowy. Niemieccy specjaliści korporacji Rheinmetall Defence[59] zaprezentowali realny i wirtualny parasol obronny, rozpięty nad zainscenizowanym obozem wojskowym (bazą, obiektem militarnym). Rozbito go w terenie, w którym zgodnie z wymogami armii kwaterująca jednostka musi się liczyć z nieprzychylnym, a nawet wrogim przyjęciem miejscowej ludności i jej zdemilitaryzowanych sił zbrojnych, a także z aktami sabotażu, a nawet otwartymi, zaplanowanymi atakami terrorystycznymi, a więc całym spektrum zagrożeń asymetrycznych. Warto, zatem zwrócić uwagę na fakt, że przyjęty scenariusz i założenia operacyjno-użytkowe prezentowanego projektu nie były dalekie od realiów irackich, czy afgańskich. Pamiętać przy tym należy, że operacje interwencyjne grup bojowych Unii Europejskiej, czy sił odpowiedzi

[57] Ustalenie lokalizacji szkoły z uwzględnieniem składu narodowościowego okolicznych mieszkańców, rozpoznanie struktury lokalnej władzy, autorytetów religijnych i politycznych wspierających budowę szkoły, rozpoznanie i identyfikacja potencjalnych zagrożeń oraz ich eliminacja we współdziałaniu z lokalnymi siłami porządkowymi.

[58] Akcja informacyjna o potrzebie odbudowy szkoły, konieczności jej ochrony, zabezpieczenia budynku szkoły przed kradzieżą i dewastacją, pozyskanie nauczycieli, zakup pomocy dydaktycznych na miejscowym rynku. Przekazanie do lokalnej prasy i rozgłośni przygotowanych komunikatów prasowych w sprawie odbudowy szkoły.

[59] Praktyczna prezentacja gotowych rozwiązań z zakresu ochrony wojsk odbyła się na poligonie w Unterluss w Dolnej Saksonii 27-29 września 2005.

NATO (NRF), w takim otoczeniu staną się w niedalekiej przyszłości codziennością militarną[60].

Korporacja Rheinmetall pragnęła wykazać zarówno wojskowym jak i cywilnym decydentom, że armia powinna być przygotowana na zagrożenia asymetryczne i już teraz dysponować połączonymi w jednorodny układ - systemami skutecznej ochrony wojsk wysłanych do zdecydowanie wrogiego środowiska[61].

Do realizacji projektu ochrony wojsk własnych przed oddziaływaniem asymetrycznym wykorzystano sprzęt budowany czasem z myślą o zupełnie innym zastosowaniu militarnym. Przyjmując założenie, iż potencjalne ataki asymetryczne będą prowadzone z wykorzystaniem różnych środków walki zaplanowano ich zwalczanie odmiennymi metodami dążąc do minimalizacji strat własnych. Na przykład dwudziałową, zdalnie kierowaną baterię *Sky-shield* szybkostrzelnych 35-mm armat szwajcarskiego *Oerlikon Contraves*, wyrzucających pociski *Ahead* (z programowanym punktem rozprysku), zastosowano z powodzeniem do zwalczania odpalonych w stronę obiektu wojskowego granatów moździerzowych. Takie ataki są przecież dniem powszednim walk asymetrycznych w Iraku i Afganistanie. W ten sposób granaty przeciwnika ęą)zaninolecą celu zostaną rozstrzelane przez pociski przeciwlotnicze z dala od ochranianego obiektu. Ze względu na zgromadzone w Iraku i Afganistanie doświadczenia w walce z terrorystami, armia amerykańska pod koniec 2004 rozpoczęła próby dział *Sky-shield* z amunicją *Ahead* w roli oręża do zwalczania ataków terrorystycznych RAM (*Rockets, Artillery shells and Mortar grenades*). Jest to kolejny dowód na to, że ochrona wojsk własnych stanowi istotny element budowy nowego systemu walki w środowisku zagrożeń asymetrycznych.

W ramach budowy nowego systemu ochrony do wykrywania ruchów potencjalnych terrorystów wykorzystano powszechnie stosowaną optoelektroniczną głowicę optoelektroniczną zainstalowaną na wieży obserwacyjnej. Produkt ten instalowany jest na wozach rozpoznawczych Fennek[62].

W działaniach asymetrycznych szczególnego znaczenia nabiera zwalczanie snajperów. Dla ochrony wojsk wykonujących zadania w rejonach zagrożonych działaniem snajperów opracowano *Sniper Locating System*, czyli laserowy przyrząd do lokalizacji snajperów w dzień i w nocy. W przeciwieństwie do dotychczas opracowanych urządzeń tego

---

[60] Zob. W. Łuczak, *Pod parasolem Rheinmetalla*, Raport WTO-11/05.

[61] Program w zakresie ochrony wojsk został umownie nazwany w ramach NATO - Protective Shield (tarcza ochronna).

[62] Zakupiony w Polsce egzemplarz głowicy elektronooptycznej wykorzystano w prototypie siemianowickiego Żbika-A (nowa wersja BRDM).

typu jest on lekki, poręczny i praktyczny. Urządzenie potrafi wskazać strzelca dysponującego lunetą snajperską na karabinie, jeszcze zanim otworzy on ogień. Działanie sytemu oparto na identyfikacji przyrządów obserwacyjnych. Według opinii konstruktorów po założeniu baterii i wciśnięciu przycisku, który wysyła promień lasera przeszukującego okolicę, w wizjerze ukazuje się czerwona jaskrawa plamka sygnalizująca lokalizację ukrytego pod drzewem karabinu snajperskiego z lunetą celowniczą. Należy wskazać na fakt, że SLS jest skuteczny także na duży dystans. Maksymalny zasięg wykrycia snajpera nie został ujawniony[63]. Zgromadzone informacje wskazują, że pomysł jest dziełem jednego z rosyjskich ośrodków optoelektronicznych, od którego odkupiono patent i prawa do produkcji. SLS został już zakupiony od Rheinmetall Waffe Munition dla służb specjalnych i wojska RFN, a nowym posiadaczem urządzenia są także Holendrzy.

Do bezpośredniej ochrony obiektów wojskowych w działaniach asymetrycznych opracowano przewoźny, dostosowany do transportu drogą powietrzną (również pod kadłubem ciężkich śmigłowców) kontener - wartownię, kryjący zautomatyzowany układ kontroli osób wchodzących na teren obiektu (weryfikacja do 400 osób na godzinę). Trzy równoległe kanały automatycznego sprawdzania i weryfikacji tożsamości osób pracują, bazując na skanerach danych biometrycznych, porównujących dane wchodzących z tymi zapisanymi w pamięci, udzielając dostępu, lub blokując osoby negatywnie zweryfikowane między drzwiami wewnętrznymi i zewnętrznymi (w opancerzonym, izolowanym pomieszczeniu). Całość operacji wejściowych nadzoruje tylko jeden strażnik w chronionym przed napadem i zabezpieczonym przed eksplozją zamachowca-samobójcy pokoju kontenera. Przewiduje się także wykorzystanie mobilnego kontenera bezpieczeństwa dostępu w zniszczonych na obszarze operacji regionalnych portach lotniczych. Ponadto mobilne kontenery kontroli osób mogą być wypożyczane w czasie świąt religijnych, podczas organizacji imprez masowych a także na posterunkach kontrolnych.

Nowym kierunkiem ochrony baz i obiektów militarnych w działaniach asymetrycznych są roboty rozpoznawcze, pełzające i latające, tworząc kolekcję robotów różnej wielkości i przeznaczenia (mikroroboty). Wiele armii poszukuje perspektywicznych środków bezpilotowych dla typowego plutonu bojowego i samodzielnych opancerzonych wozów rozpoznawczych. Jak wskazują zgromadzone doświadczenia zrezygnowano z dotychczasowych ciężkich koncepcji startujących z kontenera na ciężarówce bezpilotowych samolotów rozpoznawczych na rzecz lekkich przenośnych zestawów. Dlatego obecnie

[63] Przyrząd zdał praktyczny egzamin podczas operacji osłony wizyty Ojca Świętego Benedykta XVI w Kolonii w 2005 roku.

organizuje się w wielu armiach samodzielne pododdziały zdalnie sterowanych urządzeń rozpoznawczych działających nie tylko w powietrzu.

W działaniach asymetrycznych do operacji w terenie zurbanizowanym (np.: patrolowanie, nadzorowanie, poszukiwanie) wykorzystany będzie prosty, odporny na błędy obsługi, napędzany wydajnymi mikrosilnikami elektrycznymi, startujący pionowo bezpilotowiec wyposażony w czujniki optoelektroniczne i akustyczne. Przewiduje się, że ma go przenosić i obsługiwać tylko jeden żołnierz (z pulpitem i ekranem). Projektowany zasięg do 10 km, a masa użyteczna około 5 kg.

Z różnych źródeł można wnioskować, że aktualnie w armiach technologicznie zaawansowanych państw prowadzone są badania nad wykorzystaniem broni laserowej do oddziaływania (oślepiania) na rakiety, bomby naprowadzane laserowo, urządzenia rozpoznawcze, dalmierze laserowe,. celowniki nocne czy zapalniki laserowe. W dalszej perspektywie można spodziewać się zastosowania laserów montowanych na samolotach, lub w rakietach zdalnie kierowanych do zwalczania celów na dużych wysokościach w celu niszczenia międzykontynentalnych rakiet balistycznych. Ta sama broń, montowana na pojazdach naziemnych, będzie mogła skutecznie uszkadzać wyposażenie broni pancernej, aparatów latających i innych systemów uzbrojenia przeciwnika, wykorzystujących elektronikę.

W rozważaniach prowadzonych nad systemami ochrony i obrony przeznaczonych do działań asymetrycznych nie należy zapominać o wyposażeniu żołnierza. Nowy ubiór bojowy w opinii konstruktorów składał się będzie z trzech warstw. Warstwa zewnętrzna będzie zbudowana z lekkich, tak zwanych inteligentnych materiałów, które, jak kameleon, będą miały możliwość zmiany kolorów w zależności od środowiska. Nowy, ognioodporny uniform dla komfortu termicznego noszącego będzie przepuszczał powietrze,. Zapewniając przy tym pełną ochronę przed zagrożeniami chemicznymi lub biologicznymi, z możliwością sygnalizacji żołnierzowi obecność toksycznych związków chemicznych. Warstwa środkowa nowego munduru-pancerza, wykonana zostanie z materiałów przewodzących prąd elektryczny, aby dostarczyć energię do innych podsystemów. Stanowić będzie także tarczę redukującą lub eliminującą poświatę elektromagnetyczną emitowaną przez elektryczne komponenty wojownika przyszłości - to znaczy w zamyśle konstruktorów zapewniał będzie żołnierzowi w pewnym stopniu poziom niewidzialności. Warstwa wewnętrzna, określana jako warstwa krytyczna dla życia, zawierać będzie czujniki indywidualne, aby monitorować stan zdrowia żołnierza, a także poziom stresu i senność. Przewiduje się, że podsystem mikroklimatyczny nowego munduru dostarczał będzie energii do ogrzewania żołnierza

w czasie chłodnej pogody i zapewni wentylację w warunkach tropikalnych. Podsystem zasilania i magazynowania energii stanowić ma w projekcie baterię zasilającą o małej wadze, która mogłaby dostarczać żołnierzowi energię na okres do sześciu dni samodzielnego działania[64]. Według niektórych ekspertów wojskowych, koncepcja ta jest naprawdę rewolucyjna, potencjalnie czyniąc żołnierza znacznie lepiej chronionym. Sądzą oni również, że stanowi to technologiczny skok skuteczności żołnierza przyszłości w porównaniu z żołnierzem dnia dzisiejszego.

Przedstawione ogólne informacje na temat budowy w ramach systemów broni obezwładniającej programów skierowanych na bezpieczeństwo wojsk w działaniach asymetrycznych wskazują, że obok opracowania sposobów bezpośredniego oddziaływania na nieokreślonego przeciwnika dąży się do zabezpieczenia wojsk własnych. Konstruktorzy wojskowych i cywilnych ośrodków badawczych w różny sposób podejmują próby zabezpieczenia żołnierzy przed potencjalnym zagrożeniem asymetrycznym w rejonie konfliktu.

[64] Na potrzeby działań militarnych może być wykorzystywana żelowa bateria wykonana przez japońską firmę NEC. Ogniwo wykonane jest ze specjalnego plastiku w żelu i ma niecały milimetr grubości (*Żelowa bateria*, Newsweek z dn. 15.01.2006, s.75).

3. ROZPOZNANIE W TYŁOWEJ STREFIE DZIAŁANIA WOJSK

Analiza założeń teoretycznych, wnioski z praktyki szkoleniowej oraz doświadczenia z wojen i konfliktów lokalnych potwierdzają tezę, że właściwie prowadzone rozpoznanie w tyłowej strefie działania wojsk decyduje o bezpieczeństwie własnych wojsk, utrzymaniu ich swobody działania oraz zabezpieczeniu ciągłości dowodzenia i zaopatrywania logistycznego.

Celem rozdziału jest zaprezentowanie wyników badań z zakresu prowadzenia rozpoznania w tyłowej strefie działania wojsk.

Wysiłek zespołu badawczego ukierunkowany został na zidentyfikowanie działań asymetrycznych w tyłowej strefie działania wojsk oraz prowadzenia działalności rozpoznawczej, mającej na celu zdobycie i dostarczenie informacji niezbędnych dla zapewnienia bezpieczeństwa własnym wojskom, utrzymaniu ich swobody działania oraz zabezpieczeniu ciągłości dowodzenia i zaopatrywania logistycznego.

Zespół autorski założył, że „rozpoznanie" (czyli działalność rozpoznawcza która będzie przedmiotem rozważań w tym rozdziale) to działania podejmowane w celu pozyskania - w drodze obserwacji wzrokowej lub innymi metodami wykrywania - informacji o działaniach i środkach przeciwnika lub potencjalnego przeciwnika, albo danych meteorologicznych, hydrograficznych lub geograficznych określonego obszaru[1], jakim jest tyłowa strefa działania wojsk.

Trudno jest odnaleźć w dokumentach normatywnych a także w literaturze naukowej i fachowej jednoznacznej definicji „tyłowej strefy działania wojsk". W wielu publikacjach normatywnych „tyłowa strefa[2]" jest utożsamiana ze „strefą tyłów[3]".

Ponadto, określenia te są używane zamiennie np. „rejon (strefa) tyłów", „strefa tyłowa", „tylna strefa działań bojowych" lub też „działania w strefie tyłowej" spotyka się również nazwy „działania tyłowe"[4].

---

[1] Por. AAP-6(2005) *Słownik terminów i definicji NATO.*
[2] Zob. *Regulamin Działań Wojsk Lądowych* (DD/3.2), Szkol 809/ 2006, Warszawa 2006 pkt. 3016/2.
[3] Zob. *Regulamin Działań Wojsk Lądowych* (DD/3.2), Szkol 809/ 2006, Warszawa 2006 pkt. 6007 i 6008
[4] Zob. AAP-6(2005) *Słownik terminów i definicji NATO.* Zob. *Regulamin Działań Wojsk Lądowych* (DD/3.2), Szkol 809/ 2006, Warszawa 2006 pkt. 3010/3, 3016/4 i 5005/3.

W Słowniku terminów i definicji NATO AAP-6, „obszar/strefa tyłów" definiowany jest jako, „...obszar (dla dowolnego szczebla dowodzenia) rozciągający się w przód od jego tylnej granicy do tyłu obszaru odpowiedzialności następnego, niższego szczebla dowodzenia. Obszar ten przeznaczony jest głównie do wykonywania funkcji zabezpieczenia działań bojowych"[5]. Natomiast w „Doktrynie Narodowej – Operacje Połączone" (OP/01) - która ma ujednolicać stosowaną terminologię (dotyczy to zwłaszcza używanych polskich odpowiedników angielskich zwrotów)[6] – „strefa tyłowa" jest definiowana jako „...wyznaczony przez dowódcę obszar przeznaczony do rozmieszczenia urządzeń i instalacji logistycznych oraz jednostek wsparcia bojowego i logistycznego"[7].

W „Doktrynie prowadzenia operacji połączonych DD/3" znajdujemy inne pojęcie które brzmi: „połączony obszar tyłowy"[8], wynika to ze stwierdzenia, że „...podczas organizacji struktury dowodzenia i kierowania można także ustalić Obszar Operacyjny dowódcy Połączonego Obszaru Tyłowego (Joint Rear Area – JRA)", jednak brak jest definicji tego pojęcia.

Jeszcze z większą gamą definicji i pojęć spotykamy się w Regulaminie Działań Wojsk Lądowych (DD/3.2). Na przykład: w słowniku definicji „Obszar /strefa tyłów" definiowany jest jako „...Obszar/strefa tyłów (*rear operations area*) - obszar, w którym działania wymierzone są na:

1. Utrzymanie swobody działania sił własnych przewidywanych do działania w strefie działań bezpośrednich lub głębokich;
2. Zabezpieczenie ciągłości dowodzenia i zaopatrywania logistycznego.

Granicę przednią strefy tyłowej wyznacza tylna granica strefy działań bezpośrednich. Tylnia granica obszaru odpowiedzialności obronnej stanowi jednocześnie tylną granicę strefy tyłowej". Natomiast w punkcie 3016 „strefa tyłowa" jest definiowana jako „obszar rozpoczynający się od tylnej granicy (określonego szczebla dowódcy) do tylnej granicy obszaru odpowiedzialności dowódcy niższego szczebla. Obszar jest wyznaczany głównie dla określenia funkcji zabezpieczenia logistycznego", w innych rozdziałach regulaminu „obszar/strefa" definiowane są wg własnej inicjatywy piszącego rozdział czy też podrozdział.

---

[5] AAP-6(2005) Słownik terminów i definicji NATO.
[6] Zob. *Doktryna Narodowa – Operacje Połączone (OP/01)*, Szkol.800/2002. Warszawa 2002, wstęp.
[7] Por. tamże, str.7-8.
[8] *Doktryna Prowadzenia Operacji Połączonych DD/3*, Warszawa 2003 pkt. 427.

Z powodu bardzo dużej rozbieżności w definiowaniu tego pojęcia do dalszych badań zespół autorski przyjął definicję „obszaru/strefy tyłowej" zgodną ze słownikiem terminów i definicji NATO, która znajduje się również w Regulaminie Działań Wojsk Lądowych (DD/3.2) w rozdziale „Słownik".

Wynika z niej jednoznaczne stwierdzenie, że „tyłowy obszar/strefa działań" jest jednym z celów działań głębokich przeciwnika. Przeciwnik może w nim zastosować szeroki wachlarz środków niszczących, uszkadzających lub zakłócających działanie określonych elementów infrastruktury. Celem takich działań (działań asymetrycznych) może być przerwanie funkcjonowania służb wsparcia, przerwanie linii komunikacyjnych, izolacja głównego obszaru działań od zgromadzonych zasobów logistycznych a także pozbawienie dowódcy bezpiecznie i efektywnie funkcjonującego, zaplecza zabezpieczającego prowadzone działania. Prawdopodobnymi obiektami uderzeń mogą być: wojska, systemy transportu (kolej, porty morskie, kanały, lotniska, mosty itd.), urządzenia logistyczne (stacje MPS, rurociągi, składy materiałowe), elektrownie (w tym atomowe), fabryki, stacje łączności itp..

Przedstawione fakty skłaniają do wniosku, że istnieje konieczność rozlokowania sił zapewniających bezpieczeństwo tego rejonu oraz prowadzących działania rozpoznawcze w strefie tyłowej - mające na celu zdobycie i dostarczenie wartościowych informacji niezbędnych dla zapewnienia bezpieczeństwa własnych wojsk.

Do rozstrzygnięcia pozostają jeszcze jeden element: kto dowodzi w tyłowej strefie wojsk? Zgodnie z regulaminem DD/3.2 odpowiedzialność za bezpieczeństwo strefy tyłowej w swoich obszarach działania posiadają dowódcy sojuszniczy/koalicyjni i narodowi, natomiast dowodzenie - planowanie działań w strefie tyłowej powinno być realizowane na głównym stanowisku dowodzenia a uprawnienia do kontroli strefy tyłowej mogą być przekazane dowódcy tyłowego stanowiska dowodzenia[9].

3.1 Rozpoznanie zagrożeń terrorystycznych

Terroryzm to bez wątpienia jeden z najpoważniejszych problemów bezpieczeństwa w tyłowej strefie działań. Zjawisko to charakteryzuje się zaskoczeniem, szybkością i niezwykłą skutecznością zarówno, co do celu ataku jak i skutków tego ataku.

[9] Zob. Regulamin Działań Wojsk Lądowych (DD/3.2), Szkol 809/ 2006, Warszawa 2006 pkt. 3016/4f.

Zasadniczym problem w określeniu pojęcia „terroryzmu"[10] jest mnogość definicji, które zdaniem wielu autorów posiadają istotne braki eksplanacyjne. Tak duża liczba definicji[11] prowadzi do chaosu terminologicznego, który zdecydowanie utrudnia właściwe postrzeganie tego zjawiska. Naszym zdaniem, sytuacja ta spowodowana jest kilkoma czynnikami. Po pierwsze, niewątpliwym problemem jest niezwykła dynamiczność i złożoność tego zjawiska, które ciągle ewoluuje, zmienia się i przybiera coraz to nowe oblicza[12]. Drugim problemem uniemożliwiającym jednoznaczne zdefiniowanie terroryzmu jest kwestia motywacji terrorystów[13]. Trzecim utrudnieniem w stworzeniu uniwersalnej definicji terroryzmu jest ambiwalencja informacyjna. Ambiwalencja informacyjna to z jednej strony ograniczony dostęp do informacji na temat funkcjonowania organizacji terrorystycznych, z drugiej zaś ogromny zalew informacji, często o charakterze propagandowym na temat ich działania. Jeśli chodzi o pierwszą kwestie mamy wyraźny problem z zapoznaniem się z funkcjonowaniem organizacji terrorystycznych. Ponieważ, są to grupy szczelne, często jednorodne, nie posiadające swojego terytorium, poruszające się zazwyczaj po niedostępnych terenach. Jedyne informacje, w których możemy cokolwiek znaleźć, pochodzą z danych zgromadzonych przez wywiad i rozpoznanie osobowe. Są to bardzo często jednak informacje niepełne, mało wiarygodne i oparte jedynie na przypuszczeniach ekspertów, polityków i agentów rozpoznania. Doskonałym przykładem - na potwierdzenie tej tezy - są sprzeczne wiadomości o losie Osamy bin Ladena.

Powyższe uwarunkowania potwierdzają tezę o trudnościach we właściwym określeniu problemu terroryzmu. Poniżej dokonamy analizy kilku definicji tego

---

[10] Działania terrorystyczne. „*Słownik języka polskiego*" definiuje terror jako „stosowanie przemocy, gwałtu, okrucieństwa w celu zastraszenia, zniszczenia przeciwnika". Pojęcie „terroryzm" jest przedstawione jako „stosowanie terroru, zwłaszcza działalność niektórych ugrupowań ekstremistycznych, usiłujących za pomocą zabójstw politycznych, porwań zakładników, uprowadzenia samolotów i podobnych środków zwrócić uwagą opinii publicznej na wysuwane przez siebie hasła lub wymusić na rządach państw określone ustępstwa bądź świadczenia na swoją korzyść" lub „stosowanie gwałtu do osiągnięcia celów politycznych lub ekonomicznych w stosunkach międzynarodowych. Forma interwencji dokonywanej przemocą przez specjalne oddziały wojskowe lub policyjne, przez organizacje terrorystyczne". Celem działań terrorystycznych jest podstępne działanie, wymierzone przeciwko władzy administracyjnej lub politycznej w celu zastraszenia, wywołania paniki, niepewności i niezadowolenia wśród wojsk oraz ludności cywilnej przeciwnika. W działaniach terrorystycznych będą wykonywane następujące zadania: dokonywanie zamachów bombowych, fizyczna likwidacja osób, porywanie i przetrzymywanie zakładników. Ze względu na rozmiar oddziaływania może być stosowany terror indywidualny lub zbiorowy (masowy). Terroryzm może przybrać formę nacisku religijnego lub ideologicznego (Słownik języka polskiego, PWN, Warszawa 1992, s. 498; J. E. Osmańczyk: Encyklopedia spraw międzynarodowych i ONZ. Warszawa 1974, s. 3509/.

[11] Zob. K. Jałoszyński, *Koncepcja współczesnych działań antyterrorystycznych*, AON, Warszawa 2003 s.58.

[12] Zob. tamże s.54-75.

[13] Tamże.

zjawiska, której celem będzie przedstawienie konstruktywnej krytyki i wskazanie na ich istotne braki. Według Encyklopedii ONZ[14] „terroryzm" to stosowanie gwałtu dla osiągnięcia celów politycznych lub ekonomicznych w stosunkach międzynarodowych. Definicja ta ma charakter lakoniczny, nie wskazuje podmiotów, które mogłyby się stać celami ataku, ani motywów kierujących terrorystami. Nieco bardziej problem ten rozszerza definicja Departamentu Obrony USA, która wskazuje, że „terroryzm to przemyślane użycie przemocy lub zagrożenia w celu wywołania strachu, przemyślane wymuszenie lub zastraszenie rządów i społeczeństw w celu nacisku politycznego, ideologicznego lub religijnego"[15]. Autorzy trafnie wskazali na celowość aktu terrorystycznego, nie uwzględniając jednak motywów ataku terrorystycznego. Inne podejście zaprezentowała Komisja Europejska stwierdzając, że „terroryzm to wszelkie celowe akty popełnione przez pojedyncze osoby lub organizacje przeciwko jednemu lub kilku państwom, ich instytucjom lub ludności w celu zastraszenia oraz poważnego osłabienia lub zniszczenia struktury politycznej, gospodarczej i społecznej kraju"[16]. I również tutaj nie znajdziemy czynnika motywującego atak terrorystyczny. Co więcej Komisja Europejska – naszym zdaniem - niesłusznie zaklasyfikowała do aktów terrorystycznych czyny dokonane przez pojedyncze osoby, myląc - tym samym - terroryzm z aktami o charakterze kryminalnym. Tak sformułowana definicja miałaby oczywiście sens jedynie wtedy, gdy takie osoby byłyby powiązane z organizacjami terrorystycznymi, jednak takiego ujęcia problemu w niej nie znajdujemy. Bardzo ważną definicją, którą często można znaleźć w literaturze przedmiotu jest definicja Departamentu Stanu USA. Według niej „terroryzm to celowe, polityczne motywowane użycie przemocy przeciw celom niewojskowym, skierowane na wywołanie wpływu na opinie społeczną". Definicja ta zwraca uwagę na celowość i motywy aktu terrorystycznego oraz na jego fakt wywarcia wpływu na opinie publiczną. Niestety i ona jest obarczona błędami. Głównym zarzutem jest tu zwrócenie uwagi na polityczne motywy terroryzmu, co pozwala na bardzo szeroką interpretacje. Pewien chaos wprowadza też określenie „cele nie walczące" znajdujące się w przypisie do tej definicji. Spośród polskich badaczy ciekawe ujęcie zaprezentował B. Bolechów[17], według którego „...terroryzm to forma przemocy politycznej polegająca na stosowaniu

---

[14] E. Osmańczyk, *Encyklopedia ONZ i stosunków międzynarodowych*, Warszawa 1986, s. 125.
[15] Department of State, 2003 *Pattern of Global Terrorism*, April 2004, rozdział Introduction, punkt Definitions
[16] W. Laqueur, *The New Terrorism. Fanaticism and the Arms of Mass Destruction*, London 2001, s. 46.
[17] B. Bolechów, *Terroryzm w świecie podwubiegunowym*, Toruń 2002, s. 87.

morderstw lub zniszczenia w celu wywołania szoku i ekstremalnego zastraszenia jednostek, grup, społeczeństw lub rządów, czego efektem mają być wymuszenia pożądanych ustępstw politycznych, sprowokowanie nieprzemyślanych działań i/lub zademonstrowanie/nagłośnienie własnych politycznych przekonań".

Rozwiązanie problemu właściwego zdefiniowania zjawiska terroryzmu – a do tego jeszcze występującego w tyłowej strefie działań - jest z jednej strony, kluczowe a z drugiej raczej niemożliwe. Prawidłowa i powszechnie obowiązująca definicja terroryzmu i jej stosowanie w stosunkach międzynarodowych znacznie ułatwiłaby rozwiązanie wielu występujących problemów. Niestety zjawisko terroryzmu jest tak bardzo rozmyte, niejednorodne i nieprzewidywalne, że obiektywne zdefiniowanie go jest praktyczne niemożliwe. Co więcej, państwa z zapałem konstruują własne definicje po to by rozwiązać własne problemy polityczne. Taka sytuacja dodatkowo uniemożliwia stworzenie definicji terroryzmu.

Jak można zauważyć powyższe definicje mają w głównej mierze charakter tendencyjny ułatwiający szerokie interpretowanie tego problemu. Jednym z celów tej pracy jest podejście do kwestii terroryzmu realizowanego w tyłowej strefie działań wojsk w sposób maksymalnie obiektywny w związku z czym zespół autorski zdecydował się na stworzenie własnej definicji terroryzmu realizowanego w tyłowej strefie działania wojsk.

Naszym zdaniem: „terroryzm to metoda walki o różnym stopniu zorganizowania charakteryzująca się nieregularnymi atakami na obiekty i struktury cywilne i/lub na instalacje wojskowe powodowana motywami kulturowo-ideologicznymi, której celem jest wywołanie szoku oraz uzyskanie zamierzonych korzyści".

W definicja tej zespół autorski zwraca uwagę na kilka istotnych elementów wyróżniających terroryzm.

Są to:

- działalność o różnym stopniu zorganizowania - co przejawia się tym, że organizacje terrorystyczne mają w różnym stopniu rozbudowane struktury;
- nieregularne ataki - cecha ta pozwala odróżnić działania terrorystyczne od regularnego konfliktu zbrojnego lub wojny;
- motywy kulturowo-ideologiczne - element ten pozwala odróżnić terrorystów od osób prowadzących działalność narodowo-wyzwoleńczą.

(Przez motywy kulturowo-ideologiczne rozumiemy m.in. takie czynniki jak: religijny, etniczny, rasowy, ideologiczny, światopoglądowy);

- wywołanie szoku na opinii publicznej - większość ataków jest nastawiona na wywołanie szoku w społeczeństwie celem wywarcia presji na decydentów politycznych, co pozwala na uzyskanie korzystnych decyzji.

Na podstawie dostępnych materiałów zespół autorski ocenił, że istnieją dwa podstawowe podejścia w zwalczaniu terroryzmu - reaktywne i proaktywne. Zgodnie z reaktywnym podejściem oczekuje się na zamach terrorystyczny i liczy się na to, iż będzie się w stanie, w miarę rozwoju wydarzeń ograniczyć straty w ludziach i rozmiarze zniszczeń. Wadą tego podejścia jest to, iż działa się już po ataku, gdy straty zostały poniesione.

Inna opcją jest podejście proaktywne. Według niego można przewidywać nadchodzące zamachy terrorystyczne i dobrze przygotowywać się na nie. Wynika z tego, ze działanie proaktywne zwiększa prawdopodobieństwo zapobiegania atakom terrorystycznym i umożliwia uniknięcie zarówno strat w ludziach, jak i szkód dotyczących mienia. Dotychczasowe doświadczenia wskazują, że proaktywne podejście do terroryzmu jest lepszą z dwóch opcji. Zapewnia skuteczniejszy sposób prewencji zamachów terrorystycznych. Dzięki temu możemy zminimalizować możliwe straty.

Spójrzmy zatem na ten problem z punktu widzenia rozpoznania działalności terrorystycznej prowadzonej w tyłowej strefie działań, która ściśle łączy się ze zwalczaniem terroryzmu.

Rozpoznanie, jest narzędziem, które umożliwi zbadanie otoczenia w celu ujawnienia i ustalenia potencjalnych aktywności terrorystycznych - skierowanych przeciwko bezpieczeństwu naszych wojsk. Ponadto, pozwali na określenie własnych słabości i potencjalnych celi dla terrorystów. Proces planowania działań antyterrorystycznych wyznaczy nam również punkt wyjścia dla określania problemów z jakimi będziemy się zmagali. Mimo wszystko, wiele razy może zdarzać się, iż to, co uznajemy za problem, w rzeczywistości jest tylko symptomem prawdziwego problemu, nie jest więc też przyczyną zaistniałej sytuacji. Musimy więc zbierać wszelkie informacje, potencjalnie związane z problemem i poprawnie zanalizować, aż do momentu, w którym jesteśmy pewni z czym dokładnie mamy do czynienia.

W odniesieniu do całego problemu, rozpoznanie możemy zdefiniować jako proces zbierania i pozyskiwania informacji, które posłużą do przeanalizowania i zidentyfikowania potencjalnych działań i aktywności terrorystycznych, a także

możliwych celów zamachów oraz słabych punktów w tyłowej strefie działań wojsk. Rozpoznanie będzie głównym krokiem w przeciwdziałaniu terroryzmowi, ponieważ posiadanie informacji o nadchodzącym niebezpieczeństwie będą kluczowe dla przeciwdziałania.

Powyższe rozważania prowadzą – szczególnie w tyłowej strefie działania wojsk - do postawienia tezy, że główne funkcje w rozpoznaniu terroryzmu to: zbieranie-pozyskiwanie informacji oraz ich klasyfikację-porządkowanie w celach analizy.

W zbieraniu informacji należy wyartykułować cztery najistotniejsze cele nadające sens zbieraniu i pozyskiwaniu informacji to (tzw. 4xD):

1. Powstrzymanie (*Deter*) przed wydarzeniem zamachu terrorystycznego – (sposób proaktywny);
2. Wykrycie i rozpoznanie (*Detect*) aktywności terrorystycznej i planowanych zamachów (sposób proaktywny);
3. Obrona (*Defend*) żołnierzy oraz infrastruktury wojskowej, wojskowo-cywilnej, cywilnej przed zamachem terrorystycznym (sposób reaktywny) ;
4. Pokonanie i uniemożliwienie działania w przyszłości (*Defeat*) terrorystom, którzy już zaatakowali (sposób reaktywny).

Cele 1 oraz 2 skupiają się głównie na zewnętrznych działaniach terrorystycznych. Cele numer 3 oraz 4 skupiają się bardziej na wewnętrznym aspekcie, czyli tym jak jesteśmy przygotowani i jak możemy zareagować w momencie ataku terrorystycznego. Zbierane informacje muszą odnosić się do co najmniej jednego z tych czterech celów. Jeżeli tak nie jest, należy uznać informację za niezwiązaną z problemem.

Ostatecznym zadaniem procesu zbierania informacji powinno być wspieranie procesu planowania działań antyterrorystycznych w fazie analizowania danych. Aby spełnić to zadanie każda informacja musi zostać odpowiednio sklasyfikowana od razu po uzyskaniu. Podstawowe porządkowanie informacji polegać powinno na ocenie wiarygodności i przydatności (wartości) informacji, które mają być analizowane. Każda poszczególna informacja powinna być opisana i zapisana w odpowiednim dokumencie – bazie danych lub rejestrze.

Analizowanie informacji polegało więc będzie, między innymi, na łączeniu różnych elementów i danych razem, tak, aby wskazywały słabości terrorystów. W zaawansowanej analizie powinno się opisać konkretne instytucje finansowe, powiązania rodzinne, kontakty i znajomości, użycie pojazdów, sposoby działania,

kluczowe lokacje oraz miejsca przebywania osób podejrzanych o działalność terrorystyczną. Wspomniane łączenie danych polegać powinno na rozpatrywaniu wszystkich symptomów i części składowych problemu pod kątem wyróżnienia wspólnej istoty, tzw. „rdzenia"(core). „Rdzeń" może sprowadzać się do określonego typu zagrożenia terrorystycznego lub braku możliwości reagowania w przypadku zamachu terrorystycznego z użyciem istniejącego systemu bezpieczeństwa. Może odnosić się też do obu wymienionych kwestii.

Pozyskiwanie informacji o grupach terrorystycznych może odbywać się przede wszystkim poprzez rozpoznanie osobowe (HUMINT). Nie wymaga ono dużych nakładów finansowych, ani zaawansowanego sprzętu. Rozpoznanie osobowe powinno być przeprowadzane w podobny sposób, jak w działaniach militarnych. Ograniczone rozmiary tej pracy uniemożliwiają przedstawienie tego zagadnienia w sposób wyczerpujący, dlatego też przedstawiamy podstawowe formy rozpoznania osobowego w rozpoznaniu terrorystów:

- prowadzenie obserwacji potencjalnych celów;
- werbowanie agentów (zbierających informacje oraz pomocniczych);
- przenikanie członków do interesujących ich miejsc (np. potencjalnych celów);
- prowadzenie działań kontrwywiadowczych (np. zabezpieczających przed obserwacją).

Natomiast, rozpoznanie poprzez środki techniczne będzie ograniczone przez możliwości w tyłowej strefie. Nie zawsze będziemy w stanie rozwinąć np. rozpoznania elektronicznego na dużą skalę, dlatego też powinniśmy stosować prostsze i łatwiej dostępne (co nie znaczy, że mniej skuteczne) metody. Metody te to m.in :

- umieszczanie urządzeń podsłuchowych w miejscach interesujących terrorystów (np. celu przyszłego ataku);
- podsłuchiwanie interesujących terrorystów sieci łączności (np. łączności komórkowej lub radiowej sił policyjnych);
- stosowanie włamań do systemów informatycznych (hacking) w celu pozyskania potrzebnych informacji.

Są to tylko niektóre z możliwych do zastosowania metod zbierania informacji. Należy jednak zakładać, że pomysłowość w tym zakresie musi być bardzo duża i powinna zaskakiwać terrorystów coraz to nowymi metodami pozyskiwania informacji.

3.2 Rozpoznanie w działaniach partyzanckich

Dokonując identyfikacji problemu rozpoznania w działaniach partyzanckich należy stwierdzić, że działania partyzanckie jako forma walki zbrojnej z okupantem nie znalazły miejsca w regulaminie działań taktycznych wojsk lądowych, oprócz definicji zamieszczonej w słowniku definicji[18]. Mimo wielu doświadczeń wyniesionych chociażby z okresu drugiej wojny światowej, problem działań partyzanckich nie znajduje większego zainteresowania we współczesnych doktrynach militarnych jak również rozważaniach teoretycznych W regulaminie działań taktycznych mowa jest jedynie o działaniach nieregularnych, które w dostępnych opracowaniach definiowane są bardzo różnie, niemniej jednak działanie partyzanckie można zakwalifikować jako formę działań nieregularnych prowadzoną na obszarze tyłowej strefy działań wojsk.

Aby zrozumieć istotę rozpoznania prowadzonego w działaniach partyzanckich koniecznym będzie uświadomienie sobie różnic pomiędzy partyzantem a terrorystą.

Zespół autorski uważa, że zasadniczą różnicą pomiędzy partyzantem a terrorystą jest cel działania. Dla partyzanta jest to walka z okupantem, który ma się bać bo najechał Jego kraj, natomiast dla terrorysty - masz się bać, nie ważne z jakiego powodu, ważne abyś czuł strach (i przy okazji było o nim głośno w mediach). Ponadto musimy sobie zdawać z tego sprawę, że pomiędzy terrorystą, a partyzantem jest bardzo cienka granica. A zależy to od punktu widzenia. Na przykład takie zamachy w Iraku, dla ludności negatywnie nastawionej do wojsk koalicji to partyzant, ale już dla przeciwników to terrorysta. Jest zasadnicza różnica w sformułowaniu: „konwój zaatakowali terroryści", a „konwój zaatakowali partyzanci". Tak samo jest i z atakami na iracki rząd[19]. Może to być „partyzantka przeciwko marionetkowemu rządowi", lub „terroryzm przeciwko suwerennym i niepodległym władzą". Zależy jak na to spojrzeć i czyją się trzyma stronę.

Na podstawie niektórych materiałów, można mieć wrażenie, że część autorów łączy definicję „partyzantki" z aspektami moralnymi - przyjmując, że „partyzant" to ktoś szlachetniejszy od „terrorysty" albo przynajmniej mniej okrutny. Tymczasem większość definicji „działań partyzanckich" - które można znaleźć w dokumentach normatywnych i artykułach specjalistycznych - nie łączy definicji z kwestiami

[18] Zob. *Regulamin Działań Wojsk Lądowych* (DD/3.2), Szkol 809/ 2006, Warszawa 2006, Słownik definicji

[19] Uzbrojeni mężczyźni, przebrani w policyjne mundury, porwali 14 listopada 2006 roku w Bagdadzie około 50 osób z budynku ministerstwa edukacji.

etycznymi - określenie „partyzantka" jest łączone wyłącznie z metodami walki, a nie z tym, czy walczący są „dobrzy" czy „źli".

Na potwierdzenie powyższej tezy, przytoczymy definicję z książki „Działania partyzanckie" Czesława Kurowskiego i Bernarda Woźnieckiego (wyd. MON 1975): „działania partyzanckie we współczesnym pojęciu, to specyficzna forma walki zbrojnej, wyrażająca się w zaskakujących i gwałtownych starciach zbrojnych, zasadzkach, napadach i najściach, aktach dywersji i sabotażu w połączeniu z akcjami psychologicznymi (w tym propagandowymi), w wywiadzie i kontrwywiadzie. Prowadzi się je z reguły na terytorium własnego kraju, zajętym przez przeciwnika (przy czym przeciwnikiem mogą być albo wojska okupanta, albo rodzimego reżimu), siłami rekrutującymi się spośród miejscowej ludności, lub też siłami oddziałów i pododdziałów wojsk regularnych, które wskutek rozbicia i okupacji kraju przez nieprzyjaciela są do tego zmuszone, ze względu na odcięcie od własnych głównych sił regularnych". Autorzy, ponadto wskazują na szereg ważnych cech partyzantki jako walki: - jedną z najważniejszych cech jest fakt, że przeciwnik na zajmowanym terytorium ma z reguły zdecydowaną przewagę liczebną w wojskach, uzbrojeniu i wyposażeniu (środki komunikacji i łączności) ma rozbudowany aparat administracji i bezpieczeństwa wewnętrznego, a często także dysponuje środkami przekazu (prasa, radio, telewizja), ponadto partyzantka to zdecydowanie zaczepny charakter walki (bowiem w obliczu przewagi przeciwnika partyzanci mogą liczyć na sukces tylko wtedy, kiedy sami wybiorą miejsce, czas i formę walki) z reguły żaden okupant, ani żaden rodzimy reżim nie jest w stanie kontrolować całego terytorium, ani w pełni chronić i bronić wszystkich obiektów i urządzeń o znaczeniu wojskowym, ekonomicznym, administracyjnym i politycznym.

Ponadto zaprezentujemy inne definicje które można znaleźć w kilku starszych opracowaniach np „Mała encyklopedia wojskowa", czy też „ Leksykon wiedzy wojskowej". Leksykon wiedzy wojskowej definiuje „działania partyzanckie" jako „...specyficzną formę walki zbrojnej wyrażająca się w zaskakujących, krótkotrwałych gwałtownych starciach zbrojnych, zasadzkach, napadach, aktach dywersji i sabotażu w połączeniu z psychologicznym oddziaływaniem; dz.p. prowadzi się z reguły na terytorium własnego kraju przeciwko okupantowi lub rodzimemu reżimowi siłami rekrutującymi się przede wszystkim spośród miejscowej ludności odpowiednio zorganizowanej i uzbrojonej. dz.p. mogą też uczestniczyć jednostki wojsk regularnych, które mimo rozbicia i okupacji kraju nie zaniechały walki nieprzyjacielem, niekiedy

również ochotnicy innych narodowości polityczni związani z działającymi jednostkami partyzanckimi[20]". W podobnym stylu skonstruowana jest definicja w Małej encyklopedii wojskowej.

Powyższe stwierdzenia pozwalają na sformułowanie ogólnej tezy, że zasadniczymi celami walki partyzanckiej jest zadanie przeciwnikowi strat w sile żywej, technice wojskowej, zakłócanie normalnej pracy administracji okupacyjnej oraz funkcjonowania gospodarki wytwarzającej na korzyść okupanta, oraz ochrona ludności przed represjami. W razie pomyślnego rozwoju walki tworzenie tzw. wyzwolonych obszarów, stanowiących lepszą bazę do organizacji sił własnych i zaopatrywania.

Nietrudno dostrzec, że w dotychczasowych rozważaniach najbardziej zbliżona systemem pojęciowym jest definicję z RDWLąd która brzmi: „działania partyzanckie (*guerilla warfare*) - działania wojskowe i paramilitarne prowadzone przez nieregularne, przeważnie miejscowe oddziały zbrojne na terenie zajętym przez przeciwnika lub wrogim".

W czasie prowadzenia rozpoznania w s:działaniachpartyzanckich, bardzo ważne znaczenie ma znajomość takich danych, jak: geografia, historia, demografia (w tym grupy narodowościowe), struktura rodzinna, poziom wykształcenia, warunki socjalno-bytowe ludności, organizacje społeczno - polityczne i religijne, struktura przemysłu, transportu, łączności, rolnictwa, stosunki ekonomiczne państwa, polityka wewnętrzna, siły zbrojne (regularne i wojska terytorialne), zakres i stan przygotowania sił zbrojnych do prowadzenia działań przeciwpartyzanckich, baza partyzancka itp.

Wymienione dane można uzyskać z ogólnie dostępnych źródeł, takich jak: prasa, periodyki, encyklopedie, itp. wydawnictwa. Większość z nich może być wykorzystana w zautomatyzowanym, systemie informatyki. Ponadto ważnym zagadnieniem jest systematyczne uzupełnianie i uaktualnianie tych danych.

Do podstawowych zadań organów rozpoznania należy przede wszystkim określenie i charakteryzowanie rejonów opanowanych przez partyzantów oraz tych wszystkich, które mogą stanowić dogodną bazę dla rozwoju ich działalności, jak również rozpoznanie nastrojów ludności. Na podstawie tych informacji można wytypować rejony, w których należy przeprowadzić akcje i określić przedsięwzięcia związane z polepszeniem warunków socjalnych i bytowych ludności.

---

[20] *Leksykon wiedzy wojskowej*, Wydawnictwo MON, Warszawa 1979, s. 103.

Kolejne ważne zadanie sprowadza się do ustalenia słabych punktów w systemie ruchu partyzanckiego. W celu osłabienia tego ruchu nieodzowne jest wprowadzenie racjonowania żywności, zorganizowanie punktów kontroli, kordonów policyjnych i przeczesywania. Natomiast w celu utrudnienia partyzantom kontaktu z ludnością należy stosować dodatkowe przedsięwzięcia, takie jak: przesiedlenie ludności do rejonów będących pod kontrolą rządu, blokowanie dróg, wprowadzanie godzin policyjnych i zarządzanie identyfikacji osób na podstawie obowiązujących dokumentów (dowody osobiste, przepustki itp.).

Z przeprowadzonych badań wynika, że organa rozpoznania powinny w czasie prowadzenia działań rozpoznawczych:

- lokalizować położenie sił partyzanckich;
- neutralizować grupy ludności zaangażowane w działaniach dywersyjnych, wywiadowczych lub sabotażowych;
- prowadzić działalność prewencyjną w celu uniemożliwienia partyzantom zdobywania potrzebnych informacji i przenikania do administracji rządowej;
- zdobywać niezbędne dane potrzebne do organizowania, planowania i prowadzenia operacji przeciwpartyzanckich;
- zdobywać dane umożliwiające realizację programu pacyfikacyjnego i sprawowanie kontroli nad ludnością i zasobami miejscowymi.

Jednocześnie, należy zwrócić uwagę, także na to że ludność cywilna, stanowi w zasadzie główną bazę wsparcia sił partyzanckich i jest w związku z tym potencjalnym źródłem informacji, ponieważ ma lub może mieć bezpośredni kontakt z partyzantami. Z tego wniosek, że ludność cywilna może dostarczać niezbędne informacje o:

- terenie i warunkach atmosferycznych;
- źródłach zaopatrzenia dostępnych dla sił partyzanckich;
- systemie zaopatrywania sił partyzanckich (drogi, ukrycia, składy, tunele itp.);
- prawdopodobnych celach i obiektach ataku sił partyzanckich;
- przypuszczalnych sympatykach i .współpracownikach sił partyzanckich;
- możliwości prowadzenia sabotażu, dywersji, działalności wywiadowczej itp.;
- słabych i wrażliwych miejscach przeciwnika.

W czasie prowadzenia działań rozpoznawczych organa rozpoznania osobowego powinny stosować takie metody i sposoby kontaktowania się z potencjalnymi informatorami, które umożliwiałyby zachowanie ścisłej tajemnicy i ich ochronę przed ewentualną groźbą likwidacji przez siły partyzanckie.

Należy zdawać sobie sprawę z tego, że zespoły mogą mieć problemy w prowadzeniu działalności wśród ludności tubylczej. Potencjalni agenci lub informatorzy mogą mieć z tego tytułu poważne korzyści materialne, ale w wypadku zwycięstwa sił partyzanckich ponieść z kolei bardzo wielkie straty. Baza werbunkowa może być stosunkowo łatwa do rozszyfrowania przez partyzantów, ponieważ większość agentów pracować będzie z pobudek materialnych a środki pieniężne przeznaczy często na zakup różnych towarów.

Natomiast zakładamy, że patrole rozpoznawcze będą spełniać w działaniach rozpoznawczych bardzo ważną rolę a patrolowanie będzie jednym z głównych zadań. Patrolowanie powinno być prowadzone intensywnie i w sposób ciągły przez małe i ruchliwe pododdziały, które wykorzystują pojazdy kołowe, śmigłowce, kutry patrolowe lub działają pieszo. Patrole muszą prowadzić działania zarówno w dzień jak i w nocy. W rejonach gęsto zaludnionych i na szlakach komunikacyjnych mogą organizować zasadzki, a na obszarach o mniejszym zaludnieniu prowadzić ciągłe patrolowanie. Patrolowanie, poza demonstracją siły, spełniać może ważną rolę w rozpoznawaniu terenu, nastrojów i ewentualnych zmian w poglądach ludności oraz zdobywaniu informacji o przeciwniku. Patrole muszą być wyposażone w niezawodne środki łączności radiowej, zestawy ładunków wybuchowych, które mogą być użyte do ewentualnego niszczenia urządzeń partyzanckich, środki sygnalizacyjne do wskazywania celów oraz oznaczania rejonów lądowania dla lotnictwa (śmigłowców).

W prowadzeniu działań partyzanckich ważnymi elementami są elektroniczne urządzenia wykrywające (czujniki) które powinny być w zasadzie przeznaczone do wykrywania obecności lub przemieszczania sił partyzanckich. Mogą one być bardzo przydatne w działaniach przeciwpartyzanckich. Samoloty rozpoznawcze, wyposażone w elektroniczne urządzenia rozpoznawcze (czujniki) powinny być wykorzystywane do rozpoznawania terenów opanowanych i patrolowych przez partyzantów, lecz z dala od rejonów gęsto zaludnionych. Za pomocą urządzeń elektronicznych (czujników) zrzucanych z samolotów można uzyskiwać szereg cennych informacji o partyzantach, a zwłaszcza o zmianach zachodzących w położeniu ich sił i kierunkach przemarszu.

Niektóre oznaki działalności partyzanckiej mogą być również źródłem informacji o prawdopodobnym celu i zamiarach sił partyzanckich. Dane powinny być zbierane przez komórkę rozpoznawczą, która przeprowadza ich szczegółową analizę. Na przykład następująca działalność partyzancka może oznaczać:

- stwierdzenie dużej ilości broni ciężkiej w niektórych jednostkach partyzanckich - przygotowywanie się do obrony;
- przeprowadzanie w ścisłej tajemnicy koncentracji środków o dużej manewrowości - przygotowywanie się do działań ofensywnych.

Systematyczne śledzenie i porównywanie wskazanych powyżej oznak umożliwia podjęcie na czas decyzji w sprawie odpowiednich przeciwdziałań.

Wnioski z analizy literatury i konfliktów zbrojnych wskazują, że partyzanci zbierają skrupulatnie wszelkie informacje, które odpowiednio zakodowane notują w dziennikach, notatnikach itp. Dokumenty te mogą stanowić ważne źródło informacji o siłach partyzanckich. dW: wyniku porównania tych danych z innymi można prognozować rozwój aktualnej sytuacji oraz przewidywać zamierzenia i plany działania sił partyzanckich. Ze względu na charakter działań partyzanckich a zwłaszcza ciągłą zmianę dyslokacji jednostek partyzanckich, szczególne znaczenie ma miejsce, data i okoliczności zdobycia dokumentów.

Bardzo ważną kwestią w rozpoznawaniu działalności partyzanckiej są przesłuchania które powinny być przeprowadzane przez personel zwerbowany spośród ludności miejscowej. Przy wertowaniu takiego personelu należy zwracać uwagę nie tylko na zdolności lingwistyczne, lecz także na uczciwość, prawdomówność i inteligencję. Większość działań partyzanckich ma charakter wojny domowej i dlatego też w wielu wypadkach będzie stosowana przemoc, co rzutować może w dużym stopniu na treść zdobywanych informacji lub wykluczać możliwość ich zdobycia. W tej sytuacji może mieć istotne znaczenie sposób i metoda przesłuchiwania jeńców i ludności cywilnej. W celu uzyskania niezbędnych informacji, powinno się ich traktować stanowczo, lecz w sposób humanitarny. Często stosowaną metodą potwierdzenia wiarygodności informacji uzyskanych od jeńców i ludności jest wykorzystanie partyzantów, którzy przeszli na współpracę z wojskami. Porównywanie informacji, uzyskanych w wyniku przesłuchań oraz danych zawartych w zdobytych dokumentach i innych materiałach, umożliwia oficerowi rozpoznania wyeliminowanie elementów dezinformacji.

Reasumując, należy stwierdzić, że każdy oficer rozpoznania powinien sobie zdawać sprawę z tego, że jest jednym z ważnych ogniw aparatu rozpoznania, w którym istotne znaczenie ma systematyczna wymiana informacji między poszczególnymi organami rozpoznania, od szczebla najniższego do najwyższego.

Zdarzające się przypadki niewłaściwej pracy organów rozpoznania spowodowane mogą być następującymi przyczynami:

- niesystematyczna i niesprawna selekcja informacji;
- wadliwa metoda przesłuchiwania jeńców;
- błędna ocena informacji uzyskanych z przesłuchań jeńców i ze zdobytych dokumentów;
- niewłaściwy system rozmieszczenia organów rozpoznania w terenie;
- przywiązywanie dużej wagi do działalności organów rozpoznania w okresie przygotowawczym do planowanej operacji i poświęcenie zbyt mało czasu (w ogóle) na analizę działalności rozpoznawczej po zakończeniu operacji; powoduje to w rezultacie brak ciągłości rozpoznania.

Powyższe rozważania pozwalają na ogólne stwierdzenie: do podstawowych przedsięwzięć związanych z rozpoznaniem w działaniach partyzanckich realizowanych w tyłowej strefie działania wojsk należy zaliczyć:

- dokładne sprawdzanie personelu cywilnego zatrudnionego w instytucjach cywilnych i wojskowych;
- stałą inwigilację osób podejrzanych o współpracę z siłami partyzanckimi;
- cenzurowanie lub zawieszenie działalności cywilnych urządzeń telekomunikacyjnych;
- w razie konieczności - wprowadzenie kontroli ruchu ludności;
- wprowadzenie kontroli osobistej personelu ochrony wszystkich obiektów rządowych i wojskowych;
- zapoznanie personelu wojskowego z wymaganiami bezpieczeństwa;
- paraliżowanie partyzanckiej działalności rozpoznawczej;

zabezpieczenie i kontrolę tajnych dokumentów, planów, rozkazów, meldunków itp.

Przedstawione uwarunkowania dotyczące rozpoznania działań partyzanckich i ich identyfikacji wskazują na rozmiar zadań rozpoznawczych. Niestety obserwacja działania i analiza możliwości rozpoznawczych systemu zdobywania informacji nie

pozwala na stwierdzenie, że obecne rozwiązania są wystarczające do działania w warunkach zagrożeń asymetrycznych.

3.3 Działania sił specjalnych

Ostatnie lata przyniosły gwałtowny wzrost zainteresowania problematyką wykorzystania wojsk specjalnego przeznaczenia w tyłowej strefie działania wojsk. Jest to spowodowane - między innymi - sukcesami, jakie pododdziały specjalne odniosły w prowadzonych konfliktach zbrojnych.

Złożoność pola walki, różnorodność i duży stopień trudności wykonywanych zadań powodują, że wymaga się pododdziałów specjalnie przygotowywanych do prowadzenia rozpoznania przeciwnika, torowania drogi siłom lądowym i powietrznym, opanowywania ważnych obiektów, dezorganizowania systemów łączności i dowodzenia itp. Zadania wykonywane przez tego typu pododdziały wykraczają coraz częściej poza ramy typowego pola walki. Zwalczanie terroryzmu i likwidacja przemysłu narkotykowego, to niektóre z nowych kierunków współczesnego zastosowania jednostek specjalnych.

W literaturze przedmiotu podkreśla się fakt, że pododdziały działań specjalnych są przeznaczone do wykonywania zadań o charakterze wojskowym i akcji specjalnych, tj. rozpoznawczych, dywersyjnych oraz terrorystycznych na tyłach i zapleczu przeciwnika. Specyfika i odmienność ich starannego doboru i szkolenia według odrębnego programu wynika z faktu, iż będą musieli prowadzić działania bezpośrednio w ugrupowaniu, a nawet głębokim zapleczu przeciwnika, w warunkach jego liczebnej i technicznej przewagi zazwyczaj w środowisku niesprzyjającym, przy całkowitym osamotnieniu, często bez możliwości uzyskania z zewnątrz natychmiastowej pomocy czy wsparcia.

Z przytoczonych informacji wynika przybliżony lecz możliwy obraz działań specjalnych. Zatrzymajmy się jednak nad definiowaniem: według gen. Tadeusza Pietrzaka: działania specjalne - to organizowane, prowadzone, inspirowane lub wspomagane przedsięwzięcia osłabiające potencjał polityczny, militarny, ekonomiczny i stan moralny przeciwnika, realizowane za pomocą odmiennej taktyki niż taktyka

wojsk regularnych, a wykonywane na terenie (tyłach) lub oddziałujące na teren (tyły) przeciwnika[21].

Natomiast „Regulamin działań taktycznych wojsk lądowych" określa je jako „...działania wojskowe prowadzone przez specjalnie przygotowane, zorganizowane, wyszkolone i wyposażone siły wykorzystujące techniki operacyjne i metody postępowania nietypowe dla sił konwencjonalnych. Działania te są prowadzone we wszystkich rodzajach operacji wojskowych samodzielnie lub we współdziałaniu z siłami konwencjonalnymi dla osiągnięcia celów politycznych, wojskowych, psychologicznych i ekonomicznych. Uwarunkowania polityczno-wojskowe mogą wymagać stosowania tajnych procedur i technik oraz uwzględnienia fizycznego i politycznego ryzyka nie występującego w działaniach konwencjonalnych"[22].

Z podobnymi definicjami spotykamy się w ujęciu amerykańskim: przez pojęcie „działania specjalne" rozumieją akcje o charakterze wojskowym prowadzone przez wyszkolone, uzbrojone, wyposażone i zorganizowane siły (nazwane siłami specjalnymi lub siłami specjalnego przeznaczenia), nacelowane na osiągnięcie narodowych celów politycznych, militarnych, gospodarczych i psychologicznych. Działania te mogą być prowadzone pod kątem klasycznych operacji zbrojnych, bądź jako akcje selektywne, w przypadku gdy użycie wojsk regularnych jest niecelowe lub niemożliwe"[23].

Natomiast, Regulamin polowy Sił Zbrojnych Stanów Zjednoczonych określa „operacje specjalne" jako działania niekonwencjonalne, organizowane i prowadzone poza bezpośrednią strefą walki sił zbrojnych przez odpowiednio zorganizowane, przygotowane i wyposażone zespoły ludzi (GS, GDR, GSP) lub oddziały w celu zdezorganizowania życia publicznego, administracyjnego, gospodarczego oraz militarnego przeciwnika a także utrudnienia mu prowadzenia działań na froncie i obniżenia wartości moralnej społeczeństwa[24].

Wskazane powyżej przykłady definiowania działań specjalnych nie stanowią zbioru zamkniętego. Na ich podstawie można zidentyfikować zadania wykonywane przez siły specjalne:

---

[21] T. Pietrzak, *Działania specjalne we współczesnych warunkach prowadzenia działań bojowych*, s. 16 - 17.
[22] *Regulamin Działań Wojsk Lądowych (DD/3.2),* Szkol 809/ 2006, Warszawa 2006, Słownik definicji.
[23] *U.S. Special Operations and Special Operations Forces*, s. 23.
[24] *Regulamin polowy Sił Zbrojnych USA* - PM-31-21A.

- wsparcie bezpieczeństwa wewnętrznego innych krajów *(foreign internal defence);*[25]
- działania wojenne niekonwencjonalne *(Uncoiwentional Warfare);*[26]
- akcje uderzeniowe *(Direct Actions);*[27]
- operacje zwalczania terroryzmu *(Combating Terrorism);*[28]
- rozpoznawcze operacje specjalne *(Special Reconnaissance);*[29]
- operacje humanitarne;
- działania antynarkotykowe;
- działania poszukiwawczo-ratunkowe;
- udzielanie pomocy innym krajom w zachowaniu ich bezpieczeństwa.

Natomiast, na podstawie dostępnych materiałów można stwierdzić, że pododdziały specjalne Niemiec posiadają inną systematykę zadań i są wykorzystywane do wykonywania następujących zadań[30]:

1. **Zakłócania działań przeciwnika:**
   - mylenia lub odwracania jego uwagi;
   - niszczenia wrażliwych obiektów (położonych w obszarach przemysłowych, w portach, na lotniskach) oraz urządzeń wojskowych;
   - eliminowania stanowisk dowodzenia szczebla operacyjnego, systemu łączności i zaopatrzenia;

---

[25] Wsparcie bezpieczeństwa wewnętrznego innych krajów (foreign internal defence) - to działania podejmowane przez organizacje cywilne lub wojskowe jednego państwa, zainicjowane przez rządy drugiego państwa, celem zabezpieczenia społeczeństwa przed bezprawiem, powstaniami, działaniami wywrotowymi (Doctrine for Army Special Operations Forces - FM-100-25. Waszyngton 1991. s. 3-6

[26] Niekonwencjonalne działania wojenne (Unconventional Warfare) - to formy działań specjalnych, prowadzone na ogół przez ludność cywilną, znajdującą się na terytorium objętym działaniami wojennymi, zazwyczaj wspierane z zewnątrz. Mogą to być nieprzerwane działania prowadzone w oparciu o utworzony na siłę ruch oporu, ukierunkowane na działalność wywrotową przeciwko władzy popieranej przez przeciwnika lub przeciw ustanowionym przez niego władzom okupacyjnym. Może to być wyrażane tworzeniem ruchów wywrotowych, sabotażem oraz akcjami partyzanckim. Wojska specjalnego przeznaczenia mogą uczestniczyć w realizacji następujących form działań: operacjach wywrotowych, działaniach partyzanckich, organizowaniu ucieczek oraz sabotażu (tamże, s. 3-3).

[27] Akcje uderzeniowe (Direct Actions) są ograniczone w czasie i zasięgu działania, prowadzone przeciw obiektom o dużym znaczeniu operacyjnym i strategicznym. Celem ich może być atak na ważne obiekty, uprowadzenia różnych osób lub zdobycie sprzętu (tamże, s. 3-11).

[28] Operacje zwalczania terroryzmu (Combating Terrorizm) - to działania podejmowane przez wojskowe agencje rządowe celem zapobiegania, przeciwdziałania oraz postępowania z aktami terrorystycznymi. Podstawowym zadaniem w tym wypadku jest wydzielenie specjalistycznych pododdziałów celem przeprowadzenia akcji antyterrorystycznych za granicą. Mogą obejmować: uwalnianie zakładników, odzyskiwanie niebezpiecznych materiałów będących w posiadaniu organizacji terrorystycznych, niszczenie struktur terrorystycznych (FM-100-25, op. cit., s 3-15).

[29] Rozpoznawcze operacje specjalne (Special Reconnaissance) są wykonywane na wszystkich szczeblach: taktycznym, operacyjnym i również strategicznym. Obejmują one zdobywanie oraz potwierdzanie informacji o możliwościach, zamiarach, a także działaniach obecnego lub potencjalnego przeciwnika (tamże, s. 3-13).

[30] *Działania specjalne Bundeswehry*. (w) „Wojskowy Przegląd Zagraniczny" nr 2 z 1994 r., s. 39.

- wyłączania środków oddziaływania powietrznego;
- znakowania celów dzięki użyciu sensorów;
- dezorganizowania pracy sił i środków walki radioelektonicznej;
- utrudniania przeciwnikowi wykonywania manewrów pozornych;
- niszczenia zapór inżynieryjnych i uniemożliwiania ich stawiania.

2. **Wsparcia własnych operacji:**

- zajmowania i czasowego utrzymania ważnych punktów, tj.: lotnisk, przepraw wodnych, węzłów komunikacyjnych;
- zdobywania przedmiotów wyposażenia i uzbrojenia;
- oddziaływania psychologicznego.

Z przedstawionych analiz wynika, że w tyłowej strefie działań realizowane mogą być następujące rodzaje działań specjalnych:

- partyzanckie;
- dywersyjno-rozpoznawcze;
- sabotażowe;
- poszukiwawczo-ratownicze;
- psychologiczne.

Reasumując powyższe fakty można przyjąć, że głównymi obiektami działań specjalnych będą elementy infrastruktury gospodarczej lub bytowej. Obiektami - w tyłowej strefie wojsk - będą węzłowe punkty ośrodków przemysłowych i gospodarczych, infrastruktura energetyczna, wodna itp. Urządzenia lotniskowe, porty morskie i śródlądowe z całą infrastrukturą komunikacyjną staną się ważnymi obiektami zagrożonymi działalnością dywersyjną i obiektami ataków terrorystycznych.

Ponadto można stwierdzić, że rozpoznanie specjalne może obejmować zdobycie dokładnych, terminowych i wiarygodnych informacji o przeciwniku i obszarze działań przez grupy specjalne (ZGS) rozmieszczone w głębi ugrupowania przeciwnika oraz zapleczu.

Główne zadania - to:

- wykrywanie, określanie położenia oraz śledzenie sił i środków ogniowych, broni precyzyjnej i systemów rozpoznawczo-uderzeniowych, przegrupowujących się odwodów operacyjnych, lotnisk, wyrzutni rakiet przeciwlotniczych, stacji radiolokacyjnych systemu obrony powietrznej, przepraw, stanowisk dowodzenia i węzłów łączności przeciwnika;

- lokalizacja, identyfikacja, potwierdzanie i udokładnianie położenia obiektów wykrytych przez rozpoznanie radioelektroniczne i powietrzne;
- ustalanie rozmieszczenia zasadniczych elementów obiektów i ich parametrów, planowanych do obezwładnienia lub zniszczenia przez środki rażenia wojsk własnych;
- chwytanie jeńców oraz zdobywanie dokumentów, próbek gruntu, sprzętu i wzorów uzbrojenia;
- oznakowywanie i laserowe oświetlanie wybranych obiektów (celów) oraz naprowadzanie na nie własnego lotnictwa oraz sojuszniczego, a także korygowanie ognia artylerii (uderzeń rakiet);
- ocenianie skutków uderzeń, stopnia obezwładniania obiektów, nastrojów wojsk i ludności przeciwnika.

Działania dywersyjne (akcje bezpośrednie) mogą być prowadzone przez grupy specjalne. Obejmują one niszczenia i dezorganizowanie funkcjonowania wybranych elementów ugrupowania przeciwnika.

Główne zadania - to:

- niszczenie środków ogniowych, w tym środków przenoszenia broni jądrowej;
- niszczenie broni precyzyjnej;
- dezorganizowanie funkcjonowania systemów dowodzenia, łączności, obrony powietrznej, logistycznych, komunikacyjnych i energetycznych;
- niszczenie samolotów i śmigłowców na lotniskach i lądowiskach oraz okrętów w portach i bazach morskich;
- bojowe uzbrajanie (minowanie) terenu oraz ograniczanie swobody manewru w określonych obszarach i w określonym czasie.

Działania niekonwencjonalne mogą obejmować przedsięwzięcia wspomagające realizację planu walki wojsk operacyjnych w zakresie działań nieregularnych, oddziaływania psychologiczno-propagandowego oraz walki radioelektronicznej.

Główne zadania - to:

- wspieranie pododdziałów wojsk operacyjnych przechodzących do działań nieregularnych;
- wspieranie i organizowanie pododdziałów partyzanckich.

Działania poszukiwawczo-ratownicze mogą być prowadzone przez grupę specjalną na obszarze kraju oraz na terytorium przeciwnika w celu ratowania i ewakuowania personelu latającego, poszukiwania żołnierzy oraz osób cywilnych zaginionych w wyniku katastrof. Główne zadania - to:

- ratowanie i ewakuowanie personelu latającego;
- poszukiwanie żołnierzy oraz osób cywilnych zaginionych w wyniku katastrof.

Działania psychologiczne mogą być prowadzone przez grupy specjalne na terytorium kraju (innych państw) oraz przeciwnika w okresie pokoju, kryzysu i wojny w celu kształtowania korzystnych dla nas postaw i nastrojów wśród żołnierzy, osób cywilnych oraz władz strony przeciwnej. Główne zadania - to:

- rozpowszechnianie propagandy drukowanej;
- przeciwdziałanie panice;
- emitowanie fałszywych audycji;
- udzielanie pomocy psychologicznej ludności cywilnej;
- inspirowanie ludności do działań;
- kreowanie postawy obywatelskiej i zaufania do rządu i państwa.

Wynik powyższej analizy można sprowadzić do wniosku, że chociaż główna rola WSP związana jest przede wszystkim z walką w głębi (w tyłowej strefie wojsk) to jednak pododdziały WSP prowadzą również działania opóźniające oraz rozpoznawcze. Przedsięwzięcia z zakresu izolacji pola walki i prowadzenia rozpoznania są realizowane przeciwko tym celom (obiektom) przeciwnika, które mogłyby wywierać bezpośredni, negatywny wpływ na działanie własnych wojsk. Zadania te mogą być wykonywane przez pododdziały (grupy) prowadzące działania nieregularne rozmieszczone znacznie wcześniej na tyłach przeciwnika lub też przez siły wypadowe przerzucone specjalnie w celu wykonania konkretnych zadań. W przypadkach szczególnych, stosowane być mogą równocześnie obie formy działań.

3.4 Sabotaż i dywersja

Aby móc precyzyjnie określić obszary oddziaływania sabotażu i dywersji należałoby się zapoznać z podstawowymi definicjami, które ich dotyczą. Niestety, dokładność określeń pozostawia wiele do życzenia, dlatego też (w oparciu o pojęcia definiujące zaczerpnięte z encyklopedii i słowników) postaramy się je doprecyzować.

Poniżej przedstawiamy przykłady kilku definicji:

„Dywersja – wszelka działalność zmierzająca do zakłócenia życia politycznego i administracyjno-gospodarczego państwa (d. gospodarcza, sabotaż) oraz osłabienie jego potencjału militarnego, prowadzona dla osiągnięcia pośrednich celów politycznych, ekonomicznych i wojennych...[31]„

Dywersja - niszczące działanie na zapleczu, element z arsenału walki. Działanie wojenne mające na celu odwrócenie uwagi nieprzyjaciela. Działanie z ukrycia w celu podkopania obronności, albo gospodarki nieprzyjaciela w czasie wojny, albo wrogiego państwa w czasie pokoju. Dezorganizacja sił nieprzyjaciela, polegająca na niszczeniu lub uszkadzaniu sił zbrojnych wroga[32].

Dywersyjny sabotaż - działanie na zapleczu i tyłach wojsk wroga, mające na celu utrudnienie mu działalności na froncie. Dywersja to jeden z podstawowych elementów strategii wojny partyzanckiej. Według prawa wojennego dywersantów nie traktuje się jak jeńców wojennych[33].

Natomiast jeżeli mówimy o sabotażu powinniśmy uwzględnić poniższe sformułowania: sabotaż (fr. *sabotage)* 1. dezorganizowanie pracy przez umyślne jej niewykonywanie lub wykonywanie złe, uszkadzanie maszyn, przyrządów. 2. utajnione, zakamuflowane działania mające przeszkodzić w urzeczywistnieniu czegoś[34] lub też sabotaż - zamierzone dezorganizowanie pracy przez uchylanie się od niej lub wadliwe jej wykonywanie, a także niszczenie, uszkadzanie środków produkcji; ukryte, zamaskowane działanie mające na celu przeszkodzenie w realizacji jakiegoś planu[35].

Przedstawione powyżej definicje definiują obszar oddziaływania, nie odpowiadają jednak na najważniejsze pytania: kto jest wykonawcą zadań dywersyjnych i sabotażowych oraz czym się one różnią?

Nie wdając się w bardziej szczegółowe rozważania uważamy, że możemy odróżnić te dwa pojęcia w zależności od skali występowania lub przynależności wykonujących te czynności osób lub formacji.

Naszym zdaniem najbardziej adekwatnym i szczegółowym jest podział, który rozgranicza dywersję od sabotażu opierając się na wykonawcach. I tak działania dywersyjne to takie działania, które wykonywane są na tyłach wojsk przeciwnika przez

---

[31] *Leksykon Wiedzy Wojskowej*,Wydawnictwo MON, Warszawa 1979, s. 96
[32] Zob. http://pl.wikipedia.org/wiki/Dywersja
[33] Tamże.
[34] *Słownik Wyrazów Obcych*, Wydawnictwo Naukowe PWN, Warszawa 1996, s. 987.
[35] *Słownik Języka Polskiego*, Tom III, PWN, Warszawa 1981r. s. 167.

formacje zbrojne wchodzące w skład sił zbrojnych walczącej strony, natomiast sabotaż to działania wymierzone we własne struktury państwa i jego siły zbrojne prowadzone przez obywateli tegoż państwa.

Dlatego też definicja podana powyżej i odnosząca się do dywersyjnego sabotażu może wprowadzać w błąd, tym bardziej, że mamy tutaj do czynienia również z odniesieniami do międzynarodowego prawa wojennego.

Pozostańmy więc przy podziale zaproponowanym przez zespół badawczy tym bardziej, że zakres działań jest w obu tych pojęciach zbliżony.

Konkludując, możemy więc - uściślając te definicje stwierdzić - że jest to działalność polegająca na zamierzonym uchylaniu się od wykonywania odpowiednich funkcji lub zadań w celu przeszkodzenia osiągnięciu określonych wyników albo świadome i celowe niszczenie lub uszkadzanie obiektów, środków produkcji i innych przedmiotów.

Wyniki badań skłaniają do wniosku, że „działanie dywersyjne (intruder operation) - działanie ofensywne prowadzone na terytorium przeciwnika, w celu zniszczenia ważnych obiektów (osób) lub zdezorganizowanie jego działania"[36] lub rozwijając tą definicję, działania dywersyjne - to akcje specjalne na zapleczu lub tyłach wojsk przeciwnika prowadzone przez odpowiednio zorganizowane i przygotowane zespoły ludzi lub pododdziały wojsk, tzw. pododdziały specjalne lub oddziały partyzanckie - głównie w celu zdezorganizowania życia politycznego i administracyjno-gospodarczego w kraju przeciwnika i osłabienia jego potencjału militarnego, a także dla utrudnieniamu prowadzenia działań na froncie i obniżenia wartości moralnej i bojowej jego wojsk. Akcje specjalne wykonywane w ramach działań dywersyjnych skierowane będą przede wszystkim przeciwko aparatowi władzy administracyjno-państwowej przeciwnika, jego komunikacji, transportom wojskowym, ważnym obiektom przemysłowym i politycznym, środkom i systemom radioelektronicznym, wojskom itp.

Do prowadzenia działań dywersyjnych mogą być użyte zawczasu przygotowane i zorganizowane pododdziały specjalne, partyzanckie, rozpoznawcze, organizacje paramilitarne oraz ludność cywilna (np. mniejszości narodowe). Z przeprowadzonych badań i analizy literatury wynika, że dywersja może być przygotowywana i prowadzona w czasie pokoju i wojny. Różnica pomiędzy dywersją czasu pokoju a dywersją czasu wojny polega na stosowaniu odmiennych metod jej

[36] *Regulamin Działań Wojsk Lądowych (DD/3.2)*, Szkol 809/ 2006, Warszawa 2006, definicje.

prowadzenia i rodzaju użytych do tego sił i środków. W czasie pokoju dywersja może być prowadzona w celu osłabienia danego państwa od wewnątrz, poderwania autorytetu istniejących struktur państwa, zakłócenia normalnego toku pracy społeczeństwa, wywołania chaosu w życiu gospodarczym kraju i utrudnieniu konsolidacji życia państwowego. Cele te mogą być realizowane poprzez działalność skierowaną przeciwko ustrojowi danego państwa, sabotaż, prowadzenie akcji wywrotowych, działalność wywiadowczą itp. W czasie wojny zakres dywersji zwiększa się. Oprócz zadań wykonywanych w czasie pokoju, działania dywersyjne mogą mieć na celu odciąganie sił i środków walki z frontu zewnętrznego, hamowanie dopływu świeżych sił z wnętrza kraju (uzupełnienia mobilizacyjne), dezorganizacja kluczowych obszarów przemysłu lub poszczególnych zakładów prowadzących produkcję na potrzeby sił zbrojnych, utrudnianie planowego zaopatrywania wojsk. Wyraża się to głównie w niszczeniu linii komunikacyjnych, węzłów drogowych i kolejowych, utrudnianiu dokonywania przegrupowania wojsk, niszczeniu obiektów o dużym znaczeniu wojskowym i gospodarczym lub politycznym, składów i magazynów zaopatrywania wojsk, rurociągów paliw płynnych, dezorganizacji systemu dowodzenia wojskami, łączności oraz zbieraniu danych wywiadowczych dla potrzeb walczących stron.

Reasumując można stwierdzić, że dywersja prowadzona na szeroką skalę zmusza przeciwnika do wydzielenia znacznych sił do ochrony obiektów o znaczeniu strategicznym - tak wojskowym, jak też gospodarczym czy politycznym, osłabia jego siły, dezorganizuje dowodzenie wojskami i pracę społeczeństwa, powoduje panikę wśród walczących żołnierzy i ludności cywilnej.

Natomiast w odniesieniu do działalności sabotażowej należy stwierdzić, iż powyższe zadania dotyczące dywersji mogą być realizowane również w tym obszarze. Tym bardziej, że posiadając łatwiejszy dostęp do zakładów produkcyjnych, linii zaopatrywania i transportu wojsk czy też obiektów administracji publicznej - łatwiejsze jest prowadzenie obserwacji interesujących nas osób, obiektów czy rejonów a co za tym idzie, wzrasta możliwość skutecznego zaplanowania i przeprowadzenia akcji.

W ostatnim okresie czasu zaobserwowaliśmy znaczący wzrost rozwoju technologicznego. Jest to obszar o znaczeniu strategicznym i możliwość oddziaływania na systemy zbrojeniowe czy teleinformatyczne przeciwnika staje się priorytetem. Dlatego też należy przypuszczać, że znaczna część działań zbrojnych prowadzonych w przyszłości (a pewne symptomy tego możemy już zaobserwować) będzie dotyczyć

teleinformatyki. Dotyczy to również działalności dywersyjnej i sabotażowej. Możliwości bowiem, są w tej dziedzinie olbrzymie.

Podsumowując, należy stwierdzić, iż działania dywersyjne i sabotażowe prowadzone w tyłowej strefie działania wojsk ewoluują wraz ze zmianami w obszarze taktyki i sztuki operacyjnej, uzbrojenia, wprowadzenia nowych technologii a efekty i korzyści jakie możemy dzięki tym działaniom osiągnąć, każą przypuszczać iż działania te będą w dalszym ciągu wykorzystywane w przyszłych konfliktach, chociaż obszary ich oddziaływania mogą się zmieniać w zależności od zmian zachodzących w środowisku walki.

3.5 Zbrojne organizacje przestępcze

Organizacje przestępcze zawsze wykorzystują słabości systemu prawnego i gospodarczego, w którym działają a obszar konfliktu zapewnia im szeroką i otwartą przestrzeń do przemieszczania się. Terroryści, przemytnicy narkotyków, handlarze ludźmi, osoby „piorące" pieniądze i dokonujące nadużyć finansowych działają tak, jak gdyby nie istniały granice państw: w jednym kraju mogą zaplanować przestępstwo, w drugim go dokonać, a mieszkać w trzecim.

Dlatego lista zagrożeń w tyłowej strefie działań oraz układ priorytetów z nimi związanych zmienia się ze zmianą czasu i różni w zależności od położenia, kultury i ludności obszaru prowadzenia działań. W każdym punkcie czasu niektóre zagrożenia zanikają, ujawniają się, inne trwają nadal, a jeszcze inne wyłaniają się ponownie ze zwiększoną siłą.[37]

Spośród tych niekorzystnych zjawisk najbardziej niebezpieczna, z punktu widzenia prowadzonych działań, jest forma przestępczości określana mianem zbrojnych organizacji przestępczych. Zbrojne organizacje przestępcze zaczęły przybierać nowe, coraz bardziej groźne i skomplikowane formy. Walka z nimi, w szczególności zapobieganie przestępstwom, powinna stać się jednym z podstawowych zadań realizowanych w tyłowej strefie działań.

Definicji zbrojnych organizacji przestępczych trudno szukać w literaturze, jedynie co można znaleźć to przestępczość zorganizowana określana jako: ukierunkowane na osiągnięcie zysku lub władzy planowane popełnianie przestępstw

[37] D.B. Bobrow: *Złożoność problematyki braku bezpieczeństwa:* Implikacje redefinicji pojęcia. w: D.B. Bobrow, E. Haliżak, R. Zięba (red.): *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku.* Warszawa 1997, s. 37.

przez współdziałających dłuższy czas co najmniej dwóch uczestników, jeżeli przestępstwa te pojedynczo lub jako całość mają znaczny ciężar gatunkowy, a ich realizacja następuje:

- przy wykorzystaniu zawodowych lub struktur podobnych zawodowym;
- przy użyciu przemocy lub środków zastraszania;
- przez wywieranie wpływu na politykę, administrację publiczną, wymiar sprawiedliwości, lub gospodarkę[38].

Nie każda jednak działalność przestępcza może być określana przymiotnikiem „zorganizowana". Aby można było mówić o zorganizowanej działalności przestępczej czy też zorganizowanych organizacjach przestępczych muszą występować pewne, charakterystyczne dla nich cechy, do których należą[39]:

- występowanie trwałego związku stale współpracujących osób przy dominującej roli przestępców zawodowych;
- hierarchiczna struktura organizacyjna, odznaczająca się bezwzględną dyscypliną, przy czym „nagrodą" za posłuszeństwo jest troska organizacji o bezpieczeństwo uczestników;
- racjonalne, planowane i oparte na specjalizacji oraz podziale zadań realizowanie celów;
- dostosowanie prowadzonej działalności do aktualnych potrzeb ludności (reagowanie na potrzeby „rynku");
- dopasowanie metod i środków („technologii") działalności do warunków i rodzaju realizowanych celów (szantaż, przekupstwo, oszustwo, itp.);
- konspiracja wewnętrzna i „uszczelnianie" organizacji na zewnątrz;
- pomoc dla członków organizacji, w szczególności zaś dla objętych ściganiem (zastraszanie świadków oskarżenia, opieka nad rodziną skazanego);
- mobilność i międzynarodowość.

Z analizy literatury wynika, że aktualnie zbrojne organizacje przestępcze specjalizują się w określonej działalności przestępczej, do której należą[40]:

---

[38] A. Marek, *Przestępczość zorganizowana. Zarys problematyki*, na podstawie: U. Dörmann i in., Organisierte Kriminalität – wie gross ist die Gefahr? (BKA Forschungsreihe), Wiesbaden 1990, (w:) *Kryminologiczne i prawne aspekty przestępczości zorganizowanej*, red. A. Marek, W. Pływaczewski, WSPol Szczytno 1992, s. 32.

[39] Tamże, na podstawie: H. D. Schwind, Definition und Geschichte der organisierten Kriminalität, red. H. D. Schwind i in., Heideelberg 1986 s.30.

[40] J. W. Wójcik, *Przestępstwa w biznesie*, Warszawa 1998, s. 18.

- produkcja, przemyt i dystrybucja narkotyków i środków psychotropowych;
- przemyt i nielegalny handel bronią;
- zabójstwa na zlecenie;
- pobicia i porwania osób;
- napady na osoby podróżujące samochodami;
- produkcja i wytwarzanie ładunków wybuchowych;
- przemyt alkoholu i wyrobów tytoniowych;
- oszustwa podatkowe;
- oszustwa kredytowe;
- oszustwa ubezpieczeniowe;
- oszustwa giełdowe;
- wynajmowanie „mścicieli" – przestępców do zastraszania przedstawicieli wymiaru sprawiedliwości, którzy zajmują się ściganiem zorganizowanych grup przestępczych;
- kradzież i przemyt samochodów;
- fałszowanie środków płatniczych;
- przemyt pierwiastków promieniotwórczych;
- organizowanie nielegalnych przerzutów cudzoziemców.

Do powyższej listy należy jeszcze dodać: czerpanie zysków z prostytucji, wymuszenia haraczu, organizowanie nielegalnych zakładów hazardowych.

Dostępne materiały określają, że za najwyższą formę zorganizowanej przestępczości uważa się mafię. Termin ten, podobnie jak terroryzm, jest nadużywany i nie rozumiany przez wiele osób, w tym zwłaszcza przez dziennikarzy wypaczających jego sens. Niewłaściwe używanie i nadużywanie nazwy „mafia" lekceważy jej istotę i co najistotniejsze nie wyraża olbrzymiego ładunku niebezpieczeństwa, zła, jaki ona w sobie kryje[41].

Zasadnicze cechy mafii dostrzegł i zdefiniował człowiek włoskiego renesansu, Niccolo Machiavelli, określając ją jako: (...) zakonspirowaną organizację przestępczą, opartą na bezwzględnie przestrzeganych zakazach, nakazach milczenia, zachowania tajemnicy, posłuszeństwa i lojalności wobec szefa. Nieodłączną cechą organizacji mafijnej jest dążenie do pozyskania na swoją stronę, łapówką, szantażem lub terrorem przedstawicieli policji, sądownictwa i administracji państwowej lub samorządowej

[41] Kryminologiczno-kryminalistyczne studium: Zagrożenia przestępczością zorganizowaną (mafijną) w Polsce – w kontekście doświadczeń innych policji, Komenda Główna Policji, Warszawa 1994, s. 8.

i polityków (w dzisiejszym znaczeniu tego słowa). Każda mafia dąży do rozszerzenia swych wpływów, majątku i pola działania, a w konsekwencji zdobycia większej lub mniejszej władzy politycznej[42]. Należy przyjąć, iż mafia stanowi niejako ostatni szczebel rozwoju, jaki może przybrać, zbrojna organizacja przestępcza, dlatego też ta ostatnia musi być poddana ostremu monitorowaniu ze strony służb i wojsk odpowiedzialnych za realizację zadań w tyłowej strefie działania wojsk.

Główne niebezpieczeństwo ze strony zbrojnych organizacji przestępczych polega więc na tym, że są one elastyczne oraz wielopostaciowe. Od organizacji przestępczych do terroryzmu (terroru) droga nie jest daleka.

Zbrojne organizacje przestępcze stanowią potencjalne zagrożenie dla struktur państwa, społeczeństwa, i pododdziałów prowadzących działania w tyłowej strefie działań.

Chcąc zidentyfikować z jakimi zbrojnymi organizacjami przestępczymi będziemy mieli do czynienia w tyłowej strefie działań musimy dokonać identyfikacji obecnie istniejące formy działalności kryminalnej.

W tej chwili w Polsce działa 35–40 dużych, dobrze zorganizowanych gangów. Grupa najgroźniejszych polskich szefów gangów, organizatorów największych akcji przestępczych obejmuje ponad 400 osób. Dochodzi do tego blisko 60 grup wywodzących się z Rosji, Ukrainy i Litwy oraz kilka grup międzynarodowych, przede wszystkim z byłej Jugosławii. Niektóre grupy składają się z kilku bądź kilkunastu osób, są jednak i takie, jak choćby gang pruszkowski czy wołomiński, które mają po kilkaset osób[43]. Do pełnego obrazu rodzimej przestępczości zorganizowanej należy dodać jeszcze ponad 200 lokalnych organizacji przestępczych. Daje to obraz sytuacji w Polsce[44].

Polskie organizacje przestępcze zaczęły tworzyć się w latach siedemdziesiątych, ale już we wcześniejszym okresie następowała kryminalizacja sfery gospodarczego życia w Polsce. Zorganizowane grupy przestępcze zagarniały majątek narodowy znacznej wartości[45]. Prawdziwy rozkwit tego rodzaju form działalności przestępczej nastąpił wraz z początkiem transformacji ustrojowej w naszym kraju – w 1989 r., a zwłaszcza z jego skutkami związanymi z otwarciem granic, co oprócz swej

---

[42] Tamże.
[43] B. Hołyst, *Kryminologia wobec nowych zjawisk i współczesnych metod przestępczych*, (w): H. J. Hirsch, P. Hofmański, E. W. Pływaczewski, C. Roxin (red.): *Prawo karne i proces karny wobec nowych form i technik przestępczości*, Białystok 1997, s. 172.
[44] W innych państwach sytuacja może być inna
[45] Tamże, s.172.

ogromnej pozytywnej roli – przerwaniem izolacji obywateli wobec świata- spowodowało, między innymi wzrost przestępczości.

Bardzo niepokojącym zjawiskiem jest dynamiczny rozwój kontaktów polskich grup z grupami przestępczymi w innych krajach. Dotychczasowa ich identyfikacja wskazuje na międzynarodowy skład osobowy niektórych grup przestępczych działających na terenie Polski, w których występują obok obywateli polskich zarówno obywatele Europy Zachodniej, jak i byłego ZSRR, z przewagą tych ostatnich. W ostatnim okresie odnotowano obecność w Polsce zorganizowanych grup przestępczych składających się z obywateli wietnamskich. Grupy te mają ścisłe powiązania z istniejącymi już od dawna na terenie Europy Zachodniej wietnamskimi organizacjami przestępczymi[46].

Z opinii ekspertów Interpolu i ONZ oraz informacji policyjnych wynika, że Polska znalazła się w kręgu szczególnego zainteresowania międzynarodowych grup przestępczych poszukujących nowych tras przemytu kokainy, heroiny, haszyszu i marihuany. Wynika to z centralnego położenia Polski na kontynencie europejskim. W Europie Zachodniej coraz częściej pojawiają się narkotyki nielegalnie wytwarzane w państwach powstałych po rozpadzie Związku Radzieckiego. Najkrótsza droga przemytu z tych państw na zachodnioeuropejskie rynki zbytu prowadzi przez Polskę[47]. Liczne, udaremnione przez nasze służby graniczne i celne, próby przemytu narkotyków, zdają się potwierdzać tą tezę.

Reasumując można stwierdzić, że tak jak nie można stawiać znaku równości pomiędzy pojęciami „terror" i „terroryzm", tak też nie można uważać za tożsame pojęć zjawiska „zbrojne organizacje przestępcze" i „terroryzmu". Fakt, że zorganizowane grupy przestępcze sięgają po metody, jakimi posługują się terroryści, nie jest dostateczną przesłanką, co już kilkukrotnie podkreślaliśmy, aby mówić o terroryzmie. Uważamy, że najistotniejsza różnica pomiędzy organizacjami przestępczymi a terroryzmem leży w celu działania obranym przez liderów obu działalności. W pierwszym wypadku celem nie jest obalenie czy też destrukcja władzy, a podporządkowanie sobie jej działalności (między innymi przez korumpowanie polityków, przenikanie do ośrodków decydenckich w państwie, itp.), w drugim zaś obalenie lub destabilizowanie (uniemożliwienie normalnego funkcjonowania) istniejącego w państwie porządku: prawnego, konstytucyjnego, ekonomicznego, itp.

---

[46] Tamże, s. 173.
[47] Tamże, s. 173.

Nie można także postawić tezy, która by stwierdzała, że tam gdzie jest terroryzm nie ma przestępczości zorganizowanej i odwrotnie. Te dwa zjawiska, chociaż wykorzystujące niejednokrotnie podobne metody działania, są od siebie niezależne.

4. ROZPOZNANIE W SYSTEMIE GLOBALNEGO BEZPIECZEŃSTWA

Położenie geopolityczne Polski na mapie Europy powodowało, że kwestia zapewnienia bezpieczeństwa, integralności terytorialnej oraz nienaruszalności granic państwowych zawsze była jedna z najważniejszych w polskiej polityce zagranicznej oraz wewnętrznej. Polityka bezpieczeństwa realizowana przez szereg organów państwowych ma na celu ochronę interesów narodowych Rzeczpospolitej, przede wszystkim zaś tych, które składają się na treść polskiej racji stanu[1].

Ponieważ zarówno bezpieczeństwo obywateli jak i niepodległość oraz nienaruszalność granic są egzystencjalnymi interesami narodowymi ich zapewnienie ma charakter nakazu bezwzględnego, umożliwiającego użycie w ich obronie całego zasobu sił i środków posiadanych przez państwo.

Najważniejsze wyzwania czasu pokoju stojące obecnie przed Polską i jej polityką bezpieczeństwa oraz polskimi siłami zbrojnymi, to m.in.:

- konieczność utrzymania odpowiedniego potencjału obronnego w celu zminimalizowania ewentualnych nacisków z zewnątrz i szantażu politycznego, jak również utrzymania międzynarodowej pozycji Polski i udzielania pomocy polskiej dyplomacji;
- wnoszenie określonego wkładu w potencjał i system obrony NATO w celu wzmocnienia obronnej wiarygodności Sojuszu oraz Polski;
- działania na rzecz umacniania instytucji bezpieczeństwa międzynarodowego działającymi w dziedzinach rozbrojenia, kontroli zbrojeń oraz budowy środków zaufania międzynarodowego;
- kontynuacja udziału Polski w operacjach międzynarodowych służących pokojowi i bezpieczeństwu na świecie;
- rozwój współpracy z krajami sąsiednimi w sferze wojskowej, przełamywanie stereotypów i uprzedzeń w celu tworzenia bezpiecznego i pokojowego otoczenia Polski[2].

---

[1] Zob.: A. Ciupiński, A. Legucka, *Podstawowe elementy polityki bezpieczeństwa i obrony Rzeczpospolitej Polskiej*, AON, Warszawa 2003.
[2] Tamże.

Podsumowując, od rozpoczęcia transformacji ustrojowej związanej z zasadniczymi zmianami w otoczeniu międzynarodowym Polski, istnieje konieczność ciągłego rozpoznania w systemie globalnego bezpieczeństwa, co jest celem niniejszego rozdziału. Jest przede wszystkim przedstawienie sytuacji na arenie międzynarodowej dotyczącej proliferacji broni masowego rażenia (broni jądrowej i biologicznej) i zagrożeń związanych z przemysłem zbrojeniowym oraz wpływu ich posiadania na kształtowanie bezpieczeństwa międzynarodowego. Utrzymanie pokoju na świecie, równowagi oraz stabilizacji w rejonach najbardziej zagrożonych możliwością użycia broni masowego rażenia a także siły i środki, które należy podejmować w celu zapobiegania jej dalszemu rozprzestrzenianiu są głównymi kwestiami podejmowanymi przez autorów w tym rozdziale.

Rozpatrując tematykę związaną z proliferacją broni jądrowej i przemysłem zbrojeniowym jako źródłem zagrożeń należy scharakteryzować samo pojęcie bezpieczeństwa międzynarodowego, bowiem definicja ta potrzebna jest dla dalszego zrozumienia problemu, jakim jest m.in. rozprzestrzenianie broni jądrowej.

Zasadniczym celem, stawianym sobie przez wszystkie państwa świata, jest zapewnienie ich mieszkańcom bezpieczeństwa[3], które gwarantowałoby im swobodny i nieskrępowany rozwój. Możemy wyróżnić bezpieczeństwo wewnętrzne i zewnętrzne. Bezpieczeństwo zewnętrzne odnosi się bezpośrednio tylko do określonego, własnego narodu (tzw. narodowe), lub do grupy państw (międzynarodowe). Początkowo, definicję bezpieczeństwa ograniczano jedynie do wprowadzenia zbrojnej ochrony granic, przed niespodziewanym wrogim atakiem ze strony krajów sąsiednich. Taki sposób patrzenia na to zjawisko, dominowało w Europie w czasie istnienia bloków: radzieckiego i zachodniego, i wczesnych lat tzw. zimnej wojny. Dziś patrzy się na nie, nie tylko poprzez pryzmat wojskowy, ale również ekonomiczny, społeczny, czy kulturalny. Jego filary, opierają się na daleko posuniętej współpracy wszystkich krajów na całym świecie. „Reasumując – pisze jeden z autorów *„Małego Słownika Stosunków Międzynarodowych"* – w bezpieczeństwie rozumianym „negatywnie" dominującymi potrzebami są istnienie i przetrwanie; w rozumianym „pozytywnie" na plan pierwszy wysuwa się rozwój"[4].

[3] http://www.bryk.pl/prace/liceum/pozosta%C5%82e/wos/1487-bezpiecz%C584stwomi%C4%99dzynarodowe i jego definicja.html 16.11.2006.

[4] *Mały Słownik Stosunków Międzynarodowych*, red. G. Michałowska, Warszawa 1996.

Warto pamiętać, że bezpieczeństwo nie może opierać się na jakiś pojedynczych wystąpieniach i zmianach, a jest zjawiskiem złożonym i wielofazowym. Jego wzmacnianie, powinno należeć do głównych zadań, jakie mają wszystkie rządy państwowe na całym świecie. Często jednak, dążenie do bezpieczeństwa za wszelką cenę, nie jest adekwatne do posiadanych przez określony kraj możliwości, a prowadzenie polityki niezgodnej z panującymi na świecie tendencjami (np. stałe naruszanie głównych umów międzynarodowych), w prostej drodze może prowadzić do izolacji i zerwania, korzystnych zazwyczaj sojuszy.

Współczesnemu bezpieczeństwu zagraża obecnie nowy rodzaj zagrożeń, nazywany zagrożeniami niekonwencjonalnymi lub asymetrycznymi. Cechuje je to, że ze względu na dostępną współcześnie technikę, nowoczesne technologie, a także sposób działania i możliwość dotarcia do każdego prawie miejsca na świecie zyskały one wymiar globalny. Biorąc pod uwagę zdolność do wykonywania potencjalnych zniszczeń i zadawania strat możemy mówić o ich nieproporcjonalnie dużej skali w stosunku do posiadanych sił i środków. Inną rzeczą, jest medialność oraz sposób oddziaływania na wyobraźnię opinii publicznej. Ponadto nowe zagrożenia są bardzo trudne do zwalczania ze względu na nieprzewidywalność ich pojawienia się. Jak wcześniej zaznaczyłem problematyka odstraszania przed użyciem broni masowego rażenia przez potencjalnych proliferatorów stanowi jedno w tej chwili z najważniejszych wyzwań stojących przed Sojuszem. Zagrożenie to spowodowane jest możliwością użycia broni jądrowej zarówno przez przedmioty państwowe, jak i pozapaństwowe(ugrupowania terrorystyczne).

4.1. ROZPRZESTRZENIANIE BRONI JĄDROWEJ

Ludzie od najdawniejszych czasów bardzo mocno angażowali się w prowadzenie wojen oraz na podstawie doświadczeń, które tam zdobywali próbowali wyobrazić sobie jej przyszły charakter a może nawet i przebieg. Na podstawie tych doświadczeń próbowano wyrobić poglądy, co do sposobu jej prowadzenia oraz przygotowania. Z czasem człowiek wynajdował coraz to nowsze sposoby oraz środki walki ulepszając przy tym techniki zabijania. Przełomem był schyłek drugiej wojny światowej, kiedy to już poznano zjawisko związane z sztucznymi przemianami

jądrowymi. Energia[5], która drzemie w atomie mogła zostać wykorzystana nie tylko do celów pokojowych takich, jak na przykład budowa reaktorów atomowych.

Po zbudowaniu pierwszej bomby atomowej przez Stany Zjednoczone i użyciu jej w 1945 roku przeciwko Japonii, pojawiło się zagrożenie wojny nuklearnej. To właśnie dzięki możliwościom i sile, jaką posiada broń jądrowa możliwe stało się rozstrzygnięcie konfliktu zbrojnego bez użycia ogromnych sił wojskowych. Działalność wielu państw miała na celu udoskonalanie broni jądrowej a w rezultacie tego doprowadzono do wyścigu zbrojeń.

Dopiero 18 lat po tym jak użyto bomby atomowej ZSRR, USA, Wielka Brytania zawarły układ o zakazie doświadczeń z bronią jądrową. Układ ten zawarty został w 1963 roku i miał za zadanie spowolnić wyścig zbrojeń i oddaleniu groźby zagłady nuklearnej. Należy przy tym pamiętać, że groźba przyszłej wojny nuklearnej nie musi być spowodowana działaniem wojska. Bardzo niebezpieczne stają się elektrownie atomowe, które w czasie wybuchu mogą mieć również tragiczne konsekwencje. Takim przykładem, był wybuch elektrowni atomowej w Czarnobylu w 1986 roku i jej konsekwencje. W związku, z tym w obecnym czasie wiele uwagi poświęca się zagadnieniom związanym z problematyką nuklearną oraz zmianom, jakie zachodzą w środowisku bezpieczeństwa międzynarodowego w świetle doktryny nuklearnej NATO. Jednym z podstawowych wyzwań dla NATO na początku ubiegłego wieku stało się, zatem sformułowanie nowej strategii nuklearnej, dostosowanej do już zmienionej i zmieniającej się sytuacji bezpieczeństwa międzynarodowego. Przyjęcie nowej strategii przez NATO pod nazwą Koncepcja Strategiczna w 1991 roku było podyktowane kształtowaniem się nowego kontekstu geostrategicznego, który był różnicą w stosunku do strategii „zimnej wojny". Można ze względu na odmienność sytuacji geostrategicznej wyróżnić dwa zasadniczo odmienne etapy kształtowania i rozwoju doktryny nuklearnej Sojuszu:, tj. zimnowojenny i postzimnowojenny.

Broń jądrowa[6] rozumiana jest jako rodzaj broni masowego rażenia wykorzystująca wewnątrzjądrową energię wydzielaną podczas łańcuchowej reakcji rozszczepienia jąder ciężkich pierwiastków lub reakcji termojądrowej syntezy jąder lekkich pierwiastków; izotopów uranu i plutonu(tzw. broń atomowa) albo podczas

---

[5] Broń jądrowa swą siłę rażenia czerpie z energii drzemiącej w jądrach atomów. Źródłem energii bezpośrednio wykorzystywanej w broni jest albo proces rozszczepienia jąder pierwiastków ciężkich (klasyczna broń atomowa), albo proces syntezy jąder pierwiastków lekkich (tzw. broń termojądrowa lub wodorowa).

[6] http://pl.wikipedia.org/wiki/Bro%C5%84_j%C4%85drowa 16.11.2006r.

syntezy jąder izotopów wodoru(tzw. bomba wodorowa – o sile wybuchu znacznie większej niż broni atomowej. Z punktu widzenia NATO ma ona bardzo duże znaczenie. Dzięki istnieniu tej broni powstało przekonanie o możliwości pokonania przeciwnika bez użycia ogromnych armii, do zadania dużych zniszczeń na obszarze przeciwnika wystarczy samolot bombowy, pocisk artyleryjski lub rakieta przenosząca atomowe głowice bojowe. Świadomość użycia broni masowego rażenia oraz ogrom zniszczeń, jakie mogłaby spowodować, niszcząc przy tym nie tylko siły zbrojne danego państwa, jego infrastrukturę, ale także prawdopodobnie spowodowałaby zniszczenie sił własnych i własnej populacji. Po rozpadzie bloku wschodniego NATO stanęło przed pytaniem czy i po co potrzebna jest Sojuszowi broń jądrowa w nowej sytuacji geostrategicznej, w której brak jest przeciwnika. Zatem broń jądrowa stała się czynnikiem odstraszania. Koncepcja strategiczna ma na celu zachowanie pokoju oraz zapobieganie wojnie. Siłom nuklearnym nadal przypisuje się ogromną rolę w zapewnieniu bezpieczeństwa w Europie. Jednakże możliwe to będzie dzięki utrzymaniu odpowiedniego potencjału sił konwencjonalnych i nuklearnych. Wszystko to ma wpływ na kształtowanie się bezpieczeństwa międzynarodowego. Od chwili ukształtowania się na początku lat 90. XX w. nowej doktryny Sojuszu upłynęło już 15 lat. To doktryna ta obowiązuje do dzisiaj pomimo istotnych zmian w środowisku bezpieczeństwa międzynarodowego. Można nawet stwierdzić, że stan bezpieczeństwa w Europie, czy w strefie euroatlantyckiej pozostaje stabilny. Jednak w miejsce zagrożeń charakterystycznych dla czasów zimnej wojny pojawiły się tzw. nowe zagrożenia. Początkowo wydawało się, że największym zagrożeniem dla bezpieczeństwa międzynarodowego staną się kryzysy lub konflikty o podłożu etnicznym, religijnym i narodowościowym zarówno między państwami, jak i wewnątrz państw. Powodowały one destabilizację sytuacji nie tylko na terenie objętym konfliktem lub kryzysem, ale także źródło potencjalnej niestabilności w skali regionu. Pojawiły się one nawet w Europie w sposób szczególnie drastyczny na Bałkanach[7].

Drugim nie mniej istotnym wyzwaniem dla bezpieczeństwa międzynarodowego, jest proliferacja broni masowego rażenia i środków jej przenoszenia oraz zagrożenia wynikające z faktu wejścia w posiadanie tego rodzaju broni przez państwa lub różnego rodzaje organizacje. Zjawisko proliferacji broni jądrowej, jest niewątpliwie przejawem naruszenia ładu, porządku międzynarodowego, uosabianego przez traktaty

[7] Zob.: A. Hrynkiewicz – Żabicki; *Dylematy i wyzwania polityki nuklearnej NATO w świetle ewolucji środowiska bezpieczeństwa międzynarodowego*, Warszawa, 2004.

rozbrojeniowe reżimy nieproliferacji BMR. Nieprzestrzeganie, łamanie lub omijanie postanowień tych traktatów niewątpliwie ma na celu podważenie ich wiarygodności i skuteczności, a także zasad i wartości, które legły u ich podstaw. Proliferatorzy broni masowego rażenia poprzez rozwijanie broni masowego rażenia lub wejście w jej posiadanie – dążą do oparcia stosunków międzynarodowych na zupełnie innych zasadach, w których szantaż i dyktat siły, wynikający ze świadomości zagrożenia, jakie niesie charakter jej posiadania i skutki jej użycia, zastąpiłyby zasady prawa międzynarodowego i ogólnie przyjęte reguły współżycia międzynarodowego. Problem rozprzestrzeniania się broni jądrowej dotyczy jednak wszystkich rodzajów broni. Problem proliferacji broni jądrowej pojawił się w kontekście rozpadu ZSRR i podziału jego arsenału nuklearnego miedzy kilka państw, co wiązało się także ze zmianą zarządzania nim. Nieco później doszły obawy o bezpieczeństwo przechowywania i ochrony posrtadzieckiej broni jądrowej. W wyniku tych procesów pojawiły się opinie, że nastąpi osłabienie kontroli nad potencjałem nuklearnym i możliwy jest wypływ technologii jądrowych i specjalistów w tej dziedzinie do innych państw. Konsekwencją tego jest to, że kilka państw pracuje nad rozwojem własnych programów nuklearnych, a także programu rozwoju pocisków balistycznych zdolnych do przenoszenia broni jądrowej. Próby, które miały miejsce na subkontynencie indyjskim, mamy tu na myśli Indie i Pakistan u schyłku lat dziewięćdziesiątych. Oznaczają rozpoczęcie nuklearnego wyścigu zbrojeń. W 2003 roku świat obiegła wiadomość, że Korea Północna jest zdolna wyprodukować własną broń jądrową. 9 października 2006 roku Korea Północna przeprowadziła pierwszą próbę jądrową, wywołując wzburzenie opinii publicznej na świecie. Rada Bezpieczeństwa ONZ uchwaliła szereg sankcji finansowych i gospodarczych wobec Korei Północnej – ta jednak zareagowała zapowiedzią kolejnych testów jądrowych. Wywiady państw zachodnich potwierdzały, że prowadzone są przygotowania do takich prób[8].

Kolejnym zagrożeniem stały się państwa rządzone przez dyktatorów. Zjawisko to nie jest obce i nie jest czymś nowym. Natomiast obecnie cechuje je to, że dyktatorzy wywodzący się z poprzedniego układu, jak i nowi, zyskali swobodę działania na skutek rozluźnienia kontroli ze strony mocarstw, przez co stali się samodzielnymi aktorami na arenie międzynarodowej. Najbardziej niebezpieczni stają się dyktatorzy, którzy dążą do pozyskania lub posiadania broni jądrowej. Tacy dyktatorzy stali się poważnym

[8] Por. W. Multan; *Bezpieczeństwo międzynarodowe ery nuklearnej*, PISM, Warszawa, 1991.

zagrożeniem nie tylko w skali regionu, ale stwarzają potencjalne zagrożenie w skali społeczności międzynarodowej. Państwa te określane są mianem „państw zatroskania" lub państw „budzących zaniepokojenie"(*states of koncern*). Po 11 września 2001 roku mamy kolejną ewolucję związaną z bezpieczeństwem międzynarodowym. Pojawiło się nowe zagrożenie związane z terroryzmem, zwłaszcza inspirowanym fundamentalizmem islamskim. Zostało ono uznane za główne zagrożenie dla bezpieczeństwa na arenie międzynarodowej.

Głównymi aktorami stali się obecnie tzw. „aktorzy niepaństwowi", czyli organizacje ekstremistyczne, grupy terrorystyczne, a nie państwa. Istotną funkcją odstraszania nuklearnego staje się przeciwstawianie się takim sytuacjom związanym z możliwością użycia lub reakcją na użycie przez przeciwnika broni masowego rażenia, w tym także zagrożeniom użycia BMR przez tzw. *non state actors* w celach terrorystycznych. Jednak można zaryzykować stwierdzeniem, że zagrożenie bronią jądrową – uznaje się obecnie za mniejsze. Od pewnego czasu obserwuje się tendencje do akcentowania zagrożeń związanych z bronią biologiczną, chemiczną bądź radiologiczną. Wielu specjalistów analizuje możliwość wystąpienia zagrożenia użycia broni masowego rażenia przez grupy terrorystyczne. Jednak nie zależnie od rodzaju zagrożenia celem odstraszania nuklearnego w przypadku użycia BMR jest przekonanie, o nieopłacalności i nieracjonalności stosowania szantażu bronią masowego rażenia. Istotne, więc staje się niedopuszczenie do użycia przez przeciwnika broni masowego rażenia, ale także rezygnacja ze stosowania szantażu. Problematyka odstraszania nuklearnego w kontekście zagrożeń BMR znalazła swój udział w dyskusjach na temat reagowania kryzysowego. Uważa się, że zagrożenia wynikające z groźby użycia broni masowego rażenia mogą być istotnym elementem sytuacji kryzysowych. Inicjatywa w sprawie Przeciwdziałania Rozprzestrzenianiu Broni Masowego Rażenia (*The Proliferation Security Initiative – PSI*) jest odpowiedzią na coraz poważniejsze wyzwanie, jakim jest proliferacja broni masowego rażenia (BMR), ich systemów przenoszenia, oraz pochodnych materiałów na całym świecie. Inicjatywa w sprawie Przeciwdziałania Rozprzestrzenianiu Broni Masowego Rażenia opiera się na wysiłkach społeczności międzynarodowej skierowanych na zapobieganie proliferacji tych środków i materiałów, w tym na istniejących traktatach i reżimach. Jest ona zgodna z programem wdrażania oświadczenia Przewodniczącego Rady Bezpieczeństwa Narodów Zjednoczonych z lutego 1992 roku. Stanowi ona jednocześnie kolejny krok w jego realizacji. W oświadczeniu tym zawarte jest stwierdzenie, iż proliferacja każdego

rodzaju broni masowego rażenia jest zagrożeniem dla międzynarodowego pokoju i bezpieczeństwa. Podkreślona jest też potrzeba przeciwdziałania proliferacji przez państwa członkowskie Narodów Zjednoczonych. Inicjatywa w sprawie Przeciwdziałania Rozprzestrzenianiu Broni Masowego Rażenia jest również zgodna z niedawnymi oświadczeniami państw G8 i Unii Europejskiej, ponieważ opiera się na stwierdzeniu, że konieczne są bardziej spójne oraz wspólnie prowadzone wysiłki w celu zapobieżenia proliferacji BMR, ich systemów przenoszenia oraz pochodnych materiałów. Uczestnicy Inicjatywy są głęboko przekonani o aktualności tego zagrożenia oraz o niebezpieczeństwie wynikającym z ryzyka, iż te środki i materiały mogłyby dostać się w ręce terrorystów. Są oni zaangażowani we wspólne działanie w celu przerwania przepływu tych środków i materiałów do oraz z państw i struktur pozapaństwowych dokonujących proliferacji. Jednym z celów Inicjatywy w sprawie Przeciwdziałania Rozprzestrzenianiu Broni Masowego Rażenia jest włączenie w nią w miarę możliwości wszystkich państw, którym zależy na przeciwdziałaniu proliferacji, oraz które dysponują możliwością i chęcią podjęcia działań w celu przerwania przepływu tych środków i materiałów drogą morską, lotniczą, lub lądową. Celem Inicjatywy jest również nawiązanie współpracy z każdym państwem, którego statki, bandery, porty, wody terytorialne, przestrzeń powietrzna, lub terytorium lądowe mogłyby być użyte do dokonania proliferacji przez państwa i struktury pozapaństwowe dokonujące proliferacji. Coraz bardziej agresywne próby podejmowane przez państwa i struktury dokonujące proliferacji w celu bycia wykluczonym z obowiązku przestrzegania lub obejścia istniejących norm nieproliferacji, i czerpania zysków z handlu opartego na proliferacji wymaga podjęcia nowych i bardziej zdecydowanych działań przez wspólnotę międzynarodową. Zasady przechwytywania dla Inicjatywy w sprawie Przeciwdziałania Rozprzestrzenianiu Broni Masowego Rażenia, mówi, że Uczestnicy Inicjatywy przestrzegają niżej wymienionych zasad przechwytywania w celu utworzenia bardziej skoordynowanych i skuteczniejszych podstaw w oparciu, o które można uniemożliwiać i zatrzymywać dostawy BMR, systemów przenoszenia i pochodnych materiałów do oraz z państw i struktur pozapaństwowych dokonujących proliferacji. Podstawy te powinny być zgodne z wytycznymi narodowych organów prawnych i właściwymi przepisami prawa międzynarodowego oraz zasadami struktur międzynarodowych, takich jak Rada Bezpieczeństwa ONZ. Apelują oni do wszystkich państw zaniepokojonych zagrożeniem światowego pokoju i bezpieczeństwa, aby przyłączyły się one do Inicjatywy, przyjmując tym samym następujące zobowiązania:

1. Podejmowanie skutecznych działań, indywidualnie lub wspólnie z innymi państwami, w celu: przechwytywania transferu lub transportu BMR, ich systemów przenoszenia, i pochodnych materiałów do oraz z państw i struktur pozapaństwowych dokonujących proliferacji. Określenie „państwa i struktury niepaństwowe dokonujące proliferacji" odnosi się na ogół to tych państw lub struktur, które według uczestników Inicjatywy powinny być poddane procedurze przechwytywania, ponieważ są zaangażowane w proliferację poprzez wysiłki skierowane na wytworzenie lub nabycie broni chemicznej, biologicznej lub jądrowej oraz związanych z nią systemów przenoszenia lub transfery (sprzedawanie, odbieranie lub ułatwianie dostępu do) BMR, ich systemów przenoszenia lub materiałów pochodnych.
2. Przyjęcie usprawnionych procedur szybkiej wymiany informacji dotyczących domniemanej działalności proliferacyjnej, ochrona tajemnicy informacji tajnych przekazywanych przez inne państwa jako ich wkład w Inicjatywę, przeznaczanie odpowiednich środków i podejmowanie wysiłków w ramach operacji oraz zdolności przechwytywania, oraz usprawnianie koordynacji pomiędzy uczestnikami działań mających na celu przechwytywanie.
3. Dokonanie przeglądu swoich sił oraz działanie na rzecz umocnienia właściwych narodowych organów prawnych tam, gdzie jest to konieczne dla osiągnięcia celów Inicjatywy, oraz działanie na rzecz umocnienia, w przypadku takiej konieczności, właściwych przepisów prawa międzynarodowego i struktur międzynarodowych w odpowiedni sposób, tak by służyły one wypełnianiu tych zobowiązań.
4. Podejmowanie konkretnych działań popierających wysiłki skierowanie na przechwytywanie ładunków BMR, ich systemów przenoszenia lub pochodnych materiałów, w stopniu, w jakim pozwalają na to ich narodowe organy prawne, oraz w zgodzie z ich zobowiązaniami w świetle prawa międzynarodowego oraz przynależności do międzynarodowych struktur, między innymi:
   - Zakaz transportu oraz nie wspomaganie transportu takich ładunków do oraz z państw i struktur pozapaństwowych dokonujących proliferacji, oraz zapewnienie, aby nie mogła podejmować takich działań żadna osoba podlegająca ich jurysdykcji.
   - Ze swojej własnej inicjatywy, lub na wniosek innego państwa, poparty dobrą intencją, podejmowanie działania zmierzającego do uzyskania zezwolenia na

wejście na pokład oraz przeszukanie każdego statku pływającego pod ich banderą na ich wodach wewnętrznych lub morzach terytorialnych lub na akwenach poza morzami terytorialnymi jakiegokolwiek innego państwa, co, do którego istnieje uzasadnione podejrzenie o transportowanie takich ładunków do oraz z państw i struktur pozapaństwowych dokonujących proliferacji, oraz przejmowanie takich ładunków po ich identyfikacji.

- Poważne rozważenie udzielenia zgody przy wymagających tego okolicznościach na wejście na pokład oraz przeszukanie statków pływających pod ich banderą przez przedstawicieli innych państw, oraz na przejmowanie ładunków, BMR, które znajdują się na tych statkach, jeśli będą one zidentyfikowane przez te państwa.
- Podjęcie odpowiednich działań by zatrzymać i/lub przeszukać na swoich wewnętrznych wodach, morzach terytorialnych, lub strefach przyległych, (jeżeli są one zadeklarowane), statków, na których ciąży uzasadnione podejrzenie o przewożenie takich ładunków do oraz z państw i struktur pozapaństwowych dokonujących proliferacji, oraz przejmowanie takich ładunków po ich zidentyfikowaniu oraz egzekwowanie wymogów, które muszą spełniać statki wpływające do lub wypływające z ich portów, wód wewnętrznych lub mórz terytorialnych, jeżeli istnieje uzasadnione podejrzenie, że statki te przewożą takie ładunki. Jednym z takich wymogów może być obowiązek umożliwienia wejścia na pokład, przeszukania, oraz przejęcia takich ładunków przed wejściem do portu.
- Ze swojej własnej inicjatywy lub na wniosek innego państwa, poparty dobrą intencją nałożenie na samoloty, które przekraczają ich przestrzeń powietrzną, a co, do których istnieje uzasadnione podejrzenie o przewożenie takich ładunków do oraz z państw i struktur pozapaństwowych dokonujących proliferacji, obowiązku wylądowania w celu przeprowadzenia inspekcji oraz przejęcie wszystkich takich ładunków po ich zidentyfikowaniu; i/lub odmówienie samolotowi, co, do którego istnieje uzasadnione podejrzenie o przewożenie takich ładunków prawa przelotu przez ich przestrzeń powietrzną przed rozpoczęciem takich lotów.
- Jeżeli ich porty, lotniska, lub inne obiekty są wykorzystywane jako punkty przeładunkowe do transportu takich ładunków do oraz z państw i struktur

pozapaństwowych dokonujących proliferacji, dokonywanie inspekcji statków, samolotów, lub innych środków transportu, co do których istnieje uzasadnione podejrzenie o przewożenie takich ładunków, oraz przejmowanie takich ładunków po ich zidentyfikowaniu.

Podsumowując, należy stwierdzić, że kwestia nieproliferacji, zarówno broni masowego rażenia, jak i środków jej przenoszenia stanowi do końca XX wieku przedmiot szczególnego zainteresowania społeczności międzynarodowej. Pomimo zaangażowania wielu państw i organizacji międzynarodowych, rozwiązanie problemu proliferacji broni jądrowej i środków jej przenoszenia zostaje nadal jednym z wyzwań dla bezpieczeństwa na ziemi. Potwierdzeniem tego faktu może być aktualny rozwój kryzysu nuklearnego wokół KRLD. Z punktu widzenia państw regionu Azji Północno – Wschodniej jego rozwiązanie będzie posiadać decydujące znaczenie dla układu sił w tej części świata. W ostatnich latach również zwiększyła się rola sił nuklearnych w strategii bezpieczeństwa i strategii wojennej, w kontekście pogarszania się stanu sił zbrojnych. W chwili obecnej broń jądrowa, potencjał nuklearny państw posiadających taki rodzaj broń jest podstawowym wyznacznikiem statusu mocarstwowości[9].

Można również dodać, że zarysowują się także pozytywne tendencje w rozwijaniu dialogu między NATO –Rosja. Państwa te dążą do współpracy w dziedzinie nuklearnej, a w szczególności w zakresie bezpieczeństwa broni jądrowej. Tak, więc kwestia rozbrojenia nuklearnego jest jednym z istotniejszych wyzwań dla bezpieczeństwa międzynarodowego. Obserwuje, się obecnie wzrost zainteresowania tą kwestią zwłaszcza w kontekście systemu zakazu prób broni jądrowe, zgodnie z Traktatem Całkowitym Zakazie Prób z Bronią Jądrową(CTBF) oraz Traktatu o Nierozprzestrzeniani się broni jądrowej (NPT). Państwa jądrowe rozpatrują proces rozbrojenia nuklearnego nie tylko z punktu widzenia zagrożeń, jakie stwarza broń jądrowa, ale także analizują ten problem w kontekście własnego bezpieczeństwa, dążenia do zachowania równowagi strategicznej, itp. Ponadto państwa jądrowe wyczulone są w większym stopniu na problem proliferacji broni jądrowej, traktując jako priorytet w stosunku do rozbrojenia nuklearnego. Kluczowego znaczenia w debacie o perspektywie rozbrojenia nuklearnego nabiera od kilku lat problematyka taktycznej broni jądrowej. Widoczny, jest brak postępu w tej dziedzinie, wskazując jako

[9] Por. P. Durys; *Kryzys nuklearny wokół KRLD*, A. Marszałek, Warszawa – Toruń 2003.

niechętną przyczynę państw nuklearnych. Można powiedzieć, że od 1991r. poszczególne elementy polityki nuklearnej podlegają ciągłej ewolucji i przemianom.

4.2. ROZPRZESTRZENIANIE BRONI BIOLOGICZNEJ

Bioterroryzm utożsamiany jest z bezprawnym, nielegalnym użyciem czynników biologicznych wobec ludzi, z zamiarem wymuszenia jakiegoś działania lub zastraszenia rządu, ludności cywilnej lub jakiejkolwiek jej części dla osiągnięcia celów osobistych, politycznych, społecznych lub religijnych[10]. Możliwość użycia broni biologicznej[11] stanowi istotne zagrożenie zarówno dla wojska, jak i dla ludności cywilnej, dlatego zasadnym jest mówić o tym w kontekście wojny biologicznej rozumianej jako specjalne zastosowanie osiągnięć nauki do rozsiewania na wybranym obszarze w populacji ludzkiej, zwierzęcej i roślinnej zarazków (bakterii, wirusów i grzybów) w celu zakażania, wywoływania chorób i zabijania ludzi oraz niszczenia środowiska naturalnego[12]. Zdaniem generała brytyjskiego Williama M. Creasy'ego z korpusu chemicznego sił zbrojnych USA (US Army Chemical Corps) wojna biologiczna jest „odwrotnością zdrowia publicznego"[13]. Użycie bakterii chorobotwórczych bądź innych środków biologicznych w celu umyślnego spowodowania chorób infekcyjnych ludzi, zwierząt i roślin jest powszechnie bardziej potępiane niż broń chemiczna[14].

Historia broni biologicznej sięga czasów prehistorycznych. Przedmioty, substancje lub ciała zawierające zarazki wykorzystywano w celu wywołania epidemii wśród wrogów od starożytności. Nieczystości, ciała zmarłych ludzi lub zwierząt używane były do zanieczyszczania żywności i zbiorników wody pitnej. Istnieje wiele zapisów historycznych o tym, że za pomocą maszyn oblężniczych i katapult wrzucano

---

[10] W. Gall, J. Grzybowisk, *Wybrane zagadnienia dochodzenia epidemiologicznego w przypadkach militarnego lub terrorystycznego ataku biologicznego.* W: Chomiczewski K, Grzybowski J, Gall W. (red.) *Epidemiologia działań wojennych i katastrof, a* Medica Press 2001; s. 66-82.

[11] Broń biologiczna to żywe organizmy (bakterie, wirusy, pierwotniaki, grzyby) oraz wytwarzane przez nie substancje, a także niektóre organizmy wyższe (zakażone owady, gryzonie), wraz ze środkami ich przenoszenia i rozprzestrzeniania, przeznaczone do wywoływania masowych chorób zakaźnych (epidemii ludzi, zwierząt i roślinności).

[12] L. Jabłoński, I. D. Karwat, *Bioterroryzm i wojna biologiczna-teoria i praktyka* [w:] *Zdrowie Publiczne* 2002, t. 112, nr 1, s. 112.

[13] S. Endicott, E. Hagerman, *The United States and Biological Warfare: Secrets from the Early Cold War and Korea*, Indiana University Press, Bloomington 1998, s. 63.

[14] Broń chemiczna to środki chemiczne (śmiercionośne i nie) przeznaczone do uśmiercania lub obezwładniania siły żywej przeciwnika. Zwykle paraliżują system nerwowy, wywołując czasową ślepotę, głuchotę, paraliż, nudności lub wymioty, silne poparzenia skóry, oczu lub płuc, a także utrudniając oddychanie. Do broni chemicznej zalicza się zarówno toksyczne substancje chemiczne, jak i środki ich przenoszenia i rozprzestrzeniania.

do obleganych miast trupy zwierząt oraz bieliznę i ubrania po zmarłych na zarazę ludziach. Po licznych, znanych odkryciach zarazków przez L. Pasteura, R. Kocha i dziesiątki innych badaczy w latach dwudziestych XX wieku wielu uczonych rozpoczęło badania nad zastosowaniem bakterii do unieszkodliwiania wojsk przeciwnika.

Od czasu zakończenia Zimnej Wojny dostrzega się większe możliwości użycia broni biologicznej. Niektórzy eksperci podkreślają jednak, że zmiana dotyczy postrzegania zagrożenia, a nie samego zagrożenia. Ryzyko zagrożenia bronią biologiczną pojedynczej osoby w ciągu jej życia jest niewielkie. Mając jednak w pamięci wydarzenia z 11 września 2001 r., należy stwierdzić, że prawdopodobne skutki nawet pojedynczego, precyzyjnie wykonanego ataku biologicznego mogą być zbyt wielkie, by można było je ignorować. Użycie takiej broni, nawet w odległym państwie, może być przyczyną przeniesienia choroby zakaźnej do innego państwa (a nawet kontynentu), czemu sprzyja szybkie i masowe przemieszczanie się ludzi. Niebezpieczeństwo broni biologicznej wynika również z faktu, jest ona łatwa do ukrycia i transportowania oraz bardzo łatwa w produkcji, np. przy wykorzystaniu drobnych laboratoriów, zakładów przemysłu farmaceutycznego i zakładów analitycznych[15]. Rozpowszechnienie broni biologicznej, a także łatwy dostęp do czynników chorobotwórczych i toksycznych sprzyjają użyciu ich w wojnie lub atakach terrorystycznych. Czynniki te można przenosić w bombach, głowicach rakiet oraz w specjalnych pociskach. Program przygotowań do wojny biologicznej jest łatwy do ukrycia, gdyż nie są potrzebne duże magazyny. Podczas wojny kraj, który prowadzi skomplikowane badania i produkuje broń biologiczną, nie musi mieć długo przechowywanych zapasów środków biologicznych. Taki kraj może produkować i wprowadzić gotową do użycia broń biologiczną otrzymaną w ciągu kilku tygodni z małej ilości środka biologicznego. Ponadto, inaczej niż w przypadku zakładów produkcji broni chemicznej i nuklearnej, środki biologiczne w ilości o znaczeniu militarnym mogą być produkowane w laboratorium nie większym niż przyczepa kempingowa. Ponadto broń biologiczna jest także tania. Koszt wywołania porównywalnych strat wśród ludności cywilnej na 1 km^2 przez broń konwencjonalną

[15] K. Chomiczewski, *Współczesne poglądy na zagrożenie bronią biologiczną* [w:] *Lekarz Wojskowy* 2002, t. 78, nr. 1, s. 5.

wynosi około 2 tys. USD, broń jądrową około 800 USD, a przez broń biologiczną -1 USD[16].

Dodatkowe niebezpieczeństwo wiąże się z wysoką skutecznością czynników biologicznych, co mogą ilustrować szacunkowe obliczenia wskazujące, że 50 kg form przetrwalnikowych (zarodnikowych) wąglika, rozpylonych w postaci aerozolu z wysokości 2tys. metrów na 500 tys. aglomerację miejską, może spowodować zgony u około 100tys. mieszkańców oraz 125 tys. zachorowań z szansami na przeżycie[17]. W odpowiednich warunkach bojowe środki biologiczne mogą skazić większy obszar niż taka sama ilość chemicznych bojowych środków trujących. Jak podają autorytatywne źródła, „symulacja komputerowa rozchodzenia się chmury aerozolowej przetrwalników wąglika wskazuje, że mogą one wywołać zakażenie w odległości większej niż 200 km od miejsca rozpylenia[18]. Niektóre czynniki chorobotwórcze można poddać specjalnej hodowli, a następnie manipulacjom genetycznym i w ten sposób zaostrzyć jeszcze ich zjadliwość. W latach osiemdziesiątych XX wieku uczeni radzieccy pracujący nad bronią biologiczną doskonalili pewne szczepy bakterii w celu uodpornienia ich na antybiotyki[19]. Ówczesna Rosja budowała tak zwane chimery wirusowe. Wirusy te powstawały w wyniku połączenia wirusa ospy prawdziwej i wenezuelskiego końskiego zapalenia mózgu[20]. Współczesne techniki bioinżynierii mogą być stosowane do ulepszania istniejących środków biologicznych i czynić z nich doskonałą broń biologiczną. Z jednej strony poprzez wprowadzenie zmian genetycznych można zwiększyć możliwość użycia czynników biologicznych jako środka bojowego. Z drugiej jednak strony, ponieważ tworzenie całkowicie nowych chorób jest szczególnie trudne, preparujący broń biologiczną wolą pracować ze środkami biologicznymi, które już wcześniej znalazły się w arsenałach. Ponadto, nie można przewidzieć, czy takie „mutanty" zanikną w naturalnej populacji, czy też wywołają epidemię lub endemię niemożliwą do opanowania. Następstwa i skutki dla biologicznego istnienia nie tylko gatunku homo sapiens, ale nawet życia na ziemi mogą okazać się katastrofalne, nie do opanowania.

---

[16] Tamże, s. 5.
[17] K. Chomiczewski, *op.cit.*, s. 5.
[18] E. M. Eitzen, *Use of Biological Weapons* [w:] F. R. Sidell, E. T. Takafuji i D. R. Franz (red.), *Textbook of Military Medicine, część I: Warfare, Weaponry, and the Casualty: Medical Aspects of Chemical and Biological Warfare*, Borden Institute, Walter Reed Army Medical Center, Washington 1997, s. 442.
[19] R. Preston, *The Bioweaponeers...*, s. 58.
[20] Tymże, s. 63.

Z punktu widzenia rozpoznania główna „wada" broni biologicznej tkwi w trudności jej wczesnego wykrycia, gdyż jest ona niewidzialna w czasie ataku. Atakować można skrycie, w podstępny sposób ze względu na trudności we wczesnym wykrywaniu przyczyny zachorowania lub zgonu. Chodzi o odpowiedź na pytanie, czy epidemia wybuchła z przyczyn naturalnych czy też w wyniku sztucznego rozsiewu zarazków. Szczególnie trudne jest to w warunkach niskiego poziomu sanitarnego w danej społeczności.

W prowadzonych działaniach zbrojnych czynniki biologiczne mogą być użyte w celu trwałego lub czasowego wyeliminowania sił przeciwnika – ludzi, zwierząt i roślin. W tym aspekcie Hurlbert z Uniwersytetu w Waszyngtonie w 1997 r. określił trzy rodzaje broni biologicznej, a następnie opublikował w Internecie (www.wsu.edu). Wyróżnił:

- drobnoustroje, które zakażają gospodarza, rozwijają się w nim i prowadzą do rozwoju choroby, która w konsekwencji niszczy gospodarza lub wywołuje jego niezdolność do działania;
- bioaktywne substancje pochodzenia biologicznego - to produkty metabolizmu drobnoustrojów, które zabijają gospodarza lub w nim się implantują. W tej grupie są toksyny i substancje, które wchodzą w przemiany z hormonami, neuropeptydarni i cytokinami;
- nowo wytworzone substancje biologiczno-mimetyczne - zaprojektowane i wyprodukowane substancje o działaniu biologicznym, czego przykładem mogą być gazy działające na układ nerwowy poprzez wpływ na docelowe receptory.

Z kolei Centers for Disease Control (CDC) dokonał podziału niebezpiecznych czynników biologicznych na następujące kategorie:

- kategoria A – patogeny najwyższego priorytetu, charakteryzujące się łatwością rozprzestrzeniania, a tym samym wywoływania wysokiej śmiertelności, co nakłada obowiązek specjalnego zabezpieczenia;
- kategoria B – patogeny najwyższego priorytetu drugiego rzędu o umiarkowanie łatwym rozsiewaniu i o umiarkowanej zachorowalności i umieralności, ale wymagające wzmożonego nadzoru;
- kategoria C – także patogeny najwyższego priorytetu trzeciego rzędu, do których należą patogeny nowo pojawiające się, mogące być przedmiotem manipulacji w zakresie inżynierii genetycznej w celu masowego rozsiewania. Są one

w zasadzie łatwo dostępne i łatwo rozprzestrzeniające się, a tym samym mogą powodować wysoką zachorowalność i śmiertelność[21].

Formy użycia czynników biologicznych wynikają przede wszystkim z możliwości technicznych i postawionych celów. Zakażenie bronią biologiczną odbywa się głównie przez drogi oddechowe, pokarmowe (skażoną żywność lub wodę) oraz przez otwarte rany. Poza bezpośrednim zaatakowaniem ludności, trzeba uwzględnić także możliwość niszczenia upraw roślinnych oraz wywołania epidemii groźnych chorób zakaźnych u zwierząt hodowlanych-stąd powstało już określenie agroterroryzm[22]. Skażenie powietrza, jako tzw. wariant aerozolowy, jest najbardziej niebezpieczne, ale jednocześnie najbardziej realne w użyciu przez bioterrorystów. Do rozpylenia drobnoustrojów chorobotwórczych drogą naturalną dochodzi bardzo rzadko. Niemniej jednak właśnie droga wziewna wiąże się z największym ryzykiem szerokiego rozprzestrzeniania się choroby. Wynika to z faktu, że większość czynników biologicznych łatwo może być przenoszona drogą powietrzną. Obiektami takiego ataku mogą być wszystkie miejsca, w których gromadzi się ludność, czyli przede wszystkim: centra handlowe, dworce kolejowe, porty lotnicze, stacje metra, obiekty kulturalne i sportowe, budynki publiczne i rządowe, miejsca koncentracji wojsk. Szczególnie dogodnymi miejscami do przeprowadzenia skutecznego ataku z użyciem aerozoli biologicznych są miejsca posiadające wydajne systemy klimatyzacyjne (stacje metra, budynki użytku publicznego). Pewnym ograniczeniem dla tego sposobu jest zagrożenie dla bioterrorysty. Z natury rzeczy bojowe środki biologiczne są czynnikami rażenia o opóźnionym działaniu. Czas, który musi upłynąć od użycia środka biologicznego do pojawienia się pierwszych objawów jego działania w populacji narażonej umożliwia ucieczkę z miejsca ataku i zatarcie śladów. Niektóre bardzo zaraźliwe czynniki biologiczne mogą powodować jednak tzw. efekt bumerangu (efekt powrotny) w stosunku do ich użytkownika. Jeżeli nawet państwo lub organizacja terrorystyczna jest skłonna rozdawać sprzęt do odkażania, odzież ochronną i urządzenia do wykrywania bojowych środków biologicznych w celu ochrony własnego personelu, to przynajmniej musi być on przeszkolony i wyposażony w narzędzia potrzebne do skutecznego dostarczania tych środków. Środki te, raz uwolnione, zwłaszcza przez źle wyszkolony lub niedoświadczony personel, przenoszone z wiatrem lub przy nagłej

---

[21] D.R. Franz, F.B. Jahring, A.M. Friedlander, et al. *Clinical recognition and management of pa-tients exposed to biological warfare agents.* JAMA 1997, 278/5, s. 399-411.

[22] K. Chomiczewski, op.cit., s. 6.

zmianie temperatury, mogą obrócić się przeciwko atakującemu. Od momentu „wypuszczenia" zarazków na atakowany obszar traci się nad nimi kontrolę i możliwość sterowania. W przypadku zajęcia takiego terenu przez wojska atakujące, narażają się one na zachorowanie i na następstwa rozsiewanej choroby. Skutki tego zjawiska stają się bowiem nieprzewidywalne nie tylko dla zaatakowanych, ale także dla atakujących. Skażenie wody i żywności jest łatwiejsze niż wariant aerozolowy. Do tego celu można użyć np. drobnoustroje chorobotwórcze, które w sposób naturalny szerzą się drogą pokarmową. Ten sposób zakażania jest mniej skuteczny pod względem masowości zakażeń. Jednak po wykonaniu tajnego ataku na urządzenia wodociągowe, np. w dużym mieście, można spodziewać się epidemii. Skutek zakażenia może nastąpić stosunkowo szybko lub po pewnym czasie[23]. Wrotami zakażenia może być także skóra. Forma skórna jest szczególnie zaraźliwa, gdyż strupy i resztki naskórka zawierają bakterie i przetrwalniki. Wąglik może przenikać przez rany lub małe zadrapania na skórze. W przypadku zakażenia skóry choroba z reguły ustępuje po 7-10 dniach, wytwarzając w organizmie niekiedy trwałą odporność.

Szerokie spektrum zagrożeń biologicznych i łatwość ich wywołania spowodowało konieczność regulacji prawnych w tym zakresie. Po raz pierwszy międzynarodowe inicjatywy prawodawcze na rzecz zakazu stosowania trucizn w celach militarnych podjęto w czasie Konferencji Pokojowych w Hadze w 1899 i 1907 r. Odrażający wizerunek, jaki zostawiła broń chemiczna po I wojnie światowej, przyczynił się do opracowania podstaw traktatu „O zakazie użycia na wojnie gazów duszących i bakteriologicznych metod prowadzenia działań wojennych". Naciski, jakie wywierała delegacja polska na Konferencji Genewskiej w 1925 r. spowodowały, że wspólnota międzynarodowa ratyfikowała Protokół Genewski podtrzymujący zakaz używania trujących i duszących gazów bojowych w czasie konfliktów zbrojnych. Zakazała także używania broni bakteriologicznej. Już 75 lat wcześniej, pomysłodawca tej inicjatywy, generał Kazimierz Sosnkowski, przewidując rozpowszechnienie się broni biologicznej ostrzegał: „Broń biologiczna może być produkowana łatwiej, taniej i w zupełnej tajemnicy"[24]. Dyplomatyczne wysiłki zapisane w Protokole Genewskim

[23] W 1982 r., w okresie epidemii na terenach rolniczych w północnej Tajlandii stwierdzono 24 przypadki wąglika jamy ustnej i gardła po spożyciu skażonego mięsa bawolego. W 1987 r., także w północnej Tajlandii, opisano 14 chorych na wąglika w postaci ustno-gardłowej lub jelitowej (C. Kunanusont, K. Limpakarnjanarat, H. M. Foy, *Outbreak of anthrax in Thailand*, Parasitol, 1989, s. 507-512.)

[24] J. Witt Mierzejewski, J. E. van Courtland Moon, *Poland and Biological Weapons* [w:] E. Geissler, J.E. van Courtland Moon (red.), *Biological and Toxin Weapons: Research, Development and use from the Middle Ages to 1945*, SIPRI Chemical & Biological Warfare Studies, no. 18, Oxford 1999, s. 66.

z 1925 r., mające na celu ograniczenie możliwości użycia broni biologicznej, zabraniały jej strategicznego rozmieszczenia, ale nie zakazywały produkcji, badań bądź magazynowania bojowych środków biologicznych. Stany Zjednoczone i Japonia nie podpisały Protokołu, a Wielka Brytania, Francja i Związek Radziecki zastrzegły sobie prawo odpowiedzi bronią biologiczną na podobny atak ze strony wrogiego państwa lub jego sojusznika. Pomimo włączenia do Protokołu aneksu odnośnie broni biologicznej, uzbrojenie biologiczne nie było powszechnie postrzegane jako zagrożenie[25].

Dynamiczny rozwój atomistyki po II wojnie światowej przyczynił się do utraty strategicznego znaczenia broni biologicznej na rzecz broni jądrowej. Dyskusję o rozbrojeniu podjęto ponownie w Genewie w 1959 r. W spotkaniach, które odbywały się w latach 1962-1968, uczestniczyła grupa państw nazwana Komitetem Rozbrojeniowym Osiemnastu Państw oraz Stany Zjednoczone i Związek Radziecki. Efektem końcowym tych rozmów był plan rozbrojeniowy, w którym proponowano likwidację broni biologicznej, chemicznej i jądrowej. Jednostronne rozbrojenie zainicjowane przez prezydenta Nixona stało się podstawą uzgodnienia w 1972 r. Konwencji Broni Biologicznej i Toksycznej (BTWC), którą Stany Zjednoczone ostatecznie ratyfikowały 22 stycznia 1975 r. Biological and Toxin Weapons Conventions (BTWC), podpisana w 1972 r. przez 70 państw, pozostaje do dnia dzisiejszego podstawowym aktem normatywnym, zakazującym „...udoskonalania, produkcji i przechowywania mikroorganizmów chorobotwórczych i innych czynników biologicznych lub toksyn w ilościach, które nie mogą być uzasadnione chęcią ich pokojowego użycia, jak również uzbrojenia, wyposażenia i innych środków mogących służyć do przenoszenia broni biologicznej i chemicznej w celu wrogiego jej użycia..."[26]. Konwencja weszła w życie 26 marca 1975 r., po podpisaniu i ratyfikowaniu jej przez znaczącą liczbę państw. Do dnia dzisiejszego liczba państw-sygnatariuszy konwencji wzrosła ponad dwukrotnie, obejmując około 75% krajów świata. Ratyfikowali ją m. in. wszyscy stali członkowie Rady Bezpieczeństwa ONZ i Irak[27].

Trzy akty prawne: 1) Biological Weapons Control Act (1989 r.), 2) Chemical and Biological Weapons Control Act (1991 r.) i 3) Anti-Terrorism Act (1996 r.) stanowią podstawę rozszerzenia wielopłaszczyznowego systemu obrony przed atakiem

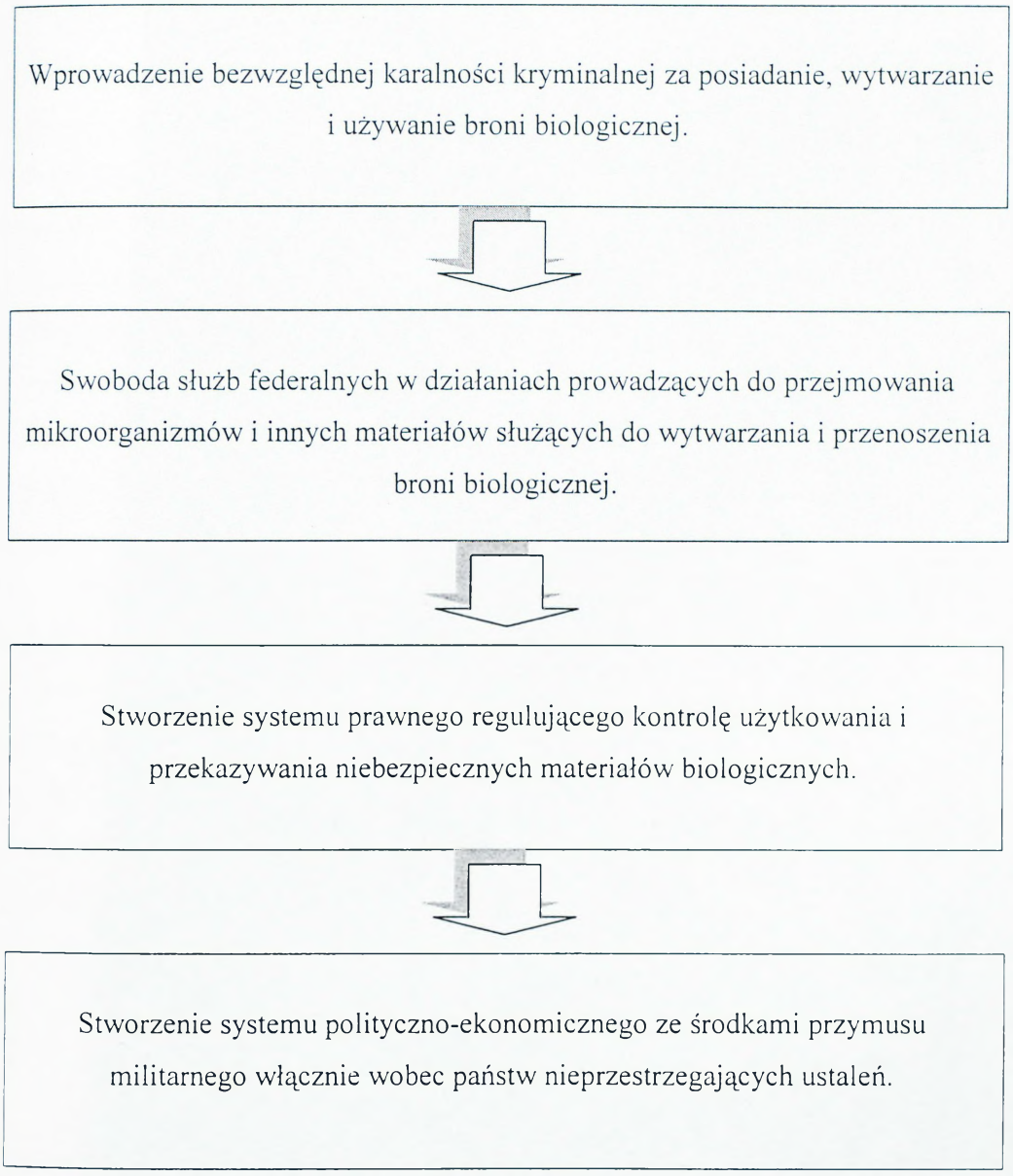
---

[25] Na przykład w 1933 r. major Leon Fox z armii Stanów Zjednoczonych utrzymywał, że współczesne środki zapobiegawcze mogłyby skutecznie przeciwstawić się broni biologicznej zastosowanej przeciwko Stanom Zjednoczonym. (E. Croddy, C. Perez-Armendariz, J. Hart, *op.cit*, s. 278).

[26] T. Targowski, T. Płusa, *op. cit.*, s. 10.

[27] Z. Dziubek, W. Basiak, *op.cit.*, s. 21.

biologiczno-chemicznym, opierającego się na czterech założeniach przedstawionych na rysunku 4.1.



Rysunek 4.1. Założenia systemu obrony przed atakiem bioterrorystycznym[28]

Obecnie nie ma możliwości skutecznej obrony większych zbiorowisk ludzkich przed skutkami użycia broni biologicznej. Szczepionki mogą zapobiegać wybranym chorobom, jednak ten sposób jest bezwartościowy, gdy czynnik biologiczny nie jest znany odpowiednio wcześniej. Podawanie antybiotyków może być nieskuteczne dopóki

[28] Źródło: T. Płusa, K. Jahnz-Różyk, *Broń biologiczna. Zagrożenie i przeciwdziałanie*, Medpress, Warszawa 2002, s. 18.

nie jest zidentyfikowany drobnoustrój i nigdy nie będzie skuteczne w sytuacji wykorzystania patogenów otrzymanych metodami inżynierii genetycznej. Postępy w dziedzinie biotechnologii i inżynierii genetycznej ułatwiają obecnie produkcję i obróbkę czynników zakaźnych. Używając prostych zautomatyzowanych urządzeń, można stworzyć broń biologiczną, zmniejszając jednocześnie ryzyko towarzyszące jej wytwarzaniu. Ponadto, dzięki zastosowaniu technologii genetycznych, w najbliższej przyszłości możliwe będzie prawdopodobnie wprowadzenie do mikroorganizmów i innych czynników zakaźnych zmian, które zwiększą ich zjadliwość, uczynią je bardziej odpornymi na antybiotyki i ochronne działanie szczepionek, a także ułatwią ich dystrybucję. Jednak nawet bez tych najnowszych osiągnięć terroryści posługujący się bronią biologiczną mogą w prosty sposób zarazić siebie samych śmiercionośnym czynnikiem zakaźnym i zapoczątkować epidemię, przebywając wśród ludzi, np. na lotnisku.

Rozwój biotechnologii i inżynierii genetycznej budzi obawy nie tylko ze względu na możliwość wykorzystania tych postępów w celach trucia ludzi lub celowego spowodowania rozprzestrzeniania się chorób, ale także z powodu przerażających wizji społeczno-politycznych skutków rewolucji biotechnologicznej. Rozwój genetyki i upowszechnianie się praktyk inżynierii genetycznej skłania człowieka do refleksji nad nimi w świetle zasad etycznych, wynikających z godności człowieka, jego doświadczenia i historii.

4.3. PRZEMYSŁ ZBROJENIOWY JAKO ŹRÓDŁO ZAGROŻEŃ

We współczesnych stosunkach międzynarodowych zbrojenia, ich regulacja i kontrola są czołowym problemem nurtującym społeczność międzynarodową. Siła nadal pozostaje jednym z zasadniczych elementów polityki zagranicznej państwa, służąc realizacji określonych potrzeb oraz interesów i przyczynia się do osiągania zamierzonych celów. Do najważniejszych atrybutów siły należy czynnik wojskowy. Parametry określające jego wartość, to możliwości demograficzne, ekonomiczne, organizacyjne i naukowo-techniczne. O możliwościach państwa świadczy jego przemysł zbrojeniowy, stan infrastruktury techniczno-obronnej, zaplecze logistyczne oraz wiele różnych elementów kształtujących poziom gotowości bojowej sił lądowych, morskich i powietrznych oraz rakietowych.

Obawy przed skutkami osiągnięcia przewagi przez potencjalnych przeciwników, dążenie do uzyskania równowagi sił lub zbudowania potencjału wojskowego dającego gwarancję sukcesu w obronie lub po dokonaniu napaści – to główne stymulatory zbrojeń. W tym kontekście należy stwierdzić, że siła militarna była i jest traktowana jako podstawowy czynnik bezpieczeństwa państwa.

Pamiętać należy, że po II wojnie światowej doszło do intensyfikacji zbrojeń. Zjawisko to występowało już w innych epokach, lecz nigdy przedtem w takim stopniu i na tak rozległą skalę. Pojawił się termin „wyścig zbrojeń" odnoszony do wzmożonej rywalizacji w dziedzinie militarnej, polegający na dążeniu państw do zwiększenia ilości lub jakości materialnych środków i zasobów koniecznych do prowadzenia działań wojskowych. Charakterystyczną cechą wyścigu zbrojeń jest jego zasięg. Uczestniczą w nim wszystkie regiony geopolityczne i większość państw. Znamionuje go szybkie tempo rozwoju uwarunkowane postępem w nauce i technice oraz rosnące wydatki. W swoim rozwoju wyścig zbrojeń przeszedł wiele etapów. Uczestniczyły w nim państwa Wschodu i Zachodu oraz państwa neutralne i niezaangażowane, nie należące do żadnych bloków wojskowych. W rezultacie wyścig zbrojeń uzyskał wymiar globalny, a następnie rozszerzony został na przestrzeń kosmiczną.

Tylko nieliczne państwa - jak na przykład Islandia czy Kostaryka - nie utrzymują sił zbrojnych. Osobliwym przypadkiem jest Japonia, którą obowiązuje konstytucyjny zakaz uczestniczenia w wojnie i zakaz utrzymywania narodowych sił zbrojnych. Japonia ma tylko liczące około 150 tys. żołnierzy tzw. siły samoobrony.

Mimo że coraz większy wpływ na siłę militarną państwa wywiera nowoczesna technika, niektóre państwa posiadają bardzo rozbudowane armie.

W latach dziewięćdziesiątych część tych armii została zredukowana. Na przykład w 1995 r. siły zbrojne Rosji zmniejszyły się do 2,2 mln, ChRL do 2,9 mln, RFN do 349,5 tys., i Polski do 235 tys., a Wietnam do 572 tys. żołnierzy. Do poziomu 590 tys. swoje siły zbrojne zredukowała również Turcja.

W wyniku dalszego zmniejszania stanu osobowego wojsk Rosji ich liczebność osiągnęła poziom 1,5 mln żołnierzy. Znaczne redukcje objęły również siły zbrojne państw członkowskich NATO. Zgodnie z przyjętymi planami przewidziano, że do końca 1997 r. m.in. Wielka Brytania zmniejszy swoją armię z 259 tys. do 241, Włochy z 325 tys. do 287 tys., Francja z 411 tys. do 371, RFN z 408 tys. do 300 tys., USA z 1 mln730 tys. do 1 mln 335 tys. żołnierzy.

W rozwoju jakościowym armii zaznaczyło się przechodzenie od tradycyjnej

triady sił militarnych, tj. wojsk lądowych, morskich i powietrznych, stanowiących siły konwencjonalne, do formacji wyposażonych w broń nuklearną, przenoszoną przez rakiety krótszego, średniego i dalekiego zasięgu. Triada atomowa to system wyrzutni rakiet przenoszących ładunki jądrowe na odległość do 5,5 tys. km. Rakiety dzielą się na międzykontynentalne rakiety balistyczne stacjonowane na lądzie (ICBM), rakiety balistyczne umieszczone na okrętach podwodnych (SLBM) oraz ciężkie bombowce dalekiego zasięgu przenoszące bomby nuklearne lub rakiety samosterujące zaopatrzone w ładunki nuklearne (ALCM).

Wyścig zbrojeń jest w dużej mierze przyspieszany przez postęp naukowo-techniczny. Miarą postępu w dziedzinie doskonalenia broni masowego rażenia jest m.in. wielogłowicowa rakieta MIRV (Multiple Independently Targetable Re-entry Vehicles). Głowice jądrowe tej rakiety są naprowadzane niezależnie na cel, co oznacza, że stosując ją można dokonać uderzenia jednocześnie na kilka lub kilkanaście celów odległych od siebie o kilkaset kilometrów. Udoskonalona wersja tej rakiety to MARV (Maneuverable Re-entry Vehicles), której poszczególne człony mogą dokonywać manewrowania w czasie lotu i mają zwiększoną celność.

Rywalizacja w dziedzinie zbrojeń doprowadziła do niebezpieczeństwa poszerzenia się ich zasięgu – co sygnalizowano na wstępie – na przestrzeń kosmiczną. W styczniu 1984 r. prezydent USA Ronald Reagan podpisał tajną dyrektywę nr 119 o bezpieczeństwie narodowym. Upoważniała ona do podjęcia szerokiego programu badawczego i rozwojowego systemu obrony rakietowej w kosmosie zwanego Inicjatywą Obrony Strategicznej (Strategic Defense Initiative – SDI), znanego też pod potoczną nazwą programu „gwiezdnych wojen". W 1985 r. na realizację tego programu przeznaczono 1,4 mld dolarów. W tym samym roku utworzono dowództwo sił kosmicznych Stanów Zjednoczonych. Po zakończeniu zimnej wojny USA odstąpiły od tego programu (1993 r.).

Część państw buduje swoje koncepcje bezpieczeństwa w oparciu o broń masowego rażenia. Coraz bardziej nowoczesne armie dysponują doskonaloną ustawicznie bronią różnego rodzaju, w tym bronią chemiczną. Według oficjalnych danych Rosja dysponuje zapasami broni chemicznej w ilości 40 tys. ton. W opiniach ekspertów zachodnich jest tej broni 60-70 tys. ton. Stany Zjednoczone mają w swoich arsenałach 32 tys. ton bojowych substancji trujących. Tę broń posiadają również Wielka Brytania i Chiny.

Rozwój nauki i techniki przyspiesza ewolucję procesu wytwarzania nowych

rodzajów uzbrojenia i wyposażenia sił zbrojnych. Wprowadzane są coraz doskonalsze rodzaje broni z wykorzystaniem osiągnięć elektroniki, nowych materiałów konstrukcyjnych, systemów napędowych i środków wybuchowych. Współczesną broń konwencjonalną nowej generacji charakteryzuje wyjątkowa precyzja działania, daleki zasięg, duża mobilność, niezależność od stanu pogody i pory dnia. Jest wyposażona w nowoczesne urządzenia komputerowe, fotooptyczne, optoelektroniczne, noktowizory, systemy kierowania, rozpoznania i łączności, a także mechanizmy pozwalające jej działać bez bezpośredniego uczestnictwa człowieka. Zastosowanie tej broni radykalnie zmienia sytuację na forum działań wojennych i na zapleczu przeciwnika, powodując straty niemniejsze aniżeli broń rakietowo-jądrowa. Wojna w Zatoce Perskiej w 1991 r. potwierdziła postęp w rozwoju broni konwencjonalnych nowej generacji.

Po raz pierwszy na masową skalę użyto tzw. „broni inteligentnej" na początku lat dziewięćdziesiątych. W produkcji tej broni zastosowano najnowsze osiągnięcia optoelektroniki, mechaniki precyzyjnej i inżynierii materiałowej. W ataku na Irak zimą 1991r. sprzymierzeni użyli bomb szybujących, naprowadzanych techniką telewizyjną, laserową lub techniką podczerwieni. Bomby sterowane laserowo, które stanowiły zaledwie 9% ogółu użytych bomb, spowodowały około 75% zniszczeń na terytorium irackim. Odpalono rakiety naprowadzające się na cel oświetlony laserem, radarem lub źródłem podczerwieni. Powszechnie stosowany sprzęt optoelektroniczny (termowizyjne urządzenia obserwacyjno-celownicze, lotnicze, czołgowe, artyleryjskie, lornetkowe dalmierze laserowe, etc.) umożliwiał wykrycie celu, rozpoznanie go i ostrzelanie w nocy. Taki poziom techniki wojennej praktycznie umożliwia prowadzenie działań bojowych przez 24 godziny na dobę.

Jednym z wielu kierunków rozwoju uzbrojenia jest konstruowanie broni o zmniejszonej śmiercionośności, przeznaczonej do czasowego wyłączenia z walki siły żywej przeciwnika i jego sprzętu wojskowego. Taka broń nie powoduje trwałego porażenia lub zniszczeń i powinna przyczyniać się do zmniejszenia ilości ofiar walk zwłaszcza wśród ludności cywilnej. Postęp naukowo-techniczny umożliwia prowadzenie badań i wyprodukowanie czterech rodzajów broni o zmniejszonej śmiercionośności:

- broń do zakłócania pracy optoelektronicznych systemów uzbrojenia (broń laserowa, promienniki laserowe, generatory promieniowania mikrofalowego dużej mocy);
- środki unieruchamiające broń samobieżną (substancje zwiększające kruchość

materiałów, wysokożrące i powodujące „superkorozję" , powodujące zmianę w spalaniu paliw oraz środki zakłócające pracę układów jezdnych pojazdów);

- broń do obezwładniania systemów dowodzenia, łączności, rozpoznania i kierowania (generatory impulsów elektromagnetycznych, generatory fal radiowych, wirusy komputerowe);
- broń do niszczenia infrastruktury i obezwładniania siły żywej (środki do uszkadzania linii energetycznych, elektrowni wodnych, bakterie o dużej aktywności, generatory infradźwięków, środki chemiczne i halucynogenne, holografia, środki metamorficzne).

Zjawiskiem nierozerwalnie związanym ze zbrojeniami jest handel bronią. Do czołówki eksporterów przez cały okres powojenny należeli stali członkowie Rady Bezpieczeństwa ONZ (USA, ZSRR, Wielka Brytania, Francja, Chiny). Drugą grupę państw eksporterów broni stanowiły: RFN, Włochy, Czechosłowacja, Hiszpania, Brazylia i Korea Południowa. Największymi dostawcami broni były ZSRR i USA. Należy zwrócić uwagę na kierunki eksportu. Większość dostaw amerykańskich skierowana była do Europy Zachodniej (Wielka Brytania, RFN, Holandia). Część przekazywano do państw Bliskiego Wschodu (Arabia Saudyjska, Izrael, Egipt) oraz Dalekiego Wschodu (Japonia, Tajwan, Korea Południowa). Poza tym odbiorcami uzbrojenia amerykańskiego były państwa Oceanii, Afryki, Azji Południowej oraz Ameryki Południowej i Północnej.

Zjawiskiem towarzyszącym nieodłącznie procesowi zbrojeń jest także, a może przede wszystkim, wysuwanie rozlicznych propozycji i postulatów, których celem jest kontrola zbrojeń. Początkowo termin ten stosowano w rokowaniach rozbrojeniowych dla oznaczenia jednej z form szeroko rozumianej kontroli międzynarodowej. Miały nią być objęte wynegocjowane ograniczenia zbrojeń i redukcja sił zbrojnych. Obecnie koncepcja regulacji zbrojeń opiera się na założeniu, iż istniejąca równowaga wojskowa jest najważniejszym czynnikiem bezpieczeństwa międzynarodowego. Można ją zapewnić, utrzymując potencjały militarne na istniejącym, niezmienianym poziomie. W toku takiego rozumowania mieści się opinia Andrzeja Towpika, który zaznaczył, że „[...] kontrola nad zbrojeniami prowadzi w kierunku, jeżeli nie odwrotnym, to w każdym razie innym niż rozbrojenie rozumiane jako ograniczenie i likwidacja zbrojeń". Pojmowanie pojęcia kontroli zbrojeń uległo znacznemu poszerzeniu i obejmuje różnorodne działania jedno- lub wielostronne, mające wpływ na zmniejszanie napięć w sferze stosunków militarnych między państwami, zmniejszanie

ryzyka wybuchu konfliktu zbrojnego na wielką skalę, zmniejszenie wydatków na cele wojskowe, tworzenie klimatu odprężenia i zaufania sprzyjającego budowie przesłanek dla rozbrojenia.

Uzyskanie powyższych celów staje się możliwe przy zastosowaniu następujących środków:

- współpracy międzynarodowej w sprawie pokojowego wykorzystania energii atomowej;
- rozrzedzenia zbrojeń (disengagement); stref bezatomawych i stref pokoju;
- stref zdemilitaryzowanych i zneutralizowanych; zakazie rozprzestrzeniania broni jądrowej;
- zakazie przeprowadzania doświadczeń z bronią jądrową; środków budowy zaufania.

Wszystkie z wymienionych środków z różnym skutkiem próbowano wykorzystać w praktyce międzynarodowej.

Wpływ przemysłu zbrojeniowego na życie gospodarcze i polityczne państw stale wzrasta. Warunki, jakie stwarzają mu poszczególne rządy, a także cele realizowane przez ich politykę zagraniczną i wewnętrzna sprzyjają ciągłemu rozwojowi tego przemysłu. W podrozdziale tym autorzy starali się wykazać dynamiczny rozwój przemysłu zbrojeniowego oraz jaki on ma wpływ na decyzje rządowe w sferze polityki wewnętrznej i zagranicznej, a także jego rolę w życiu gospodarczym państw i bloków, a także niebezpieczeństwa, jakie niesie z sobą wyścig zbrojeń.

Podkreślenia wymaga również fakt, że przemysł zbrojeniowy wrósł na trwałe w rzeczywistość a produkcja uzbrojenia i handel bronią stały się ważnym instrumentem polityki i gospodarki krajów.

WNIOSKI

Koniec zimnej wojny i upadek bipolarnego podziału świata przesądziły o zmianie globalnego środowiska bezpieczeństwa. Zaistniała sytuacja, która charakteryzuje się niskim stopniem zagrożenia militarnego, zwłaszcza w skali globalnej, ale też niskim poziomem bezpieczeństwa międzynarodowego[29]. Sytuacja, która jednocześnie wymaga szczególnego rozpoznania w systemie globalnego

[29] *Broń masowego rażenia w świetle prawa międzynarodowego. Wybrane problemy*, Praca zbiorowa, AON, Warszawa 2004.

bezpieczeństwa.

Wyłoniło się wiele nowych wyzwań i zagrożeń, które zmusiły analityków i strategów wojskowych do szeregu przewartościowań w zakresie planowania i prowadzenia współczesnych operacji – monitorowania globalnego bezpieczeństwa. Zmiana przedmiotowego zakresu bezpieczeństwa międzynarodowego oraz pojawienie się nowych kryteriów oceny bezpieczeństwa, uczyniły aktualnym pytanie o miejsce i rolę siły militarnej – zwłaszcza zaś broni masowego rażenia – w kształtowaniu stosunków międzynarodowych i bezpieczeństwa w pierwszych dekadach XXI wieku.

Kwestie bezpieczeństwa narodowego maja dla Polaków znaczenie szczególne. Wydarzenia, jakie nastąpiły po 1989 r., miały wpływ na sytuacje Europy Środkowej i Wschodniej, a także na układ geopolityczny świata. Polska, jako członek NATO stała się aktywnym propagatorem dalszego rozszerzenia Sojuszu. Jednocześnie RP wsparła inicjatywę zastosowania artykułu 5 Traktatu Waszyngtońskiego w odpowiedzi na ataki terrorystyczne 11 września 2001 r. Jako lojalny sojusznik przystąpiła także do koalicji antyterrorystycznej. Polscy żołnierze znajdują się m.in. w Afganistanie i Iraku. W związku ze zmianą sytuacji geostrategicznej zmieniło się także postrzeganie kwestii bezpieczeństwa narodowego.

Polacy w ślad za społeczeństwami Europy Zachodniej wyszli poza wąskie, polityczno-wojskowe rozumienie bezpieczeństwa narodowego. Coraz większego znaczenia nabrały pozostałe jego aspekty: gospodarcze, socjalne, ekologiczne i inne. Dlatego też, szczególnie pod kątem nowych wyzwań i zagrożeń, konieczne jest prowadzenie rozpoznania w systemie globalnego bezpieczeństwa.

Dokonana analiza ewolucji zagrożeń traktująca o broni masowego rażenia i przemyśle zbrojeniowym, wskazuje na znaczący w tym obszarze dorobek. Proces globalizowania się bezpieczeństwa oraz wzrost zagrożeń transnarodowych, jak również prawdopodobieństwo postępującej asymetrii, podpowiadają pilną potrzebę ciągłego śledzenia sytemu globalnego bezpieczeństwa, ale nade wszystko stworzenia i wcielania w życie instytucji prowadzącej monitoring ich przeobrażeń (ewolucji). Współczesne zagrożenia, z jakimi mamy obecnie do czynienia na świecie, powinny pobudzić społeczność międzynarodową oraz instytucje na rzecz egzekwowania pokoju w zakresie rozpoznania i przeciwdziałania rozprzestrzenianiu się broni masowego rażenia oraz rozwoju zagrożeń wynikających z handlu bronią.

5. ROZPOZNANIE W ŚRODOWISKU INFORMACYJNYM

Po doświadczeniach wyniesionych z konfliktów lokalnych siły zbrojne szeregu państw przykładają obecnie coraz większą wagę do rozwoju i budowy programów zmierzających do prowadzenia rozpoznania w środowisku informacyjnym[1]. Działalność rozpoznawcza prowadzona w przestrzeni fal elektromagnetycznych (ale nie tylko) jest tym rodzajem rozpoznania, które zaczęło stanowić dominującą rolę na współczesnym polu walki. Złożoność środowiska informacyjnego spowodowała, że systemy elektroniczne występują już nieomal w każdej rzeczy nas otaczającej. Nie inaczej jest w środowisku wojskowym. Powszechność zastosowania elektroniki stała się faktem, dlatego każda armia w większym lub mniejszym stopniu wykorzystuje zdobycze techniki elektronicznej. Nawet oddziały partyzanckie, nieregularne, przestępcze (terroryści) bez środków elektronicznych (przede wszystkim środków telekomunikacji) nie mogą działać.

Efektywne wykorzystanie współczesnych sił i środków walki w działaniach bojowych (obrona, natarcie, działania opóźniające, asymetryczne) jest możliwe pod warunkiem posiadania aktualnych informacji o położeniu i działaniu sił przeciwnika w całym obszarze działania. Może to zapewnić jedynie należycie zorganizowany system rozpoznania wykorzystujący różnorodne środki, zdolne do pozyskiwania danych w całym obszarze operacyjnym lub taktycznym.

W obszarze operacyjnym może działać bardzo wiele różnych systemów elektronicznych powiązanych odpowiednią siecią informacyjną lub teleinformacyjną, tworząc sieci przysyłania danych, dlatego system rozpoznania elektronicznego w wojskach lądowych powinien występować organizacyjnie na wszystkich szczeblach dowodzenia do pododdziału włącznie. Tak organizowany system pozwala efektywnie wykorzystać różnorodne środki rozpoznania, i zapewnia napływ danych na potrzeby oceny sytuacji i środków rażenia. Jednakże o rzeczywistych możliwościach tak zorganizowanego systemu decydują indywidualne możliwości wykorzystywanych środków rozpoznawczych oraz relacje informacyjne w tym systemie.

Zakładając, że rozpoznanie w działaniach asymetrycznych ma bardzo szeroki zakres i może być realizowane w różnych strefach zarówno przedniej, głównej, jaki i tyłowej, to

[1] Np.: USA, WB, Francja, Federacja Rosyjska.

w odniesieniu do rozpoznania elektronicznego strefy te dzielimy na dwie: tam gdzie działają urządzenia przeciwnika, czyli strefę odpowiedzialności rozpoznawczej (w odniesieniu do rozpoznania elektronicznego - WE) i tyłową strefę działania. W każdej z tych stref będzie realizowane rozpoznanie elektroniczne, ale w każdej na inne sposoby będzie położony główny nacisk i inne będą priorytety użycia elektronicznych podsystemów rozpoznawczych. Poszczególne zadania rodzajów rozpoznania będą zmieniały się w zależności od rozwoju sytuacji.

5.1. ROZPOZNANIE ELEKTRONICZNE W DZIAŁANIACH ASYMETRYCZNYCH

Literatura przedmiotu definiuje rozpoznanie elektroniczne jako: zdobywanie, analizowanie i ocenianie informacji o przeciwniku, terenie, warunkach meteorologicznych i rejonie przyszłych działań, niezbędnych do skutecznego prowadzenia wojny, operacji lub walki[2]. Dodając określenie „elektroniczne", można wówczas zdefiniować rozpoznanie elektroniczne jako: zdobywanie i przetwarzanie tych treści informacyjnych o przeciwniku, których nośnikami są fale elektromagnetyczne, przebiegi elektryczne oraz inne efekty uboczne towarzyszące działaniom bojowym, na przykład: akustyczne, sejsmiczne, magnetyczne, chemiczne itp.[3]. Należy jednak zauważyć, iż rozpoznanie elektroniczne traktowane jest niekiedy w innym ujęciu, a mianowicie rzeczowym, i wówczas mówi się o zbiorze sił i środków[4].

Rozpoznanie elektroniczne, będąc jednym z elementów składowych rozpoznania wojskowego, jest rozpoznaniem pośrednim (bez rozpatrywania rozpoznania radiolokacyjnego), rozumianym jako zespół sił i środków rozpoznania dostosowanych do zdobywania treści informacyjnych (informacji potencjalnych) w postaciach bezpośrednio nieodbieranych przez układ recepcyjny człowieka.

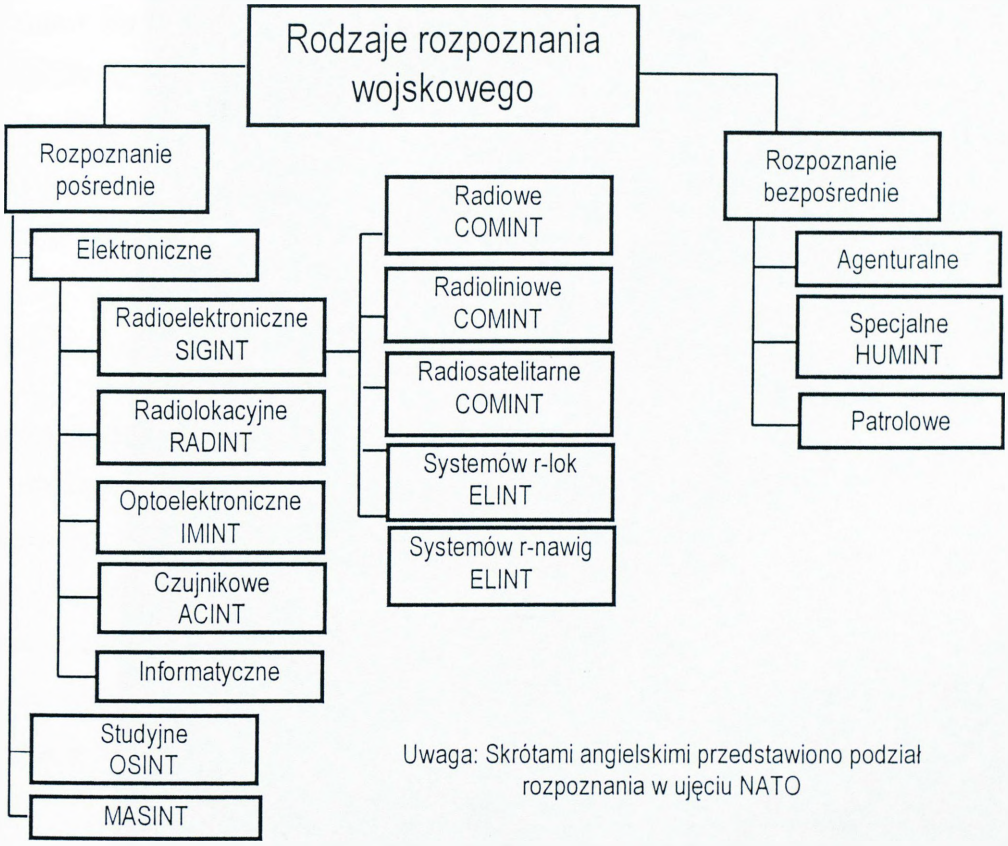
Rozpoznanie elektroniczne prowadzi się w każdej porze dnia i w każdych warunkach atmosferycznych, bez względu na usytuowanie środków rozpoznania elektronicznego, które nie powoduje istotnego zróżnicowania wartości uzyskanych efektów[5]. Jest skrytym rodzajem rozpoznania, ale podatnym na zakłócenia. Dane uzyskane w wyniku

---

[2] *Leksykon wiedzy wojskowej...*, s. 372.
[3] M. Łokociejewski, *Taktyczny system rozpoznania i walki elektronicznej wojsk lądowych,* Warszawa, AON 2000, s. 63.
[4] L. Ciborowski, *Rola i miejsce rozpoznania w systemie obronnym Rzeczypospolitej Polskiej,* Warszawa, AON 1993, s. 17.
[5] J. Kisiel, *Rozpoznanie wojskowe,* Warszawa, AON 1998, s. 58.

prowadzonego rozpoznania elektronicznego dotyczą parametrów technicznych emisji oraz położenia i działalności bojowej środków elektronicznych przeciwnika. Zdobyte w ten sposób informacje o przeciwniku są wykorzystywane do realizacji zadań walki elektronicznej, ale nie tylko, także do wsparcia ogniowego oraz wypracowania decyzji w procesie informacyjnego i elektronicznego przygotowania pola walki. Rozpoznanie elektroniczne dzieli się na:

- rozpoznanie radioelektroniczne,
- rozpoznanie radiolokacyjne,
- rozpoznanie optoelektroniczne,
- rozpoznanie czujnikowe
- rozpoznanie informatyczne.



Rys. 5.1. Rodzaje rozpoznania wojskowego w ujęciu polskiej doktryny rozpoznawczej i opracowaniu akademickim

Źródło: Łokociejewski M., (red), Rozpoznanie Wojskowe, cz 1 Podstawy teoretyczne, AON, Warszawa 2003

Przedstawiony na rys 5.1. podział rozpoznania wojskowego zawiera połączenie rodzajów rozpoznania z ww. opracowania z ich odpowiednikami sojuszniczymi zgodnie z doktryną rozpoznawczą. Z schematu wyraźnie wynika, iż rozpoznanie informatyczne nie ma swojego odpowiednika w ujęciu systematyki NATO. Taki stan rzeczy jest głównie związany

z występowaniem tego rodzaju działań w walce informacyjnej jako odrębnego rodzaju prowadzenia działań. W polskiej teorii działań informacyjnych tego typu działania nie występują. Dlatego, autorzy adaptowali założenie, iż przy obecnym poziomie wiedzy można przyporządkować rozpoznanie informatyczne do ogólnego rozpoznania elektronicznego. Występują również inne poglądy klasyfikujące i przyporządkowujące rozpoznanie informatyczne. Niektórzy teoretycy wojskowi, sugerują, iż rozpoznanie informatyczne należy przyporządkować do rozpoznania studyjnego (odpowiednik NATO - OSINT rozpoznanie ze wszystkich dostępnych źródeł). Zespół badawczy stoi jednak na stanowisku, iż konieczne jest wyodrębnienie tego typu rozpoznania jako osobnego z uwagi iż działa on w środowisku elektronicznym i podlega prawom przepływu energii elektromagnetyczne (przynajmniej w jej części). Na tym poziomie wiedzy takie założenie jest słuszne i wystarczające.

W literaturze przedmiotu spotyka się także inne podziały rozpoznania elektronicznego, np. u J. Kisiela, który wymienia tylko rozpoznanie radioelektroniczne, radiolokacyjne i czujnikowe. Jednak zdaniem zespołu badawczego, przedstawiony wyżej podział jest pełny zarówno ze względu na metody pracy środków elektronicznych, jak i zastosowane środki.

5.1.1. Charakterystyka rodzajów rozpoznania elektronicznego

Rozpoznanie radioelektroniczne (SIGINT)

Rozpoznanie radioelektroniczne zdefiniowane jest jako ogół przedsięwzięć organizacyjnych i technicznych, wzajemnie powiązanych celem, miejscem i czasem, które umożliwiają zdobywanie danych o środkach promieniujących energię elektromagnetyczną[6]. Źródłami rozpoznania radioelektronicznego są wszystkie środki pracujące w systemach łączności radiowej (KF i UKF, łączności radioliniowej, łączności satelitarnej) oraz w systemach radiolokacyjnych i radionawigacyjnych. Rozpoznanie radioelektroniczne[7] dzieli się na:

1) radiowe(COMINT):
   a) KF,
   b) UKF,
   c) rozpoznanie łączności radioliniowej,
   d) rozpoznanie łączności satelitarnej,
2) sygnałów radiolokacyjnych (ELINT),

[6] J. Janczak, *Kierunki rozwoju rozpoznania i zakłócania elektronicznego,* Warszawa, AON 2001, s. 18.
[7] J. Janczak, *Kierunki...*, s. 43-89.

3) sygnałów radionawigacyjnych (ELINT).

Rozpoznanie radioelektroniczne dostarcza różnych treści informacyjnych o przeciwniku i jego środkach radioelektronicznych.

W systemie rozpoznania wojskowego szczebla operacyjnego rozpoznanie radioelektroniczne jest istotną częścią rozpoznania pośredniego lub, rozpatrując problem z punktu widzenia urządzeń technicznych, rozpoznania technicznego. Prowadzi się je za pomocą urządzeń rozpoznawczych w wyselekcjonowanych pasmach widma elektromagnetycznego wykorzystywanych przez środki przeciwnika.

Rozpoznanie radiowe jest rodzajem rozpoznania radioelektronicznego, które obejmuje środki łączności radiowej i środki zakłócające tę łączność. Ma na celu zdobycie informacji o stanie ilościowym i jakościowym tych środków, miejscu ich rozmieszczenia i sposobach wykorzystania. Owe środki mogą pracować w systemach łączności radiowej krótkofalowej (KF) i ultrakrótkofalowej (UKF), łączności radioliniowej (horyzontowej i pozahoryzontowej) oraz łączności satelitarnej[8].

Rozpoznanie radiowe zdobywa informacje o przeciwniku za pomocą takich urządzeń, jak: odbiorniki radiowe i namierniki radiowe. Jego zadaniem jest zdobywanie informacji o składzie, ugrupowaniu, działaniach i zamierzeniach przeciwnika, analizowanie zdobytych treści informacyjnych oraz uogólnianie i odtwarzanie sytuacji operacyjnej i bojowej wojsk przeciwnika.

Obiektami rozpoznania radiowego są stanowiska dowodzenia, węzły łączności oraz radiowe systemy rozpoznania i kierowania uzbrojeniem. Źródłami dla rozpoznania radiowego są również urządzenia łączności znajdujące się w obiektach rozpoznania radiowego, zaspokajające potrzeby dowodzenia, współdziałania, rozpoznania oraz kierowania uzbrojeniem.

Obiektami rozpoznania radiowego mogą być także środki radiowe łączności komórkowej bardzo powszechnie wykorzystywanej przez różnego rodzaju grupy dywersyjne lub przestępcze o charakterze terrorystycznym. Do tej grupy źródeł rozpoznania można także zaliczyć środki radiowe inicjujące zdalnie odpalane ładunki wybuchowe, które w strefie tyłowej mogą poczynić poważne zniszczenia.

Rozpoznanie sygnałów radiolokacyjnych jest kolejną częścią składową rozpoznania radioelektronicznego, w którym przedmiotem rozpoznania są pracujące stacje radiolokacyjne (SRL) przeciwnika.

---

[8] *Walka elektroniczna w działaniach taktycznych wojsk lądowych,* pod red. J. Janczaka, Warszawa, AON 1999, s. 34.

Rozpoznanie sygnałów radiolokacyjnych polega na zdobywaniu danych o środkach radiolokacyjnych: rozpoznania pola walki, artylerii, środków napadu powietrznego, okrętów, OP i OPL. Realizuje się je przez poszukiwanie, przechwytywanie i analizę sygnałów wypromieniowanych przez te środki oraz ich umiejscowienie. Wykrycie środków radiolokacyjnych przeciwnika, dzięki analizie operacyjno-taktycznej umożliwia ustalenie rozmieszczenia jego SRL, a jednocześnie posterunków rozpoznania pola walki, pododdziałów i oddziałów artylerii ze stanowiskami dowodzenia i kierowania, posterunków radiotechnicznych OP i innych obiektów ugrupowania przeciwnika.

Aby nastąpiło wykrycie pracującego źródła promieniowania radiolokacyjnego, muszą być spełnione warunki: energetyczny, częstotliwościowy, przestrzenny oraz czasowy. Warunki te określają możliwości prowadzenia rozpoznania sygnałów radiolokacyjnych oraz mają zasadniczy wpływ na rozwiązania konstrukcyjne i sposoby działania urządzeń rozpoznawczych. Szczególne znaczenie dla możliwości poszukiwania i wykrywania stacji radiolokacyjnych mają warunki: przestrzenny i częstotliwościowy, ponieważ wykrycie źródła emisji następuje w kierunku i w częstotliwości[9].

Rozpoznanie sygnałów radionawigacyjnych to sposób prowadzenia rozpoznania polegający na wykrywaniu sygnałów i lokalizacji środków radionawigacyjnych wykorzystywanych przez przeciwnika.

System radionawigacyjny tworzy zespół współpracujących z sobą specjalnych urządzeń (radionawigacyjnych), rozmieszczonych na ziemi i na obiektach ruchomych (samoloty, okręty, sztuczne satelity Ziemi). Przeznaczony on jest do zapewnienia prawidłowego poruszania ruchomych obiektów po wyznaczonych trasach, ich naprowadzania na określone punkty terenowe oraz do kontroli własnego położenia, dowiązywania stanowisk i obiektów itp[10], dlatego dokładne umiejscowienie środków radionawigacji pozwala zidentyfikować sposób zabezpieczenia lotnictwa przeciwnika w czasie nalotu.

Rozpoznanie radiolokacyjne (RADINT)

Rozpoznaniem radiolokacyjnym nazywa się proces wykrywania obiektu ruchomego i nieruchomego w przestrzeni powietrznej, naziemnej, morskiej lub kosmicznej oraz pomiar jego współrzędnych i parametrów ruchu za pomocą stacji radiolokacyjnej[11].

W rozpoznaniu radiolokacyjnym wykorzystane jest zjawisko odbicia fal radiowych od obiektów (celów) znajdujących się w powietrzu, na morzu lub na lądzie oraz

---

[9] J. Janczak (red) *Walka elektroniczna w działaniach taktycznych związku taktycznego*, AON, Warszawa 2000, s. 22.
[10] Tamże, s. 32.
[11] *Walka elektroniczna w działaniach taktycznych wojsk* ..., s. 59.

promieniowanie odzewowe, a także emisja „własna" obiektów (każde pracujące urządzenie elektroniczne emituje energię elektromagnetyczną). Właściwości te stosowane są do wykrywania oraz pomiaru współrzędnych i parametrów ruchu celów radiolokacyjnych. Obszarem prowadzonego rozpoznania jest przestrzeń otaczająca stację radiolokacyjną.

Radiolokacja opiera się na zasadzie prostolinijnego rozprzestrzeniania się fal radiowych ze stałą prędkością w środowisku jednorodnym. Ta właściwość umożliwia określenie współrzędnych obiektu oraz parametrów ruchu lub wielkości bryłowej obiektu.

Wszystkie obiekty, które mogą być wykryte za pomocą fal radiowych (samoloty, okręty, rakiety, infrastruktura naziemna, chmury itp.), a nie są obiektami własnymi, nazywane są celami radiolokacyjnymi, zaś sygnał odbity od tych obiektów - echem radarowym lub echem radiolokacyjnym. Rozpoznanie radiolokacyjne wykorzystuje się do: rozpoznania obszaru powietrznego, nadzorowania pola walki, kierowania ogniem, obrony przeciwlotniczej oraz rozpoznania powierzchni ziemi[12].

Wyróżnia się dwa sposoby prowadzenia rozpoznania radiolokacyjnego: pasywne i aktywne. Rozpoznanie radiolokacyjne pasywne polega na odbiorze energii elektromagnetycznej emitowanej przez obiekty przeciwnika w sposób niezamierzony lub zamierzony[13], natomiast aktywne wykorzystuje własne środki emitujące w sposób celowy energię elektromagnetyczną.

Rozpoznanie optoelektroniczne (IMINT)

Rozpoznanie optoelektroniczne ma na celu zdobywanie oraz przetwarzanie tych treści rozpoznawczych o przeciwniku, których nośnikami są fale elektromagnetyczne pasma optycznego (zakresu optycznego), stanowiącego promieniowania: ultrafioletowe (długość fali: 0,01-0,38 μm), widzialne (długość fali: 0,38-0,76 μm) i podczerwone (długość fali: 0,76-1000 μm)[14]. Podstawą rozpoznania optoelektronicznego są fizyczne procesy warunkujące przetwarzanie sygnałów elektrycznych na optyczne i sygnałów optycznych na elektryczne oraz procesy wytwarzania informacji niesionych przez światło.

Do pracy w tym paśmie wykorzystuje się rodzinę urządzeń optoelektronicznych pozwalających na prowadzenie rozpoznania w zakresie promieniowania ultrafioletowego, w zakresie promieniowania widzialnego oraz w podczerwieni. W rozpoznaniu optoelektronicznym wykorzystuje się urządzenia:

- telewizyjne,

---

[12] M. Łokociejewski, *Taktyczny* ..., s. 68.
[13] W literaturze przedmiotu jest to rodzaj rozpoznania sygnałów radiolokacyjnych.
[14] *Walka elektroniczna w działaniach taktycznych wojsk* ..., s. 39.

- termowizyjne,
- noktowizyjne,
- laserowe.

Urządzenia telewizyjne przekazują na odległość, za pomocą elektrycznego kanału łączności, obrazy ruchome wraz z towarzyszącym dźwiękiem[15].

Urządzenia termowizyjne umożliwiają tworzenie obrazów widzialnych dla oka ludzkiego przetworzonych z obrazów w widmie promieniowania podczerwonego.

Urządzenia noktowizyjne umożliwiają obserwację obiektów w podczerwieni. Noktowizja wykorzystuje promieniowanie własne obiektów (wszystkie ciała, których temperatura jest wyższa od zera bezwzględnego, wysyłają własne niekoherentne promieniowanie podczerwone) lub odbite. W związku z tym przyrządy noktowizyjne dzieli się na pasywne i aktywne[16].

Urządzenia laserowe wykorzystują monochromatyczne fale elektromagnetyczne zakresu optycznego.

Rozpoznanie czujnikowe (ACINT)

Rozpoznanie czujnikowe to zdobywanie informacji, których nośnikami są wszelkiego rodzaju efekty uboczne towarzyszące działaniom zbrojnym, dające się rejestrować za pomocą różnego rodzaju urządzeń elektronicznych (czujników) i przetwarzać na sygnały elektromagnetyczne[17].

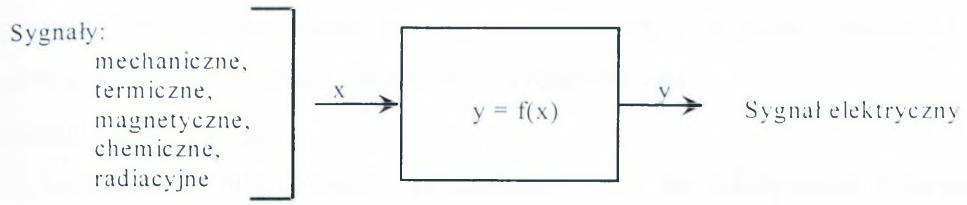
Czujnik jest odbiornikiem informacji ze świata zewnętrznego i odwzorowuje w sposób jednoznaczny wejściowy sygnał nieelektryczny (fizyczny lub chemiczny) na wyjściowy sygnał elektryczny. Funkcja f(x), opisująca wzajemnie jednoznaczne przyporządkowanie między wielkością wejściową x i wyjściową y, nosi nazwę funkcji przetwarzania (rys. 5.2.). Wielkościami wejściowymi mogą być np. wielkości mechaniczne, termiczne, magnetyczne, chemiczne i radiacyjne, natomiast wyjściowymi są przeważnie sygnały elektryczne[18].

Tworząc matrycę czujników (wykorzystując kilka czujników odbierających różne sygnały zewnętrzne), można zdobywać informacje lub treści informacyjne z otoczenia, dotyczące działalności przeciwnika w danym rejonie. Sposób ten gwarantuje zbieranie danych

---

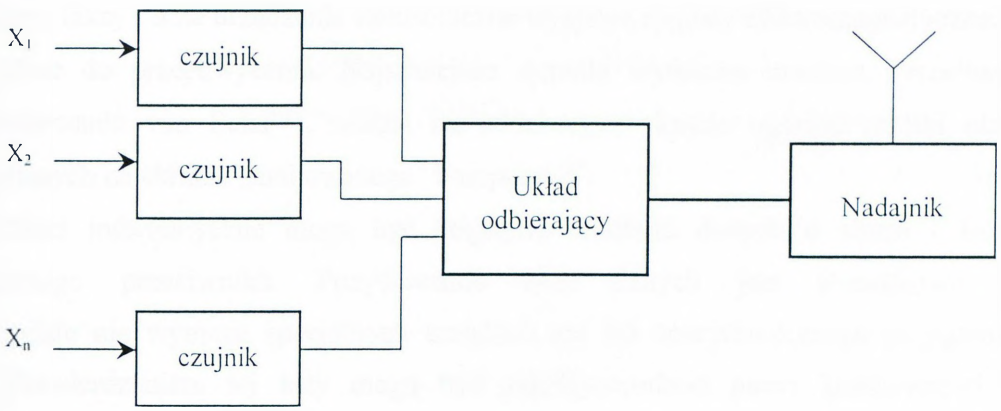
[15] *Encyklopedia techniki wojskowej,* Warszawa, MON 1978, s. 728.
[16] J. Janczak, *Kierunki ...*, s. 105.
[17] L. Ciborowski, *Rozpoznanie i walka elektroniczna*, Warszawa, AON 1993, s. 59.
[18] http: //www.imm.org.pl/czujniki inteligentne.htm

na podstawie niezależnych od siebie skutków ubocznych towarzyszących działaniom wojsk (rys. 5.3.).



Rys. 5.2. Funkcja przetwarzania

Źródło: http://www.imm.org.pl/Czujniki inteligentne.htm



Rys. 5.3. Matryca czujników z możliwością przesyłania danych

Źródło: opracowanie własne

Dzięki czujnikom drgań akustycznych lub sejsmicznych, czujnikom ciśnienia można wykryć strzały i ruchy dużych maszyn. Posługując się czujnikami magnetycznymi, można rozróżnić na podstawie wagi i składu stali różne rodzaje pojazdów. Czujniki chemiczne umożliwiają wykrycie obecności i ruchów dużych ssaków oraz wykrycie niektórych działań przemysłowych[19].

Wykorzystując parametry sygnału elektrycznego wyjściowego, przesyłając go drogą radiową do „centrum analizy danych", można zdalnie monitorować:

1. Aktywność przeciwnika w wybranych rejonach,
2. Natężenie ruchu i poziomu aktywności przeciwnika wzdłuż wybranych tras,
3. Aktywność przeciwnika w rejonach przepraw rzecznych, mostów i brodów,
4. Rejony umożliwiające lądowanie desantów przeciwnika,
5. Zmiany w funkcjonowaniu wybranych elementów ugrupowania przeciwnika,

[19] D. E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa, WNT 2002, s. 217.

6. Cele do rażenia ogniowego lub szczegółowego rozpoznania.

Rozpoznanie czujnikowe jest perspektywicznym rodzajem rozpoznania na szczeblu taktycznym, bowiem umożliwia pozyskiwanie danych z rejonów niedostępnych innym rodzajom rozpoznania w czasie zbliżonym do rzeczywistego.

Rozpoznanie informatyczne

Rozpoznanie informatyczne przeznaczone jest do zdobywania informacji, które znajdują się w systemach (sieciach) komputerowych. Realizowane jest poprzez włamania do systemu i przechwyt treści w nich przechowywanych lub odbiór promieniowania elektromagnetycznego urządzeń informatycznych. Komputery, monitory, drukarki, klawiatury, faksy i inne urządzenia elektroniczne wysyłają sygnały elektromagnetyczne, które są możliwe do przechwycenia. Najsilniejsze sygnały wytwarza monitor. Przechwytując „promieniowanie van Ecka"[20], można na oddzielnym ekranie oglądać repliki obrazów wyświetlanych na ekranie „atakowanego" komputera[21].

Sieci informatyczne mogą być bogatymi źródłami danych o siłach i środkach potencjalnego przeciwnika. Pozyskiwanie tych danych jest stosunkowo łatwe i w zasadzie nie wymaga specjalnych urządzeń ani też specjalistycznego przygotowania załóg. Potwierdzeniem tej tezy mogą być międzynarodowi piraci komputerowi (ang. *hackers),* którzy bez większych przeszkód włamują się do dobrze zabezpieczonych systemów komputerowych. Nie trzeba zatem być bogatym państwem z rozbudowanym zapleczem naukowym, technicznym i technologicznym, aby skutecznie prowadzić rozpoznanie informatyczne[22].

Rozpoznanie informatyczne może być realizowane przez podsłuch bierny i podsłuch czynny[23]. Podsłuch bierny polega na zdobywaniu danych z systemów informatycznych, zazwyczaj bez wykrycia tego faktu przez podsłuchiwanego. Informacje są kopiowane na nośniki informacji dokonującego podsłuch. W sieciach komputerowych można śledzić przepływ informacji i na tej podstawie ustalać strukturę systemu łączności. Podsłuch czynny polega na celowym modyfikowaniu strumienia danych.

Na bazie wymienionych rodzajów rozpoznania organizowane są podsystemy będące częścią składową działań systemu walki elektronicznej. Nie wszystkie będą realizowane w każdych działaniach. Również na nie wszystkie są wystarczająco wyposażone środki

[20] Holenderski naukowiec, profesor Wim van Eck, opublikował w 1985 r. pracę, w której ocenia, że maksymalna odległość odbioru promieniowania elektromagnetycznego monitora przy posługiwaniu się normalnym odbiornikiem telewizyjnym wynosi około 1 km. Od tego czasu przyjęło się nazywać sygnały wysyłane przez te urządzenia „promieniowaniem van Ecka".
[21] D. E. Denning, wyd. cyt., s. 216.
[22] J. Janczak, *Kierunki* ..., s. 109.
[23] Tamże, s. 111.

elektroniczne. Z uwagi na skromność urządzeń tylko część jest realizowana, ale nie zwalnia to decydentów od tworzenia teorii działania systemów elektronicznych w działaniach asymetrycznych. Sprzęt możny zakupić, natomiast personel obsługujący sprzęt nie można wyszkolić w krótkim czasie.

5.2. ROZPOZNANIE SIECI INFORMACYJNYCH

Rozpoznanie zagrożeń asymetrycznych na aktualnym poziomie globalnej informatyzacji nie może przejść obojętnie wobec faktu bardzo szerokiego wykorzystania łączy internetowych do przekazywania informacji lub jej zaboru. Jednocześnie coraz częściej słyszy się o celowym destrukcyjnym działaniu wyspecjalizowanych narzędzi (programów) i wspomagających je osoby niepożądane, w destrukcji systemów komputerowych lub ścisłego monitorowania przepływu informacji. Przeszukiwanie sieci informatycznych przez osoby niepowołane poddawane są nie tylko stanowiska czy sieci komputerowe konkretnych jednostek administracji państwowej, wojskowej, ale również osobiste komputery wyselekcjonowanych funkcjonariuszy państwowych, dowódców i przywódców politycznych. Już te przesłanki wystarczają, aby rozpocząć badania nad prawomocnym usankcjonowaniem rozpoznania informatycznego systemów komputerowych w działalności wojskowej zarówno w czasie pokoju jak i wojny.

Jest to jednak tylko jeden aspekt rozpoznania informacyjne, co prawda bardzo waży i może najważniejszy w przyszłych działaniach, ale są także inne aspekty rozpoznania w sieciach informacyjnych. Wśród wielu sieci informacyjnych wyróżniamy także te, już dobrze znane i opisane, które często nazywane są sieciami radiowymi. Przekazywane informacje w tych sieciach także podlegają rozpoznaniu. Ten problem szeroko opisuje literatura przedmiotu, dlatego zespół badawczy na tym problemem nie będzie się skupiał. Szerzej natomiast przedstawi nowy, naszym zdaniem, problem rozpoznania informatycznego z uwagi na szeroką powszechność i globalny przepływ danych w sieciach komputerowych oraz rosnące zagrożenia jakie przynosi niekontrolowany dostęp i rozpowszechniane informacji drogą Internetu.

Jeżeli założymy, że ten rodzaj rozpoznania będzie funkcjonował w siłach lądowych należy dla niego określić zadania. Jednym z podstawowych jest skryte monitorowanie przepływów danych w sieciach komputerowych oraz prób wtargnięcia osób nieuprawnionych do systemu. W zależności od typu i charakteru operacji kryzysowych oraz ograniczeń mandatowych do kontroli rozpoznawczej może być wytypowana odpowiednio duża liczba

sieci lub komputerów (jawnych). Nie wszystkie i wszystko da się kontrolować. Jeżeli spotkamy się z działalnością grup terrorystycznych lub innych o charakterze przestępczym to należy spodziewać się, iż nie będą one dysponowały własnymi sieciami (zamkniętymi), lecz mogą korzystać z sieci ogólnodostępnych, zgodnie z maksymą (w tłumie szybciej się zgubić). Zadanie rozpoznania informatycznego będzie wówczas polegało na odnalezieniu takich osób i zidentyfikowaniu miejsc, z których łącza się z siecią.

Natomiast w typowych działaniach bojowych lub nawet asymetrycznych rozpoznanie informatyczne jest bardzo trudne. Stanowiska dowodzenia mają z reguły zamknięty system informatyczny. Z podwładnymi komunikują się albo za pomocą łącz stałych (działania obronne) albo na niewielkie odległości drogą radiową. Moc takiej transmisji jest ograniczona i dostępność energetyczna uniemożliwia śledzenie ruchów takiej sieci. Dlatego należy poszukiwać miejsc i osób, które będą łączyły się z siecią otwartą i wówczas próbować wtargnąć do sieć. Zbliżenie się z systemami rozpoznawczymi w pobliże takie sieci jest skuteczne, ale mało efektywne. Należy dysponować odpowiednio dużym czasem, aby rozpoznać sieci i dokonać odpowiednich modyfikacji. Na takie działania z pewnością przeciwnik sobie nie pozwoli.

Natomiast w działaniach asymetrycznych możemy spotkać się często z dostępnością do sieci otwartych, wówczas należy zastosować odpowiednie środki bezpieczeństwa, aby można był niezauważenie penetrować sieci przeciwnika.

Rozpoznanie informatyczne powinno być realizowane przez oficerów w wyspecjalizowanych komórkach organizacyjnych, z odpowiednio przygotowanymi narzędziami (programami) wraz z odpowiednimi urządzeniami. Rozpoznanie informatyczne można podzielić na dwie główne grupy zadań:

- związane z ochroną własnych systemów informatycznych przed niepowołanym dostępem;
- związane z monitorowaniem przepływu danych w sieciach komputerowych podejrzanych organizacji[24] (realizacja zadań o charakterze aktywnym).

W rozpoznaniu elektronicznym wyróżnia się kilka sposobów pozyskiwania danych elektronicznych. Należą do nich: poszukiwanie, przechwytywania, śledzenie, namierzanie i analiza techniczno-operacyjna. Analogicznie do tych sposobów można prowadzić rozpoznanie w sieciach informatycznych. Poszukiwanie informacji np. w globalnej sieci, jaką

[24] Warunkiem koniecznym jest otwartość sieci komputerowej. W przypadku zamkniętych sieci komputerowych nie jest możliwe wtargnięcie do ich struktur chyba, że odnajdzie się środki transmisji danych i wepnie się w ich kanały przepływu. Ten rodzaj działań jest możliwy po odnalezieniu łączy transmisyjnych.

jest Internet, polega na posługiwaniu się różnego rodzaju programami poszukującymi, dołączonymi do stron internetowych. Obsługa takiego narzędzia internetowego nie jest skomplikowana. Informacje uzyskiwane tą drogą będą jednak z reguły informacjami jawnymi - ogólnie dostępnymi.

Innym sposobem zdobywania informacji jest możliwość przechwytywania danych poprzez programy ukierunkowane na wyłapywanie w „gąszczu" danych, tych najbardziej istotnych, na których potencjalnemu wywiadowcy najbardziej zależy. Mogą to być kluczowe słowa lub ich ciągi słów albo sygnały cyfrowe o ustalonej kombinacji.

Kolejnym sposobem pozyskiwania informacji jest śledzenie. Śledzenie rozumiane jako analiza przepływu informacji (danych cząstkowych) w sieciach i wyłapywanie tych, które są niebezpieczne (np. programy uruchamiające automatyczne formatowanie dysków) i zagrażają bezpieczeństwu systemu komputerowego lub utraty danych. Śledzenie możne wykorzystać także do analizowania dróg upływności danych do potencjalnego przeciwnika. W takim przypadku nie chodzi o natychmiastową neutralizacje intruza a o zbadanie możliwych dróg jego dostępu do naszych systemów komputerowych. Ten sposób śledzenia można nazwać namierzaniem. Jest to kolejny sposób pozyskiwania danych o potencjalnych włamywaczach i ich metodach oraz sposobach włamania i drogach ucieczki. Efektem finalnym powinno być zidentyfikowanie włamywacza. Jest to już kolejny sposób pozyskiwania danych nazywany często w rozpoznaniu analizą operacyjno-techniczną przechwyconych sygnałów.

Wykorzystanie sieci komputerowych, w tym przede wszystkim Internetu, do działalności o charakterze przestępczym, związanym z pozyskiwaniem niejawnych danych. Powszechnie uważa się, że dane niejawne są najcenniejszą rzeczą przechowywaną na dyskach. Uzyskanie niejawnych danych narusza przede wszystkim tajność i integralność zasobów, wymaga nieco więcej wiedzy i specyficznych narzędziach (programach) do jej uzyskania, ale nie są to koszy tak duże jak np. skonstruowanie i wyprodukowanie systemów satelitarnych.

Dla wyspecyfikowania prowadzenia rozpoznania informatycznego i określenia jakie mogą wystąpić zagrożenia, w pierwszej kolejności zespół badawczy rozpatrzył możliwe sposoby dostępu do systemów komputerowych. Wyróżniono ogólnie dwa sposoby: wewnętrzny i zewnętrzny. Do zewnętrznych dróg dostępu do systemów komputerowych zaliczono:

1. Dostęp do sieci komputerowej lub sieci komutacji pakietów (dostęp do zasobów systemu) przez każdego posiadającego dostęp do sieci i odpowiednie uprawnienia w sieci.
2. Połączenie z wykorzystaniem modemu.
3. Podłączenie się (legalne lub nielegalne) do linii dzierżawionej.
4. Wejście na odpowiednie pasmo częstotliwości w sieciach komputerowych połączonych drogą radiową.
5. Wykorzystanie promieniowania ujawniającego - na tej drodze nie jest możliwa manipulacja w zakresie integralności informacji, można natomiast naruszyć jej tajność.

Natomiast o wewnętrznych sposobów wtargnięcia do systemów komputerowych zaliczono:

1. Fizyczny dostęp do systemu komputerowego - w przypadku pojedynczego systemu komputerowego jedynym wejściem do systemu są terminale i napędy pamięci zewnętrznych.
2. Działalność szpiegowską w składzie osób upoważnionych do pracy na poszczególnych terminalach komputerowych.
3. Zaniedbanie i gadulstwo personelu. Nieroztropność w pozostawieniu kluczy dostępu do systemów.

Niejednokrotnie zdarza się, że kraje zawiązane sojuszem mają wspólne poglądy na zagadnienia terytorialne, ideologiczne, czy też gospodarcze. Sojusznik jest jednak pojęciem czysto dyplomatycznym. Nic nie stoi na przeszkodzie, by kraj sprzymierzony podejmował działania szpiegowskie względem swoich przyjaciół np. w celu kontroli ich lojalności. Podobnie może się dziać w odniesieniu do sił pokojowych w operacjach kryzysowych czy w innych działaniach bojowych. Nie tylko zasoby danych wywiadowczych sił walczących są cennymi danymi dla potencjalnego przeciwnika (wywiadowców), ale także stan techniczny sprzętu, możliwości zaopatrzenia, morale żołnierzy itp. Bardzo cenne informacje dotyczące taktyki działania, struktur i charakterystyk osobowych poszczególnych dowódców. Dlatego znajomość sposobów utraty informacji w systemach komputerowych może spowodować ochronę informacji przed niepowołanymi osobami.

Każde działania bojowe są i będą ukierunkowane na powstrzymywanie utraty informacji. Niemniej jednak każda ze stron konfliktu będzie prowadziła swoją działalność informacyjną. Szpiegostwo to tylko jedna strona pozyskiwania danych. Grozi nam coś dużo poważniejszego, a mianowicie atak informacyjny. W wielu krajach prowadzi się badania i symulacje dotyczące ataku na systemy komputerowe. Najczęściej mówi się o ataku w czasie

wojny - ale są specjaliści, którzy uważają, że może on nastąpić w czasie pokoju: „Rząd Stanów Zjednoczonych powinien zdać sobie sprawę, ze atak informacyjny może pojawić się przed formalną deklaracją wrogich zamiarów ze strony wrogiego państwa (...) Sytuacji takiej możemy już oczekiwać w roku 2020 lub wcześniej"[25]. Te słowa dobitnie wskazują jak poważnie traktują ten problem państwa w dużej części uzależnionego do przepływu danych w sieciach informatycznych. Ten problem będzie narastał w czasie prowadzenia działań o charakterze asymetrycznym.

5.3. Bezpieczeństwo informacyjne

Znaczenie bezpieczeństwa informacji określa wprowadzona polityka bezpieczeństwa w każdej armii i państwie. Obejmuje zasady i sposoby ochrony informacji mających największe znaczenie dla instytucji, organizacji. Przeznaczona jest dla osób mających jakikolwiek dostęp do przetwarzanych informacji. Odpowiednie bezpieczeństwo informacji może mieć kluczowe znaczenie dla rozwoju, czy nawet istnienia jednostki. W czasach, gdy informacja stała się cennym towarem błędy czy niedopatrzenia w jej zabezpieczeniu mogą spowodować duże straty. Na pytanie „co to jest polityka bezpieczeństwa?" można odpowiedzieć: „przede wszystkim zbiór przepisów, zasad, wymagań i zaleceń regulujących sposób zarządzania, ochrony i udostępniania aktywów (informacyjnych i materiałowych) w określonym środowisku"[26].

Utrata danych ściśle związana jest z czynnikiem finansowym. W pracy J. Janczaka i G Świdzikowakiego[27] można przeczytać jak wielkie jest zagrożeniu utraty informacji związanych z kradzieżami danych oraz oszustwami finansowymi, a wiec celowe działania czynnika ludzkiego mającego na uwadze jedynie własny zysk. Nie od dziś wiadomo, że najsłabszym ogniwem bezpieczeństwa jest człowiek i głównie od niego będzie zależało utrzymanie bezpiecznych informacji z dala od osób trzecich. Maszyna i programy są tylko narzędziami, które człowiek programuje, obsługuje i wykorzystuje.

Utrzymanie bezpieczeństwa informacji w kanałach i sieciach je przesyłających jest przedsięwzięciem niezmiernie trudnym. W kanałach łączności bezpieczeństwo informacyjne zachowane jest głównie poprzez utrzymywanie odpowiednich kodów (dawniej stosowano książki kodowe, aktualnie stosuje się mikro układy szyfrujące). Nie na każdym szczeblu

[25] Płk Richard Szafranski, USAF, http://www.cdsar.ar.mil/apj/szfran.html
[26] J. Janczak, G. Świdzikowski; *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*, AON, Warszawa 2004.
[27] Tamże.

dowodzenia w kanałach łączności należy stosować kodowanie. Nie w każdej też sieci informacyjnej należ takie zabezpieczenia stosować. Informacje zabezpieczone przed nieuprawnionym dostępem to głównie te, które dotyczą życia osób lub podjęcia decyzji o skutkach istotnych dla określonej grupy. Inne, których żywotność jest mniej istotna mogą być szyfrowane, ale niekoniecznie szyfrem o liczbie kombinacji4096 bitów jak to ma miejsce używać programu *Pretty Dood Privacy* (PGP)[28]. Aktualnie szyfrowanie stosuje się częściej w sieciach komputerowych, w których droga do adresata jest dłuższa a jej żywotność przekracza kilka dni.

W działaniach asymetrycznych ataki na systemy informatyczne narażone są głównie systemy komputerowe i systemy łączności. Te ostatnie głównie poprzez zakłócanie elektroniczne, a te pierwsze poprzez włamania osób niepowołanych.

Każda działająca sieć komputerowa może być obiektem ataków. Obiekt, przedmiot i sposób ataku są specyficzne dla danego systemu. Są również silnie zależne od uwarunkowań zewnętrznych i wewnętrznych w danej chwili czasowej. Sieci komputerowe muszą być nadzorowane i chronione, aby zapewnić ich prawidłowe działanie a tym samym zapewnić właściwy poziom i wiarygodność świadczonych usług np. na stanowisku dowodzenia.

Warto zdać sobie sprawę z kilku obowiązujących aksjomatów dla budowy i działania skutecznych systemów bezpieczeństwa. O bezpieczeństwie sieci decyduje - podejście systemowe - kompleks działań technicznych, logistycznych i organizacyjnych. Techniczna realizacja systemu zabezpieczeń jest równie ważna jak pozostałe działania. Bezpieczeństwo jest procesem ciągłym - w chwili obecnej odkrywane jest tygodniowo około trzech problemów związanych z bezpieczeństwem w systemach informatycznych. Fakt ten w połączeniu z silnym sprzężeniem systemów informatycznych poprzez sieć powoduje, że zagrożenia rozprzestrzeniają się bardzo szybko. Dlatego zapewnia się szybką reakcję na potencjalne zagrożenia. W systemach komputerowych najważniejszą rzeczą nie jest system zabezpieczeń sprzętu, ale przede wszystkim oprogramowanie. Każdy eksploatowany system teleinformatyczny może być podatny na ataki ze względu na:

- słabość stosowanej technologii,
- błędy konfiguracyjne,
- złą definicję polityki bezpieczeństwa.

Większość protokołów sieciowych używanych współcześnie powstała w czasie, gdy ilość użytkowników była ograniczona. Użytkownicy wywodzili się głównie ze środowisk

[28] E. Yourdon, *Wojna na bity, wpływ wydarzeń z 11 września na technikę informacyjną*, WNT, Warszawa 2004, s.82.

uniwersyteckich i częściowo wojskowych. Masowe rozpowszechnienie Internetu, a tym samym protokołów, które powstały wiele lat temu dla innej grupy użytkowników jest źródłem poważnych zagrożeń. Do niebezpiecznych należą tak znane protokoły jak: telnet, rlogin, rsh, SNMP czy SMTP. Błędy implementacji stosu TCP/IP otwierają również drogę do ataków typu DoS (ang *Denial of Service*). Komplikacja współczesnych systemów komputerowych powoduje, że praktycznie w chwili instalacji systemu operacyjnego z nośnika CD, wymaga on wielu uaktualnień głównie dotyczących bezpieczeństwa systemu. Częstym zagrożeniem jest pozostawienie standardowych haseł administratora lub ich brak na urządzeniach sieciowych. Stwarza to nie tylko zagrożenie bezpośrednie, ale również pośrednie. Źle skonfigurowane urządzenia sieciowe mogą służyć jako węzły do maskowania dróg ataku. W literaturze przedmiotu można przeczytać o wielu przykładach badań firm konsultingowych wskazujących, że wiele firm posiada, bardzo dobre systemy zabezpieczeń, ale są one niewłaściwie skonfigurowane. Ten problem nie pozostaje bez echa w systemach wojskowych. Niezwykle istotnym problemem konfiguracyjnym, w punktach styku z sieciami zewnętrznymi, jest pozostawienie protokołów dynamicznego *routingu*, czy też innych specyficznych protokołów pozwalających na odkrycie infrastruktury sieciowej.

Najczęściej spotykane błędy wynikające z niewłaściwej konfiguracji to niezabezpieczone konta użytkowników, brak zmiany standardowych haseł dostępu poprzez lub podanie prostych haseł podatnych na ataki słownikowe. Do jednego z najważniejszych aksjomatów w konfigurowaniu systemów zabezpieczeń należy zasada, konfiguracji minimalnej. Nie należy konfigurować serwisów, z których nie będziemy korzystali. Często ustawienia standardowe stosowanych aplikacji otwierają intruzom dostęp do naszych zasobów. Do czynników niemniej istotnych, należą zagrożenia organizacyjno-logistyczne. Brak spisanej polityki bezpieczeństwa, niezgodność wdrożenia systemu zabezpieczeń z polityką bezpieczeństwa, brak planów awaryjnych to najbardziej rażące przykłady zaniedbań. Najważniejsze etapy w planowania i wdrażaniu systemów bezpieczeństwa to:

a) analiza wymagań systemu:
   - wydajność,
   - wymagany poziom bezpieczeństwa,
   - dostępność i niezawodność systemu,
   - analiza procesów i procedur organizacyjnych,
   - zgodność założeń z polityką bezpieczeństwa

b) projekt powinien uwzględniać:

- modularną budowę systemu,
- planowanie zarządzania systemem,
- zasadę najsłabszego ogniwa,
- zasadę blokowania potencjalnych zagrożeń na brzegu sieci,
- zasadę wielopoziomowej struktury systemu zabezpieczeń,
- zasadę heterogeniczności komponentów systemu zabezpieczeń,
- strukturę zarządzania siecią,
- fizyczne bezpieczeństwo urządzeń,

c) wdrożenie:

- techniczna realizacja przedsięwzięcia,
- działania organizacyjne - reorganizacja procesów,
- procedury,

d) kontrola poprawności wdrożenia systemu:

- kontrola pasywna,
- aktywna kontrola poziomu zabezpieczeń,
- kontrola poziomu realizacji przedsięwzięć organizacyjnych,

e) dokumentacja powykonawcza.

Najbardziej znanym systemem zabezpieczającym są ściany ogniowe (*firewall*). Są to zarówno rozwiązania sprzętowe jak i programowe. Oprogramowanie do ochrony systemów styku z sieciami zewnętrznymi obejmuje nie tylko zapory ogniowe, ale również programy do filtracji przesyłanych informacji. Filtracja zawartości przesyłanych informacji chroni użytkowników przed złośliwymi programami, wirusami komputerowymi etc. odrzucając je już na wejściu do naszych sieci. W chwili obecnej również tam można umieścić programy skanujące treść wysyłanych na zewnątrz informacji, chroniąc organizację przed nabierającym znaczenia problemem wycieku danych.

Niezmiernie ważnym elementem systemu zabezpieczeń jest system wykrywania włamań (ang. Intrusion Detection System). Zapory ogniowe filtrują pakiety zgodnie z ustawionymi regułami. Niestety w ramach dozwolonych typów połączeń intruz może przesyłać specjalnie spreparowane pakiety sieciowe, które mogą blokować serwery, doprowadzać do ich czasowej niedostępności etc. Systemy IDS nie tylko wykrywają potencjalne ataki, ale potrafią również je blokować.

W przypadku systemów bezpieczeństwa często mówi się o modelu AAA. Jego nazwa pochodzi od pierwszych liter angielskich słów: *authentication, authorization, accounting*,

czyli uwierzytelniania, autoryzacji i rozliczania użytkowników sieciowych. Proponowane rozwiązania zawierają proste systemy kontroli dostępu oparte o parę hasło/użytkownik do systemów haseł jednokrotnych, oraz rozwiązań infrastruktury klucza publicznego.

Sieci VPN zadomowiły się na dobre w systemach zabezpieczeń. Oprócz docenianej przez wszystkich roli ochrony kanałów przesyłu danych dają wiele możliwości, między innymi możliwość budowy dowolnej struktury logicznej ponad warstwą fizyczną sieci. Tradycyjnie oferowane rozwiązania podnoszenia niezawodności opierają się na pomyśle zwielokrotnienia elementów zabezpieczających, gdzie tylko jeden z tych elementów jest aktywny. Oznacza to w praktyce, że przepustowość tak zbudowanego systemu można skalować tylko poprzez zwiększanie przepustowości pojedynczego elementu. Dzięki stosowanym technologiom możemy dziś uzyskać skalowanie rozwiązania poprzez balansowanie obciążenia pomiędzy elementami systemu zabezpieczeń. Ważnym uzupełnieniem oferty bezpieczeństwa są systemy antywirusowe chroniące nie tylko system na styku z Internetem, ale również komputery i serwery sieci LAN. Nadzorowanie i administracja systemami antywirusowymi jest równie ważna jak dla pozostałych systemów. W chwili obecnej czas od wykrycia wirusa do powstania szczepionki jest mierzony w minutach.

Kontrola skuteczności posiadanych systemów zabezpieczeń jest równie ważnym elementem jak pozostałe. Pozwala nam ona również na znalezienie potencjalnych błędów zarówno konfiguracyjnych jak i systemowych. Obejmuje ona zarówno skanery sieciowe, jak i oprogramowanie do analizy i ochrony konkretnych serwerów czy aplikacji.

Bezpieczeństwo organizacji to nie tylko sprzęt i jego konfiguracja, ale całokształt działań i regulacji w tym zakresie. Projektowanie systemów bezpieczeństwa wymaga całościowego spojrzenia na bezpieczeństwo danej organizacji - nie można tworzyć skutecznego systemu bezpieczeństwa bez ogarnięcia całości potrzeb. Systemy zabezpieczeń muszą integrować produkty pochodzące od różnych producentów, aby zapewnić właściwy poziom bezpieczeństwa.

5.3.1. Metody ochrony systemów informacyjnych

Ochrona programowa

Zabezpieczenie programowe to najtańsza metoda zabezpieczenia informacji przed ich ujawnieniem. Niestety jest ono zwykle najbardziej narażone na ataki osób korzystających ze specjalistycznej literatury czy nawet Internetu. Większość włamań do rządowych lub

wojskowych systemów komputerowych ma charakter żartobliwy (rys. 5.7), a ich celem jest ośmieszenie wybranych instytucji. Najłatwiej zrobić to, podmieniając np. zawartość strony głównej atakowanego serwisu. Zdarza się jednak, że haker po spenetrowaniu sieci poważnej instytucji wchodzi w posiadanie danych, dzięki którym może zagrozić bezpieczeństwu kraju, a nawet świata. Taka sytuacja miała miejsce w marcu 2001 roku, gdy nieznany sprawca uzyskał dostęp do komputerów amerykańskiej marynarki wojennej. Przejął on kontrolę nad danymi dotyczącymi systemu globalnej lokalizacji GPS oraz obroną strategiczną USA. Zdobył także tajne kody umożliwiające kierowanie statkami kosmicznymi, satelitami oraz pociskami. Jak podała szwedzka prasa, skradzione kody mogły zostać użyte przez terrorystów do zniszczenia systemów komputerowych sterujących projektami kosmicznymi, a także do szpiegostwa przemysłowego. Według amerykańskiej marynarki wojennej kody te nie były wcale tajne.[29]

Jak wynika z danych przedstawionych przez Mi2g Intelligence Unit[30] w ostatnich latach znacząco wzrasta liczba ataków na rządowe serwisy internetowe [31]. Chroniąć własne systemy komputerowe przede wszystkim należy korzystać z zawsze aktualnych wersji oprogramowania antywirusowego. W przypadku szybkich łączy internetowych, bazy wirusów powinny być aktualizowane możliwie najczęściej, tj. z maksymalną częstotliwością oferowaną przez dostawcę systemu antywirusowego. Korporacyjne instalacje systemów powinny być centralnie monitorowane pod kontem aktualności bazy wirusów na wszystkich chronionych komputerach. Użytkownicy powinni być szkoleni w zakresie bezpiecznego użytkowania poczty elektronicznej w szczególności:

- nie należy otwierać podejrzanej poczty elektronicznej (o nieznanym pochodzeniu, dziwnych tytułach itp.) – powinna być kasowana od razu gdyż poczta w formacie HTML może zawierać złośliwy kod, który uruchomi się natychmiast po otworzeniu,
- nie należy otwierać podejrzanych załączników o nieznanym pochodzeniu,
- nie należy ściągać przez www plików wykonywalnych o nieznanym i niesprawdzonym pochodzeniu.

Dodatkowym narzędziem wspomagającym zapobieganie włamaniom mogą być „osobiste zapory ogniowe" (ang. *personal fewall*), które można zainstalować na wszystkich komputerach.

---

[29] http://www.hotnews.pl/

[30] Firma Mi2g zajmuje się między innymi: łagodzeniem ryzyka przestępstw cybernetycznych, atakami hakerów na systemy komputerowe, kradzieżą pieniędzy z banków poprzez Internet, wykradaniu numerów kont i haseł.

[31] http://www.vnunet.com/news/1128072

Programy antywirusowe

Skuteczny system antywirusowy musi stanowić istotną część całego systemu bezpieczeństwa teleinformatycznego jednostki. Najlepszym jest połączenie oprogramowania z procedurami bezpieczeństwa, nie tylko w momencie infekcji, ale także w celach profilaktycznych dla zmniejszenia ryzyka ataku. Należałoby także uniemożliwić użytkownikom instalację na stacjach roboczych oprogramowania niewiadomego pochodzenia. W miarę możliwości zezwolić na przesyłanie pocztą elektroniczną tylko „bezpiecznych" załączników oraz wyeliminować z treści wiadomości elementy wykonywalne (m.in. aplety Javy). Zmutowane robaki wykorzystują często luki w systemach operacyjnych czy aplikacjach użytkowych, należy przy tym pamiętać o systematycznym uaktualnianiu wersji i instalowaniu poprawek. Należy też pamiętać, że nasze bezpieczeństwo nigdy nie będzie stuprocentowe, a wirusy mogą zniszczyć nasze dane. Systematyczna archiwizacja również i z tego względu jest podstawowym obowiązkiem administratora. W przypadku ochrony stacji roboczych wskazane jest zaopatrzenie się w oprogramowanie skanujące w czasie rzeczywistym tzn. skanującej dane przy każdej próbie dostępu do plików oraz w momencie odbierania poczty. Dla pewności należy także przeprowadzać, co jakiś czas skanowanie wszystkich zasobów komputera. Aktualizacja baz sygnatur wirusów powinna odbywać się automatycznie w sposób niewidoczny dla użytkownika (np. raz dziennie). Przy dużej liczbie stacji trzeba umożliwić wszystkim regularną aktualizację lub wyznaczyć osobę odpowiedzialną za dopilnowanie tego.

Za najważniejsze kryteria wyboru odpowiedniego produktu (programu antywirusowego) uznano:

- Wykrywalność - Ważne, by wybrany system miał możliwość detekcji nie tylko tradycyjnych wirusów, ale także innych niebezpiecznych programów m.in. koni trojańskich, złośliwych apletów Javy i ActiveX,
- Skanowanie w czasie rzeczywistym - monitor działający on-line umożliwia w porę wykryć wirusa. Nie należy jednak zapominać o dodatkowym systematycznym skanowaniu na żądanie. Najlepiej, jeśli program umożliwia ustalenie harmonogramu przeszukiwania oraz zautomatyzowanie procesu skanowania danych,
- Pomoc techniczna - dobrze, jeśli w ramach serwisu mamy zagwarantowane nie tylko uaktualnienia sygnatur wirusów, ale również regularne informacje i ostrzeżenia o nowych zagrożeniach oraz wsparcie na wypadek ataku lub problemów technicznych,

- Wydajność przetwarzania - nie wszyscy mogą sobie pozwolić na regularną wymianę sprzętu, często jest to również bezzasadne. Ważne więc, by skaner antywirusowy nie obciążał zanadto zasobów sytemu i nie przeszkadzał w pracy,
- Regularne i automatyczne uaktualnianie baz wzorców - każdy dobry skaner ma możliwość zautomatyzowania tego procesu, trudno polegać na systematyczności użytkownika. Centralne zarządzanie - ta funkcja jest kluczowa zwłaszcza dla dużych sieci, pozwala utrzymać jednolitą politykę ochrony dla całej firmy i mieć kontrolę nad poczynaniami użytkowników. Dodatkowo udostępnianie oprogramowania i baz wzorców z jednego punktu znacznie poprawia bezpieczeństwo i ułatwia pracę administratorów,
- Ostrzeżenia w języku polskim - niewiele programów antywirusowych posiada polski interfejs, w związku z tym powinniśmy mieć możliwość lokalizacji komunikatów. Nagminne są przypadki paniki użytkowników czytających informację o wykryciu i usunięciu wirusa, jako alarm o infekcji. Przeważnie jest to spowodowane nieznajomością programu lub języka np. angielskiego. Dla wielu administratorów kryterium wyboru będą także funkcje takie jak: zdalne zarządzanie, rozbudowany system raportowania, ustalenia polityki antywirusowej dla użytkowników zdalnych i mobilnych,
- Organizacja systemu antywirusowego - Za stosowaniem jednego rodzaju programu przemawia: łatwość integracji poszczególnych elementów, wspólne zarządzanie, jednolitość interfejsów, jeden punkt pomocy technicznej, *update'y* z jednego miejsca, co daje obniżenie kosztów związanych ze szkoleniami oraz obsługą i utrzymaniem systemu. Jednak argumentami przeciwko stosowaniu tego typu organizacji bezpieczeństwa jest to, że system może przepuścić wirusa, a kolejny punkt ochrony np. na stacji roboczej pochodzący od tego samego producenta go również nie wykryje. Większość producentów wymienia się informacjami o nowych zagrożeniach. Można dla pewności stosować rozwiązania pochodzące z różnych źródeł, ale nie więcej niż dwóch. Najlepiej, gdy styk z Internetem i serwery chronione są przez produkty jednego dostawcy, a stacje robocze innego.

Specjaliści bezpieczeństwa przewidują dalszy rozwój wirusów hybrydowych i ich koncentrację na unieszkodliwianiu *firewalli* oraz systemów antywirusowych. Stąd tak ważne jest stałe monitorowanie zdarzeń w sieci z uwagą czy nie nastąpiła infekcja. Należy także wciąż uświadamiać użytkowników, aby ich działania nie stały się zagrożeniem. Od ich

czujności zależy czy uda się uniknąć infekcji w momencie, gdy zawiedzie skaner antywirusowy.

Systemy sprzętowo-programowe

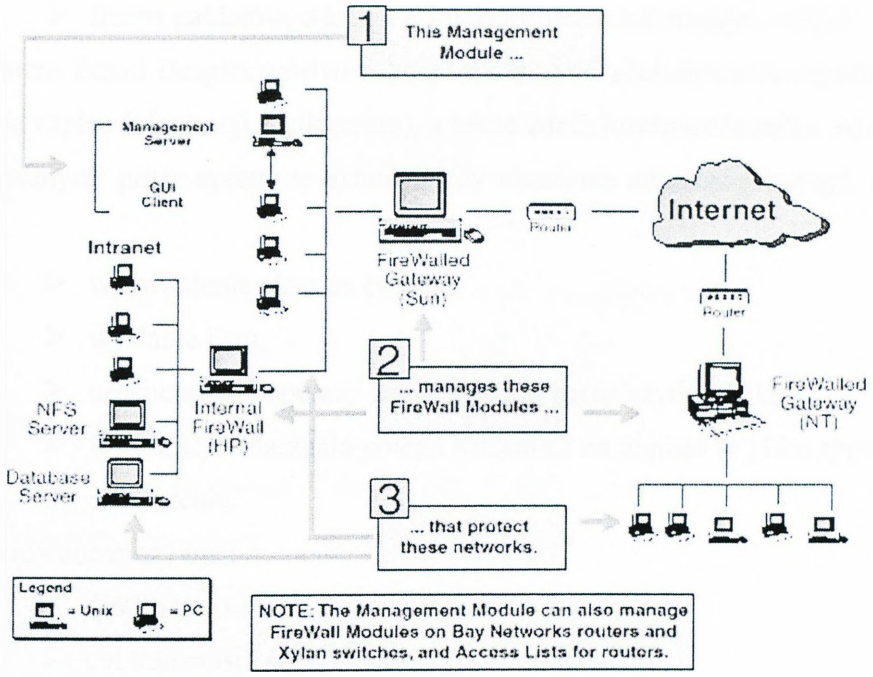
Często efektywnym sposobem zabezpieczenia systemu przed atakami z jego otoczenia jest odseparowanie go od pozostałych elementów sieci przez zastosowanie tzw. ściany ogniowej (ang. firewall). W architekturze takiej, system informatyczny - mający połączenie z globalną siecią komputerową - połączony jest do niej za pośrednictwem struktury sprzętowo-programowej (może to być jeden komputer lub pewna podsieć z odpowiednim oprogramowaniem). Ściana ogniowa wykonuje na jego rzecz różnego rodzaju działania np: Zajmuje się filtrowaniem (kontrolowaniem) komunikacji sieciowej między systemem organizacji a zewnętrzną siecią komputerową. Selekcja ta odbywa się na poziomie sprawdzania pakietów sieciowych. Często zdarza się, że komputer za pośrednictwem, którego sieć organizacji podłączona jest do sieci zewnętrznej - tzw. gateway - pełni również rolę ściany ogniowej. Wówczas do jego zadań należy nie tylko przesyłanie pakietów między siecią wewnętrzną a siecią zewnętrzną, ale również sprawdzanie czy dany pakiet można przesłać. Sposób działania ściany ogniowej wynika z przyjętej w organizacji polityki bezpieczeństwa. Prosty przykład sposobu filtracji pakietów przez ścianę ogniową może być następujący:

- blokowane są wszystkie połączenia z komputerami sieci zewnętrznej uznanymi za niegodne zaufania,
- blokowane są wszystkie przychodzące połączenia oprócz połączeń pocztowych (aby możliwe było odbieranie poczty),
- służy jako tzw. serwer pośredniczący. Wówczas komputery wewnętrznej sieci organizacji zwracają się z żądaniami wykonania określonych usług nie bezpośrednio do interesujących ich komputerów sieci zewnętrznej lecz do serwera pośredniczącego działającego na ścianie ogniowej (rys. 5.4.), który przesyła je dalej. Również odpowiedzi od właściwych serwerów przekazywane są za pośrednictwem serwerów pośredniczących. Takie działanie nazywane bywa często ochroną na poziomie aplikacji.

Należy zdawać sobie sprawę z tego, że nie istnieje uniwersalna konfiguracja sprzętowo-programowa ściany ogniowej. Działanie każdej takiej architektury wiąże się ze specyfiką systemu informatycznego organizacji i wynika z jej polityki bezpieczeństwa oraz zakresu ochrony.

Manager Obiektów Sieciowych służy do definiowania jednostek, dla których określona jest polityka bezpieczeństwa. Jednostkami takimi mogą być:

- sieci i podsieci,
- hosty i gateway-e,
- serwery,
- routery,
- przełączniki (switch-e),
- domeny Internetowe,
- serwery logiczne,
- grupy powyższych obiektów.



Rys. 5.4. Przykład sieci z zastosowaniem sprzętowo-programowej ochrony

Manager Użytkowników umożliwia definiowanie użytkowników i grup użytkowników. Dla każdego użytkownika możliwe jest określenie następujących parametrów:

- grupy, do których należy,
- okres ważności użytkownika w systemie,
- pory aktywności,
- adresy źródeł i miejsc docelowych dopuszczalnych dla użytkownika,
- parametry związane z uwierzytelnianiem (hasła, klucze itp.).

Monitor Stanu Systemu służy do wyświetlania informacji o stanie komputerów, na których działają Moduły firewall. Moduł sterujący uzyskuje tego rodzaju informacje od Modułów firewall za pośrednictwem protokołu SNMP. Monitor wyświetla następujące informacje o każdym załadowanym (aktywnym) Module firewall:

- data instalacji polityki bezpieczeństwa,
- status obiektu (Moduł załadowany, nie załadowany, brak odpowiedzi, nierozwiązywalny adres),
- nazwa obiektu,
- nazwa pliku zainstalowanej polityki bezpieczeństwa,
- data ostatniej aktualizacji informacji o stanie obiektu,
- liczba skontrolowanych pakietów sieciowych,
- liczba pakietów nie przepuszczonych,
- liczba pakietów, o których zarejestrowano informacje.

W Edytorze Zasad Bezpieczeństwa istnieje możliwość zdefiniowania rejestrowania zdarzeń (w sensie zapisu informacji o zdarzeniu), a także zdefiniowania alarmów. Alarmy są akcjami wykonywanymi przez system w sytuacji, gdy określone zdarzenie wystąpi. Alarmem może być:

- wyświetlenie okna na ekranie,
- wysłanie listu,
- uruchomienie operacji zdefiniowanej przez użytkownika,
- Rejestracja zdarzenia polega natomiast na zapisie w pliku typu log informacji o zdarzeniu.

Zarejestrowane może być:

- źródło transmisji,
- cel transmisji,
- usługa, protokół, port źródłowy,
- czas i data zdarzenia,
- przedsięwzięta akcja (przyjęcie, odrzucenie komunikacji),
- numer reguły, do której dopasowano zdarzenie,
- Moduł FireWall, którego dotyczyło zdarzenie,
- użytkownik, sposób uwierzytelnienia,

Hasła

Hasło (ang. password) jest ciągiem znaków, które mogą być użyte do uwierzytelniana tożsamości użytkownika systemu automatycznego przetwarzania danych i w niektórych przypadkach do udzielania lub odrzucenia dostępu do prywatnych danych. Hasła powinny się składać ze zbioru 95 znaków graficznych alfabetu. Długość hasła jest ściśle związana z przydatnością tegoż ciągu znaków. Bezpieczeństwo hasła zależy od jego składu, długości i jego zabezpieczeniem przed jego ujawnieniem i podstawieniem.

Hasła powinny być ważnie nie dłużej niż rok. Użyteczny okres ważności hasła zależy od paru zmiennych, wśród nich:

- koszt zmiany hasła,
- ryzyko związane ze złamaniem,
- ryzyko związane z dystrybucją,
- prawdopodobieństwo „odgadnięcia" hasła,
- liczba użyć hasła,
- czas znalezienia hasła przez wyczerpująca metodę prób i błędów.

- Osobiste hasło powinno być własnością bardziej indywidualną aby nie należało do grupy użytkowników z powodu osobistej odpowiedzialności w systemie komputerowym. Jest to zalecane nawet wtedy, gdy cała grupa posiada identyczne uprawnienia do tych samych zasobów danych.

5.3.2. Zagrożenia dla systemów informacyjnych

Wirusy

Wirusy to programy, które maskują się podczepiając pod inne użyteczne pliki. Są to głownie pliki z rozszerzeniem; *.exe, *.doc, *.xls, *.com, również e-maile i pliki *.html*. Wirusy głównie kopiują się w dziesiątki miejsc, ale są i takie, które czynią duże szkody. Zastosowanie dobrego programu antywirusowego zapobiega zagrożeniu w 99%. Programy te winny być aktualizowane i muszą monitorować wszystko to co dzieje się w systemie. Skanować należy również to co przychodzi z zewnątrz począwszy od e-maili, a kończąc na płytach z pism komputerowych.

Trojany

Jednymi z programów, które są najczęściej stosowane są trojany. Trojan – zwany też „backdor" (tylnie drzwi) to program, który instaluje się na komputerze bez naszej wiedzy, najczęściej podszywając się pod jakąś popularną aplikację np. Winamp'a. Umożliwiając atakującym zdalne administrowanie naszym komputerem. „Konie trojańskie" składają się z 2-3 plików *.exe, aplikacji klienta, serwera i czasami konfiguracyjnej. Aplikacja serwera służy do zarażania komputera ofiary. Po uruchomieniu takiego programu, najczęściej wyskakuje okno informujące o jakimś błędzie, lub fałszywe okno instalacyjne. W tym czasie jest tworzona kopia pliku i zapisywana w którymś z katalogów „windows", „x:\Windows\system" lub „x:\Windows\system32" (gdzie; x jest katalogiem głównym).

Stosowanie tego typu programów jest karalne a ściślej: bezprawne uzyskanie informacji, naruszenie integralności komputerowego zapisu danych, podsłuch i sabotaż komputerowy, a prościej uszkodzenie, usunięcie zmianę danych, także zapoznanie się z treścią bezprawnie uzyskanych informacji jest karalne art.267 § 1 k.k. art.267§ 2art.268 § k.k. art.269 k.k.

Sniffing

Sniffing stanowi zagrożenie bezpieczeństwa niższych warstw struktury sieciowej, na której opierają się aplikację internetowe. Sniffing jest zagrożeniem biernym. W tym przypadku dane odczytywane są przez interfejs sieciowy, dla którego nie były one przeznaczone. Samo pojecie oznacza „wąchanie" zostało zaczerpnięte z języka angielskiego. Nie powoduje żadnych zmian w normalnym przepływie danych ani też nie wprowadza danych do sieci – stanowi jednak zagrożenie dla prywatności informacji, które to sytuacje są czasami nie do zaakceptowania, powodują bowiem ujawnienie danych osobom nie uprawnionym. Może być traktowany do przygotowania czynnego ataku na jednostkę gdy mamy do czynienia z podsłuchiwaniem haseł. Co w efekcie może spowodować utratę lub modyfikację czy pozyskanie danych przez nieuprawnioną osobę. Sam mechanizm podsłuchu nie jest zakazany ponieważ nie zawsze służy do uzyskiwania informacji.

Przykładem takich programów są sprzedawane jako analizatory sieci aplikacje. Pomagają one w diagnozowaniu administratorom wielu ukrytych problemów, które mogą być niewidoczne dla serwera. Dostęp do tego oprogramowania jest wielkim ułatwieniem. Dostępność tego oprogramowania oznacza jednak również, że inni użytkownicy mogą przechwytywać dane płynące przez sieć i wykorzystując je do nieuprawnionych działań przeciwko właścicielowi informacji. Sniffing danych z sieci prowadzi do utraty prywatności informacji.

W celu ochrony przed podsłuchem stosuje się następujące techniki zabezpieczające:

- segmentacji sieci – używanie hubów przełączających (switchy), które często nazywane są routerami warstwy łącza. Umożliwiają one skonfigurowanie sieci w ten sposób, że określone ramki są kierowane najczęściej do znanego wcześniej segmentu. Można rozwijać koncepcje segmentacji sieci aż do tzw. Mikrosegmentacji, w której nawet pojedyncza stacja robocza może mieć przydzielony samodzielny segment. Zwykle maksymalnie cztery poziomy.
- wymianie we wszystkich komputerach kart sieciowych na takie, które nie pracują w trybie mieszanym (promiscous), sprawdzić okablowanie (ktoś mógł przeciąć okablowanie i podpiąć własne urządzenie)

- używaniu antysnifferów. Są to urządzenia, których zadaniem jest wykrycie, czy do segmentu lokalnej sieci podłączone interfejsy sieciowe ustawione w tryb mieszany zbierają informacje, które nie są dla nich przeznaczone.

Znane są również inne metody ochrony, ale najlepszym jest uświadomienie wszystkim użytkownikom komputerów o niebezpieczeństwie. Opracowanie polityki bezpieczeństwa w zakresie używania i zmieniania haseł. Używając różnych haseł w systemach o różnym poziomie bezpieczeństwa. Tworzenie niełatwych do odgadnięcia nazw, ale jednocześnie żeby nie były zbyt trudne. Najlepszym zabezpieczeniem przez sniffingiem jest wprowadzenie i egzekwowanie dobrej polityki bezpieczeństwa (procedury, kontrole, ograniczenia dostępu).

Ochrona sprzętowa

Jednym ze sposobów ograniczenia możliwości zapoznania się z ogólnie nie dostępnymi informacjami są metody biometryczne. Mogą być one stosunkowo pewnym sposobem dostępowym ze względu na to, że klasyczne hasła mogą zostać zapomniane lub podejrzane przez niepowołane osoby oraz za jednym dotknięciem palca rozpoznają one użytkownika i poświadczają autentyczność osoby szukającej dostępu. Biometryczne metody uwierzytelniania obejmują techniki rozpoznania odcisków palców, skanowanie siatkówki oczu, skanowanie geometrii dłoni i charakteru pisma oraz rozpoznawanie głosu. Wszystkie te metody opierają się na fizycznych własnościach identyfikowanej osoby.

Zdecydowanie najbardziej znanym i najszerzej wykorzystywanym sposobem identyfikacji i weryfikacji jest analiza linii papilarnych. Jest to sposób powszechnie uważany za jeden z najlepszych mechanizmów biometrycznych, a przede wszystkim najbardziej dopracowany i zbadany. Niestety identyfikacja za pomocą linii papilarnych ma swoje wady: głębsze uszkodzenia powierzchni skóry mogą mieć wpływ na odczyt, a więc i na identyfikację danej osoby. Porównywanie linii papilarnych odbywa się poprzez wybór punktów charakterystycznych. Punkty te znajdują się w miejscach rozdzielenia, połączenia lub zakończenia linii rys. 5.10. Do opisu linii papilarnych z reguły wystarcza 30 – 40 punktów. Opis odcisku palca ma objętość kilkuset bajtów (tym większa im dokładniejsze jest badanie).

Systemy biometryczne, wykorzystujące geometrię dłoni są stosunkowo proste i szybkie w obsłudze. Specjalny czytnik, umieszczony wewnątrz urządzenia za pomocą promieni podczerwonych rejestruje: długość i szerokość dłoni użytkownika, grubość czterech palców (oprócz kciuka), a także obszar pomiędzy kostkami palców. Wszystkie te dane pozwalają na stworzenie trójwymiarowego zdjęcia ludzkiej dłoni pełniącego role wzorca do

pamięci systemu. Autoryzacja dokonuje się poprzez porównywanie kolejnych odczytów cech biometrycznych z wzorcem lub bazą wzorców[32] dłoni. Uwierzytelnienie na podstawie geometrii dłoni wykorzystuje fakt zróżnicowania kształtu dłoni u poszczególnych osób jak również niewielkie zmiany kształtu dłoni u danej osoby z biegiem czasu. System dokonuje pomiaru 90 cech charakterystycznych dłoni, w tym szerokość i grubość dłoni oraz długość i szerokość palców. Pomiary odbywają się przy zastosowaniu kamer lub metod mechanicznych tzw. rolek. Plik opisujący zajmuje jedynie kilka bajtów, co stanowi ważną zaletę, ponieważ umożliwia nie tylko weryfikację, ale również identyfikacje osób. Weryfikacja geometrii dłoni jest bardzo wygodną i wiarygodną metodą - dzięki temu znajduje zastosowanie w wielu systemach kontroli dostępu i rejestracji czasu pracy. Zalety tego rodzaju weryfikacji zostały uznane i docenione między innymi przez wiele amerykańskich instytucji rządowych i wojskowych.

Techniki rozpoznawania mowy koncentrują się na dwóch problemach: rozpoznawaniu mowy ciągłej (dzięki czemu możliwe będzie dyktowanie tekstu komputerowi) oraz rozpoznawanie charakterystycznych cech mowy. Jak się okazuje tempo głosu każdego z nas, sposób stawiania akcentu, szybkość wypowiadania zgłosek, charakterystyczne brzmienie tych głosek może być dobrym zestawem cech identyfikujących. Niestety zapewnienie najwyższego poziomu bezpieczeństwa autoryzacji dokonywanej głosem komplikuje dostępność doskonałych systemów nagrywania i odtwarzania dźwięku. Istnieje przecież możliwość zapisania ludzkiego głosu z dużą dokładnością a następnie odtworzenia tego dźwięku, że urządzenie weryfikujące nie będzie w stanie zorientować się, że jest oszukiwane. Dlatego też identyfikację przy użyciu rozpoznawania mowy warto wzbogacić o dodatkowe zabezpieczenia. Skonstruowano zaawansowane systemy rozpoznawania mowy połączone z systemami badającym geometrię twarzy. Nie chodzi tu jednak o statyczne „zdjęcie" twarzy człowieka. Urządzenie weryfikujące obserwuje bowiem napięcie mięśni twarzy jakie powstaje podczas mówienia. Każdej z weryfikowanych osób odpowiadać musi specyficzny wzorzec: złożony nie tylko z informacji na temat brzmienia poszczególnych głosek, ale również z informacji na temat sposobu poruszania ustami, specyficznych grymasów itd. Weryfikator przy pomocy wbudowanej kamery oraz czułego mikrofonu porównuje następnie sposób wypowiedzi danej osoby z tym zapisanym już w pamięci. Systemy tego typu zapewniają niezwykle łatwą autoryzację. W systemach biometrycznych

[32] Porównywanie cech biometrycznych z bazą wzorców rozumieć należy jako wyznaczenie minimum dolnej odległości miedzy wyznaczonymi cechami, a każdym z wzorców znajdujących się w bazie.

jednym z kluczowym problemów jest zapewnienie odpowiedniej unikalności odpowiedniej cechy. Problemem nie jest więc np. zbadanie wymiarów dłoni, ale przeprowadzenie badań stwierdzających jakie cechy dłoni i w jakiej kombinacji są odpowiednio unikalne. Z przeprowadzonych badań wynika jeden wniosek: jednym z najbardziej unikalnych identyfikatorów jest tęczówka oka. Posiada ona aż 266 punktów charakterystycznych. Jest to parokrotnie więcej niż punktów charakterystycznych odcisku palca. Jednak skanowanie oka jak na razie nie jest wykorzystana jako technologia powszechnego użytku. Dzieje się tak ponieważ w momencie wprowadzania tego typu urządzeń skanowanie siatkówki oka było procesem niewygodnym i nie przyjemnym dla użytkownika. Trzeba ustawić się w niewygodnej pozycji i znieść oślepiające białe światło skanera. Ponadto badania wskazują, że system ochrony na podstawie odcisku palca mają większą skuteczność i mniejszy margines błędu. W przypadku uwierzytelniania na podstawie wzoru tęczówki istnieje 400 różnych charakterystyk (zwanych stopniami swobody) pozwalającymi na jej opisanie. Systemy stosujące badanie tęczówki wykorzystują około 260 stopni swobody. Obecne systemy rozpoznawania tęczówki najpierw robią ogólne „rozpoznanie" zarysów twarzy w celu znalezienia oczu, w przeciwieństwie np. do urządzeń skanujących np. dłoń, którą trzeba w miarę równo ułożyć na urządzeniu.

Mechanizmy biometryczne oparte na charakterystycznych cechach twarzy użytkownika również zdobywają rosnącą popularność. Ich funkcjonowanie oparte jest po prostu na zasadzie niepowtarzalności ludzkich twarzy. Obrazy twarzy przechowywane są w postaci specyficznych matematycznych matryc, umożliwiających weryfikację twarzy użytkownika z zapisanym algorytmem. Metoda weryfikacji geometrii twarzy należy (obok weryfikacji tęczówki oka) do najmniej inwazyjnych. Nie jest wymagany absolutnie żaden kontakt fizyczny z urządzeniem. Wykorzystuje się fakt, że twarze dwóch różnych osób nigdy nie będą identyczne.

Biometria podpisu jest jedną ze starszych technik zabezpieczających. Dawniej analizowana przez grafologów, obecnie jest poważnym przedmiotem badań specjalistów od systemów biometrycznych. Podobnie, jak w przypadku urządzeń do identyfikacji mowy, także i tutaj zastosowano połączenie kilku technik. Weryfikacja odbywa się nie tylko na zasadzie porównania podpisu (dodajmy, że niezbędnym warunkiem jest tutaj takie samo podpisywanie się użytkownika), ale także na analizie powstawania podpisu - na jego dynamice. Systemy dokonujące uwierzytelniania na podstawie odręcznego podpisu bazują na statystycznej lub dynamicznej analizie podpisu. Analizie statycznej podlega sam podpis, natomiast analizie dynamicznej proces tworzenia podpisu nacisk długopisu, ruch ręki,

szybkość ruchu ręki przy poszczególnych fragmentach podpisu. Analiza na podstawie korzystania z klawiatury komputera opiera się na sposobie korzystania z komputera. Brana jest pod uwagę szybkość wpisywania znaków, czas, w jakim klawisz zostaje wciśnięty oraz czas pomiędzy naciśnięciem poszczególnych klawiszy.

Dziewięćdziesiąt dziewięć procent firm zajmujących się bezpieczeństwem koncentrują swoje wysiłki na technologiach szyfrowania i firewall'ach jako punktach kontrolnych do zastosowania w firmach. Szyfrowanie z pewnością zabezpiecza proces dostarczania danych a firewall strzeże dostępu do sieci wewnętrznych, lecz jeżeli intruz zna prawidłową nazwę użytkownika wchodząc np. w ich posiadanie przez metody z zastosowaniem inżynierii socjalnej i hasło może zdobyć dostęp do utajnionych informacji a tym samym spowodować zagrożenie bezpieczeństwa. Obie metody bowiem nie mają możliwości stwierdzenia czy odpowiednia osoba zyskała dostęp do danych. Biometria wypełnia poważną lukę powstałą w systemie zabezpieczeń. Pozwala zwiększyć pewność, że nazwa użytkownika i hasło zostały na prawdę wpisane przez ich posiadacza. Wielu pracowników poprzez zabezpieczenie prostym hasłem podważa bezpieczeństwo całej sieci. Bardzo trudno tego uniknąć, jednak przy zastosowaniu Biometrii nawet najprostsze hasła stają się niemal niemożliwe do przejścia przez niepowołane osoby. Nawet, jeżeli ktoś zna hasło innego użytkownika wciąż nie uzyskuje dostępu do jego konta czy systemu, podczas gdy prawowity właściciel nie ma z tym najmniejszego problemu. Systemy biometryczne są bardzo ciekawą alternatywa dla innych mechanizmów uwierzytelniania, ponieważ wykorzystują zarówno cechy anatomiczne jak i behawioralne użytkowników. Do pierwszej grupy zaliczamy identyfikację odcisków palców, tęczówki lub siatkówki oka, kształt dłoni, identyfikacje twarzy itp. Przykładami systemów uwierzytelniających na podstawie cech behawioralnych są rozwiązania wykorzystujące statyczna lub dynamiczną identyfikacje podpisu, biegłość w posługiwaniu się klawiaturą identyfikacje głosu itp. Nadal trwają badania nad ulepszaniem i wprowadzaniem nowych systemów uwierzytelniania, które są pewniejsze i wygodniejsze od przedstawionych tu. Są to takie identyfikacje jak na podstawie kształtu ucha, zapachu czy na podstawie zasolenia ciała.

5.4. Ochrona fizyczna

Jednym z podstawowych założeń w bezpieczeństwie informacji jest ochrona fizyczna. Nie jest to działanie czysto fizyczne, ale w jego skład wchodzi ograniczenie dostępu do miejsc, w których po dostaniu się do nich, mogło by dojść do ujawnienia informacji. Firmy

przeważnie wybierają „oszczędne" warianty ochrony. Jednak w przypadku informacji niejawnych niezbędne minimum regulują wydane ustawy i rozporządzenia.

W Polsce takimi dokumentami normatywnymi są:

1. Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych,
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji oraz Obrony Narodowej z dnia 26 lutego 1999 roku w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów,
3. Rozporządzenie Rady Ministrów z dnia 9 lutego 1999 roku w sprawie organizacji kancelarii tajnych

Jednostki organizacyjne, w których materiały zawierające informacje niejawne są wytwarzane, przetwarzane, przekazywane lub przechowywane, mają obowiązek stosowania środków ochrony fizycznej w celu uniemożliwienia osobom nieupoważnionym dostępu do takich informacji, a w szczególności przed:

- działaniem obcych służb specjalnych,
- zamachem terrorystycznym lub sabotażem,
- kradzieżą lub zniszczeniem materiału,
- próbą wejścia osób nieuprawnionych.

Służyć temu ma wprowadzenie stref bezpieczeństwa do poruszania się w jednostce. Strefa bezpieczeństwa jest to obszar, obiekt, fragment budynku, jedno lub kilka pomieszczeń, posiadające ściśle określone, oznaczone i strzeżone granice, w których są przechowywane, przetwarzane lub wytwarzane informacje niejawne o klauzuli „Poufne" lub wyższej.

Sygnał jest także emitowany do sieci energetycznej, z której urządzenia te są zasilane. Każdy z tych sygnałów niesie ze sobą pewne informacje. Wystarczy tylko je odczytać. Informacje te można odczytać wykorzystując specjalnie przystosowane anteny czy np. sieć wodną, elektryczną, grzewczą, oraz przewody klimatyzacyjne, nawet z kilkuset metrów. Odczytane w ten sposób informacje mogą być bezprawnie wykorzystane przez osoby nieupoważnione. Metody zabezpieczeń przed zjawiskiem promieniowania elektromagnetycznego są różne:

- wyklejanie ścian pomieszczeń metalowymi foliami i siatkami; zabezpieczenie komputerów przenośnych, według amerykańskich norm TEMPEST,
- kabiny elektromagnetyczne tzw. klatki Farradaya, w których umieszczane są urządzenia przetwarzające informacje niejawne - są odpowiednio uziemione i poziom promieniowania elektromagnetycznego wychodzący na zewnątrz jest tak niski, że nie jest możliwe jego odczytanie,

Głównymi zaletami kabin ekranujących są: duża i trwała skuteczność ekranowania (uziemienia); tłumienie fal akustycznych i elektromagnetycznych, zabezpieczenie przed przechwyceniem treści rozmów prowadzonych wewnątrz, bezpieczne wytwarzanie dokumentów na sprzęcie komputerowym, odseparowanie urządzeń elektronicznych od zakłóceń zewnętrznych w trakcie badań, strojenia lub pracy.

5.5. Wnioski

1. Systematyka rozpoznania elektronicznego różni się zasadniczo w ujęciu polskiej teorii i praktyce w stosunku do pojęć Sojuszu NATO. Występują części wspólne jak na przykład rozpoznanie optoelektroniczne OPTINT, ale są też i takie które zasadniczo się różnią nie tylko tym co robią ale i przeznaczeniem. Głównym tego przykładem jest rozpoznanie SIGINT. Rozpoznane SIGINT (dosłowne tłumaczenie wywiad sygnałów) w realizuje zadania na potrzeby wszystkich uczestników pola walki nie tylko konkretnej jednostki oraz instytucji rządowych. Dla konkretnej walczącej jednostki informacje z rozpoznania zabezpieczane są przez wsparcie elektroniczne (*Electronic Support Measure - ESM*) Ten typ rozpoznania występuje w pododdziałach WE. Natomiast w ujęciu polskiej teorii rozpoznanie elektroniczne zdobywa dane zarówno dla wojsk walczących, pozostałych uczestników pola walki i instytucji rządowych. Realizuje, więc całość zadań bez podziału.

Z tym podziałem ściśle wiąże się kierowanie rozpoznaniem i zakłócaniem. W polskiej armii rozpoznanie i zakłócanie jest w G2 natomiast w armiach NATO rozpoznanie jest w G2 a zakłócanie w G3. Wypracowana teoria przez polskich naukowców dotycząca połączenia i ujednolicenia metod i sposobów oraz rodzajów rozpoznania jak dotąd przynosi skutek pozytywny. Przy szybko zmieniającej się sytuacji na polu walki trudno sobie wyobrazić, aby „rozpoznanie robiło swoje a zakłócanie swoje". Jedność zadań i realizacji celu jest czynnikiem spajającym. Ten czynnik jeszcze mocniej będzie się uwidaczniał w działaniach o charakterze asymetrycznym, gdzie dowódca ciągle będzie narażony na brak informacji a gdyby jeszcze te dane zostały mu zakłócone przez własne pododdziały pozbawimy go możliwości przewidywania posunięć przeciwnika.

2. Aktualnie prawo polskie pozwala na podsłuchiwanie i monitorowanie przepływów informacji w sieciach informacyjnych jedynie w odniesieniu do łączności radiowej i to po stronie przeciwnej, natomiast zabrania w odniesieniu do przepływu informacji w sieciach komputerowych przez organy wojskowe. Takie prawo mają jedynie jednostki Ministerstwa Spraw Wewnętrznych za zgodą prokuratora oraz Służby Kontrwywiadowcze. Można, więc

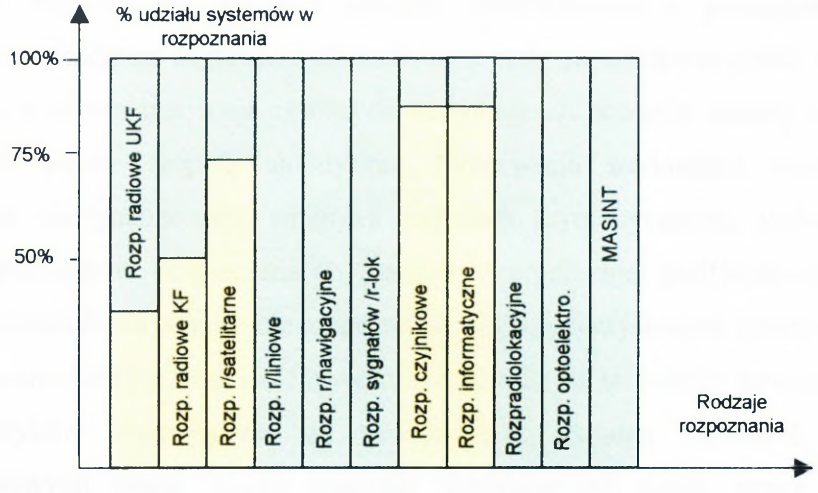
zadać pytanie: jak nazwać osoby zarządzające serwerami komputerowymi w sieci? Osoby te mogą w każdej chwili wtargnąć w system i dokonać zmian lub uniemożliwić dokonanie zmian. Czy zgodnie z prawem są przestępcami? Jaki jest zakres ich kontroli? Ustawa o ochronie danych osobowych zabrania ściągania i rozpowszechniania dla osiągnięcia korzyści danych informacyjnych o charakterze poufnym, a do takich niewątpliwie należą np. dane osobowe. Jak więc szkolić żołnierzy, którzy wyjeżdżają na misje pokojowe, gdzie może wystąpić konieczność działalności rozpoznawczej w lokalnych sieciach komputerowych, w których potencjalni terroryści przekazują sobie nawzajem informacje. Zajdzie wówczas potrzeba poszukania danych świadczących o zagrożeniu dla sił komponentu. Gdzie ich szkolić? Czy zatrudnić hakerów? Podobny problem szkolenia odnosi się nie tylko do żołnierzy wyjeżdżających w misje ale i do tych którzy mają realizować zadnia w innych operacjach. Brak nawyków i wiedzy w tym sposobie prowadzenia rozpoznania może skutkować niewłaściwymi decyzjami lub nawet poważnymi stratami w działaniach bojowych. Postawione pytania, w większości jeszcze dzisiaj, pozostają bez odpowiedzi. Zespół autorski jest przekonany, że w niedalekiej przyszłości ten rodzaj rozpoznania będzie podstawowym wykorzystywanym w siłach zbrojnych.

3. Każdy z przedstawionych sposobów prowadzenia rozpoznania elektronicznego jest wykorzystywany w większym lub mniejszym stopniu przez poszczególne podsystemy rozpoznawcze. Oczywistym jest, że nie wszystkie sposoby będą wykorzystywane przez wszystkie podsystemy, niektóre będą wykorzystywać tylko poszukiwanie i namierzanie elektroniczne jako wystarczający sposób zdobycia informacji, inne przechwytywanie, a jeszcze inne tj. rozpoznanie informatyczne traktuje poszczególne sposoby nieco inaczej. W rozpoznaniu elektronicznym namierzanie kojarzone jest z określeniem kierunku na źródło i jego lokalizacją, w rozpoznaniu informatycznym namierzanie to podążanie za potencjalnym włamywaczem do miejsca, z którego wtargnął do sieci. Musimy, więc rozróżnić poszczególne podejścia do problemu namierzania. Głównym mianownikiem pozostaje nadal wskazanie miejsca źródła. Zmienia się tylko metoda dotarcia do niego.

Realizując zadania w działaniach asymetrycznych często realizuje się zadania nie tylko strefie odpowiedzialności rozpoznawczej narzuconej przez przełożonego, ale także w tyłowej strefie. Zmienia się wówczas sposób prowadzenia rozpoznania i wykorzystywane rodzaje rozpoznania.

Na wykresie przedstawiono kolorem zielonym te rodzaje rozpoznania, które będą wykorzystywane w strefie odpowiedzialności rozpoznawczej a kolorem żółtym te, które będą wykorzystywane w tylnej strefie. Są to dane szacunkowe. Każde działanie i zmiana sytuacji

może doprowadzić do zmiany wartości procentowej. Niemniej przedstawione rodzaje rozpoznania elektronicznego w ogólnym założeniu nie powinny ulec zmianie. Komentarza wymaga rozpoznanie MASINT. Nie jest ono realizowane w naszych SZ z uwagi na brak urządzeń i możliwości prowadzenia tego typu rozpoznania. Zespół autorski uważa, iż ten typ rozpoznania głównie będzie realizowany w strefie odpowiedzialności rozpoznawczej przez pododdziały rozpoznawcze i grupy dywersyjne z uwagi na specyficzny sprzęt.



Rys. 5.5. Podział procentowy udziału poszczególnych rodzajów rozpoznania elektronicznego w strefie odpowiedzialności rozpoznawczej i strefie tyłowej

4. Bezpieczeństwo informacyjne jest na tyle bezpieczne na ile jego najsłabsze ogniowo jest odporne na oddziaływanie czynników zewnętrznych. Opierając się na badaniach firm komercyjnych najsłabszym ogniwem pozostaje człowiek i jego zachłanność. Nie można tego problemu generalizować, ale dane liczbowe przedstawiają człowieka jako ten element, który podatny jest najbardziej. Podnosząc świadomość żołnierzy obsługujących urządzenia przesyłające dane powinniśmy uzyskać oczekiwany efekt. Proces ten niestety jest czasochłonny i nie zawsze skuteczny. Dlatego doskonalenie sprzętu i oprogramowania pozwala na uniknięcie utraty informacji. Jeżeli osoby obsługujące dany system będą niewiele wiedziały o jego budowie i działaniu oprogramowania, tym system będzie bezpieczniejszy. Odnosi się to do zagrożeń wewnętrznych. Podobnie jest w odniesieniu do zagrożeń zewnętrznych. Im mniej o systemach zabezpieczeń przedostaje się do czynników ogólnodostępnych tym trudniej potencjalnym włamywaczom złamać systemy bezpieczeństwa.

6. EFEKTY POZNAWCZE

Zagrożenia asymetryczne współczesnego świata to problem zajmujący nie tylko specjalistów wojskowych. Z racji szeregu uwarunkowań i powiązań gospodarczo-politycznych potencjalne zagrożenia asymetryczne stały się obiektem analiz wielu ośrodków badawczych, a szereg instytucji cywilnych utrzymuje na potrzeby analizy i oceny sytuacji kryzysowych własne zespoły analityczne. Obserwacja środowiska międzynarodowego wskazuje, że zasygnalizowana tematyka zagrożeń asymetrycznych, wobec wzrastającej złożoności problemów bezpieczeństwa, zmiany uwarunkowań polityczno-militarnych oraz przemian strukturalnych w systemie rozpoznania sytuacji kryzysowych zyskuje na znaczeniu.

Wspomniana już duża ilość ośrodków badawczych na świecie sprawia, że lansowane przez teoretyków zajmujących się problematyką działań zbrojnych i stosunków międzynarodowych teorie, często znacznie odbiegają od siebie, przez co utrudniają, a niekiedy nawet uniemożliwiają konstruowanie wspólnych scenariuszy dotyczących przyszłości. W związku z tym trudno jest także prognozować i oceniać potrzeby rozpoznawcze skierowane na pozyskiwanie danych rozpoznawczych o zagrożeniach asymetrycznych.

Z militarnego punktu widzenia, na podstawie wniosków z analizy literatury można wyróżnić cztery typy ewentualnych przeciwników, z jakimi mogą mieć do czynienia siły zbrojne w pierwszych dekadach XXI wieku:

a) siły zbrojne konkretnego państwa, dysponujące kompleksowymi systemami uzbrojenia i odpowiednim zapleczem logistycznym (typowy konflikt zbrojny);

b) siły będące kombinacją grup kryminalnych i grup terrorystycznych (działania policyjno-wojskowe);

c) nieuzbrojone grupy wyznawców religijnych, będących pod wpływem ideologii (demonstracje, zamachy i walki partyzanckie);

d) kooperacja przestępców informatycznych oraz szpiegów gospodarczych.

Podział ten jednoznacznie wskazuje, że wymienione typy sił, z wyjątkiem pierwszego przypadku, mają charakter asymetryczny. Biorąc pod uwagę analizę konfliktów przełomu XX i XXI wieku, wielu ekspertów stwierdza, że współczesne siły zbrojne, przygotowane do prowadzenia klasycznych operacji wojennych, nie nadają się do

wykorzystania w konfliktach zbrojnych o charakterze asymetrycznym.

W podsumowaniu prowadzonych rozważań warto wskazać na fakt, że badania nad prognozowaniem i rozpoznawaniem zagrożeń asymetrycznych nie są nowym kierunkiem. Wieloaspektowość przedmiotowa i metodologiczna tej problematyki stwarza duże możliwości w poszukiwaniu metod i technik służących rozwiązywaniu problemów bezpieczeństwa. Do złożoności problematyki dochodzi także sceptycyzm odbiorców rezultatów prowadzonych ocen. Wątpliwości budzi szczególnie jakość otrzymywanych pomiarów i szereg założeń determinujących opisywane zjawiska w odniesieniu do potencjalnego – asymetrycznego - przeciwnika. Jednak jak wynika ze zgromadzonych doświadczeń, w procesie rozpoznawania zagrożeń, w tym szczególnie asymetrycznych mogą się realizować specjaliści z różnych dziedzin. Z racji złożoności badanych zjawisk szeroko rozumiana problematyka bezpieczeństwa w odniesieniu do działań asymetrycznych stwarza szansę zaprezentowania swej wiedzy zarówno ekspertom wojskowym jak i cywilnym.

Celem niniejszej pracy było określenie możliwości i wskazanie potrzeb w zakresie rozpoznawania i identyfikacji zagrożeń asymetrycznych? W związku z tak postawionym problemem zespół badawczy poszukiwał odpowiedzi na następujące pytania szczegółowe:

1. Jak identyfikować działania asymetryczne?
2. Jakie są możliwości rozpoznawania zagrożeń asymetrycznych w tyłowej strefie działań wojsk własnych?
3. Jaki są potrzeby w zakresie przygotowania systemu rozpoznania do realizacji zadań rozpoznawczych w systemie globalnego bezpieczeństwa?
4. Jak rozpoznawać zagrożenia asymetryczne spowodowane intensywnym rozwojem środków zdobywania, przetwarzania i dystrybucji informacji?

Identyfikacja i precyzowanie definicji odnoszących się do terminu zagrożenia asymetryczne sprawiła zespołowi autorskiemu szereg trudności[1]. Po pierwsze należy wskazać na fakt, że wobec braku jednolitego postrzegania problematyki zagrożeń asymetrycznych nie można w sposób jednoznaczny określić wszystkich cech badanego zjawiska. Po drugie kontekstowość postrzegania zagrożeń asymetrycznych wprowadza szereg utrudnień, co do rozróżnienia sposobu działania potencjalnego przeciwnika i wojsk własnych. Kolejną barierą jest brak jasno określonych wymagań dowódców, co do sposobu i zakresu wysiłku rozpoznawczego w działaniach asymetrycznych. Dlatego biorąc pod uwagę powyższe fakty przyjęto, że przez asymetrię rozumie się między innymi: odmienną taktykę walki, oddziaływanie na wrażliwe punkty w systemie walki strony przeciwnej, walkę informacyjną,

[1] Pierwszy problem badawczy.

zmagania informacyjne w sferze opinii publicznej, oraz groźbę lub wykorzystanie broni masowego rażenia. Przyjęcie do dalszego toku badawczego zaprezentowanego podziału sprawiło, że w kolejnych etapach pracy poszukiwano rozwiązań koncentrując uwagę na strefie tyłowej wojsk, rozprzestrzenianiu broni masowego rażenia i walce informacyjnej w kontekście dotyczącym rozpoznania, a więc zagadnień walki elektronicznej.

Z przeprowadzonych badań wynika jednoznacznie, że „tyłowy obszar/strefa działań" jest jednym z celów działań głębokich potencjalnego przeciwnika[2]. Ze względu na znajomość terenu i wsparcie miejscowej ludności przeciwnik może na tyłach wojsk stosować szeroki wachlarz środków niszczących, uszkadzających lub zakłócających działanie określonych obiektów infrastruktury. Celem działań asymetrycznych może być dezorganizacja funkcjonowania służb wsparcia, przerwanie linii komunikacyjnych, izolacja głównego obszaru działań od zgromadzonych zasobów logistycznych, a także pozbawienie dowódcy bezpiecznie i efektywnie funkcjonującego zaplecza zabezpieczającego prowadzone działania. Prawdopodobnymi obiektami uderzeń mogą być: wojska, systemy transportu (kolej, porty morskie, kanały, lotniska, mosty itd.), urządzenia logistyczne (stacje MPS, rurociągi, składy materiałowe), elektrownie (w tym atomowe), zakłady przemysłowe, stacje łączności itp.

Przedstawione fakty skłaniają do wniosku, że istnieje konieczność rozlokowania sił zapewniających bezpieczeństwo rejonu operacji oraz prowadzących działania rozpoznawcze w strefie tyłowej. Szczególnie istotne jest to w operacjach stabilizacyjnych i pokojowych, gdzie strefa tyłowa to w praktyce obszar odpowiedzialności sił wielonarodowych.

W kontekście działalności rozpoznawczej stwierdzono, że największe zagrożenie asymetryczne generowane jest przez organizacje terrorystyczne. Stwierdzono, że istnieją dwa podstawowe podejścia w zwalczaniu terroryzmu - reaktywne i proaktywne. Zgodnie z pierwszym podejściem wojska świadome swej sytuacji, oczekują na zamach terrorystyczny i podejmują działania aby, w miarę rozwoju wydarzeń ograniczyć straty osobowe i rzeczowe. Inna opcją jest podejście proaktywne. Zgodnie, z którym można przewidywać nadchodzące zamachy terrorystyczne i dobrze przygotowywać się na ich efekty. Wynika z tego, ze działanie proaktywne zwiększa prawdopodobieństwo zapobiegania atakom terrorystycznym i umożliwia uniknięcie zarówno strat w ludziach, jak i szkód dotyczących środowiska operacji. Dotychczasowe doświadczenia wskazują, że proaktywne podejście do terroryzmu jest lepszą opcją bowiem zapewnia skuteczniejszy sposób prewencji zamachów terrorystycznych. W rezultacie otrzymanych wyników badań można stwierdzić, że rozpoznanie, jest narzędziem, które umożliwi zbadanie otoczenia w celu ujawnienia

[2] Drugi problem badawczy.

i ustalenia potencjalnych rejonów i źródeł aktywności terrorystycznej. Ponadto stwierdzono, że zgromadzone informacje rozpoznawcze pozwolą na określenie potencjalnych obiektów będących w zainteresowaniu terrorystów.

Dokonując identyfikacji problemu rozpoznania w działania partyzanckich należy stwierdzić, że nie znajdują one większego zainteresowania we współczesnych doktrynach militarnych jak również rozważaniach teoretycznych. Ogólnie można stwierdzić, że działania partyzanckie można zakwalifikować jako formę działań nieregularnych prowadzoną na obszarze tyłowej strefy.

Ponadto jedną z istotnych cech partyzantki jest fakt, że przeciwnik na zajmowanym terytorium ma z reguły zdecydowaną przewagę liczebną w wojskach, uzbrojeniu i wyposażeniu (środki komunikacji i łączności) posiada rozbudowany aparat administracji i bezpieczeństwa wewnętrznego, a często także dysponuje środkami przekazu (prasa, radio, telewizja). Działania partyzanckie to zdecydowanie zaczepny charakter walki (bowiem w obliczu przewagi przeciwnika partyzanci mogą liczyć na sukces tylko wtedy, kiedy sami wybiorą miejsce, czas i formę ataku). Jak wskazują doświadczenia historyczne żaden okupant, ani żaden rodzimy reżim nie jest w stanie kontrolować całego terytorium, ani w pełni chronić i bronić wszystkich obiektów i urządzeń o znaczeniu wojskowym, ekonomicznym, administracyjnym i politycznym. Stąd wynika wyskoki poziom zagrożenia asymetrycznego[3].

W procesie badawczym ustalono, że w prowadzeniu rozpoznania poziomu aktywności działań partyzanckich ważnymi elementami są elektroniczne urządzenia wykrywające (czujniki), które powinny być w zasadzie przeznaczone do wykrywania obecności lub przemieszczania sił partyzanckich. Dodatkowo do rozpoznawania terenów opanowanych i patrolowych przez partyzantów powinny być wykorzystywane samoloty rozpoznawcze, wyposażone w elektroniczne urządzenia rozpoznawcze (czujniki). Za pomocą urządzeń elektronicznych (czujników) zrzucanych z samolotów można uzyskiwać szereg cennych informacji o partyzantach, a zwłaszcza o zmianach zachodzących w położeniu ich sił i kierunkach przemarszu.

Bardzo ważną kwestią w rozpoznawaniu charakteru działalności partyzanckiej są przesłuchania, które powinny być przeprowadzane przez personel rozpoznania oraz tłumaczy zwerbowanych pośród miejscowej ludności. Jak wskazują doświadczenia, istotą działań rozpoznawczych tego rodzaju jest pozyskiwanie informacji bezpośrednio od osób utrzymujących kontakt z partyzantami.

[3] Afganistan, Irak, Somalia.

W zakresie rozpoznania działalności sił specjalnych potencjalnego przeciwnika ustalono, że głównymi obiektami działań specjalnych będą elementy infrastruktury gospodarczej lub bytowej. Zatem obiektami oddziaływania asymetrycznego, szczególnie w tyłowej strefie wojsk będą wybrane elementy ośrodków przemysłowych i gospodarczych, infrastruktura energetyczna, wodna itp. Dlatego można wnioskować, że urządzenia lotniskowe, porty morskie i śródlądowe wraz z całą infrastrukturą komunikacyjną staną się ważnymi obiektami zagrożonymi działalnością dywersyjną i obiektami ataków sił specjalnych.

Wyniki badań skłaniają do wniosku, że działanie dywersyjne to całe spektrum przedsięwzięć podejmowanych przez odpowiednio zorganizowane i przygotowane zespoły ludzi lub pododdziały wojsk, z zasady w celu zdezorganizowania życia politycznego i administracyjno-gospodarczego w kraju i obniżenia potencjału militarnego strony przeciwnej. Dlatego rozpatrując działania asymetryczne należy się liczyć, że będą skierowane przede wszystkim przeciwko strukturom władzy administracyjno-państwowej, komunikacji, transportom wojskowym, wybranym obiektom przemysłowym, a nawet przedstawicielom politycznym. Do prowadzenia działań dywersyjnych mogą być użyte zawczasu przygotowane i zorganizowane pododdziały specjalne, partyzanckie, rozpoznawcze, organizacje paramilitarne oraz lokalne grupy ludności (np.: mniejszości narodowe).

W rezultacie przeprowadzonych badań ustalono, że działania asymetryczne mogą mieć na celu skupienie sił i środków walki z frontu zewnętrznego, hamowanie dopływu zaopatrzenia z wnętrza kraju, dezorganizację kluczowych obszarów przemysłu lub poszczególnych zakładów prowadzących produkcję na potrzeby sił zbrojnych, utrudnianie zaopatrywania wojsk i ludności na obszarze konfliktu[4]. Wyraża się to głównie w dezorganizacji funkcjonowania linii komunikacyjnych, w tym szczególnie węzłów drogowych i kolejowych, utrudnianiu przegrupowania wojsk, niszczeniu składów oraz magazynów, rurociągów paliw płynnych, dezorganizacji systemu dowodzenia wojskami i łączności.

Innym źródłem zagrożeń asymetrycznych są organizacje przestępcze, które zawsze wykorzystują słabości systemu prawnego i gospodarczego, w jakim działają a obszar konfliktu zapewnia im szczególnie dobre warunki funkcjonowania[5]. Terroryści, przemytnicy narkotyków, handlarze ludźmi, osoby dokonujące nadużyć finansowych działają tak, jak gdyby nie istniały granice państw: w jednym kraju mogą zaplanować przestępstwo, w drugim

[4] Powyższą tezę potwierdzają wydarzenia z Afganistanu, Iraku i Somalii.
[5] Brak sił porządkowych, zmiana władzy, trudności zaopatrzeniowe, itd.

zrealizować plan, a mieszkać na stałe w trzecim. Każda organizacja przestępcza dąży do rozszerzenia swych wpływów, majątku i pola działania, a w konsekwencji zdobycia większej lub mniejszej władzy politycznej. Należy zatem przyjąć, iż zorganizowana przestępczość w postaci mafii stanowi niejako ostatni szczebel organizacyjnego rozwoju, jaki może przybrać, zbrojna organizacja przestępcza. Dlatego też w opinii zespołu autorskiego, działalność zorganizowanej przestępczości musi być poddana stałemu monitorowaniu ze strony służb bezpieczeństwa i wojsk odpowiedzialnych za realizację zadań, szczególnie w tyłowej strefie działania wojsk lub w obszarze operacji pokojowej.

Powyższe argumenty wskazują, dlaczego lista zagrożeń asymetrycznych w tyłowej strefie działań oraz układ priorytetów z nimi związanych zmienia się wraz z czasem operacji oraz w zależności od położenia, kultury i składu demograficznego ludności obszaru działań. Analizując przebieg działań operacyjnych, zespół autorski stwierdził, że w określonym punkcie przestrzeni i czasu operacyjnego niektóre zagrożenia zanikają, inne się ujawniają lub trwają nadal, a jeszcze inne wyłaniają się ponownie ze zwiększoną siłą.

Podsumowując zatem uzyskane wyniki badań, należy stwierdzić, iż rodzaje zagrożenia asymetrycznego w obszarze operacji ewoluują wraz ze zmianami w dziedzinie taktyki i sztuki operacyjnej, rozwoju środków walki oraz wprowadzenia nowych technologii. Efekty i korzyści, jakie są ich wynikiem, pozwalają przypuszczać, iż będą one w dalszym ciągu doskonalone w przyszłych konfliktach, chociaż obszary ich oddziaływania mogą się zmieniać w zależności od zmian zachodzących w środowisku walki.

W ramach kolejnego problemu badawczego poszukiwano rozstrzygnięcia kwestii możliwości rozpoznania sposobów rozprzestrzeniania broni masowego rażenia, postrzeganej jako jedna z form zagrożenia asymetrycznego we współczesnym świecie[6]. Punktem wyjścia do rozważań było założenie, iż od rozpoczęcia transformacji ustrojowej związanej z zasadniczymi zmianami w otoczeniu międzynarodowym Polski, istnieje konieczność ciągłego rozpoznania w systemie globalnego bezpieczeństwa, proliferacji broni masowego rażenia (broni jądrowej i biologicznej) i zagrożeń związanych z przemysłem zbrojeniowym. Ponadto w ramach badań ustalono wpływ posiadania broni masowego rażenia na kształtowanie bezpieczeństwa międzynarodowego. Stwierdzono, że utrzymanie pokoju regionalnego i lokalnego, równowagi oraz stabilizacji w rejonach najbardziej zagrożonych możliwością użycia broni masowego rażenia zależy od skutecznego zapobiegania jej dalszemu rozprzestrzenianiu się, w tym szczególnie technologii i środków pozyskiwania materiałów do produkcji.

[6] Trzeci problem badawczy.

Problem proliferacji broni jądrowej pojawił się w kontekście rozpadu ZSRR i podziału jego arsenału nuklearnego miedzy kilka państw. Nieco później doszły obawy o bezpieczeństwo przechowywania i ochrony posrtadzieckiej broni jądrowej. Pojawiły się opinie ekspertów, że nastąpi osłabienie kontroli nad potencjałem nuklearnym i możliwy jest wypływ technologii jądrowych i specjalistów w tej dziedzinie do innych państw. Konsekwencją braku kontroli nad wiedzą z zakresu broni jądrowej jest fakt, że kilka państw pracuje nad rozwojem własnych programów nuklearnych, a także programu rozwoju pocisków balistycznych zdolnych do przenoszenia broni jądrowej. Próby, które miały miejsce na subkontynencie indyjskim (np.: Indie i Pakistan u schyłku lat dziewięćdziesiątych) oznaczają rozpoczęcie nowego nuklearnego wyścigu zbrojeń. W 2003 roku świat obiegła wiadomość, że Korea Północna jest zdolna wyprodukować własną broń jądrową. Natomiast 9 października 2006 roku Koreańczycy przeprowadzili pierwszą próbę jądrową, wywołując wzburzenie opinii publicznej na świecie[7].

Kolejnym źródłem zagrożeń asymetrycznych w zakresie rozprzestrzeniania się broni masowego rażenia stały się państwa rządzone przez dyktatorów. Dyktatorzy zyskali swobodę działania na skutek rozluźnienia kontroli ze strony organizacji międzynarodowych, przez co stali się samodzielnymi aktorami na arenie świata. Najbardziej niebezpieczni z nich, którzy dążą do pozyskania lub posiadania broni jądrowej stali się poważnym zagrożeniem nie tylko w skali regionu, ale stwarzają potencjalne zagrożenie dla społeczności międzynarodowej.

Istotnym elementem w pracy zespołu badawczego była analiza możliwości rozpoznania wykorzystania w działaniach asymetrycznych broni biologicznej. Na podstawie wniosków z literatury przedmiotu stwierdzono, że możliwość użycia broni biologicznej stanowi istotne zagrożenie zarówno dla wojska, jak i dla ludności cywilnej, dlatego zasadnym jest mówić o tym w kontekście wojny biologicznej rozumianej jako specjalne zastosowanie osiągnięć nauki do rozsiewania na wybranym obszarze w populacji ludzkiej, zwierzęcej i roślinnej zarazków (bakterii, wirusów i grzybów) w celu zakażania, wywoływania chorób i eksterminacji wybranej populacji oraz niszczenia środowiska naturalnego.

Z punktu widzenia rozpoznania głównym problemem jest czas wykrycia ataku, gdyż środki broni biologicznej są trudne do identyfikacji. Uderzenie przeprowadzone skrycie, ze względu na trudności we wczesnym wykrywaniu przyczyny zachorowania lub zgonu zostaje rozpoznane dopiero w głównej fazie operacji. W takim bowiem przypadku chodzi

[7] Rada Bezpieczeństwa ONZ uchwaliła szereg sankcji finansowych i gospodarczych wobec Korei Północnej – ta jednak zareagowała zapowiedzią kolejnych testów jądrowych. Wywiady państw zachodnich potwierdzają, że prowadzone są przygotowania do następnych prób.

o odpowiedź na pytanie, czy epidemia wybuchła z przyczyn naturalnych czy też w wyniku sztucznego rozsiewu zarazków. Szczególnie trudne jest rozpoznanie przyczyn epidemii w warunkach niskiego poziomu sanitarnego społeczności dotkniętej tragedią. Dlatego należy domniemywać, że działaniach asymetrycznych środki biologiczne mogą być zastosowane w celu trwałego lub czasowego wyeliminowania sił strony przeciwnej z walki.

W ocenie zespołu badawczego rozwój biotechnologii i inżynierii genetycznej budzi obawy nie tylko ze względu na zagrożenia, a więc możliwość wykorzystania efektów naukowych badań w celach eliminacji ludzi lub celowego spowodowania rozprzestrzeniania się chorób, ale także z powodu przerażających wizji społeczno-politycznych skutków rewolucji biotechnologicznej.

We współczesnych stosunkach międzynarodowych zbrojenia, ich regulacja i kontrola są czołowym problemem nurtującym społeczność międzynarodową. Siła militarna nadal pozostaje jednym z zasadniczych elementów polityki zagranicznej państwa, służąc realizacji określonych potrzeb oraz interesów i przyczynia się do osiągania zamierzonych celów. W tym kontekście należy stwierdzić, że o możliwościach państwa świadczy jego przemysł zbrojeniowy, stan infrastruktury techniczno-obronnej, zaplecze logistyczne oraz wiele różnych elementów kształtujących poziom gotowości bojowej sił zbrojnych. W ocenie zespołu autorskiego obawy przed skutkami osiągnięcia przewagi militarnej przez potencjalnych przeciwników, dążenie do uzyskania równowagi sił lub zbudowania potencjału wojskowego dającego gwarancję sukcesu w obronie lub po dokonaniu napaści – to główne stymulatory zbrojeń.

Rozwój nauki i techniki przyspiesza ewolucję procesu wytwarzania nowych środków uzbrojenia i wyposażenia sił zbrojnych. Wprowadzane są coraz doskonalsze rodzaje broni z wykorzystaniem osiągnięć elektroniki, nowych materiałów konstrukcyjnych, systemów napędowych i środków wybuchowych. Współczesną broń konwencjonalną nowej generacji charakteryzuje wyjątkowa precyzja działania, daleki zasięg, duża mobilność, niezależność od warunków atmosferycznych. Systemy rażenia są wyposażone w nowoczesne urządzenia komputerowe, fotooptyczne, optoelektroniczne, noktowizory, inteligentne elementy kierowania, rozpoznania i łączności, a także mechanizmy pozwalające jej działać bez bezpośredniego uczestnictwa człowieka. Zastosowanie nowoczesnej broni radykalnie zmienia sytuację w obszarze operacji[8]. Udostępnienie lub pozyskanie nowych technologii przez

[8] Wojna w Zatoce Perskiej w 1991 r. potwierdziła postęp w rozwoju broni konwencjonalnych nowej generacji. Według źródeł amerykańskich, bomby sterowane laserowo, które stanowiły zaledwie 9% ogółu użytych środków rażenia, spowodowały około 75% zniszczeń na terytorium irackim.

państwa niedemokratyczne może prowadzić do eskalacji zagrożeń asymetrycznych i niekontrolowanego starcia zbrojnego o wysokiej intensywności. Zjawiskiem nierozerwalnie związanym ze zbrojeniami jest handel bronią. Należy wskazać na fakt, że do czołówki eksporterów broni należą również stali członkowie Rady Bezpieczeństwa ONZ. Od wielu lat grono eksporterów broni rozdzieliło rynki handlu między USA, Federację Rosyjską, Wielką Brytanię, Francję i Chiny. Jak wynika z analizy materiałów źródłowych większość dostaw środków uzbrojenia skierowana była do Europy Zachodniej. Część przekazywano do państw Bliskiego Wschodu (Arabia Saudyjska, Izrael, Egipt) oraz Dalekiego Wschodu (Japonia, Tajwan, Korea Południowa). Poza tym odbiorcami uzbrojenia pozostają państwa Oceanii, Afryki, Azji Południowej oraz Ameryki Południowej i Północnej.

W efekcie przeprowadzonych analiz ustalono, że aktywność przemysłu zbrojeniowego jest w dużej mierze warunkowana przez postęp naukowo- techniczny. Jednym z wielu nowych kierunków rozwoju środków walki jest konstruowanie broni o zmniejszonej śmiercionośności (obezwładniającej), przeznaczonej do czasowego wyłączenia z walki siły żywej przeciwnika i jego sprzętu wojskowego. Taka broń nie powoduje trwałego porażenia lub zniszczeń przyczynia się do zmniejszenia ilości ofiar starcia zwłaszcza wśród ludności cywilnej. Dlatego w sferze zainteresowania zespołu badawczego znalazły się także aspekty dotyczące przeciwdziałania zagrożeniom asymetrycznym z wykorzystaniem broni obezwładniającej.

Reasumując można stwierdzić, że proces globalizowania się bezpieczeństwa oraz wzrost zagrożeń transnarodowych, jak również prawdopodobieństwo postępującej asymetrii, podpowiadają pilną potrzebę ciągłego śledzenia sytemu ogólnego bezpieczeństwa, ale nade wszystko stworzenia i wcielania w życie instytucji prowadzącej rozpoznanie ich przeobrażeń (ewolucji). Zagrożenia asymetryczne w tym szczególnie kwestie rozprzestrzeniania się broni masowego rażenia oraz handlu bronią powinny stanowić przedmiot zainteresowania systemów rozpoznania.

Zgromadzone fakty wskazują, że po doświadczeniach wyniesionych z konfliktów lokalnych siły zbrojne szeregu państw przykładają obecnie coraz większą wagę do rozwoju i budowy programów zmierzających do prowadzenia rozpoznania w środowisku informacyjnym[9]. Ponadto z przebiegu konfliktów wynika, że efektywne wykorzystanie współczesnych sił i środków walki w działaniach militarnych jest możliwe pod warunkiem posiadania aktualnych informacji o położeniu i działaniu sił potencjalnego przeciwnika w całym obszarze operacji. Zadanie to może zapewnić jedynie należycie zorganizowany

[9] Czwarty problem badawczy.

system rozpoznania wykorzystujący różnorodne środki, zdolne do pozyskiwania danych w całej strefie odpowiedzialności rozpoznawczej. Stwierdzono, że w każdej ze stref rozpoznania będą realizowane zadania w spektrum elektromagnetycznym, ale w każdej z nich z wykorzystaniem innych sposobów działania i inne będą priorytety użycia elektronicznych podsystemów rozpoznawczych. Poszczególne zadania rodzajów rozpoznania będą zmieniały się w zależności od rozwoju sytuacji.

Infrastruktura informacyjna coraz bardziej nabiera charakteru globalnego, jeśli chodzi o wzajemne połączenia między łączami transmisyjnymi a sieciami, rozwój podstawowych technik oraz własność zasadniczych, eksploatowanych części składowych. Ta coraz bardziej widoczna międzynarodowa natura infrastruktury i jej operatorów stanowi ważne zagadnienie przy analizowaniu kierunków rozwoju zagrożeń asymetrycznych.

Ruch w sieciach telekomunikacyjnych przekraczający granice państw wzrasta systematycznie. Ciągły postęp technik telekomunikacyjnych i informacyjnych sprawił, że zachowanie kontroli informacyjnej stało się trudne. Powstanie szerokopasmowego Internetu umożliwiło bezprzewodowe przesyłanie informacji przez granice, co jest w ocenie specjalistów znacznie trudniejsze do monitorowania i kontroli niż transmisja telegraficzna czy telefoniczna. Rozpoznanie zagrożeń asymetrycznych na aktualnym poziomie globalnej informatyzacji nie może przejść obojętnie wobec faktu bardzo szerokiego wykorzystania łączy internetowych do przekazywania informacji lub jej zaboru.

Z uzyskanych wyników badań wyraźnie wynika, iż rozpoznanie informatyczne nie ma swojego odpowiednika w ujęciu systematyki NATO. Taki stan rzeczy jest głównie związany z występowaniem tego rodzaju działań w walce informacyjnej jako odrębnego rodzaju działalności. W polskiej teorii działań informacyjnych nie występuje termin rozpoznanie informatyczne. Dlatego, autorzy mając świadomość, że występują inne poglądy klasyfikujące i przyporządkowujące rozpoznanie informatyczne, przyjęli, iż przy obecnym stanie wiedzy można przyporządkować rozpoznanie informatyczne do zakresu zadań rozpoznania elektronicznego.

Stwierdzono, że w typowych działaniach militarnych rozpoznanie informatyczne jest bardzo trudne. Po pierwsze - stanowiska dowodzenia mają z reguły zamknięty system informatyczny. Po drugie – przełożeni z podwładnymi komunikują się albo za pomocą łącz stałych (np.: działania obronne) albo drogą radiową na niewielkie odległości. Po – trzecie moc transmisji jest ograniczona i dostępność energetyczna uniemożliwia śledzenie wymiany danych w sieci. Dlatego należy poszukiwać miejsc i osób, które będą łączyły się z siecią otwartą i wówczas próbować pozyskiwać dane rozpoznawcze.

Rozpoznanie informatyczne powinno być realizowane przez oficerów w wyspecjalizowanych komórkach organizacyjnych, z odpowiednio przygotowanymi narzędziami (programami) wraz z odpowiednimi urządzeniami. Rozpoznanie informatyczne można podzielić na dwie główne grupy zadań. Pierwsza obejmuje zadania związane z ochroną własnych systemów informatycznych przed niepowołanym dostępem. Druga grupa zadań dotyczy monitorowania przepływu danych w sieciach komputerowych podejrzanych organizacji.

W działaniach asymetrycznych obiektami ataków w wymiarze elektronicznym są głównie systemy komputerowe i systemy łączności. Te ostatnie szczególnie poprzez zakłócanie elektroniczne, a te pierwsze poprzez włamania osób niepowołanych. W tym kontekście nowego wymiaru nabiera utrzymanie bezpieczeństwa informacji w kanałach i sieciach informacyjnych. Stwierdzono, że bezpieczeństwo informacyjne zachowane jest głównie poprzez stosowanie odpowiednich kodów (mikroukłady szyfrujące). Ustalono także, iż o bezpieczeństwie sieci decyduje - podejście systemowe, a więc kompleks działań technicznych, logistycznych i organizacyjnych. Dlatego należy stwierdzić, że projektowanie systemów bezpieczeństwa wymaga całościowego spojrzenia na bezpieczeństwo danej organizacji, bowiem nie można tworzyć skutecznego systemu bezpieczeństwa bez ustalenia kompleksowych potrzeb. Ponadto w odniesieniu do armii, trzeba wskazać na fakt, że aby zapewnić właściwy poziom bezpieczeństwa systemy zabezpieczeń muszą integrować produkty pochodzące od różnych producentów. Dlatego jak ustalono w rezultacie przeprowadzonych badań, stosuje się różne metody ochrony systemów informacyjnych.

Proces ten niestety jest czasochłonny, a mimo to, jak wskazuje praktyka nie zawsze skuteczny[10]. Dlatego jedynie doskonalenie sprzętu i oprogramowania pozwala na uniknięcie utraty informacji. Ponadto nie budzi wątpliwości teza, że im mniej informacji o systemach zabezpieczeń przedostaje się do czynników ogólnodostępnych tym trudniej potencjalnym agresorom złamać systemy bezpieczeństwa.

[10] Mimo wielu wysiłków informatyków kolejne wersje programów Microsoft nie zawsze są wolne od błędów.

ZAKOŃCZENIE

Współczesne bezpieczeństwo narażone jest obecnie na nowy rodzaj zagrożeń, nazywany powszechnie zagrożeniami niekonwencjonalnymi lub asymetrycznymi. Biorąc pod uwagę zdolność do wykonywania potencjalnych zniszczeń i zadawania strat można wnioskować o ich nieproporcjonalnie dużej skali oddziaływania potencjalnego przeciwnika w stosunku do zastosowanych sił i środków. Istotnym aspektem nowych zagrożeń jest ich medialność oraz sposób oddziaływania na wyobraźnię opinii publicznej[1]. Ponadto zagrożenia asymetryczne są bardzo trudne do rozpoznania a co za tym idzie również i do zwalczania. Przede wszystkim ze względu na nieprzewidywalność ich wystąpienia i wysoką skuteczność.

W wyszczególnionych w pracy, problemach badawczych wyeksponowano zasadnicze efekty naukowego poznania, które odzwierciedlają stopień osiągnięcia celu pracy i zakres rozwiązania wyznaczonych w kontekście celu zagadnień szczegółowych. Wyniki uzyskane w efekcie przeprowadzonych badań w pełni potwierdziły zasadność i celowość podjęcia prac nad tematem.

Przedstawione w efektach poznawczych pracy ustalenia powinny zostać empirycznie zweryfikowane podczas ćwiczeń i treningów sztabowych (szczególnie zagrożenie strefy tyłowej, proliferacja broni masowego rażenia, zakłócenia w pracy sieci teleinformatycznych) w procesie kształcenia w Akademii Obrony Narodowej. Niemniej jednak zebrany materiał naukowy zdaniem autorów, w zaprezentowanej postaci może być traktowany jako źródło wiedzy o zagadnieniach związanych z problematyką rozpoznania w działaniach asymetrycznych. Zebrana wiedza w opinii autorów, może być także wykorzystana w praktycznej działalności szkoleniowej wojsk (sztaby i dowództwa). Podkreślić należy jednak, że ze względu na teoretyczny charakter pracy, w wymiarze jednostek wojsk operacyjnych koniecznym jest przełożenie zgromadzonych treści na rozwiązania praktyczne, dlatego muszą być one poparte empiryczną weryfikacją. Bowiem jak wykazano w toku badań zakres zagrożeń asymetrycznych jest warunkowany szeregiem czynników, a do najważniejszych należy zaliczyć: poziom dowodzenia, charakter operacji i rodzaj środowiska.

Koncentrując się na aspektach poznawczych, zespół autorski starał się, aby praca miała charakter utylitarny, aby jej wyniki – wnioski z badań mogły być wykorzystane:

---

[1] Zamach terrorystyczny w Madrycie doprowadził do wycofania wojsk hiszpańskich z Iraku.

1. W wojskach lądowych – dla pogłębienia wiedzy w obszarze rozpoznania. Wyniki badań mogą być przyczynkiem zmian racjonalizujących system rozpoznania oraz pracę sztabową zintegrowanych zespołów rozpoznania w zakresie oceny i prognozowania zagrożeń asymetrycznych.
2. W zespołach badawczych – pracujących nad nowymi rozwiązaniami w dziedzinie systemów rozpoznania, dowodzenia i kierowania ogniem.
3. W procesie dydaktycznym realizowanym w AON jako źródło wiedzy o źródłach zagrożeń asymetrycznych i sposobach ich rozpoznawania.
4. Dla pracowników nauki – jako inspiracja do podjęcia badań w obszarach, o których z racji tematu i celu pracy wspomniano tylko sygnalnie, a które wymagają badań szczegółowych (np.: proces oceny zagrożeń asymetrycznych w operacjach stabilizacyjnych).

Zespół autorski zakłada, że propozycje rozwiązań poszczególnych problemów mogą być przydatne w procesie kształcenia kadry nie tylko na potrzeby rozpoznania. Prezentowana praca w opinii zespołu autorskiego jest pierwszą, która wypełnienia istniejącą lukę w wiedzy dotyczącej szeroko rozumianej problematyki rozpoznania w działaniach asymetrycznych na potrzeby procesu dydaktycznego w Akademii Obrony Narodowej.

BIBLIOGRAFIA:

1. Antoszkiewicz J., *Metody heurystyczne*, Warszawa 1986.
2. Balcerowicz B., *Wybrane problemy obronności państwa*, Warszawa 1997.
3. *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku.* pod. red. D.B. Bobrow, E. Haliżak, R. Zięba, Warszawa 1997.
4. Bolechów B., *Terroryzm w świecie podwubiegunowym*, Toruń 2002.
5. *Broń masowego rażenia w świetle prawa międzynarodowego. Wybrane problemy*, Praca zbiorowa, AON, Warszawa 2004.
6. Brzeziński Z., *Wielka szachownica*, Warszawa 1998.
7. Ciborowski L. *Rola i miejsce rozpoznania w systemie obronnym Rzeczypospolitej Polskiej,* Warszawa, AON 1993.
8. Ciupiński A., Legucka A. *Podstawowe elementy polityki bezpieczeństwa i obrony Rzeczpospolitej Polskie*j, AON, Warszawa 2003.
9. Denning D. E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa, WNT 2002.
10. Durys P. K*ryzys nuklearny wokół KRLD*, A. Marszałek, Warszawa – Toruń 2003.
11. Endicott S., Hagerman E., *The United States and Biological Warfare: Secrets from the Early Cold War and Korea*, Indiana University Press, Bloomington 1998.
12. *Epidemiologia działań wojennych i katastrof,* pod. red. Chomiczewski W. Grzybowski K. Gall, J. Medica Press 2001.
13. Gawliczek P, Pawłowski J., *Zagrożenia asymetryczne*, AON, Warszawa 2003.
14. Hrynkiewicz – Żabicki A. *Dylematy i wyzwania polityki nuklearnej NATO w świetle ewolucji środowiska bezpieczeństwa międzynarodowego*, Warszawa, 2004.
15. Huntington S., *Zderzenia cywilizacji*, Warszawa 1998.
16. Jałoszyński K., *Koncepcja współczesnych działań antyterrorystycznych*, AON, Warszawa 2003.
17. Janczak J. *Kierunki rozwoju rozpoznania i zakłócania elektronicznego*, Warszawa, AON 2001.
18. Janczak J., Świdzikowski G. *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*, AON, Warszawa 2004.
19. Kamiński S., *Nauka i metoda, Lublin*, Towarzystwo Naukowe Katolickiego Uniwersytetu Lubelskiego 1992.
20. Kisiel J., *Rozpoznanie wojskowe,* Warszawa, AON 1998.
21. Kisielnicki J., *Metody systemowe*. PWE, Warszawa 1986.
22. *Kryminologiczne i prawne aspekty przestępczości zorganizowanej*, pod. red. A. Marek, W. Pływaczewski, WSPol Szczytno 1992.
23. Laqueur W., *The New Terrorism. Fanaticism and the Arms of Mass Destruction*, London 2001.
24. Lewicki C., *Zbiór zadań ze statystyki dla pedagogów*, Rzeszów 1996.
25. M. Łokociejewski, *Taktyczny system rozpoznania i walki elektronicznej wojsk lądowych,* Warszawa, AON 2000.
26. Multan W. *Bezpieczeństwo międzynarodowe ery nuklearnej*, PISM, Warszawa, 1991.
27. *Ocena warunków środowiska i przeciwnika*, pod red. M. Wrzosek, Warszawa 2003.
28. *Planowanie, organizowanie i prowadzenie działań rozpoznawczych*, pod red. A. Nowak, Warszawa 2003.

29. Płusa T., Jahnz-Różyk K., *Broń biologiczna. Zagrożenie i przeciwdziałanie*, Medpress, Warszawa 2002.
30. *Pojęcie, istota oraz tendencje zagrożeń asymetrycznych*, pod kier J. Pawłowskiego, Warszawa 2002.
31. *Prawo karne i proces karny wobec nowych form i technik przestępczości*, pod. red. H. J. Hirsch, P. Hofmański, E. W. Pływaczewski, C. Roxin, Białystok 1997.
32. *Przemiany w teorii sztuki wojennej lat dziewięćdziesiątych*, pod. red. B. Szulc Warszawa, 1997.
33. *Rozpoznawcze przygotowanie pola walki*, pod red. M. Wrzosek, Warszawa 2004.
34. Sołoma L., *Metody i techniki badań socjologicznych, wybrane zagadnienia*, Olsztyn, WSP 1995.
35. Stoner J, Wankel Ch., *Kierowanie*, Warszawa, PWE 1996.
36. *Teoria organizacji i zarządzania*, pod. red. Kurnal J. Warszawa, PWE 1979.
37. *Textbook of Military Medicine, część I: Warfare, Weaponry, and the Casualty: Medical Aspects of Chemical and Biological Warfare*, pod. red. Sidell F. R., Takafuji E. T. Franz D. R. Borden Institute, Walter Reed Army Medical Center, Washington 1997.
38. Toffler A., H., *Wojna i antywojna*, Warszawa 1997.
39. Toffler A.*Trzecia fala*, Warszawa 1986.
40. Tyszkiewicz A. *Operacje stabilizacyjne*, Warszawa 2005.
41. *Walka elektroniczna w działaniach taktycznych wojsk lądowych*, pod red. J. Janczaka, Warszawa, AON 1999.
42. Wiatr M., *Między strategią a taktyką*, Toruń 1999.
43. Wójcik J. W. *Przestępstwa w biznesie*, Warszawa 1998.
44. Wrzosek M., *Rozpoznanie w operacjach pokojowych*, Warszawa AON 2006.
45. Yourdon E., *Wojna na bity, wpływ wydarzeń z 11 września na technikę informacyjną*, WNT, Warszawa 2004.
46. *Zagrożenia przestępczością zorganizowaną (mafijną) w Polsce – w kontekście doświadczeń innych policji*, Komenda Główna Policji, Warszawa 1994.
47. *Zarządzanie bezpieczeństwem jako problem nauki i dydaktyki szkoły wyższej*, pod. red. C.Rutkowski, Warszawa 2003.

ARTYKUŁY:

1. Balcerowicz B., *Wojny współczesne. Wojny przyszłe*, Myśl Wojskowa 2003 nr 5.
2. Bąk T., *Doświadczenia z Kosowa*, Przegląd Wojsk Lądowych, 2001 nr 5.
3. Chomiczewski K., *Współczesne poglądy na zagrożenie bronią biologiczną*, Lekarz Wojskowy, 2002 nr 1.
4. Dukaczewski M. *Informacyjne zabezpieczenie operacji „Iracka Wolność"* [w:] *Operacja „Iracka Wolność"*, materiały z konferencji naukowej, AON, Warszawa 2003.
5. *Działania specjalne Bundeswehry*. Wojskowy Przegląd Zagraniczny, 1994 nr 2.
6. Flis J. *Globalne zagrożenia*, Polska Zbrojna 2004 nr 27.
7. Jabłoński L., Karwat I. D. *Bioterroryzm i wojna biologiczna-teoria i praktyka*, Zdrowie Publiczne 2002 nr 1.
8. Kaczmarek J., *Strategia bezpieczeństwa Unii Europejskiej*, Zeszyty Naukowe AON 2004 nr 1 (54).
9. Kozub M., *Charakter zagrożeń oraz konfliktów zbrojnych w pierwszych dekadach XXI wieku*, Myśl Wojskowa 2006 nr 1.

10. Łuczak W. *Pod parasolem Rheinmetalla*, Raport WTO-2005 nr 11.
11. Nowak I. *Broń obezwładniająca o działaniu akustycznym*, Przegląd Wojsk Lądowych 2003 nr 6.
12. Wrzosek M., *Formy oceny przeciwnika*, Przegląd Sił Zbrojnych 2007 nr 1.
13. Wrzosek M., *Prognozowanie działania przeciwnika*, Przegląd Wojsk Lądowych 2006 nr 5.
14. Wrzosek M., *Prognozowanie zagrożeń w nowych uwarunkowaniach międzynarodowych*, Zeszyt Naukowy AON 2006 nr 2.
15. Wrzosek M., *Wybrane Aspekty koordynacji działań powietrzno-lądowego systemu rozpoznania*, Zeszyt Naukowy WSO WLąd 2003, nr 1(127).
16. Rosłan G.,Wrzosek M. *Zagrożenia i ochrona strefy tyłowej*, Przegląd Wojsk Lądowych 2006 nr 9.
17. *Żelowa bateria*, Newsweek z dn. 15.01.2006.

Dokumenty doktrynalne:

1. *A secure Europe in a better World, European Security Strategy*, Brussels 2003.
2. AAP-6(2005) *Słownik terminów i definicji NATO.*
3. *Doktryna Narodowa – Operacje Połączone (OP/01)*, Szkol.800/2002. Warszawa 2002.
4. *Doktryna Prowadzenia Operacji Połączonych* DD/3, Warszawa 2003.
5. *Joint Vision 2010,* Chairman of the Joint Chiefsof Staff, Washington 1997.
6. *Koncepcja Strategiczna Sojuszu Północnoatlantyckiego* 1999
7. *Regulamin Działań Wojsk Lądowych* (DD/3.2), Szkol 809/ 2006, Warszawa 2006.
8. *Regulamin polowy Sił Zbrojnych USA* - PM-31-21A.
9. *Stability operations and support operations (SOSO)*, US Army Training and Doctrine Command TRADOC, Fort Leavenworth 2003.
10. *Strategia bezpieczeństwa narodowego RP*, Warszawa 2003.
11. *Strategic Vision: The Military Challenge*, NATO Strategic Commanders, 2004.

Słowniki i encyklopedie:

1. *Encyklopedia techniki wojskowej*, Warszawa, MON 1978.
2. *Leksykon wiedzy wojskowej*, Wydawnictwo MON, Warszawa 1979.
3. *Mały Słownik Stosunków Międzynarodowych*, pod. red. G. Michałowska, Warszawa 1996.
4. Osmańczyk E., *Encyklopedia ONZ i stosunków międzynarodowych*, Warszawa 1986.
5. *Pattern of Global Terrorism*, Department of State, April 2004.
6. *Słownik języka polskiego* PWN, Warszawa 1992.
7. *Słownik Języka Polskiego*, Tom III, PWN, Warszawa 1981.
8. *Słownik Wyrazów Obcych*, Wydawnictwo Naukowe PWN, Warszawa 1996.
9. Tęgos M., Górecki M., Łokociejewski M., *Słownik podstawowych terminów rozpoznawczych*, Warszawa ASG WP 1988.

Strony internetowe:

1. http: //www.imm.org.pl/Czujniki inteligentne.htm.

2. http://pl.wikipedia.org/wiki/Dywersja
3. www.bbn.gov.pl/pl/nato/szczyt/nsc.html
4. www.bbn.gov.pl/dokument/strategiabezpieczeństwa.html

ZAŁĄCZNIKI

1. Arkusz obserwacji
2. Kwestionariusz ankiety
3. Wyniki przeprowadzonej ankiety
4. Kwestionariusz wywiadu
5. Opracowane wyniki wywiadu
6. Szacunkowa liczba ofiar ataku biologicznego
7. Zagrożenia asymetryczne w rejonie misji pokojowej
8. Zagrożenia asymetryczne w strefie tyłowej
9. Sprawozdanie z obserwacji

Załącznik 1

ARKUSZ OBSERWACJI

Obiekt obserwacji: .....

Rodzaj obserwacji: .....

Data .....

ELEMENTY PODLEGAJĄCE OBSERWACJI:

1. Procedury realizowane przez ćwiczące sztaby i wojska w zakresie oceny zagrożeń asymetrycznych.
2. Sposób i zakres oceny zagrożeń asymetrycznych.
3. Podział obowiązków funkcyjnych w komórkach stanowiska dowodzenia w zakresie realizacji przedsięwzięć planistycznych i wykonawczych w ramach oceny zagrożenia.
4. W jakich etapach procesu planowania działań realizowane jest ocena sytuacji w strefie tyłowej.
5. Rodzaj wykonywanych dokumentów odzwierciedlających zagrożenia asymetryczne:
6. Inne spostrzeżenia.

Załącznik 2

AKADEMIA OBRONY NARODOWEJ
WYDZIAŁ WOJSK LĄDOWYCH

INSTYTUT ZARZĄDZANIA I DOWODZENIA

KWESTIONARIUSZ ANKIETY

Treść kwestionariusza związana jest z wybranymi zagadnieniami dotyczącymi problemu rozpoznania w działaniach asymetrycznych. Celem przeprowadzanej ankiety jest uzyskanie empirycznego materiału faktograficznego dotyczącego poglądów respondentów w zakresie przedmiotu badań.

Ankieta jest anonimowa, wyniki badań będą wykorzystane wyłącznie do celów naukowych i prezentowane w sposób zbiorczy.

Ankieta wykorzystana zostanie jako cenne źródło informacji i wzbogaci wiedzę z zakresu rozpatrywanych zagadnień, a jej wyniki stanowić będą podstawę opracowania wniosków końcowych zawartych w pracy naukowo-badawczej.

Serdecznie dziękuję za współpracę

płk dr Marek Wrzosek

1. Które, Pana zdaniem, z niżej wymienionych zadań rozpoznawczych najczęściej realizowane są w działaniach asymetrycznych?

(proszę wybrać odpowiedź i określić jej rangę, wg wskazanych rozwiązań:
1 – bardzo często, 2 – często, 3 – rzadko, 2- tylko czasami)

- Rozpoznanie rozprzestrzeniania broni masowego rażenia (BMR);
- Rozpoznanie struktur przestępczości zorganizowanej w rejonie kryzysu;
- Rozpoznanie szlaków przemytu broni i narkotyków;
- Rozpoznanie kierunków i składu migrującej ludności.

2. W jakich Pana zdaniem, obszarach tematycznych powinno koncentrować się współdziałanie zespołów rozpoznawczych w ramach identyfikacji zagrożeń asymetrycznych podczas wielonarodowej operacji pokojowej?

.....

.....

.....

3. Jakie, Pana zadaniem, można wskazać uwarunkowania rozpoznania w kontekście zagrożeń asymetrycznych?

.....

.....

.....

.....

4. Jakie zagrożenia, Pana zdaniem, są najczęściej określane jako zagrożenia asymetryczne?

.....

.....

.....

.....

5. Które ze znanych Panu zagrożeń asymetrycznych występują najczęściej podczas operacji poza granicami kraju?

.....

.....

.....

.....

6. Jakie są, zdaniem Pana, sposoby zapewnienia bezpieczeństwa wojskom w działaniach asymetrycznych?

.....

.....

.....

7. Jakie zagrożenia, w Pana ocenie, występują w tyłowej strefie działań i które z nich są najistotniejsze?

(Proszę uszeregować odpowiedzi według znaczenia:
1 - ważne, 2 – istotne, 3- bardzo istotne, 4 – najistotniejsze)

Znaczenie	Rodzaj zagrożenia
1	
2	
3	
4	

8. Które z poniżej wymienionych elementów mogą stanowić obiekt ataku asymetrycznego?

Znaczenie	Rodzaj zagrożenia
	Sieci informatyczne
	Stanowiska dowodzenia
	System łączności radiowej
	System łączności przewodowej

9. Proszę uszeregować według rangi (znaczenia) wskazane poniżej zagrożenia asymetryczne dla systemów informacyjnych:

Znaczenie	Rodzaj zagrożenia
	Wirusy komputerowe
	Monitoring przepływu danych (sniffing)
	Przejęcie danych
	Zakłócenie przekazu

10. Które z wymienionych zagrożeń asymetrycznych stanowią, zdaniem Pana, największe zagrożenie dla systemu bezpieczeństwa światowego?

Proszę uszeregować odpowiedzi według znaczenia:
1 - ważne, 2 – istotne, 3- bardzo istotne, 4 – najistotniejsze)

Znaczenie	Rodzaj zagrożenia
	Proliferacja broni masowego rżenia
	Handel bronią i środkami walki
	Cyberterroryzm
	Zorganizowana przestępczość

METRYCZKA *(proszę zakreślić wybrany numer stosownie do odpowiedzi)*

Stopień wojskowy:

1. Oficer młodszy
2. Oficer starszy

Stanowisko służbowe:

1. Dowódcze
2. Sztabowe
3. Szkolnictwo wojskowe
4. Inne

Specjalność zawodowa:

1. Wojska pancerne lub zmechanizowane
2. Rozpoznanie (ogólnowojskowe i rodzajów wojsk, WE, działania psychologiczne i specjalne)
3. Rodzaje wojsk

Załącznik 3

WYNIKI PRZEPROWADZONEJ ANKIETY

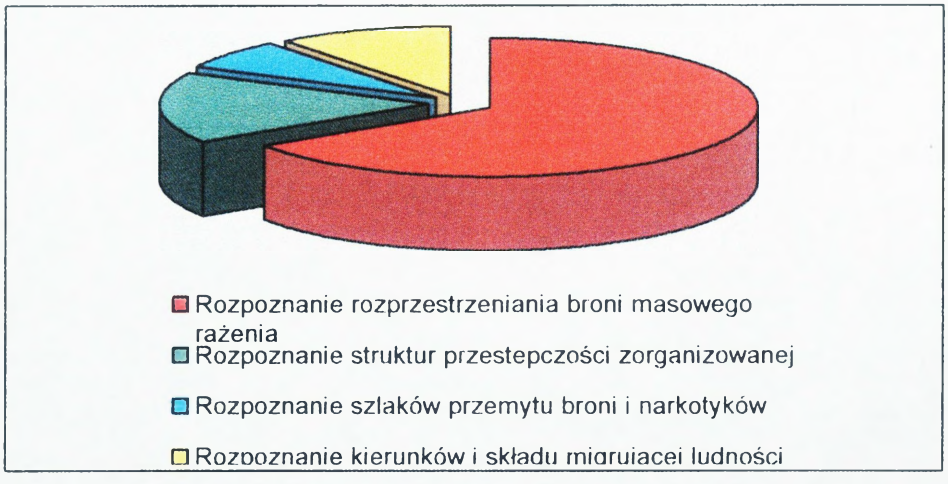
W związku z podjęciem badań w obszarze rozpoznania w działaniach asymetrycznych przygotowano i przeprowadzono ankietowanie.

Celem przeprowadzanej ankiety było uzyskanie empirycznego materiału faktograficznego dotyczącego poglądów respondentów w zakresie przedmiotu badań.

Ankieta stanowiła cenne źródło informacji i wzbogaciła wiedzę z zakresu rozpatrywanych zagadnień, a jej wyniki były podstawą do opracowania wniosków końcowych ujętych w pracy naukowo-badawczej.

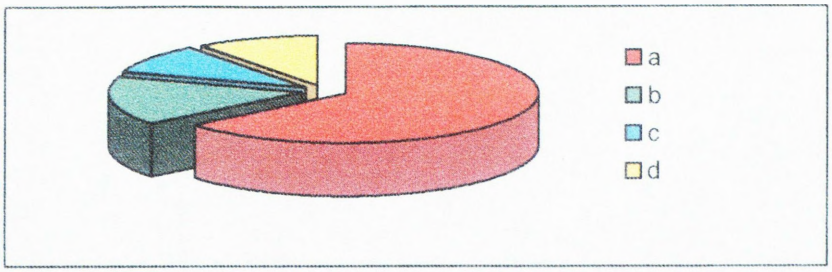
Poniżej zaprezentowano zbiorcze rezultaty uzyskane w toku prowadzonych badań.

1. Które, Pana zdaniem, z niżej wymienionych zadań rozpoznawczych najczęściej realizowane są w działaniach asymetrycznych?



Wykres 1. Zadania rozpoznawcze realizowane w działaniach asymetrycznych

2. W jakich Pana zdaniem, obszarach tematycznych powinno koncentrować się współdziałanie zespołów rozpoznawczych w ramach identyfikacji zagrożeń asymetrycznych podczas wielonarodowej operacji pokojowej?
   a. systematycznym korzystaniu ze zbiorów informacyjnych;
   b. koordynacji działań i wzajemnym uzupełnianiu się poszczególnych podsystemów rozpoznania;
   c. połączeniu odpowiednich sensorów w jeden system zbierania i analizowania danych;
   d. bieżącym opracowywaniu wiadomości i komunikatów rozpoznawczych.

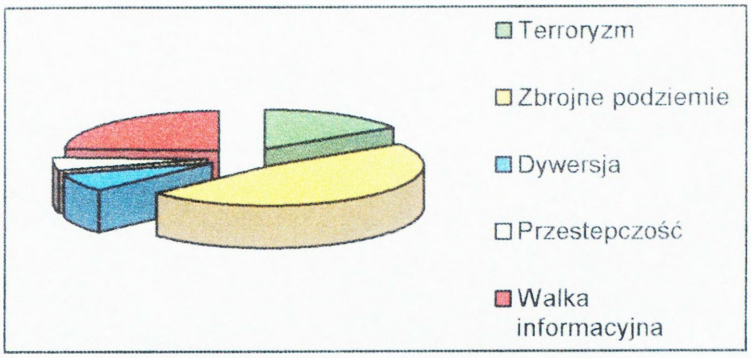


Wykres 2. Obszary tematyczne współdziałania zespołów rozpoznania

3. Jakie, Pana zadaniem, można wskazać uwarunkowania rozpoznania w kontekście zagrożeń asymetrycznych?

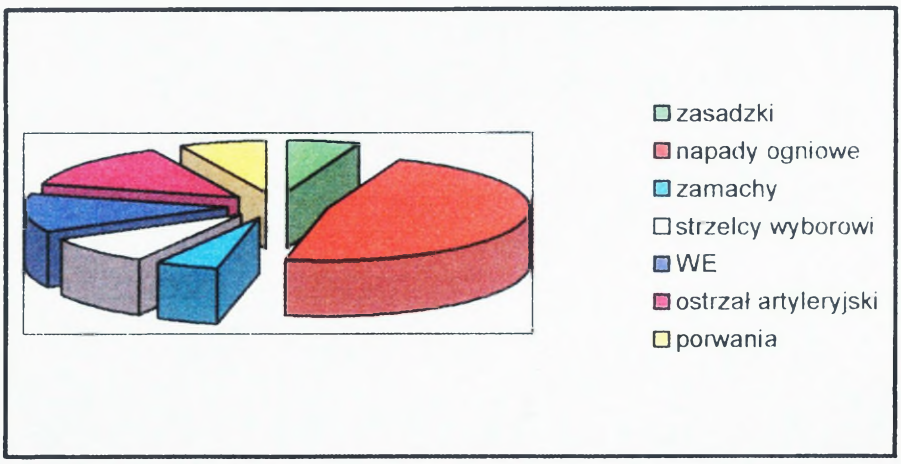
- dynamiczne zmiany w rozmieszczeniu sił aktualnego i potencjalnego przeciwnika,
- stosunek miejscowej ludności oraz państw ościennych do sił interwencyjnych, w tym przypadku należy się liczyć z brakiem akceptacji, a nawet wrogim nastawieniem i przeciwdziałaniem mieszkańców, traktujących - z powodów politycznych, religijnych i kulturowych – wojska biorące udział w operacji jako agresora;
- funkcjonowanie ugrupowań bojowych przeciwnika, które nie zostały rozbite lub zlikwidowane oraz grup zbrojnego podziemia (dywersyjno-sabotażowych), gotowych do ewentualnych działań partyzanckich na terenach zajętych przez siły stabilizacyjne lub pokojowe;
- odmienność warunków klimatycznych, kulturowych oraz religijnych;
- możliwość kierowania w rejon operacji zbrojnej przez organizacje terrorystyczne zamachowców, w celu podjęcia działań wymierzonych w siły interwencyjne na terytorium państwa, na którym jest prowadzona operacja. Nie należy także wykluczać wsparcia udzielanego ugrupowaniom wrogim w stosunku do sił pokojowych lub stabilizacyjnych przez państwa sąsiadujące z krajem objętym działaniami interwencyjnymi;
- działalność przestępczości zorganizowanej związanej głównie z nielegalnym handlem bronią i narkotykami, czemu sprzyja - charakterystyczny dla konfliktów zbrojnych - proces ubożenia społeczeństwa oraz niski poziom sprawności lokalnych sił porządkowych;
- występowanie zjawisk kryminalnych, typowych dla kraju objętego działaniami wojennymi, w tym przede wszystkim wynikających z działalności grup przestępczych, a także - jak wskazują doświadczenia z minionych operacji - grabieży mienia prywatnego i państwowego dokonywanej przez miejscową ludność na terenach zajętych przez siły pokojowe lub stabilizacyjne;
- obecność na zajętym terenie służb specjalnych i lojalnych pracowników wobec dotychczasowych władz kraju, w którym prowadzona jest operacja;

4. Jakie zagrożenia, Pana zdaniem, są najczęściej określane jako asymetryczne?



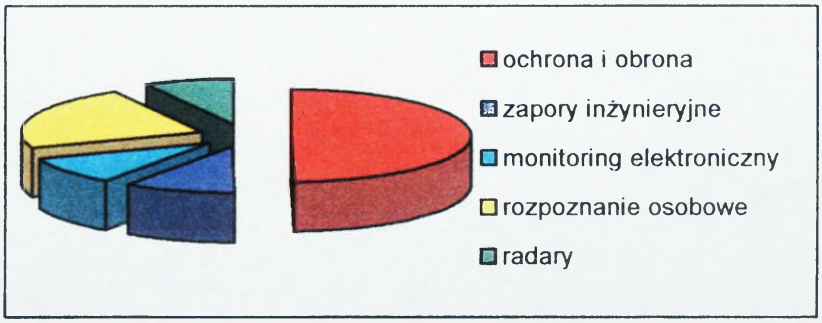
Wykres 3. Identyfikacja zagrożeń asymetrycznych

5. Które ze znanych Panu zagrożeń asymetrycznych występują najczęściej podczas operacji poza granicami kraju?



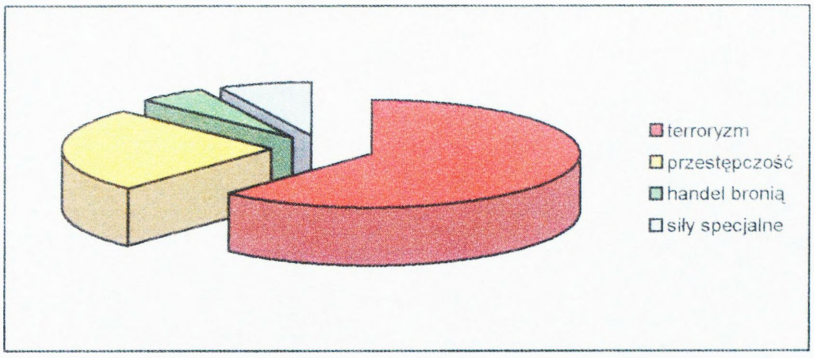
Wykres 4. Zagrożenia asymetryczne występujące poza granicami kraju

6. Jakie są, zdaniem Pana, sposoby zapewnienia bezpieczeństwa wojskom w działaniach asymetrycznych?

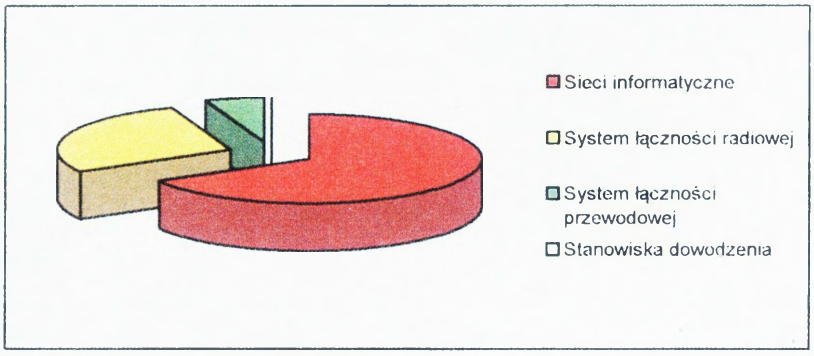


Wykres 5. Sposoby zapewnienia wojskom bezpieczeństwa działaniach asymetrycznych

7. Jakie zagrożenia, w Pana ocenie, występują w tyłowej strefie działań i które z nich są najistotniejsze?

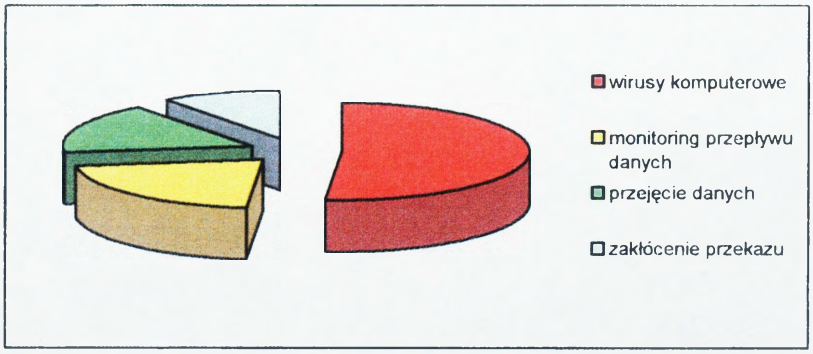


8. Które z poniżej wymienionych elementów mogą stanowić obiekt ataku asymetrycznego?



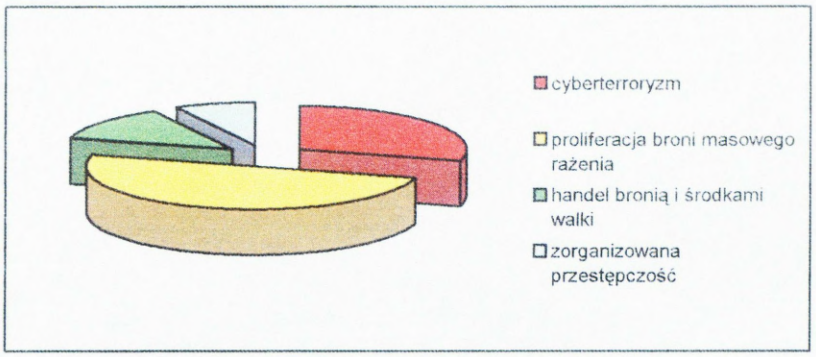
Wykres 6. Obiekty ataku asymetrycznego

9. Proszę uszeregować według rangi (znaczenia) wskazane poniżej zagrożenia asymetryczne dla systemów informacyjnych:



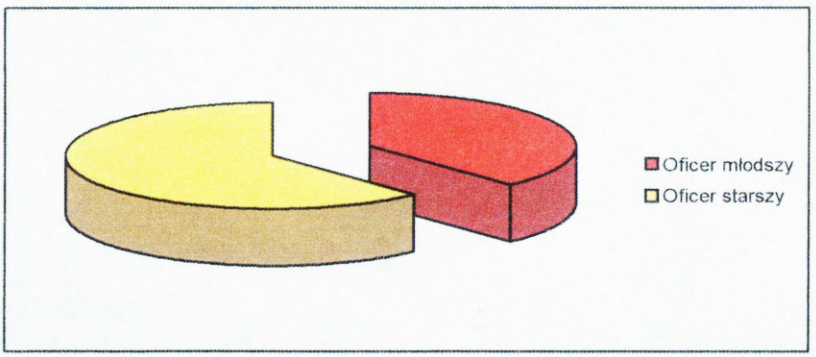
Wykres 7. Zagrożenia asymetryczne dla systemów informacyjnych

10. Które z wymienionych zagrożeń asymetrycznych stanowią, zdaniem Pana, największe zagrożenie dla systemu bezpieczeństwa światowego?

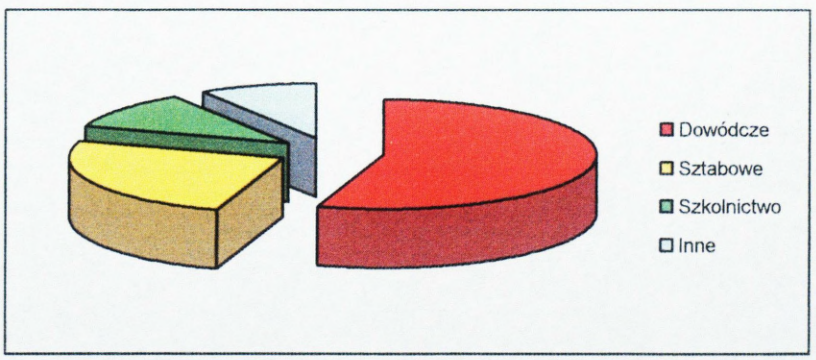


Wykres 8. Zagrożenia asymetryczne dla systemu bezpieczeństwa światowego

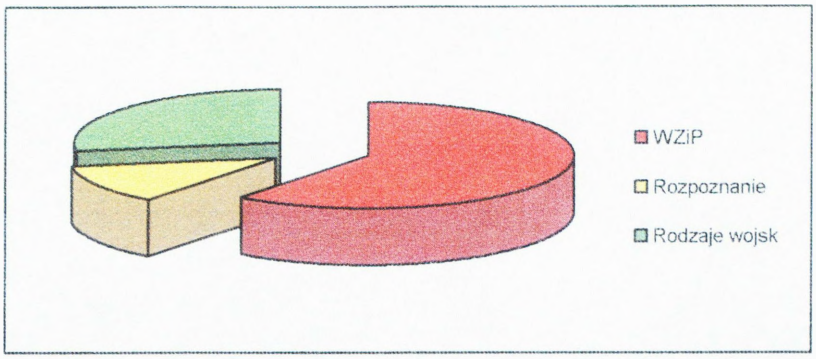
Środowisko respondentów ankiety



Wykres 9. Środowisko respondentów ze względu na stopień wojskowy



Wykres 10. Środowisko respondentów według stanowisk służbowych



Wykres 11. Środowisko respondentów według specjalności wojskowych

Załącznik 4

KWESTIONARIUSZ WYWIADU

W ostatnim czasie, na podstawie szeregu nowych doświadczeń wynikających z przebiegu misji pokojowych, działań militarnych i ćwiczeń dowódczo-sztabowych w publikacjach wojskowych pojawiają się wypowiedzi na temat wzrostu poziomu zagrożenia asymetrycznego w strefie tyłowej. Źródłem zagrożeń mogą być: zbrojne grupy dywersyjne, organizacje terrorystyczne i pododdziały partyzanckie potencjalnego przeciwnika. Wskazana problematyka zdaniem wielu oficerów nie jest zjawiskiem nowym, gdyż już w czasie II wojny światowej strony konfliktu stosowały z powodzeniem różne formy walki.

Zatem w związku z prowadzonymi badaniami w obszarze rozpoznania w działaniach asymetrycznych proszę o przygotowanie odpowiedzi na poniżej wyszczególnione pytania problemowe.

1. Jakie zagrożenia asymetryczne występują w strefie tyłowej?
2. Jakie będą prawdopodobne obiekty działań terorrystycznych?
3. Jakie są sposoby i techniki wykorzystywane przez grupy zbrojnego podziemia?
4. Jakie są sposoby prowadzenia działań dywersyjnych?
5. Czy rozproszone oddziały potencjalnego przeciwnika mogą stanowić zagrożenie dla sił koalicji?
6. Czy formacje aeromobilne stanowią zagrożenie dla tyłowej strefy działania wojsk?
7. Jakie środki walki i sposoby prowadzenia działań są wykorzystywane przez grupy ekstremistów?

Załącznik 5

OPRACOWANE WYNIKI WYWIADU

Obserwując przebieg konfliktów zbrojnych można stwierdzić, że we współczesnych, złożonych operacjach militarnych zagrożenie strefy tyłowej nie tylko nie zmalało, lecz w opinii specjalistów wykazuje dalszą tendencję wzrostu z uwagi na znaczne rozśrodkowanie oddziałów, a więc poszerzenie rejonów odpowiedzialności i zwiększenie głębokości ugrupowania jednostek. Poza tym w wyniku nasycenia wojsk lądowych środkami transportu powietrznego, znacznie wzrosła ruchliwość i manewrowość formacji aeromobilnych. Wnioski z obserwacji ćwiczeń wskazują na wzrastające zagrożenie strefy tyłowej przez jednostki przeciwnika przerzucane na śmigłowcach.

Zgromadzone doświadczenia wskazują, że w strefie tyłowej można oczekiwać działań zróżnicowanych strukturalnie sił potencjalnego przeciwnika a także organizacji przeciwników politycznych.

W ocenie potencjalnego zagrożenia należy zakładać, że strefa tyłowa to dogodny obszar dla działalności agentów obcych wywiadów, którzy jeszcze przed rozpoczęciem działań wojennych znajdą się w rejonie przyszłych walk. Mimo, że walka z nimi jest w zasadzie obowiązkiem służb kontrwywiadowczych, to jednak trzeba wskazać na fakt, że będą one korzystały z pomocy i współpracy wojsk operacyjnych.

Dużym zagrożeniem w strefie tyłowej są rozproszone oddziały wojsk przeciwnika, które w różnej sile pozostały na zapleczu, przeniknęły, włamały się albo zostały desantowane z powietrza lub morza. Sposoby ich działania są odpowiednio określone zasadami użycia poszczególnych formacji. Może się zdarzyć, że pododdziały przeciwnika uzyskają wsparcie lokalnej społeczności i będą stanowiły bazę sił antyrządowych. Ponadto jest sprawą oczywistą, że siły specjalne przeciwnika celem wykonania zadań na terytorium zajmowanym przez wojska lub siły stabilizacyjne będą szeroko stosowały środki i metody walki podziemnej, w tym także techniki terrorystyczne.

Na podstawie zgromadzonych doświadczeń można stwierdzić, że siły przeciwnika mogą występować w ubraniach cywilnych ze znakami rozpoznawczymi. Jak wskazuje praktyka, w wielu misjach pokojowych ekstremiści działają w mundurach jednostek zaangażowanych w misję lub ich sojuszników, uniformach służbowych

urzędów lub lokalnych organizacji rządowych czy sojuszniczych, jak np.: policji, poczty, Czerwonego Krzyża, pracowników ONZ, itp.

W ocenie zagrożenia, nie należy lekceważyć siły przeciwników politycznych wywodzących się z kraju lub przybyłych z innych państw. Szczególnie należy się liczyć z ich działalnością w okresie pokonfliktowym, gdy brak jest autorytetu nowej władzy, zorganizowanych struktur politycznych i lokalnych władz samorządowych. Działanie przybyłych z zagranicy przedstawicieli religijnych lub politycznych będzie ułatwione chociażby z racji posługiwania się tym samym językiem, a sposób zachowania się we wszystkich dziedzinach życia nie będzie się różnił od powszechnie akceptowanego.

Nie należy wykluczać, że każde działanie przeciwnika będzie starannie przygotowane. Zebrane doświadczenia wskazują, że grupa uderzeniowa ekstremistów będzie usiłowała podejść niezauważenie w rejon obiektu ataku lub przeniknąć w jego pobliże stosując różne metody postępowania. Uczestnicy ataku mogą usiłować przeniknąć do obiektu jako osoby zatrudnione w obiekcie zainteresowania (np.; personel pomocniczy) lub mające do niego wolny wstęp (np.; lekarze, dziennikarze). Wykorzystując maskowanie bezpośrednie zamachowcy mogą pokonać system ochrony i stosując napad ogniowy zniszczyć obiekt ataku. Nie należy także wykluczać możliwości bezpośredniego atakowania obiektów położonych w strefie tyłowej z wykorzystaniem środków transportowych wyładowanych materiałami wybuchowymi (Irak, Afganistan, Izrael).

W ramach działań dywersyjnych prowadzonych w strefie tyłowej należy się także liczyć z próbami podłączania się do systemów łączności lub nawet prób niszczenia urządzeń komunikacyjnych. Wykonanie tych zadań ułatwia dywersantom znajomość stosowanych systemów zabezpieczenia urządzeń łączności i informatyki. Dlatego tego rodzaju obiekty muszą być objęte szczególną ochroną i bezpośrednią obroną sił osłonowych. Przy obecnym poziomie technologicznego zaawansowania prawdopodobnie nie będzie również problemu z włączeniem się rebeliantów w sieć dowodzenia wojsk rozmieszczonych w strefie tyłowej, co może umożliwić potencjalnemu przeciwnikowi przekazywanie nieprawdziwych informacji o sytuacji

Reasumując zebrane fakty, można wnioskować, że prawdopodobne działania przeciwnika można podzielić na trzy grupy: dywersja, działania terrorystyczne i działania bojowe. Wszystkim tym elementom będą zawsze towarzyszyły akcje psychologiczne, skierowane na pozyskanie przychylności lokalnej ludności. Szczególnie środki masowego przekazu stanowią doskonały sposób propagowania działalności

antyrządowej. Z charakteru działalności stacji telewizyjnych czy radiowych wynika konieczność informowania społeczeństwa o zaistniałej sytuacji i zdarzeniach. Innym rodzajem działania z wykorzystaniem środków masowego przekazu może być rozpowszechnianie przez przeciwnika dezinformacji, które w konsekwencji mogą często doprowadzić do nieprawidłowych decyzji i oczekiwanego przeciwdziałania.

Z działaniami dywersyjnymi w strefie tyłowej należy się liczyć bezpośrednio przed rozpoczęciem działań militarnych oraz później nieprzerwanie w toku całej operacji. Będą one skierowane głównie przeciw obiektom, których zniszczenie lub uszkodzenie utrudni swobodę operacyjną sił zbrojnych lub obniży potencjał militarny. W odniesieniu do misji pokojowych aktywizacji działań sabotażowych ekstremistów należy się spodziewać już przed przybyciem kontyngentów wojskowych, a następnie jak wskazują doświadczenia, omawiane zjawisko będzie narastać.

Z przeprowadzonych analiz wynika, że w strefie tyłowej możliwe są także działania bojowe. Na obiekty dobrze chronione będą prawdopodobnie prowadzone niespodziewane ataki ogniowe, przy czym mogą być stosowane uderzenia poprzedzające lub pozorne. Należy się liczyć z tym, że wszystkie przedsięwzięcia potencjalnego przeciwnika będą ubezpieczane i kierowane z zewnątrz obiektu. Wojska własne lub siły pokojowe podchodzące do obiektu w ramach przeciwdziałania powstałemu zagrożeniu powinny zwracać szczególną uwagę na możliwość organizacji zasadzki, rozmieszczenie pułapek wybuchowych lub zaminowanych odcinków terenu. Kupno lub wykonanie aparatów radiowych czy też urządzeń zdalnego sterowania nie stanowi obecnie żadnego problemu technicznego. Dlatego wiele min-pułapek może być odpalanych drogą radiową z ukrytych stanowisk obserwacyjnych.

Z rozpoczęciem bezpośrednich wystąpień zbrojnych należy się liczyć z chwilą wzrostu ilości sił przeciwnika w strefie tyłowej. Z reguły czas rozpoczęcia tych działań będzie uzależniony od rozwoju sytuacji polityczno-militarnej w rejonie konfliktu (np.: rozpoczęcie rozmów pokojowych, wybory lokalne, aresztowania lub schwytanie poszukiwanych przywódców politycznych). Wielkość sił potencjalnego przeciwnika w strefie tyłowej zależeć będzie od postawy społeczeństwa i jego zaangażowania ideologicznego. Pamiętać jednak trzeba, że nawet siły o mniejszej liczebności mogą wyrządzić znaczne szkody, czego przykładem jest działalność partyzantów wietnamskich, bojówek islamskich w Iraku czy obrońców Groznego.

W powszechnej opinii specjalistów mała ilość atakujących jest rekompensowana zaskoczeniem. Dokładnie opracowany plan każdej akcji decyduje

o sposobie jej przeprowadzenia. W przypadku działań nieregularnych, na plan przeprowadzenia ataku składa się wiele elementów, do najważniejszych z nich należą: informacje o obiekcie, drogi podejścia i odejścia, przedsięwzięcia maskowania oraz dywersja na pomocniczych kierunkach działania sił głównych. Przeciwnik będzie usiłował wprowadzać w błąd ścigające wojska, sugerując poprzez podjęcie akcji w innych punktach strefy tyłowej zorganizowanych działań. Dlatego do centrum dowodzenia, w chwili ataku sił rebeliantów na zasadniczy obiekt uderzenia, mogą napływać meldunki o licznych podpaleniach, napadach na posterunki policji, koszary i bazy wojskowe rozmieszczone w różnych, czasem odległych rejonach. Wszystko po to, aby jak najwięcej sił odciągnąć od ochrony i obrony atakowanego obiektu.

Do transportu grup bojowych i środków walki, będą prawdopodobnie wykorzystywane różnego rodzaju samochody, w tym zdobyte pojazdy wojskowe, nielegalnie przejęte samochody specjalne firm budowlanych i handlowych, ambulanse pocztowe, sanitarne, a nawet karawany. Ułatwi to przeciwnikowi maskowanie działań i przemieszczanie sił. Dostosowanie tych pojazdów oraz do walki, ich przebudowa np.: zamontowanie lekkiego opancerzenia, może zapewnić rebeliantom ochronę przed odłamkami i ogniem broni strzeleckiej. Z zasady siły przeciwnika działające w strefie tyłowej będą wyposażone w sprzęt i pojazdy, które są, na co dzień wykorzystywane przez miejscową ludność.

Poważne zagrożenie w strefie tyłowej stanowi również możliwość użycia broni biologicznej lub chemicznej, szczególnie w przypadku skażenia wody i środków spożywczych. Im później zostanie ujawnione ich użycie, tym większe będą jego skutki.

Przedsięwzięcia terrorystyczne będą miały na celu zastraszenie społeczeństwa, a przez to zahamowanie działań wojska i policji w strefie tyłowej. W czasie wojny w Zatoce Perskiej odnotowano przypadek kobiety, która machając białą flagą ostrzegła Amerykanów przed niebezpiecznym terenem, później znaleziono ją powieszoną na latarni[1].

Działania terrorystyczne skierowane przeciwko siłom zbrojnym mogą polegać na:

- porywaniu lub eliminacji dowódców niższych szczebli;
- zamachach bombowych dokonywanych w rejonach ześrodkowania wojsk, na trasach przejazdu kolumn i na punktach kontrolnych;

[1] Fakt ten podaje H., M. Królikowski, C. Marcinkowski, *Irak 2003*, Warszawa 2003, s. 55.

- bezwzględnym traktowaniu ujętych żołnierzy;
- zakażeniach i zarażeniach stanu osobowego (zatruta żywność, alkohol).

Świadomość, że w rękach przeciwnika znajdują się żołnierze własnych wojsk, którzy spełniają rolę zakładników i mogą stracić życie, będzie miała poważny wpływ zarówno na podejmowanie decyzji czy rozkazy, jak też na działanie własnych żołnierzy. Odnosi się to również do ludności cywilnej, która niekiedy może być zmuszona nawet do działań przeciwko siłom zbrojnym własnego kraju. Samo tylko przeświadczenie o możliwości działań terrorystycznych może zdecydowanie osłabić morale sił ochrony.

Na podstawie wniosków z przebiegu działań militarnych w końcu minionego i początku obecnego wieku można stwierdzić, że grupy ekstremistyczne, a tym także zbrojne grupy miejscowej ludności współdziałające z przeciwnikiem, będą bazowały i powstawały raczej w miastach. Struktura środowiska społecznego w dużych miastach, gdzie mieszkańcy żyją w zasadzie niedostrzegani przez sąsiadów, stwarza dogodne warunki do rozproszenia się, ukrycia i koncentracji przed wykonaniem akcji bojowej. Możliwości wynajmu mieszkań lub stojących na uboczu domków jednorodzinnych pozwalają na skryte zamieszkanie przez osoby poszukiwane przez policję, a nawet przez międzynarodowe organizacje bezpieczeństwa. W tych warunkach jest stosunkowo łatwo przygotować każdą nawet najtrudniejszą operację.

W tej sytuacji należy, więc przypuszczać, że większość aktów sabotażowych, dywersyjnych, a nawet dużych akcji zbrojnych, będzie przeprowadzana w miastach. Priorytetowymi obiektami ataków będą prawdopodobnie lotniska, dworce kolejowe, porty morskie lub rzeczne, mosty, łącza komunikacyjne oraz inne urządzenia i obiekty infrastruktury, których zniszczenie lub czasowe opanowanie będzie miało szczególne znaczenie dla przebiegu działań.

Powyższe fakty nie powinny skłaniać do wniosku, że działania partyzanckie będą prowadzone tylko w miejscowościach. Przykładem wykorzystania terenu do działań nieregularnych są obszary górskie i leśne gdzie istnieją doskonałe warunki maskowania i ukrycia. Ponadto lokalne społeczeństwo w przeciwieństwie do osiedli miejskich, zna się nawzajem i rozpoznaje obcych, którzy pojawiają się w rejonie. Dodatkową przeszkodą utrudniającą pozyskanie informacji o działalności jednostek partyzanckich jest surowa etyka życiowa obywateli zakładająca lojalność i bezinteresowność w pomocy potrzebującym oraz izolację obcych od wewnętrznych spraw lokalnej społeczności.

W ocenie potencjalnego przeciwnika należy zakładać, że wszelkie działania w strefie tyłowej będą prowadzone skrycie w celu uniknięcia walki tam, gdzie sytuacja będzie dla atakujących niekorzystna. Działania będą przeprowadzane głównie w nocy, w złych warunkach atmosferycznych, w rejonach gdzie ogólnie panujący ruch będzie decydował o niezauważalnym podejściu sił uderzeniowych. Jak wskazują doświadczenia, ugrupowanie bojowe napastników mogą stanowić małe, niezależne grupy, a ich koncentracja nastąpi tuż przed obiektem ataku lub bezpośrednim uderzeniem. Wyniki zgromadzonych wniosków z przebiegu ataków zbrojnych wskazują, że zaskoczenie, silne uderzenie ogniowe, szybkie odejście i skryte rozproszenie atakujących sił to zasady, które mają przeciwnikowi gwarantować efekt działania. Uderzenia będą prawdopodobnie skierowane na obiekty, których ochrona może być w krótkim czasie zlikwidowana lub, której działalność będzie czasowo ograniczona, co umożliwi zniszczenie chronionego obiektu. Ponadto w miarę możliwości atakujące grupy zbrojne będą zabierały lub niszczyły broń, amunicję (magazyny), wyposażenie i zaopatrzenie (np.: przez podpalenie, wysadzenie). Celem napadów może też być ujęcie jako zakładników ważnych osobistości (dowódców, urzędników organizacji międzynarodowych, przedstawicieli lokalnych władz, dziennikarzy, itp.). Ponadto jeńcy i zakładnicy mogą być wykorzystywani jako „żywa tarcza" podczas odwrotu po wykonaniu zadania.

Nie należy także wykluczać innych sposobów działania zorganizowanych formacji zbrojnych w strefie tyłowej. Doświadczenia wskazują, że wojskowe i cywilne kolumny marszowe i transportowe mogą być kierowane w rejony wcześniej przygotowanych zasadzek, organizowanych w terenie zakrytym, a także na ulicach miast, które utrudniają manewr i zorganizowane podjęcie walki wojskom regularnym. Uogólnienie wniosków z przebiegu ataków przeprowadzonych na konwoje prowadzi do tezy, że napastnicy otwierali ogień dopiero po przejściu ubezpieczeń marszowych, atakując kolumny sił głównych.

Nie należy także wykluczać, że w strefie tyłowej przeciwnik będzie dążył do dezorganizacji przegrupowania wojsk poprzez blokowanie dróg, zmianę znaków drogowych, wystawianie mylących kierunkowskazów itp. Zahamowanie ruchu kolumn może spowodować trudności w przegrupowaniu wojsk, co przy jednoczesnym przemieszczaniu cywilnych pojazdów uchodźców będzie potęgować zjawisko chaosu organizacyjnego. Fakt ten może być wykorzystany w środkach masowego przekazu jako

element działań psychologicznych deprecjonujący skuteczność działania zarówno wojsk jak i lokalnej władzy.

Uzbrojenie sił przeciwnika w strefie tyłowej w początkowym okresie działań zbrojnych będzie w zasadzie ograniczać się głównie ze względów maskujących, do broni strzeleckiej, w tym także karabinów maszynowych, granatów ręcznych i materiału wybuchowego. Jeżeli jednak działania militarne będą się przedłużać, należy się liczyć z użyciem moździerzy, granatników przeciwpancernych, przenośnych wyrzutni rakietowych, a nawet dział bezodrzutowych. W każdym jednak przypadku należy brać pod uwagę możliwość wykorzystania materiałów wybuchowych oraz innych środków walki, które mogą być skradzione, zdobyte lub wyprodukowane we własnym zakresie, np.:

- miotacze ognia wykonane z gaśnic lub opryskiwaczy ogrodowych;
- materiały wybuchowe z ładunkiem kumulacyjnym w różnych pojemnikach;
- miotacze ładunków wybuchowych wykonane z broni myśliwskiej lub konstrukcji rurowych;
- miny przeciwpiechotne.

W toku działań militarnych należy się liczyć z zaopatrywaniem organizacji zbrojnych dostarczonym z zewnątrz. Będzie to w szczególności broń i amunicja oraz ważniejsze środki walki nieregularnej – przeciwpancerne pociski kierowane, wyrzutnie rakiet przeciwlotniczych, miny. Nie należy wykluczać także możliwości uzyskiwania zaopatrzenia ze składów amunicji i magazynów wojsk stacjonujących w strefie tyłowej. Środki walki mogą być przedmiotem handlu lub wymiany towarowej pomiędzy miejscową ludnością i żołnierzami. Będzie to dodatkowe źródło zaopatrzenia sił rebeliantów, tym bardziej realne, im gorsze będzie zaopatrzenie w strefie tyłów w materiały i produkty pierwszej potrzeby.

Załącznik 6

SZACUNKOWA LICZBA OFIAR ATAKU BIOLOGICZNEGO

Tabela 1.

Szacunkowa liczba ofiar ataku biologicznego[1]

Czynnik chorobotwórczy	Zasięg z wiatrem (km)	Spodziewana liczba ofiar śmiertelnych	Spodziewana liczba zachorowań
gorączka Rift Valley	1	400	35 000
kleszczopochodne zapalenie	5	9 500	35 000
tyfus	10	19 000	85 000
bruceloza	>20	500	125 000
gorączka Q	>20	150	125 000
tularemia	>20	30 000	125 000
wąglik		95 000	125 000

* po rozpyleniu w powietrzu 50 kg czynnika wzdłuż 2 km linii od strony nawietrznej miasta liczącego 500 tys. mieszkańców

Tabela 2

Drobnoustroje chorobotwórcze jako potencjalne biologiczne środki masowego rażenia kategorii A i B w CDC

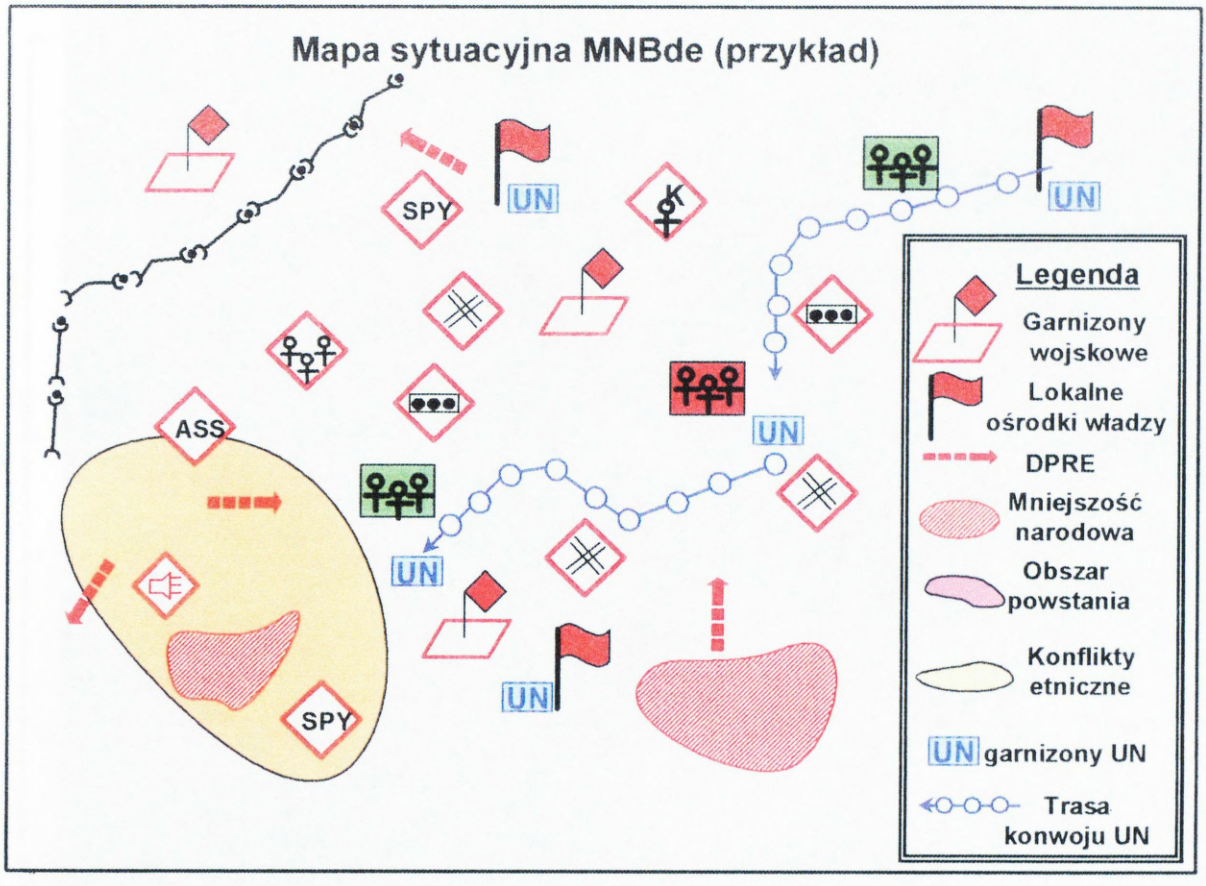
Drobnoustrój	Wywoływana choroba	Czas wylęgania (dni)	Śmiertelność
Bakterie Bacillus anthracis	wąglik	1-3	postać płucna i jelitowa ok. 100 proc.
Clostridium botulinum	botulizm	0,5-2	100 proc.
Frantisella tularensis	tularemia	2–7 (do 21)	umiarkowana
Yersinia pestis	dżuma	1-10	postać płucna do 100 proc.
Brucella abortus	choroba Banga	7-20	umiarkowana
Brucella melitiensis	gorączka maltańska	5-21	ok. 20 proc.
Burkholderia mallei	nosacizna	2-5	60-90 proc.

[1] Źródło: T. Płusa, *Zagrożenie bioterroryzmem*, (w:) Praktyka medyczna, s. 10-11 za H.C. Holloway, A.E. Norwood, C.S. Fullerton, et al. The treat of biological weapons. Prophy-laxis and mitigation of psychological and social consequences. JAMA 1997, 278/5, s. 425-7.

Burkholderia pseudomallei	melioidioza	2-6	90 proc.
Wirusy	gorączka Lassa	7-21	30–50 proc.
Arenaviridae Junin, Sabial, Machupo	południowo-amerykańskie gorączki krwotoczne	7-14	ok. 30 proc.
Arboviridae	gorączka krwotoczna doliny Rift	4-6	30 proc. (ślepota)
Bunyaviridae Hantaan	gorączka krwotoczna z zespołem płucnym	7-14-21	30 proc.
Filoviridae	gorączka krwotoczna Ebola	3-7	50–90 proc.
	gorączka krwotoczna Marburg		30 proc.
Ortopoxviridae Poxvirus	ospa prawdziwa	5-7	20–40 proc.
Equine MorbillMrus	gorączka krwotoczna z zapaleniem mózgu	3-4	100 proc.
Riketsje Coxiella burnetti	gorączka Q	14-21	umiarkowana
Rickettsia rickettsii	gorączka plamista Gór Skalistych	3-10	20 proc.
Rickettsia provazeki	dur plamisty	8-15.	do 30 proc
Grzyby Coccidioides imitis	kokcydiomykoza	7-28	duża przy obniżonej odporności
Wirusy Togaviridae Alphavirus	Zachodnie końskie zapalenie mózgu i rdzenia	5-10	30 proc.

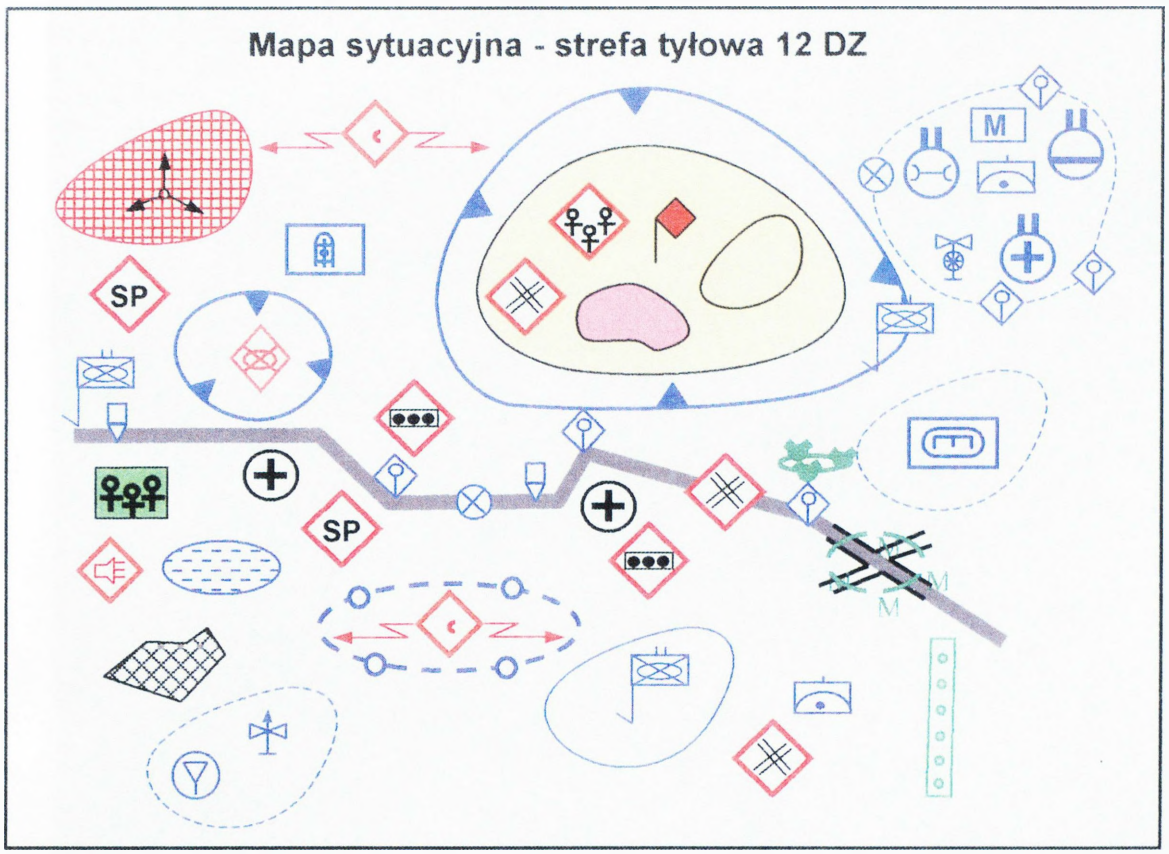
Załącznik 7

ZAGROŻENIA ASYMETRYCZNE W REJONIE MISJI POKOJOWEJ



Załącznik 8

ZAGROŻENIA ASYMETRYCZNE W STREFIE TYŁOWEJ



Załącznik 9

SPRAWOZDANIE Z OBSERWACJI

1. TEMAT: Rozpoznanie w działaniach asymetrycznych.
2. TECHNIKA OBSERWACJI: Obserwacja zewnętrzna.
3. CEL BADAŃ:
   a) określić zakres zadań rozpoznawczych w działaniach asymetrycznych,
   b) ustalić sposób oceny zagrożeń asymetrycznych w tyłowej strefie działania wojsk,
   c) poznać zasadnicze uwarunkowania organizacji systemu rozpoznania w działaniach asymetrycznych.
4. CZAS BADAŃ: 2004-2006
5. OPIS PRZEBIEGU BADAŃ:

Badanie przeprowadzono metodą obserwacji standaryzowanej zewnętrznej w czasie ćwiczeń dowódczo-sztabowych, grupowych oraz treningów prowadzonych w wojskach operacyjnych (szczególnie *GRANICA-04, CAPABLE WARRIOR-04, COMACT EAGLE-05, ANAKONDA-06, ORZEŁ-06*), a także w ramach procesu kształcenia w AON. Ponadto źródłem wiedzy byli studenci (oficerowie rozpoznania) uczestniczący w ćwiczeniach, którzy mieli możliwość sprawdzenia teorii w praktycznej pracy w strukturach komórek rozpoznawczych wojsk operacyjnych i na tej podstawie przekazania wielu dodatkowych spostrzeżeń.

Badaniami objęto działanie sztabowej komórki rozpoznawczej w okresie planowania i kierowania działaniami. Badania prowadzono, wykorzystując możliwość stałego kontaktu z ćwiczącymi na stanowiskach funkcyjnych – oficerami rozpoznania, a także korzystając z uwag wymienianych między uczestnikami ćwiczenia po kolejnych jego etapach. Bardzo cenne okazały się ogólne wnioski zgłaszane w czasie odpraw koordynacyjnych kierownictwa ćwiczenia.

Obserwacja standaryzowana była bardzo przydatna, bowiem umożliwiła uzyskanie odpowiedzi dotyczącej aktualnego stanu rzeczy (jak jest?) – obserwacji faktów. Stąd wynikał szeroki zakres pola badawczego, który obejmował problematykę zagrożeń asymetrycznych w procesie oceny sytuacji organizacji rozpoznania.

6. WYNIKI OBSRWACJI:

W oparciu o wyniki prowadzonej obserwacji sformułowano w odniesieniu do przedmiotu badań następujące ogólne wyniki obserwacji stanowiące podstawę do opracowania wniosków końcowych i weryfikacji przyjętych założeń.

W toku ćwiczeń zaobserwowano, że każdego dnia w ramach odprawy informacyjnej dowódcy prezentowane były zmiany w położeniu przeciwnika oraz jego oddziaływanie w tyłowej strefie, ze szczególnym uwzględnieniem ataków grup zbrojnego podziemia i aktów terrorystycznych.

W toku obserwacji stwierdzono, że o ile szczeble taktyczne posiadają większą swobodę działania o tyle na szczeblu korpusu zintegrowany zespół rozpoznania korpusu był zależny od rozmieszczenia i manewru zasadniczego stanowiska dowodzenia. Sytuacja tak powodowała, że zasoby informacyjne wykorzystywane do procesu oceny zagrożenia przesyłane były z tyłowego stanowiska dowodzenia do zespołu analiz i ocen rozpoznawczych na zasadniczym stanowisku dowodzenia. W procesie planistycznym wykorzystywano zasoby informacyjne obejmujące zarówno położenie poszczególnych podsystemów rozpoznania jak i aktualną wiedzę o przeciwniku. Na podstawie wyników rozpoznania ćwiczący dowódca określał zasadnicze potrzeby informacyjne na kolejny etap operacji. Sprecyzowane przez szefa zespołu rozpoznania priorytetowe potrzeby rozpoznawcze stanowiły podstawę dla zespołu planowania do określenia zadań dla jednostek rozpoznawczych.

Sposób oceny w zakresie zagrożeń asymetrycznych nie odbiegał od obowiązujących standardów i był ściśle realizowany w ramach oceny sytuacji zarówno w zespole rozpoznania na głównym stanowisku dowodzenia, jak i w ramach tyłowego stanowiska dowodzenia. Odmienny zaś był zakres oceny. Bowiem w strefie tyłowej skala zagrożeń asymetrycznych była zdecydowanie większa od strefy działań bezpośrednich. Stąd większość zadań z zakresu rozpoznania zagrożeń asymetrycznych realizowana była przez jednostki pozostające w odwodzie. Wyjątek stanowiły ćwiczenia, gdzie wojska realizowały zadania związane z ochroną strefy tyłowej (*Granica -05*). Stwierdzono, że brak jest umiejętności precyzowania zadań rozpoznawczych w działaniach asymetrycznych. Dla wojsk operacyjnych jest to temat nowy, wymagający opracowanie teoretycznego i weryfikacji założeń w toku ćwiczeń. Zgromadzone doświadczenia z misji pokojowych i operacji stabilizacyjnych w zakresie oceny zagrożeń asymetrycznych oficerowie rozpoznania wykorzystywali jako stałe procedury działania.

W czasie obserwowanych ćwiczeń, w większości przypadków, ćwiczący przystąpili do realizacji zadań służbowych bez należycie opracowanych standardowych procedur operacyjnych. Jak wykazały wyniki obserwacji, brak tego rodzaju dokumentu (SOP) skutkuje ogólnym chaosem organizacyjnym i niewłaściwą realizacją zadań na poszczególnych stanowiskach. W zespole rozpoznania nie dokonywano podziału obowiązków w zakresie organizacji rozpoznania w strefie tyłowej i działań bezpośrednich. Nie można przy obecnej

strukturze organizacyjnej wyodrębnić specjalistycznych stanowisk do realizacji zadań w zakresie zagrożeń asymetrycznych. Sytuacja taka powoduje, że oficerowie rozpoznania nie są w stanie selektywnie oceniać szczególnego rodzaju zagrożenia związanego z działaniami asymetrycznymi potencjalnego przeciwnika.

W zakresie dokumentów dotyczących oceny zagrożeń asymetrycznych, a szczególnie zagrożenia w strefie tyłowej stwierdzono, że w większości przypadków oficerowie rozpoznania wykorzystują w tym celu mapę sytuacyjną. Naniesione na mapę poszczególne zdarzenia stanowią podstawę do podejmowania stosownych działań i organizacji systemu rozpoznania. Inaczej sprawa ta wygląda w korpusie (*ćwiczenie Capable Warrior -04*) gdzie rozdzielone są strefy rozpoznania. Tyłowa strefa stanowi obszar zainteresowania zespołów rozpoznania osobowego i patroli rozpoznawczych. Przeprowadzone w ramach ćwiczenia *Orzeł-06* sprawdzenie zdolności pułku rozpoznawczego do realizacji zadań w strefie tyłowej w pełni potwierdziło założenia teoretyczne, co do sposobu użycia formacji rozpoznania osobowego. Wiele wątpliwości natomiast powstało odnośnie sposobu oceny działania grup specjalnych przeciwnika, zbrojnego podziemia i organizacji terrorystycznych, w tym zakresie konieczne są dalsze treningi sztabowe i ćwiczenia grupowe.

W obserwowanych ćwiczeniach ocena sytuacji militarnej w okresie kryzysu uwzględniała zasadnicze zagrożenia militarne. Brak było natomiast szerszego spojrzenia na problematykę eskalacji kryzysu. Tymczasem w okresie poprzedzającym konflikt zbrojny należy się liczyć z operacjami informacyjnymi potencjalnego przeciwnika, wzrostem aktywności działań asymetrycznych na zapleczu (działalność terrorystyczna, dywersja, sabotaż), aktywizacją grup niezadowolenia społecznego. Nie należy także zapominać o działaniach psychologicznych czy wykorzystaniu sił specjalnych w okresie kryzysu.

Należy uwzględnić fakt, że ocena ogólna, a więc odnosząca się tylko do nacierających sił przeciwnika, nie stanowi podstawy do określenia zagrożenia w obszarze tyłowym. Dopiero połączenie wszystkich trzech stref walki potencjalnego przeciwnika (działania głębokie, bezpośrednie i tyłowe) w całość umożliwia otrzymanie jednolitej sytuacji operacyjno-taktycznej. W tym aspekcie należy wskazać na brak powiązania taktycznej oceny przeciwnika z sytuacją operacyjną, brak umiejętności dostrzegania związku pomiędzy głównym i pomocniczym kierunkiem działania przeciwnika oraz pomiędzy strefami walki na poszczególnych kierunkach operacyjnych, a w konsekwencji realizmem zagrożeń asymetrycznych w toku działań.

Dla przykładu w poszczególnych etapach operacji zaczepnej przeciwnika należy w odniesieniu do położenia wojsk własnych określić stopień realności zagrożenia (np.:

desantowanie sił morskiego zgrupowania uderzeniowego, zrzut sprzętu i wyposażenia dla grup zbrojnego podziemia na obszar zajętym przez wojska własne, dywersja, ataki terrorystyczne na stanowisko dowodzenia?).

Nie budzi wątpliwości teza, że właściwa analiza rozmieszczenia sił przeciwnika na kierunku działania musi być prowadzona z wykorzystaniem wzorca doktrynalnego. O ile sztaby wojsk z zasady w styczności koncentrują swój wysiłek na określeniu położenia pierwszego rzutu i odwodu przeciwnika, to w jednostkach odwodowych (drugi rzut) zapomniano o wzorcach doktrynalnych działania dla grup dywersyjno-rozpoznawczych, specjalnych, oddziałów zbrojnego podziemia czy wreszcie o siłach desantowych czy aktach terroru. Tymczasem to właśnie w oparciu o wzorce doktrynalne określane są potencjalne cele i obiekty oddziaływania przeciwnika, rejony wysadzenia desantów i zadania dla oddziałów wydzielonych, grup desantowo-szturmowych, itd. Dlatego wydaje się za celowe, aby w przyszłości zespół autorski ćwiczenia przygotowywał obok wzorców doktrynalnych dla jednostek zgrupowania uderzeniowego także wzorce doktrynalne działania wybranych sił potencjalnego przeciwnika w tyłowej strefie korpusu.

Najwięcej trudności sprawiło ćwiczącym określenie możliwości wykorzystania formacji specjalnych. Jednostki specjalne potencjalnego przeciwnika są strategicznym narzędziem pozyskiwania danych rozpoznawczych. Ich zadania koncentrują się na obiektach położonych w tyłowej strefie działań. Zadania są realizowane na głębokości ponad 70-100 km od linii styczności wojsk, w związku z tym obiektami rozpoznania mogą być np.: elementy ugrupowania operacyjnego pozostające w rejonach wyjściowych, obiekty infrastruktury, grupy niezadowolenia społecznego. Na podstawie przyjętych w ćwiczeniach rozwiązań zespół autorski stwierdził, że ćwiczący nie mają pełnej wiedzy z tego obszaru tematycznego.

Powierzchowna także była ocena zagrożenia powietrznego. Tymczasem strefa tyłowa to przede wszystkim środki napadu powietrznego, uderzenia rakietowe na obiekty infrastruktury i zakłady przemysłowe, system komunikacji, stanowiska kierowania. Niestety ćwiczące sztaby nie zdobyły się nawet na wskazanie ilości sił i środków, jakimi dysponuje przeciwnik. Wnioski w zakresie oceny działania przeciwnika powietrznego powinny wynikać z etapów, w których mogą być wykorzystane siły powietrzne i lotnictwo wojsk lądowych, tak aby na tej podstawie możliwe było wskazanie potencjalnych obiektów uderzeń środków napadu powietrznego.

Obok szeregu sprawdzonych i dobrze działających rozwiązań zaobserwowano także zakłócenia w systemie komunikacji wewnętrznej zespołu rozpoznania. Podłączenie wszystkich użytkowników do sieci sprawiało, że poprzez pocztę elektroniczną każdy

użytkownik otrzymywał każdą informację wprowadzona do systemu. Tymczasem jak wykazała praktyka działania system, który sprawdza się w czasie pokoju na stanowisku dowodzenia nie jest przydatny w operacji (nawet w czasie ćwiczeń). Do użytkowników trafiało bardzo wiele informacji nieprzydatnych, co wprowadzało szum informacyjny i wydłużało czas na opracowanie i przetworzenie informacji. Każdą wiadomość otrzymaną za pomocą poczty elektronicznej, użytkownik musiał otworzyć, aby zapoznać się z jej treścią i ocenić wartość informacyjną. Sytuacja tak komplikowała proces przetwarzania informacji i niepotrzebnie angażowała do zbędnej pracy oficerów rozpoznania. Ogólny wniosek wynikający z tego faktu sprowadza się do stwierdzenia, że konieczna jest wstępna weryfikacja treści informacyjnej oraz kierunkowe przesyłanie informacji szczególnie ważnych (kluczowych w danej sytuacji). Stąd konieczność kierowania strumienia informacji do odbiorców według ustalonych zasad. Niebagatelną rolę odgrywa w tej sytuacji sprawa zrozumienia i poznania potrzeb użytkowników w zakresie wiedzy o zagrożeniach asymetrycznych. Określenie zarówno priorytetów otrzymywania informacji jak i treści informacyjnej stanowić powinno zasadnicze kryterium udostępnienia informacji. Jak zatem wynika z przytoczonych faktów możliwość powiadomienia wszystkich o wszystkim nie jest złotym środkiem do uzyskania przewagi informacyjnej. Brak kierowania strumieniem zasobów informacyjnych niejednokrotnie powodował, bowiem zakłócenia w pracy zespołu rozpoznania.

Należy podkreślić fakt, że w zasobach informacyjnych ćwiczących obok regularnych jednostek przeciwnika znajdowały się zbiory obejmujące zagrożenia asymetryczne. Szczególne miejsce zajmowały informacje dotyczące terroryzmu, rebelii zbuntowanych dowódców, działań partyzanckich, powstań zbrojnych, przemytu, przestępczości zorganizowanej oraz handlu narkotykami. Selekcja informacji prowadzona przez poszczególnych użytkowników umożliwiała ocenę i analizę pozyskiwanych treści informacyjnych oraz ich dystrybucję w pionach funkcjonalnych. Zasoby informacyjne dotyczące bezpieczeństwa wojsk obejmowały także kwestie sabotażu, dywersji, terroryzmu i mniejszości narodowych. Cała wiedza w formie komunikatu stanowiła podstawę do opracowania prognozy zagrożenia dla elementów ugrupowania operacyjnego lub bojowego rozmieszczonych w obszarze tyłowym.

Specyficzne zasoby informacyjne obejmowały treści dotyczące struktury społecznej ludności na obszarze objętym działaniami i w bezpośrednim sąsiedztwie. W praktycznej działalności rozpoznawczej można było zaobserwować, że istniało wiele obszarów wspólnych dla szeregu podmiotów informacyjnych. Migracja ludności stanowiła przedmiot

zainteresowania zarówno oficerów G-2 jak i zespołu kontaktów cywilno-wojskowych (CIMIC), logistyki a nawet biura prasowego dowódcy korpusu. Stąd konieczna była wymiana poszczególnych zbiorów informacyjnych w trybie cyklicznym oraz doraźnie w sytuacjach wymagających koordynacji. Zbudowana baza danych gromadziła zasoby informacyjne wykorzystywane na potrzeby organizacji obozów dla uchodźców, zapewnienia zorganizowanego powrotu ludności do miejsc zamieszkania, poszukiwania przestępców kryminalnych i zbrodniarzy wojennych. Ważną kwestią była ocena stopnia zorganizowania poszczególnych grup etnicznych oraz możliwości odbudowy lokalnej władzy państwowej. Przeprowadzane analizy umożliwiły określenie charakteru i potencjalnych rejonów zagrożeń związanych z działalnością organizacji zbrojnego podziemia, grup niezadowolenia społecznego oraz przestępczości zorganizowanej.

Nową kategorią zagrożeń asymetrycznych dla ćwiczących wojsk okazał się terroryzm. Zasoby informacyjne umożliwiały zbudowanie i odtworzenie poznanych w toku ćwiczenia struktur organizacji terrorystycznych oraz ustalenie ośrodków kierowania. Niestety, ponieważ problematyka tego typu jest nowa dla sił zbrojnych w poszczególnych zbiorach informacyjnych występowały luki. Ćwiczenia wykazują, że konieczna jest szersza współpraca z lokalną policją i służbami bezpieczeństwa kraju gospodarza. Okazało się także, że wystąpiły problemy z generowaniem potrzeb informacyjnych. Zapotrzebowanie na informacje kierowane do przełożonych pozostawały bez odpowiedzi. Na podstawie praktycznej działalności rozpoznawczej (Irak, Afganistan) można stwierdzić, że wielką rolę w uzupełnianiu zasobów informacyjnych obejmujących zagrożenia asymetryczne spełniają jednostki rozpoznania osobowego (HUMINT). Niestety w trakcie ćwiczeń nie przewidziano elementów podgrywki, co było powodem braku stosownych informacji.

Obserwacja ćwiczeń dowódczo-sztabowych przyniosła wymierne korzyści polegające na pogłębieniu wiedzy i pozyskaniu doświadczeń w zakresie rozwiązywania problemów dotyczących rozpoznania w działaniach asymetrycznych. Niestety część zgromadzonej wiedzy ma charakter informacji niejawnych i nie może być zaprezentowana w rezultatach badawczych.

Zebrane wnioski wskazują, że w procesie kształcenia oficerów rozpoznania w AON wskazane byłoby zwiększenie zakresu specjalistycznego przygotowania do realizacji zadań w działaniach asymetrycznych.

Należy przypuszczać, że wprowadzenie do problematyki kształcenia studentów rozpoznania zajęć obejmujących zagadnienia oceny i prognozowania zagrożenia w tyłowym obszarze działania korpusu (dywizji) umożliwi pełniejsze wykorzystanie zasobów

informacyjnych rozpoznania oraz pomoże w generowaniu potrzeb informacyjnych. Konieczne w tej sytuacji celowe wydaje się także opracowanie stosownych wariantów dokumentów rozpoznawczych uwzględniających problematykę zagrożeń asymetrycznych.