AKADEMIA
OBRONY
NARODOWEJ

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

UWARUNKOWANIA ZAGROŻENIA BEZPIECZEŃSTWA FIZYCZNEGO I ELEKTRONICZNEGO WOJSK W OPERACJACH WIELONARODOWYCH

Praca naukowo-badawcza

Kryptonim „ELEFIZ"

Kod pracy: II.2.14.2.0.

WARSZAWA

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ ZARZĄDZANIA I DOWODZENIA

INSTYTUT WOJSK LĄDOWYCH

ZAKŁAD ROZPOZNANIA I WALKI ELEKTRONICZNEJ

UWARUNKOWANIA ZAGROŻENIA BEZPIECZEŃSTWA FIZYCZNEGO I ELEKTRONICZNEGO WOJSK W OPERACJACH WIELONARODOWYCH

Praca naukowo - badawcza

Kryptonim „ELEFIZ"

Kod pracy: II.2.14.2.0.

WARSZAWA **2008**

Opracował zespół autorski:
Pod kierownictwem ppłka dr. inż. Waldemara SCHEFFSA
w składzie:

1. mjr mgr Szymon MARKIEWICZ
2. mjr mgr Zbigniew MODRZEJEWSKI

Poszczególni członkowie zespołu opracowali:

1. **Ppłk dr inż. Waldemar SCHEFFS** *wprowadzenie, rozdział pierwszy, piąty oraz zakończenie*;
2. **mjr mgr Szymon MARKIEWICZ:** *rozdział drugi i czwarty, oraz załączniki 1,2 i 13.*
3. **mjr mgr Zbigniew MODRZEJEWSKI**: *rozdział trzeci i załączniki 3-12.*

Recenzent pracy: dr hab. inż. Józef JANCZAK

SPIS TREŚCI

WPROWADZENIE 5

1. PROBLEMATYKA PRACY I PROCEDURA BADAWCZA 9
   - 1.1. Problematyka pracy i problemy badawcze 14
   - 1.2 Hipoteza robocza 15
   - 1.3 Obszar badań i przedmiot badań 16
   - 1.4. Metody badawcze 19
   - 1.5 Przebieg badań 21

2. BEZPIECZEŃSTWO DZIAŁAŃ DOWÓDZTWA I WOJSK W OPERACJI WIELONARODOWEJ 25
   - 2.1. Podstawowe pojęcia bezpieczeństwa fizycznego i zagrożeń elektronicznych 26
   - 2.2. Istota działań wielonarodowych 30
   - 2.3. Analiza zagrożeń 39
   - 2.4. Analiza działania komórek sztabowych w połączonych działaniach wielonarodowych 43
   - 2.5. Rodzaje działań wojsk w operacji wielonarodowej 52
   - 2.6. Uwarunkowania bezpieczeństwa działań na szczeblu połączonego dowództwa wielonarodowego 58
   - 2.7. Wnioski 61

3. DIAGNOZA ŻAGROŻEŃ BEZPIECZEŃSTWA FIZYCZNEGO W OPERACJACH WIELONARODOWYCH 63
   - 3.1. Uwarunkowania bezpieczeństwa fizycznego w operacjach wielonarodowych 64
   - 3.2. Kryteria bezpieczeństwa fizycznego 65
   - 3.3. Analiza aktualnych rozwiązań systemowych ochrony fizycznej w operacjach wielonarodowych 66
     - 3.3.1. Analiza systemu ochrony i obrony bazy wojskowej na przykładzie VI zmiany PKW Irak 70
     - 3.3.2. Analiza środowiska bezpieczeństwa 79
     - 3.3.3. Analiza miejscowej ludności 80
     - 3.3.4. Analiza środków ochrony fizycznej wewnętrznej i zewnętrznej 88
     - 3.3.5. Analiza obiegu informacji alarmowych 94
   - 3.4. Wnioski 98

4. DIAGNOZA ŻAGROŻEŃ BEZPIECZEŃSTWA ELEKTRONICZNEGO 100

4.1. Uwarunkowania bezpieczeństwa elektronicznego w operacjach wielonarodowych 106
4.2. Kryteria bezpieczeństwa elektronicznego 109
4.3 Analiza aktualnych rozwiązań systemowych ochrony elektronicznej w działaniach wielonarodowych 113
4.3.1. Analiza środowiska bezpieczeństwa (obszary intensywności elektronicznej, funkcjonalne) 113
4.3.2. Analiza środków ochrony elektronicznej wewnętrznej i zewnętrznej 117
4.3.3. Analiza obiegu informacji 123
4.4. Wnioski 125

5 EFEKTY POZNANIA 127

ZAKOŃCZENIE 137

BIBLIOGRAFIA 141

SŁOWNIK SKRÓTÓW 143
WYKAZ ZAŁĄCZNIKÓW 144

WPROWADZENIE

„Bezpieczeństwo jest w głównej mierze zabobonem. Ani nie istnieje w przyrodzie, ani też dzieci człowiecze jako zbiorowość go nie doświadczają. Unikanie niebezpieczeństwa nie jest na dłuższą metę bezpieczniejsze niż wystawianie się na nie. Życie jest albo śmiałą przygodą, albo niczym"

Helen Keller

Wybuchające konflikty pomiędzy sąsiadami budzą zawsze niepokój wśród narodów z bliskiego sąsiedztwa. Jest to zrozumiałe, chociażby ze względu na falę uchodźców. Problem będzie znacznie większy, gdy sąsiedzi zostaną wciągnięci w działania zbrojne. Wówczas reakcja organizacji pokojowych zawsze będzie jedna – doprowadzenie do stanu przed wybuchem konfliktu. Organizacje pokojowe będą czyniły wówczas starania o wydelegowanie w rejon działań sił pokojowych przywracających ład i porządek. Dzisiaj, gdy świat stał się globalną wioską połączoną sieciami informatycznymi, wiedza, gdzie wybuchają konflikty i jaki mają przebieg nie jest tajemnicą. Trudnością jest określenie skali konfliktu. Zarysowane od końca XX wieku trendy rewolucyjnego porządkowania świata przez międzynarodowe organizacje terrorystyczne burzą dotychczasowy porządek świata. Coraz częściej zadajemy pytanie: jak będzie przebiegała wojna? czy będzie to starcie dwóch przeciwstawnych sobie stron wrogo do siebie nastawionych, czyli tego co nazywa T. Kotarbiński – kooperacją wzajemnie negatywną, czy wojna asymetryczna? Od określenia charakteru konfliktu zależeć będzie zarówno skala działań sił pokojowych jak i jego charakter. Eksperci wielu krajów oceniają, że dzisiejsze wojny opierają się na zjawiskach towarzyszących terroryzmowi, które w głównej mierze mają podłoże niemocy militarnej strony słabszej w stosunku do wysoko uprzemysłowionych państw świata. Spotyka się także określenie, że jest to odmiana działań militarnych w małej skali (small-scale conflict). Eksperci przewidują, że chociaż aktualnie nie są one jeszcze dominujące, to wkrótce staną się częstym rodzajem konfliktu, który należałoby dobrze zdefiniować. Często działania terrorystyczne nazywane są „brudną partyzantką", ale jak spojrzymy na teorię działań partyzantów to można wyróżnić zasadnicze różnice pomiędzy nimi i nie można ich utożsamiać. Tym bardziej, że działania terrorystyczne obejmują bardzo rozległe obszary, można powiedzieć, że nie istnieją granice dla ich działań, w przeciwieństwie do działań partyzantów, które ograniczają się do konkretnego obszaru.

Czynione sugestie, co do rodzajów konfliktów wiążą się ściśle z organizowaniem struktur wojsk do działań. Jest bardzo prawdopodobne, że wcześniej lub później, liczne państwa zostaną uwikłane, bezpośrednio lub pośrednio, w różnego typu konflikty militarne. Należy, więc przygotować swoje wojska do działań w operacjach pokojowych w ramach sojuszu oraz do działań w ramach sił wielonarodowych. Organizacje pokojowe, tj. ONZ czy OBWE nie zawsze będą zwracały się do jednej organizacji o pomoc. Z uwagi na duże koszty takich działań do operacji pokojowych delegowane są siły z wielu państw, czasami odmiennych kulturowo, etnicznie i technologicznie. Pewne wydaje się także, iż zróżnicowane doświadczenia wyniesione ze współczesnych walk z przeciwnikiem nieokreślonym, pozbawionym jasnych struktur organizacyjnych i standardowej taktyki (np.: walki w Wietnamie, Algierii, Jugosławii, Somalii, Afganistanie, Iraku) zmienią sposób myślenia o prowadzeniu regularnych działań zbrojnych i skłaniają decydentów do poszukania rozwiązań optymalnych struktur sił wielonarodowych.

Zgromadzone doświadczenia sugerują, że aktualne i przyszłe działania o charakterze poniżej progu wojny odbywać się będą w dużym zagrożeniu życia żołnierzy biorących udział w operacji. Należy zwrócić uwagę, że konflikty mają głównie podłoże narodowo-wyzwoleńcze oraz religijne. Odwaga i bitność żołnierzy walczących o swój kraj przeplata się z fanatyzmem religijnym niemającym swojego odniesienia w historii (nie wliczamy tu średniowiecznych wojen religijnych). Walka z takim przeciwnikiem lub chociażby kontrolowanie zawieszenia broni jest olbrzymim wyzwaniem da wojsk. Każde państwo wysyłające swoje wojska do innego kraju pragnie, aby powróciło w całości bezpiecznie. Zachowanie bezpieczeństwa stało się priorytetem każdej misji stabilizacyjnej lub operacji pokojowej.

Mając na uwadze obszar zagrożeń, z jakimi będą się spotykać wojska wielonarodowe działające w patrolach, konwojach czy w bazach, należy się liczyć z aktywnym oddziaływaniem zarówno grup eksternistycznych, terrorystów lub różnych grup przestępczych pragnących destabilizować sytuację w danym regionie. Możliwość wystąpienia rozległego ryzyka związanego z użyciem i rozprzestrzenianiem broni masowego rażenia, oddziaływaniem improwizowanymi ładunkami wybuchowymi (IED), porwaniami, napadami, zabójstwami przez strzelców (snajperów) jest bardzo duża. W tym kontekście głównymi celami bezpieczeństwa wojsk w ramach organizowanych operacji wielonarodowych będzie szybkie i skuteczne rozpoznanie zagrożeń i neutralizacja możliwości oddziaływania ogniowego na bazy i wojska w terenie. Należy się liczyć, że zapewnienie bezpieczeństwa będzie trudne, bowiem pomysłowość terrorystów i ich nieprzewidywalność stanowi główne

źródło zagrożeń. Mnogość zagrożeń, ich różnorodność wymaga od specjalistów wojskowych szerszego spojrzenia na procedury bezpieczeństwa wojsk. Zarówno w kontekście ochrony fizycznej, jak i obrony oraz ochrony elektronicznej. Wśród systemów, które jako pierwsze mogą być obiektami ataku występują te, które w czasie pokoju zapewniają stabilność biorących udział w działaniach na własnym terenie. Do takich obiektów można zaliczyć: koszary, magazyny, budynki sztabowe, węzły łączności, a także systemy telekomunikacyjne, teleinformacyjne, energetyczne itd. Ich podatność na dezorganizację, oddziaływanie ogniowe lub działania w przestrzeni fal EM może powodować określone skutki destabilizacji działań. Chociażby z przytoczonych powodów, zapewnienie właściwego działania wojsk i systemów przez nie wykorzystywanych w obszarze działania sił wielonarodowych jest jednym z podstawowych wymogów bezpieczeństwa.

Aktualne założenia i ustalenia dotyczące bezpieczeństwa działania wojsk podczas operacji pokojowych, wypracowane w ostatniej dekadzie XX wieku i pierwszej XXI wieku podlegają ciągłej analizie i ocenie z jednoczesną modyfikacją podstawowych ich założeń. Przeprowadzone badania dostępnych dokumentów normatywnych oraz standaryzacyjnych NATO, a także dotychczasowego dorobku wojsk w zakresie bezpieczeństwa w odbytych już misjach i operacjach, stały się podstawą do przedstawienia ogólnych uwarunkowań bezpieczeństwa fizycznego i elektronicznego w operacjach wielonarodowych.

Na przestrzeni kilkunastu lat daje się zauważyć pewną stagnację w publikacjach dotyczących problematyki bezpieczeństwa fizycznego i elektronicznego. Częściej wspomina się o bezpieczeństwie informatycznym, łączności, zasadach działania niż o systemie bezpieczeństwa w operacjach wielonarodowych. Coraz częstsze wyjazdy na misje i operacje pokojowe wojsk polskich a jednocześnie przynależność do Sojuszu NATO wymaga nowego spojrzenia na problemy związane z bezpieczeństwem działań w ogóle i bezpieczeństwem fizycznym i elektronicznym w szczególności w operacjach wielonarodowych. Nowe poglądy były prezentowane w różnych opracowaniach naukowych i publikacjach autorów , nie miały jednak odzwierciedlenia w dokumentach normalizacyjnych sygnaturowanych przez Sztab Generalny WP.

Charakter współczesnych operacji wielonarodowych stawia przed wojskami stale rosnące wymagania. Aby im sprostać, działania poszczególnych kontyngentów powinny być przede wszystkim ciągłe w czasie i przestrzeni, prowadzone przy pełnej koordynacji wysiłków wszystkich sił zaangażowanych w proces ochrony i obrony z zachowaniem zasady wzajemnego uzupełniania się. Zgodnie z ogólnie przyjętymi zasadami, organem integrującym

działalność całego systemów bezpieczeństwa powinien być sztab sił wielonarodowych z odpowiednią komórką odpowiedzialną za planowanie i realizowanie całości przedsięwzięć. Komórka ta koordynuje działania sił interwencyjnych: patrolowych, wartowniczych i specjalistycznych (np. WE) delegowanych z każdego państwa. Wszystkie zarządzenia i wytyczne tej komórki w zakresie działań podejmowanych na rzecz bezpieczeństwa są obowiązujące dla wszystkich uczestników biorących udział w operacji wielonarodowej. Komórka bezpieczeństwa poprzez swoje odpowiednie narzędzia dowodzenia angażuje wszystkie dostępne siły i środki, scalając ich wysiłek w jednolity system bezpieczeństwa wojsk i baz wojskowych. Kieruje działaniami stawiając (przekazując) kolejne zadania wynikające z celu operacji wielonarodowych. Szczególnie istotna jest tu współpraca i koordynowanie przedsięwzięć z komórką rozpoznania i operacyjną. Wynika z tego, że działania komórki bezpieczeństwa stanowią celowe, skoordynowane połączenie wysiłków wszystkich sił i środków przewidzianych do ochrony i obrony, jakie posiadają siły wielonarodowe, działające według jednolitego planu bezpieczeństwa. Takie działania pozwalają na:

- podporządkowanie systemu bezpieczeństwa dowódcy i organom odpowiedzialnym za bezpieczeństwo działania wojsk i baz wojskowych;
- skupienie wysiłku sił i środków ochrony fizycznej i elektronicznej na wykonaniu najbardziej istotnych zadań oraz wykorzystanie różnorodnych sił i środków w jednym czasie, na określonej przestrzeni;
- bieżącą wzajemną wymianę informacji o zagrożeniach przez różne siły i środki uczestniczące w operacji wielonarodowej;
- szybką, pełną i kompleksową ocenę zdobytych informacji o realnych zagrożeniach.

Jak wynika z dotychczasowych rozważań, zadania dla sił ochrony i obrony powinny być realizowane według planu opartego na jednolitej myśli zapewnienia bezpieczeństwa żołnierzom. Działania sił ochrony, organizowane w sposób kompleksowy z racjonalnym wykorzystaniem jakościowo nowych środków, stwarzają warunki stosunkowo pełnego ogarnięcia i zidentyfikowania wszystkich najważniejszych obszarów zagrożeń oraz elementów powodujących te zagrożenia.

Aby osiągnąć takie efekty, niezbędne staje się wykonanie szeregu przedsięwzięć w zakresie identyfikacji zagrożeń bezpieczeństwa fizycznego i elektronicznego wojsk biorących udział w operacji wielonarodowej.

1. PROBLEMATYKA PRACY I PROCEDURA BADAWCZA

Wojska z całym bagażem doświadczeń o minionych i aktualnie prowadzanych konfliktach stają w obliczu wielu zagrożeń związanych z dzianiem pokojowym. Można powiedzieć, że przecież w czasie pokoju szkoli się tylko wojsko a nie prowadzi działania bojowe. Wojska zawsze realizowały dwa główne zadania: działania zbrojne z przeciwnikiem ściśle określonym i dziania pokojowe przeciwko określonemu lub nie przeciwnikowi. Przykładów w historii chociażby Europy jest wiele świadczących o działalności pokojowej. Żeby daleko nie szukać dla przykładu podczas powstań śląskich państwa Ententy delegowały siły wojskowe do nadzorowania przestrzegania porządku podczas plebiscytów, lub bliższe czasom współczesnym działania pokojowe w byłej Jugosławii, Kosowie, a na kontynencie afrykańskim w Somalii, Etiopii itd. Organizacje pokojowe stają, więc przed trudnym zadaniem utrzymania pokoju w regionach i na całym świecie. Gdy ucichły zagrożenia wojny totalnej pomiędzy dwoma supermocarstwami zrodziły się inne, może bardziej niebezpieczne zagrożenia dla sytuacji pokojowej. Zagrożenia niemilitarne, jakie nasiliły się począwszy od końca XX wieku (szczególnie terroryzm) przenoszą się coraz częściej na środowisko życia cywilnego. Siły zbrojne stały się gwarantem utrzymania stabilizacji i pokoju prawie w każdym regionie świata. Zobowiązania, jakie przyjęła Polska po wstąpieniu do Sojuszu Północnoatlantyckiego nakłada na nasze siły zbrojne powinność uczestniczenia w operacjach pokojowych przede wszystkim pod auspicjami NATO, a następnie Unii Europejskiej, ONZ, OBWE. Owa powinność, a zarazem chęć uczestnictwa w operacjach pokojowych razem z innymi siłami zbrojnymi lub organizacjami działającymi na rzecz utrzymywania i utrwalania pokoju na świecie, zobowiązują nasze Siły Zbrojne do szukania coraz nowszych sposobów działania, z doskonalszymi niż dotychczas rozwiązaniami organizacyjnymi i technicznymi zdolnymi sprostać wyzwaniom obecnych i przyszłych operacji. Obecność naszych sił zbrojnych w wielu rejonach świata, gdzie toczą się walki o utrzymanie pokoju stawia przed nami nowe, inne znaczeniowo zadania. Różnorodność realizowanych zadań bezpośrednio przekłada się na technikę i taktykę stosowaną przez komponent wojskowy delegowany do udziału w operacji.

Każde działania w rejonie objętym mandatem pokojowym są inne od już odbytych. Każde ma innych charakter i do każdych wojska przygotowują się inaczej. Osiągnięcie wymaganych zdolności wojsk w złożonej sytuacji ciągłego zagrożenia stawia przed dowódcą konkretne zadania do realizacji. Dlatego też bezpieczeństwo wojsk w tych działaniach stało się priorytetowym zadaniem. Żadne społeczeństwo nie wybaczy administracji rządzącej nieuzasadnionej śmierci swoich żołnierzy. Organizując komponent wojsk delegowanych do działań w operacji wielonarodowej szczególną uwagę poświęca się opracowaniu zadań i procedur bezpieczeństwa fizycznego i elektronicznego. Podczas organizacji systemu bezpieczeństwa należy zwrócić uwagę na wiele istotnych czynników występujących w terenie i środowisku przyszłych działań. Zagrożeń jest wiele, a w erze globalizacji, gdy świat stał się tak mały, informacja jest cennym aktywem, szczególnie ta dotycząca zagrożeń. Oczywiście każdą informację można kupić, sprzedać, ukraść lub zdobyć samemu na bazie doświadczeń. Pytaniem jest jednak jedno na ile te informacje o zagrożeniach będą pełne i wystarczą do opracowania odpowiednich procedur bezpieczeństwa. Czy przeanalizowano wszystkie uwarunkowania zagrożeń czy coś pominięto? Zdobyte informacje o działaniach wielu grup terrorystycznych, bojowników działających nie zawsze są prawdziwe, często preparuje się specjalne informacje dezinformując wojska o faktycznej sytuacji w rejonie działania wojsk pokojowych. Od sprawnego wydziału bezpieczeństwa, rozpoznania zależy jak będą interpretowane.

Epistemologiczny dorobek problematyki bezpieczeństwa wojsk w operacjach wielonarodowych w polskiej literaturze przedmiotu jest niezwykle ubogi i nawet trudno jest go odnaleźć. Bardziej ogólne publikacje dotyczące działań są dostępne, natomiast szczegółowe nie, z uwagi na ich poufny charakter, bowiem nadal niektóre rozwiązania organizacyjne są wykorzystywane w aktualnie prowadzonych operacjach pokojowych. Trudno jest, zatem w ramach jednej pracy naukowo- badawczej wypełnić obszar niewiedzy, tak ubogo eksploatowany w przeszłości.

Potrzeba uporządkowania badań w obszarze zapewnienia bezpieczeństwa fizycznego i elektronicznego wojsk w działaniach wielonarodowych narastała stopniowo w toku pracy naukowej i dydaktycznej. Pierwsze oznaki braku wiedzy o tej problematyce w wojskach lądowych zidentyfikowano w czasie organizowania misji pokojowych w ramach SFOR, KFOR, a następnie misji stabilizacyjnej sił wielonarodowych w Iraku. Wówczas to przeprowadzono cykl badań wstępnych zmierzających do wyjaśnienia problematyki bezpieczeństwa głównie elektronicznego przez siły delegowane do działań poniżej progu wojny.

W okresie tym rozpoczęto pierwsze prace w ramach wspomnianej problematyki. Konsekwencją rozpoczętej naukowej penetracji były badania poświęcone zagrożeniom w nowych uwarunkowaniach organizacyjnych i strukturalnych w AON[1]. Uzyskany we wspomnianych latach materiał badawczy pozwolił na porównanie i jednoczesne wykorzystanie otrzymanych wyników badań, które kontynuowano aż do opracowania niniejszej pracy.

Pierwsze potrzeby poszerzenia wiedzy zaistniały już w połowie lat 90 tych ubiegłego wieku, gdy wyniknął problem działania polskich jednostek w misjach stabilizacyjnych w byłej Jugosławii. Pogłębienie dociekań nad problemem bezpieczeństwa podczas działań patrolowych, konwojowych ochrony ludności czy baz wojskowych w operacji wielonarodowej uwidoczniły się jeszcze bardziej jaskrawo w pierwszych latach XXI wieku. Zidentyfikowane problemy podczas badań wstępnych oraz niewiedza o organizowaniu systemu bezpieczeństwa w sztabie sił wielonarodowych posłużyły do opracowania zasadniczych założeń pracy.

Konstatacja, że brakuje dostatecznej wiedzy na temat uwarunkowań zagrożeń bezpieczeństwa fizycznego i elektronicznego w operacjach wielonarodowych, potwierdzały wnioski napływające z wojsk operacyjnych podczas ćwiczeń oraz spostrzeżenia własne autorów, uczestników tych operacji i potrzeby zgłaszane przez oficerów powracających z operacji pokojowych i stabilizacyjnych np. z byłej Jugosławii czy Iraku. Potrzeba wyodrębnienia zagadnień bezpieczeństwa wojsk przez siły delegowane do działań wielonarodowych wynikała z różnych procedur przygotowania i analizy zagrożeń w SZ, które delegowały swoje pododdziały. Różnice w procedurach przygotowania i opracowania dokumentów bojowych, procedurach koordynacyjnych wynikały także z konieczności rozdzielenia treści informacyjnych będących efektem pracy oficerów odpowiedzialnych za ochronę i obronę w obszarze działania sił komponentu wojsk lądowych (sił zadaniowych) we wszystkich jej strefach działania i zainteresowania. Częściowych rozwiązań w tym obszarze niewiedzy dostarczyły minione konflikty i wnioski z nich płynące oraz własne doświadczenia i wypracowane procedury szkolenia w kraju. Była to podstawa wyjściowa przygotowania rozwiązań organizacyjnych i strukturalnych proponowana przez zespół badawczy.

Jednym z ważnych etapów prowadzonych badań była analiza literatury dotyczącej organizowania systemu bezpieczeństwa fizycznego i elektronicznego (SOP dywizji

---

[1] *Walka elektroniczna w operacjach pokojowych*, pod red. W. Scheffsa, AON Warszawa 2005; *Walka elektroniczna w operacjach kryzysowych*, pod red. W. Scheffsa, AON, Warszawa 2006. Rozpoznanie w działaniach asymetrycznych pod red. M. Wrzoseka, AON, Warszawa 2006, *Walka elektroniczna w działaniach asymetrycznych*, pod red. W. Scheffsa, AON, Warszawa 2007.

wielonarodowej w Iraku) i organizowania komórek odpowiedzialnych za wspólne bezpieczeństwo działania wszystkich przydzielonych sił. Wnioski wynikające z ćwiczeń i konfliktów zbrojnych, opinie ekspertów powracających z misji w Iraku i z byłej Jugosławii stanowiły uzupełnienie prowadzonej analizy. Literatura przedmiotu jest bardzo uboga[2], można rzec, że bardzo nieliczne publikacje traktują problem wybiórczo, nie identyfikując zaistniałych faktów i zdarzeń z operacjami wielonarodowymi, raczej z incydentami wynikającymi ze specyfiki działań. Z tego powodu zespół badawczy dociekał problemu w dużej części w dostępnych publikacjach doktrynalnych NATO i opracowaniach charakteryzujących problematykę bezpieczeństwa fizycznego i elektronicznego w działaniach wielonarodowych. Literatura traktująca bezpieczeństwo fizyczne odnosi się głównie do wyposażenia żołnierza i zasad jego zachowania, brak jest natomiast rozwiązań organizacyjnych całości problemu bezpieczeństwa sił wielonarodowych. Nieco więcej informacji na temat bezpieczeństwa elektronicznego można znaleźć literaturze narodowej i NATO. Pomimo i tak skromnej literatury wyodrębniono szereg uwarunkowań organizacyjnych dla systemu bezpieczeństwa i zinterpretowano zakres badanego zjawiska w tych działaniach. Zespół autorski bazując na doświadczeniach ekspertów i własnych przykładach oraz wnioskach z minionych konfliktów, a także teorii operacji wielonarodowych, przyjął ogólne założenie, że bezpieczeństwo fizyczne i elektroniczne w operacjach wielonarodowych stanowi połączony wysiłek podejmowany przez odpowiednio do tego przygotowane i zorganizowane komórki bezpieczeństwa. Głównym celem działania takiej komórki jest integrowanie przydzielonych sił pod jednym dowództwem i jednolitymi procedurami działania na poziomie dowództwa. Każdy dowódca delegowanych sił dowodzi własnymi pododdziałami zgodnie z narodowymi procedurami. Organem zarządzającym tymi działaniami jest komórka bezpieczeństwa koordynująca wszystkie przedsięwzięcia związane z rozpoznaniem, oddziaływaniem na zaistniałe zagrożenia wojsk i baz wojskowych oraz dowództw realizujących zadania.

Jednym z cenniejszych źródeł wiedzy dla autorów był udział w konferencjach i seminariach naukowych organizowanych zarówno w Akademii Obrony Narodowej jak i przez inne placówki dydaktyczno-naukowe tj, Wojskowa Akademia Techniczna, Państwowy Instytut Telekomunikacji czy Centrum Techniki Morskiej. Watro wymienić między innymi:

[2] Dokumenty w dużej części są niejawne. Prezentowane poglądy stanowią tylko możliwe fragmenty analizowane z pozyskanych materiałów źródłowych.

1) Konferencję na temat „Bezpieczne Niebo" zorganizowana 10 września 2002 w AON pod patronatem Biura Bezpieczeństwa Narodowego oraz Ministerstwa Obrony Narodowej;
2) Seminarium na temat „Prognozowanie zagrożenia w nowych uwarunkowaniach międzynarodowych", zorganizowana w dniu 5 kwietnia 2006 przez Zakład Rozpoznania Wojskowego i Walki Elektronicznej, Instytutu Zarządzania i Dowodzenia w Wydziale Wojsk Lądowych AON z udziałem przedstawicieli przemysłu, oficerów Sztabu Generalnego Wojska Polskiego, Dowództwa Wojsk Lądowych i rodzajów wojsk;
3) Seminarium na temat „Charakter przyszłych operacji militarnych", zorganizowane 2005 przez Katedrę Sztuki Operacyjnej i Taktyki Wydziału Wojsk Lądowych AON z oficerów rodzajów wojsk i Sztabu Generalnego Wojska Polskiego;

Pozyskane ta 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.

Sytuacja problemowa powstała wskutek zaistnienia szeregu czynników. Do decydujących czynników można zaliczyć powstanie nowych wyzwań, przed którymi stanęliśmy w ostatnich latach (udział w działaniach stabilizujących w Iraku i aktualnie Afganistanie), gdzie przeciwnik używał i nadal używa różnych środków zagrażających życiu żołnierzy (IED, ostrzał artyleryjski, snajperzy, porwania, zamachy, środki elektroniczne). Brak dostatecznej analizy i oceny zagrożeń powoduje, że jesteśmy mało skuteczni i zmuszeni do korzystania z informacji od innych. Narastające zagrożenia ze strony różnych nieformalnych grup, których przywódcy nawołują do zachowań destabilizacyjnych (szczególnie na tle religijnym) w danym rejonie, regionie lub kraju są głównymi przyczynami zaistniałej sytuacji problemowej. Dodatkowym czynnikiem rysującym sytuację problemową jest organizowanie za każdym razem innej i inaczej funkcjonujących organizacji odpowiedzialnej za bezpieczeństwo wojsk. Dokonywane zmiany powinny podnosić jakość i możliwości skutecznego oddziaływania na zaistniałe zagrożenia, a nie zawsze takie działania są efektywne.

Najważniejszym, zatem problemem jest uświadomienie sobie różnic, jakie występują w teorii i praktyce ochrony w czasie pokoju we własnych koszarach a jakie występują w bazach wojskowych w kraju objętym działaniami sił wielonarodowych w ramach operacji pokojowych. Pozwoli to, na określenie uwarunkowań zagrożenia bezpieczeństwa oraz przedstawi możliwości i potrzeby wypracowania propozycji koniecznych zmian w teorii

i praktyce organizowania i wykorzystania systemu bezpieczeństwa wojsk w operacjach wielonarodowych.

Wymienione podstawowe czynniki legły u podstaw sformułowanego głównego celu pracy, celów szczegółowych i problemów badawczych oraz założonej hipotezy roboczej.

1.1. CELE I PROBLEMY BADAWCZE

Odpowiedzialność za bezpieczeństwo fizyczne i elektroniczne w operacji wielonarodowej ponoszą dowódcy. Jednak wspierani są przez odpowiednie organa sztabowe, których rola i znaczenie w naszych Siłach Zbrojnych jest nieco inna niż wynika to z dokumentów normatywnych NATO.

Zaistniała sytuacja problemowa wymaga przeprowadzenia rzetelnych badań, których wyniki będą asumptem do rozwiązań praktycznych w zakresie określenia w pierwszej kolejności uwarunkowań bezpieczeństwa fizycznego i elektronicznego, a następnie zaproponowania rozwiązań strukturalnych komórki bezpieczeństwa w operacji wielonarodowej. Zachodzi także pilna potrzeba sprecyzowania optymalnych procedur koordynacji i realizacji zadań przez siły delegowane do ochrony.

W aspekcie powyższego **celem poznawczym** prowadzonych badań uczyniono: zidentyfikowanie zagrożeń dla wojsk i baz wojskowych w operacjach wielonarodowych.

Założono, że praca będzie miała także wymiar praktyczny, wobec powyższego uznano, że jej **celem utylitarnym** jest przedstawienie do praktycznego wykorzystania zaprezentowanych wniosków w zakresie sposobów ochrony i obrony przed nieprzewidywalnym przeciwnikiem w czasie działań wojsk w bazie i poza nią.

Aby osiągnąć tak określone cele pracy badawczej należało rozwiązać **problem główny**, wyrażony w pytaniu:

Jakie uwarunkowania zagrożenia bezpieczeństwa dla wojsk wielonarodowych determinują skuteczne ich działanie w operacjach wielonarodowych?

Przedstawiony cel pracy oraz problem główny wymagał znalezienia wiarygodnych i w miarę wyczerpujących odpowiedzi na następujące **pytania problemowe:**

1. *Jakie występują zagrożenia dla wojsk wielonarodowych podczas realizacji zadań?*
2. *Jakie warunki muszą być spełnione, aby zapewnić bezpieczeństwo fizyczne i elektroniczne wojsk wielonarodowych?*
3. *Jakie są potrzeby i możliwości ochrony fizycznej w bazach wojskowych i podczas realizacji zadań poza bazą przez siły wielonarodowe?*
4. *Jakie są potrzeby i możliwości obrony elektronicznej baz wojskowych i wojsk podczas realizacji zadań poza bazą przez siły wielonarodowe?*
5. *Jaka powinna być rola i zadania podsystemów ochrony fizycznej i elektronicznej wspomagających system bezpieczeństwa sił wielonarodowych?*

Szczególną uwagę zespół autorski poświęcił tym obszarom, w których wskazana jest konieczność wprowadzenia zmian. Wynikają one z wielu uwarunkowań. Przede wszystkim zmiany w dotychczasowym ujęciu przedmiotu badań. W obszarze zainteresowania zespołu autorskiego znalazły się również problemy wynikające z uwarunkowań zarządzania i kierowania, w tym kierowania przez zespoły funkcyjne zbiorowością międzynarodową. Tak zarysowany przedmiot badań ukazuje zakres problemowy zainteresowań naukowych zespołu badawczego. Uwzględniono przy tym aktualny stan wiedzy w temacie[3], dorobek naukowy[4] i doświadczenie osób tworzących zespół badawczy.

1.2. HIPOTEZA ROBOCZA

W wyniku określenia celów pracy naukowo-badawczej i sformułowania problemów badawczych autorzy sprecyzowali następującą *hipotezę roboczą*:

Dotychczasowa organizacja systemu bezpieczeństwa wojsk w operacjach wielonarodowych organizowana był głównie w oparciu o doświadczenia sił amerykańskich. Tak było w przypadku wielonarodowej dywizji pod dowództwem polskim. Przenoszenie doświadczeń narodowych lub innych państw nie jest rozwiązaniem w pełni dobrym. Wnioski i doświadczenia wyniesione z operacji pokojowych w byłej Jugosławii przez różne państwa wskazują, że to głównie zagrożenia występujące w rejonie działań sił wielonarodowych są

[3] Wykorzystano prace naukowe, promocyjne i publikacje popularno-naukowe.
[4] Kierownik pracy opracował rozprawę doktorską z zakresu organizowania elementów WE.

wykładnią organizacji systemu bezpieczeństwa. One, bowiem sugerują, jakie zastosować rozwiązania organizacyjne i sprzętowe w ochronie fizycznej, jakie w obronie i ochronie elektronicznej. Doraźna metoda organizowania systemu bezpieczeństwa fizycznego i elektronicznego w ramach komponentu wojsk lądowych w operacji wielonarodowej w świetle uwarunkowań zagrożeń bezpieczeństwa wydaje się niewystarczająca. Może doprowadzić do sytuacji, kiedy system bezpieczeństwa nie wypełni w wymaganym zakresie swoich elementarnych zadań. Taka sytuacja może skutkować obniżeniem zdolności bojowej komponentu lądowego i doprowadzić do znacznego obniżenia skuteczności prowadzenia operacji wielonarodowych..

Transformacja systemu bezpieczeństwa wojsk powinna przebiegać w kilku zasadniczych kierunkach:

- *integracji wszystkich systemów i sposobów ochrony fizycznej i elektronicznej, zarówno organicznych jak i współpracujących, w jeden efektywny spójny system;*
- *poszukiwania nowych metod i sposobów zabezpieczenia przed zagrożeniami szczególnie terrorystycznymi;*
- *innowacji technologicznej (wprowadzanie nowych technik i narzędzi - sprzętu);*
- *strukturalnej - tworzenie elastycznie reagujących komórek bezpieczeństwa;*
- *organizacyjnej dotyczącej efektywnego koordynowania wszystkich przedsięwzięć z zakresu ochrony i obrony w działaniach wielonarodowych.*
- *proceduralnej – doskonalenie dotychczasowych i wypracowanie nowych procedur bezpieczeństwa.*

Przy takich założeniach niezbędna jest weryfikacja aktualnej teorii organizowania baz wojskowych jej systemu bezpieczeństwa i weryfikacja dotychczasowego sposobu organizowania komórki odpowiedzialnej za bezpieczeństwo wojsk. Jednocześnie należy doskonalić system bezpieczeństwa pod względem technicznym i taktycznym na poziomie komponentu wojsk lądowych delegowanego do operacji wielonarodowej.

1.3. OBSZAR BADAŃ I PRZEDMIOT BADAŃ

Obszar badań stanowił system bezpieczeństwa fizycznego i elektronicznego w kontyngencie sił wielonarodowych działającym poza granicami kraju w uwarunkowaniach zagrożeń wynikających z prowadzonej operacji. Dodatkowo bliższe i dalsze otocznie systemu.

Obszarem badań była, więc komórka bezpieczeństwa oraz powiązane z nią strukturalnie, hierarchicznie, funkcjonalnie i informacyjnie inne komórki sztabowe i przydzielone siły do ochrony fizycznej i elektronicznej działające w wymiarze wielonarodowym.

System bezpieczeństwa sił wielonarodowych został określony jako system ochrony obiektów. W takim rozumieniu jest „... to jakikolwiek obiekt fizyczny lub abstrakcyjny, w którym można wyróżnić jakieś wzajemne powiązane dla operatora elementy. W tym sensie podział czegoś na systemy jest względny i zależy od tego kto, przy pomocy czego i do czego poklasyfikował jakiś zbiór na systemy. Dlatego elementy jednego systemu mogą stanowić składniki innych systemów[5]".

Czyli dla potrzeb pracy autorzy przyjęli definicję systemu bezpieczeństwa o następującej treści: System bezpieczeństwa wojsk w operacji wielonarodowej to rozwinięty (na lądzie i w powietrzu) potencjał środków ochrony fizycznej i elektronicznej (siły i środki), wewnętrznie powiązany i skoordynowany jednolitymi więziami organizacyjnymi (hierarchicznymi, funkcjonalnymi, informacyjnymi i technicznymi), działający na rzecz wojsk w bazach i wojsk poza bazą w odniesieniu do przyjętej koncepcji bezpieczeństwa". System bezpieczeństwa jest częścią składową systemu walki sił wielonarodowych, a jednocześnie częścią systemu działań pokojowych, a skuteczność jego funkcjonowania determinuje, w sposób zasadniczy, powodzenie tych działań (działań pokojowych). Skuteczny system bezpieczeństwa pozwala w znacznej mierze rekompensować zagrożenia ze strony terrorystów lub innych grup ekstremistycznych.

Ze struktury systemu bezpieczeństwa wynika, że składa się on z podsystemów: ochrony fizycznej, obrony i ochrony elektronicznej, realizacji zadań ochrony oraz informacyjnego.

Przedmiotem badań były rozwiązania przedstawione w dokumentach standaryzacyjnych NATO w zakresie ochrony i obrony oraz dotychczasowe założenia teoretyczne dotyczące bezpieczeństwa wojsk i baz wojskowych w SZ RP, a także aktualne siły i środki zabezpieczające bezpieczeństwo żołnierzy wraz z ich powiązaniami hierarchicznymi, funkcjonalnymi i informacyjnymi.

Z uwagi na złożoność przedmiotu badań proces badawczy odbywał się w kilku płaszczyznach, w których rozpatrywano:

— przyjętą procedurę badawczą;

---

[5] Instrukcja o Ochronie obiektów wojskowych, OIN 3/2008, Warszawa, s. 8.

— teoretyczne założenia operacji wielonarodowych;

— implikacje organizacji sztabowych komórek bezpieczeństwa w rozwiązaniach dowództw wielonarodowych;

— identyfikację zagrożeń dla bezpieczeństwa fizycznego i elektronicznego w bazie wojskowej i ocenę aktualnych możliwości delegowania sił przeciwdziałania zagrożeniom w ramach działań wielonarodowych;

— pożądany kształt systemu bezpieczeństwa dla sił wielonarodowych.

Podczas badań analizowano materiały teoretyczne dotyczące zarówno poglądów na organizowanie ochrony fizycznej i elektronicznej, prowadzenie akcji przeciwko terrorystom z bazy oraz podczas partoli lub zasadzek. Analizowano również dotychczasowe dokumenty normatywne obowiązujące w NATO i naszych siłach zbrojnych.

Na potrzeby badań problematyka badawcza została przez zespół autorski ograniczona do:

- teoretycznych aspektów uwarunkowań zagrożenia bezpieczeństwa w misji stabilizacyjnej w Iraku,
- możliwości organizacji sytemu ochrony fizycznej i elektronicznej przez siły wielonarodowe.

Już na etapie badań wstępnych zespół autorski zmierzył się z problemem braku dokumentów normatywnych opisujących i zatwierdzających działanie systemu ochrony w operacjach wielonarodowych zarówno w NATO jak i wojskach lądowych RP. Dlatego w pierwszej części wiedzę oparto o dokumenty pochodzące z poszczególnych zmian polskiego kontyngentu w IRAKU oraz z doświadczeń osób powracających z misji pokojowych. Zweryfikowano założenia teoretyczne organizacji komórek sztabowych odpowiedzialnych za przygotowanie i prowadzenia WE w działaniach wielonarodowych.

Analiza trendów panujących w Sojuszu Północnoatlantyckim dotyczących bezpieczeństwa pozwoliła na konstatację, iż wielonarodowość jednostek organizacyjnych wojsk lądowych na poziomie sił delegowanych do zadań jest faktem. Prawdziwym zatem wydaje się twierdzenie, iż bezpieczeństwo wojsk należy rozpatrywać nie przez pryzmat tylko swoich doświadczeń ale korzystać i wykorzystać doświadczenia innych.

1.4. Metody badawcze

W procesie badawczym posługiwano się podejściem systemowym, strukturalnym i funkcjonalnym. Zastosowanie takich metod - sposobów podejścia wynikało z potraktowania przedmiotu badań jako systemu, zarówno w samych badaniach jak i w ich wyniku.

Podejście strukturalne stanowiło logiczne uzupełnienie podejścia systemowego, gdyż przyjętemu przedmiotowi badań przysługuje cecha strukturalności, bez której głębszego poznania optymalizacja działalności systemu bezpieczeństwa byłaby niemożliwa.

Posłużenie się podejściem funkcjonalnym związane było ściśle z zastosowanym podejściem systemowym i strukturalnym. Stosując zasadę włączenia dokonywano analizy wewnętrznej systemu oraz określono ocenę funkcji podsystemów w odniesieniu do ogólnych właściwości działalności bezpieczeństwa sił wielonarodowych. Stosując zasadę wyjścia, badano natomiast funkcjonowanie poszczególnych podsystemów przez pryzmat funkcjonowania działań nadrzędnych.

W czasie prowadzenia badań posługiwano się empirycznymi i teoretycznymi metodami badawczymi.

Wśród metod teoretycznych dominowała analiza, która umożliwiła określenie cech, związków i zależności badanych elementów komórki bezpieczeństwa, ze szczególnym uwzględnieniem koordynowania przydzielanych sił do ochrony fizycznej i elektronicznej z innych państw. Analizę stosowano zarówno jako proces myślowy oraz jako metodę badawczą. Analiza literatury przedmiotu oraz dokumentów normatywnych umożliwiła pogłębienie wiedzy zespołu badawczego w obszarze założonej problematyki badawczej, pozwoliła przedstawić i uzasadnić ważność i aktualność sprecyzowanych problemów naukowych. Uzyskany tą metodą materiał wykorzystano jako podbudowa 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 poglądzie na organizację komórki bezpieczeństwa), różnic (np.: różne procedury ochrony baz wojskowych przez poszczególne siły delegowane do operacji oraz różne procedury przygotowania dokumentów) 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 struktur organizacyjnych ochrony fizycznej i elektronicznej, gdzie możliwe było wyodrębnienie sił i środków w operacjach wielonarodowych). Stanowiła podstawę przy formułowaniu i weryfikacji hipotezy roboczej, 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-procentwej pewności wnioskowania, dają natomiast wystarczające prawdopodobieństwo.

Abstrahowanie pozwoliło na usunięcie z obszaru badań cech i zależności mało istotnych (np.: jak funkcjonowanie komórek sztabowych na SD w operacji wielonarodowej) oraz uwzględnienie tych, które były najważniejsze w aspekcie badanego problemu (np.: zagrożenia dla bezpieczeństwa baz wojskowych w wyniku ataku terrorystycznego możliwości organizacji i koordynacji działań przedzielonych sił do ochrony baz wojskowych oraz wyposażenie elektroniczne uwzględniające spektrum pracy środków elektronicznych przeciwnika).

Uogólnienie – wiążące się ściśle ze wskazanymi powyżej metodami – pozwoliło na sformułowanie wniosków wyższego rzędu, wniosków ogólnych, co szczególnie ujawniło się w części pracy dotyczącej określenia wyników końcowych.

Metody empiryczne posłużyły do zgromadzenia danych w postaci materiału faktograficznego. Obserwację wykorzystano jako technikę uczestniczącą i nieuczestniczącą oraz standaryzowaną i niestandaryzowaną[6]. Stosowana była w ramach działalności służbowej autorów, umożliwiając dostrzeganie wielu faktów, zdarzeń i zjawisk z pozycji wykładowcy. Obserwacja (zewnętrzna – nieuczestnicząca i wewnętrzna – uczestnicząca) prowadzona była na bazie własnych doświadczeń z odbytej misji w Iraku (IV zmiana) oraz w trakcie szeregu ćwiczeń w AON organizowanych w latach 1996-2008, ćwiczeń dowódczo-sztabowych wojsk operacyjnych („Marzec 2002", „Granica", „Bieszczady"). Zaobserwowane, istotne dla problematyki badawczej fakty (wyniki obserwacji) zarejestrowano w postaci notatek.

Z metod badania opinii zastosowano ankietowanie respondentów, szczególnie tych, którzy powrócili z misji pokojowych z byłej Jugosławii i Iraku. Ankietę stosowano w celu

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

zebrania doświadczeń wielu specjalistów tj. rozpoznania, WE, saperów, logistyków. Dodatkowo korzystano z opinii ekspertów Zarządu Analiz Wywiadowczych i Rozpoznawczych P2, Zarządu Rozpoznania i WE Dowództwa Wojsk Lądowych, ośrodków radioelektronicznych oraz środowiska naukowego.

1.5. PRZEBIEG BADAŃ

Proces badawczy podzielono na trzy etapy:

1. Wstępny etap badań.
2. Etap badań właściwych.
3. Końcowy etap badań.

Analiza sytuacji problemowej oraz konstatacja celów badań pozwoliła na sformułowanie podstaw merytoryczno-metodologicznych pracy oraz scenariusza badań. Jednocześnie zrozumienie i dostrzeżenie luk w istniejącej wiedzy dotyczącej problematyki planowania, organizowania realizacji przedsięwzięć ochrony fizycznej i elektronicznej w operacjach wielonarodowych, będącej obszarem zainteresowania zespołu autorskiego poszerzyło sytuację problemową. Zespół autorski podjął próby teoretycznego rozwiązania problemu poprzez analizy, porównania, analogie, wywiady i dalsze studiowanie literatury. W ich trakcie pojawiła się potrzeba dokonania podziału głównego problemu naukowego na elementy ograniczające zakres rozpatrywanych zagadnień. W tym celu wyodrębniono problemy szczegółowe zapoczątkowując etap badań właściwych.

Etap badań właściwych wymagał zastosowania szeregu metod badawczych w celu rozwiązania przedstawionych uprzednio problemów szczegółowych. Wybór tych metod uwarunkowany był przede wszystkim charakterem poszczególnych problemów i literatury źródłowej, którą stanowiły dokumenty o charakterze normatywnym i częściowo o znaczeniu okresowym. Konsekwencją rozwiązania problemów szczegółowych było uzyskanie nowych faktów naukowych, które pozwoliły na weryfikację hipotezy.

Rozwiązywanie problemów szczegółowych powodowało uzyskiwanie kolejnych faktów naukowych. Te zaś z kolei dawały możliwość zweryfikowania i przedstawienia potencjalnego rozwiązania głównego problemu w postaci hipotezy roboczej:

Skuteczne kierowanie systemami bezpieczeństwa fizycznego i elektronicznego delegowanych sił z każdego państwa w operacjach wielonarodowych, możliwe było tylko

w warunkach posiadania właściwego organu koordynującego te działania. Każda operacja powiedzie się, gdy przydzielone siły (wyposażone w nowoczesny sprzęt ochronny i elektroniczny) będą skutecznie zarządzanie i kierowane. Twierdzenie to pozostaje aktualne, a potwierdzają to zmiany w dziedzinie organizacji i wyposażenia pododdziałów ochronnych (wartowniczych i doposażenie patroli) oraz struktura komórki bezpieczeństwa. Działania w terenie wybitnie niesprzyjającym z przeciwnikiem nieprzewidywalnym i niewidzialnym, czyli działania poniżej progu wojny muszą być realizowane z użyciem nowoczesnego systemu zabezpieczeń życia ludzkiego. Przekonania niektórych teoretyków, że systemy obrony elektronicznej są zbyteczne w działaniach wielonarodowych szczególnie, gdy przeciwnik przedstawia niski potencjał wojskowy, bowiem sama liczba sił już odstrasza wroga, nie znajduje uzasadnienia i w kontekście wyniesionych doświadczeń oraz nabytej wiedzy jest niezasadna. Z podobną oceną zespół autorski spotkał się w stosunku do ochrony fizycznej, szczególnie w opiniach oficerów w czasie trwania ostatnich kadencji (przy dość znacznym spokoju). W krajach takich, jak Irak czy Afganistan nie można sobie pozwolić na chwilę słabości. Przeciwnik natychmiast ją wykorzysta, dlatego utrzymywanie bezpieczeństwa do końca powinno być wysokie.

Wyniki badań pozwalają na konkluzję, iż pożądany system bezpieczeństwa fizycznego i elektronicznego (traktowany jako podsystemy) sił wielonarodowych musi zapewnić w każdym rodzaju operacji wielonarodowych skuteczną ochroną i obronę wojsk wykonujących zadania i odpoczywających w bazie. Jednocześnie, aby podsystemy fizyczny i elektroniczny mogły sprawnie działać muszą być odpowiednio zarządzane i kierowane. Każdorazowo komórka bezpieczeństwa musi posiadać uprawnienia do koordynowania działań wszystkich podległych pododdziałów ochrony. Dopiero wówczas osiągniemy właściwy poziom bezpieczeństwa.

Zespół autorski zakłada, że w działaniach wielonarodowych komórka bezpieczeństwa powinna zapewnić realizację następujących funkcji:

- Zarządzanie podległymi podsystemami ochrony i obrony na czas operacji wielonarodowej
- Oceny informacji o zgromadzonych i napływających danych dotyczących zagrożenia dla wojsk w czasie patrolu i wojsk w bazie;
- Oceny informacji uzyskanych z podsystemów ochrony i obrony na potrzeby środków rażenia ogniowego i elektronicznego,
- Koordynacyjnej użycia sił delegowanych do systemu ochrony fizycznej i obrony elektronicznej oraz koordynowania zadań pomiędzy komórkami J2, J3, J5 i J6,

- Kierowania bezpośrednio działaniami w trakcie ataku na bazę lub konwój,
- Kontrolą dotyczącą sprawdzania gotowości baz do odparcia ataku.

Potwierdzona została teza, iż spełnienie surowych wymogów bezpieczeństwa nakłada na organizatorów bardzo duże wymagania organizacyjne, techniczne i finansowe. Jednocześnie organ dowodzący musi posiadać najnowszy sprzęt ochronny lub posiadać możliwość zakupu takiego sprzętu. Aktualnie w czasie pokoju system ochrony koszar to gównie płot żelbetonowy lub z siatki, zwieńczony drutem kolczastym i kilka posterunków wartowniczych. Rzadziej spotyka się system monitoringu kamerami czy bariery mikrofalowe. Takie zabezpieczenia gwarantują bezpieczeństwo w kraju przy stabilnej sytuacji natomiast w kraju objętym jeszcze do niedawna działaniami bojowymi takie zabezpieczenia nie wystarczają.

W ramach dalszych badań hipoteza została poddana weryfikacji, mającej na celu jej ostateczne uzasadnienie i sprawdzenie. Główną problematykę badań zespół autorski poddał weryfikacji podczas spotkań z ekspertami oraz uczestnictwa w ćwiczeniach dowódczo sztabowych.

W końcowym etapie badań dokonano podsumowania wyników badań, ich uogólnienia i syntezy. Autorzy przyjęli wiarygodną interpretację rozwiązania problemu badawczego przedstawioną w pisarskim opracowaniu wyników badań i tym samym stworzyli bazę kontynuacji badań w kolejnych etapach dotyczących bezpieczeństwa wojsk w operacji wielonarodowej.

Autorzy zamierzają wyniki badań opublikować w opracowaniu książkowym i prasie specjalistycznej, poddać weryfikacji na konferencjach naukowych, sympozjach oraz seminariach naukowych a także wykorzystać do opracowania materiałów dydaktycznych na potrzeby AON i innych placówek dydaktycznych Sił Zbrojnych RP, szczególnie Dowództwa Wojsk Lądowych.

Praca badawcza zawiera, więc wyniki badań w zakresie założeń teoretycznych uwarunkowań zagrożenia bezpieczeństwa fizycznego i elektronicznego w operacjach wielonarodowych, organizowania komórki bezpieczeństwa. W pracy uwzględnione są wnioski z doświadczeń wielu oficerów przebywających na misji, w tym własne, oraz wyniki prowadzonych badań. Praca składa się z wprowadzenia czterech rozdziałów merytorycznych, efektów poznania, zakończenia, wykazu bibliograficznego i załączników.

Prezentując wyniki badań zespół autorski uznał, że prace powinny rozpoczynać się jednoznacznym określeniem pojęć i definicji, aby jednoznacznie posługiwać się wszystkim określeniami. Następnie dokonano głębokiej i kompletnej identyfikacji istoty działań

wielonarodowych i charakterystyki struktur organizacyjnych realizujących zadania w ramach działań wielonarodowych. Stąd też, po części wprowadzającej w genezę przedmiotu procesu i części metodologicznej, opisującej przebieg badań, nastąpiła analiza struktury poszczególnych elementów składowych. Logicznym następstwem w dalszej części pracy jest przedstawienie uwarunkowań bezpieczeństwa w operacjach wielonarodowych (rozdział drugi), a następnie analiza uwarunkowań bezpieczeństwa fizycznego (rozdział trzeci) i elektronicznego (rozdziała czwarty) pododdziałów delegowanych do operacji wielonarodowych. W stosunku do pożądanego kształtu przyszłościowego systemu bezpieczeństwa przedstawiono modelową strukturę systemu oraz modelową komórkę bezpieczeństwa możliwą do wykorzystania w operacjach wielonarodowych (rozdział piąty). Dopełnieniem przedstawionych rozwiązań są wnioski ogólne prezentujące wyniki badań.

2. BEZPIECZEŃSTWO DZIAŁAŃ DOWÓDZTWA I WOJSK W OPERACJI WIELONARODOWEJ

Każda operacja wielonarodowa jest i będzie inna, niepowtarzalna. Odmienność dotyczy również zagrożeń, które są zazwyczaj specyficzne dla działań, rodzaju i charakteru operacji, obszaru geograficznego oraz składu sił wielonarodowych (określonych narodowości biorących udział w operacji wielonarodowej). Charakter zagrożeń, ich intensywność, wzajemne powiązania oraz rodzaj będą warunkowały poczucie bezpieczeństwa zarówno wojsk jak i dowództw biorących udział w operacjach wielonarodowych.

W dokumentach doktrynalnych bezpieczeństwo operacji (działań) definiowane jest jako: zespół przedsięwzięć zapewniających ukrycie stanu i położenia sił własnych oraz planów operacji w celu ograniczenia dostępu przeciwnikowi do informacji dotyczących możliwości i zamiaru użycia sił własnych[1].

W ramach przedsięwzięć bezpieczeństwa operacji wymieniane są działania bierne i aktywne. W ramach działań biernych wskazuje się:

1. bezpośrednią ochronę personelu;
2. ograniczenie swobody ruchu i kontaktów;
3. ochronę dokumentów niejawnych;
4. stosowanie środków technicznych (kamuflaży, osłon, barier, zapór, min itp.).

Natomiast w ramach działań aktywnych wskazuje się:

1. zakłócanie i zwalczanie sił i środków rozpoznania powietrznego, naziemnego i morskiego przeciwnika;
2. przeciwdziałanie elektroniczne realizowane przeciwko systemom łączności i dowodzenia przeciwnika;
3. wprowadzanie przeciwnika w błąd (w ramach dezinformacji) oraz działania informacyjne i psychologiczne

Konstatując, zagrożenia dla operacji wielonarodowych są składową wielu czynników zewnętrznych, należy więc wnioskować, że przedsięwzięcia w zakresie bezpieczeństwa będą pochodną istniejących i dających się przewidzieć w przyszłości zagrożeń.

[1] Doktryna narodowa operacje połączone, MON, Warszawa 2002, s. 6-26.

2.1. Podstawowe pojęcia bezpieczeństwa fizycznego i zagrożeń elektronicznych

Analizując problematykę bezpieczeństwa fizycznego rozpoczniemy od wyjaśnienia znaczenia podstawowych terminów związanych z desygnatem pojęcia bezpieczeństwa.

Zgodnie z zapisami zawartymi w Słowniku terminów i definicji NATO, „bezpieczeństwo, to stan osiągany, gdy określona informacja, sprzęt, personel, działania i urządzenia są zabezpieczone przed szpiegostwem, sabotażem, dywersją i terroryzmem, jak również przed utratą lub ujawnieniem tajemnicy"[2]. Analogicznie, „bezpieczeństwo fizyczne */ang. physical security/*, to część systemu bezpieczeństwa, która związana jest z fizycznymi zabezpieczeniami przeznaczonymi dla personelu ochraniającego, nie dopuszcza osób nieupoważnionych do sprzętu, instalacji, materiałów i dokumentów oraz chroni je przed szpiegostwem, sabotażem, zniszczeniem i kradzieżą"[3]. Konkludując, bezpieczeństwo fizyczne oznacza ochronę obiektów, osób, materiałów i dokumentów przed dostępem fizycznym, podglądem, podsłuchem lub inną formą penetracji wraz z procedurami dopuszczającymi i sprawdzającymi.

Zgodnie zapisami obowiązującej w Wojsku Polskim instrukcji Rozpoznanie wojskowe, bezpieczeństwo fizyczne obok bezpieczeństwa osobowego, przedsięwzięć organizacyjnych w zakresie bezpieczeństwa i bezpieczeństwa informacji/systemów informatycznych, jest jedną z kategorii określających zabezpieczenie ochronne. Zabezpieczenie ochronne jest to zorganizowany system przedsięwzięć obronnych ustanowiony i utrzymywany na wszystkich poziomach dowodzenia, mający na celu osiągnięcie i utrzymanie wymaganego stopnia bezpieczeństwa.[4]

Bezpieczeństwo wojsk, w czasie działań bojowych nabiera szczególnego znaczenia w przypadku, gdy wykonują one zadania poza granicami kraju w ramach wielonarodowych grup zadaniowych działających w ramach operacji reagowania kryzysowego.[5]

Ochrona to zorganizowany system środków ochronnych ustanowiony i utrzymywany na wszystkich szczeblach dowodzenia w celu osiągnięcia zamierzonego stanu bezpieczeństwa.[6]

W doktrynie prowadzenia operacji połączonych (DD/3) elementy dotyczące ochrony wojsk zamieszczone są w rozdziałach 4 i 5 dotyczących bezpieczeństwa operacji w okresie rozwijania sił oraz w toku jej prowadzenia. Pod pojęciem ochrona wojsk rozumie się proces

---

[2] *Słownik terminów i definicji NATO, AAP-6 (2005) PL*, MON 2005, s. 315.
[3] *Słownik terminów ...*, wyd. cyt., s.269.
[4] *Rozpoznanie wojskowe,* Szt. Gen. WP, Warszawa 2001, s. 46.
[5] *Tamże*, s. 48.
[6] *Bi – S.C. Force Protection Directive*, 80 –25 Aneks B, Norfolk 2003, p. 5, s. B – 3.

kontrolowania ryzyka w oparciu o obiektywną ocenę zagrożenia i wynikający z niej dobór odpowiednich środków zapobiegawczych.

Ochrona wojsk jest zbiorem przedsięwzięć, których nie można traktować oddzielnie lub w oderwaniu od niej. Obiektywna i dokładna ocena faktycznych i możliwych zagrożeń, stanowi podstawę pozwalającą zaplanować pasywne lub aktywne środki ochrony wojsk.[7]

Ochrona wojsk /*ang. Force Protection*/, to wszelkie przedsięwzięcia i środki podejmowane w celu zminimalizowania podatności siły żywej, urządzeń, sprzętu i podejmowanych działań na jakiekolwiek zagrożenia, w celu zachowania swobody działania i zdolności operacyjnej wojsk.[8]

Zgodnie z definicją zawartą w amerykańskim słowniku terminów militarnych, pod pojęciem **Force Protection** rozumiane są działania mające na celu zapobieżenie lub zmniejszenie oddziaływania przeciwnika wobec personelu Ministerstwa Obrony (włączając członków rodzin), zasobów, obiektów lub informacji. Działania te ochraniają posiadany potencjał wojsk, tak aby mógł on być użyty we właściwym czasie i miejscu, w celu umożliwienia efektywnego użycia siły przy jednoczesnym ograniczaniu możliwości przeciwnika. Force Protection nie obejmuje działań zmierzających do pokonania przeciwnika lub ochrony przed wypadkami, pogodą lub chorobami.[9]

Ochrona sił i środków oznacza natomiast realizowanie szeregu przedsięwzięć w celu niedopuszczenia do powstania niepotrzebnych strat własnych w ludziach i sprzęcie (szczególnie w wyniku samoostrzału) oraz wśród ludności cywilnej. Od dowódcy sił wielonarodowych wymaga się podjęcia wszelkich kroków w celu ochrony żołnierzy, dokumentów i wyposażenia przed różnymi zagrożeniami, poczynając od szeroko zakrojonych operacji bojowych przeciwnika, a kończąc na aktach sabotażu i akcjach terrorystycznych o ograniczonym zasięgu.

W innym ujęciu pod terminem ochrona wojsk rozumiane są wszystkie środki i sposoby, użyte w celu minimalizowania wrażliwości personelu, urządzeń, wyposażenia i działań na wszelkie zagrożenia i sytuacje, w celu zachowania swobody działania i skuteczności wojsk.[10]

Zgodnie z obowiązującą od 01 grudnia 2008r. Instrukcją o ochronie obiektów wojskowych, ochrona obiektów wojskowych stanowi zespół przedsięwzięć uniemożliwiających nielegalne przedostanie się osób, pojazdów, statków pływających lub

---

[7] *Doktryna prowadzenia operacji połączonych (DD/3)*, Szt. Gen. WP, Warszawa 2004, s.81.
[8] *Słownik terminów ...*, wyd. cyt., s. 161.
[9] *Słownik terminów militarnych,* Departament Obrony *USA, 2005.*
[10] *Bi-SC Functional Planning Guide for Force Protection (Initial Draft),* Norfolk 2004, s. 8.

powietrznych, a także wniesienie sprzętu lub materiałów niebezpiecznych na teren chronionych obiektów wojskowych i zabezpieczających znajdujące się tam mienie przed jego kradzieżą, zniszczeniem lub uszkodzeniem.[11]

Instrukcja ta zawiera również definicję ochrony fizycznej. Zgodnie z przytaczaną instrukcją - ochrona fizyczna, to zespół przedsięwzięć ochronnych realizowanych przez warty i służby wewnętrzne lub garnizonowe, oddziały wart cywilnych, specjalistyczne uzbrojone formacje ochronne przedsiębiorców, portierów i dozorców, a także przez psy wartownicze. Ochrona fizyczna obiektów zagrożonych atakami terrorystycznymi wzmacniana jest w okresie wzrostu tych zagrożeń siłami Żandarmerii Wojskowej (ŻW).

Ochrona techniczna stanowi zespół przedsięwzięć ochronnych realizowanych przy wykorzystaniu technicznych środków wspomagających ochronę fizyczną.[12]

W celu właściwej ochrony obiektu wojskowego, jakim niewątpliwie jest baza wojskowa, należy z poszczególnych przedsięwzięć zbudować system.

System jest pojęciem desygnującym pewną całość tworzoną przez określony zbiór obiektów (elementów) i powiązań (relacji) między nimi, rozpatrywaną z określonego punku widzenia (aspektu badań).[13]

Innymi słowy system, to jakikolwiek obiekt fizyczny lub abstrakcyjny, w którym można wyróżnić jakieś wzajemnie powiązane dla obserwatora elementy. W tym sensie podział czegoś na systemy jest względny i zależy od tego kto, przy pomocy czego i do czego poklasyfikował jakiś zbiór na systemy. Dlatego też elementy jednego systemu mogą stanowić składniki innych systemów.[14]

Zgodnie z definicją zawartą w Instrukcji o ochronie obiektów wojskowych, system ochrony obiektów, to zespół przedsięwzięć organizacyjno – technicznych, obejmujących ochronę fizyczną i techniczną obiektów.[15]

Obszar chroniony /*ang. secure area*/, to wyznaczone miejsce lub rejon, w którym siły NATO lub dowodzone przez NATO przyjmują określony poziom odpowiedzialności za osoby i obiekty oraz mogą nakładać ograniczenia w ruchu i przemieszczaniu się.[16]

Dokonując diagnozy zagrożeń elektronicznych systemu bezpieczeństwa wojsk w operacjach wielonarodowych należy wyjaśnić ponadto pojęcie zagrożenie. Pojęcie

---

[11] *Instrukcja o ochronie obiektów wojskowych*, OIN 3/2008, Warszawa 2008, s. 7.
[12] *Tamże*, s. 7.
[13] Sienkiewicz P., *Podstawy teorii systemów*, Warszawa 1993, s. 16.
[14] *http://pl.wikipedia.org/wiki/System*
[15] *Instrukcja o ochronie ...*, wyd. cyt., s. 10.
[16] *Słownik terminów i definicji NATO,* wyd. cyt., s. 315.

zagrożenia jest przez każdego człowieka intuicyjnie zrozumiałe, brak jest jednak powszechnej zgodności stanowisk w jego interpretacji. W wyniku analizy literatury stwierdzić należy, że nie jest ono jednoznacznie interpretowane. Ogólnie można zagrożenie zinterpretować jako sytuacja lub stan, które komuś czymś zagrażają lub w którym ktoś czuje się zagrożony[17]. W wąskim znaczeniu zagrożenie ma miejsce wtedy, gdy „(...) w człowieku rodzi się obawa o utratę wysoko cenionych wartości, z własnym życiem na pierwszym miejscu"[18], rozumiane jest jako sytuacja uświadamiana przez podmiot. W szerszym znaczeniu „(...) zagrożenia obejmują także sytuacje, które nie są przez podmiot uświadamiane" [19].

W grupie zagrożeń wyróżnia się zagrożenia wewnętrzne i zewnętrzne.[20] Do zagrożeń zewnętrznych zalicza się zagrożenia, których źródłem są: przyroda, wytwory ludzkiej cywilizacji, inny człowiek lub ludzie.

Wśród zagrożeń wewnętrznych wyróżnia się: samobójstwa, skłonność do autoagresji, uzależnienia, choroby i zaburzenia psychiczne, oraz stres (zwłaszcza silny i przedłużający się - chroniczny). Można wskazać zależności zagrożeń wewnętrznych od zagrożeń zewnętrznych i odwrotnie, co może utrudniać jednoznaczną ich klasyfikację.

Oddzielne miejsce w analizie skutków zagrożeń zajmują sytuacje kumulowania zagrożeń, co ma miejsce w działaniach wielonarodowych. W sytuacji takiej negatywne oddziaływanie ma źródło nie w jednej kategorii zagrożeń, ale w dwu lub więcej. W zależności od rodzaju i ilości zagrożeń, skutki wywołane ulegają intensyfikacji. Sytuacja taka rodzi zwiększone wymagania wobec profilaktyki występowania zagrożeń oraz sposobów przeciwdziałania ich skutkom.

Poczucie zagrożenia wpływa na zaspokojenie potrzeby bezpieczeństwa, im jest wyższe, tym zaspokojenie potrzeby bezpieczeństwa jest mniejsze i odwrotnie. Poczucie zagrożenia wzrasta, gdy występujące zagrożenia są w sposób nieuzasadniony, nadmiernie, nazbyt często traktowane jako osobiste (odnoszące się do reagującej jednostki).

Świadomość zagrożeń stanowi istotny czynnik działań zapobiegawczych ukierunkowanych na uniknięcie bądź redukcję zagrożeń. Świadomość jest definiowana jako „(...) wewnętrzny, subiektywny stan zdawania sobie sprawy z czegoś, stan czuwania"[21]. Świadomość zagrożeń jest istotnym elementem profilaktyki zagrożeń, której zadaniem jest nie dopuścić do zagrożenia. Zakłada nie tylko utożsamienie jej z aktywnością poznawczą,

---

[17] *Uniwersalny słownik języka polskiego*, Wydawnictwo Naukowe PWN, Warszawa 2003, T. 5, s. 460.
[18] B. Hołyst, *Wiktymologia*, Wydawnictwo Prawnicze LexisNexis, Warszawa 1997, s. 64-65.
[19] *Tamże*, s. 65.
[20] *Tamże*, s. 65.
[21] A.S. Reber, *Słownik psychologii*, Wydawnictwo Naukowe SCHOLAR, Warszawa 2000, s. 740.

której wynikiem jest prawidłowa identyfikacja zagrożeń, ale również zaangażowanie w kierunku odpowiednio wczesnej ich identyfikacji, prawidłowej oceny skutków i reakcji na nie. W tym zakresie istotne jest adekwatne dopasowanie środków przeciwdziałania do rodzaju i rozmiarów zagrożenia.

Świadomość zagrożeń polepsza zarówno ich percepcję jakościową (identyfikację zagrożenia) jak również ilościową (identyfikację rozmiarów zagrożenia: *jak dużo?*, nasilenia: *jak bardzo?* i bezpośredniości: *jak blisko?*). Należy szczególną uwagę zwrócić na potrzebę zadaniowej percepcji zagrożeń. Jest ona możliwa przy pełnym uświadomieniu przyczyn zagrożeń, ich przejawów oraz sposobów przeciwdziałania. Istotna rola świadomości w profilaktyce zagrożeń polega również na uruchomieniu twórczej inicjatywy w kierunku poznania zagrożeń, ich źródeł i możliwych sposobów przeciwdziałania.

2.2. Istota działań wielonarodowych

Po rozpadzie dwubiegunowego świata, scenariusz konfliktu do którego sposobił się Sojusz Północnoatlantycki zaczął tracić na aktualności. Ciągłe redukcje sił zbrojnych poszczególnych państw, które miały miejsce w latach 90-tych XX wieku sprawiły podjęcie działań koncepcyjnych przeorientowania zadań, do których Sojusz miał być przygotowany.

Powstanie inicjatywy Partnerstwa dla Pokoju (PdP), wzrost znaczenia tożsamości europejskiej oraz wydarzenia w byłej Jugosławii doprowadziły do identyfikacji, a następnie dopracowania koncepcji wielonarodowych sił połączonych (*Combined Joint Task Force Consept – CJTF Koncept*[22]). Współcześnie działania wielonarodowe (*Combined*) realizowane są w zasadzie w formie wielonarodowych działań połączonych (*Combined Joint Operations*). Charakteryzują się one tym, iż prowadzą je co najmniej dwa rodzaje sił zbrojnych z co najmniej dwóch państw pod wspólnym dowództwem. Jako że *działania połączone* i *operacje połączone* to dwa znaczeniowo różne terminy, nasuwa się pytanie, czy mogą one występować zamiennie. Główną przyczyną problemu jest tłumaczenie na język polski terminu *joint operation.* Tłumaczenie terminu *joint* nie stanowi problemu i znaczy połączone, o tyle termin *operation* może być tłumaczony różnie. W znaczeniu ogólnym oznacza on „działanie", w szczegółowym „operację", natomiast w terminologii technicznej oznacza „obsługę". Nie

[22] J. Kręcikij, M. Trzoda, J. Trembecki, *Założenia teoretyczne wielonarodowej operacji połączonej,* AON, Warszawa 2000, s. 13.

mniej jednak nasuwające się w pierwszej chwili rozwiązanie problemu skłania zespół autorski do przyjęcia tezy, że działania połączone są częścią składową operacji połączonej. Można również założyć, iż są to terminy równoważne[23]. Jednakże porównując polskie rozumienie terminu *operacja* z sojuszniczym, zawartymi w *Joint Publications* dochodzi się do zgoła odmiennych wniosków:

„Operacja- akcja wojskowa lub wykonywanie wojskowych misji strategicznych, taktycznych, szkoleniowych, zabezpieczających lub administracyjnych; proces prowadzenia walki, włącznie z przemieszczeniem, dostawami zaopatrzenia, atakiem, obroną i ruchem potrzebnymi do osiągnięcia celów bitwy lub kampanii[24].

„Operacja to zespół walk, bitew, uderzeń ogniowych i manewrów toczonych lub wykonywanych na lądzie, w powietrzu i na morzu przez związki operacyjne (zgrupowania operacyjne) różnych rodzajów wojsk i sił zbrojnych, połączonych wspólną myślą przewodnią, prowadzonych pod jednym kierownictwem dla doprowadzenia do osiągnięcia celu operacji (bitwy) lub celu strategicznego" [25].

„Operacja połączona to operacja, w której biorą udział komponenty co najmniej dwóch rodzajów sił zbrojnych kierowanych przez jednego dowódcę" [26].

„Operacja połączona to całokształt przedsięwzięć militarnych i niemilitarnych planowanych przez kierownictwo strategiczne i realizowanych przez jednolite dowództwo operacyjne dla osiągnięcia celu strategicznego (uzyskania rozstrzygnięcia). W tego typu operacji biorą udział komponenty co najmniej dwóch rodzajów sił zbrojnych. Mogą w niej uczestniczyć również instytucje i organizacje pozamilitarne"[27].

Biorąc powyższe pod uwagę, w kontekście uwarunkowań współczesnych konfliktów zbrojnych, jak również możliwości naszych Sił Zbrojnych, termin *działania połączone* jako tłumaczenie angielskiego *joint operations* jest bardziej adekwatny. Nie zawęża on rozważań nad problematyką dotyczącą zasad dowodzenia do szczebla operacyjnego i strategicznego. Będąc pojęciem szerszym i obejmując *operacje połączone* znacznie ułatwia określenie i zunifikowanie zasad dowodzenia jako ogólnych praw rządzących procesem dowodzenia. Reasumując, termin *joint operations* w zależności od kontekstu, w jakim występuje, oraz obszaru znaczeniowego, może oznaczać: wspólne działania (jako procesy w obszarze

---

[23] R. Kwećka, *Działania czy operacje połączone*, [w:] Myśl Wojskowa nr 3, MON, Warszawa, 2003, s. 124.
[24] AAP-6 (2005) Słownik Terminów i definicji NATO (Nato glossary of terms and definitions) s. 256.
[25] *Leksykon Wiedzy Wojskowej*, MON, Warszawa, 1979.
[26] M. Wiatr, *Między strategią a taktyką*, Wydawnictwo Adam Marszałek, Toruń, 2000. s. 138.
[27] *Doktryna narodowe operacje połączone OP/01*, MON, Warszawa, 2002, s. 1-1.

niemilitarnym lub na styku procesów w obszarze militarnym i niemilitarnym); wspólne akcje; wspólne operacje - w obszarze militarnym. W obszarze niemilitarnym lub na styku procesów militarnych i niemilitarnych termin ten może oznaczać działania połączone. Natomiast w obszarze militarnym może oznaczać operacje połączone[28].

Istotą działań wielonarodowych jest zasada dobrowolności udziału elementów sił zbrojnych z różnych krajów działających razem w celu wykonania określonego zadania. Ta synchronizacja wysiłków komponentów rodzajów sił zbrojnych różnych państw we wspólnej realizacji zadań wymagających wykorzystania ich zróżnicowanych możliwości, ma doprowadzić do powstania efektu synergiczności. Wskazuje on, że skutki połączonych działań są większe niż suma skutków działania rodzajów sił zbrojnych każdego państwa z osobna[29].

Podstawowym dokumentem normatywnym, zawierającym założenia wspólnych działań operacyjnych połączonych sił sojuszniczych, jak również i państw spoza Sojuszu Północnoatlantyckiego, jest „Sojusznicza doktryna działań połączonych AJP-01(A)" (*Allied Joint Operations Doctrine AJP-01*)[30]. Zawarte są w niej zapisy dotyczące zasad prowadzenia wspólnych działań (operacji) państw członków NATO z państwami spoza Sojuszu w ramach zgrupowań wielonarodowych sił połączonych. Doktryna charakteryzuje i wyjaśnia podstawowe funkcje i przedsięwzięcia związane z operacjami sił wielonarodowych, włączając w to również operacje militarne inne niż wojna.

Kolejnym dokumentem poruszającym problematykę działań wielonarodowych jest „Doktryna Narodowa Operacje Połączone OP/01". Znajduje się w niej zapis, iż operacje wielonarodowe „prowadzone są z udziałem wojsk sojuszniczych oraz partnerskich", które uczestniczą w tego typu działaniach na zasadzie dobrowolności[31]. W nomenklaturze sojuszniczej identyfikowane one są jako operacje reagowania kryzysowego oraz jako operacje spoza Artykułu 5 Traktatu Waszyngtońskiego. Istnieje także wariant „wielonarodowej operacji połączonej", w której zaangażowane są tylko komponenty sił zbrojnych państw należących do Sojuszu. Operacja taka nosi nazwę „sojuszniczej operacji połączonej" (Allied Joint Operations)[32]. Są to więc działania, w których biorą udział elementy co najmniej dwóch

---

[28] R. Kwećka, *Działania czy operacje połączo*ne, [w:] Myśl Wojskowa nr 3, MON, Warszawa, 2003, s. 128.
[29] J. Zieliński, (red.), *Teoretyczne podstawy operacji połączonych p.k. „Podstawy"*, AON, Warszawa, 1991, s. 21.
[30] *Allied Joint Operations Doctrine AJP-01 (A),* MAS, September 1998.
[31] Por. Doktryna narodowa operacje połączone OP/01, MON, Warszawa 2002, s. 4-1.
[32] J. Kręcikij, *Organizacja dowodzenia w operacjach wielonarodowych*, praca naukowo-badawcza pk. Koalicja, AON, Warszawa 2007, s. 17.

rodzajów sił zbrojnych z co najmniej dwóch państw NATO. Klasyfikowane są jako operacje wojenne w ramach obrony kolektywnej jednego z państw NATO lub całego Sojuszu oraz jako operacje reagowania kryzysowego wynikające zarówno z Artykułu 5 Traktatu Waszyngtońskiego jak i spoza tego artykułu.

Celem wielonarodowej operacji połączonej w ramach Artykułu 5 jest zniszczenie sił przeciwnika i załamanie jego woli kontynuowania jego dalszych działań. Natomiast celem operacji połączonej poza Artykułem 5 jest wymuszenie na stronach konfliktu zaprzestania działań zbrojnych, niedopuszczenie do przekształcenia się kryzysu w konflikt zbrojny poprzez nakłonienie stron do rokowań pokojowych.

Zasadniczą rolą sił militarnych Sojuszu jest ochrona pokoju i zagwarantowanie terytorialnej integralności, niepodległości i bezpieczeństwa państwom członkowskim. Siły Sojuszu muszą być zdolne do skutecznego odstraszania i obrony, utrzymania i przywracania terytorialnej integralności sojuszniczych państw, a w razie konfliktu, do szybkiego zakończenia wojny poprzez spowodowanie, by agresor rozważył ponownie swoje decyzje, przerwał działania ofensywne i wycofał się[33]. Cele strategiczne operacji sojuszniczych NATO wynikają głównie z ogólnych celów polityczno – militarnych (zbieżnych z celami polityki zagranicznej państw członkowskich) oraz stanu zagrożeń dla bezpieczeństwa całego Sojuszu i jego członków. Są one jednocześnie spodziewanym stanem po zakończeniu działań. Skuteczność sił sojuszniczych w czasie pokoju, kryzysu i wojny zależy od zdolności i możliwości wspólnego działania. Sojusznicze operacje powinny być przygotowane, planowane i prowadzone w sposób, który stwarza warunki do najlepszego wykorzystania sił i środków uczestniczących państw oraz sił przeznaczonych do operacji. Zgodnie z dokumentami normatywnymi tego rodzaju operacja będzie z reguły prowadzona w trzech fazach:

- Faza początkowa (*Initial*), trwająca od decyzji Rady Północnoatlantyckiej do wprowadzenia do rejonu operacji sił głównych. W fazie tej z uwagi na prawdopodobne narastanie intensywności konfliktu od wymiaru regionalnego (w ramach lub spoza art.5) do konfliktu na dużą skalę, użyte zostaną w pierwszej kolejności „Siły Zdolne do Przerzutu" (*Deployable Forces – DF*);
- Faza podtrzymywania (*Sustainment*), w której prowadzi się połączone wielonarodowe działania do osiągnięcia celu operacji. W tej fazie, oprócz sił użytych w fazie początkowej, użyte zostaną siły główne, tzn. „Siły Miejscowe". Będą to „Siły

[33] *Allied Joint Doctrine AJP-01(B)*, Ratification draft 1, NATO 2000, s. 1-2.

Zarezerwowane dla NATO" (*NATO Enmarked Forces*), lub inne siły dla NATO (*Other Forces for NATO*) o wydłużonym czasie osiągania gotowości bojowej (*Long Term Build-up Forces – LTBF*). Wymaga to posiadania przez państwo zdolności do rozwijania i uzupełniania potencjału w dłuższym czasie, stosownie do prawdopodobnego czasu ostrzeżenia i reagowania na zagrożenie Sojuszu na dużą skalę;

–Faza przejścia (*Transition*), w której nie przewiduje się już działań o wysokiej intensywności, a obecność wojskowa konieczna jest dla stabilizacji sytuacji[34].

Zgodnie z zapisami zawartymi w dokumentach normatywnych Sojuszu Północnoatlantyckiego, identyfikacji rodzaju sił ze względu na ich skład dokonuje się następująco[35]:

- Joint Forces (JF) - Siły Połączone, zgrupowania składające się z elementów dwóch lub więcej rodzajów sił zbrojnych tego samego państwa;
- Allied Forces (AF) - Siły Sojusznicze, zgrupowania składające się z elementów dwóch lub więcej państw członków NATO;
- Combined Forces (CF) - Siły Wielonarodowe, rozumiane jako zgrupowania składające się z elementów dwóch lub więcej rodzajów sił zbrojnych i dwóch lub więcej państw - nie tylko członków NATO;
- Multinational Forces (MF) - Siły Międzynarodowe, zgrupowania składające się z elementów dwóch lub więcej państw nie będących członkami NATO[36].

Z połączenia poszczególnych terminów tworzy się nazwy zgrupowań odpowiadające ich faktycznemu składowi. Zgodnie z tą zasadą, zgrupowanie sił składające się z elementów więcej niż jednego rodzaju sil zbrojnych i więcej niż jednego państwa (ale członka NATO), określa się terminem Sojusznicze Siły Połączone - Allied Joint Forces (AJF). Natomiast zgrupowanie sił składające się z elementów więcej niż jednego rodzaju sił zbrojnych i więcej niż jednego państwa (w tym także z poza NATO) nazywa się Wielonarodowymi Siłami Połączonymi - Combined Joint Forces (CJF). Termin Wielonarodowe Połączone Siły Zadaniowe - Combined Joint Task Forces (CJTF), zarezerwowany jest dla wspomnianej wcześniej koncepcji wielonarodowych sił połączonych, wykreowanej przez Sojusz Północnoatlantycki.

---

[34] Doktryna narodowa operacje połączone ..., wyd. cyt., s. 3-1.

[35] Kręcikij J., *Wybrane problemy kierowania zgrupowaniami wielonarodowych sił połączonych*, AON, Warszawa 2003, s.35.

[36] *AAP-6(2003), NATO Glossary of Terms and Definitions*, MAS, Brussels, 2003, s. 1-8.

Kontyngenty w ramach połączonych sił zadaniowych grupuje się odpowiednio do wymogów operacyjnych według kryteriów funkcjonalnych, narodowych lub organizacyjnych. Toteż siły prowadzące operacje połączone mogą składać się z komponentów narodowych, komponentów rodzajów sił zbrojnych lub komponentów funkcjonalnych[37]. W komponencie narodowym *(National Component)* skupione są wszystkie siły danego państwa przeznaczone do uczestnictwa w operacji. Podlegają one narodowemu dowódcy komponentu. Komponent rodzaju sił zbrojnych *(Service Component)* składa się z wojsk jednego rodzaju sił zbrojnych jednego lub kilku państw. Odpowiednio do potrzeb mogą być tworzone komponenty sił lądowych *(Army Component)*, sił powietrznych *(Air Force Component)* i sił morskich *(Navy Component)*. Mogą otrzymać zadanie prowadzenia samodzielnych działań. Komponent funkcjonalny *(Functional Component)* składać się może z sił o podobnych lub uzupełniających się możliwościach. Toteż w zależności od charakteru zadań tworzyć można różne komponenty funkcjonalne kierowane przez dowódcę komponentu. Dowódca taki otrzymuje od dowódcy sił połączonych zadanie, które realizuje na korzyść całych sił zadaniowych. Komponenty funkcjonalne stanowią najbardziej typowe elementy strukturalne połączonych sił zadaniowych.

Typowe siły zadaniowe składają się z komponentu lądowego sił połączonych (*Joint Force Land Component - JFLC*), komponentu powietrznego sił połączonych (*Joint Force Air Component - JFAC*) oraz komponentu morskiego sił połączonych (*Joint Force Maritime Component – JFMC*). Odpowiednio do potrzeb operacyjnych, ale w zależności od charakteru operacji i wielkości sił, tworzone mogą być także komponenty specjalne, takie jak: komponent tyłowy sił połączonych (*Joint Force Rear Area Component – JFRAC*), komponent działań specjalnych (*Joint Force Special Operations Component – JFSOC*) oraz komponent działań psychologicznych (*Joint Force Psychological Operations Component – JFPOC*)[38].

Współpraca wielonarodowa państw w sferze militarnej do realizacji określonych celów może przybierać charakter koalicji albo sojuszu. Koalicja zazwyczaj dotyczy wspólnej realizacji ściśle określonych zadań w ograniczonym czasie. Tworzy się ją zazwyczaj doraźnie w celu rozwiązania określonych problemów i osiągnięcia tym samym zakładanych celów. Po ich osiągnięciu jest z reguły rozwiązywana. Kiedy państwa realizują wspólne długoterminowe cele zawarte w traktatach, taka współpraca nosi nazwę sojuszu. Toteż sojusz jest jakby

---

[37] Tomaszewski A., Kaczmarek W., Wiatr M., *Wojska lądowe w operacjach połączonych,* praca naukowo-badawcza p.k. Operacje połączone, AON, Warszawa, 2003, s. 26.
[38] Tomaszewski A., Kaczmarek W., Wiatr M., *Wojska lądowe w operacjach ...*, wyd. cyt., s. 27.

wyższą formą koalicji ale z inną, tak charakterystyczną dla działań wielonarodowych „dobrowolnością udziału". Sojusz ze swoim formalnym i trwałym charakterem posiada ściśle określone w umowach zasady udziału poszczególnych państw-członków we wspólnych działaniach. Ponadto posiada stałe organy kierowania oraz zasady i procedury podejmowania decyzji o użyciu wspólnych sił.

W działaniach połączonych biorą udział elementy co najmniej dwóch rodzajów sił zbrojnych lub wojsk (które nie należały dotychczas do tej samej struktury) zgodnie z zasadą pełnej integracji. Występują one na wszystkich poziomach organizowania i prowadzenia działań militarnych. Są to działania planowane i realizowane przez jednego głównodowodzącego. Jak już wspominano, wielonarodowa operacje (*Combined Operations*) to działania prowadzone przez siły dwóch lub więcej krajów. Są one prowadzone z udziałem sił zbrojnych państw sojuszniczych oraz wojsk państw partnerskich. Współcześnie wszystkie operacje są połączone ze względu na środowisko osiąganych celów, angażowane siły oraz skuteczność i ekonomiczność działania. Stąd, w każdej operacji występują działania połączone na wszystkich poziomach osiągania jej celów.

Jak wskazuje analiza dokumentów normatywnych dotyczących problematyki działań wielonarodowych, operacje wielonarodowe prowadzone są na podstawie mandatu organizacji międzynarodowych, takich jak Organizacja Narodów Zjednoczonych, Organizacja Bezpieczeństwa i Współpracy w Europie czy Unia Europejska. Celem ich jest osiągnięcie oczekiwanego stanu ujętego w mandacie, którym najczęściej jest: łagodzenie sytuacji kryzysowej, powstrzymanie konfliktu zbrojnego, przywrócenie pokoju i bezpieczeństwa w określonym rejonie świata. Celami pośrednimi zazwyczaj są[39]:

- zmuszenie stron zwaśnionych (stron konfliktu) do zawieszenia broni i rozpoczęcia negocjacji pokojowych;
- zmuszenie stron do przestrzegania ustaleń układu pokojowego;
- ochrona i kontrola tymczasowych granic obszarów niepaństwowych;
- ochrona ludności cywilnej (zwłaszcza osób wypędzonych, prześladowanych i uciekinierów);
- kontrola przepływu ludności, mienia, uzbrojenia przez granice stałe i tymczasowe.

Działania wielonarodowe opierają się na jedności celów. Chociaż może to w określonych sytuacjach sprawiać pewne trudności, wynikające między innymi z różnych interesów narodowych państw, to wspólne sformułowanie celów i zasad działania jest

[39] *Doktryna narodowa ...*, wyd. cyt., rozdział 4.

podstawą każdego sojuszu lub koalicji. Do najważniejszych zasad, warunkujących sukces działań wielonarodowych można zaliczyć:

- celowość działania, współdziałanie i jedność wysiłków;
- elastyczność i ciągłość działania;
- inicjatywę i zaskoczenie;
- wzajemne zaufanie[40].

Mówiąc o celowości działania, współdziałaniu i jedności wysiłków w działaniach wielonarodowych, rozumie się przez to przede wszystkim konieczność jednoznacznego określenia celów działania i zadań poszczególnych uczestników, a także stworzenia warunków do koordynacji realizowanych przedsięwzięć. Elastyczność, to zapewnienie dowódcy swobody działania i możliwości reagowania na sytuacje nieprzewidziane planami. Ciągłość działania, to stworzenie warunków do bezproblemowej realizacji zaplanowanych przedsięwzięć przy ich odpowiednim zabezpieczeniu i wsparciu. Inicjatywa i zaskoczenie umożliwiają dowódcy prowadzenie działań według własnego zamiaru, umożliwiając jednocześnie osiąganie większych efektów przy użyciu stosunkowo małego wysiłku. Wzajemne zaufanie jako warunek niezbędny wspólnych działań, opierać się powinno między innymi we wzajemnym szacunku, wiedzy na temat partnerów, cierpliwości, a także na podtrzymywaniu życzliwych relacji i wzajemnym poszanowaniu wartości.

Z dokumentów sojuszniczych wynika, że działania wielonarodowe realizowane są na poziomach: strategicznym, operacyjnym i taktycznym. Na szczeblu strategicznym, reprezentowanym przez organizację międzynarodową lub sojusz, następuje przekształcenie woli politycznej w cele polityczne i wydzielenie do ich osiągnięcia niezbędnych sił i środków (zarówno wojskowych jak i niemilitarnych). Na podstawie celi politycznych najwyższe dowództwo wojskowe, będąc fachowym organem doradczym kierownictwa politycznego, określa cele strategiczne (wojskowe) a następnie dokonuje podziału sił i środków. Z kolei dowództwo operacyjne na podstawie wytycznych kierownictwa strategicznego przekształca cele strategiczne w cele operacyjne. Wydanie dyrektywy dla dowódców komponentów wchodzących w skład wielonarodowych sił połączonych, a w dalszej kolejności kierowanie połączonymi działaniami rodzajów sił zbrojnych sił wielonarodowych zamyka niejako cały proces.

W odniesieniu do kwestii kompetencyjnych w aspekcie poziomów wielonarodowych operacji połączonych, należy zwrócić uwagę na to, że planowanie i prowadzenie działań jest

---

[40] J. Kręcikij, *Organizacja dowodzenia* ..., wyd. cyt., s. 12

domeną operacyjną, natomiast cele i ogólne ramy działań powstają na szczeblu strategicznym jako wynik ustaleń politycznych. Zasadniczym uwarunkowaniem planowania działań połączonych będzie charakter sytuacji planistycznej, czyli odpowiedź na pytanie czy planowanie będzie odbywać się w czasie pokoju, kryzysu, czy wojny? Będzie to implikować dwa zasadniczo różne procesy planowania. Pierwszy z nich to planowanie wyprzedzające. Rezultaty tego procesu będą miały charakter planów antycypacyjnych. Najczęściej będą stanowiły podstawę do opracowania planów będących efektem drugiego procesu planistycznego, czyli planowania operacji reagowania kryzysowego. Te plany z kolei będą miały charakter implementacyjny, czyli będą najczęściej realizowane w praktyce. W przypadku planowania o charakterze wyprzedzającym podstawą będą koncepcje wynikające z obowiązujących strategii i doktryn. Natomiast planowanie operacyjne opierać się będzie na wnioskach z oceny konkretnej sytuacji i prowadzić będzie wprost do decyzji o wyborze konkretnego wariantu działania.

Militarna współpraca wielonarodowa w obecnych czasach niesie za sobą ogromne korzyści polityczne dla organizacji międzynarodowych. Oprócz udziału w przedsięwzięciach wojskowych praktycznie niemożliwych do realizacji wyłącznie w wymiarze narodowym, pozwala ona poszczególnym państwom na realizację własnych celów (bez rezygnacji |z narodowych interesów i tożsamości), także w procesie współkształtowania wielonarodowych struktur wojskowych. Owa współpraca może być realizowana w ramach struktur permanentnych (sojusze), jak i tworzonych doraźnie (koalicje)[41]. Trzeba jednak pamiętać, iż w działaniach wielonarodowych istnieją także pewne ograniczenia rzutujące na sprawność tego typu działań, do których zaliczyć można:

- ograniczenia prawne politycznej i wojskowej swobody działania poszczególnych państw;
- bardziej skomplikowane i czasochłonne procedury podejmowania decyzji;
- przedłużanie się działań;
- konieczność uwzględniania narodowych interesów partnerów w trakcie podejmowania decyzji.

Rozpatrując problem podporządkowania części sił zbrojnych w działaniach wielonarodowych odpowiednim strukturom, trzeba mieć na uwadze, że nie oznacza to całkowitego oddania uprawnień, a co za tym idzie odpowiedzialności narodowej. Kwestie odpowiedzialności za własnych żołnierzy pozostają w gestii narodowej a przekazanie

[41] J. Kręcikij, *Wybrane problemy kierowania* ..., wyd. cyt., s. 21.

uprawnień dotyczą maksymalnie poziomu dowodzenia operacyjnego. Pełne dowodzenie zostaje zarezerwowane dla dowódców narodowych. Do obszarów narodowej odpowiedzialności w tego typu działaniach należą również: podległość służbowa, ochrona i bezpieczeństwo wojsk, wywiad, rozpoznanie i przeciwrozpoznanie, narodowe wsparcie dowodzenia, logistyka, współpraca z organizacjami (instytucjami) wojskowymi i cywilnymi, współpraca z mediami.

2.3. Analiza zagrożeń

Prowadzone analizy dowodzą, że celem działań sił antykoalicyjnych było przede wszystkim zakłócenie procesu stabilizacji i wywołanie ogólnego niezadowolenia Irakijczyków. Na szczególną uwagę zasługuje fakt, że działania sił antykoalicyjnych były z upływem czasu coraz lepiej zorganizowane. Świadczy o tym dobór miejsc, czasu i sił zaangażowanych w kolejne zamachy, co wskazuje na pełną koordynację tych działań. Zakres celów i obiektów ataków zwiększał się wraz z kolejnymi zmianami Polskiego Kontyngentu Wojskowego w Iraku, a obiektami ataków byli nie tylko żołnierze sił koalicyjnych i przedstawiciele lokalnych władz, ale również dziennikarze, przedstawiciele firm zagranicznych oraz ludność cywilna.

Sposoby i techniki działań sił terrorystycznych były różnorodne: od spontanicznego, niejednokrotnie przypadkowego użycia broni strzeleckiej (ang. small arms fire – SAF), po dokładnie zaplanowane zamachy, w których terroryści wykorzystywali różnorodne środki walki.

Do najczęściej stosowanych sposobów i technik ataków przeciwnika należy zaliczyć: zamachy osobowe, zamachy na infrastrukturę militarną, zamachy na infrastrukturę przemysłową, zamachy na obiekty administracji i władz tymczasowych.[42]

Klasyfikując ataki ze względu na sposób i technikę ich przeprowadzenia, można wyróżnić uderzenia wymierzone w: patrole sił koalicyjnych, konwoje z zaopatrzeniem i konwoje z pomocą humanitarną, posterunki i punkty kontrolne, bazy sił koalicyjnych, samoloty i śmigłowce sił koalicyjnych, infrastrukturę przemysłową, a także przywódców religijnych i członków władz.

W celu niedopuszczenia do niespodziewanego uderzenia przeciwnika oraz

[42] S. Pawlikowski, G. Majewski, *Wybrane uwarunkowania sytuacji polityczno – militarnej w Iraku*, „Myśl Wojskowa", Ministerstwo Obrony Narodowej, Warszawa rocznik XLVIII, s. 77.

zminimalizowania skutków jego działań, a tym samym zachowania zdolności do wykonywania zadań, organizowano ochronę i obronę kolumn samochodowych w formie patroli i konwojów. W trakcie ataków na przemieszczające się kolumny bardzo często wykorzystywano zdalnie detonowane ładunki wybuchowe, umieszczane wzdłuż tras przejazdów patroli i konwojów. Poza używaniem materiału wybuchowego do konstrukcji improwizowanych ładunków /materiałów/ wybuchowych (ang. *improvised explosive device - IED*) zamachowcy używali również klasycznych min przeciwpiechotnych oraz min przeciwpancernych, które były łatwo dostępne. Miny najczęściej odpalane były zdalnie lub używano zapalników czasowych.

Zgodnie z definicją zawartą w Słowniku Terminów i Definicji NATO, AAP-6 /2005/), improwizowane urządzenie wybuchowe, to urządzenie wykonane w sposób improwizowany, zawierające niszczące, śmiertelne, szkodliwe środki pirotechniczne lub zapalające środki chemiczne przeznaczone do niszczenia, unieszkodliwienia, nękania lub odwracania uwagi. Może zawierać materiały wojskowe, ale zwykle skonstruowane jest z elementów pochodzących z innych źródeł.[43]

Improwizowane ładunki wybuchowe to przede wszystkim broń tania, łatwa do skonstruowania i zastosowania. Pomysłowość terrorystów w zakresie konstruowania IED jest bardzo duża. Do ich konstruowania najczęściej używane są różnego rodzaju materiały wybuchowe, pociski artyleryjskie i moździerzowe, amunicja różnego typu, środki zapalające oraz urządzenia elektroniczne. Wśród opakowań używanych do ukrycia IED są samochody, opony, sterty kamieni, kanistry/beczki, rury stalowe/PCV, torby/walizki, butelki/słoiki/dzbany, lub wykonywane specjalnie w tym celu elementy prefabrykowane, zastępujące elementy oryginalne (krawężniki, płyty chodnikowe). Niekiedy do tego celu używane są zwierzęta domowe i ludzkie zwłoki.

Ponad 50% ogólnej liczby sposobów inicjowania IED, to detonacja za pomocą fal radiowych przy użyciu nadajników o mocy powyżej 1 W. Pozostałe 50% detonowanych IED, to odpalane przewodowo lub przy zastosowaniu samochodów pułapek albo samobójców.

Najgroźniejszą bronią w rękach terrorystów są samochody pułapki wypełnione materiałem wybuchowym. Odpalenie następuje na dwa sposoby: zdalnie (*ang. vehicle borne improvised explosive device – VBIED)* lub przez samobójcę (*ang. suicide vehicle borne improvised explosive device – SVBIED)*.

Z analizy miejsc dotychczasowych ataków z użyciem IED wynika, że najczęściej były

[43] *Słownik terminów* ..., wyd. cyt., s. 187.

to pobocza dróg, miejsca pomiędzy pasami dróg, przydrożne zarośla i znaki drogowe. Jak wykazały oceny działań terrorystów, ataki z użyciem improwizowanych ładunków wybuchowych stanowią jedno z głównych zagrożeń dla wielonarodowych. Tak było w Iraku i jest w Afganistanie.

Do najczęściej stosowanych sposobów ataków na patrole i konwoje należą:

- odpalaniu IED podłożonych na poboczu drogi lub na pasie rozdzielającym jezdnię;
- zasadzki na pojazdy, które zostały zmuszone do ograniczenia prędkości przez naturalne bądź sztuczne przeszkody terenowe;
- ostrzał kolumny pojazdów z broni maszynowej lub granatników przeciwpancernych;
- ataki przy użyciu samochodów – pułapek.

Natomiast do największych zagrożeń dotyczących baz i obiektów koalicyjnych zaliczyć można:

- ostrzał moździerzowy;
- ostrzał rakietowy;
- ataki samobójców przy użyciu pojazdów mechanicznych wypełnionych materiałem wybuchowym.

Szczególną uwagę należy zwrócić na ataki przeprowadzone przy użyciu pojazdów wypełnionych materiałami wybuchowymi i substancjami łatwopalnymi (ang. *Vehicle Borne Improvised Explosive Device - VBIED*). Samochody - pułapki wykorzystywane są najczęściej na dwa sposoby. Po pierwsze, mogą być przygotowane i przeznaczone do wcześniej określonego celu, np. baza wojskowa lub obiekt użyteczności publicznej. Po drugie, samochód załadowany materiałem wybuchowym może poruszać się po drogach w poszukiwaniu obiektu ataku. Irackie ataki z użyciem samochodów – pułapek w większości przypadków polegały na zastosowaniu trzech pojazdów. Pierwszy pojazd wskazuje drugiemu /wypełnionemu materiałem wybuchowym/ obiektu ataku, a w trzecim pojeździe jedzie operator kamery wideo, który filmuje całe zdarzenie. Następnie cały atak pokazywany jest w telewizji arabskiej sprzyjającej zamachowcom i w ten sposób film pokazywany jest na całym świecie. Terroryści wykorzystują niekiedy do tego typu zamachów dwa pojazdy z materiałem wybuchowym. Pierwszy pojazd przełamywał barierę fizyczną chroniącą obiekt, a tym samym umożliwiał drugiemu, który miał większą ilość materiału wybuchowego, dotarcie jak najbliżej do obiektu ataku i jego zniszczenie. Przykładem użycia VBIED do zamachu na obiekty wojskowe był atak na obóz Lima w Karbali w dniu 27.12.2003 roku.

Najczęściej wykorzystywanym sposobem przeprowadzania zamachów w Afganistanie jest użycie improwizowanych ładunków wybuchowych instalowanych w pojazdach mechanicznych /SVBIED/ oraz improwizowanych ładunków wybuchowych odpalanych z użyciem nadajnika radiowego (ang. – *radio controlled IED – RCIED).* Atak może być przeprowadzany pośrednio (przy pomocy nadajnika lub mechanizmu czasowego) lub przez zamachowca-samobójcę, wykorzystującego do tego celu tzw. pas szachidzki, samochód osobowy, a rzadziej motocykl lub rower. Obiektami ataków są głównie patrole i konwoje państw NATO i armii afgańskiej, przedstawiciele administracji rządowej oraz ludność cywilna. Większość ataków przeprowadzana jest podobnie jak w Iraku, w rejonach koncentracji ludności cywilnej oraz na głównych drogach dojazdowych. Często stosowany jest kombinowany sposób ataku, tzn. po detonacji ładunku wybuchowego, następuje ostrzał z broni ręcznej, granatników przeciwpancernych lub moździerzy. Głównymi celami zamachów było i nadal pozostaje zakłócenie procesu stabilizacji i pogłębienie chaosu, spotęgowanie uczucia zagrożenia oraz uzyskanie jak największego efektu psychologicznego poprzez zastraszenie stanu osobowego sił koalicyjnych.

W czasie trwania VI zmiany Polskiego Kontyngentu Wojskowego w Republice Iraku, zaczęło dochodzić w strefie odpowiedzialności MND CS do bardzo groźnych w skutkach ataków na kolumny pojazdów opancerzonych z użyciem kumulacyjnych improwizowanych urządzeń wybuchowych kierunkowego działania (ang. *explosively formed penetrator – EFP*). Wykonywane one były w warunkach domowych, sposobem chałupniczym. Ładunki są zazwyczaj rozmieszczane na poboczach dróg z zachowaniem odpowiedniego kąta rażenia lub na barierach ochronnych na wysokości ok. 1 m i odpalane w kierunku przedziału załogi pojazdu w celu jej zabicia. Takie ładunki mogą być ustawiane pojedynczo, w szyku, a niekiedy w kombinacji z improwizowana miną kierunkową. W praktyce atak polega na ustawieniu kilku lub nawet kilkunastu ładunków EFP po obu stronach drogi i zdetonowaniu ich po nadjechaniu kolumny.

Dodatkową trudność w utrzymaniu porządku sprawia wszechobecna broń ręczna. Każdy mieszkaniec tych krajów może posiadać broń i użyć jej w stosunku do wojsk koalicji.

2.4. Analiza działania komórek sztabowych w połączonych działaniach wielonarodowych

Prowadzenie operacji sojuszniczych NATO w obecnych uwarunkowaniach umożliwić ma koncepcja wielonarodowych połączonych sił zadaniowych - *Combined Joint Task Forces (CJTF)* nawiązująca bezpośrednio do stosowanej już od wielu lat przez siły zbrojne USA koncepcji połączonych sił zadaniowych (*US Joint Task Force*). Umożliwia ona realizację zadań również w takich sytuacjach, gdzie istniejące struktury dowodzenia nie mogą właściwie spełniać swojej roli. Toteż radykalnie zwiększa ona możliwości operacyjne Sojuszu, zwłaszcza w zakresie działań poza obszarem państw członkowskich. Obecnie koncepcja połączonych sił zadaniowych znajduje zastosowanie zarówno w operacjach prowadzonych w ramach obrony sojuszniczej, operacjach reagowania kryzysowego, w tym operacjach wsparcia pokoju, jak i innych działaniach realizowanych pod auspicjami ONZ, UE lub OBWE. Z praktycznego punktu widzenia koncepcja CJTF oznacza dla Sojuszu możliwość tworzenia w pełni samowystarczalnych, funkcjonalnych, wielonarodowych związków operacyjnych, zdolnych do realizacji szerokiego spektrum zadań nie tylko pod egidą NATO, lecz także z polecenia mandatu organizacji międzynarodowych. Jest to „narzędzie", które ma zapewnić Sojuszowi możliwość rozwinięcia w krótkim czasie wielonarodowych formacji, łączących różne rodzaje sił zbrojnych, sił wydzielanych przez różne państwa (zorganizowanych dla potrzeb przeprowadzenia konkretnej misji wojskowej). Co charakterystyczne, istota koncepcji CJTF nie polega na tworzeniu nowych stałych struktur, opartych na sztabach i związanych z nimi trwale formacji wojskowych, lecz na elastycznym gospodarowaniu istniejącymi zasobami, które dzięki uzgodnionym procedurom pozwolą na stworzenie spójnego mechanizmu operacyjnego[44]. Wyznaczone, przez dowództwa strategiczne, właściwe dowództwa regionalne posiadają w swych strukturach zespoły planowania działań połączonych (*Combined Joint Planning Staff – CJPS*), które przygotowują plany rozwinięcia dowództw CJTF ze składu dowództw macierzystych (*CJTF Parent HQ*). Są to stałe zalążki przyszłych dowództw CJTF. Do zalążków tych (w rejonie działań) dołączane są pozostałe komponenty i moduły z dowództw podregionalnych NATO oraz państw członkowskich Sojuszu i państw partnerskich.

Wyniki analiz doświadczeń dotychczasowych konfliktów wskazują, iż osiągnięcie zakładanych celów możliwe jest jednak tylko poprzez połączony wysiłek

[44] M. Obrusiewicz, *Wielonarodowe Połączone Siły Zadaniowe CJTF*, AON, Warszawa, 2002, s. 20.

rodzajów sił zbrojnych. Wypracowana w ramach NATO koncepcja *CJTF (Combined Joint Task Force)*, obejmuje w istocie stworzenie elastycznych struktur pozwalających na szybkie zorganizowanie i użycie sił w zależności od konkretnej sytuacji. Koncepcja umożliwia realizację zadań również w takich sytuacjach, gdzie istniejące struktury dowodzenia nie mogą właściwie spełniać swojej roli. Połączone siły zadaniowe radykalnie zwiększą możliwości operacyjne Sojuszu, zwłaszcza w zakresie działań poza obszarem państw członkowskich.

Podstawę do organizacji struktur dowództw można odnaleźć w wymienianych wcześniej dokumentach, które regulują funkcjonowanie dowództw w wojskach lądowych sił zbrojnych państw NATO (np. ATP-3.2. Land Operations – Działania wojsk lądowych). Struktury organizacyjne dowództw dzielą się na komóreki organizacyjno-funkcjonalne organów dowodzenia, które z kolei dzielą się na grupy, którym porządkowano ściśle określone obszary odpowiedzialności. Są to:

- grupa dowódcy;
- grupa główna;
- grupa specjalistyczna;
- grupa oficerów łącznikowych.

Wszystkie razem tworzą dowództwo (*Headquaters – HQ lub Command*), a trzy ostatnie zasadniczą część dowództwa jaką jest sztab (*Staff*)[45].

Grupę główną (*Primary Staff Group*) w dowództwach sił połączonych (*Joint Force Command*) tworzą komórki oznaczone literą J (*Joint*), a w dowództwie wielonarodowych sił połączonych – zestawienie liter CJ (*Combined Joint*).

Grupa specjalistyczna (*Special Staff* lub *Special staff group*) obejmuje specjalistów rodzajów wojsk, wspomagających dowódcę w rozwiązywaniu szczegółowych problemów dotyczących wojsk i służb. Większość z nich pracuje w ścisłym współdziałaniu z odpowiednimi komórkami grupy głównej, niektórzy wspierają dowódcę bez pośrednictwa oficerów sztabu. Specjaliści ci są zazwyczaj jednocześnie dowódcami jednostek reprezentowanych przez siebie rodzajów wojsk.

Grupa dowódcy zazwyczaj składa się z adiutanta, doradców oraz innych osób funkcyjnych powoływanych do rozwiązywania innych, nie rozwiązywanych przesz sztab problemów.

Oficerowie łącznikowi przeznaczeni są przede wszystkim do zapewnienia wymiany informacji i współdziałania pomiędzy dowódcami sił realizującymi wspólne cele a także

[45] J. Kręcikij, Organizacja dowodzenia w operacjach ..., wyd. cyt., s. 64

koordynacji wzajemnego wsparcia.

Zasady tworzenia struktur dowództw wielonarodowych sił połączonych (Combined Joint Task Force Headąuarters - CJTF HQs) reguluje szereg sojuszniczych dokumentów normatywnych, m.in. Sojusznicza doktryna działań połączonych AJP-01(A)" (*Allied Joint Operations Doctrine AJP-01*). Podstawowym elementem, niezbędnym do ich powstania są dowództwa macierzyste. W NATO istnieją trzy takie dowództwa, a jednym z ich zadań jest planowanie, przygotowanie oraz szkolenie personelu niezbędnego do organizacji dowództwa wielonarodowych sił połączonych. Zasadniczą rolę w tym procesie odgrywa personel kluczowy (*key nucleus staff*) i personel zalążkowy (*nucleus staff*) dowództwa macierzystego. Personel kluczowy stanowią oficerowie pełniący obowiązki w dowództwie macierzystym, ale zajmujący się wyłącznie problematyką planowania, powoływania, organizowania i rozmieszczania dowództwa wielonarodowych sił połączonych na bazie swojego dowództwa macierzystego. Personel zalążkowy natomiast to element budujący skład dowództwa wielonarodowych sił połączonych. Są oni przewidziani do zajęcia zasadniczych stanowisk w dowództwie *CJTF*. Na co dzień wykonują oni obowiązki związane z ich funkcjonowaniem w dowództwie macierzystym a zadania związane z dowództwem wielonarodowych sił połączonych są ich niejako dodatkowym obciążeniem. Dodatkowo dowództwo *CJTF* tworzyć będą reprezentanci innych państw - uczestników przyszłej operacji na zasadzie wzmocnienia (uzupełnienia) indywidualnego lub zespołowego. Indywidualne może polegać na przekazaniu w podporządkowanie *CJTF HQ* pojedynczych specjalistów w danej dziedzinie, zespołowe natomiast - na przekazaniu kompletnych zespołów funkcjonalnych z innych dowództw podległych dowództwu macierzystemu lub z innych dowództw, które funkcjonują w strukturze dowodzenia NATO. Może ono także być realizowane przez państwa nienależące do NATO. Tak utworzone dowództwo wielonarodowych sił połączonych posiada zazwyczaj w swojej strukturze następujące komórki organizacyjno-funkcjonalne i osoby funkcyjne[46]:

- dowódcę z grupą dowódcy;
- doradców politycznych i prawnych;
- przedstawicieli dowódców komponentów i kontyngentów poszczególnych państw;
- oficerów łącznikowych i łącznikowe zespoły logistyczne sił narodowych i międzynarodowych;

[46] *AJP-01(B),* wyd. cyt., s. 4-10.

- narodowe komórki rozpoznawcze *(National Intelligence Cells – NIC),* przeznaczone do zapewnienia przepływu informacji pomiędzy narodowymi strukturami rozpoznawczymi a sztabową komórką CJ2;
- połączony sztab kierowany przez szefa sztabu.

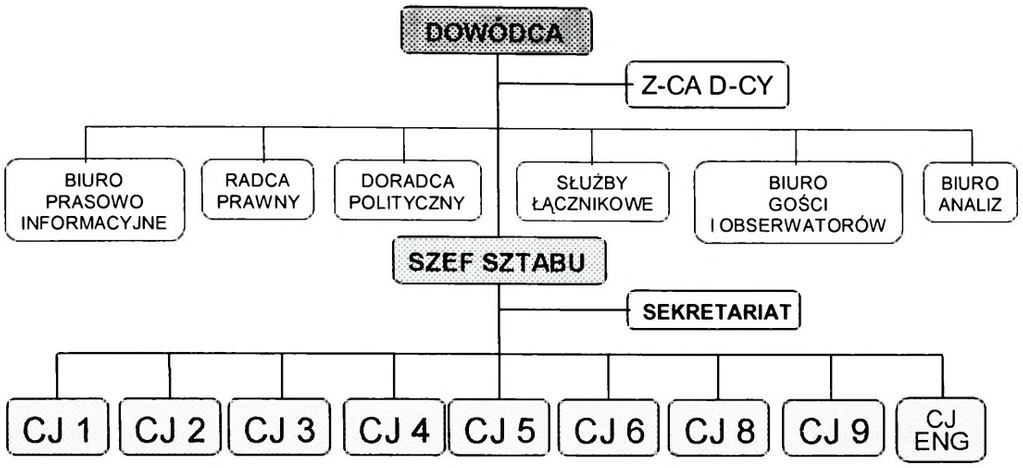
Sztab zorganizowany może być w następujące komórki funkcjonalne[47]:

- CJ1 - wielonarodowa połączona komórka personalno-administracyjna *(Personel and Administration);*
- CJ2 - wielonarodowa połączona komórka rozpoznawcza *(Intelligence)*;
- CJ3 - wielonarodowa połączona komórka operacyjna *(Operations)*, a w niej wielonarodowe komórki operacji lądowych, morskich, powietrznych, specjalnych i innych (w zależności od składu sił);
- CJ4 - wielonarodowa połączona komórka logistyczna *(Logistics)*;
- CJ5 - wielonarodowa połączona komórka planistyczna *(Plans and Policy)*;
- CJ6 - wielonarodowa połączona komórka wsparcia dowodzenia i łączności *(CIS – Command and Information System)*;
- CJ7- wielonarodowa połączona komórka doktryn i szkolenia *(Doctrine and Training)*[48];
- CJ8 - wielonarodowa połączona komórka finansowa *(Resources and Finance)*;
- CJ9 - wielonarodowa połączona komórka współpracy cywilno-wojskowej *(CIMIC - Civil - Military Cooperation)*;
- Jednostki zabezpieczające, które odpowiadają za zapewnienie niezbędnego personelu, organizację systemu łączności, transport, wyposażenie i bezpieczeństwo podczas funkcjonowania dowództwa.

Pozostałe elementy będące poza połączonym sztabem (niewchodzące w skład CJ1…CJ9) mogą mieć różny skład uzależniony od konkretnych wymagań.

[47] Kręcikij J., *Organizacja dowodzenia ...*, wyd. cyt., s. 72

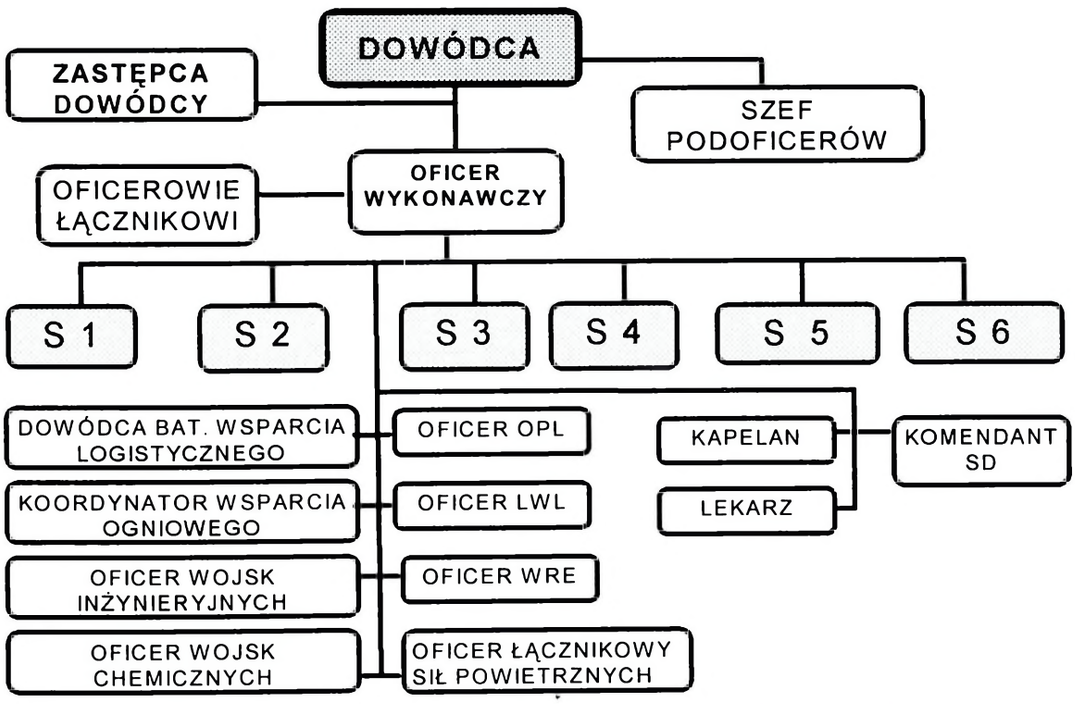
[48] Komórka ta występuje zazwyczaj tylko w pokojowej strukturze dowództwa lub w dowództwach wielonarodowych, których działania koncentrują się na odbudowie struktur wojskowych i szkoleniu wojsk.



Źródło: Opracowano na podstawie J. Kręcikij, Wybrane problemy kierowania zgrupowaniami wielonarodowymi sił połączonych, AON, Warszawa, 2003

Rys.2.1. Przykładowa struktura dowództwa wielonarodowych sił połączonych.

Zespół badawczy pragnie na przykładzie wielonarodowej Brygady –Wschód (*Multinational Task Force East MNB-E*) będącej jedną z wydzielonych sojuszniczych sił zadaniowych w Kosowie, dokonać analizy organizacji sztabu. Jej dowódca wobec podległych mu batalionów z siedmiu państw koalicyjnych posiadał uprawnienia typu *OPCON*. Struktura dowództwa brygady wyglądała następująco:



Źródło: Opracowano na podstawie J. Kręcikij, Organizacja dowodzenia w operacjach wielonarodowych, praca naukowo-badawcza pk. Koalicja, AON, Warszawa 2007

Rys.2.2. Struktura dowództwa Brygady Wielonarodowej-Wschód (*Multinational Task Force East MNB-E*)

Analiza komórek dowództwa pozwala na wysunięcie następujących wniosków. Dowództwo składało się z grupy dowódcy, grupy koordynacyjnej, i oficerów specjalistów[49]. Dowódca posiadał zastępcę i bezpośrednio podlegał mu szef podoficerów. Na czele sztabu stał oficer wykonawczy (szef sztabu), odpowiadający za pracę grupy koordynacyjnej i oficerów specjalistów. Współpracował on bezpośrednio z grupą oficerów łącznikowych. Grupa koordynacyjna złożona była z sekcji funkcjonalnych S1 do S6, z taktycznym centrum operacyjnym (*Tactical Operation Center – TOC*) w sekcji operacyjnej S3. W grupie specjalistycznej znajdowali się oficerowie rodzajów wojsk i służ, jak również dowódcy pododdziałów (np. dowódca batalionu wsparcia dowodzenia, koordynator wsparcia ogniowego). Występowali oni w podwójnej roli: jako dowódcy organicznych pododdziałów i jako specjaliści rodzajów wojsk - w czasie planowania działań w brygadzie.

Osiągnięcie wspólnych celów poprzez umiejętne działania militarne w operacjach wielonarodowych zależy przede wszystkim od sprawnego systemu dowodzenia, a to uzależnione jest w głównej mierze od organizacji dowodzenia i struktur dowództw. Różnice w strukturach dowództw, wojsk, systemach dowodzenia, zasadach działania, interoperacyjności i narodowej specyfiki pracy sztabów, możliwościach militarnych, uzbrojeniu a także różnice kulturowe, religijne czy interesy narodowe poszczególnych państw wydzielających siły do wspólnych działań, nie ułatwiają dowodzenia w układzie wielonarodowym. W zasadniczych dokumentach normatywnych armii państw NATO znalazły się postanowienia normujące zasady dowodzenia działaniami sił wielonarodowych[50].

Jak już wcześniej wspomniano, wielonarodowa współpraca wojskowa może być realizowana w różnych formach organizacyjnych a wielonarodowe struktury militarne mogą być organizowane zgodnie z zasadami: państwa wiodącego (ang. Lead Nation), państwa określającego ogólne ramy (ang. Framework Nation) i integracji (ang. Integration)[51].

Zasada państwa wiodącego (Lead Nation) określa, że struktura wielonarodowa kierowana jest przez przedstawicieli jednego państwa, zgodnie z zasadami dowodzenia i prowadzenia działań tego państwa. Dowództwo jest w zasadzie obsadzone przez przedstawicieli owego państwa a pojedyncze stanowiska w sztabie mogą być zajmowane przez przedstawicieli sił zbrojnych wydzielających swe kontyngenty do danej struktury.

---

[49] W publikacji *AJP-3.2.1. Command and Control of Land Forces* (Dowodzenie siłami lądowymi) dla opisania komórek 1...n w sztabie publikacja stosuje się określenie „grupa koordynacyjna" (*Coordinating Staff Group*). Natomiast w dokumencie nadrzędnym - *ATP-3.2. Land Operations* (Działania wojsk lądowych) przyjęty jest podział sztabu na komórki 1...9.

[50] Na przykład struktury dowództw w działaniach połączonych wraz z charakterystyką zadań ich komórek funkcjonalnych [w:] *AJP-01(A)*, s. 4A1-1 – 4A1-3.

W tym przypadku jednostki innych państw podporządkowywane są tylko na okres działań.

Zasada państwa określającego ogólne ramy (Framework Nation) oznacza, że w takiej wielonarodowej strukturze jedno z państw spełnia decydującą rolę. Odpowiada ono głównie za dowodzenie, administrację i wsparcie logistyczne. Przedstawiciele tego państwa zajmują kierownicze stanowiska i stanowią zdecydowaną większość pracowników dowództwa. Zasady dowodzenia i prowadzenia działań odpowiadają zasadom narodowym lub po wcześniejszym uzgodnieniu procedurom NATO. Przedstawiciele państw wydzielających kontyngenty do takiej struktury zajmują w niej stanowiska według ustalonego wcześniej podziału. Wojska podporządkowywane są tylko na okres wspólnych działań i obowiązują je procedury narodowe lub NATO.

Zasada integracji (Integration) określa, że w przypadku przyjęcia takiej struktury wielonarodowej, stanowiska w sztabie wielonarodowym z reguły odpowiadają udziałowi kontyngentu danego państwa w organizowanych strukturach. Najważniejsze stanowiska podlegają określonej rotacji, zasady dowodzenia, prowadzenia działań (czasami również szkolenia), odpowiadają procedurom NATO lub też ustalane są przez uczestniczące państwa. Charakterystyczne dla takiego rozwiązania jest również to, że wydzielone jednostki państw reprezentowanych w takiej wielonarodowej strukturze mogą być podporządkowane już w okresie pokoju, najczęściej jednak są podporządkowywane na okres działań na zasadach dowodzenia operacyjnego (ang. Operational Command – OPCOM) lub kontroli operacyjnej (ang. Operational Control – OPCON)[52]. Pozostają one jednak nadal w narodowej podległości służbowej i dyscyplinarnej a ich zasady działania są zgodne z procedurami NATO lub też ustaleniami podjętymi przez poszczególne państwa.

Prowadzenie wielonarodowych połączonych działań sił zbrojnych w układzie koalicyjnym (z współudziałem w nich komponentów państw z poza Sojuszu) wymaga zorganizowania sprawnych struktur dowodzenia. To przede wszystkim od nich zależeć będzie osiągnięcie celów militarnych. Ze względu na wspomnianą wcześniej specyfikę prowadzenia takich działań, szczególnego znaczenia nabiera problematyka dowodzenia. Jest to niejako nowa jakościowo sytuacja, w której zarówno w relacjach dowodzenia (podległości), jak i funkcjonalnych oraz współdziałania występować będą organa dowodzenia różnych, koalicyjnych armii. Analiza struktur dowództw sił wielonarodowych zawartych w wydawnictwach sojuszniczych i narodowych wskazuje, że struktura organizacyjna sił

---

[51] J. Kręcikij, *Organizacja dowodzenia* ..., wyd. cyt., s. 20.

[52] Kręcikij J., *Zakres uprawnień i odpowiedzialności dowódców wobec podległych im wojsk*, AON, Warszawa 2000.

wielonarodowych może przybierać trzy główne formy organizacyjne:

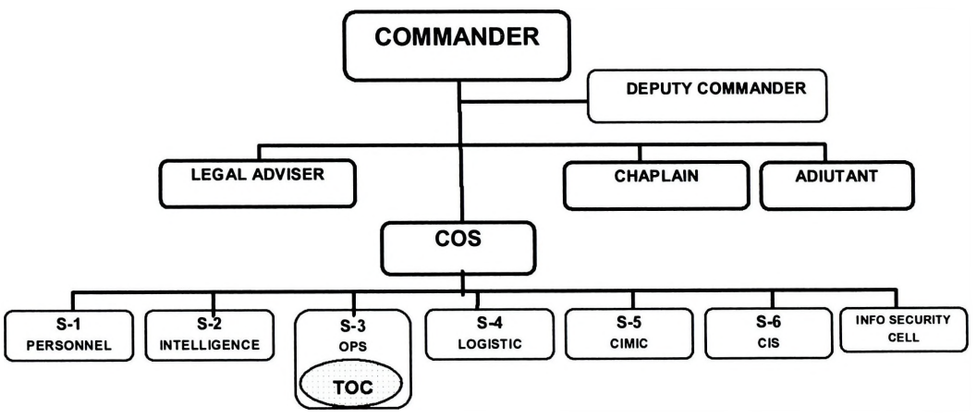
– bezpośredniego podporządkowania;

– dowodzenia komponentowego (komponenty narodowe, komponenty rodzajów sił zbrojnych, komponenty funkcjonalne);

– koordynowanej struktury koalicyjnej.

Forma bezpośredniego podporządkowania, czyli bezpośredniego sprawowania dowodzenia w działaniach wielonarodowych, polega na bezpośrednim podporządkowaniu dowódcy sił wielonarodowych elementów różnych rodzajów sił zbrojnych wydzielanych z różnych państw. Swoistą wadą tego sposobu jest to, iż jest on jednak możliwy do realizacji jedynie w przypadku działań prowadzonych stosunkowo niewielkimi siłami i na małą skalę. Wiąże się to z zasadą, iż zbyt duża rozpiętość dowodzenia powoduje, iż skuteczne sprawowanie dowodzenia staje się bardzo trudne a wręcz niemożliwe.

Ciekawym rozwiązaniem struktury dowództwa wielonarodowego była międzynarodowa brygada pod polskim dowództwem (*Multinational Brigade Combat Team - MBCT*) w ramach dywizji wielonarodowej w Iraku. Był to „twór" wzorowany na potrzeby misji, głównie na amerykańskich brygadowych zespołach bojowych (*Brigade Combat Team - BCT*). W skład struktury dowództwa wchodzili oprócz polskich, żołnierze państw wchodzących w skład *MBCT (ang. Multinational Brigade Combat Team – MBCT).* Struktura dowództwa Brygady Wielonarodowej przedstawiała się następująco:



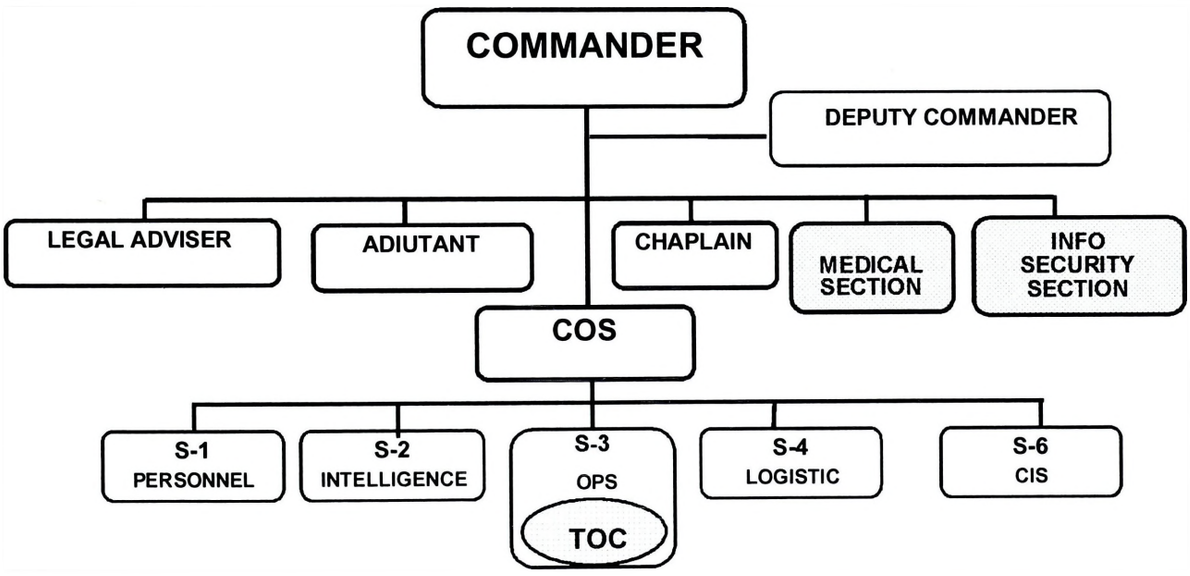
Źródło: Opracowano na podstawie J. Kręcikij, Organizacja dowodzenia w operacjach wielonarodowych, AON, Warszawa 2007.

Rys.2.3. Struktura Dowództwa Brygady Wielonarodowej (*MBCT*) w I zmianie

Grupę dowódcy stanowili radca prawny, kapelan i adiutant dowódcy. Sztab *MBCT* składał się z sześciu sekcji - od S1 do S6 - i komórki ochrony (bezpieczeństwa) informacji podległej bezpośrednio szefowi sztabu. Wraz z następowaniem kolejnych zmian struktura

dowództwa *MBCT* ulegała stosownie do zadań, potrzeb i wymagań, pewnym ewolucjom. Główne zmiany dotyczyły sekcji operacyjnej S-3. W związku ze wzrostem zadań operacyjno-szkoleniowych i szkoleniowo-doradczych pojawiły się problemy dotyczące koordynacji działań brygady i batalionu, jak i prowadzenia bieżącej działalności operacyjnej, planistycznej i szkoleniowej. Jedną z ich przyczyn byłą niewystarczająca obsada Taktycznego Centrum Operacyjnego (*Tactical Operational Center – TOC*).

Początki wspólnych działań z nowo odbudowywaną z Armią Iracką, zmniejszenie zadań stricte operacyjnych i skupienie wysiłku na szkoleniu wojsk były konsekwencją przyjętych wcześniej założeń dotyczących stopniowego oddawania odpowiedzialności za bezpieczeństwo w prowincjach siłom irackim. Toteż struktury organizacyjne dowództwa Wielonarodowej Brygady (*MBCT)* ulegały dalszym modyfikacjom. W czwartej i piątej zmianie przedstawiały się one następująco:



Źródło: Opracowano na podstawie J. Kręcikij, Organizacja dowodzenia w operacjach wielonarodowych, AON, Warszawa 2007

Rys.2.4. Struktura Dowództwa Brygady Wielonarodowej (*MBCT*) w IV i V zmianie

Zadania sekcji S-5 (CIMIC) przejęły sekcje S3 i S4. Do grupy dowódcy włączono sekcję bezpieczeństwa informacji (*Info security section*) i dodano sekcję medyczna (*Medical section*). W szóstej zmianie dowództwu brygady podporządkowano Zespół doradczo-szkoleniowy (*Military Transition Team – MiTT*), którego głównym zadaniem było szkolenie oficerów sztabu brygady irackiej.

Z powyższej analizy wynika, że nie ma sztywnych zasad tworzenia struktur dowództw w operacjach wielonarodowych. Szczegółowe rozwiązania w tym zakresie zależą

od specyfiki operacji, stron zaangażowanych w tworzenie sił wielonarodowych oraz od państwa wiodącego, tworzącego określone dowództwo.

2.5. Rodzaje działań wojsk w operacji wielonarodowej

Analizując rodzaje działań wojsk w operacji wielonarodowej należy stwierdzić, że zależą one od rodzaju operacji. Zasadniczo, współczesne operacje wielonarodowe można określać jako misje (operacje) pokojowe. Typologia operacji pokojowych jest generalnie różna. Według Sekretarza Generalnego ONZ typologia operacji pokojowych przedstawia się następująco[53]:

- dyplomacja prewencyjna (*ang. preventive diplomacy)* oznacza działania dyplomatyczne prowadzące do zapobieżenia powstawaniu sporów pomiędzy skłóconymi stronami, przeciwdziałać przerodzeniu się sporów w konflikty militarne, a w przypadku ich powstania, ograniczyć zasięg ich oddziaływania. W jej ramach dopuszcza się zapobiegawcze rozmieszczanie sił;
- tworzenie pokoju (*ang. peacemaking)* oznacza działania prowadzące do porozumienia stron walczących nawet do operacji wymuszania pokoju;
- utrzymanie pokoju *(ang. peacekeeping)* oznacza rozmieszczanie sił ONZ w rejonie objętym konfliktem, jednak przy zgodzie wszystkich zainteresowanych stron. W skład sił wielonarodowych mogą wchodzić komponenty: wojskowy, policyjny i cywilny. Należy zauważyć, że utrzymanie pokoju poszerza możliwości zapobiegania konfliktom jak również tworzenia pokoju;
- budowanie pokoju *(ang. peacebuilding)* obejmujące wszelkie działania po zakończeniu konfliktu zmierzające do utworzenia i wsparcia struktur władzy w zakresie umocnienia i utrwalenia osiągniętego pokoju.

Inny podział stosowany jest w dokumentach Sojuszu Północnoatlantyckiego. W operacjach innych niż wojna nazywanych również operacjami nie wynikającymi z artykułu V wyróżnia się[54]:

- zapobieganie konfliktom *(ang. conflikt prevention)* obejmujące misje dyplomatyczne, konsultacje, inspekcje, monitorowanie sytuacji, obserwację, a także prewencyjne

[53] F. Gągor, K. Paszkowski, Międzynarodowe operacje pokojowe w doktrynie obronnej RP, Wydawnictwo Adam Marszałek, Toruń 1999, s. 44.
[54] Tamże, s.46.

rozwinięcie sił mające na celu nie dopuścić do powstania konfliktu zbrojnego;

- tworzenie pokoju *(ang. peacemaking)* obejmujące dyplomację prowadzoną po wybuchu konfliktu zmierzającą do zaprzestania walk i porozumienia pokojowego. Szczegółowo mogą być realizowane poprzez misje mediacyjne i rozjemcze, sankcje i izolowanie dyplomatyczne;
- utrzymanie pokoju *(ang. peacekeeping)* obejmuje bezstronną interwencję sił zbrojnych i komponentu cywilnego strony trzeciej (sił wielonarodowych) celem ograniczenia, łagodzenia a w efekcie zakończenia działań zbrojnych pomiędzy zwaśnionymi stronami. Jest traktowane jako uzupełnienie politycznego procesu rozwiązywania konfliktów;
- wymuszanie pokoju *(ang. peace enforcement)* polega na przywracaniu pokoju w rejonie konfliktu przy wykorzystaniu środków militarnych. Wskazuje się, że operacje tego typu prowadzone są w przypadku konfliktu zarówno międzypaństwowego jak i wewnętrznego. Celami tych operacji jest pomoc humanitarna lub tworzenie władz w przypadku gdy przestały działać instytucje państwowe;
- budowanie pokoju *(ang. peacebuilding)* obejmujące działania po konflikcie zmierzające do zapewnienia warunków uniknięcia odnowienia konfliktu;
- pomoc humanitarna (*ang. humanitarian aid)* obejmująca niesienie pomocy ludności cywilnej w trudnej sytuacji.

Typologia operacji pokojowych według poszczególnych narodów charakteryzuje się odmiennym podejściem do problemu, co ma odzwierciedlenie w nazewnictwie i specyfikacji. Według poglądów brytyjskich wyróżnia się: utrzymanie pokoju, rozszerzone utrzymanie pokoju oraz wymuszanie pokoju[55]. W dokumentach amerykańskich wymienia się: wsparcie dyplomacji, utrzymanie pokoju oraz wymuszanie pokoju[56]. Również inny podział występuje w rosyjskiej myśli wojskowej, a mianowicie: ustanowienie pokoju, utrzymanie pokoju oraz przymuszanie do pokoju[57].

Z powyższej analizy wynika, że każde państwo inaczej interpretuje poszczególne misje pokojowe, a co za tym idzie, inaczej przedstawia użycie sił zbrojnych w ramach operacji pokojowych (wielonarodowych).

Pomimo tych rozbieżności w typologii operacji pokojowych, działania sił wielonarodowych zależne będą od mandatu im udzielonego przez ONZ oraz od rozwoju sytuacji w obszarze operacji. Celem dokonania analizy działań sił wielonarodowych zasadne

---

[55] Tamże, s.47.
[56] Tamże, s. 48.
[57] Tamże, s.49.

jest przedstawienie rodzajów działań realizowanych w dotychczasowych misjach[58].

W misji UNEF II *(ang. Second United Nations Emergency Force),* trwającej od października 1973 r. do lipca 1979, około 7 tyś. żołnierzy nadzorowało porozumienie, pomiędzy Izraelem a Egiptem, o przerwaniu walk. Siły wielonarodowe nadzorowały również przemieszczanie sił stron konfliktu oraz utworzyły i kontrolowały strefę buforową między wcześniej wspomnianymi państwami.

Misją realizowaną w Europie było UNTAES *(ang. United Nations Transitional for Eastern Slavonia, Baranja and Western Sirmium)* realizowana przez prawie dwa lata, na przestrzeni styczeń 1996 r.- grudzień 1997 r. Siły wielonarodowe w ilości ponad 4300 żołnierzy nadzorowały demilitaryzację regionu oraz monitorowały powrót uchodźców. Zapewniały również pomoc we wprowadzaniu w życie postanowień porozumienia pokojowego oraz tworzeniu tymczasowych sił policyjnych. Nie mniej ważnym zadaniem było również zapewnienie tymczasowej administracji.

We wcześniejszą misję prowadzoną w regionie byłej Jugosławii, UNPROFOR (*ang. United Nations Protection Force)*, zaangażowano ponad 30 tyś. żołnierzy sił wielonarodowych. Trwała ona od marca 1992 r. do grudnia 1995. W jej ramach siły pokojowe monitorowały przerwanie ognia w Chorwacji, nadzorowały wycofanie armii jugosłowiańskiej, zapewniały demilitaryzację i ochronę ludności w strefach ochronnych, zapewniały pomoc w akcjach humanitarnych a także prewencyjnie rozmieściły siły w byłej jugosłowiańskiej Republice Macedonii.

Następną misją w regionie Bałkan była UNCRO *(United Nations Confidence Restoration Operation in Croatia)*. Trwała od marca 1995 r. do stycznia 1996 r. na terenie Chorwacji. Siły wielonarodowe w ilości prawie 15 tyś. miały za zadanie nadzorować przestrzeganie porozumienia o przerwaniu ognia, monitorować przebieg procesu demilitaryzacji oraz obserwować i meldować o ruchach wojsk przez granicę między Chorwacją a Jugosławią. Oprócz zadań wojskowych miały ponadto ułatwiać wprowadzania w życie porozumienia gospodarczego oraz ułatwianie transportów z pomocą humanitarną dla Bośni i Hercegowiny przez terytorium Chorwacji.

Siły pokojowe prowadziły działania mandatowe w Kambodży m.in. w ramach misji pokojowej UNTAC *(Unitek Nations Transitional Autority In Cambodia)*. Ponad 15 tyś. żołnierzy realizowało, w okresie od marca 1992 r. do września 1993 r., nadzorowanie

---

[58] Opracowano na podstawie: www.unic.un.org.pl/misje pokojowe oraz F Gągor, K. Paszowski, międzynarodowe operacje pokojowe w doktrynie obronnej RP, Wydawnictwo Adam Marszałek, Toruń 1999.

koncentracji i demobilizacji wojsk stron konfliktu. Oprócz zadań militarnych prowadziły również: monitorowanie przestrzeganie praw człowieka, pomoc w zapewnieniu porządku publicznego i funkcjonowania administracji cywilnej, nadzorowanie repatriacji i osiedlania uchodźców oraz organizacji i przeprowadzenia wyborów. Nie mniej ważnym zadaniem sił wielonarodowych UNTAC była pomoc w odbudowie niezbędnej infrastruktury.

Realizacją nieco innych zadań charakteryzowała się misja UNMIH *(ang. Unitede Nations Mission In Haiti)*. W okresie od września 1993 r. do czerwca 1996 r. ponad 6 tyś. „błękitnych hełmów" niosło pomoc w utrzymaniu bezpieczeństwa i ochronie głównych obiektów wraz z międzynarodowym personelem. Zadaniem spoza zainteresowania wojskowego była pomoc w organizacji i przeprowadzeniu wyborów.

Operacja prowadzoną w obszarze kontynentu afrykańskiego była misja UNOSOM II *(Unitek Nations Operaton In Somalia)*. Została ustanowiona rezolucją S/RES/814 Rady Bezpieczeństwa z 26 marca 1993 r. Wprowadzono ją na miejsce operacji UNOSOM I. Przejęła ona także zadania wykonywane przez siły międzynarodowe UNITAF. W ramach swojego mandatu UNOSOM II mógł podejmować działania, włącznie z użyciem siły, których efektem byłoby ustanowienie bezpieczeństwa i niczym niezakłócone dostawy środków humanitarnych dla miejscowej ludności. Operacja UNOSOM II miała ukończyć zadania zaczęte przez UNITAF - przywrócić pokój, stabilizację, prawo i porządek. Do głównych obowiązków należał także nadzór nad zakończeniem przemocy, powstrzymywanie walk zbrojnych, odbieranie nielegalnie posiadanej broni, utrzymanie bezpieczeństwa w portach i na lotniskach, oczyszczanie z min, udział w powrocie uchodźców do swoich domów. UNOSOM II miał także służyć pomocą w odbudowie gospodarczej, społecznej i politycznej w Somalii, restytucji najważniejszych struktur państwowych i zasad demokratycznych. W lutym 1994 r., po serii krwawych incydentów i atakach na żołnierzy ONZ, Rada Bezpieczeństwa przekształciła mandat UNOSOM II wyłączając możliwość używania przymusu. W marcu 1995 r. operacja ta zakończyła swoją działalność. Uczestniczyło w niej 14969 żołnierzy i policjantów oraz międzynarodowy personel cywilny i lokalny.

Kolejnym przykładem operacji pokojowej prowadzonej na wyżej wspomnianym kontynencie była misja UNAMIR *(ang. United Nations Assistance Mission for Rwanda)*. Prowadzona była w okresie od października 1993 r. do marca 1996 r. Mandat UNAMIR obejmował:

- udział w zapewnianiu bezpieczeństwa w stolicy Rwandy Kigali;
- monitorowanie przestrzegania porozumienia o zawieszeniu broni, w tym ustanowienie strefy zdemilitaryzowanej i procedur demobilizacyjnych;

- nadzór nad bezpieczeństwem w trakcie sprawowania władzy przez rząd tymczasowy;
- udział w oczyszczaniu terenów z min;
- udział w koordynacji działań humanitarnych.

W okresie trwania jednej zmiany misji działania prowadziło 1252 żołnierzy, 146 obserwatorów wojskowych, 160 międzynarodowego personelu cywilnego, 160 personelu lokalnego i 56 wolontariuszy ONZ[59].

Powyżej przedstawiono wybrane misje pokojowe prowadzone pod egidą ONZ, zakończone, w ramach których zadania mandatowe realizowane były przez siły zbrojne. Zasadnym jest również przedstawić misje prowadzone w chwili obecnej przez NATO. Przykładem takiej operacji pokojowej jest misja SFOR *(Stabilisation Force),* która prowadzona jest na terytorium Bośni i Hercegowiny. Siły wielonarodowe realizują zadania od grudnia 1996 r. obejmujące: zapobieganie ponownemu podjęciu walk poprzez odstraszanie lub użycie siły, monitorowanie i wymuszanie przestrzegania postanowień porozumienia pokojowego oraz utrzymanie kontroli przestrzeni powietrznej. Zadaniami wykraczającymi poza działania typowo wojskowe są: zapewnienie warunków do funkcjonowania instytucji państwowych, utrzymanie kontaktów ze wszystkimi stronami porozumienia pokojowego oraz zapewnienie wsparcia powietrznego a w razie potrzeby ewakuacji.

Kolejnym przykładem jest operacja ISAF *(ang. International Security Assistance Force)* w Afganistanie[60]. Głównym celem misji ISAF jest wsparcie rządu afgańskiego w zapewnieniu oraz utrzymaniu bezpieczeństwa, pomoc w odbudowie Afganistanu i stworzeniu demokratycznych struktur państwowych. Zadania realizowane w ramach ISAF przyczynić się mają do poprawy sytuacji gospodarczej kraju, wzrostu społecznej akceptacji demokratycznie wybranego rządu oraz zwiększenia współpracy międzynarodowej. W ramach realizacji powyższych celów ISAF koncentruje się na przedsięwzięciach, które najbardziej przyczyniają się do poprawy warunków życia ludności cywilnej, jak również wzrostu znaczenia rządu w jego dążeniach do poprawy sytuacji ekonomicznej. Szczegółowe działania sił wielonarodowych obejmują m.in.:

- pomoc w zapewnieniu bezpieczeństwa zasobów mineralnych, przejść granicznych, sieci dróg, ujęć wody;
- wsparcie rządu afgańskiego w prowadzonej kampanii antynarkotykowej;
- wsparcie rządu afgańskiego w rozwoju strategii ekonomicznej i zasobów ludzkich;

---

[59] Stan na luty 1996 r.
[60] Opracowano na podstawie: www.isaf.wp.mil.pl/isaf.html.

- prowadzenie działań na rzecz wygaszenia konfliktów i zmniejszenia napięć w Afganistanie, skupiając się głównie na walce z działaniami terrorystycznymi w kraju;
- wspieranie i szkolenie Narodowych Sił Afganistanu do momentu uzyskania przez nie poziomu umożliwiającego im przejęcie pełnej odpowiedzialności za wewnętrzne i zewnętrzne bezpieczeństwo kraju.

Specyficzną operacją sił wielonarodowych jest działanie w ramach Międzynarodowych Sił Stabilizacyjnych w Republice Iraku[61]. Głównym celem operacji było stworzenie bezpiecznych warunków funkcjonowania praworządnego i demokratycznego państwa irackiego. W tym celu podjęto następujące działania:

- zjednoczenie postępowych sił politycznych Iraku i stworzenie zrębów władz państwowych – Irackiej Rady Zarządzającej działającej przy wsparciu Tymczasowych Sił Koalicyjnych;
- przygotowanie konstytucji i pomoc w demokratycznych wyborach prezydenckich, państwowych i samorządowych;
- przekazanie władzy i kierowania działaniami państwa cywilnym strukturom irackim;
- pomoc przy tworzeniu warunków do poprawy sytuacji ekonomicznej, również poprzez utrzymanie odpowiedniego poziomu pomocy humanitarnej dla ludności irackiej, a także pomoc przy usuwaniu negatywnych skutków własnych działań ofensywnych;
- tworzenie struktur nowych irackich sił bezpieczeństwa, w tym: armii, policji, policji granicznej oraz korpusu obrony cywilnej.

W zakresie wojskowo-policyjnych działań stabilizacyjnych prowadzono i prowadzi się nadal:

- wsparcie działań irackich sił bezpieczeństwa *(ang. ISF - Iraqi Security Forces)* w utrzymywaniu ładu i porządku publicznego. Wyposażanie, szkolenie i bezpośrednie wsparcie irackich sił bezpieczeństwa oraz zabezpieczenie prowadzonych przez nie operacji o charakterze wojskowym i policyjnym;
- zapewnienie ludności irackiej pomocy medycznej i sanitarnej;
- zamknięcie wszystkich nielegalnie działających sądów szariackich oraz osłabienie ugrupowań terrorystycznych w celu wzmocnienia lokalnych władz cywilnych,

[61] Opracowano na podstawie: www.pkwirak.wp.mil.pl/pl/27.html

zapewnienia poszanowania prawa i porządku publicznego oraz wzbudzenie zaufania lokalnej społeczności do ISF;

- zabezpieczenie rurociągów oraz linii energetycznych przed kradzieżami i dewastacją oraz aktami sabotażu i dywersji;
- zapewnienie bezpieczeństwa transportom sił koalicyjnych w całym obszarze odpowiedzialności;
- likwidacja składów amunicji byłej Armii Irackiej oraz rozminowanie kraju;
- udzielanie pomocy gospodarczej ludności cywilnej w ramach Współpracy Cywilno – Wojskowej CIMIC *(ang. Civil-Military Cooperation)*;

Charakter działania sił stabilizacyjnych ulegał stopniowej modyfikacji w zależności od zmian jakie następowały w Iraku. Początkowy, militarny charakter sił rozjemczych w kwietniu 2005 r. zmienił się na militarno – szkoleniowy, a w marcu 2006 r. został przekształcony w szkoleniowo – militarny.

2.6. Uwarunkowania bezpieczeństwa działań na szczeblu połączonego dowództwa wielonarodowego

Podstawą prowadzenia operacji wielonarodowych są wspólnie określone cele dla sił wielonarodowych. Ich realizacja jest jednak zawsze warunkowana interesami narodowymi, które nie zawsze są zbieżne. Dla trwałości i spoistości koalicji tworzącej siły wielonarodowe decydujące znaczenie ma w takim przypadku znajomość i uwzględnianie celów partnerów. Przy tworzeniu wielonarodowych sił niezbędna jest wola polityczna zainteresowanych państw. Należy jednak zaznaczyć, że podstawą koalicji jest formułowanie wspólnych celów, natomiast ich realizacja wyrazem międzynarodowej solidarności oraz uznania i obrony wspólnych wartości. Wielonarodowość działań stwarza również dodatkowy atut, a mianowicie polityczną legitymizację podejmowanych działań militarnych co pozytywnie wpływa na ich postrzeganie przez opinię międzynarodową.

Z analizy uwarunkowań operacji wielonarodowych można wnioskować, że wielonarodowość w prowadzeniu operacji niesie za sobą również zagrożenia. Można do nich zaliczyć[62]:

- ograniczenia politycznej i wojskowej swobody działania;

[62] J. Kręcikij, M. Strzoda, J. Trembecki, *Założenia teoretyczne wielonarodowej operacji połączonej, AON, Warszawa 2000, s. 46.*

- wydłużenie i skomplikowanie procedur podejmowania decyzji;
- przeciąganie się działań;
- konieczność realizacji dodatkowych zadań i uwzględniania narodowych interesów partnerów.

Przedstawione wyżej trudności wynikają z różnic w: możliwościach militarnych, odmiennych zasadach działania, narodowej specyfiki pracy sztabowej oraz różnic kulturowych i religijnych. Szczegółowo analizując problematykę w zakresie bezpieczeństwa na szczeblu połączonego dowództwa można wnioskować, że problem osiągnięcia interoperacyjności[63] dotyczyć będzie następujących dziedzin:

- organizacji dowodzenia i kierowania;
- procesu dowodzenia i kierowania;
- środków dowodzenia.

Konkludując, należy stwierdzić, że problemem, a co za tym idzie zagrożeniem dla sił wielonarodowych, są różne rozwiązania narodowe w zakresie systemu dowodzenia. Zasadniczym więc zadaniem w zakresie przygotowania sił wielonarodowych winno być dążenie do takiego stanu, w którym:

- wszystkie uczestniczące dowództwa i sztaby wielonarodowe identycznie będą rozumieli zagadnienia związane z dowodzeniem i pracą sztabu;
- organizacja pracy w sztabach, na różnych szczeblach dowodzenia i zasady planowania działań, w tym kierowania działaniami będą jednakowo interpretowane;
- środki dowodzenia stanowiące podstawę sprawnego działania, w tym również oprzyrządowanie miejsc pracy na poszczególnych stanowiskach dowodzenia będzie kompatybilne a personel będzie potrafił sprawnie się nimi posługiwać;
- znajomość języka (angielskiego) zapewni sprawną komunikację pomiędzy wielonarodowymi członkami dowództwa.

Oprócz zagrożeń wewnętrznych już wymienionych, a wynikających z tworzenia dowództwa i sztabu występują zagrożenia zewnętrzne. Związane są bezpośrednio z sytuacją w obszarze operacji wielonarodowej. Zagrożenia takie podlegają analizie i stanowią podstawę tworzenia planów bezpieczeństwa.

Przedsięwzięcia z zakresu bezpieczeństwa operacyjnego planują i koordynują wyspecjalizowane komórki sztabowe pionu operacyjnego w porozumieniu z pionem rozpoznania wojskowego. Pion rozpoznania generuje możliwe scenariusze

[63] Interoperacyjność – współdziałanie dowództw różnych szczebli podczas realizacji wspólnych zadań.

zagrożeń, natomiast pion operacyjny planuje przedsięwzięcia mające na celu zapobiec zagrożeniu lub zminimalizować jego skutki. Plan bezpieczeństwa operacji powinien obejmować różne możliwe warianty wydarzeń i być podatny na zmiany, stosownie do zaistniałych sytuacji.

Planowanie bezpieczeństwa operacji realizowane jest w pięciu fazach[64]:

- faza pierwsza obejmuje: ocenę możliwości wywiadowczych i rozpoznawczych przeciwnika. Na jej podstawie określane są elementy działań. które przeciwnik jest w stanie wykryć te które mogą być ujawnione. te które mają wprowadzić w błąd oraz te które muszą być bezwzględnie chronione;
- faza druga obejmuje: analizę zagrożeń pod kątem tego jaką przeciwnik zdobył informację o naszym potencjale wojskowym lub wydedukował na podstawie dostępnych mu danych;
- faza trzecia obejmuje: określenie najbardziej wrażliwych elementów operacji i optymalnych środków bezpieczeństwa zapewniających pożądane efekty ochrony;
- faza czwarta obejmuje: określenie wpływu środków bezpieczeństwa na efektywność operacyjną oraz stopnia ryzyka przy niepomyślnym zastosowaniu lub braku zastosowania środków bezpieczeństwa;
- faza piąta obejmuje: opracowanie planu bezpieczeństwa operacyjnego (jako załącznika do planu operacji) oraz procedury jego realizacji, monitorowania i meldowania w przypadku naruszeń.

W trakcie działań wielonarodowych plan bezpieczeństwa operacji podlega stałej ocenie przez pion operacyjny we współpracy z pionem rozpoznawczym. Przy czym pion operacyjny działa jako punkt centralnego monitorowania i meldowania o sytuacji a pion rozpoznawczy dostarcza niezbędnych informacji mających wpływ na korekty i skuteczność działań ochronnych. W sytuacji fiaska działań osłonowych i świadomości przeciwnika dotyczącej szczegółów operacji, pion operacyjny ocenia wpływ zaistniałej sytuacji na dalszy przebieg operacji i melduje dowódcy w celu wprowadzenia niezbędnych modyfikacji do planu operacyjnego.

[64] Doktryna narodowa..., wyd. cyt., s. 6-27.

2.7. Wnioski

1. Zagrożenie, zarówno wewnętrzne jak i zewnętrzne należy traktować jako obawę o utratę wysoko cenionych wartości przez człowieka, gdzie sytuacja zagrożenia jest uświadamiana przez podmiot. Jednocześnie poczucie zagrożenia jest odwrotnie proporcjonalne do zaspokojenia potrzeby bezpieczeństwa.
2. Działania wielonarodowe są to wszystkie przedsięwzięcia sił, realizowane w ramach jednej operacji przez zgrupowania wojsk składające się z elementów więcej niż jednego państwa. Jeżeli wszystkie zaangażowane państwa należą do sojuszu, to działania ich są nazywane sojuszniczymi (swoista odmiana działań wielonarodowych). Każde działania sojusznicze są działaniami wielonarodowymi, lecz nie każde wielonarodowe są sojuszniczymi. Działania wielonarodowe są w praktyce działaniami połączonymi, w których cele są realizowane przy użyciu, co najmniej dwóch rodzajów sił zbrojnych z co najmniej dwóch państw.
3. Działania wielonarodowe charakteryzują się dobrowolnością uczestniczenia w nich przez poszczególnych członków – państwa. Zadania sił wielonarodowych są kompromisem uzyskanym w ramach negocjacji tworzenia sił. Cele narodowych komponentów, w zależności od celów politycznych państw zaangażowanych, mogą znacznie się różnić, a co za tym idzie, stanowić pewnego rodzaju zagrożenie wewnętrzne dla sił wielonarodowych.
4. W ramach warunków działania dowództw i wojsk wielonarodowych należy wyróżnić wystąpienie kryzysu lub wojny, czyli sytuacji zagrożenia dla społeczności międzynarodowej. Jest to podstawą do podjęcia decyzji przez organizację międzynarodową o użyciu sił militarnych. Do tworzenia sił wielonarodowych niezbędna jest zgoda państw na wydelegowanie sił do operacji, co pociąga za sobą podział stanowisk w komórkach dowództwa przydzielanych dla państw dostarczających siły do operacji. Po generacji sił niezbędna jest zgoda na podział obszaru podlegającego kontroli pomiędzy siły delegowane.
5. W ramach operacji prowadzonych przez siły wielonarodowe występują działania wojskowe, policyjne i administracyjne. Wielozakresowość działań jest przyczyną pojawiania się różnego rodzaju zagrożeń, dotyczących zarówno działań militarnych w klasycznym ujęciu przeciwko siłom wielonarodowym, jak również działań asymetrycznych z użyciem siły - terrorystycznych.

6. Tworzenie struktur sił wielonarodowych nie posiada rozwiązań prawnych (oprócz działań sojuszniczych). Odpowiedzialność za tworzenie struktur dowodzenia przypada na „państwo wiodące" przy aktywnym uczestnictwie wszystkich stron partycypujących przy generowaniu sił. Nie jest jednak zabronione korzystanie ze sprawdzonych rozwiązań przyjętych przez Sojusz NATO.
7. Przy tworzeniu struktur dowództwa sił wielonarodowych przedsięwzięcia powinny ogniskować wokół problemów związanych z jednakowym rozumieniem zagadnień związanych z dowodzeniem i pracą sztabu przez wszystkich uczestników, właściwym interpretowaniem kierowania działaniami, właściwym wykorzystaniem środków dowodzenia oraz zapewnieniem sprawnej komunikacji między wielonarodowymi członkami dowództwa.
8. Zadania poszczególnych komponentów sił wielonarodowych są determinowane celami politycznymi poszczególnych państw – uczestników operacji oraz zadaniami określonymi przez organizację, pod auspicjami której siły będą działać.
9. W ramach zapewnienia bezpieczeństwa własnych wojsk niezbędne jest opracowanie procedur dotyczących: postępowania na SD, użycia broni w czasie wykonywania zadań mandatowych oraz użycia środków informatycznych, łączności i rozpoznania. Istotnym warunkiem bezpieczeństwa jest posiadanie: własnych sił rozpoznania i wywiadu, sił lotniczych do kontroli przestrzeni powietrznej oraz narzędzi przymusu w stosunku do ludności cywilnej i wojskowej.
10. W analizowanych strukturach dowództw brak jest jednoznacznego wyróżnienia komórki odpowiadającej za bezpieczeństwo sił wielonarodowych. Odpowiedzialność w tym zakresie jest rozproszona. Świadczy to o dość niskim poziomie świadomości zagrożeń lub nieodpowiednim podejściu do problematyki bezpieczeństwa wojsk.

3. DIAGNOZA ZAGROŻEŃ BEZPIECZEŃSTWA FIZYCZNEGO W OPERACJACH WIELONARODOWYCH

Duże zagrożenie bezpieczeństwa wojsk i dowództw w czasie wykonywania zadań w ramach wypełnianych obowiązków na misjach pokojowych jest przyczynkiem do zwiększenia wymogów związanych z ochroną wojsk (ang. *Force Protection*). Dowódcy wszystkich szczebli dowodzenia w Iraku czy Afganistanie lub Czadzie, Kosowie, Bośni i Hercegowinie, przykładają wielką wagę do zagadnień związanych z zapewnieniem bezpieczeństwa żołnierzom i pracownikom wojska wykonującym zadania zarówno w bazie, jak i poza bazą.

Problematyka organizacji ochrony wojsk, stosownej do zagrożeń występujących w obszarach prowadzonych operacji lub misji stabilizacyjnych, odzwierciedlona jest w opracowaniach teoretycznych i praktycznym działaniu wojsk. Wiele dokumentów sojuszniczych opisuje lub wręcz nakazuje zachować stosowne działania w razie zagrożenia. Problematyka bezpieczeństwa znalazła także odzwierciedlenie w narodowych dokumentach doktrynalnych, np. w *„Doktrynie prowadzenia operacji połączonych (DD/3)"*, regulaminach walki, np. *„Regulamin działań wojsk lądowych (DD/3.2)*, instrukcjach np. *„Rozpoznanie wojskowe"*, *„Instrukcja o ochronie obiektów wojskowych"* i wydawnictwach szkoleniowych, np. *„Konwoje, patrole, VBIED, przeszukiwanie. MEDEVAC, SALUTE, IED Report.*", czy *„Sposoby i techniki przeprowadzania zamachów na Siły Koalicyjne w Iraku"*.

Wysiłek zespołu badawczego ukierunkowany został na zidentyfikowanie czynników, które mają zasadnicze znaczenie dla skuteczności sytemu bezpieczeństwa fizycznego. W treści rozdziału zaprezentowano wyniki badań dotyczące aktualnych rozwiązań systemowych oraz analizę środowiska bezpieczeństwa i ludności zamieszkującej obszar prowadzonych działań i ich wpływ na bezpieczeństwo wojsk.

3.1. UWARUNKOWANIA BEZPIECZEŃSTWA FIZYCZNEGO W OPERACJACH WIELONARODOWYCH

Różnorodność współczesnych form działań operacyjnych i taktycznych powoduje nowe jakościowo zadania stawiane przed Wojskiem Polskim. Zaangażowanie w prowadzenie działań poza granicami kraju w ramach operacji wielonarodowych stwarza nowe wyzwania przed którymi staje wojsko. Udział wydzielonych komponentów wymaga także zaplanowania i skoordynowania działań jednostek sił zbrojnych państw uczestniczących w działaniach koalicyjnych. Nabiera to szczególnego znaczenia w obliczu konieczności dostosowania wielu aspektów działalności do wymagań osiągnięcia kompatybilności i interoperacyjności z innymi państwami zarówno Sojuszu oraz wchodzących tylko doraźnie w koalicje.

Jednym z zasadniczych wniosków jaki zdołano ustalić w toku prac badawczych to, brak możliwości przedstawienia uwarunkowań bezpieczeństwa fizycznego w operacjach wielonarodowych bez wykazania znaczenia czynników decydujących o właściwym funkcjonowaniu bazy. Do takich czynników należą: dobór sił i środków ochronnych, nieszablonowość opracowanych planów i szybkość podejmowania decyzji. Wielonarodowa współpraca umożliwia korzystanie z narodowych zasad działania, doświadczeń i zasobów wszystkich partnerów, osiągając w ten sposób szczególną, dodatkową jakość. Doświadczenia z działań w Iraku wynikały głównie ze ścisłej współpracy z wojskiem amerykańskim, które ma wieloletnie doświadczenie w prowadzeniu operacji poza granicami kraju. Również pod względem bezpieczeństwa fizycznego współpraca z nimi była nieodzownym elementem, a ich pomoc polegała nie tylko na doradzaniu, ale również wspieraniu materialnym. Dostarczali gotowe prefabrykaty i urządzenia wspomagające ochronę. Doraźna pomoc dotyczyła także opracowania procedur i jednoznaczne rozumienie definicji. Przyjęta definicja bezpieczeństwa fizycznego oznaczała ochronę obiektów, osób, materiałów i dokumentów przed dostępem fizycznym, podglądem, podsłuchem lub inną formą penetracji wraz z procedurami dopuszczającymi i sprawdzającymi.

Zagrożenia, które niesie ze sobą rzeczywistość, wymagają przemyślanych rozwiązań w zakresie stworzenia systemu zabezpieczeń dla każdego obiektu i na każdą okoliczność. Zgodnie z definicją ochrony fizycznej zawartą w podrozdziale 2.1, pod tym pojęciem należy rozumieć zespół przedsięwzięć ochronnych realizowanych przez odpowiednio wyposażone (w środki przymusu bezpośredniego) i przeszkolone warty i służby wewnętrzne, mające na celu zapobieganie przestępstwom i wykroczeniom przeciwko powierzonemu do ochrony

mieniu, przeciwdziałanie powstaniu szkód wynikających z tych zdarzeń oraz niedopuszczenie do wstępu osób nieuprawnionych na teren chroniony, a także zapewnienie bezpieczeństwa osobom przebywającym na terenie bazy.

Bardzo duże znaczenie ma właściwy dobór ochrony fizycznej, czyli adekwatny do zagrożeń, a jednocześnie wpływający na efektywność i skuteczność ochrony. Bez sprzętu technicznego trudno wyobrazić sobie obecnie skuteczne Force Protection, dlatego tak dużą wagę przykłada się do wyposażenia baz w nowoczesny sprzęt wspomagający ochronę. Sprzęt przeznaczony do wykrywania materiałów wybuchowych, wykrywania metalu, skanery ludzi i pojazdów, czy sensory magnetyczne, to tylko część możliwych urządzeń w systemie ochrony fizycznej.

Analiza istniejącej literatury przedmiotu (dokumentów normatywnych, regulaminów, instrukcji obowiązujących w Siłach Zbrojnych RP) wykazała, że problem ochrony wojsk jest ściśle związany z ochroną obiektów wojskowych i obejmuje ogólne zasady organizacji i funkcjonowania ochrony w czasie pokoju, co znalazło swoje odzwierciedlenie w obowiązującej „Instrukcji o ochronie obiektów wojskowych". Natomiast brak jest dokumentów odzwierciedlających stan bezpieczeństwa wojsk podczas działań wojennych, kryzysowych i misji pokojowych.

3.2. KRYTERIA BEZPIECZEŃSTWA FIZYCZNEGO

Kryterium podziału, to zasada organizująca, według której dokonujemy podziału logicznego jakiegoś zbioru. Kryterium podziału jest jednym z trzech niezbędnych warunków (obok rozłączności i adekwatności) poprawnie dokonanego podziału logicznego. Kryterium podziału jest wybierane przez osobę dokonującą podziału zgodnie z jej potrzebami poznawczymi. Według tak rozumianych pojęć zespół autorski dokonał podziału bezpieczeństwa fizycznego.

Dotyczy ono wyboru czynnika, za pomocą którego dokonano podziału ochrony fizycznej w operacjach wielonarodowych.

Uznano, że podstawą podziału będzie kryterium „ochrona indywidualna żołnierza". Możemy wówczas wyróżnić następujące elementy mające zasadnicze znaczenie:

- hełmy kompozytowe typu kevlar;
- kamizelki kuloodporne zapewniające ochronę przed pociskami i odłamkami;
- broń strzelecka wyposażona w celowniki holograficzne;

- noktowizja i termowizja;
- środki ochrony przed bronią masowego rażenia;
- system nawigacji satelitarnej GPS;
- rękawiczki taktyczne;
- okulary ochronne;

Innym kryterium, które może być rozpatrywane, to „ środki ochrony zbiorowej". Wówczas możemy wyróżnić:

- nowoczesne transportery opancerzone;
- pojazdy o podwyższonej odporności minowej klasy MRAP;
- broń zespołowa, np. granatniki automatyczne;
- telefony satelitarne, np. Thuraya;
- cyfrowe środki łączności;
- systemy zagłuszające odpalanie przez radio ładunków wybuchowych;
- bezzałogowe środki latające;

Analizując ochronę fizyczną można określić kolejne kryterium, jakim może być „ochrona personelu w bazie". Rozpatrując ten czynnik możemy wyodrębnić:

- warty i służby dyżurne;
- posterunki kontrolne;
- pododdziały szybkiego reagowania;
- schrony dla personelu i ukrycia dla sprzętu;
- system zapór inżynieryjnych;
- system monitorowania terenu;
- dyżurne środki ogniowe.

Kryteriów podziału jest oczywiście bardzo wiele, a co więcej, ten sam zbiór można dzielić według rozmaitych kryteriów, zależnie od doraźnych potrzeb. Przyjęte przez zespół badawczy kryteria wystarczają do przeprowadzenia analizy uwarunkowań bezpieczeństwa wojsk podczas realizacji zadań w operacjach wielonarodowych.

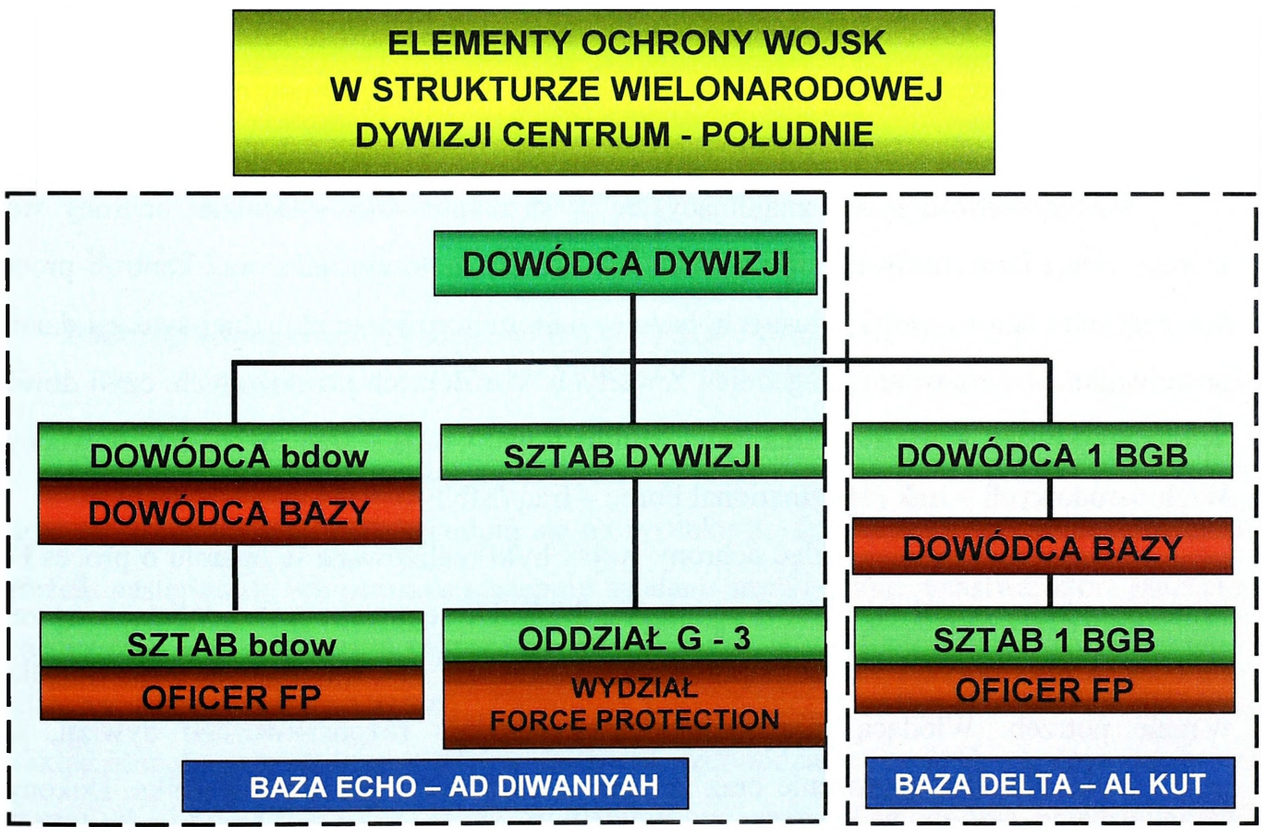
3.3. ANALIZA AKTUALNYCH ROZWIĄZAŃ SYSTEMOWYCH OCHRONY FIZYCZNEJ W OPERACJACH WIELONARODOWYCH

Zgodnie z definicjami zawartymi w podrozdziale 2.1, system może być bardziej lub mniej złożony, a jednocześnie może stanowić podsystem systemu wyższego szczebla.

Posiłkując się definicją tam zawartą można przyjąć, że systemem ochrony obiektów wojskowych, to określony zbiór wzajemnie powiązanych ze sobą i współzależnych przedsięwzięć, w tym również realizowanych przez wojska własne i sojusznicze w przypadku wspólnego użytkowania obiektów, obejmujący ochronę fizyczna i techniczne środki wspomagające oraz przedsięwzięcia organizacyjne.

Podstawowe aspekty każdego systemu to: skład, struktura i otoczenie, czyli relacje występujące pomiędzy poszczególnymi elementami systemu oraz między elementami systemu, a jego otoczeniem. O skuteczności systemu możemy mówić wtedy, gdy spełnione są zakładane warunki, a więc w tym konkretnym przypadku musi on być odporny na zakłócenia, a struktura i środki muszą być adekwatne do zagrożenia. Bardzo istotną rolę odgrywa również wyszkolenie personelu, który będzie praktycznie wykonywał zadania związane z zapewnieniem bezpieczeństwa fizycznego. Nieodzownym wydaje się również wieloaspektowe podejście do ochrony fizycznej. Dodatkowo, jednym z najważniejszych elementów jest właściwy i niezawodny obieg informacji alarmowych zarówno na terenie bazy, jak i między elementem realizującym zadania poza bazą a bazą oraz między poszczególnymi wozami patrolu, czy konwoju.

Sprawne działanie systemu ochrony fizycznej w działaniach wielonarodowych polega na realizacji wielu przedsięwzięć wykonywanych przez wszystkie elementy systemu ochrony.



źródło: opracowanie własne

Rys. 3.1. Elementy ochrony wojsk (Force Protection) w strukturze sił wielonarodowych (MND CS) VI zmiany PKW IRAK

System ochrony fizycznej w działaniach wielonarodowych można podzielić na następujące elementy:

- dowódca bazy /ang. *Camp Commander*/;
- wydział /sekcja/ ochrony wojsk;
- służb dyżurnych /w tym centrum operacyjne, warta, patrole, siły szybkiego reagowania/;
- zapór inżynieryjnych /bariery, zasieki itp./;
- urządzeń wspomagających ochronę baz /skanery, wyrywacze metali/;
- wieże, posterunki obserwacyjne i kontrolne, patrole;

Jedną z najważniejszych osób odpowiedzialnych za ochronę fizyczną bazy jest dowódca bazy, który zgodnie z wymogami zawartymi w Planie Ochrony Bazy ma prawo:

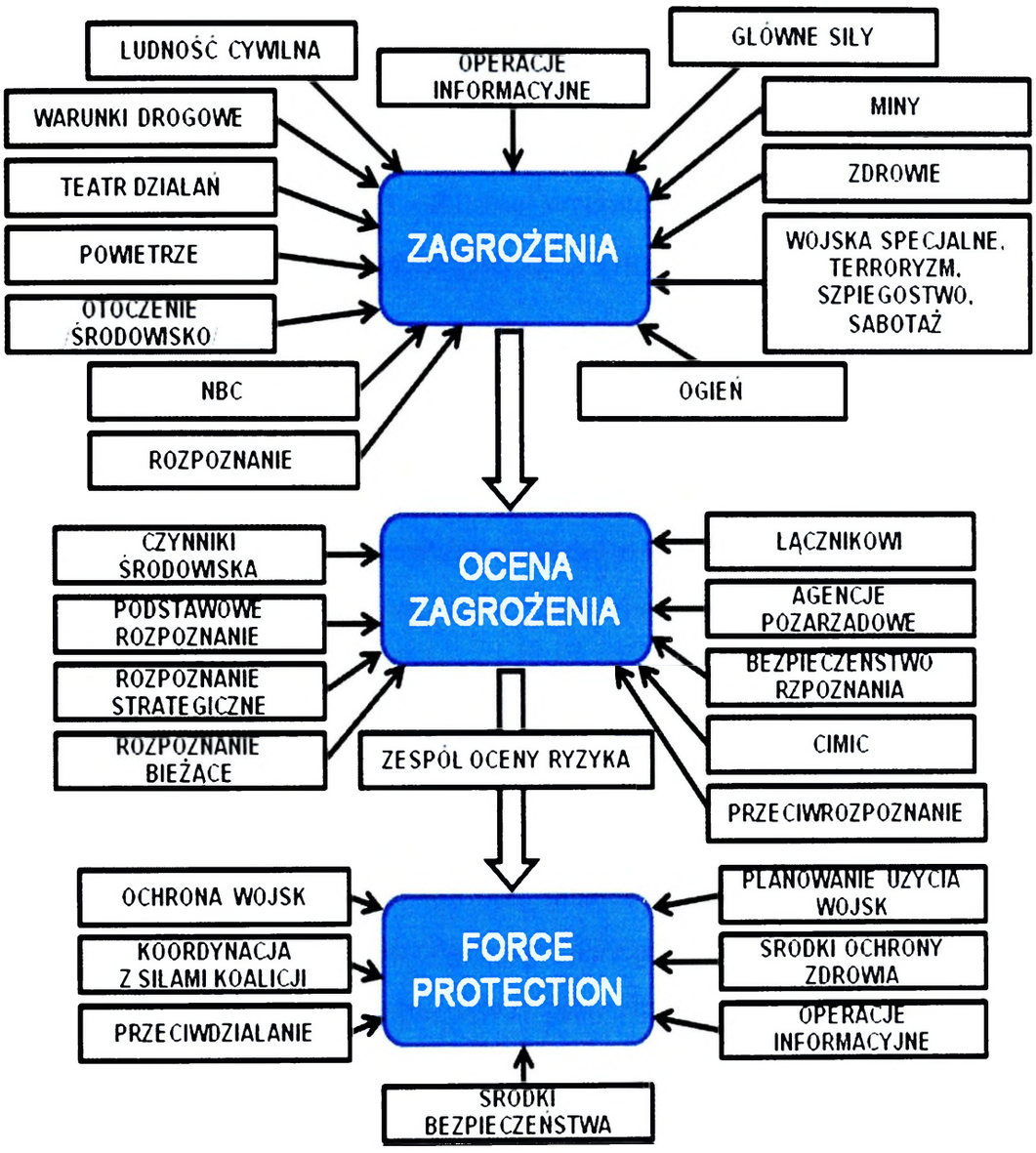
- dokonywać wszelkich zmian w procedurach dotyczących bazy, w ramach postanowień, rozkazów, wytycznych określonych przez jego przełożonych;
- ustalać i egzekwować na terenie bazy stany gotowości systemu ochrony wojsk, kody ruchu pojazdów, statusy uzbrojenia stosownie do zaistniałej sytuacji, stopnia zagrożenia i wytycznych przełożonych.

Analiza obserwacji wykazała, że tak przyjęta struktura systemu miała miejsce w praktycznym zastosowaniu podczas działań w Iraku. Bazując na doświadczeniu, w czasie VI zmiany PKW Irak dowódcą bazy Echo był dowódca batalionu dowodzenia, zaś w bazie Delta – zastępca dowódcy Brygadowej Grupy Bojowej. W obu bazach zastosowano przedstawione rozwiązanie.

Istotną rolę odgrywał znajdujący się w strukturze G-3 - Wydział ochrony wojsk, którego praca koncentrowała się na analizowaniu, przygotowywaniu oraz kontroli procedur dotyczących ochrony wojsk własnych, bazując na monitorowaniu aktualnej sytuacji działania przeciwnika oraz rozwijaniu zagadnień zawartych w rozkazach przełożonych, czyli dowódcy Wielonarodowego Korpusu – Irak (ang. Multinational Corps – Iraq /MNC-I/) i dowódcy Sił Wielonarodowych – Irak (Multinational Force – Iraq /MNF-I/).

Planowanie przedsięwzięć ochrony wojsk było realizowane w oparciu o proces Force Protection, który został przedstawiony na rys. 3.3.2. Do tego celu został wyznaczony zespół roboczy, który spotykał się na odprawie cyklicznie raz na dwa tygodnie oraz dodatkowo w razie potrzeb. Wiodącą rolę spełniał szef oddziału rozpoznawczego dywizji, który przedstawiał aktualne zagrożenie oraz zmiany w taktyce działania przeciwnika. Dokonywał również oceny przeciwnika określając prawdopodobny cel i sposób działania sił antykoalicyjnych oraz miejsca, w których spodziewana jest szczególna aktywność

przeciwnika. Na podstawie dokonanej oceny prze szefa G-2, podejmowano działania służące zabezpieczeniu wojsk przed skutkami ataków rebeliantów.



źródło: opracowanie własne na podst. MND(CS) SOP FORCE PROTECTION

Rys. 3.2. Proces Force Protection

Ochrona wojsk była w pierszym rzędzie procesem oceny niebezpieczeństwa, który składał się z elementów, które znajdują się na rysunku 3.3.2. Tak więc, po wygenerowaniu zagrożeń, następowała ich ocena, a następnie ustalano środki bezpieczeństwa, które należało przedsięwziąć, aby ograniczyć zagrożenie lub całkowicie je wyeliminować. Dokonywał tego nieetatowy zespół oceny zagrożeń. Zespołowi przewodniczył zastępca dowódcy dywizji, a w skład zespołu wchodzili: zastępca szefa sztabu, szef oddziału G – 2, G – 3, dowódca bazy oraz szef sekcji Force Protection. Dodatkowo mogli być wezwani na odprawę przedstawiciele innych oddziałów sztabu dywizji, np. G – 4, G – 9, G – 1, itd.

Dokonana analiza rozwiązań systemowych ochrony fizycznej wskazuje, że zastosowane w praktyce rozwiązania nadają się do wykorzystania w innych operacjach wielonarodowych. Były one wynikiem doświadczeń zarówno sił polskich, jak i sojuszników wspomagających proces bezpieczeństwa. Nie oznacza to jednak, że są uniwersalne. Każda operacja to inne środowisko i inny charakter działań, każdorazowo też należy indywidualnie rozpatrywać problem ochrony fizycznej.

3.3.1. Analiza systemu ochrony i obrony bazy wojskowej na przykładzie VI zmiany PKW Irak

W celu zapewnienia ochrony pododdziałów przebywających w bazach wojskowych w czasie wykonywania zadań przez PKW w Republice Iraku wprowadzono jednolity systemem przedsięwzięć bezpieczeństwa w zakresie przyjętych stanów alarmowych, kodów obowiązującego oporządzenia ochronnego, kodów ograniczeń w ruchu pojazdów, a także przyjęto określone zasady postępowania w przypadku wystąpienia różnego rodzaju zagrożeń. Podstawowym dokumentem regulującym realizację przedsięwzięć bezpieczeństwa każdej bazy wojskowej był „Plan ochrony i obrony". Zawierał on graficzny plan ochrony z naniesionymi rubieżami obrony, punktami obserwacyjnymi, punktami kontrolnymi, stanowiskami ogniowymi oraz trasami patrolowania. Dodatkowo umieszczone były tam sygnały alarmowania i ostrzegania, sygnały wewnętrznego ostrzegania, opis stanów zagrożenia alarmowego, kodów ubioru, ruchu pojazdów i uzbrojenia oraz wzór tablicy ze stanem zagrożenia alarmowego i kodami ubioru i ruchu pojazdów.

System ochrony i obrony baz zawierał zarówno elementy ochrony wewnętrznej, jak i zewnętrznej. Przedsięwzięcia realizowane w celu zapewnienia najlepszej ochrony podzielono na bierne i czynne.

Sytuacja w rejonie odpowiedzialności MND CS oraz występujące tam zagrożenia wykazały duże znaczenie ochrony biernej w systemie ochrony wojsk i obrony baz wojskowych.

W bazie Echo ochrona bierna realizowana były głównie wewnątrz obozu polegała na zapewnieniu ochrony dla żołnierzy sztabu wielonarodowej dywizji oraz pododdziałów stacjonujących w bazie, systemie schronów i ukryć ochronnych, które zostały wykonane w rejonie stanowiska dowodzenia dywizji oraz w miejscach zakwaterowania. Należy podkreślić, że miejsca w schronach oraz ukryciach zarówno w miejscach pełnienia służby, jak

i w rejonach odpoczynku zostały podzielone pomiędzy poszczególne komórki funkcjonalne sztabu, a ich zajmowanie było objęte cyklicznymi treningami.

W szczególności ważną rolę spełniały różnego rodzaju bariery ochronne w postaci gotowych barier żelbetowych. Prefabrykowane bariery żelbetowe wykorzystywano zarówno jako bariery utrudniające ruch, ale również jako ogrodzenie i zabezpieczenie bazy przed atakami samobójczymi z użyciem pojazdów. Niewątpliwą zaletą tego rodzaju elementów jest prostota ich składania i rozkładania oraz krótki czas wykonania zapory, ponadto rozbudowa inżynieryjna prowadzona z wykorzystaniem wyżej wymienionych barier może być prowadzona w sposób modułowy.

Kolejnym elementem ochrony biernej było wyznaczenie na terenie obozu stref bezpieczeństwa, gdzie obowiązywała zasada szczególnej kontroli zasadności przebywania. W bazie Echo dokonano podziału na trzy strefy: I strefa bezpieczeństwa objęła rejon kancelarii tajnej, węzeł łączności; w II strefie bezpieczeństwa znalazły się sztab, kancelaria dowódcy, skład amunicji; natomiast III strefa administracyjna obejmowała rejon rozmieszczenia pododdziałów. Wejście do poszczególnych stref było możliwe jedynie po okazaniu identyfikatora. Każdy żołnierz i pracownik przebywający na terenie bazy musiał posiadać w widocznym miejscu identyfikator zezwalający na wejście do danej strefy. Jak z powyższego wynika, nie każdy miał dostęp do wszystkich stref i było to ściśle przestrzegane.

System ochrony biernej, zewnętrznej obozu Echo obejmował podsystem umocnień inżynieryjnych, podsystem punktów kontrolnych, wieże obserwacyjne, ogrodzenia, zapory małowidoczne oraz podsystem min sygnalizacyjnych, które zapewniały ochronę bierną obozu.

Przedsięwzięcia ochrony czynnej, mające zapewnić właściwy poziom bezpieczeństwa wojsk w obozach wojskowych obejmowały: posterunki przy bramach wjazdowych do obozu, posterunki obserwacyjne rozmieszczone wokół obozu jak również patrole piesze, patrole na pojazdach, posterunki kontrolne przy strefach I i II. Każda baza dywizji objęta była stałym - 24 godzinnym systemem wartowniczym polegającym na obserwacji z wież i posterunków obserwacyjnych, pokrywających cały obszar wokół obozu, uniemożliwiając tym samym ewentualne próby jego penetracji.

Wieże obserwacyjne w bazie Echo znajdowały się w newralgicznych miejscach obozu. Wartownicy na wieżach mieli określone sektory obserwacji oraz w razie niebezpieczeństwa mogli udzielić pomocy wartownikowi pełniącemu służbę na sąsiednim

posterunku. Wszystkie wieże objęte były zasadą wzajemnej widoczności. W porze nocnej na wszystkich wieżach byli wartownicy, zaś w dzień tylko znajdujące się w newralgicznych punktach. Wynikało to przede wszystkim ze szczupłości sił jakie można było wykorzystać do ochrony bazy. Obszar bazy był otoczony wysokim murem z elementów żelbetonowych tzw. „Alaska Barier" o wysokości 3,7 m, który uniemożliwiał obserwację wzrokową osobom przebywającym na zewnątrz bazy, a tym samym podnosił poziom bezpieczeństwa bazy.

Do bazy prowadziły dwie bramy na których zorganizowano punkty kontrolne stworzone w celu kontroli ruchu pojazdów i personelu wjeżdżającego i wyjeżdżającego z bazy. Ich zadaniem było uniemożliwienie nielegalnego przewozu i wywozu mienia, a także zabezpieczenie wjazdu przed bezpośrednim atakiem terrorystycznym z użyciem pojazdów przystosowanych do ataków samobójczych – VBIED (ang. V*ehicle Borne Improvised Explosive Devices*). Ponadto zapobiegały wnoszeniu na teren bazy urządzeń i materiałów do konstrukcji min pułapek. Oczywiście system ochrony zewnętrznej bazy był dostosowany do warunków terenowych panujących w Ad Diwaniyah oraz lokalizacji bazy. Cały ruch samochodowy odbywał się praktycznie jedynie przez bramę południową, zaś brama północna była bramą alarmową oraz służyła do wpuszczania i kontroli Irakijczyków zatrudnionych w bazie oraz kupców handlujących w wydzielonym dla nich miejscu na skraju bazy. Wokół bazy postawione były pola minowe z min sygnalizacyjnych oraz wykopany był rów.

Dodatkowo, w skład systemu ochrony czynnej bazy Echo wchodziły wydzielone mobilne i stacjonarne siły ochrony oraz wystawiane całodobowe służby dyżurne. Skład systemu ochrony był następujący:

- posterunki wartownicze wewnętrzne;
- patrole piesze;
- pododdział reagowania, przeznaczony do wzmocnienia ochrony w momencie otrzymania sygnału o zagrożeniu oraz w razie wystąpienia zagrożenia pożarowego. Pododdział utrzymywał gotowość do działania w czasie 30 minut od otrzymania sygnału;
- siły szybkiego reagowania dywizji – wystawiane przez Samodzielną Grupę Powietrzno – Szturmową. W swoim zestawie miał do dyspozycji możliwość wykorzystania śmigłowca W3-W „Sokół" lub Mi -24 oraz śmigłowca Mi-8. Siły były uruchamiane przez centrum operacyjne dywizji. Gotowość do działania 15 minut od otrzymania sygnału;

- grupy specjalne – wystawiane przez kompanię specjalną. Uruchamiane przez centrum operacyjne dywizji. Gotowość do działania 15 minut od otrzymania sygnału.

Tabela 3.1.

Zadania rutynowe realizowane w tygodniu

ZADANIA	BAZA ECHO	BAZA DELTA
Ilość żołnierzy dziennie zaangażowanych w przedsięwzięcia FORCE PROTECTION	~ 170	~ 180
Wieże	48	90
Bramy	66	45
QRF Wysuniętych baz operacyjnych /FOBs QRF/	20	30
QRF powietrzny / lądowy	30	-
Inne /TOC, Ochrona stołówki, patrole wewnętrzne i inne/	6	18

źródło: opracowanie własne na podst. materiałów z przekazania V zmiany PKW Irak

Oczywiście każda kolejna zmiana w Iraku miała inny skład sił wyznaczonych do ochrony, a zależało to w szczególności od posiadanych pododdziałów oraz sprzętu.

Do systemu ochrony zewnętrznej bazy należy również zaliczyć system posterunków (punktów) kontrolnych (ang. *Check Point*), które były jednym z najważniejszych, a jednocześnie skutecznym sposobem ograniczania i kontroli aktywności przeciwnika w wyznaczonej strefie odpowiedzialności.

Posterunki kontrolne organizowane były w celu:

- uniemożliwienia przejazdu sprzętu wojskowego, amunicji, uzbrojenia, materiałów wybuchowych przez strefę;
- prowadzenie obserwacji wszelkich zdarzeń w terenie;
- demonstrowanie obecności sił pokojowych stronom konfliktu i ludności cywilnej;

Do podstawowych zadań posterunków kontrolnych należała:

- kontrola ruchu wszystkich pojazdów i osób przejeżdżających lub przechodzących przez posterunki kontrolne;
- zapobieganie przemytowi broni i materiałów wybuchowych;
- prowadzenie ewidencji ruchu pojazdów wojskowych stron konfliktu;
- współdziałanie z innymi posterunkami kontrolnymi w trakcie wykonywania rutynowych zadań;

- składanie meldunków o wszystkich ważnych zdarzeniach.

Posterunki kontrolne stanowiły wrażliwy punkt ochrony i obrony bazy, dlatego tak duże znaczenie przywiązywano do ich rozbudowy inżynieryjnej, zapewniającej z jednej strony ochronę żołnierzy pełniących służbę, z drugiej strony skuteczne wykonywanie przez nich powierzonych obowiązków.

Punkty obserwacyjne rozlokowywano w miarę możliwości w dominujących punktach terenowych w sposób umożliwiający prowadzenie dookolnej obserwacji terenu. W początkowym okresie misji punkty budowano z gotowych elementów dostarczanych przez kontraktorów lub sporządzane były we własnym zakresie z drewna i sklejki, a następnie wykorzystywano do tego celu kosze brezentowe wzmocnione siatką metalową do których wsypuje się piasek tzw. *„Hesco Bastion"* i worki z piaskiem.

Podczas początkowego okresu trwania misji w Republice Iraku nie ustrzeżono się błędów przy organizacji punktów kontrolnych. Błędy te polegały zarówno na niewłaściwym rozmieszczaniu punktów kontrolnych, jak i brakach w ich wyposażeniu i słabym wyszkoleniu żołnierzy. Część punktów kontrolnych wystawiono zbyt blisko miejsc zakwaterowania i pracy. Przykładem są obozy dyslokowane w Karbali (INDIA, JULIET, KILO), w których to bazach każda eksplozja na którymkolwiek punkcie kontrolnym groziła dużymi stratami wśród wojsk koalicji. Dodatkowo występowały utrudnienia w zorganizowaniu dla punktów kontrolnych stref przeszukiwania pojazdów, oddalonych bezpiecznie od punktów kontrolnych i pochłaniających energię ewentualnego wybuchu. W kilku przypadkach strefy te znajdowały się na terenie punktów kontrolnych, co w razie wybuchu groziło śmiercią i ranami wśród załogi punktu kontrolnego. W części punktów kontrolnych brakowało specjalistycznego wyposażenia pozwalającego wykrywać samochody pułapki. Z kolei brak ciężkiego/szybkostrzelnego uzbrojenia utrudniał skuteczne powstrzymywanie samochodów pułapek próbujących przełamać systemy obrony obozów. Nie zawsze żołnierze pełniący służbę na punktach kontrolnych posiadali wystarczającą wiedzę i umiejętności pozwalające rozpoznawać samochody pułapki.[1]

Jednym z działań kluczowych większości operacji pokojowych jest patrolowanie. Siły pokojowe nadzorujące wypełnianie postanowień umów między stronami konfliktu realizują powyższe zadania między innymi poprzez patrolowanie. Istotą patrolowania jest zapewnienie pełnej kontroli w strefie nie pokrytej systemem posterunków kontrolnych i obserwacyjnych.

Do celów patrolowania należy zaliczyć:

---

[1] Górniak D., *Ochrona wojsk. Doświadczenia I zmiany Polskiego kontyngentu Wojskowego w Iraku*, Warszawa 2006.

- utrzymanie pełnej kontroli nad strefą;
- demonstrowanie obecności sił pokojowych wszystkim stronom konfliktu w rejonie operacji;
- zbieranie informacji i badanie incydentów;
- powstrzymanie incydentów i ochrona miejscowej ludności;
- utrzymanie przyjacielskich stosunków z ludnością zamieszkującą strefę odpowiedzialności.

Do zadań patroli można zaliczyć:

- nadzorowanie strefy niepokrytej obserwacją prowadzoną przez posterunki kontrolne lub obserwacyjne;
- monitorowanie sił stron walczących;
- wyjaśnianie incydentów i reagowanie na zamieszki cywilne;
- zbieranie informacji i meldowanie;
- wspieranie organizacji pozarządowych;
- nadzorowanie dystrybucji pomocy humanitarnej;

Nieodzownym elementem każdej misji jest prowadzenie działań konwojowych. W celu niedopuszczenia do niespodziewanego ataku przeciwnika oraz zminimalizowania skutków jego uderzeń, a tym samym ograniczenia strat podczas transportu z zaopatrzeniem samochodami ciężarowymi, eliminowano pojedynczy, niezorganizowany ruch pojazdów na rzecz ich przemieszczania w zbiorowych konwojach.

Konwój to grupa osób odpowiednio wyposażona, posiadająca wewnętrzną hierarchiczną strukturę, działająca według określonej taktyki, wyznaczona rozkazem dziennym dowódcy jednostki wojskowej do konwojowania mienia wojskowego[2].

Konwój (eskorta) w działaniach sił koalicyjnych /pokojowych/ – to kolumna odpowiednio oznakowanych pojazdów, chronionych przez wyznaczonych żołnierzy.

Głównym zadaniem eskorty jest zapewnienie bezpiecznego i terminowego przemieszczenia kolumny do wyznaczonego punktu lub rejonu. Trasa przejazdu konwoju musi być naniesiona na mapę dowódcy eskorty. Każda zmiana jej przebiegu musi zostać zaznaczona na mapie, a dowódca w miarę możliwości, powinien jak najszybciej poinformować przełożonego poprzez środki łączności o zaistniałym fakcie.

Konwój organizuje się w celu:

- ewakuacji ludności cywilnej z zagrożonych rejonów;

---

[2] *Instrukcja o ochronie obiektów wojskowych*, Szt.Gen. 1569/2004, Warszawa 2004, s. 73.

- przewozu zaopatrzenia dla rozmieszczonych w strefie buforowej wojsk własnych;
- dostarczenia pomocy humanitarnej dla ludności cywilnej.

Działalność logistyczna wielonarodowej dywizji skupiała się na planowaniu, organizowaniu, realizowaniu oraz monitorowaniu konwojów z dostawami żywności, paliw, materiałów fortyfikacyjnych i innych środków materiałowych w rejonie odpowiedzialności MND CS. Konwoje obejmowały dostawy zarówno dla wojsk koalicji, jak również pomoc (np. paliwo, woda, pomoc humanitarna itd.) dla ludności cywilnej zamieszkującej prowincje w rejonie odpowiedzialności dywizji.

Przemieszczanie konwojów w rejonie odpowiedzialności dywizji realizowano według ogólnych zasad dotyczących organizacji marszu. Prędkość przemieszczania zależała od rodzaju środków transportowych, stanu dróg, warunków meteorologicznych, pory roku, stanu technicznego pojazdów oraz umiejętności kierowców. Do ochrony pojazdów konwoju wyznaczano z reguły pododdział w sile wzmocnionego plutonu. Pododdział wyznaczony do ochrony konwoju otrzymywał zadanie ochrony konwoju wzdłuż trasy przemieszczania zwłaszcza przez niebezpieczne rejony. W celu zminimalizowania zagrożenia atakami dowództwo MND CS opracowało i wdrożyło do realizacji procedury dotyczące organizacji i przemieszczania konwojów.

źródło: MND(CS) SOP FORCE PROTECTION

Rys. 3.3. Organizacja konwoju wykonującego zadanie w czasie dnia.

Do konwoju wyznaczano minimum dwa transportery opancerzone bez względu na porę dnia. W każdym pojeździe było minimum trzech uzbrojonych żołnierzy. Jeden lub więcej transporter utrzymywał łączność przez radio z siłami koalicji. Konwój do miejsc niebezpiecznych (Bagdad, Karbala, Nadżaf) osłaniany był przez minimum trzy transportery. Oczywiście były to minimalne wymagania, ale w praktyce celem podniesienia bezpieczeństwa konwojów, ilość pojazdów opancerzonych wydzielanych do ochrony była znacznie większa.

Warto zauważyć, że do realizacji przedsięwzięć związanych z ochroną zewnętrzną wojsk i obozów angażowano duże siły i środki dywizji.

Sprawne funkcjonowanie systemu ochrony wojsk to zasługa nie tylko dowództwa dywizji, które opracowało dokumentację ochrony, ale także skuteczne jej przestrzeganie.

Podstawowym dokumentem normującym zagadnienia z zakresu ochrony wojsk na szczeblu dywizji była instrukcja „*Stałe Procedury Operacyjne Ochrony Wojsk Wielonarodowej Dywizji Centrum - Południe*", w którym zawarte były między innymi:

a) Załącznik A - Stany alarmowe, kody oporządzenia, kody ruchu pojazdów;
b) Załącznik B - Stany alarmowe - minimalne środki ochronne;
c) Załącznik C - Sygnały zagrożenia NBC;
d) Załącznik D - Środki bezpieczeństwa dla miejsc szczególnie zagrożonych;
e) Załącznik E - Ochrona obozów wojskowych;
f) Załącznik F - Uzbrojenie i taktyka działania;
g) Załącznik G - Oznakowanie dokumentów niejawnych;
h) Załącznik H - Ochrona informacji niejawnej;
i) Załącznik I - Bezpieczeństwo systemów informacyjnych;
j) Załącznik J - Działania podejmowane po zaistnieniu wypadku drogowego z udziałem miejscowej ludności;
k) Załącznik K - Skład i zadania grupy doradzania w zakresie Force Protection;
l) Załącznik L - Proces Force Protection.

Na podstawie tych dokumentów komendanci poszczególnych obozów opracowywali dla każdego z nich „*Plan ochrony i obrony bazy*". W planach tych szczegółowo były określone:

- zagrożenia występujące w rejonie odpowiedzialności;
- zasady użycia siły (ang. *Rules of engagement - ROE*);
- system ochrony i obrony baz;
- siły i środki do realizacji funkcji ochronnych i obronnych;
- procedury postępowania w przypadku zagrożenia atakami terrorystycznymi i działaniami dywersyjnymi;
- system alarmowania;
- organizacja konwojów;
- instrukcje przeciwpożarowe;
- wzory przepustek.

Poza wyżej wymienionymi dokumentami zasadniczymi, opracowano szereg dokumentów pomocniczych. Wypracowali je specjaliści z poszczególnych komórek organizacyjnych sztabu dywizji oraz batalion dowodzenia, w celu uszczegółowienia przedsięwzięć systemu ochrony wojsk. Do tego typu dokumentów należy zaliczyć: „*Plan rozbudowy inżynieryjnej systemów ochrony i obrony bazy*" (ang. *Force Protection Engineers Project*), „*SOP Force Protection - Procedury*" oraz „*Convoy Commander Handbook*".

Nieco odmiennie wyglądała sytuacja w Afganistanie do czasu przeniesienia się całości polskich sił do Ghazni, czyli do października 2008r. Poszczególne Polskie Grupy Bojowe były rozlokowane w różnych bazach i znajdowały się pod dowództwem amerykańskim. Dla przykładu, w bazie Sharana dokumentem podstawowym z zakresu ochrony bazy był *SOP FOB Sharana /Forward Operating Base Sharana Force Protection Standing Operating Procedures/.* Dodatkowo Zespół Dowodzenia Polskiej Grupy Bojowej opracował *Plan ochrony FOB Warrior*, który zawierał wytyczne w zakresie ochrony bazy w stałej gotowości bojowej oraz załączniki:

a) Załącznik nr 1 – Graficzny plan ochrony;
b) Załącznik nr 2 – Sygnały alarmowania i ostrzegania oraz sygnały wewnętrznego ostrzegania;
c) Załącznik nr 3 – Opis stanów zagrożenia alarmowego oraz kodów ubioru, ruchu pojazdów oraz uzbrojenia;
d) Załącznik nr 4 – Wzór tablicy ze stanem zagrożenia alarmowego oraz kodami.

Na podstawie doświadczeń z pierwszych zmian Polskiego Kontyngentu Wojskowego w Iraku, zespół oficerów, który pełnił służbę w Iraku, opracował poradnik pt. „Konwoje, patrole, IED, VBIED, przeszukiwanie, MEDEVAC, SALUTE, IED Report, informacje podstawowe.". Zawiera on praktyczne rady i wskazówki dla żołnierzy, m.in. zestaw wyposażenia, jaki żołnierz wyjeżdżający na działania konwojowe powinien posiadać przy sobie oraz sposoby zachowania się w wypadku ataku na konwój. Wyposażenie indywidualne żołnierza w konwoju, patrolu składa się m.in. z broni, amunicji, granatów, świec dymnych i ręcznych pocisków typu HLZ, hełmu, kamizelki kuloodpornej, gogli, rękawiczek taktycznych, opatrunku osobistego, maski przeciwgazowej, urządzenia do wskazywania własnego położenia dla lotnictwa, tabliczki identyfikacyjnej, ID, numeru telefonu do centrum operacyjnego i MEDEVAC. Dodatkowo na każdym pojeździe: apteczka, pistolet sygnałowy oraz sucha racja żywnościowa i 4 butelki wody na żołnierza.

- wyposażenie dodatkowe dla dowódcy konwoju:

- telefon satelitarny THURAYA;
- pozwolenie na opuszczenie strefy (wg potrzeb);
- lornetka;
- dane radiowe – tylko wyciąg;
- rozkaz wyjazdu;
- mapa lub szkic z aktualną sytuacją wzdłuż drogi marszu;
- GPS (zaprogramowane dane dotyczące zadania) + baterie.[3]

Analiza systemu ochrony i obrony bazy wojskowej dokonana przez zespół autorski dowodzi, że przyjęty system przedsięwzięć bezpieczeństwa zapewniał skuteczną ochronę żołnierzom i pracownikom przebywającym w bazie. Zastosowane rozwiązania systemowe pozwalały na szybką reakcję na występujące zagrożenia. Zagadnienia z zakresu ochrony wojsk miały odzwierciedlenie w szeregu dokumentów, które regulowały zasady postępowania na wypadek zaistnienia różnych niebezpiecznych sytuacji, takich jak np. atak na bazę, atak na patrol lub konwój, czy pożar. Przeprowadzone badania dowiodły, że bardzo istotnym aspektem zapewnienia bezpieczeństwa w bazach jest ochrona bierna.

3.3.2. Analiza środowiska bezpieczeństwa

W każdej bazie wojskowej można wyróżnić obszary podlegające szczególnej ochronie, rejony lub miejsca przeznaczone do zapewnienia sprawnego funkcjonowania bazy i misji oraz obszary, w których ryzyko wystąpienia niekorzystnych zjawisk jest podwyższone.

Analizując ochronę bazy PKW w Iraku, do obszarów chronionych możemy zaliczyć przede wszystkim pomieszczenia dowództwa i sztabu, centrum operacyjnego, węzeł łączności, kancelarię tajną, magazyny amunicji i materiałów wybuchowych oraz magazyny żywnościowe. Do newralgicznych miejsc należy zaliczyć także stołówkę żołnierską, podczas spożywania posiłków. Ochrona tych miejsc polegała głównie na ochronie czynnej, czyli wystawianiu posterunków wartowniczych. Wejście do nich możliwe było tylko po okazaniu przepustki.

W bazach wojskowych z uwagi na duże zagrożenie atakami terrorystycznymi można wyróżnić dwa obszary podlegające ochronie, będą to obszary funkcjonalne, tam gdzie funkcjonują dowództwa i obszary zakwalifikowane do konfliktowych.

---

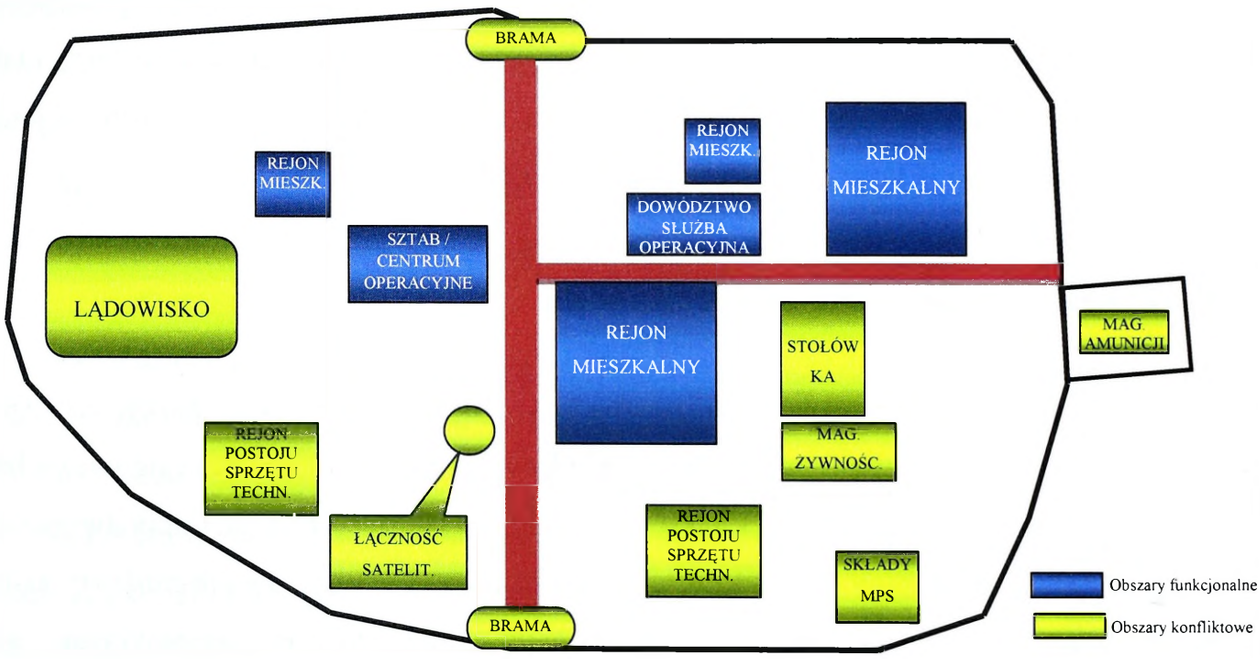
[3] *Konwoje, patrole, IED, VBIED, przeszukiwanie, MEDEVAC, SALUTE, IED Report, informacje podstawowe*, Warszawa 2004, s. 9.

Do obszarów funkcjonalnych na przykładzie bazy Echo można zaliczyć: centrum operacyjne /*ang. Tactical Operation Center*/, miejsca pracy poszczególnych komórek sztabu, miejsca przeznaczone na zakwaterowanie żołnierzy oraz postój sprzętu technicznego.

Do obszarów konfliktowych zaliczono przede wszystkim bramy, na których zorganizowano punkty kontrolne, wytypowane najbardziej prawdopodobne miejsca podkładania IED oraz miejsca, z których rebelianci prowadzili ostrzał bazy.

Obszary funkcjonalne i konfliktowe były miejscami, które w szczególny sposób ze względu na ich przeznaczenie, podlegały monitorowaniu.

Zarówno obszary funkcjonalne, jak i obszary konfliktowe należy zaliczyć do obszarów chronionych, czyli podlegających szczególnej ochronie.



źródło: opracowanie własne
Rys. 3.4. Obszary funkcjonalne i konfliktowe bazy Echo

3.3.3. Analiza miejscowej ludności

Bardzo duże znaczenie dla prowadzenia działań ma wcześniejsza analiza ludności zamieszkującej teren planowanej misji. Niezbędna przy tym jest znajomość kultury, przekonań religijnych oraz zwyczajów tubylców. Żołnierze jeszcze przed wyjazdem na misję zapoznawani są z zagadnieniami związanymi z kulturą i religią państwa, w której planowany jest ich udział.

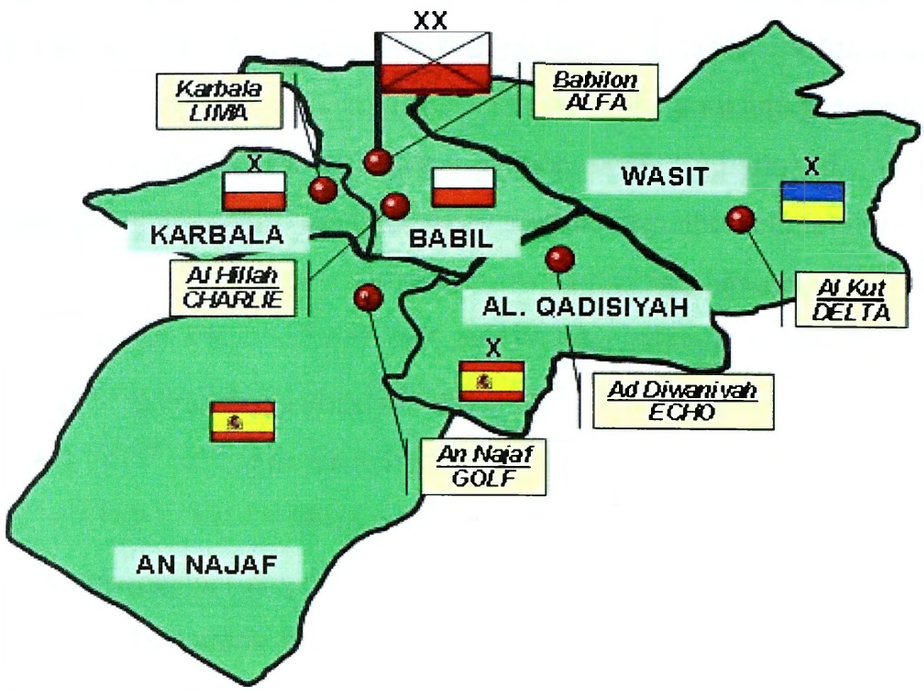
Przygotowanie żołnierzy do każdej misji wymaga zapoznania ich z problematyką, dotyczącą kultury i obyczajów panujących w rejonie misji. Dlatego też podczas szkolenia omawia się następujące zagadnienia:

- historię i współczesność danego państwa (np. Iraku),
- religie i odłamy religijne występujące w strefie stabilizacyjnej,
- prawo danego kraju,
- techniki operacyjne,
- zasady negocjacji i mediacji z miejscową ludnością,
- zasady działania terrorystów na terenie misji,
- zasady bezpieczeństwa misji pokojowej.

Charakterystyka miejscowej ludności rozpoczyna się głównie od podania ogólnych danych o państwie, np. Republika Iraku, to państwo zamieszkiwane przez około 24 mln obywateli. Arabowie stanowią 77 procent ogółu ludności, Kurdowie 19 procent, a 4 procent to Turkmeni, Persowie i Asyryjczycy. Po wojnie w Zatoce Perskiej w 1991 roku, Kurdowie korzystając z ochrony amerykańskich samolotów utworzyli na północy Iraku Wolny Kurdystan, niezależny od Bagdadu. Większość ludności (ponad 70%) mieszka w miastach. Blisko 40% ludności w wieku powyżej 15 lat nie umie czytać i pisać.

Następnie można scharakteryzować poszczególne zagadnienia dotyczące religii, prawa, ustroju, mentalności itp. Charakterystyka religii Iraku jest stosunkowo prosta i jasna. Dominującą w Iraku religią jest islam. Muzułmanie stanowią 96 proc. społeczeństwa, ale są podzieleni. Największą grupę religijną - około 62% - stanowią szyici, mieszkający głównie w południowym Iraku. Ale krajem rządzą sunnici, stanowiący ok. 35% mieszkańców kraju. Chrześcijanie i wyznawcy innych religii stanowią 3% społeczeństwa.

W czasie trwania misji stabilizacyjnej, w której brało udział polskie wojsko, zmianie uległy zarówno zadania, jak i wielkość strefy odpowiedzialności. W końcowym etapie misji Międzynarodowa Dywizja odpowiadała już tylko za ochronę dwóch środkowo – południowych prowincji: Wasit i Al Quadisiyah, zajmujących obszar 24 263 km^2 i zamieszkałych przez ok. 1,1 mln Irakijczyków.



źródło: http://www.pkwirak.wp.mil.pl/pl/27.html

Rys. 3.5. Strefa odpowiedzialności Międzynarodowej Dywizji Centrum – Południe w czasie I zmiany PKW Irak.

Strefa środkowo – południowa, w której przyszło służyć polskim żołnierzom, prawie w całości jest zamieszkana przez ludność arabską, z czego 85% mieszkańców to szyici. Strefa miała zatem prawie jednorodny, szyicki charakter. W okresie reżimu Saddama Husajna, sunnici zamieszkujący głównie centrum kraju, sprawowali władzę i pełnili role gwaranta integralności terytorialnej Iraku. Natomiast szyickie południe, po krwawo stłumionej rewolcie 1991 r., było obiektem represyjnej polityki i w konsekwencji chronicznie niedoinwestowane. Powyższe zjawiska z różnym natężeniem wpłynęły na stan rozwoju prowincji. Obszar ten nie posiada ośrodka administracyjnego porównywalnego z Bagdadem, czy też Basrą. Do ważnych ośrodków miejskich należą Al Kut, Al Hillah, Ad Divanijah, An Nadżaf i Karbala.

W głównych miastach kultu religijnego szyitów - Karbali i An Najaf, nastawienie miejscowej ludności do wojsk koalicyjnych było raczej negatywne. W miejscach bezpośrednio przylegających do świątyń szyickich obecność wojsk była niepożądana, a siły koalicyjne uznawane były za siły okupacyjne. O takim nastawieniu świadczą antyamerykańskie wystąpienia szyitów w Karbali. Ich działania inspirowane były głównie przez mułłów, którzy w trakcie cotygodniowych kazań w meczetach udzielali „instruktaży" dotyczących postępowania wobec wojsk koalicji.

Charakteryzując ludności należy określić nastawienie jej do wojsk wielonarodowych. W misji stabilizacyjnej w Iraku duża część ludności uważała wojska koalicyjne jako najeźdźców i odnosiła się do żołnierzy polskich wrogo. Pełnienie służby w takich warunkach

było niezwykle trudne, gdyż trudno było odróżnić przyjaciela od wroga. Częstym przejawem nienawiści było chociażby obrzucanie polskich patroli kamieniami przez młodzież i dzieci. Trudną kwestią była również odmienność religijna. Dlatego ważne było poznanie zwyczajów religijnych jeszcze przed wyruszeniem na misję, ażeby nie popełnić jakiegoś „faux pas". To co jest przyjęte w polskiej kulturze może być uznane za nietakt w Iraku. W codziennych kontaktach należy zachować powściągliwość, uprzejmość i w żadnym razie nie okazywać wyższości. Należy unikać wszelkich zgromadzeń i demonstracji, a także nie wchodzić do meczetów, zwłaszcza w porze modlitw. Praktycznie obowiązuje zakaz spożywania alkoholu w miejscach publicznych. W okresie ramadanu (święty miesiąc postu muzułmanów) nie powinno się w miejscach publicznych, a zwłaszcza w okolicach meczetów, palić papierosów, spożywać pokarmów, alkoholu i innych napojów. Te zakazy dotyczą w szczególności takich miast jak Nadżaf, Karbala, Kufa.

Analiza zachowań ludności, to nie tylko zachowania religijne, ale także aktywność ludności niesprzyjającej Irakowi. Siły antyirackie działały głównie takich miejscach jak Bagdad, Faludża, Karbala i Nadżaf. Na tę sytuację wewnątrz strefy wpływało również bezpośrednie graniczenie z Iranem. Do niebezpiecznych rejonów w naszym obszarze należały: północno-zachodni i centralny Wasit oraz zachodnia Al Diwaniyah. Główne zagrożenie stanowili ekstremiści islamscy, radykalni działacze Armii Mahdiego (Mahdi Militia)[4] oraz byli funkcjonariusze reżimu Saddama Husajna.

Dodatkową trudnością była wszechobecna korupcja panująca w instytucjach państwowych, np. w wojsku i policji. Istniała zasada „ograniczonego zaufania" do przedstawicieli tych instytucji. Poza tym, wielu przede wszystkim policjantów w prowincjach administrowanych przez Polaków, należało do organizacji radykalnego duchownego szyickiego Muktady as - Sadra. Ten młody przywódca w kwietniu 2004 r. stanął na czele rebelii przeciw obecności sił USA i całej koalicji w Iraku. Jego oddziały atakowały między innymi polskich żołnierzy w Karbali i bazie Babilon.

Niezwykle ważnym czynnikiem był proces zubożenia społeczeństwa, który tworzył korzystne warunki dla powstawania pospolitych grup przestępczych. Obok ataków na konwoje z pomocą humanitarną tworzył się „czarny rynek" i rozwijała się działalność przemytniczo-mafijna.

---

[4] Szyicka milicja stworzona w 2003 r. i przewodzona przez młodego działacza szyickiego Muktadę Al Sadra. Brała ona udział w dwóch powstaniach przeciwko wojskom koalicyjnym. Część bojowników aktywnie działała w naszym obszarze, a w szczególności w Ad Diwaniyah, gdzie znajdowało się biuro Sadra.

Podobne, aczkolwiek nie takie same uwarunkowania panują w Afganistanie. Operacja stabilizacyjna w Afganistanie w ramach Międzynarodowych Sił Wsparcia Bezpieczeństwa (*ang. International Security Assistance Force – ISAF*) stanowi dla Sił Zbrojnych RP jedno z największych wyzwań wojskowych ostatnich lat. Misja realizowana jest w warunkach, które pod względem kulturowym, cywilizacyjnym i klimatycznym całkowicie odbiegają od realiów europejskich.

Afganistan zamieszkuje ponad 20 narodów, głównie ludy irańskie z rodziny indoeuropejskiej: Pasztunowie, zwani też Afganami (42% ogółu ludności), Tadżycy (27%), Hazarowie (9%), Beludżowie, Nuristańczycy oraz ludy tureckie z rodziny ałtajskiej: Uzbecy (ok. 9%), Turkmeni i Kirgizi. Większość ludności żyje w strukturach plemiennych, wyznaje islam, który jest religią państwową. Około 84% wyznawców stanowią sunnici, zaś 15% - szyici. Poziom życia ludności i jej zdrowotność należą do najniższych w świecie. Powszechnym zjawiskiem jest analfabetyzm - 79% ogółu ludności.

Mimo rozbicia państwa talibów część bojowników tej organizacji przeczekała amerykański atak i korzystając z warunków terenowych kraju ukryła się w górach, skąd rozpoczęła walkę partyzancką z afgańskim rządem i oddziałami międzynarodowymi stacjonującymi w Afganistanie.

Należy pamiętać, że Afganistan to miejsce światowej produkcji opium (90%), a przetwarzaniem lub handlem narkotyków zajmuje się szacunkowo co dziesiąty Afgańczyk. Korelacja między rejonami, gdzie uprawia się największą ilość opium, a obszarami destabilizacyjnymi jest oczywista. Najbardziej niebezpiecznym rejonem kraju jest prowincja Helmand, która jednocześnie jest potentatem w produkcji opium. Środki finansowe otrzymywane ze sprzedaży narkotyków są źródłem finansowania grup terrorystycznych przez lokalnych watażków, baronów narkotykowych i talibów.

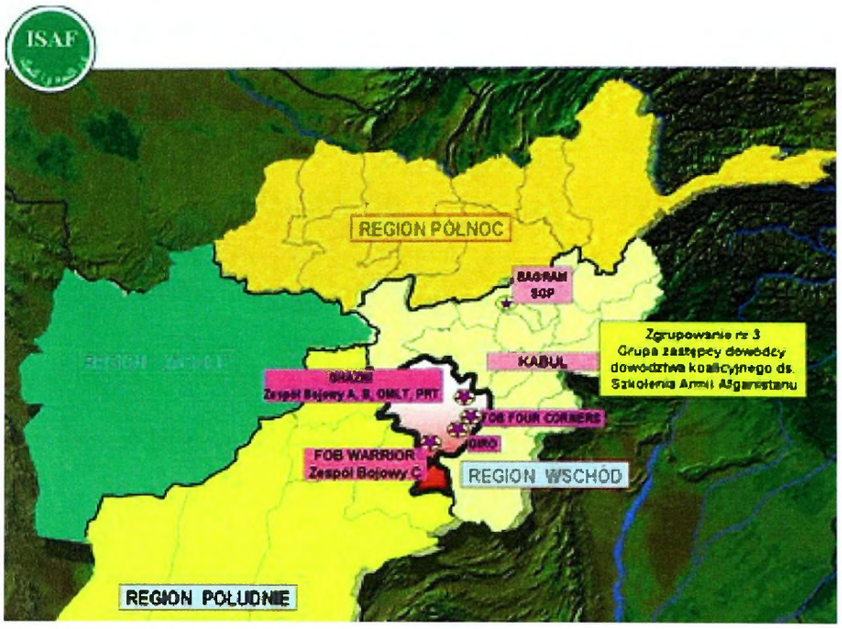
Niestety, sprzedaż narkotyków to niekiedy jedyny sposób uzyskania środków na utrzymanie rodziny. Nadal ponad połowa Afgańczyków żyje w ubóstwie, 40 procent nie ma pracy, a według danych ONZ – 2,5 mln ludności żyje w skrajnej nędzy. Ubóstwo ludności jest największym wrogiem wojsk koalicyjnych. Prawdziwa stabilizacja jest możliwa dopiero wraz z rozwojem gospodarki, która stworzy miejsca pracy oraz szansę rozwoju i normalnej egzystencji, bez konieczności trudnienia się produkcją i sprzedażą narkotyków.

Panujące powszechnie ubóstwo, niedoinwestowanie, brak planów rozwoju powoduje, że nastawienie ludności lokalnej do wojsk koalicyjnych z przychylnej i neutralnej (u Hazarów) lub neutralnej i wrogiej (u Pasztunów) zmieni się na wrogą.

źródło http://pl.wikipedia.org/wiki/Talibowie

Rys.3.6. Terytorium Afganistanu pod kontrolą talibów w 1996 r. (kolor żółty)

Głównymi czynnikami generującymi zagrożenia zbrojne w Afganistanie pozostają działania terrorystyczne talibów, radykalnej frakcji Hizb - i - Islami Gulbuddina Hekmatjara i nieliczne bojówki Al–Kaidy. Zagrożenia generują także organizacje przestępcze oraz tzw. „baronowie narkotykowi". Na terenie Afganistanu działa ok. 1800 nielegalnych formacji zbrojnych, skupiających ponad 70 tys. bojowników. Oprócz grup terrorystycznych, funkcjonują też „prywatne" armie tzw. „baronów narkotykowych" oraz regionalnych przywódców, które również podejmują działania antykoalicyjne. Należy podkreślić, że organizacje terrorystyczne są przygotowane do wykonywania ataków na terytorium całego państwa. Działalność poszczególnych ugrupowań zbrojnych w Afganistanie koncentruje się wzdłuż linii komunikacyjnych oraz kluczowych pozycji sił koalicyjnych i Afgańskich Sił Bezpieczeństwa.



źródło: http://www.isaf.wp.mil.pl/kontyngent.html

Rys. 3.7. Rejony stacjonowania polskich żołnierzy

Dokonując charakterystyki środowiska walki obok wiedzy dotyczącej całego państwa pododdziały wojsk wielonarodowych muszą dokładnie zapoznać się z przydzielonym obszarem do kontroli. Na przykładzie polskiego kontyngentu działającego w Afganistanie zespół autorski krótko scharakteryzuje prowincję i jej otoczenie. Charakterystykę rozpoczniemy od stolicy prowincji.

Ghazni, to dawna stolica potężnego imperium Ghaznawidów sprzed dziesięciu wieków, nie jest głównym polem bitewnym w afgańskiej wojnie. Leżąc z dala od głównych aren wojny, a także od szlaków partyzanckich karawan z afgańsko-pakistańskiego pogranicza, Ghazni uważana jest za prowincję spokojniejszą także niż Paktika, gdzie dotychczas stacjonowali Polacy i przez którą talibowie przeprawiali się w drodze z obozowisk w Pakistanie. Ta licząca prawie 23 tys. km^2 afgańska prowincja jest zamieszkała przez około 1.5 miliona mieszkańców. Jedynie około 50 tys. żyje w mieście, reszta jest rozsiana po całej prowincji, w małych wsiach bądź koczowniczych osadach. Około 49% mieszkańców to Pasztuni, 46% Hazarzy i niecałe 5% Tadżyków. Pasztuni, dumni i honorowi nie uznają zwierzchnictwa Hazara, czy to w armii, czy policji lub w lokalnym rządzie. Polityka ISAF zakłada „mieszanie" etniczne oddziałów, tym samym może się zdarzyć, że Pasztunami będzie dowodził Hazar. Dlatego też jednym z trudniejszych zadań będzie właściwy podział środków pomocowych i w tym obszarze należy być bardzo wyczulonym. Najłatwiej byłoby po prostu postawić na przywódców Pasztunów i problem byłby teoretycznie rozwiązany. Jeżeli nie zadbamy jednak o odpowiedni podział władzy to Pasztuni całą pomoc dla prowincji

przeznaczą na tereny zamieszkałe przez siebie, a nie przez Hazarów – co może rodzić konflikty i wpływać na postrzeganie wojsk koalicji.

Wielkie znaczenie strategiczne Ghazni polega jednak na tym, że biegnie przez nią najważniejsza droga kraju z Kabulu do Kandaharu. Wyrównana i wyasfaltowana przez Amerykanów, uchodzi za symbol wprowadzonych przez nich nowych porządków w Afganistanie. Objęcie Ghazni oznacza, że Polacy przestaną patrolować afgańsko-pakistańskie pogranicze, gdzie roi się od pułapek i zasadzek. W Ghazni ich najważniejszym zadaniem będzie utrzymanie bezpieczeństwa na drodze z Kabulu.

Choć jest to prowincja o małej aktywności oddziałów Talibów, to są tam oni lubiani, zwłaszcza w regionach zamieszkałych przez Pasztunów. Zaraz po Kandaharze, Helmandzie i Nuristani Ghazni jest czwartą prowincją, gdzie największy odsetek ludności wierzy w to co mówią Talibowie (25%). Jeżeli od ogólnej liczby odejmiemy odsetek Hazarów, którzy są w zdecydowanej większości przeciwko Talibom, to okaże się, że około 50% Pasztunów wierzy bardziej Talibom niż rządowi centralnemu.

W Ghazni istnieje podobny problem z miejscową policją, jak w Iraku. Nie można mieć do nich zaufania i należy uważać, czy nie informują np. talibów o wyjeździe patrolu lub nie przekazują innych informacji. Poważne problemy są z dyscypliną, policjanci są wierni powiązaniom klanowym, słabo opłacani, więc jest poważny problem z korupcją. Nagminnym jest, że ze względu na brak pieniędzy na wynagrodzenie dla policjantów, uciekają i przechodzą na drugą stronę, gdzie płacą im więcej. Bardzo często są oni szantażowani albo zastraszani, że np. jeśli będzie pracował dla Amerykanów - zabiją jego rodzinę.

Dużo lepiej sytuacja wygląda z żołnierzami armii rządowej, którzy często są włączani do patroli ze względu na znajomość terenu i łatwość porozumiewania się z cywilami. Polscy żołnierze szanują ich, bo nieraz udowodnili, że potrafią się bić z talibami.

Misja w Afganistanie, która wkroczyła w kolejną fazę jest niewątpliwie bardzo trudną. Jej ciężar to nie tylko zagrożenie ze strony talibów, zamachowców, czy min - pułapek. To także trudności związane z odmiennym klimatem, panującymi chorobami w tamtym rejonie świata, czy dużą wysokością. To prawdziwa próba charakterów. Misja w Iraku była bardzo trudna, ale obecna w Afganistanie jest jeszcze trudniejsza i bardziej niebezpieczna.

3.3.4. Analiza środków ochrony fizycznej wewnętrznej i zewnętrznej

Działania terrorystyczne są niezwykle trudne do przewidzenia. Zazwyczaj nieznane jest miejsce i sposób przeprowadzenia ataku. Przeciwdziałanie zagrożeniom sprowadza się głównie do przedsięwzięć ochrony indywidualnej żołnierzy w sprzęt oraz baz wojskowych w różnego typu urządzenia wspomagających ochronę.

Do urządzeń wspomagających ochronę należy zaliczyć m.in. sprzęt do kontroli osób i pojazdów, taki jak np. bramowe wykrywacze metali, ręczne wykrywacze materiałów wybuchowych czy ręczne wykrywacze metali.

Analizując środki i urządzenia dotychczas wykorzystywane w operacjach wielonarodowych np. w Iraku, należy zauważyć, że dodatkowo system ochrony był wspomagany radiolokatorami pola walki, a później także środkami optoelektronicznymi.

Ten ostatni był wykorzystywany do monitorowania sytuacji wokół bazy Echo. System ten spełnia warunki w zakresie prowadzenia obserwacji w dzień (kamera dzienna) i w nocy (kamera termalna). Praktyczny zasięg, który uzależniony jest od panujących warunków atmosferycznych wynosi 4 – 6 km. System posiada zdolność wykrycia zagrożenia, ale nie posiada możliwości reakcji na nie. System może być wykorzystywany nie tylko do ochrony baz wojskowych poza granicami kraju, ale również do ochrony składów i magazynów w Polsce. W skład systemu wchodzą następujące zasadnicze elementy: maszt przewoźny, stabilizowana optoelektroniczna głowica obserwacyjna, kontener stanowiska operatora, kamera telewizyjna, kamera termalna, dalmierz laserowy, układ stabilizacji, układ śledzenia automatycznego, układ obserwacji dookólnej i sektorowej.

Analizując środki przewidziane do osłony przed oddziaływaniem ogniowym system bezpieczeństwa baz posiadał własne środki rażenia. Wykorzystywano moździerze M-98 kalibru 98 mm i armaty przeciwlotnicze kalibru 23 mm ZU-23-2. Moździerz przeznaczony był do obezwładniania i niszczenia siły żywej oraz sprzętu wojskowego przeciwnika, a także do oświetlania i zadymiania terenu. Środki te były rozmieszczone na stanowiskach ogniowych wewnątrz bazy i służyły do odpowiedzi ogniem w wypadku ataku rebeliantów.

Armaty przeciwlotnicze kalibru 23 mm ZU-23-2 na samochodzie ciężarowym Star wykorzystywane były do osłony nie tylko baz, ale również konwojów w Iraku. Ich mankamentem był brak osłon chroniących załogę. Działko ZU-23-2 przeznaczone było do zwalczania celów niskolecących w odległości do 2,5 km oraz pojazdów opancerzonych na dystansie do 2 km, bezpośredniej osłony wojsk i ważnych obiektów strategicznych przed środkami napadu powietrznego.

W celu maksymalnego zwiększenia bezpieczeństwa polskich żołnierzy, kontyngent otrzymał śmigłowce Mi-24 D, Mi-8 oraz W-3W/WA Sokół, które były wykorzystywane do monitorowania przemieszczających się pielgrzymek do miejsc świętych islamu, m.in. do Karbali podczas święta Ashura[5], monitorowanie dróg po których poruszały się patrole i konwoje, transportu żołnierzy i prowadzenia rozpoznania powietrznego.

Mi – 24 D jest śmigłowcem uderzeniowym przeznaczonym, do zwalczania siły żywej i celów opancerzonych na polu walki i jego bezpośrednim zapleczu, a także wysadzania i osłony desantów taktycznych. Takie też zadania głownie wykonywał. Często był wykorzystywany do odstraszania ewentualnych napastników z uwagi na swój wygląd i przenoszone uzbrojenie.

Kolejny śmigłowiec wykorzystywany w operacjach wielonarodowych, to Mi -8. Jest to dwusilnikowy śmigłowiec wielozadaniowy. Jeden śmigłowiec w wojskowej wersji transportowej może przewieźć 24 żołnierzy z pełnym ekwipunkiem. W Iraku śmigłowce te były w wersji nieuzbrojonej i dlatego musiały latać w asyście śmigłowców Mi - 24 lub W -3W Sokół. Służył głównie do transportu żołnierzy.

Następny śmigłowiec to W-3W/WA Sokół to śmigłowiec przeznaczony jest do realizacji zadań: transportu i desantu siły żywej, sprzętu i zaopatrzenia, ewakuacji, osłony i wsparcia ogniowego sił lądowych, rażenia celów naziemnych, nawodnych i powietrznych, ratownictwa lotniczego i morskiego, rozpoznania radioelektronicznego oraz dowodzenia. Jego uzbrojenie to 23 mm działko GSz-23Ł, z zapasem 250 nabojów o szybkostrzelności 3000-3400 strz/min. Uzbrojenie podwieszane mogą stanowić zasobniki z niekierowanymi pociskami rakietowymi Mars-2M lub UB-16 (16 szt. S-5 kal. 57 mm) albo B8-10 (10 szt. S-8 kal. 80 mm), kasetowe zasobniki bombowe ZR-8 na 120 bomb odłamkowych, zasobniki Platan z minami narzutowymi.

W czasie misji w Iraku Polski Kontyngent Wojskowy nie posiadał na wyposażeniu bezzałogowych aparatów latających i korzystał z rumuńskich środków – BSL Shadow, a w Oddziale Rozpoznawczym dywizji znajdował się rumuński oficer łącznikowy poprzez którego Szef G - 2 stawiał zadania do wykonania lotów rozpoznawczych.

Polski rząd podnosząc poziom bezpieczeństwa sukcesywnie doposażył kontyngent w nowoczesny sprzęt. W czasie trwania misji na wyposażeniu pojawiły się nowe rodzaje sprzętu i uzbrojenia: samochody HMMWV, 40 mm automatyczne granatniki MK-19, kombinezony

[5] Ashura - święto mniejszości muzułmańskiej Shia. Ashura jest najważniejszym wydarzeniem religijnym tej kasty. Celebrują oni śmierć zamordowanego w Karbali wnuka proroka Mahhometa w 680 r. naszej ery.

przeciwwybuchowe, kamizelki kuloodporne typu KLV, sprzęt noktowizyjny nowej generacji i nowoczesny sprzęt łączności (terminale łączności satelitarnej, radiostacje KF/UKF).

Pojazdy typu HMMWV, przeznaczone były do transportu żołnierzy oraz prowadzenia działań rozpoznawczych i patrolowych i mimo, że nie były to pojazdy najnowocześniejsze, to podniosły znacznie bezpieczeństwo żołnierzy w Iraku.

Pojazd ten produkowany jest w kilku wersjach, z których najbardziej popularny jest model M1025A2/26, zapewniający II poziom bezpieczeństwa. W te pojazdy wyposażeni byli żołnierze Polskiego Kontyngentu Wojskowego w Iraku oraz zdecydowana większość żołnierzy USA. Najnowsza wersja HMMWV – model M1114 charakteryzuje się lepszymi parametrami technicznymi oraz opancerzeniem zapewniającym V poziom bezpieczeństwa.

Zdając sobie sprawę z niedoskonałości popularnego Humvee, starano się własnymi siłami i środkami doskonalić opancerzenie pojazdów. Doświadczenia wyniesione z Iraku, spowodowały, że na kolejną misję w Afganistanie polscy żołnierze pojechali wyposażeni w nowe, spełniające wymagania bezpieczeństwa pojazdy typu Rosomak.

W 2003 r. zostały opracowane, a następnie skierowane na misję zmodernizowane transportery BRDM – 2 o nazwie Szakal. Posiada ona silnik Iveco Aifo 8040SRC, klimatyzację przedziału załogi, nowe akumulatory, uzbrojenie w postaci 12,7 mm wkm NSW (z zapasem 500 naboi) i 7,62 mm km PKT (2000 naboi) z celownikiem dzienno-nocnym CDN-1, przyrządy obserwacyjne kierowcy PNK-72 i dowódcy POD-72, system łączności wewnętrznej Fonet, radiostację pokładową RRC-9500 i przenośne radio R-3501.

Nieco inne, aczkolwiek podobne wyposażenie ochronne żołnierzy używane jest w operacji wielonarodowej w Afganistanie. Bazy w Afganistanie są wyposażone w urządzenia wspomagających ochronę, takie jak skanery do kontroli osób i pojazdów, czy wykrywacze materiałów wybuchowych i metali.

Dodatkowo w wysuniętej bazie Sharana sprawdzano pracowników kontraktowych sprawdzano na bramie wejściowej za pomocą skanerów siatkówki oka oraz odcisków linii papilarnych, gdyż dla żołnierzy kontyngentu wszyscy Afgańczycy są bardzo podobni do siebie i trudno ich zidentyfikować po wyglądzie zewnętrznym.

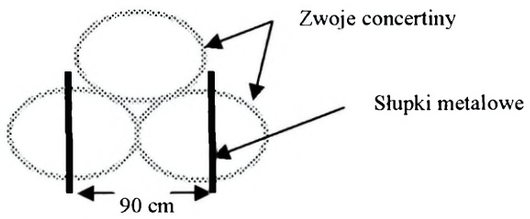
W Afganistanie do ochrony baz dotychczas używane były i są następujące rodzaje zapór i fortyfikacji:

- pola minowe /mine fields/;
- zapory z płotów /fences/;
- zapory z concertiny /concertina/;

- hesco bastiony /hesco walls/;
- ściany betonowe /T- walls/;
- osłony ogniowe /revetments/.

Część pól minowych ustawionych jeszcze przez Rosjan w pobliżu starych baz lub wewnątrz. Celowo ich nie rozminowano, aby można było je wykorzystać ich do podniesienia poziomu bezpieczeństwa.

Zapory z płotów były stosowane np. w bazie FOB Warrior na przemian z zaporami z concertiny. Pierwsza linia zapór była zbudowana z concertiny (dwa zwoje na dole i trzeci na nich), druga linia to płoty z siatki, które w górnej części były zakończone drutem kolczastym lub concertiną, trzecia linia to concertina ułożona w taki sam sposób jak linia pierwsza.



źródło: Sharana FP SOP

Rys.3.8. Sposób wykonania zapory z concertiny

Płoty stosowane do chronienia obiektów przed penetracją wzrokową dodatkowo pokrywa się drobną siatką plastikową.

Amerykanie w Afganistanie najczęściej stosują hesco bastiony w trzech rozmiarach:

- małe: szerokość – 61cm, grubość – 61 cm, wysokość – 61,5 cm;
- średnie: szerokość – 54 cm, grubość – 106 cm, wysokość – 132 cm;
- duże: szerokość – 107cm, grubość – 211 cm, wysokość – 217 cm.

Osłony ogniowe stosowane były i są do osłony pojazdów przed skutkami ataków, tzw. „efekt domino", kiedy od jednego trafionego pojazdu, uszkadzają się kolejne pojazdy stojące w pobliżu.

System ochrony baz w Afganistanie był i jest podobny do rozwiązań zastosowanych w Iraku. System ochrony także jest wspomagany przez system elektroniczny i ogniowy. Do osłony np. w bazie Sharana wykorzystywano amerykańskie radarów artyleryjskich Q - 36 i Q – 37, lokalizujące miejsca stanowisk ogniowych. Natomiast do osłony baz wykorzystywano haubice M119 A2 105 mm i moździerze 120 mm oraz polskiej produkcji moździerze M-98

Podobnie jak w Iraku, w czasie trwającej misji w Afganistanie następowała stała i znacząca poprawa zarówno wyposażenia indywidualnego żołnierzy (np. nowoczesne kamizelki kuloodporne, karabinki Beryl), jak i zbiorowego (np. Rosomaki).

Dla potrzeb Polskiego Kontyngentu Wojskowego w Afganistanie przeznaczono najnowocześniejsze uzbrojenie i wyposażenie, jakie znajduje się na wyposażeniu Wojska Polskiego. Dokonano także szeregu zakupów oraz dostosowania posiadanego wyposażenia do warunków, w jakich polscy żołnierze pełnią służbę w Afganistanie. Ponadto w celu maksymalnego zwiększenia bezpieczeństwa polskich żołnierzy, kontyngent otrzymał najnowocześniejszy, dostępny sprzęt, w tym m.in.:

- transportery ROSOMAK;
- pojazdy opancerzone typu HUMMER;
- wozy pomocy medycznej RYŚ;
- trały przeciwminowe BOŻENA;
- pojazdy opancerzone DZIK;
- zestawy artyleryjskie ZU-23-2;
- 40 mm moździerze Mk -19 (MARK - 19);
- 7,62 mm karabiny maszynowe;
- granatniki RPG-7 i Pallad-M;
- broń osobistą: 9 mm pistolety WIST, 5,56 mm kbs Beryl i Mini-Beryl;
- kamizelki kuloodporne i hełmy kompozytowe;
- kamery i gogle noktowizyjne;
- środki łączności zapewniające łączność satelitarną i radiową;
- urządzenia zakłócające odpalanie improwizowanych ładunków wybuchowych;
- urządzenia określające położenie wojsk własnych;
- systemy zobrazowania pola walki;
- systemy naprowadzania i wskazywania celów na podczerwień;
- system lokalizacji strzelca i wybuchu;
- sprzęt noktowizyjny umożliwiający prowadzenie działań w nocy;
- środki łączności satelitarnej;
- Mobilne Moduły Stanowisk Dowodzenia;
- Systemy Wspomagania Dowodzenia;
- Zintegrowane Węzły Teleinformatyczne;
- radiostacje krótkofalowe i ultrakrótkofalowe do łączności z lotnictwem.

Na potrzeby PKW Afganistan zostały specjalnie przygotowane do działań w ramach ISAF śmigłowce Mi-17-1V. Przystosowano je do lotów w nocy, dodatkowo wyposażając śmigłowce w okularowy wzmacniacz obrazu NVG. Wprowadzono dodatkowe uchwyty zwiększające możliwość wykorzystania w działaniach desantowych i osłonowych, zainstalowano zintegrowany system łączności, zainstalowano środki ochrony własnej oraz system identyfikacji „swój – obcy" SUPRAŚL.

Jednym ze skuteczniejszych pojazdów opancerzonych jest Rosomak. Uzbrojony w wieżę z działkiem 30 mm sprawdza się w działaniach bojowych i sieje postrach wśród talibów, którzy nazwali go "zielonym czołgiem". Jest to pojazd bardzo nowoczesny pod względem technologii wojskowej. Można swobodnie prowadzić go w nocy. Kierowanie ogniem odbywa się za pomocą dżojstika przez ciekłokrystaliczny monitor i przypomina grę komputerową. Pojazd ten nie ma problemów w poruszaniu się w terenie górzystym. Dodatkowy pancerz chroni go przed ogniem z granatników przeciwpancernych, a elastyczne zawieszenie sprawia, że energia wybuchu miny - pułapki jest mniej odczuwalna dla żołnierzy przebywających w pojeździe.

Przykładem skuteczności rozwiązań technicznych niech będzie zdarzenie z 11 sierpnia 2007 r., kiedy w czasie rutynowego patrolu, Rosomak wjechał na minę - pułapkę. Wszyscy żołnierze przeżyli ten wypadek i jak dotychczas ataków przy użyciu min-pułapek na Rosomaki było kilka, ale nikt nie zginął. W zgodnej opinii wielu żołnierzy pełniących służbę w Afganistanie, Rosomak sprawdził się w tamtych warunkach i żołnierze chętnie z niego korzystają. Talibowie nazywają żołnierzy jeżdżących Rosomakami "czarnymi diabłami".

Innym urządzeniem charakterze zarówno rozpoznawczym, jak i ochronnym są bezzałogowe aparaty latające. W PKW Afganistan używane są bezzałogowe statki latające o nazwie Orbiter.

W skład systemu Orbiter wchodzą trzy statki powietrzne, wyrzutnia oraz naziemne stacje kontroli i kierowania.

Sercem Orbitera jest komputer zarządzający lotem aparatu i wykonaniem misji, w tym także pracą systemu nawigacyjnego, głowic optoelektronicznych oraz systemu przesyłania danych. Orbiter jest wykonany całości z kompozytu (węglowego i szklanego), pokryty jest specjalną farbą, a napędzany za pomocą silnika elektrycznego. Dzięki temu jest on praktycznie niesłyszalny podczas lotu na wysokości ok. 100 m, a tym samym trudnym do wykrycia.

BSL realizuje lot autonomicznie po wcześniejszym wprowadzeniu przez operatora danych granicznych, jak wysokość lotu czy punkty trasy, od momentu wystrzelenia z przenośnej katapulty. Orbiter ląduje w punkt za pomocą spadochronu oraz poduszki powietrznej, co ma istotne znaczenie w przypadku operowania w terenie obfitującym w skały i kamienie. Praca operatora systemu sprowadza się do kontrolowania 6 zadanych wcześniej trybów wykonania zadania.

Bezpieczeństwo wojsk w operacjach wielonarodowych jest i powinno zostać priorytetem wszystkich przełożonych, dlatego każda kolejna zmiana w Iraku posiadała coraz nowocześniejsze wyposażenie.

W czasie trwania misji dokonano wielu zakupów oraz dostosowano posiadane wyposażenie do irackich warunków, w jakich polscy żołnierze pełnili służbę. Dążąc do poprawienia bezpieczeństwa żołnierzy, dokonano modernizacji części sprzętu. Podjęto działania na rzecz doskonalenia środków zakłócających detonację ładunków wybuchowych oraz rozwijania wsparcia medycznego.

Doświadczenia zdobyte w Iraku oraz wnioski żołnierzy, którzy pełnili tam służbę zostały wykorzystane do przygotowania misji w Afganistanie, a wyposażenie polskich żołnierzy nie odbiega jakością od najlepszych armii świata.

3.3.5. Analiza obiegu informacji alarmowych

Podstawową zasadą ochrony wojsk jest wzajemny przepływ informacji z każdego szczebla dowodzenia. Wymiana informacji powinna w szczególności dotyczyć:

- zagrożenia;
- taktyki przeciwnika;
- szkolenia antyterrorystycznego;
- sposobu działania sił ochronnych na zagrożenia;
- sposobu powiadamiania stanu osobowego o sytuacjach alarmowych;

Dokonując analizy obiegu informacji na przykładach operacji pokojowych i misji stabilizacyjnej w Iraku, wypracowano jednolity system bezpieczeństwa ustalający stany alarmowe (ang. *alert states*), kody oporządzenia, kody ruchu pojazdów oraz przyjęto określone zasady postępowania w przypadku różnego typu zagrożeń. Dzięki temu zwiększono skuteczność ochrony wojsk przed groźbą ataków terrorystycznych na patrole, konwoje oraz bazy wojskowe. W najważniejszych punktach baz eksponowano na tablicach informacyjnych

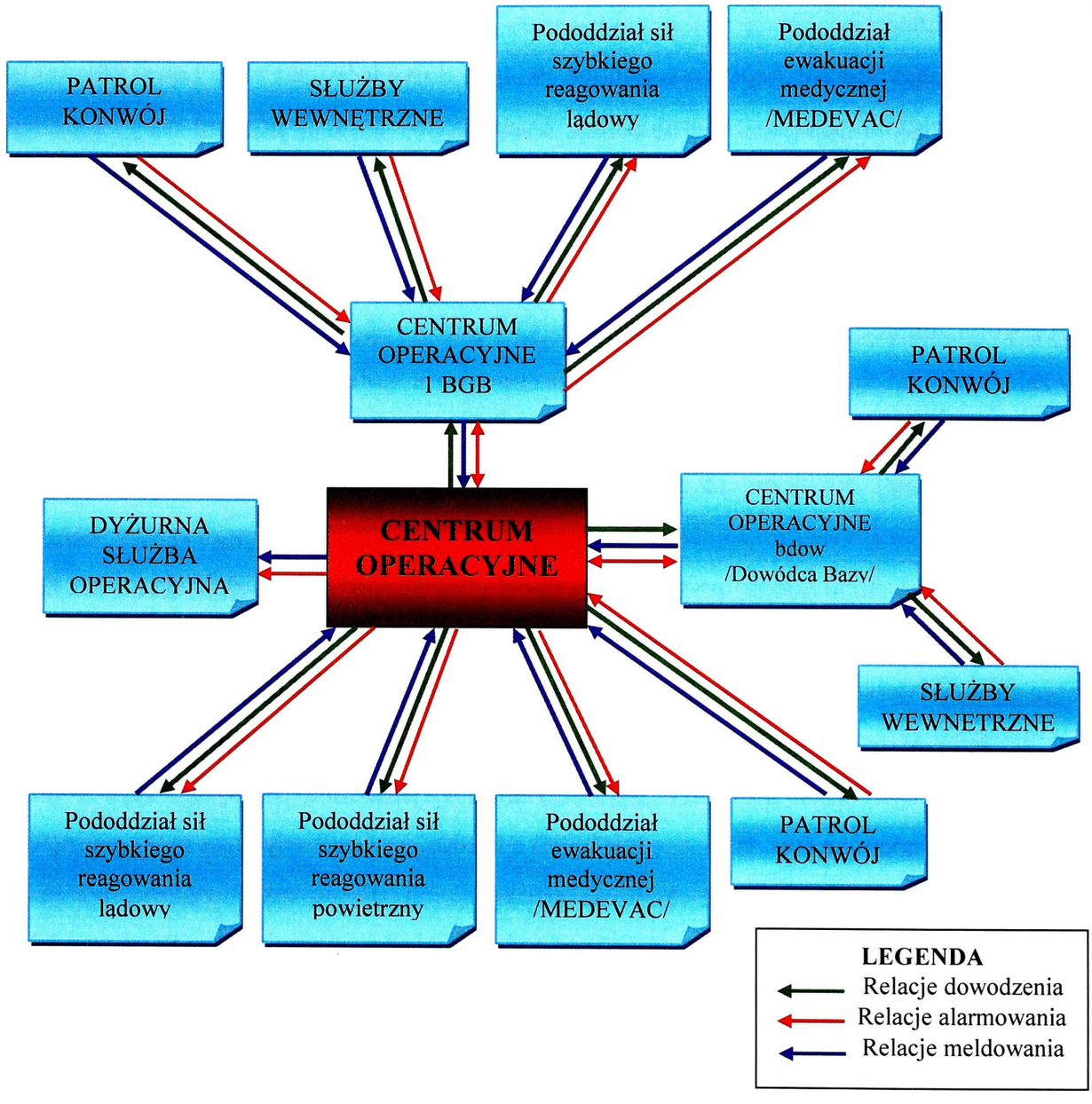
aktualne stany alarmowe, żeby każdy żołnierz i pracownik bazy wiedział jaki jest aktualny stan zagrożenia.

Do obowiązków osób funkcyjnych, w tym dowódców patroli i konwojów, należała znajomość aktualnego stanu alarmowego, związanych z tym ograniczeń dotyczących m.in. ruchu pojazdów oraz oporządzenia jakie każdy żołnierz musi posiadać przy sobie. Stany alarmowe określały poziom aktualnego zagrożenia, a na ich podstawie przyjmowano odpowiednie kody oporządzenia oraz kody ruchu pojazdów. Kody oporządzenia określały szczegóły umundurowania i wyposażenia, które żołnierze byli zobowiązani nosić w zależności od wprowadzonego stanu alarmowego. Z kolei kody ruchu pojazdów ustalały zasady poruszania się pojazdami w granicach strefy oraz określały wymogi bezpieczeństwa.

Głównym dokumentem regulującym procedury wprowadzania stanów alarmowych był „*SOP Force Protection MND CS*".

Rodzaje stanów alarmowych, kody oporządzenia, kody ruchu pojazdów oraz możliwe opcje wprowadzania stanów alarmowych wraz z kodami oporządzenia i kodami ruchu pojazdów obwiązujące w PKW Irak i PKW Afganistan przedstawiono w załącznikach 5 - 10.

Jednym z poważniejszych zagrożeń dla żołnierzy koalicji pozostających w bazach wojskowych był ostrzał moździerzowy lub rakietowy. Gros ataków było przeprowadzanych w godzinach nocnych (ok. 90% między 01.00 a 03.00), a więc kiedy baza była „pogrążona we śnie" i tylko służby dyżurne były na posterunkach. Ponieważ z reguły był to ogień niekierowany, dlatego też skuteczność jego była niewielka, niemniej jednak zagrożenie było realne. Ze względu na niewielki obszar baz, ostrzałowi mógł podlegać cały teren bazy.



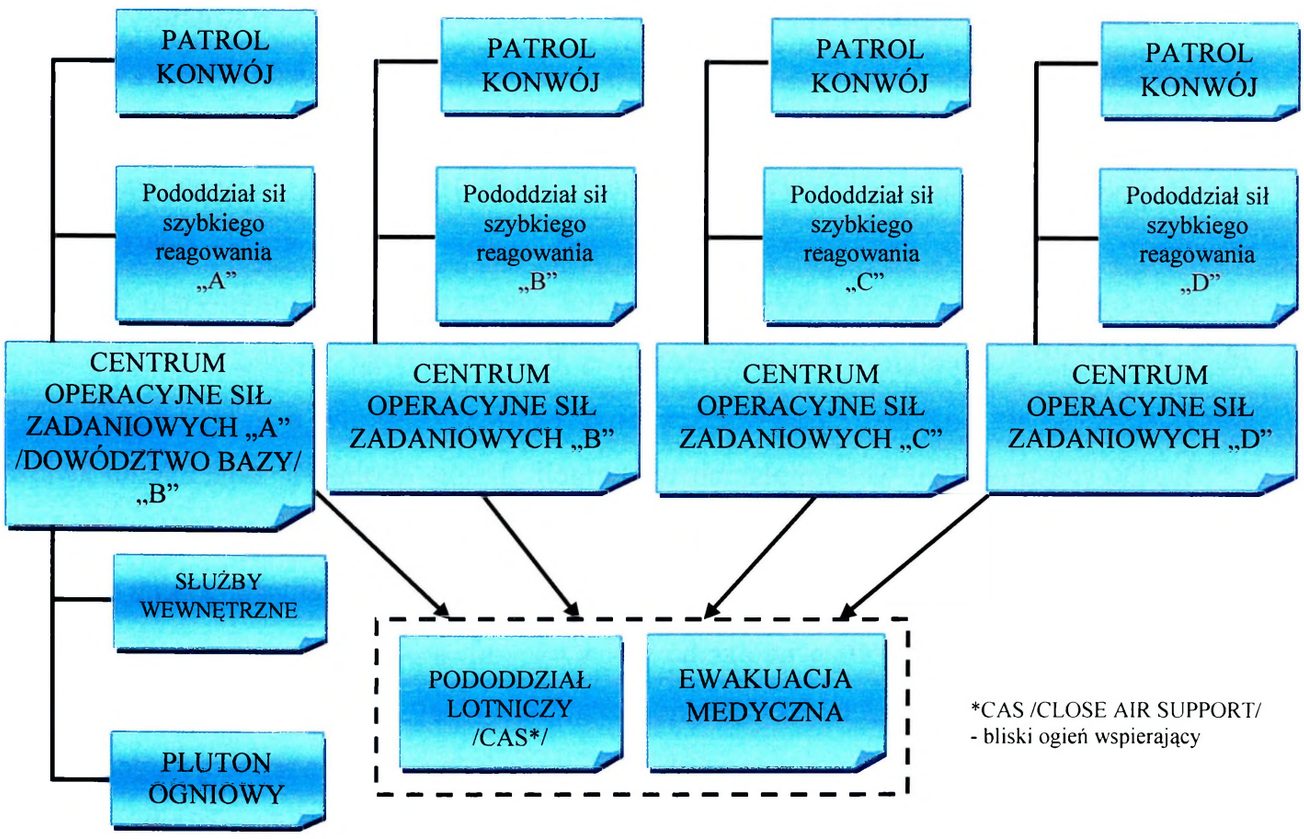
źródło: opracowanie własne

Rys. 3.9. Schemat obiegu informacji alarmowych VI zmiany PKW IRAK

Zgodnie z przyjętymi procedurami, w sytuacji wystąpienia ataku moździerzowego na bazę Echo, służba operacyjna obozu ogłaszała alarm dla stanu osobowego, po czym żołnierze i personel cywilny udawali się do schronów i ukryć. Następnie, powiadomione siły szybkiego reagowania, w zależności od sytuacji, podejmowały stosowne działanie w celu wyeliminowania zagrożenia i ewentualnego ujęcia sprawców. Monitorowaniem sytuacji zajmowało się centrum operacyjne (ang. *Tactical Operation Center - TOC*), w którym oficerowie pełnili służbę całodobowo w systemie 3 - zmianowym.

Cyklicznie, w celu sprawdzenia reagowania stanu osobowego obozu na wypadek wystąpienia zagrożenia atakiem moździerzowym organizowano w godzinach dziennych treningi.

Nieco odmiennie obieg informacji alarmowych wyglądał w Afganistanie do października 2008r., a więc do momentu przejęcia prowincji Ghazni. W Sharanie każda grupa bojowa, przebywająca w danej bazie posiadała własne centrum operacyjne /TOC/ i pododdział sił szybkiego reagowania /QRF/. Jednakże za sprawy ochrony fizycznej bezpośrednio odpowiadało amerykańskie dowództwo bazy, które jednocześnie było centrum operacyjnym . W wypadku ogłoszenia alarmu o zagrożeniu wszyscy żołnierze i pracownicy udawali się do schronów. Na stanowiskach pozostawali jedynie żołnierze pełniący służbę w poszczególnych centrach operacyjnych. Pluton ogniowy zajmował stanowiska, a wszystkie pododdziały szybkiego reagowania wyjeżdżały poza bazę w kierunku, z którego prowadzono ostrzał i dopiero za bramą obozu dostawały zadania drogą radiową. Dla przykładu w bazie w Sharana były cztery Grupy Zadaniowe i każda posiadała własne centrum operacyjne i pododdział sił szybkiego reagowania.



źródło: opracowanie własne

Rys. 3.10. Schemat obiegu informacji baza Sharana - Afganistan

Kolejnym rodzajem zagrożenia, który był rozważany jako możliwy do realizacji było zagrożenie atakami lądowymi oraz atakami terrorystycznymi na pododdziały znajdujące się w obozach wojskowych. Na podstawie wniosków i przeprowadzonych analiz zagrożeń zostały opracowane szczegółowe procedury postępowania na wypadek ataku lądowego. Zgodnie z opracowanym *„Planem postępowania na wypadek ataku lądowego"* dla poszczególnych komórek funkcyjnych sztabu dywizji oraz pododdziałów stacjonujących na terenie obozu wyznaczono rubieże obrony, z których planowano odpieranie ataku.

Do odpierania ataku byli przewidziani prawie wszyscy oficerowie ze sztabu dywizji oraz oczywiście żołnierze pododdziałów. Jedynie po jednym oficerze w każdej komórce sztabu pozostawało na stanowisku pracy. Wszyscy żołnierze w ramach szkolenia zostali zapoznani z przydzielonymi im do obrony stanowiskami ogniowymi oraz zostały wskazane sektory ostrzału.

Z powodu warunków atmosferycznych panujących w rejonie misji zagrożenie pożarami było kolejnym ważnym problemem. Zadania organizacji ochrony przeciwpożarowej realizowały sekcje pionu ochrony i obrony batalionu dowodzenia nadzorowane przez przedstawiciela wojskowej straży pożarnej, który wchodził w struktury wydziału infrastruktury oddziału inżynieryjnego dywizji i odpowiadał bezpośrednio za przygotowanie i nadzorowanie funkcjonowania systemu ochrony przeciwpożarowej. Zadania gaśnicze na terenie polskich obozów realizowały polskie jednostki wojskowej straży pożarnej.

3.4. Wnioski

1. Do czasu udziału wojsk polskich w operacji „Iracka Wolność" zagadnienia związane z ochroną wojsk były postrzegane przez pryzmat zabezpieczenia bojowego działań bojowych. W okresie pokoju problematyka ta była identyfikowana z ochroną obiektów wojskowych.
2. Udział Sił Zbrojnych RP w misji stabilizacyjnej w Iraku spowodował zmianę podejścia do zagadnień związanych z ochroną i bezpieczeństwem wojsk.
3. Obrona przed atakiem terrorystycznym jest zadaniem szczególnie trudnym ze względu na to, że to terroryści wybierają czas i miejsce ataku oraz nie są ograniczeni przepisami prawa.
4. Ochrona wojsk to oczywisty priorytet dowódcy w czasie działania poza granicami kraju. Jego zapewnienie jest podstawowym warunkiem podjęcia jakiegokolwiek

działania. Ochrona ta powinna być rozumiana w dwóch kategoriach. Pierwsza to ochrona baz i innych miejsc stałego przebywania. Druga natomiast to zapewnienie bezpieczeństwa pododdziałom wykonujących zadania poza bazami.

5. Planowanie ochrony wojsk odbywa się na podstawie oceny zagrożenia, która jest punktem wyjścia do planowania działań zmierzających do minimalizacji podatności na ataki terrorystyczne.
6. Doskonaleniu ulegały techniki operacyjne oraz struktury pododdziałów przewidzianych do realizacji przedsięwzięć ochrony wojsk. Również ilość i jakość sprzętu technicznego wykorzystywanego do ochrony baz wpływa znacząco na podniesienie poziomu bezpieczeństwa. Wyposażenie pododdziałów ochrony w środki techniczne ułatwiające kontrolowanie osób i pojazdów wjeżdżających na teren bazy, takie jak np. wykrywacze materiałów wybuchowych, wykrywacze metalu, skanery czy przeszkolone psy to w obecnych czasach priorytet.
7. Do realizowania zadań ochronnych należy przewidzieć etatowe pododdziały ochrony podległe bezpośrednio Komendantowi Bazy, mające siły i środki umożliwiające obsadzenie wszystkich kluczowych elementów systemu ochrony bazy. Do ochrony i obrony baz wojskowych poza granicami kraju potrzeba jest angażowania dużych sił i środków.
8. Bazy wojskowe powinny być lokalizowane poza obszarami zurbanizowanymi. Pozwoli to z jednej strony bezpiecznie rozbudować bazy pod względem inżynieryjnym. Z drugiej strony umożliwi to zorganizowanie głębokiego systemu ochrony i obrony na przedpolach z wykorzystaniem mobilnych patroli i punktów obserwacyjny, a tym samym wczesne ostrzeżenie bazy o zbliżającym się przeciwniku i szybką reakcję na zagrożenie.
9. Doświadczenia kolejnych zmian zarówno w Iraku, jak i w Afganistanie przyczyniły się do poprawy wyposażenia zbiorowego i indywidualnego żołnierzy.
10. Nie bez znaczenia jest także fakt, że dzięki udziałowi w misjach w Iraku i Afganistanie, wartość bojowa żołnierzy znacznie wzrosła, a doświadczenie w zakresie ochrony wojsk nabyte w czasie ich trwania jest wykorzystywane w szkoleniu żołnierzy przygotowywanych do udziału w kolejnych zmianach Polskich Kontyngentów Wojskowych.

4. DIAGNOZA ZAGROŻEŃ BEZPIECZEŃSTWA ELEKTRONICZNEGO

Dokonując diagnozy zagrożeń elektronicznych systemu bezpieczeństwa wojsk w operacjach wielonarodowych należy wyjaśnić pojęcie zagrożenie elektroniczne.

Zagrożenie elektroniczne w literaturze nie jest tłumaczone w sposób bezpośredni. Należy jednak stwierdzić, że skoro walka elektroniczna to: „działania militarne polegające na rozpoznawaniu źródeł emisji elektromagnetycznej przeciwnika wykorzystujących energię elektromagnetyczną, w tym energię wiązkową, przy jednoczesnym zapewnieniu warunków jej efektywnego użycia przez wojska własne”[1], to zagrożenie elektroniczne jest bezpośrednią przyczyną tych działań w środkach i systemach elektronicznych. Można zatem stwierdzić, że zagrożenie elektroniczne obejmuje brak bezpieczeństwa w urządzeniach i systemach elektronicznych wojsk własnych (wielonarodowych). Konkludując, zagrożenie elektroniczne wynika z użycia systemów elektronicznych przez stronę przeciwną. Wiąże się nierozerwalnie z możliwością uzyskania informacji bezpośrednio z systemów elektronicznych (przechowywania, przetwarzania i przesyłania informacji) przy wykorzystaniu środków elektronicznych przez potencjalnego przeciwnika[2], celem destrukcyjnego oddziaływania na siły wielonarodowe.

W trakcie realizacji operacji wielonarodowych można wyodrębnić następujące po sobie fazy[3]:

- planowanie i przygotowanie;
- przemieszczanie i rozwinięcie operacyjne;
- właściwe działania;
- zakończenie konfliktu i powrót do miejsc stałej dyslokacji;
- odtworzenie stanu wyjściowego, analiza przebiegu operacji.

Planowanie i przygotowanie operacji wielonarodowej polega na ustaleniach dotyczących sił wydzielanych przez poszczególne państwa, oraz określeniu zasad ich wykorzystania przez dowództwo wielonarodowe. Dotyczy to przede wszystkim zasad użycia broni, wskazania rejonów przewidzianych do użycia sił poszczególnych państw, jak również określenie relacji dowodzenia. Przygotowanie operacji przez poszczególnych uczestników

[1] Regulamin działań wojsk lądowych DD/3.2, MON, SGWP, Warszawa 2006, s.88.
[2] Rozumiane w sensie szerokim, od prowadzenia RE po inicjowanie wybuchów ładunków wybuchowych przy wykorzystaniu spektrum elektromagnetycznego.
[3] M. Wiatr, Operacje połączone, Adam Marszałek, Toruń 2006, s. 22.

realizowane jest na terytorium krajów uczestniczących. W fazie tej zastosowanie mają narodowe rozwiązania w zakresie bezpieczeństwa elektronicznego.

Przegrupowanie sił w obszar operacji realizowane jest sposobem mieszanym przy wykorzystaniu militarnego i cywilnego potencjału transportowego, środkami lądowymi, powietrznymi i morskimi.

Faza trzecia polega na organizowaniu baz wojskowych na terenie zazwyczaj objętym kryzysem (wojną) oraz działaniami mandatowymi w obszarze operacji. Jest to zasadnicza faza operacji wielonarodowej. Czas jest trwania jest trudny do oszacowania. Może trwać do kilkudziesięciu lat. W odniesieniu do bezpieczeństwa sił, w opinii zespołu autorskiego, wymagająca największej pracy koncepcyjno-organizacyjnej.

Zakończenie działań i przegrupowanie sił do terytorium własnego państwa jest w gestii narodowej. Brak jest jednoznacznych wskazań różnic pomiędzy działaniami narodowymi a wielonarodowymi.

Ostatnią fazą operacji wielonarodowych (operacji w ogólności) jest odtworzenie struktur i stanów wyjściowych oraz analiza przebiegu operacji. Wynikiem są wnioski odnoszące się do pozytywnych i negatywnych zjawisk zaistniałych w trakcie działań. Ze względów praktycznych, ważne jest wygenerowanie wszystkich słabych stron tak, aby w przyszłej operacji skutecznie im przeciwdziałać.

Zagrożenie elektroniczne w działaniach wielonarodowych ściśle związane jest z fazą operacji.

Czas trwania operacji wielonarodowych zazwyczaj jest trudny do oszacowania. Początkowe analizy dotyczące czasu trwania działań nie sprawdzają się, dlatego w trakcie prowadzenia operacji wymagane jest rotowanie sił biorących w niej udział. Zmiana sił odbywa się w podobnych etapach jak ich tworzenie, należy jednak zauważyć, że nie istnieje potrzeba tworzenia baz, gdyż żołnierze zajmują już istniejące. Nie jest to jednak zasada, gdyż w trakcie prowadzenia działalności mandatowej, wynikają okoliczności nieprzewidziane wymagające interwencji. Dotyczy ona rozbudowy bazy, zwiększenia ochrony fizycznej i elektronicznej. Etapy realizowane na terytorium własnego kraju podlegają ochronie fizycznej i elektronicznej zgodnie z przepisami danego państwa. Największym problemem zapewnienia bezpieczeństwa jest etap organizowania baz i realizacji zadań zgodnych z mandatem sił wielonarodowych. Wynika to z różnych przepisów obowiązujących w państwach biorących udział w operacji wielonarodowej, mentalności poszczególnych nacji oraz braku świadomości zagrożenia jakie może zaistnieć w trakcie funkcjonowania sił wielonarodowych.

Do ochrony bazy w bezpośredniej bliskości wystarczająca jest ochrona fizyczna, jednak ze względu na obszar baz (300 ha i więcej przy długości ogrodzenia od 7 km)[4] jej zapewnienie wiązałoby się z wydzieleniem nieproporcjonalnie dużych sił ochrony. Siły ochrony zastępowane są (uzupełniane) środkami technicznymi wspomagającymi ochronę. Z analizy literatury i wniosków z misji stabilizacyjnej w Republice Iraku wynika, że zagrożenie dla bazy i ludzi w niej stacjonujących oddala się od ogrodzenia proporcjonalnie do zasięgów posiadanych środków ogniowych przez stronę przeciwną. Zazwyczaj są to moździerze i pociski rakietowe odpalane z improwizowanych wyrzutni. Dokładność trafień świadczy o dobrej znajomości rozkładu bazy, jak również procedurach w niej obowiązujących.

W takich przypadkach bezwzględnym jest wykorzystywanie przez ochronę bazy urządzeń zwiększających zdolności recepcyjne człowieka. Do takich urządzeń zaliczyć można stacje rozpoznania pola walki, noktowizory, kamery termalne.

Wykonywanie zadań przez żołnierzy poza bazą wiąże się również z ryzykiem ataku w postaci min (bomb) pułapek odpalanych przewodowo, radiowo lub przy użyciu zapalników: naciskowych, elektromagnetycznych, odciągowych lub wszystkich jednocześnie. Należy wnioskować, że ataki wynikają z pozyskiwania informacji przez stronę przeciwną z zasobów informacyjnych sił wielonarodowych (koalicyjnych). Nie można wykluczyć prób wprowadzenia błędnych informacji do zasobów informacyjnych sił koalicyjnych.

Środki destrukcyjne wykorzystywane przez stronę przeciwną wobec wojsk wielonarodowych, zazwyczaj są mało skomplikowane. Nie posługują się techniką nowej generacji, lecz środkami walki prostymi w obsłudze, niewymagającymi dużej ilości czasu do szkolenia. Bojownicy (terroryści) dążą do wyników „medialnych", które nękają psychikę żołnierzy i opinii publicznej. Prostota wykorzystywanych środków sprzyja skrytemu ich przemieszczaniu (przewożeniu lub przenoszeniu). Należy się również liczyć z wspieraniem bojowników przez kraje „niezaangażowane w konflikt", a wykorzystujące środki walki elektronicznej (w głównej mierze rozpoznania elektronicznego).

Zagrożenia dla sił wielonarodowych mogą wynikać z sytuacji społeczno-wyznaniowej, związanej zwłaszcza z niestabilnością społeczną, która ze względu na zamieszkującą obszar działań większość wyznaniową, inspirowaną przez lokalnych przywódców religijnych, może być przeciwna obecności sił koalicji, uważanych zazwyczaj za okupacyjne.

---

[4] Np. Baza ECHO w PKW Irak.

Czynnikiem sprzyjającym radykalizacji postaw większości wyznaniowej może być narastający fanatyzm religijny wyrażający się m.in. w dążeniach do swobody poruszania się w rejonach miejsc kultu religijnego, a także nasilające się dążenia do odbudowy wpływów określonego wyznania religijnego i budowy państwa wyznaniowego. Wiązać się to może z oddziaływaniem sąsiednich państw, w szczególności charakteryzujących się takim samym wyznaniem religijnym, poprzez wysyłanie w obszar sił wielonarodowych grup specjalnych. Ich głównym zadaniem może być mobilizacja związków wyznaniowych do walki przeciwko „zewnętrznym okupantom", w tym także przygotowanie przyszłych działań partyzanckich. W działaniach tych mogą brać udział żołnierze wywodzący się z poprzedniej władzy, a wynikiem mogą być działania zbrojne i dywersyjno-sabotażowe.

Działania o charakterze dywersyno-sabotażowym i terrorystycznym mogą prowadzić grupy powstałe z ukrywających się członków rozbitych formacji postreżimowych, ekstremiści wyznaniowi, byli żołnierze oraz funkcjonariusze reżimowych służb specjalnych i bezpieczeństwa. Nie należy wykluczać także prób działalności ekstremistów wyznaniowych, które będą dążyć do pozyskania w swoje szeregi członków grup terrorystycznych i prowadzić walkę przeciwko siłom wielonarodowym. W działaniach dywersyjno-sabotażowych i terrorystycznych mogą być wykorzystane m.in.:

a) materiały wybuchowe;

b) detonatory (kapsuły detonujące) – detonatory uzyskane z prowizorycznych „mechanizmów" wybuchowych i magazynów ze środkami wybuchowymi;

c) mechanizmy wyzwalające[5]:

- elektroniczne mechanizmy zegarowe o zaprogramowanej zwłoce czasowej (uzyskano szereg takich urządzeń o zaprogramowanym czasie odpalenia od jednej do kilku godzin);
- elektroniczne mechanizmy zegarowe o regulowanej zwłoce czasowej (niektóre mechanizmy pochodzenia irackiego składały się z dwóch zintegrowanych zegarowych układów scalonych typu Motorola „MC 14536 B" zamontowanych wspólnie z innymi elementami elektronicznymi na otwartej płytce montażowej);
- radiowy mechanizm odpalający (terroryści używali radiowego mechanizmu odpalającego składającego się z odbiornika i wyzwalacza);

[5] Treści przedstawione w informatorze dla IV zmiany PKW Irak.

– urządzenie wyzwalające stosowane w operacjach specjalnych (uzyskano mechanizmy produkowane komercyjnie, przeznaczone do użycia w specjalnych operacjach wojskowych);
– urządzenie spowalniające na bazie budzika (uzyskano budzik turystyczny firmy CASIO zmodyfikowany w celu wykorzystania w prowizorycznym mechanizmie wybuchowym).

Grupy dywersyjno-sabotażowe i terrorystyczne mogą dysponować ponadto całą gamą uzbrojenia osobistego, przenośnymi wyrzutniami pocisków rakietowych, w tym ppanc., a także minami-pułapkami, przeciwpiechotnymi i przeciwpancernymi.

Wrogie nastawienie do wojsk sił wielonarodowych może wynikać również z niewystarczającej pomocy humanitarnej i pogłębiającej się biedy i ubóstwa lokalnej społeczności. Zagrożenie takie osiąga realizm jeśli społeczność, przed interwencją sił wielonarodowych, korzystała z dostarczanych zasobów w ramach programów pomocy humanitarnej. Zdaniem zespołu autorskiego, proces zubożenia społeczeństwa może tworzyć coraz korzystniejsze warunki dla powstawania pospolitych grup przestępczych, które obok ataków na konwoje z pomocą humanitarną mogą rozwijać „czarny rynek" oraz działalność przemytniczo-mafijną.

Powyżej przedstawiono analizę zagrożeń występujących w czasie trwania misji w Iraku, natomiast zasadnym jest zwrócić uwagę na zagrożenia elektroniczne ze szczególnym uwzględnieniem infrastruktury telekomunikacyjnej.

Współczesne siły wielonarodowe w szerokim zakresie wykorzystywały i będą wykorzystywały systemy gromadzenia, przetwarzania i przesyłania informacji określane mianem sieci teleinformatycznych. W literaturze przedmiotu dotyczącej bezpieczeństwa sieci teleinformatycznych spotyka się ogólną klasyfikację zagrożeń jako: wewnętrzne i zewnętrzne, oraz szczegółową, dotyczącą konkretnej sieci, gdzie uwzględnia się jej organizację, możliwości konfiguracji, zastosowane środki telekomunikacyjne oraz urządzenia końcowe. Opracowanie szczegółowej klasyfikacji zagrożeń zależy od przyjętych przez organizatora warunków początkowych oraz kryterium oceny możliwości wystąpienia zagrożenia lub grupy zagrożeń.

Z analizy literatury przedmiotu i dokumentów normatywnych, regulujących tę materię, wynika, że do potencjalnych źródeł ujawnienia informacji zalicza się[6]:

- infrastrukturę telekomunikacyjną;

[6] Praca pod kier. J. Michniaka, Bezpieczeństwo i ochrona informacji w sieciach łączności i informatyki wojskowej w okresie pokoju, kryzysu i wojny, AON, Warszawa 2004, s. 86.

- elementy (urządzenia) telekomunikacyjne;
- elementy (urządzenia) informatyczne;
- aplikacje (oprogramowanie) systemowe;
- personel techniczny i użytkowników systemu.

W *Metodyce opracowywania szczególnych wymagań bezpieczeństwa systemu lub sieci teleinformatycznej (SWB)*[7] wyróżniono następujące rodzaje zagrożeń:

- zagrożenia zewnętrzne;
- zagrożenia wewnętrzne;
- zagrożenia fizyczne.

Do zagrożeń wewnętrznych zaliczyć można:

- utratę lub uszkodzenie danych w wyniku celowego działania użytkownika;
- brak możliwości obsługi systemów z powodu nieprawidłowego funkcjonowania;
- utratę lub uszkodzenie danych spowodowanych nieautoryzowanym dostępem;
- zniszczenie danych z powodu błędów w aplikacjach użytkowych, oprogramowaniu systemowym bądź działanie oprogramowania złośliwego – wirusa.

Zagrożenie zewnętrzne dotyczy możliwości utraty lub uszkodzenia danych, brak możliwości obsługi sieci teleinformatycznej w wyniku działania osób nieuprawnionych w zewnętrznym otoczeniu sieci.

Pojecie zagrożenia fizycznego nieodłącznie kojarzy się ze zniszczeniem infrastruktury, urządzeń bądź samych obiektów, w których poszczególne elementy systemów elektronicznych są zainstalowane. Ich zniszczenie może nastąpić w wyniku celowego działania potencjalnego przeciwnika, bądź też jako efekt zaistnienia klęski żywiołowej, takiej jak: pożar, powódź, trzęsienie ziemi itp. W operacjach wielonarodowych do tej grupy należy zaliczyć zagrożenia płynące ze strony organizacji terrorystycznych. Wynikają głównie z konieczności zdobycia informacji niezbędnych do wykonania zamierzonego działania terrorystycznego. Dotyczyć mogą zdobycia informacji o lokalizacji obiektu, planów obiektów, planów działania w sytuacjach zagrożenia, informacji na temat stanu i możliwości sił bezpieczeństwa itp.

W odniesieniu do systemów teleinformatycznych bezpieczeństwo informacji określane jest jako *definiowanie*, *osiąganie* i *utrzymywanie* sześciu podstawowych cech, do których zalicza się[8]:

---

[7] Metodyka opracowania szczególnych wymagań bezpieczeństwa dla systemów lub sieci teleinformatycznych, SGWP, Warszawa 2000, s. 8.
[8] Tamże, s. 41

- *poufność* – dostęp do informacji musi być ograniczony jedynie do kręgu uprawnionych użytkowników;
- *integralność* – informacja musi być zachowana w swojej oryginalnej postaci, z wyjątkiem przypadków, gdy jest ona legalnie aktualizowana lub usuwana przez uprawnione osoby;
- *dostępność* – informacja musi być dostępna dla uprawnionych użytkowników zawsze, kiedy mają taką potrzebę;
- *rozliczalność* – dostęp użytkownika do informacji może być przypisany w sposób jednoznaczny tylko temu użytkownikowi;
- *autentyczność* – tożsamość (pochodzenie) informacji lub podmiotu z nią związanego (np. osoba wysyłająca daną wiadomość) musi być zgodna z zadeklarowaną (osobą);
- *niezawodność* – zachowanie i skutki działania np. urządzeń zawierających informacje, które podlegają ochronie, które należy zapewnić i utrzymać jako podstawowe atrybuty bezpieczeństwa informacji.

Należy zaznaczyć, że zapewnienie wszystkich przedstawionych cech gwarantuje poziom bezpieczeństwa informacji możliwy do zaakceptowania w czasie operacji wielonarodowej.

4.1. Uwarunkowania bezpieczeństwa elektronicznego w operacjach wielonarodowych

Bezpieczeństwo elektroniczne należy rozumieć jako stan braku zagrożenia wobec systemów elektronicznych wykorzystywanych w obszarze operacji przez przeciwnika i brak zagrożeń utraty informacji przez wszystkie pododdziały narodowe. Bezpieczeństwo jest pojęciem używanym do określenia stanu pewności, spokoju i braku zagrożenia. Obejmuje zaspokojenie takich potrzeb jak[9]:

- istnienie;
- przetrwanie;
- całość;
- tożsamość (identyczność);

[9] Słownik Języka Polskiego- PWN, Warszawa 1978

- niezależność;
- spokój;
- posiadanie;
- pewność rozwoju.

Problematyka bezpieczeństwa elektronicznego, zdaniem zespołu autorskiego, obejmuje: systemy informatyczne (przetwarzania informacji), łączności (transmisji informacji), przeciwdziałania elektronicznego (urządzenia zakłócania zapalników bomb i min inicjowanych drogą radiową), elektroniczne systemy kontroli dostępu oraz systemy elektroniczne wykorzystywane do monitorowania otoczenia wokół baz i sił manewrowych działających poza bazami. Wobec ludzi i sprzętu należy liczyć się z sabotażem, terroryzmem jak również szpiegostwem przez służby wywiadu innych państw. Nie można wykluczyć sytuacji, w której wywiady państw nie zaangażowanych w konflikt, będą realizować skryte działania mające na celu pozyskiwanie informacji o sprzęcie i procedurach działania.

Bezpieczeństwo łączności zależne jest m.in. od spełnienia warunków kompatybilności sprzętowej i elektromagnetycznej. Kompatybilność elektromagnetyczna (ang. *ElectroMagnetic Compatibility - EMC*) - zdolność danego urządzenia elektrycznego lub elektronicznego do poprawnej pracy w określonym środowisku elektromagnetycznym i nieemitowanie zaburzeń fali elektromagnetycznej zakłócającej poprawną pracę innych urządzeń pracujących w tym środowisku.

Oznacza to spełnienie trzech warunków:

- urządzenie (system) nie powoduje zakłóceń w pracy innych urządzeń (systemów);
- urządzenie (system) nie jest wrażliwe na zakłócenia emitowane przez inne urządzenia;
- urządzenie (system) nie powoduje zakłóceń w swojej pracy.

Środowisko elektromagnetyczne jest to miejsce użytkowania urządzenia określone poziomem i charakterem zaburzeń pochodzących od ich źródeł. Źródłami tymi mogą być obiekty emitujące fale elektromagnetyczne celowo (np. nadajniki radiowe, telewizyjne lub radiolokacyjne) lub przypadkowo (np. urządzenia AGD).

Wykorzystywanie różnorodnych środków łączności przez siły wielonarodowe (rozwiązania narodowe w zakresie środków łączności) sprawia, że nie jest możliwe zapewnienie łączności pomiędzy pododdziałami różnych narodowości. Istnieje zatem konieczność wymiany grup łącznikowych ze sprzętem, celem wymiany informacji. Wysoką rangę w bezpieczeństwie łączności osiąga zapewnienie kompatybilności elektromagnetycznej. Wskazanie częstotliwości użytkowej zapewniającej pracę urządzeń łączności bez zakłóceń, jak również niewpływającej ujemnie na pracę innych środków lub systemów, jest dużym

wyzwaniem. Brak odpowiedniego przydziału pasm częstotliwości może bowiem skutkować brakiem łączności oraz wadliwą pracą urządzeń teleinformatycznych.

Należy stwierdzić, że wykorzystywanie dużych ilości środków radiowych wymaga dokładnego planowania przydziału pasm częstotliwości, tak aby ich praca nie wpływała negatywnie na innych użytkowników urządzeń łączności. Problemem jest również wykorzystywanie różnych emisji. Właściwe zarządzanie przydziałem pasm łączności ze spektrum elektromagnetycznego staje się dużym wyzwaniem. Z analizy literatury wynika, że w działaniach wielonarodowych, w których udział biorą wojska USA, zarządzaniem częstotliwościami zajmuje się komórka zarządzania częstotliwościami w obszarze operacji TFMC (Theatre Frequency Managament Centrum)[10]. W zarządzaniu spektrum elektromagnetycznym wykorzystuje program informatyczny *Spectrum XXI,* uważany za bardzo wydajny. Program, w trakcie analizy, bazuje na przepisach regulujących problematykę przydziału częstotliwości w danym kraju oraz zasadach zawartych w Międzynarodowych Regulacjach Telekomunikacyjnych (ITU – International Telekomunication Regulation). Oprócz regulacji prawnych, analizowane są poszczególne częstotliwości w zależności od regionu (na podstawie wcześniej przeprowadzonych badań geotermalnych ziemi). Reasumując, właściwe wykorzystanie programu Spectrum XXI zapewnia przydział częstotliwości dla sił wielonarodowych i organizacji pozamilitarnych (np. z pomocą humanitarną) bez zakłóceń wzajemnych.

Podsumowując, zagrożenia systemów elektronicznych występujące w operacji wielonarodowej to:

- naruszenie integralności danych przetwarzanych przez system teleinformatyczny (modyfikacje, dodanie, zniszczenie);
- nieuprawnione skopiowanie danych przez osobę mającą dostęp do systemu;
- włamania do systemu teleinformatycznego;
- nieuprawniony dostęp do zasobów systemu możliwy dzięki ujawnieniu haseł innych użytkowników;
- niepowołany dostęp do miejsca przetwarzania danych;
- zniszczenie elementów lub całości infrastruktury technicznej systemów elektronicznych;
- nieodpowiednie parametry pracy systemu teleinformatycznego (np. wilgotność, temperatura);

[10] B. Stachnik, Zarządzanie częstotliwościami, PWL 8/2008, s. 41.

- błędy popełnione przez użytkowników;
- kradzież lub uszkodzenie sprzętu;
- instalacja nielegalnego oprogramowania (wirusy);
- brak zapewnienia kompatybilności elektromagnetycznej;
- fizyczne, destrukcyjne oddziaływanie na urządzenia elektroniczne.

Konkludując, bezpieczeństwo elektroniczne zależy od przestrzegania przepisów eksploatacyjnych (w tym przepisów korespondencji radiowej) oraz ścisłego stosowania procedur określających zasady bezpieczeństwa wydanych przez dowództwo sił wielonarodowych.

4.2. Kryteria bezpieczeństwa elektronicznego

W wyniku analizy literatury przedmiotu należy stwierdzić, że jednym z kryteriów podziału bezpieczeństwa elektronicznego można przyjąć przeznaczenie urządzeń elektronicznych, które są wykorzystywane. Dla tak przyjętego kryterium można wyróżnić :

- bezpieczeństwo systemów informatycznych obejmuje zarówno brak zagrożenia dla informacji gromadzonych w bazach danych (w serwerach i stacjach roboczych) jak również informacji przekazywanej pomiędzy urządzeniami sieci komputerowej. Do zagrożeń bezpieczeństwa sieci komputerowych zaliczyć należy: włamania do systemów komputerowych, podsłuch sieci, wirusy, dodatkowe obciążenie sieci wiadomościami niechcianymi tzw. spamming oraz podszywanie się pod upoważnioną osobę;
- bezpieczeństwo łączności obejmuje ochronę: osobistą użytkowników środków łączności, promieniowania elektromagnetycznego urządzeń, szyfrograficzną, fizyczną środków łączności i procedur łączności oraz ochronę transmisji, a także zapewnienie warunku kompatybilności elektromagnetycznej;
- bezpieczeństwo przeciwdziałania elektronicznego obejmuje skryte użycie urządzeń zakłócających poprzez montowanie ich na pojazdach stosowanych powszechnie (wykorzystywanych przez żołnierzy sił wielonarodowych), ukrycie danych taktyczno-technicznych wykorzystywanego sprzętu oraz skryte użycie energii elektromagnetycznej poprzez zaskoczenie na wybranych częstotliwościach, kierunkach i obiektach;

- bezpieczeństwo systemów elektronicznych monitorujących otoczenie wokół baz i sił manewrowych obejmuje właściwe wykorzystanie sprzętu zgodnie z przeznaczeniem oraz w odpowiednich warunkach pogodowych z zapewnieniem co najmniej dualizmu bezpieczeństwa (strefa-sektor monitorowana przez co najmniej dwa niezależne systemy ochrony elektronicznej).

Bezpieczeństwem łączności rozumiane jest jako zdolność przeciwstawiania się rozpoznaniu łączności przez przeciwnika oraz zdolność przeciwstawienia się wprowadzeniu do systemu łączności fałszywych informacji (dezinformacji). Dla tak interpretowanego bezpieczeństwa łączności należy wskazać jej cel, którym jest ochrona treści przekazywanych wiadomości przez techniczne środki łączności przed rozpoznaniem radioelektronicznym, penetracją pisemnych informacji przekazywanych środkami wojskowej poczty polowej, dywersją radiową oraz zabezpieczenie przed ucieczką informacji[11]. Określając wymagania bezpieczeństwa informacji dla sieci teleinformatycznej należy wyodrębnić następujące obszary[12]:

- bezpieczeństwo personalne;
- bezpieczeństwo źródeł informacji;
- kontrola dostępu do zasobów sieci teleinformatycznej.

Bezpieczeństwo personalne (osobowe), którego zadaniem jest odsunięcie od dostępu do informacji i niedopuszczenie osób, które z różnych względów nie dają rękojmi zachowania tajemnicy. Mogą być podatne do ujawnienia informacji o szczególnym znaczeniu lub sposobów ich przekazywania przez sieci teleinformatyczne. Dotyczy wielu osób, które mogą mieć dostęp do urządzeń sieci teleinformatycznej, poprzez ich obsługę lub serwis. Działania w zakresie zapewnienia bezpieczeństwa personalnego mają na celu właściwy wybór i sprawdzenie użytkowników sieci poprzez organy zarządzania bezpieczeństwem. Należyty dobór użytkowników powinien skutecznie eliminować ewentualne zagrożenia. Podstawą działania powinno być określenie strefy administracyjnej oraz stref bezpieczeństwa, zorganizowanie właściwego systemu przepustowego i identyfikacji oraz ograniczenie dostępu osób nieupoważnionych do miejsc, w których istnieje zagrożenie nieautoryzowanego dostępu do informacji. System bezpieczeństwa powinien uwzględniać konieczność ochrony i obrony elementów sieci teleinformatycznej. Zastosowane środki techniczne powinny mieć zabezpieczenia uniemożliwiające celowe ich zdobycie przez osoby nieuprawnione.

---

[11] J. Michniak, A.Wisz, Bezpieczeństwo i ochrona informacji w wojskowych sieciach telekomunikacyjnych i zautomatyzowanych systemach dowodzenia, Warszawa 2000, s.11
[12] Tamże, s.11.

Bezpieczeństwo nośników informacji o charakterze niejawnym w sieciach teleinformatycznych wykorzystywanych w działaniach wielonarodowych, wymusza konieczność tworzenia systemu ich rejestrowania, ewidencji dostępu osób uprawnionych i kontroli zapobiegających ich przechwyceniu przez osoby nieuprawnione oraz próbom modyfikowania ich treści. Wiadomości w nich zawarte należy chronić od chwili ich powstania, aż do zmiany klauzuli informacji na „jawne" bądź ich zniszczenia.

Mając na uwadze specyfikę prowadzenia działań wielonarodowych poza miejscami stałego pobytu jednostek, w rejonach rozmieszenia stanowisk dowodzenia powinny być zorganizowane lub rozmieszczone specjalne pomieszczenia do ich przechowywania, ochraniane przez osoby do tego wyznaczone oraz środki techniczne. Są to kancelarie tajne w których należy gromadzić źródła informacji wrażliwych, zawierających ważne dane w różnej postaci. Wymusza to konieczność stosowania barier utrudniających uzyskanie informacji z urządzeń je przekazujących, gromadzących i przetwarzających, a ewidencja dokumentów powinna umożliwiać uzyskanie danych o stanie ilościowym dokumentów, o tym, kto był i jest ich użytkownikiem.

Bezpieczeństwo źródeł informacji w sieciach teleinformatycznych można zapewnić poprzez środki i przedsięwzięcia realizowane w każdym z wymienionych aspektów[13]:

- dostępu (kontroli dostępu);
- uwierzytelnienia;
- zdolności rozliczania;
- audytu (kontroli);
- ponownego użycia obiektów;
- integralności;
- dostępności;
- wymiany danych;
- ryzyka szczątkowego.

Dostęp jest swoistym oddziaływaniem pomiędzy użytkownikiem a obiektem. Wynikiem oddziaływania jest przepływ informacji od jednego do drugiego. Kontrola dostępu polega na prowadzeniu nadzoru takiego oddziaływania. Należy zwrócić uwagę na fakt, że przepływ informacji następuje zarówno poprzez odczyt i zapis informacji jak i wnioskowanie z kombinacji bezpośrednio dostępnych źródeł informacji. Dostęp do sieci teleinformatycznej powinien być możliwy tylko dla osób posiadających odpowiednie

[13] Metodyka opracowania szczególnych wymagań bezpieczeństwa dla systemów lub sieci teleinformatycznych, SGWP, Warszawa 2000, s. 19-20.

poświadczenie bezpieczeństwa osobowego z zachowaniem zasady wiedzy niezbędnej. Osoby bez odpowiedniego poświadczenia bezpieczeństwa osobowego lub uzasadnionej potrzeby uzyskania informacji mogą przypadkowo lub celowo uzyskać dostęp do informacji niejawnych, danych, sprzętu lub oprogramowania chroniącego informacje niejawne w systemie lub sieci teleinformatycznej.

Uwierzytelnienie to proces ustanawiania wiarygodności wnioskującego podmiotu. Wszyscy użytkownicy mający dostęp do informacji niejawnych muszą być zidentyfikowani oraz powinna nastąpić ich autoryzacja. Oznacza to, że wszystkie zautomatyzowane procesy realizowane w imieniu określonych osób powinny być jednoznacznie do nich przypisane. Każda operacja[14] przeprowadzona w ramach sieci teleinformatycznej musi być jednoznacznie przypisana do użytkownika ją realizującego. Nie może być sytuacji gdzie osoby podające się za inne uzyskują dostęp do informacji, bądź osoby uprawnione przeprowadzają operacje podlegające rozliczeniu bez odnotowania tego faktu.

Zdolność rozliczania jest to rejestrowanie faktów wytwarzania, przesyłania, modyfikowania lub kasowania (usuwania) informacji. Powinna istnieć zdolność do indywidualnego rozliczania wytwarzanych i udostępnianych informacji niejawnych. Jest to realizowane poprzez monitorowanie i dokonywanie przeglądów zapisów archiwalnych oraz dokonywanie identyfikacji osób odpowiedzialnych za określone działania związane z bezpieczeństwem informacji w sieci teleinformatycznej.

Audyt wyraża się w monitorowaniu zdarzeń związanych z bezpieczeństwem. Celem jego jest wykrycie i ostrzeganie przed działaniami w sieci teleinformatycznej, które mogą zagrozić bezpieczeństwu tej sieci. Wszystkie wykryte luki w systemie bezpieczeństwa sieci teleinformatycznej powinny być ujawnione oraz w miarę możliwości usunięte. Zagrożeniami w tej dziedzinie mogą być umyślne lub przypadkowe działania naruszające bezpieczeństwo sieci oraz nie podjęcie środków zapobiegających naruszaniu bezpieczeństwa.

Ponowne użycie obiektów (przechowujących zapisane dane) obejmować powinno kontrolę wielokrotnego wykorzystywania nośników danych (pamięć główna, obszary dysków twardych). Powinno obejmować wszystkie funkcje mające na celu zainicjowanie, wyczyszczenie lub zniszczenie komputerowych danych wielokrotnego użytku oraz oczyszczanie urządzeń wyjściowych (np. ekranów wyświetlaczy) kiedy nie są wykorzystywane.

---

[14] Operacja – rozumiana w tej sytuacji jako czynność lub zbiór czynności wykonanych w ramach sieci teleinformatycznej.

Integralność jest właściwością polegającą na zapewnieniu dokładności i kompletności danych i informacji przechowywanej i przesyłanej w sieci teleinformatycznej. W każdej sieci należy ustanowić procedury dostępu, które uniemożliwiają zmodyfikowanie lub kopiowanie danych przez osobę nieuprawnioną oraz by nie była możliwa zmiana źródłowego i docelowego adresu przekazywanej informacji.

Dostępność jest to właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu. Jest to zapewnienie dostępu do danych i informacji w czasie gdy jest to konieczne, oraz że nie będą niepotrzebnie udostępniane lub przetrzymywane.

Wymiana danych w ramach której powinna być zapewniona bezpieczna transmisja zabezpieczająca przed nieuprawnionych odczytaniem danych, oraz odczytaniem danych przez adresata w formie nie zmienionej. Odnosi się zazwyczaj do kanałów łączności, które powinny uwzględniać uwierzytelnienie, kontrolę dostępu, poufność danych oraz integralność i niezaprzeczalność danych.

Ryzyko szczątkowe obejmuje zarówno zidentyfikowane lecz akceptowalne ryzyko dla sieci, oraz nieprzewidziane w okresie użytkowania sieci, a wynikające z postępu technologicznego urządzeń i oprogramowania komputerowego.

4.3 Analiza aktualnych rozwiązań systemowych ochrony i obrony elektronicznej w działaniach wielonarodowych

Poczucie bezpieczeństwa w działaniach wielonarodowych staje się w ostatnim czasie priorytetem działalności dowódców sił. Każdy skuteczny atak na siły wielonarodowe odbierany jest w kraju macierzystym negatywnie przez opinię publiczną. Jest często powodem debat o potrzebie utrzymywania wojsk własnych w siłach wielonarodowych. Dlatego też, zwraca się szczególną uwagę na zapewnienie maximum poczucia bezpieczeństwa. Organizowane systemy ochrony baz wojskowych, procedury działania na wypadek ataku mają zapewnić to poczucie. Elementem wspomagającym ten proces są urządzenia elektroniczne.

4.3.1. Analiza środowiska bezpieczeństwa (obszary intensywności elektronicznej, funkcjonalnej)

Ważnym przedsięwzięciem w zakresie bezpieczeństwa elektronicznego jest prowadzenie rozpoznania elektronicznego. Analizę tego problemu, zespół autorski rozpoczął

od doświadczeń w zakresie zadań polskiej grupy SIGINT w wielonarodowych działaniach stabilizacyjnych w Republice Iraku.

Zadaniem polskiej grupy SIGINT (G2 PL SIGINT Group) było informowanie dowództwa Wielonarodowej Dywizji, wspólnie z wyznaczonymi siłami koalicji o zagrożeniu elektronicznym i ważnych wydarzeniach w strefie odpowiedzialności dywizji, z dokładnością umożliwiającą pomoc w procesie planowania działań przez G-2 Wielonarodowej Dywizji.

Działalność polskiej grupy SIGINT ukierunkowana była na:

- przeszukiwanie pasm częstotliwości, które mogły zawierać informacje dotyczące różnych zagrożeń dla ludzi, techniki bojowej i obiektów w strefie odpowiedzialności wielonarodowej dywizji;
- przechwytywanie relacji radiowych o zidentyfikowanym źródle lub obiekcie;
- identyfikowanie źródeł pracujących na przechwyconych częstotliwościach oraz tłumaczenie ważnych informacji przechwyconych tekstem otwartym;
- informowanie G-2 wielonarodowej dywizji w formie specjalnych raportów (określonych w standardowej procedurze operacyjnej) o zagrożeniach;
- gromadzenie i identyfikowanie informacji zakwalifikowanych do baz danych. Głównie były to zidentyfikowane częstotliwości wykorzystywane przez stronę przeciwną;
- utrzymywanie wymiany informacji z komórką rozpoznawczą sił wielonarodowych.

Zakres odpowiedzialności grupy SIGINT zawierał się w:

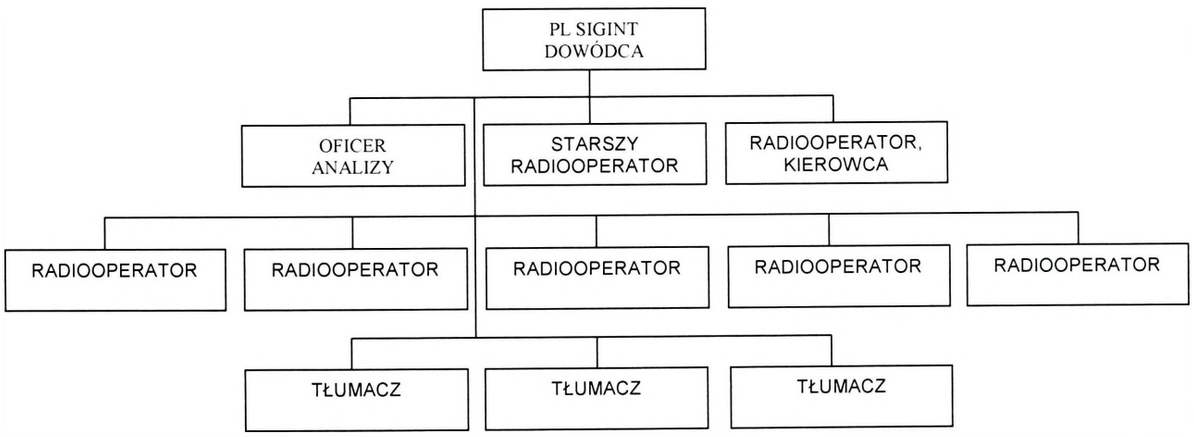
- prowadzeniu rozpoznania z bazy ECHO, którego celem było zdobycie informacji o środkach radioelektronicznych oraz systemach radiokomunikacyjnych;
- dostarczaniu dowództwu wielonarodowej dywizji informacji niezbędnych do organizowania procesu ochrony wojsk, w szczególności alarmowanie i ostrzeganie na wypadek zagrożenia.

Działalność rozpoznania sygnałowego określona była w procedurach jego wykorzystania. Procedury dostosowywane były do sytuacji operacyjnej panującej w określonym czasie. Przykładowe procedury wykorzystania grupy SIGINT przedstawiają się następująco:

- posterunek rozpoznania grupy SIGINT rozwijany na terenie stacjonowania sił wielonarodowej dywizji (na terenie bazy);
- grupa SIGINT realizuje zadania w formie dyżurowej zgodnie z harmonogramem opracowanym przez dowódcę grupy;

- zmiana miejsca rozwinięcia sprzętu rozpoznania sygnałów zależna jest od aktualnej sytuacji oraz poziomu bezpieczeństwa w strefie odpowiedzialności;
- militarna analiza przechwyconych relacji radiowych jest prowadzona przez analityków grupy danych, po wcześniejszym tłumaczeniu jawnej wymiany przez sekcję tłumaczy;
- wszystkie informacje użyteczne dla potrzeb sił wielonarodowych muszą być umieszczane w bazie danych;
- współpraca z grupami SIGINT innych narodowości powinna następować poprzez G-2 sił wielonarodowych (szczebel nadrzędny);
- grupa SIGINT otrzymuje i prowadzi dokumentację bojową zgodnie z poleceniami szefa G-2 wielonarodowej dywizji;
- archiwizacja danych z rozpoznania SIGINT realizowana jest codziennie.

Struktura grupy rozpoznania sygnałowego (SIGINT) przedstawiona jest na rys. 4.1.



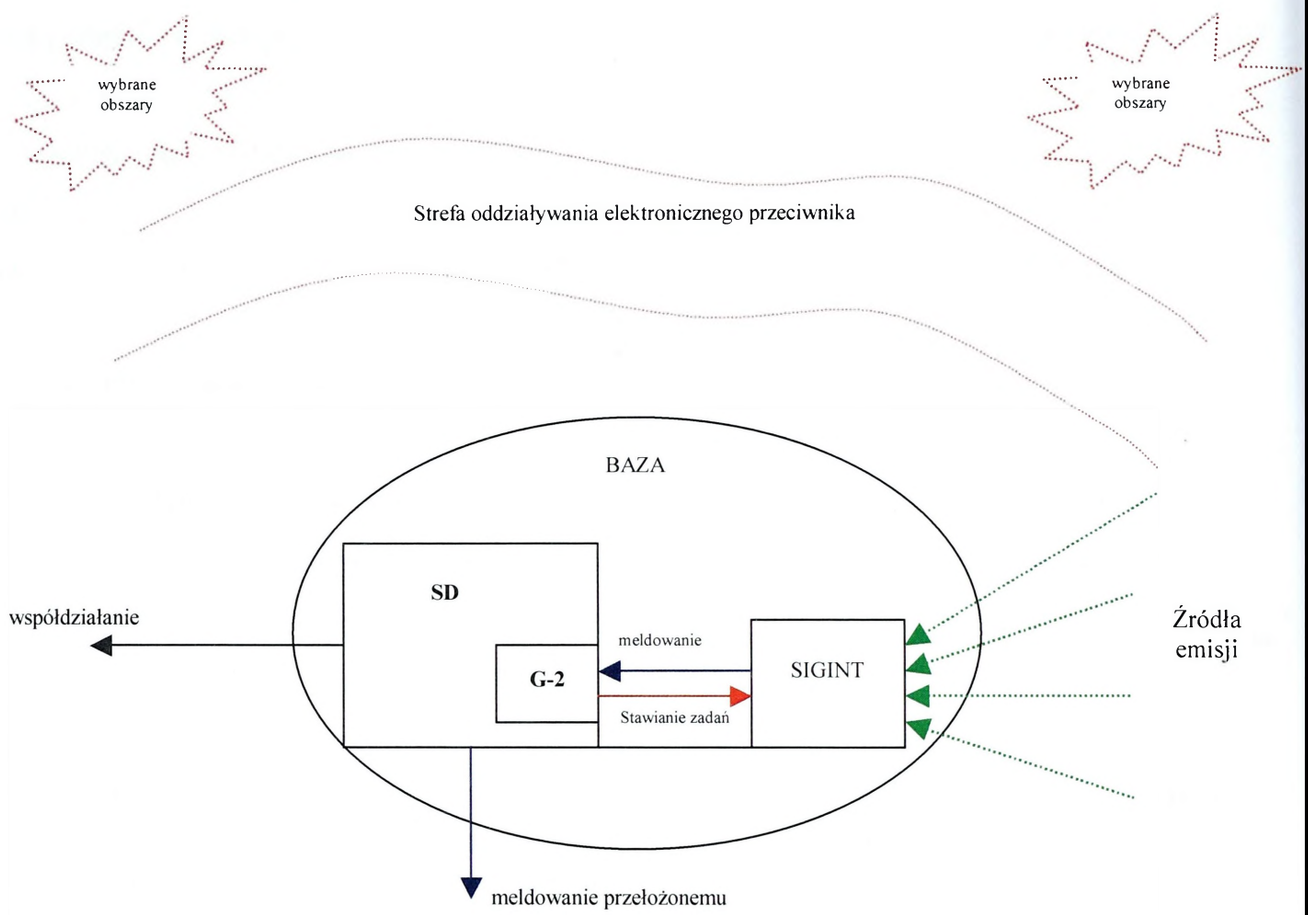
Źródło: SOP PL SIGINT z 4 zmiany PKW Irak.

Rys. 4.1. Struktura grupy rozpoznania sygnałowego (SIGINT).

Praca na stanowisku rozpoznania sygnałowego prowadzona była całodobowo. Nad podziałem zadań i zmian czuwał dowódca grupy. Przechwyconą relację łączności analizował oficer analizy, a następnie tekst tłumaczony był na język angielski. Wnioski z prowadzonego rozpoznania SIGINT dostarczane były do komórki rozpoznawczej.

Dokonując analizy środowiska bezpieczeństwa w zakresie rozpoznania elektronicznego zasadnym jest wskazać obszary intensywnej pracy urządzeń elektronicznych

strony przeciwnej oraz obszary funkcjonalne relacji: SIGINT – dowództwo sił wielonarodowych.



Źródło: opracowanie własne

Rys. 4.2. Obszary intensywności elektronicznej i funkcjonalne.

Na rys. 4.2 przedstawiono schematycznie obszary funkcjonalne i intensywności elektronicznej. W ramach obszarów intensywności elektronicznej, zespół autorski wyróżnił strefę oddziaływania elektronicznego oraz wybrane obszary. Jako strefę oddziaływania elektronicznego przyjęto obszary terenowe z których przeciwnik może prowadzić działania w spektrum elekromagnetycznym bezpośrednio zagrażające siłom wielonarodowym (wymianę radiową przy organizacji ataków na bazę i patrole działające poza nią, a także zdalne odpalanie ładunków wybuchowych).

Wybrane obszary dotyczą przewidywanych rejonów terenowych w których strona przeciwna będzie wykorzystywała środki elektroniczne, lecz bez bezpośredniego zagrożenia dla sił biorących udział w operacji wielonarodowej.

Powiązania funkcjonalne przedstawione pomiędzy grupą SIGINT a G-2 dotyczą pionowej relacji wymiany informacji. Z rozpoznania sygnałowego przedstawiane są meldunki

z pracy bojowo-rozpoznawczej grupy do komórki rozpoznawczej, natomiast odwrotnie, stawiane są zadania dotyczące prowadzonej działalności SIGINT.

Wewnątrz sztabu występujące relacje są poziome tzn. G-2 informuje zainteresowane komórki G-3 i G-6 o wynikach prowadzonego rozpoznania, wskazuje na wynikające z tego zagrożenia zarówno w sferze bezpieczeństwa fizycznego jak i elektronicznego. Powiązania funkcjonalne na zewnątrz sztabu wynikają z potrzeby meldowania przełożonemu o wynikach rozpoznania sygnałowego oraz w ramach współdziałania, informowanie sąsiadów o możliwym zagrożeniu dla ich sił.

4.3.2. Analiza środków ochrony elektronicznej wewnętrznej i zewnętrznej

Bezpieczeństwo sił jest priorytetem. Jak wskazano wcześniej, zagrożenia występujące w operacjach wielonarodowych są wieloaspektowe. Do każdego rodzaju zagrożenia należy podejść indywidualnie, czyli zastosować adekwatne do zagrożenia środki ochrony. Zespół autorski pragnie przedstawić możliwe do wykorzystania środki ochrony elektronicznej, w zależności od rodzaju zagrożenia.

Zdalnie odpalane ładunki wybuchowe stanowią jedno z większych zagrożeń współczesnego pola walki w operacji wielonarodowej. Jednym ze sposobów ochrony przed takimi ładunkami jest zakłócanie transmisji wykorzystywanej do bezprzewodowego inicjowania wybuchu ukrytych min pułapek i bomb. Umożliwiają to zestawy m.in. EJAB (Electronic Jammer Against Bombs)[15]. Wykonywane są one w dwóch wersjach: EJAB-MB-C i EJAB-B. Podstawowymi elementami systemu są: urządzenie EJAB-B, zestaw anten, komputer (laptop) umożliwiający programowanie częstotliwości emisji zakłóceń oraz źródło zasilania. System można montować na różnego typu pojazdach, natomiast wersję EJAB-MB-C również w obiektach. Zapewnia blokowanie łączności dla wielu częstotliwości w pasmach VHF, UHF które można programować za pomocą zewnętrznego komputera. Współpracuje z antenami zamontowanymi na pojeździe. Zasilanie urządzenia może być realizowane z sieci pokładowej pojazdu lub z sieci prądu przemiennego (z agregatu będącego na wyposażeniu zestawu lub z sieci energetycznej). Zestaw ten umożliwia osłonę do trzech pojazdów przed inicjacją wybuchu drogą radiową z telefonu komórkowego, telefonu bezprzewodowego, CB radio, walkie-talkie, urządzeń wykorzystywanych w modelach zdalnie sterowanych.

Kolejnym urządzeniem wchodzącym w skład systemu bezpieczeństwa elektronicznego baz wojskowych był radar obserwacji pola walki. Radary rozpoznania pola

[15] Opracowano na podstawie materiałów reklamowych firmy RADWAR SA

walki są urządzeniami wykorzystywanymi na polu walki oraz w operacjach innych niż wojna, np. do ochrony baz wojskowych, lotnisk i innych ważnych obiektów.

Do monitorowania terenu wokół baz sił wielonarodowych może być wykorzystywany radiolokator SOWA. Sensor obserwacyjno-wykrywający SOWA[16] jest przenośnym radarem o fali ciągłej służącym do wykrywania i lokalizacji (określania współrzędnych: odległość, azymut) obiektów ruchomych pojawiających się na dozorowanym obszarze. Lekka konstrukcja oraz łatwość przenoszenia i instalacji w każdych warunkach daje możliwość zastosowania urządzenia do ochrony: granicy, obszarów i obiektów. Dostępne tryby pracy umożliwiają obserwację dookolną, wybranych sektorów lub wybranego kierunku. Urządzenie sterujące zapewnia zdalne bezprzewodowe przesyłanie danych na odległość 100 m, pomiędzy konsolą operatora i radarem. Dodatkowo można konsolę wykorzystać jako detektor pracujący w systemie sieci LAN. Informacje o położeniu wykrytego obiektu ułatwiają jego identyfikację przy użyciu innych urządzeń, np. sterowanych kamer CCTV. Zestaw składa się z następujących elementów: radar, komputer (konsola operatora), statyw oraz źródła zasilania. Radar SOWA umożliwia wykrywanie obiektów ruchomych w odległości do 2,4 km poprzez wybieralne zakresy detekcji: 300 m, 600 m, 1200 m, 2400 m. W czasie pracy radiolokator SOWA automatycznie inicjuje i śledzi do 30 wykrytych obiektów z ciągłym ich zobrazowaniem wraz z podawaniem historii ich ruchu.

Innym przedstawicielem urządzeń radiolokacyjnych przeznaczonych do wykrywania i lokalizacji obiektów ruchomych, a wykorzystywany do ochrony baz wojskowych był radar AN/PPS-5C MSTAR[17]. Jest urządzeniem radiolokacyjnym służącym do wykrywania, lokalizowania, śledzenia oraz klasyfikowania obiektów poruszających się w odległości do 42 km. Może być zasilany z baterii lub sieci pokładowej wozu bojowego. Posiada możliwość lokalizowania miejsc wybuchu pocisków artyleryjskich, co może być wykorzystywane do oceny skuteczności ognia. Głównym przeznaczeniem radaru jest wykrycie i lokalizacja obiektów na powierzchni ziemi oraz identyfikowanie nisko lecących statków powietrznych. Radar AN/PPS-5C MSTAR jest urządzeniem impulsowo-dopplerowskim. Generuje i wysyła ciąg krótkich impulsów rzędu mikrosekund. Przeszkody zbudowane z materiału przewodzącego mają zdolność do odbijania fal elektromagnetycznych. Fala odbita powraca do radaru i stanowi echo radarowe. Na podstawie pomiaru czasu od wypromieniowania energii i powrotu w postaci echa obliczana jest odległość do obiektu. Zasada pracy jest

[16] Tamże.
[17] M. Dejek, Taktyczny radar rozpoznania Pola walki AN/PPS-5C MSTAR, PWL 8/2006, s. 71.

podobna do radiolokatora SOWA. Odległości z jakich radar może wykryć dany obiekt przedstawiono w tabeli 4.1.

Tabela 4.1.

Zasięgi wykrywania radaru MSTAR

CEL	Radar I wersja (km)	Radar II wersja (km)
Człowiek	**10**	**12**
Pojazd lekki	**15**	**24**
Pojazd ciężki	**24**	**36**
Mały śmigłowiec, samolot	**10**	**14**
Śmigłowiec uderzeniowy	**15**	**20**
Wybuch pocisku	**12**	**15**

Źródło: M. Dejek, Taktyczny radar rozpoznania Pola walki AN/PPS-5C MSTAR, PWL 8/2006, s.72.

Radar charakteryzują następujące dane taktyczno-techniczne[18]:

- częstotliwość pracy – pasmo Ku - (ok.17 GHz – 4 częstotliwości oddalone o 37,5 MHz),
- czas trwania impulsu - 0,1 lub 6,5μs,
- częstotliwość powtarzania impulsów – 3155 lub 7555 Hz,
- moc impulsowa – 4 W,
- moc średnia - 112 mW,
- minimalna prędkość radialna obiektu –3 km/h,
- pobór mocy < 50 W,
- całkowita waga systemu – ok. 35 kg

Radar MSTAR może pracować w trybach rozpoznanie i śledzenie. Tryb rozpoznanie służy do wykrywania poruszających się obiektów. Wykryte obiekty i trasy ich przemieszczania zobrazowane są na wyświetlaczu. Przy pracy automatycznej, gdzie definiowany jest sektor obserwacji, o wykryciu obiektu operator informowany jest poprzez sygnał dźwiękowy. Antena radaru zapewnia prowadzenie rozpoznania z szerokością wiązki promieniowania w płaszczyźnie poziomej - $2,5^0$, natomiast w płaszczyźnie pionowej $3,1^0$. Tryb pracy śledzenie stosuje się w celu dokładnego przedstawienia obszaru rozpoznania. Przy tym rodzaju pracy wycinek sektora rozpoznania jest zobrazowany w postaci kwadratu o wymiarach 1,5x1,5 km. Istnieje możliwość identyfikacji rodzaju obiektu, dzięki

[18] Opracowano na podstawie materiałów reklamowych firmy DRS Technologies.

odsłuchaniu składowej dopplerowskiej sygnału odbitego. Każdy obiekt wprowadza, do echa radarowego, właściwą dla siebie sygnaturę. Na podstawie wyodrębnionej składowej możliwe jest sklasyfikowanie wykrytego obiektu. W trybie AUDIO (możliwość odsłuchania składowej doplerowskiej) antena jest nieruchoma i opromieniowuje jedynie wybrany obiekt. Takie rozwiązanie ogranicza moc sygnału wypromieniowanego z urządzenia.

Stacje radiolokacyjne umożliwiają również określanie współrzędnych strzelających baterii artylerii przeciwnika w każdych warunkach pogodowych i o każdej porze doby. Zasada działania stacji polega na dokonywaniu analizy toru lotu pocisku. Wynikiem analizy jest określenie współrzędnych rejonów rozwinięcia stanowisk ogniowych strzelającej artylerii (dział i moździerzy). Po otwarciu ognia przez baterie artylerii (moździerzy) obsługa stacji jest w stanie określić jej współrzędne, zanim wystrzelone pociski spadną w rejonie celu.

Urządzenia radiolokacyjne umożliwiają stwierdzenie poruszającego się obiektu w dozorowanym obszarze. W działaniach wielonarodowych ważnym jest jednak zidentyfikowanie obiektu, określenie potencjalnego zagrożenia dla sił wielonarodowych ze strony tego obiektu. Pomocnymi w identyfikowaniu obiektów wykrytych przez radiolokatory są urządzenia optroniczne. Przedstawicielami takich urządzeń są kamery termowizyjne i kamery dzienno-nocne dalekiego zasięgu oraz systemy optroniczne dzienno-nocne (CCTV/IR) przeznaczone do dozoru i obserwacji terenu. Wykorzystywanie tych urządzeń zwiększa świadomość sytuacyjną żołnierzy, możliwości oceny zagrożenia, natychmiastowej reakcji bez dodatkowego ryzyka i stresu jaki często towarzyszy zasadzce lub czuwaniu nad bezpieczeństwem.

Systemy optroniczne mogą być w tym zakresie używane do:

- ochrony baz wojskowych;
- ochrony półstałych baz wojskowych;
- ochrony posterunków kontrolnych;
- ochrony obiektów infrastruktury kluczowej (elektrownie, rafinerie, instalacje wydobycia, przeładunku, magazynowania ropy naftowej);
- ochrony placówek dyplomatycznych w szczególnych rejonach;
- dozoru odcinków drogowych;
- dozoru terenu.

Przedstawicielem systemów optronicznych, nie wykorzystywanym dotychczas w działaniach wielonarodowych, jest BLACK WOLF firmy EMX[19]. Jest to zamontowany na

[19] http://www.cenrex.com/dokumenty/CNRX_EMX_Black_Wolf.pdf

przyczepie jednoosiowej maszt o wysokości 7,62 m (rozwinięty), będący nośnikiem sensorów oraz modułu łącza radiowego. Podstawowy moduł sensorów obejmuje kamerę termowizyjną serii EMX MidWatch oraz zaawansowaną kolorową kamerę CCD z 26 krotnym zoomem optycznym oraz 10 krotnym zoomem elektronicznym (łączny współczynnik powiększania x 260). Zapewnia obserwację dzienno-nocną na średnich i dalekich dystansach. System jest niemalże samowystarczalny pod względem zasilania panele słoneczne uzupełnione są akumulatorami o długim cyklu żywotności (7 dni pracy bez oświetlenia słonecznego). Zapewnia to minimalne wymagania odnośnie codziennej obsługi sprzętu. Kamery termowizyjne serii MidWatch pozwalają na wykrycie człowieka z odległości od 1,5 km do 3,5 km, oraz pojazdu z odległości od 3 km do 6 km. W pojeździe C2 WOLF PACK operator może kontrolować do czterech systemów BLACK WOLF będących w zasięgu do ok. 6 km. Konfiguracja WOLF PACK pozwala na dozór terenu o długości ok. 20 km oraz szerokości do 6 km, co pozwala na ograniczenie liczby personelu. Taki system może być wykorzystywany w bazach stacjonarnych, jednak duża mobilność umożliwia jego wykorzystanie w organizowaniu ochrony posterunków kontrolnych i czasowego pobytu sił wielonarodowych poza bazą.

W czasie przemieszczania lub wykonywania zadań patrolowych bądź konwojowych zagrożeniem dla sił wielonarodowych jest ostrzał z broni osobistej, moździerzy RPG lub PPK. Dlatego tak ważne jest wykrycie i wskazanie miejsca prowadzenia ostrzału na konwój (patrol). Urządzeniem realizującym taką funkcję jest akustyczny system lokalizacji strzału i strzelca PILAR. System do lokalizacji strzałów i strzelca typu PILAR MK-IIw[20] należy do środków rozpoznania akustycznego (ACINT -Acoustic Intelligence) szczebla taktycznego. Przeznaczony jest do automatycznej detekcji strzałów i lokalizacji broni małych kalibrów (5.45 mm do 20 mm), RPG, moździerzy i PPK. Funkcją systemu jest zobrazowanie w czasie rzeczywistym parametrów określających azymut (z dokładnością 2^0 na postoju i 5^0 w ruchu), elewacje (z dokładnością 5^0) i odległości do strzelca (z dokładnością do 20 %) do 1500 m. System zapewnia stosowanie go zarówno w marszu jak i na postoju z zachowaniem zbliżonych parametrów odczytu zobrazowanych danych. Wersja mobilna systemu, zdaniem zespołu autorskiego, powinna być montowana na każdym pojeździe będącym na wyposażeniu sił wielonarodowych. Wersja stacjonarna umożliwia stosowanie systemu w każdych warunkach terenowych do osłony wojsk.

[20] http://www.01db-metravib.com/fileadmin/pdf/BU4/gb_GDS_Vehicle.pdf

Przypadki ataków terrorystycznych na bazy nie są jedynym zagrożeniem. Dochodzi do prób wejścia, na teren baz sił wielonarodowych, osób nieupoważnionych o każdej porze doby i w każdych warunkach atmosferycznych. Celem wtargnięć jest często działalność typowo kryminalna (kradzież sprzętu, dokumentów, części zamiennych, broni i amunicji, żywności lub leków).

Obiektami wymienianymi w literaturze jako najbardziej zagrożonymi atakami terrorystów są składy materiałów budowlanych, żywności i leków[21]. W zainteresowaniu organizacji przestępczych występują nadal obiekty elektroniczne (tj. węzły łączności, radiolatarnie radionawigacyjne, wieże kontroli lotów, stacje radiolokacyjne), magazyny (materiałów pędnych, uzbrojenia, części elektronicznych, leków), garaże ze sprzętem, ujęcia wody pitnej, stacje zasilania energetycznego oraz budynki (kontenery) mieszkalne[22]. Wyżej przedstawione obiekty powinny podlegać szczególnej ochronie, zarówno bezpośredniej jak i technicznej. W ramach organizowania ochrony technicznej (przy wykorzystaniu urządzeń elektronicznych) należy dążyć do zapewnienia wysokiego prawdopodobieństwo wykrycia, z jednoczesną eliminacją przypadkowych i fałszywych alarmów.

W ochronie baz sił wielonarodowych tworzone są systemy aktywnego dozoru elektronicznego. W ich skład może wchodzić kilka radiolokatorów np. MSTAR oraz kamery do obserwacji w warunkach dobrej widoczności oraz w podczerwieni. Zapewnia to weryfikację alarmów otrzymywanych z rozpoznania radiolokacyjnego poprzez sprawdzenie obrazowe wycinka terenu z którego pochodził sygnał alarmowy. Unika, lub przynajmniej ogranicza, się w ten sposób ilość alarmów dla sił ochrony bazy, które muszą reagować na każde zagrożenie. Całość wykorzystywana jest do obserwacji i dozorowania terenu przylegającego do bazy sił wielonarodowych. Celowym jest montowanie urządzeń obserwacji i dozoru na maszcie lub na wieży w celu zwiększenia zasięgu oraz zapewnienia obserwacji dookolnej i dobrego wglądu w teren.

Urządzeniami ostrzegającymi o wtargnięciach do ochranianych miejsc są przede wszystkim systemy czujników. System czujników można podzielić na podsystemy: wewnętrzny i zewnętrzny[23]. Podsystem zewnętrzny zapewnia ochroną bazy na zewnątrz ogrodzenia (urządzenia wymienione wyżej), natomiast podsystem wewnętrzny dotyczy ważnych pomieszczeń i obiektów, które zostały wskazane w rozdziale trzecim.

---

[21] W. Scheffs, Elektroniczny wartownik baz wojskowych, PWL nr 6/2008, s.38.
[22] Tamże, s.38.
[23] Tamże, s.39.

4.3.3. Analiza obiegu informacji

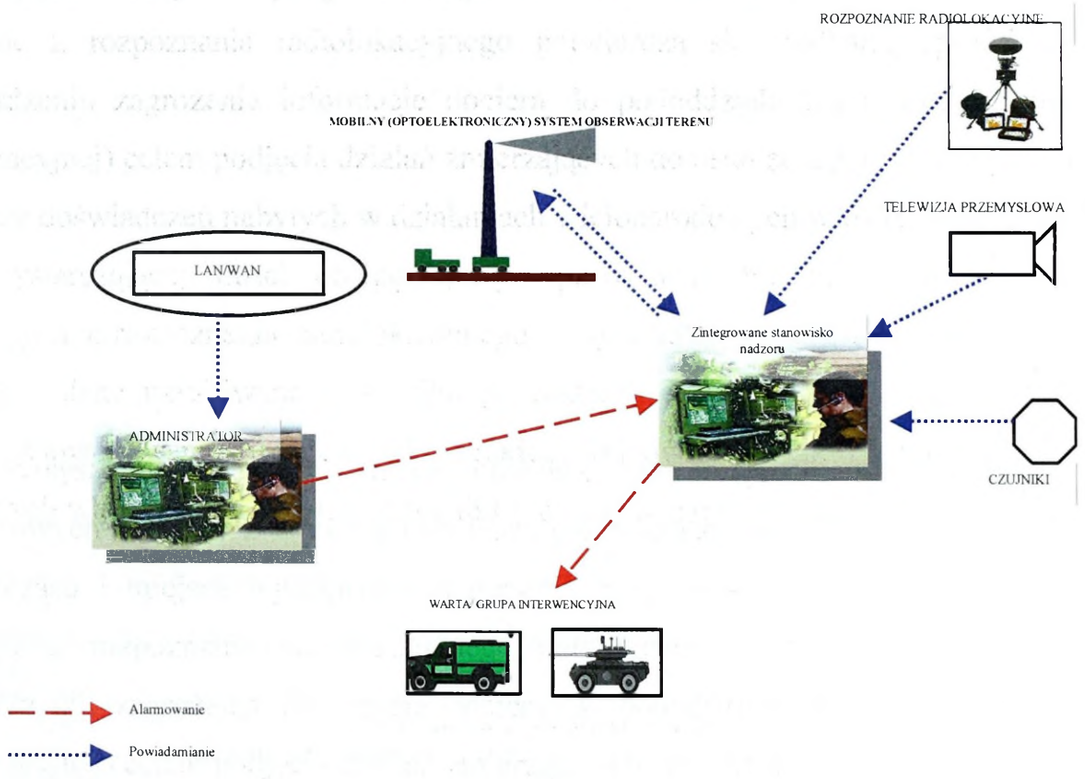
Zachowanie bezpieczeństwa elektronicznego w działaniach wielonarodowych zależne jest w dużym stopniu, od prawidło zorganizowanych relacji powiadamiania o istniejącym zagrożeniu. Każda przesłanka zagrożenia w zakresie elektronicznym powinna być zgłaszana do osób bezpośrednio odpowiedzialnych za bezpieczeństwo w określonej sferze działalności elektronicznej.

W obszarze sieci i systemów teleinformatycznych powinien być powołany administrator, który sprawuje nadzór nad organizacją bezpieczeństwa oraz wykonuje wszystkie prace niezbędne do efektywnego zarządzania siecią teleinformatyczną. Stosując odpowiednie środki i metody kontroli dostępu zapewnia, że wyłącznie autoryzowany personel posiada bezpośredni dostęp do sieci teleinformatycznej. Zapewnia odpowiedni stan bezpieczeństwa sieci poprzez udzielanie porad użytkownikom, a także organizuje i prowadzi szkolenia z zakresu bezpieczeństwa. Administrator sieci zbiera informacje o zagrożeniach. Wszystkie informacje dotyczące zjawisk zauważonych przez użytkowników, a mogące naruszyć bezpieczeństwo sieci teleinformatycznej, osób, sprzętu, oprogramowania, komunikacji, dokumentów lub bezpieczeństwa fizycznego muszą być do niego niezwłocznie zgłoszone. Zgłoszenie powinno następować w sposób sformalizowany np. w postaci meldunku
o naruszeniu bezpieczeństwa w systemie. Przypadki wykrycia oprogramowania złośliwego (wirusów komputerowych) również zgłasza się do administratora sieci, który w takim przypadku przeprowadza analizę i bada przyczyny nieprawidłowego działania sieci.

W zakresie bezpieczeństwa łączności odpowiedzialność ponosi komórka G6. Szef tej komórki zbiera wszystkie informacje dotyczące symptomów obniżenia bezpieczeństwa łączności. Odpowiada za zapewnienie kompatybilności elektromagnetycznej, przestrzeganie przepisów korespondencji radiowej, wykorzystanie środków łączności oraz wdrażanie procedur zapewniających odpowiedni poziom bezpieczeństwa łączności.

Przy zapewnieniu bezpieczeństwa przeciwdziałania elektronicznego, obejmującego skryte użycie urządzeń zakłócających zapalniki inicjowane drogą radiową, zdaniem zespołu autorskiego, zbieraniem informacji powinna zajmować się komórka rozpoznawcza. W porozumieniu z komórką operacyjną i łączności powinna planować zakłócanie pasm częstotliwości wykorzystywanych do zdalnego inicjowania wybuchu, z jednoczesnym pozostawieniem przedziałów częstotliwości wolnych od zakłóceń, a wykorzystywanych przez siły wielonarodowe do łączności.

W systemie bezpieczeństwa elektronicznego monitorującego otoczenie wokół baz i sił manewrowych jest stworzony obieg informacji gwarantujący reakcję sił ochronnych właściwą co do czasu i miejsca wystąpienia zagrożenia bezpieczeństwa. Informacje o zagrożeniu uzyskane z rozpoznania radiolokacyjnego potwierdza się środkami optronicznymi. Po potwierdzeniu zagrożenia informacje dociera do pododdziału alarmowego (warty, grupy interwencyjnej) celem podjęcia działań zmierzających do usunięcia potencjalnego zagrożenia. Z analizy doświadczeń nabytych w działaniach wielonarodowych w Iraku wynika, że niestety brak wystarczającej ilości obsług sprzętu powodował błędną interpretację sygnałów alarmowych z rozpoznania radiolokacyjnego. Częste fałszywe alarmy sprawiły, że zaczęto ignorować dane uzyskiwane w wyniku prowadzenia tego rodzaju rozpoznania. Fałszywe alarmy spowodowane również były brakiem odpowiedniej ilości wyszkolony obsług, umiejących właściwie interpretować wyniki prowadzonego rozpoznania.



Źródło: opracowanie własne.

Rys. 4.3. Obieg informacji w monitorowaniu bezpieczeństwa bazy sił wielonarodowych.

Celem zabezpieczenia właściwego obiegu informacji rozbudowuje się instalację okablowania systemu transmisji alarmów (powiadamiania), np. o strukturze gwiazdy. Okablowanie powinno być nadmiarowe, czyli pozwalające na podłączanie budowanych w przyszłości dodatkowych systemów ochrony. Zamiast łączy kablowych można wykorzystać łącza radiowe pomiędzy centrum nadzoru a poszczególnymi monitorowanymi

podsystemami. Sposób realizacji powinien przede wszystkim gwarantować zapewnienie niezawodności i bezpieczeństwa transmisji. Gwarancję niezawodności i bezpieczeństwa, zdaniem zespołu autorskiego, zapewnia sieć światłowodowa o strukturze pierścienia z punktami przyłączeniowymi. Ilość punktów przyłączeniowych zależna jest od ilości elementów monitorujących, jednak należy pamiętać o nadmiarowości przyłączeń (na potrzeby rozbudowy systemów ochrony elektronicznej).

4.4. Wnioski

1. Efektem zagrożenia elektronicznego jest brak bezpieczeństwa własnych sił i środków, wynikające z użycia systemów elektronicznych przez stronę przeciwną. Wiąże się nierozerwalnie z możliwością zdobycia informacji bezpośrednio z systemów elektronicznych sił wielonarodowych oraz wykorzystanie przez stronę przeciwną środków elektronicznych celem destrukcyjnego oddziaływania.
2. W ramach bezpieczeństwa sił wielonarodowych w bazach, stosowanie środków rozpoznania elektronicznego sprzyja wczesnemu wykryciu zagrożeń wynikających z wykorzystania przez potencjalnego przeciwnika środków rażenia o zasięgu przekraczającym zasięg rozpoznania wzrokowego.
3. W działaniach sił wielonarodowych poza bazą użycie aktywnych środków zakłócania elektronicznego minimalizuje możliwość ataku na konwoje przy wykorzystaniu improwizowanych ładunków wybuchowych inicjowanych drogą radiową.
4. W zakresie bezpieczeństwa sieci i systemów teleinformatycznych stosowanie procedur bezpieczeństwa obowiązujących w kraju minimalizuje możliwość zdobywania informacji przez stronę przeciwną z tych zasobów informacyjnych, ale nie jest rozwiązaniem idealnym. Procedury innego kraju mogą nie być szczelne i informacje mogą zostać utracone lub przechwycone. Mając na uwadze wielonarodowość działań, należy opracowywać stosowne procedury na potrzeby wszystkich uczestników operacji wielonarodowej.
5. Organizacja systemu łączności sił wielonarodowych ogniskuje wokół zapewnienia kompatybilności elektromagnetycznej i sprzętowej. Nie traci na aktualności również przestrzeganie przepisów korespondencji radiowej oraz skryte użycie urządzeń wykorzystywanych przy realizacji łączności.

6. Wykorzystanie sił i środków rozpoznania elektronicznego dostarcza informacji niezbędnych w procesie organizowania ochrony sił oraz alarmuje i ostrzega w wypadku zagrożenia.
7. W systemie monitorowania otoczenia należy stosować dualizm rozpoznania, każdy sygnał powiadamiający o zagrożeniu powinien być zweryfikowany innym środkiem elektronicznym.
8. W ramach ochrony baz zasadne jest tworzenie sieci gwarantujących niezawodność działania i bezpieczeństwo transmisji z jednoczesnym zapewnieniem możliwości rozbudowy systemu ochrony (redundancja w kanale przesyłu informacji).
9. Bezpieczeństwo w działaniach wielonarodowych wynika bezpośrednio z zagrożeń zewnętrznych (ze strony potencjalnego przeciwnika) jak również wewnętrznych (z różnic kulturowych, mentalności, wyposażenia oraz rozwiązań narodowych w zakresie zapewnienia bezpieczeństwa przez poszczególne narodowości biorące udział w działaniach wielonarodowych).

5. EFEKTY POZNANIA

Przeprowadzone w ramach pracy badania ugruntowały przekonanie zespołu autorskiego o potrzebie i aktualności ich podjęcia. Współczesne zagrożenia występujące w operacjach pokojowych dla sił wielonarodowych to problem zajmujący nie tylko specjalistów wojskowych, ale całe grono specjalistów cywilnych zajmujących się problematyką bezpieczeństwa. Z racji wielu uwarunkowań zagrożenia bezpieczeństwa dla sił, w znacznej większości asymetryczne, stały się przedmiotem analiz wielu ośrodków naukowo -badawczych.

Mając na uwadze obszar zagrożeń, z jakimi spotykają się i będą się spotykać siły wielonarodowe realizujące zadania w ramach operacji wielonarodowej, należy się liczyć z aktywnym oddziaływaniem zarówno sił, przeciwko którym wysłano wojska z misję rozjemczą jak i wielu grup eksternistycznych, terrorystów, czy pospolitych grup przestępczych. Celem każdej z wymienianych ugrupowań jest i będzie destabilizowanie sytuacji w obszarze działania sił wielonarodowych. Istnienie wieloaspektowego zagrożenia związanego z użyciem broni niekonwencjonalnej, atakami przy wykorzystaniu improwizowanych ładunków wybuchowych (IED), porwaniami, napadami, zabójstwami przez strzelców (snajperów) jest bardzo duża. W tym kontekście zasadniczymi celami bezpieczeństwa wojsk w operacjach wielonarodowych będzie sprawne i skuteczne rozpoznanie zagrożeń, a co za tym idzie, podjęcie działań mających na celu minimalizację ich skutków. Pomysłowość terrorystów i ich nieprzewidywalność stanowi główne źródło zagrożeń co utrudnia zapewnienie bezpieczeństwa. Wielość i różnorodność zagrożeń wymaga od specjalistów wojskowych szerokiego spojrzenia na procedury bezpieczeństwa, zarówno ochrony fizycznej, jak i elektronicznej. Wśród obiektów lub systemów, które jako pierwsze mogą być obiektami ataku można wyróżnić: koszary, magazyny, budynki sztabowe, węzły łączności, a także systemy telekomunikacyjne, teleinformatyczne, energetyczne itd. Ich podatność na dezorganizację, oddziaływanie ogniowe lub działania w przestrzeni fal EM powoduje określone skutki destabilizacji działań. Wynika z tego, że zapewnienie właściwego działania wojsk i systemów przez nie wykorzystywanych w obszarze działania sił wielonarodowych jest jednym z podstawowych wymogów bezpieczeństwa.

W wyniku prowadzonych badań ustalono, że zadania dla pododdziałów ochrony i obrony powinny być realizowane według planu opartego na jednolitej myśli zapewnienia

bezpieczeństwa żołnierzom. Działania sił ochrony, organizowane w sposób kompleksowy z racjonalnym wykorzystaniem jakościowo nowych środków ochrony, stwarzają warunki stosunkowo pełnego zidentyfikowania najważniejszych obszarów zagrożeń oraz elementów je powodujących. Niezbędnym, zatem jest wykonanie szeregu przedsięwzięć w zakresie identyfikacji zagrożeń bezpieczeństwa fizycznego i elektronicznego wojsk biorących udział w operacji wielonarodowej.

Zaistniała sytuacja problemowa wymagała przeprowadzenia rzetelnych badań, których wyniki były asumptem do rozwiązań praktycznych w zakresie określenia w pierwszej kolejności uwarunkowań bezpieczeństwa fizycznego i elektronicznego, a następnie zaproponowania rozwiązań strukturalnych komórki bezpieczeństwa w operacji wielonarodowej.

Celem niniejszej pracy było zidentyfikowanie zagrożeń fizycznych i elektronicznych dla wojsk i baz wojskowych w operacjach wielonarodowych. Sprecyzowany cel wymagał określenia i postawienia szeregu problemów badawczych, na które zespół autorski poszukiwał odpowiedzi:

1. Jakie występują zagrożenia dla wojsk wielonarodowych podczas realizacji zadań?
2. Jakie warunki muszą być spełnione, aby zapewnić bezpieczeństwo fizyczne i elektroniczne wojsk wielonarodowych?
3. Jakie są potrzeby i możliwości ochrony fizycznej w bazach wojskowych i podczas realizacji zadań poza bazą przez siły wielonarodowe?
4. Jakie są potrzeby i możliwości obrony elektronicznej baz wojskowych i wojsk podczas realizacji zadań poza bazą przez siły wielonarodowe?
5. Jaka powinna być rola i zadania podsystemów ochrony fizycznej i elektronicznej wspomagających system bezpieczeństwa sił wielonarodowych?

Szczególną uwagę zespół autorski poświęcił tym obszarom, w których wskazana jest konieczność wprowadzenia zmian. Wynikają one z wielu uwarunkowań. Przede wszystkim zmiany w dotychczasowym ujęciu przedmiotu badań. W obszarze zainteresowania zespołu autorskiego znalazły się również problemy wynikające z uwarunkowań zarządzania i kierowania, w tym kierowania przez zespoły funkcyjne zbiorowością międzynarodową.

W wyniku prac badawczych ustalono, że zagrożenie, zarówno wewnętrzne jak i zewnętrzne należy traktować jako obawę o utratę wysoko cenionych wartości przez człowieka, gdzie sytuacja zagrożenia jest uświadamiana przez podmiot. Jednocześnie poczucie zagrożenia jest odwrotnie proporcjonalne do zaspokojenia potrzeby bezpieczeństwa. Bezpieczeństwo w działaniach wielonarodowych wynika bezpośrednio z zagrożeń

zewnętrznych (ze strony potencjalnego przeciwnika) ale także z wewnętrznych (z różnic kulturowych, mentalności, wyposażenia w sprzęt oraz rozwiązań narodowych w zakresie zapewnienia bezpieczeństwa przez poszczególne narodowości biorące udział w działaniach wielonarodowych).

Przyjęto, że efektem zagrożenia elektronicznego jest brak bezpieczeństwa własnych sił i środków, wynikające z użycia systemów elektronicznych przez stronę przeciwną. Wiąże się nierozerwalnie z możliwością zdobycia informacji bezpośrednio z systemów elektronicznych sił wielonarodowych oraz wykorzystanie przez stronę przeciwną środków elektronicznych celem destrukcyjnego oddziaływania.

Dla potrzeb niniejszej pracy, zespół autorski przyjął, że działania wielonarodowe są to wszystkie przedsięwzięcia sił, realizowane w ramach jednej operacji przez zgrupowania wojsk składające się z elementów więcej niż jednego państwa bez względu na to, czy należy do sojuszu państw czy nie. Jeżeli wszystkie zaangażowane państwa należą do sojuszu, to prowadzą działania sojusznicze (swoista odmiana działań wielonarodowych). Przyjęto również, że każde działania sojusznicze są działaniami wielonarodowymi, lecz nie każde wielonarodowe są sojuszniczymi. Działania wielonarodowe są w praktyce działaniami połączonymi, w których cele są realizowane przy użyciu, co najmniej dwóch rodzajów sił zbrojnych, z co najmniej dwóch państw. Działania wielonarodowe charakteryzują się dobrowolnością uczestniczenia w nich przez poszczególnych członków – państwa. Cele narodowych komponentów, w zależności od celów politycznych państw zaangażowanych, nie zawsze są zbieżne, a co za tym idzie, stanowią pewnego rodzaju zagrożenie wewnętrzne dla sił wielonarodowych.

W ramach operacji prowadzonych przez siły wielonarodowe wyodrębniono działania wojskowe, policyjne i administracyjne. Wielozakresowość działań jest przyczyną pojawiania się różnego rodzaju zagrożeń, dotyczących zarówno działań militarnych w klasycznym ujęciu, przeciwko siłom wielonarodowym, jak również działań asymetrycznych z użyciem sił terrorystycznych.

Przy tworzeniu struktur dowództwa sił wielonarodowych przedsięwzięcia powinny ogniskować wokół problemów związanych z jednakowym rozumieniem zagadnień związanych z dowodzeniem i pracą sztabu przez wszystkich uczestników, właściwym interpretowaniem kierowania działaniami, właściwym wykorzystaniem środków dowodzenia oraz zapewnieniem sprawnej komunikacji między wielonarodowymi członkami dowództwa.

W ramach zapewnienia bezpieczeństwa własnych wojsk niezbędne jest opracowanie procedur dotyczących: postępowania na SD, użycia broni w czasie wykonywania zadań

mandatowych oraz użycia środków informatycznych, łączności i rozpoznania. Istotnym warunkiem bezpieczeństwa jest posiadanie: własnych sił rozpoznania i wywiadu, sił lotniczych do kontroli przestrzeni powietrznej oraz narzędzi przymusu w stosunku do ludności cywilnej i wojskowej. Stosowanie środków rozpoznania elektronicznego sprzyja wczesnemu wykryciu zagrożeń wynikających z wykorzystania przez potencjalnego przeciwnika środków rażenia o zasięgu przekraczającym zasięg rozpoznania wzrokowego. W działaniach sił wielonarodowych poza bazą, użycie aktywnych środków zakłócania elektronicznego minimalizuje możliwość ataku na konwoje przy wykorzystaniu improwizowanych ładunków wybuchowych inicjowanych drogą radiową. W zakresie bezpieczeństwa sieci i systemów teleinformatycznych stosowanie procedur bezpieczeństwa obowiązujących w kraju minimalizuje możliwość zdobywania informacji przez stronę przeciwną z tych zasobów informacyjnych, ale nie jest rozwiązaniem idealnym. Procedury innego kraju mogą nie być szczelne i informacje mogą zostać utracone lub przechwycone. Mając na uwadze wielonarodowość działań, należy opracowywać stosowne procedury na potrzeby wszystkich uczestników operacji wielonarodowej.

W analizowanych strukturach dowództw wskazano brak jednoznacznego wyróżnienia komórki odpowiadającej za bezpieczeństwo sił wielonarodowych. Odpowiedzialność w tym zakresie jest rozproszona. Planowanie ochrony wojsk odbywa się na podstawie oceny zagrożenia, która jest punktem wyjścia do planowania działań zmierzających do minimalizacji podatności na ataki terrorystyczne. Doskonalenie technik operacyjnych oraz struktur pododdziałów przewidzianych do realizacji przedsięwzięć ochrony wojsk oraz ilość i jakość sprzętu technicznego wykorzystywanego do ochrony baz, wpływa znacząco na określenie poziomu bezpieczeństwa. Wyposażenie pododdziałów ochrony w środki techniczne ułatwiające kontrolowanie osób i pojazdów wjeżdżających na teren bazy, np. w wykrywacze materiałów wybuchowych, wykrywacze metalu, skanery czy przeszkolone psy to w obecnych operacjach wielonarodowych podstawa bezpieczeństwa traktowana jako priorytet działań.

Do realizowania zadań ochronnych należy przewidzieć etatowe pododdziały ochrony podległe bezpośrednio Komendantowi Bazy, które dysponując odpowiednimi środkami umożliwiają obsadzenie wszystkich kluczowych elementów systemu ochrony bazy. Bazy wojskowe winny być lokalizowane poza obszarami zurbanizowanymi. Pozwoli to z jednej strony bezpiecznie rozbudować bazy pod względem inżynieryjnym. Z drugiej strony umożliwi zorganizowanie głębokiego systemu ochrony i obrony na przedpolach z wykorzystaniem mobilnych patroli i punktów obserwacyjny, a tym samym wczesne

ostrzeganie wojsk w bazie o zbliżającym się przeciwniku i szybką reakcję na zaistniałe zagrożenie. Wykorzystanie sił i środków rozpoznania wzrokowego i elektronicznego zapewni dostarczenie informacji niezbędnych w procesie organizowania ochrony sił oraz zaalarmuje i ostrzeże w wypadku zagrożenia. W systemie monitorowania otoczenia należy stosować dualizm rozpoznania tzn., że każdy sygnał powiadamiający o zagrożeniu od systemu rozpozna wzrokowego powinien być zweryfikowany innym środkiem elektronicznym.

W wyniku określenia celów pracy naukowo-badawczej i sformułowania problemów badawczych autorzy sprecyzowali hipotezę roboczą:

Przenoszenie doświadczeń narodowych lub innych państw nie jest rozwiązaniem w pełni dobrym. Wnioski i doświadczenia wskazują, że to głównie zagrożenia występujące w rejonie działań dla sił wielonarodowych są wykładnią organizacji systemu bezpieczeństwa. Doraźna metoda organizowania systemu bezpieczeństwa fizycznego i elektronicznego w ramach komponentu wojsk lądowych w operacji wielonarodowej w świetle uwarunkowań zagrożeń bezpieczeństwa wydaje się niewystarczająca. Może doprowadzić do sytuacji, kiedy system bezpieczeństwa nie wypełni w wymaganym zakresie swoich elementarnych zadań. Taka sytuacja może skutkować obniżeniem zdolności bojowej komponentu lądowego i doprowadzić do znacznego obniżenia skuteczności prowadzenia operacji wielonarodowych.

Transformacja systemu bezpieczeństwa wojsk powinna przebiegać w kilku zasadniczych kierunkach:

- integracji wszystkich systemów i sposobów ochrony fizycznej i elektronicznej, zarówno organicznych jak i współpracujących, w jeden efektywny spójny system;
- poszukiwania nowych metod i sposobów zabezpieczenia przed zagrożeniami szczególnie terrorystycznymi;
- innowacji technologicznej (wprowadzanie nowych technik i narzędzi - sprzętu);
- strukturalnej - tworzenie elastycznie reagujących komórek bezpieczeństwa;
- organizacyjnej dotyczącej efektywnego koordynowania wszystkich przedsięwzięć z zakresu ochrony i obrony w działaniach wielonarodowych.
- proceduralnej – doskonalenie dotychczasowych i wypracowanie nowych procedur bezpieczeństwa.

Przy takich założeniach, zespół autorski podjął próbę przedstawienia systemu ochrony baz wojskowych oraz sposobu organizowania komórki odpowiedzialnej za bezpieczeństwo wojsk. Rozwiązanie jednak, należy traktować jako hipotezę, która powinna podlegać weryfikacji w toku dalszych badań nad problemem ochrony wojsk w operacjach wielonarodowych.

W ochronie tradycyjnej w dalszym ciągu podstawowym elementem ochrony bazy (rzadko posterunku, punktu kontrolnego) jest ogrodzenie. Jednak ogrodzenie, oparte tylko na przeszkodzie fizycznej nie występuje. Zazwyczaj, w taką przeszkodę wbudowany jest układ wykrywania elektronicznego, warunkujący pewne rozwiązania konstrukcyjne ogrodzenia zasadniczego. Wykrywanie zagrożenia na granicy strzeżonej bazy zapewniają urządzenia czujnikowe rozmieszczane na ogrodzeniu, bądź umieszczone w gruncie. Mogą to być np. czujniki o wyrównanym ciśnieniu. Składają się z elastycznych przewodów wypełnionych glikolem i zakopanych w ziemi. Każde przejście osób nad przewodami wywiera nacisk na ziemię co powoduje zmianę ciśnienia w przewodach i wyzwala sygnał alarmowy. Innym urządzeniem jest czujnik drgania ogrodzenia. Składa się z przełączników rtęciowych umieszczanych na ogrodzeniu. Warunkiem koniecznym jest, aby ogrodzenie zbudowane było z elementów elastycznych (siatka metalowa, drut kolczasty itp.) Nie celowe jest wykorzystanie tych urządzeń na ogrodzeniu stabilnym (np. betonowym). Kolejnym wykorzystywanym urządzeniem jest punktowy czujnik sejsmiczny, reagujący na wszelki zmiany drgań na ograniczonym obszarze wokół czujnika. Następnymi elementami wykorzystywanymi w zabezpieczeniu technicznym są podziemne czujniki kablowe, działające na zasadzie wykrywania fal sejsmicznych i elektromagnetycznych. Skuteczne działanie wspomnianych wyżej czujników wymaga właściwego ich rozmieszczenia i zainstalowania.

Przedstawione powyżej urządzenia mogą generować fałszywe sygnały alarmowe spowodowane np. przez zwierzęta. Zasadne jest zatem weryfikowanie alarmów systemem optycznym, lub za pośrednictwem telewizji przemysłowej (może być mało efektywne gdy np. będzie burza pisakowa). Kamery winny zapewnić obserwację całości ogrodzenia. Trudnością jest ciągłe obserwowanie podglądu z kamer, zasadne jest zatem, inicjowanie włączenia kamer przez system czujników. Sygnał alarmowy jest wtedy weryfikowany.

Przedstawione powyżej elementy systemu ochrony zapewniają sygnalizowanie przekroczenia ogrodzenia, natomiast celowym jest tworzenie pasa ochronnego bezpośrednio przed ogrodzeniem. W tych warunkach usiłowanie przekroczenia ogrodzenia jest sygnalizowane zanim się ono zacznie lub sygnalizowane jest potencjalne usiłowanie przekroczenia chronionej strefy.

Podstawowymi urządzeniami dozorowania obszaru poza ogrodzeniem powinny być detektory podczerwieni wykrywających ruch, detektory podczerwieni wykrywające ciepło, detektory wykrywające zmiany pola magnetycznego oraz detektory radiolokacyjne. Przy

instalowaniu tych urządzeń należy dążyć do „zachodzenia" na siebie sektorów dozorowania poszczególnych czujników.

Z prowadzonych badan wynika, że do dozorowania obszaru w znacznej odległości od bazy zasadne jest wykorzystywanie radiolokatorów pola walki. Z analizy przeprowadzonej w rozdziale 4 wynika, że radar umożliwia wykrycia potencjalnego przeciwnika z odległości większej, niż agresor może skutecznie oddziaływać na bazę wykorzystując do tego środki artyleryjskie. Istnieje jednak możliwość częstych fałszywych alarmów powodowanych przez spacerujące np. zwierzęta. Eliminacja fałszywych alarmów może następować poprzez weryfikację z systemu optronicznego dalekiego zasięgu. Systemy optroniczne mogą być montowane na bezzałogowych aparatach latających (BAL), jednak pod warunkiem ciągłego lotu BAL. Ciągłe utrzymywanie aparatów w powietrzu jest trudnione zarówno organizacyjnie jak i techniczne. Spełnienie tych wymogów wymaga posiadania co najmniej czterech aparatów, które rotacyjnie mogły by realizować zadania dozorowania obszaru wokół bazy.

W związku z przedstawionymi ograniczeniami zasadnym wydaje się zastosowanie sprzętu optronicznego zamontowanego na maszcie znajdującym się w bazie. Sygnał z rozpoznania radiolokacyjnego uruchamia system dozoru optycznego wraz ze wskazaniem kierunku i odległości. Zadaniem operatora będzie wówczas, przy użyciu systemów optronicznych, zweryfikowanie obiektu będącego przyczyną sygnału alarmowego. W przypadku potwierdzenia alarmu, sygnał podawany będzie do grupy interwencyjnej (będącej w dyspozycji do zwalczania zagrożenia bazy) celem podjęcia akcji w rejonie z którego istnieje zagrożenie dla sił będących w bazie.

Baza w operacji wielonarodowej jest obiektem zazwyczaj częściowo otwartym, tzn. wejście na jej teren wiąże się z uzyskaniem pozwolenia (przepustki) Weryfikacja przepustki może następować elektronicznie poprzez czytnik kart magnetycznych lub wzrokowo przez wartownika. Sprawdzana jest jednak przepustka, a nie okaziciel. Prowadzone badania wykazały, że niektóre siły zbrojne uczestniczące w operacjach pokojowych zaczęły stosować systemy weryfikacji cech osobowych. Stosowano są czytniki odcisków palców, barwy głosu, koloru tęczówki oka itp.. Dotyczyć to może obiektów o dużym znaczeniu militarnym takich jak stanowiska dowodzenia lub obiektów cywilnych ważnych dla miejscowej ludności, których uszkodzenie spowoduje pretekst do wystąpienia przeciwko siłom wielonarodowym.

Wykorzystywane urządzenia techniczne powinny charakteryzować się możliwością pracy w różnych warunkach klimatycznych, geologicznych i topologicznych. Powinny

zapewniać wykrywanie zagrożenia na granicy strzeżonego obiektu, jak również na odległość zapewniającej czas reakcji na zagrożenie (np. ostrzał moździerzowy, rakietowy itp.).

Prowadząc syntezę wcześniejszych rozważań można stwierdzić, że przy organizacji systemu bezpieczeństwa sił wielonarodowych należy brać pod uwagę przedsięwzięcia organizacyjne, techniczne i proceduralne.

W zakres przedsięwzięć organizacyjnych należy zaliczyć tworzenie stref bezpieczeństwa: administracyjnej, klasy II i Klasy I. Strefa bezpieczeństwa służy do kontroli osób i pojazdów oraz zwiększenia skuteczności ochrony fizycznej i elektromagnetycznej. Jej granicę stanowić powinno ogrodzenie bazy. Wstęp do niej powinien być umożliwiony wyłącznie za zgodą osób odpowiedzialnych za ochronę bazy, zgodnie z wytycznymi dowódcy bazy. Przebywanie w strefie administracyjnej nie powinno się wiązać z dostępem do informacji niejawnych oraz do obiektów podlegających szczególnej ochronie (charakterystyka zawarta w rozdziale 3).

Z ustaleń zespołu badawczego wynika, że strefa bezpieczeństwa klasy II powinna obejmować obszar, na którym są wytwarzane, przechowywane i przetwarzane informacje niejawne oraz teren obiektów podlegających szczególnej ochronie. Wejście do niej nie powinno być równoważne z dostępem do informacji niejawnych oraz samodzielnego wykonywania czynności służbowych w obiektach wcześniej wspomnianych. Osoby, które nie wykonują czynności służbowych bezpośrednio w tej strefie, nie powinny w niej przebywać lub mogą pod nadzorem albo po wyrażeniu zgody dowódcy bazy.

Strefa bezpieczeństwa klasy I obejmuje obszar, na którym przebywanie wiąże się z bezpośrednim dostępem do informacji niejawnych lub dostępem do urządzeń znajdujących się w obiektach podlegających szczególnej ochronie. Do przebywania w tej strefie upoważnione są osoby dające rękojmię zachowania tajemnicy (posiadające poświadczenie bezpieczeństwa). Kontrola wejścia do tej strefy powinna obejmować identyfikację biometryczną oraz uniemożliwić wnoszenie wszelkiego rodzaju urządzeń elektronicznych i innych rejestratorów do zapisu informacji w każdej postaci. Niestety w warunkach polowych takie obostrzenia nie zawsze mogą być spełnione. Zespół badawczy zaproponował, że do strefy klasy I należy zastosować najprostsze możliwe rozwiązanie jak kary magnetyczne. Urządzenia są proste i tanie a w warunkach polowych skuteczne.

Przedsięwzięcia techniczne w zakresie bezpieczeństwa obejmują wykorzystanie dostępnych urządzeń zastępujących wartowników oraz poszerzających zdolności recepcyjne służb zajmujących się ochroną. Rodzaje takich urządzeń przedstawiono w rozdziale 4. Przy przedsięwzięciach technicznych należy pamiętać o dualizmie środków ochrony (co najmniej

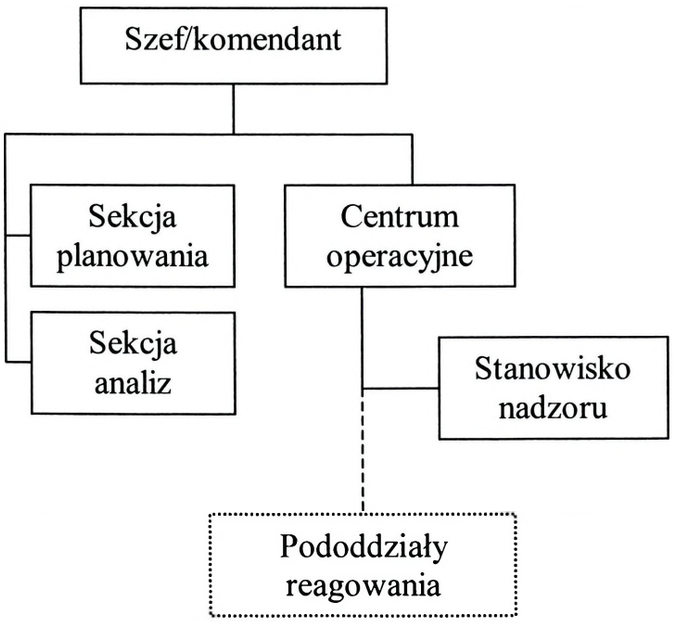
dwa systemy dublujące dozorowanie zarówno w zakresie obszaru jak i rodzaju prowadzonego monitorowania).

Podsumowując, przedsięwzięcia proceduralne obejmują przedstawienie w formie pisemnej sposobu działania na wypadek sygnału alarmowego, postępowanie w sytuacjach zagrożenia oraz metody kontroli osób i weryfikacji alarmów. Wariant struktury systemu ochrony baz w operacjach wielonarodowych przedstawiono w załączniku 13.

Zespół autorski ustalił, że do zarządzania bezpieczeństwem sił wielonarodowych zasadne jest tworzenie komórki bezpieczeństwa, której zadaniem winno być monitorowanie sytuacji w obszarze zagrożeń, przeciwdziałanie nim oraz planowanie systemu ochrony fizycznej i elektronicznej przeciwdziałający tej sytuacji. W działaniach wielonarodowych komórka bezpieczeństwa powinna zapewnić realizację następujących funkcji:

- zarządzanie podległymi podsystemami ochrony i obrony;
- ocena informacji o zagrożeniach dla wojsk w czasie patrolu i w bazie;
- ocena informacji uzyskanych z podsystemów ochrony i obrony oraz jej wykorzystanie na potrzeby środków rażenia ogniowego i elektronicznego;
- koordynacja użycia sił systemu ochrony fizycznej i elektronicznej;
- kierowanie bezpośrednio działaniami w trakcie ataku na bazę lub konwój;
- kontrola dotycząca sprawdzania gotowości baz do odparcia ataku.

Do takich funkcji zaproponowano modelową strukturę organizacyjną komórki bezpieczeństwa przedstawioną na rysunku 5.1.



Źródło: opracowanie własne

Rys. 5.1. Modelowa struktura komórki bezpieczeństwa

Wyżej przedstawiony wariant organizacji systemu ochrony sił wielonarodowych jest jednym z wielu rozwiązań problemu. Należy pamiętać, że każda operacja sił wielonarodowych odbywa się w innych uwarunkowaniach polityczno-prawnych oraz prowadzona jest w zmiennym otoczeniu kulturowo-religijnym. Przy planowaniu ochrony zawsze należy uwzględniać powyższe czynniki.

W celu weryfikacji wyników analiz, prowadzonych przez zespół autorski, przeprowadzono w środowisku oficerów ankietę. Grupa ankietowanych składała się z przedstawicieli: wojsk lądowych, różnych rodzajów wojsk, ze stażem służby powyżej 10 lat. Środowisko ankietowanych było zbiorowością zarówno uczestników misji wielonarodowych jak i żołnierzy wykonujących obowiązki służbowe tylko w kraju. Szczegółowa analiza wyników ankiety przedstawiona jest w załączniku 2.

W toku badań uzyskano, zdaniem zespołu badawczego, odpowiedzi na sformułowane, w postaci pytań, problemy badawcze, które w stopniu wyczerpującym wyjaśniły sprecyzowane problemy badawcze, potwierdziły trafność przyjętej hipotezy roboczej i umożliwiły uzyskanie zamierzonych celów badawczych.

Treści przedstawione w pracy badawczej nie stanowią jednak pełnego i wyczerpującego rozwiązania problemu określenia uwarunkowań bezpieczeństwa fizycznego i elektronicznego wojsk w operacji wielonarodowej. Przedstawione poglądy i rozwiązania stanowią jednak solidną bazę do budowania pełniejszych koncepcji działań w tym zakresie.

ZAKOŃCZENIE

Przeprowadzone w ramach pracy badania ugruntowały przekonanie zespołu autorskiego o potrzebie i aktualności ich podjęcia. Życie żołnierzy jest największym skarbem armii i kraju. Takie motto przyświecało autorom przez cały czas prowadzonych badań. Jest ono aktualne również dla wszystkich decydentów w organizacjach wielonarodowych wysyłających wojska w rejon konfliktowy. Wymagania jakie musza spełnić siły pokojowe w doprowadzeniu do sytuacji stabilności i porządku w rejonach zapalnych wymaga od organizatorów tych operacji wysokiej odpowiedzialności i wiedzy jak, gdzie, czym i przeciwko komu doprowadzić operację pokojową siłami wielonarodowymi. To ostatnie pytanie może wydawać się oczywiste, bowiem siły pokojowe udają się w rejon konfliktu już określonych stron. Na miejscu jednak okazuje się że walące strony osiągnęły względny spokój a do głosu dochodzą odłamy nie zadowolonych bojowników, partyzantów, terrorystów lub jeszcze innych grup określanych jako eksternistyczne destabilizujące zawarty pokój. Zastała sytuacja jest, więc bardzo niespokojna, a zagrożenia zgoła inne od typowych działań bojowych. Owe zagrożenia są głównym przyczyną niepokojów decydentów kierujących żołnierzy w do zadań operacjach charakterze poniżej progu wojny. Zadania takie często nieprzewidywalne w skutkach oraz powstają dopiero na miejscu w danym rejonie. Asymetryczność takich działań powoduje, że zagrożenie bezpieczeństwa żołnierzy pełniących służbę pokojowa są bardzo wysokie. operacji.

W tej sytuacji niezbędna była intensyfikacja prac badawczych nad określeniem uwarunkowań zagrożenia bezpieczeństwa fizycznego i elektronicznego wojsk w operacjach wielonarodowych. Potrzebne są też zmiany w teorii organizowania bezpieczeństwa w czasie pokoju, kryzys i wojny we własnym kraju i poza jego granicami.

W świetle tak przytoczonej tezy zespół badawczy w toku prowadzonych prac badawczych zbadał uwarunkowania założenia bezpieczeństwa fizycznego i elektronicznego wojsk w operacjach wielonarodowych. Zdaniem autorów, określono optymalne rozwiązania teoretyczne w zakresie uwarunkowań bezpieczeństwa zarówno fizycznego jak i elektronicznego. Jednocześnie zaproponowano strukturę organizacyjną

komórki bezpieczeństwa zdolnej do realizacji zadań w operacjach wielonarodowych. Zgodnie z założonymi problemami badawczymi:

1. Dokonano ogólnej analizy uwarunkowań zagrożenia bezpieczeństwa dla wojsk w operacji wielonarodowej;
2. Ustalono warunki bezpieczeństwa jakie musza być spełnione aby wojska mogły wykonywać swoje zadania
3. Ustalono jakie są potrzeby i możliwości ochrony i obrony wojsk w czasie prowadzonej operacji wielonarodowej;
4. Oceniono stan i możliwości wykorzystania sił i środków do ochrony fizycznej i elektronicznej w operacjach wielonarodowych;
5. Wskazano na potrzebę ścisłego koordynowania przedsięwzięć ochrony fizycznej i elektronicznej podczas ataków na bazy wojskowe lub konwoje.
6. Zaproponowany nowoczesny komórkę bezpieczeństwa jako organu koordynującego działania bezpieczeństwa wojsk.

Przynależność do NATO, budowa nowej strategii obronnej RP oraz deklaracje uczestnictwa w różnych misjach pokojowych SZ RP, wymagają nowego spojrzenia na problemy zagrożeń w operacjach i misjach oraz blisko z tym związane problemy bezpieczeństwa wojsk wykonujących zadania. Wystarczy powiedzieć, że brak koordynacji pomiędzy poszczególnymi podsystemami ochrony fizycznej i elektronicznej może w konsekwencji doprowadzić do sytuacji stwarzającej zagrożenie dla sił wielonarodowych zarówno w bazie jak podczas akcji poza nią.

Koncepcje ochrony baz na obecnym etapie nie różnią się w kwestiach zasadniczych od ochrony koszar. Używane są środki adekwatne do zagrożenia i wielkości obiektu. Główna różnica w zapewnieniu bezpieczeństwa baz wojskowych w czasie operacji za granicą a działalnością bojową w kraju wynika z zidentyfikowania zagrożeń i ich wpływowi na organizację systemu. Głównie chodzi o różnice w realizacji niektórych celów oraz odmiennych podziałach ochrony. Narodowe rozwiązania dotyczą jednolitej struktury ochrony w postaci warty, natomiast w operacjach pokojowych z szczególnie użyciem sił wielonarodowych jest to struktura składająca się z wielu różnych pododdziałów ochrony (warty) odmiennych kulturowo, organizacyjnie i elementów oddziaływania czynnego (patrole piesze, zmotoryzowane i lotnicze wsparcie śmigłowcowe) Kwestią odmienną pozostały także obszar oddziaływania i podległość sztabowych organów bezpieczeństwa.

Ogromne znaczenie dla procesu funkcjonowania organów WE ma problem jednoznacznego określenia roli, funkcji i zadań komórki bezpieczeństwa. Występujące różnice powodują niespójności w dziedzinie budowy struktur ochrony i mają bezpośredni wpływ na organizację bezpieczeństwa wojsk. Różnice koncepcyjne wielu krajów nie pozostają bez wpływu na budowę i funkcjonowanie systemu bezpieczeństwa w operacjach wielonarodowych. Za każdym razem należy uwzględniać doświadczenia, nawyki, gotowość bojową wszystkich uczestników sił wielonarodowych, które będą wykorzystywane w budowie systemu ochrony.

Zmieniające się teorie w operacjach a co za tym idzie przyszłe pole walki nie pozostają bez znaczenia na sposoby i wymagania organizacji systemów bezpieczeństwa. Dokonujący się postęp techniczny, odchodzenie od założeń operacji z okresu II wojny światowej, nowe zagrożenia, wymusiły nowe podejście do realizacji zadań ochrony i obrony wojsk. Bezpośrednim następstwem są zaproponowane przez zespół autorski zmodernizowane sposoby prowadzenia ochrony fizycznej i elektronicznej.

W Siłach Zbrojnych RP główny ciężar ochrony spoczywał na warcie jako elemencie wykonującym zadania bojowe w czasie pokoju. Watra ma za zadanie ochraniać obiekt z wyznaczonych posterunków, czyli wybrane obiekty z całości koszar (nie ludzi). Natomiast w czasie operacji pokojowych jest odwrotnie, ochrania się głównie ludzi a w następnej kolejności mniecie. Podobnie jest w rozpoznaniem i oddziaływaniem elektronicznym. Zadana walki elektronicznej dotyczą głównie szkolenia wojsk w koszarach i na poligonach w rozpoznaniu systemów łączności potencjalnego przeciwnika. W operacji wielonarodowej środki elektroniczne rozpoznają i zakłócają relacje radiowe zagrażające życiu żołnierzy, głównie relacji kierowania zdalnego improwizowanych ładunków wybuchowych.

Trzeba jednak pamiętać, iż stworzenie odpowiednich podstaw teoretycznych, kompatybilnych z koncepcjami wszystkich uczestników operacji wielonarodowej jest dużym wyzwaniem i wymaga jeszcze wielu badań. Może jednak być pierwszym krokiem do budowy nowoczesnego systemu bezpieczeństwa wojsk, które wspierając operacje sił pokojowych, mogą odegrać decydującą rolę w wprowadzeniu i utrzymaniu pokoju w rejonie konfliktowym.

Każda operacja wsparcia pokoju charakteryzuje się własną specyfiką prowadzania. Każda jest odmienna i ma swoje właściwości. Autorzy wychodząc naprzeciw potrzebom opracowania wymogów, sposobów i możliwości budowy sytemu bezpieczeństwa

w operacji wielonarodowej, podjęli próbę przedstawienia praktycznych rozwiązań realizacji tych zadań. Uwzględnili zagrożenia wynikajże dla wojsk działających w innym środowisku, nowo wprowadzone środki ochrony indywidualnej i zbiorowej żołnierzy oraz systemy rozpoznania elektronicznego i zaproponowali taktykę ich wykorzystania.

Niniejsza praca mająca na celu określenie uwarunkowań bezpieczeństwa fizycznego i elektronicznego wojsk w operacjach wielonarodowych realizowanych przez komponent wojsk lądowych oraz weryfikację założeń teoretycznych budowy systemu bezpieczeństwa, może być jednocześnie asumptem do budowy nowego bardziej sprawnego systemu na każdym poziomie dowodzenia zdolnego do realizacji zadań w operacjach wielonarodowych.

W toku badań uzyskano, zdaniem zespołu badawczego, odpowiedzi na sformułowane, w postaci pytań, problemy badawcze, które w stopniu wyczerpującym wyjaśniły interesujące zdarzenia, potwierdziły trafność przyjętej hipotezy roboczej i umożliwiły uzyskanie zamierzonych celów badawczych.

Treści przedstawione w pracy badawczej nie stanowią jednak pełnego i wyczerpującego rozwiązania problemu realizacji zadań ochrony i obrony wojsk w operacjach wielonarodowych. Przedstawione poglądy i rozwiązania stanowią jednak solidną bazę do budowania pełniejszych koncepcji działań w tym zakresie.

Czy zostaną one wykorzystane w działalności praktycznej? Odpowiedź na to pytanie możliwa będzie w niedalekiej przyszłości. Zespół autorski uważa jednak, że zaprezentowane rozwiązania powinny być wzięte pod uwagę przez decydentów podczas podejmowania stosownych decyzji w zakresie budowy systemu bezpieczeństwa wojsk w aktualnie odbywającej się operacji pokojowej w Afganistanie i przyszłych, które z pewność wystąpią.

BIBLIOGRAFIA

1. Gągor F, Paszowski K., Międzynarodowe operacje pokojowe w doktrynie obronnej RP, Wydawnictwo Adam Marszałek, Toruń 1999.
2. Górniak D., „Ochrona wojsk. doświadczenia i zmiany Polskiego Kontyngentu Wojskowego w Iraku", Warszawa 2006.
3. Hołyst B., Wiktymologia, Wydawnictwo Prawnicze LexisNexis, Warszawa 1997.
4. Iwanowski S., Scheffs W., Walka elektroniczna w działaniach wielonarodowych, praca nauk.-bad., AON, Warszawa 2008.
5. Kwećka R., Działania czy operacje połączone, [w:] Myśl Wojskowa nr 3, MON, Warszawa, 2003.
6. Konwoje, patrole, VBIED, przeszukiwanie. MEDEVAC, SALUTE, IED Report, DWLąd Wewn. 46/2004, Warszawa 2004.
7. Kręcikij J., Organizacja dowodzenia w operacjach wielonarodowych, praca naukowo-badawcza pk. Koalicja, AON, Warszawa 2007.
8. Kręcikij J., Strzoda M., Trembecki J., Założenia teoretyczne wielonarodowej operacji połączonej, AON, Warszawa 2000.
9. Kręcikij J., Wybrane problemy kierowania zgrupowaniami wielonarodowych sił połączonych, AON, Warszawa 2003.
10. Kręcikij J., Zakres uprawnień i odpowiedzialności dowódców wobec podległych im wojsk, AON, Warszawa 2000.
11. Michniak J., A.Wisz, Bezpieczeństwo i ochrona informacji w wojskowych sieciach telekomunikacyjnych i zautomatyzowanych systemach dowodzenia, Warszawa 2000.
12. Michniak J. (red.), Bezpieczeństwo i ochrona informacji w sieciach łączności i informatyki wojskowej w okresie pokoju, kryzysu i wojny, AON, Warszawa 2004.
13. Obrusiewicz M., Wielonarodowe Połączone Siły Zadaniowe CJTF, AON, Warszawa, 2002.
14. Sienkiewicz P., Podstawy teorii systemów, Warszawa 1993.
15. Sposoby i techniki przeprowadzania zamachów na Siły Koalicyjne w Iraku, Szt. Gen. Wewn. 5/1/2004, Warszawa 2004.
16. Tomaszewski A., Kaczmarek W., Wiatr M., Wojska lądowe w operacjach połączonych, praca naukowo-badawcza p.k. Operacje połączone, AON, Warszawa, 2003.
17. Wiatr M., Między strategią a taktyką, Wydawnictwo Adam Marszałek, Toruń, 2000.
18. Wiatr M., Operacje połączone, Adam Marszałek, Toruń 2006.
19. Zieliński J., (red.), Teoretyczne podstawy operacji połączonych p.k. „Podstawy", AON, Warszawa, 1991.

MATRERIAŁY Z KONFERENCJI:

20. Materiały z konferencji przeprowadzonej w CSNPSP w Kielcach w dniach 27 – 28 lutego 2008 nt. „Ochrona sił – doświadczenia z misji w Iraku i Afganistanie.", Kielce 2008.
21. Operacja „Iracka Wolność" (materiał z konferencji naukowej), AON Warszawa 2005, s. 151.

CZASOPISMA:

22. Dejek M., Taktyczny radar rozpoznania Pola walki AN/PPS-5C MSTAR, PWL 8/2006.
23. Kwećka R., Działania czy operacje połączone, [w:] Myśl Wojskowa nr 3, MON, Warszawa, 2003.
24. Pawlikowski S., Majewski G., Wybrane uwarunkowania sytuacji polityczno – militarnej w Iraku, „Myśl Wojskowa", Ministerstwo Obrony Narodowej, Warszawa rocznik XLVIII.
25. Pawłesa W., Szkolenie wojsk do zadań pokojowych, „Przegląd Wojsk Lądowych" wydanie specjalne – sierpień 2003..
26. Scheffs W., Elektroniczny wartownik baz wojskowych, PWL nr 6/2008.
27. Stachnik B., Zarządzanie częstotliwościami, PWL 8/2008.

28. Tyszkiewicz A., Doświadczenia i wnioski z przygotowana i udziału I zmiany dywizji międzynarodowej w misji stabilizacyjnej w Iraku, „Przegląd Wojsk Lądowych" 2004, dodatek do nr 8.

DOKUMENTY DOKTRYNALNE:

29. ADP-1 Operations, 1994, s. 6-2, Zob. także ADP-2 Command, 1994.
30. Allied Joint Operations Doctrine AJP-01 (A), MAS, September 1998.
31. Allied Joint Doctrine AJP-01(B), Ratification draft 1, NATO 2000.
32. Bi – S.C. Force Protection Directive, 80 –25 Aneks B, Norfolk 2003.
33. Bi-SC Functional Planning Guide for Force Protection (Initial Draft), Norfolk 2004.
34. Doktryna narodowa operacje połączone OP/01, MON, Warszawa, 2002.
35. Doktryna prowadzenia operacji połączonych (DD/3), Szt. Gen. WP, Warszawa 2004.
36. FM 101-5 Staff Organization and Operations, Washington 1984.
37. Instrukcja o ochronie obiektów wojskowych, OIN 3/2008, Warszawa 2008.
38. Instrukcja o ochronie obiektów wojskowych, Szt.Gen. 1569, Warszawa 2004.
39. Metodyka opracowania szczególnych wymagań bezpieczeństwa dla systemów lub sieci teleinformatycznych, SGWP, Warszawa 2000.
40. Regulamin działań wojsk lądowych DD/3.2, MON, SGWP, Szkol.809/2006, Warszawa 2006.
41. Rozpoznanie wojskowe, Szt. Gen. 1531/2001, Warszawa 2001.

SŁOWNIKI I ENCYKLOPEDIE:

42. AAP-6(2003), NATO Glossary of Terms and Definitions, MAS, Brussels, 2003.
43. AAP-6 (2005) Słownik Terminów i definicji NATO (Nato glossary of terms and definitions).
44. Leksykon Wiedzy Wojskowej, MON, Warszawa, 1979.
45. Reber A.S., Słownik psychologii, Wydawnictwo Naukowe SCHOLAR, Warszawa 2000.
46. Słownik Języka Polskiego- PWN, Warszawa 1978
47. Słownik terminów militarnych, Departament Obrony USA, 2005.
48. Uniwersalny słownik języka polskiego, Wydawnictwo Naukowe PWN, Warszawa 2003.

STRONY INTERNETOWE:

49. http://pl.wikipedia.org/wiki/System
50. Materiały reklamowe firmy DRS Technologies.
51. Materiały reklamowe firmy RADWAR S.A.
52. www.cenrex.com/dokumenty/CNRX_EMX_Black_Wolf.pdf.
53. www.01db-metravib.com/fileadmin/pdf/BU4/gb_GDS_Vehicle.pdf.
54. www.isaf.wp.mil.pl/isaf.html.
55. www.pkwirak.wp.mil.pl/pl/27.html
56. www.unic.un.org.pl/misje pokojowe

SŁOWNIK SKRÓTÓW

Skrót	Rozwinięcie skrótu	Znaczenie polskie
CAS	CLOSE AIR SUPPORT	bliski ogień wspierający
FOB	FORWARD OPERATING BASE	wysunięta baza operacyjna
HMMWV	HIGH MOBILITY MULTIPURPOSE WHEELED VEHICLE	Wielozadaniowy kołowy pojazd wysokiej mobilności
ID	IDENTIFICATION DOCUMENT	dokument tożsamości
IED	IMPROVISED EXPLOSIVE DEVICE	Improwizowany ładunek wybuchowy
MNC – I	MULTINATIONAL CORPS - IRAQ	Wielonarodowy Korpus - Irak
MND CS	MULTINATIONAL DIVISION CENTRAL - SOUTH	Wielonarodowa Dywizja Centrum - Południe
MEDEVAC	MEDICAL EVACUATION	Pododdział ewakuacji medycznej
MNF – I	MULTINATIONAL FORCE - IRAQ	Siły Wielonarodowe w Iraku
MRAP	MINE RESISTANT AMBUSH PROTECTED	klasa pojazdów opancerzonych zabezpieczonych przed skutkami wybuchów min i ładunków improwizowanych
QRF	QUICK REACTION FORCES	siły szybkiego reagowania
PGCS	PERSONAL GROUND CONTROL STATION	naziemny zestaw kontroli
SOP	STANDING OPERATING PROCEDURE	obowiązująca procedura działania
TOC	TACTICAL OPERATION CENTER	taktyczne centrum operacyjne
VBIED	VEHICLE BORNE IMPROVISED EXPLOSIVE DEVICE	Improwizowany ładunek wybuchowy zamontowany na samochodzie

ZAŁACZNIKI

1. Kwestionariusz ankiety
2. Opracowane wyniki ankiety
3. System ochrony bazy echo – Ad Diwaniyah /Irak/
4. System ochrony bazy Sharana /Afganistan/
5. Stany alarmowe – PKW Irak
6. Kody ubioru – PKW Irak
7. Kody ruchu pojazdów - PKW Irak
8. Stany zagrożenia alarmowego – PKW Afganistan
9. Kody uzbrojenia
10. Zapory fortyfikacyjne stosowane w PKW
11. Kody ubioru – PKW Afganistan
12. Kody ruchu pojazdów – PKW Afganistan;
13. System ochrony baz w działaniach wielonarodowych – wariant

Załącznik 1

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH
INSTYTUT ZARZĄDZANIA I DOWODZENIA

KWESTIONARIUSZ ANKIETY

Treść kwestionariusza związana jest z wybranymi zagadnieniami dotyczącymi problemu bezpieczeństwa fizycznego i elektronicznego operacji wielonarodowej.

Celem przeprowadzanej ankiety jest uzyskanie empirycznego materiału faktograficznego dotyczącego poglądów respondentów w zakresie przedmiotu badań.

Ankieta jest anonimowa, wyniki badań będą wykorzystane 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 podstawą opracowania wniosków końcowych zawartych w pracy naukowo-badawczej.

Serdecznie dziękuję za współpracę
ppłk dr inż. Waldemar Scheffs

1. Jakie, Pana/Pani zdaniem, zagrożenia występują w operacjach wielonarodowych?
   Proszę wskazać rangę niżej przedstawionych odpowiedzi: (1-wysoki,2- średni, 3- niski, 4-nie mam zdania.)

   - ☐ Porwanie osób
   - ☐ Zamach
   - ☐ Szantaż
   - ☐ Kradzież danych
   - ☐ Walki w rozumieniu klasycznym
   - ☐ Ingerencja w systemy teleinformatyczne strony koalicyjnej /własnej/
   - ☐ Inne .....
   - ☐ .....
   - ☐ .....

2. Które, Pana/Pani zdaniem, przedsięwzięcia walki elektronicznej są realizowane przez stronę przeciwną w operacji wielonarodowej?
   Proszę wskazać rangę niżej przedstawionych odpowiedzi: (1-bardzo często,2- często, 3- rzadko, 4-czasami, 5- nigdy, 6- nie mam zdania.)

   - ☐ Rozpoznanie elektroniczne systemów łączności radiowej
   - ☐ Rozpoznanie elektroniczne systemów informatycznych
   - ☐ Rozpoznanie elektroniczne systemów radiolokacyjnych
   - ☐ Przeciwdziałanie elektroniczne systemów łączności radiowej
   - ☐ Przeciwdziałanie elektroniczne systemów informatycznych
   - ☐ Przeciwdziałanie elektroniczne systemów radiolokacyjnych
   - ☐ Obrona własnych systemów łączności radiowej
   - ☐ Obrona własnych systemów informatycznych
   - ☐ Obrona własnych systemów radiolokacyjnych

3. Które, Pana/Pani zdaniem, przedsięwzięcia walki elektronicznej są realizowane przez stronę koalicyjną w operacji wielonarodowej?
Proszę wskazać rangę niżej przedstawionych odpowiedzi: (1-bardzo często,2- często, 3- rzadko, 4-czasami, 5- nigdy, 6- nie mam zdania.)

- ☐ Rozpoznanie elektroniczne systemów łączności radiowej
- ☐ Rozpoznanie elektroniczne systemów informatycznych
- ☐ Rozpoznanie elektroniczne systemów radiolokacyjnych
- ☐ Przeciwdziałanie elektroniczne systemów łączności radiowej
- ☐ Przeciwdziałanie elektroniczne systemów informatycznych
- ☐ Przeciwdziałanie elektroniczne systemów radiolokacyjnych
- ☐ Obrona własnych systemów łączności radiowej
- ☐ Obrona własnych systemów informatycznych
- ☐ Obrona własnych systemów radiolokacyjnych

4. Które, Pana/Pani zdaniem, zagrożenia systemów informatycznych występują w operacji wielonarodowej?
Proszę wskazać rangę niżej przedstawionych odpowiedzi: (1-bardzo często,2- często, 3- rzadko, 4-czasami, 5- nigdy, 6- nie mam zdania.)

- ☐ Naruszenie integralności danych przetwarzanych przez system teleinformatyczny (modyfikacje, dodanie, zniszczenie)
- ☐ Nieuprawnione skopiowanie danych przez osobę mającą dostęp do systemu.
- ☐ Włamania do systemu teleinformatycznego
- ☐ Nieuprawniony dostęp do zasobów systemu możliwy dzięki ujawnieniu haseł innych użytkowników
- ☐ Niepowołany dostęp do miejsca przetwarzania danych
- ☐ Zniszczenie elementów lub całości infrastruktury technicznej systemu teleinformatycznego
- ☐ Nieodpowiednie parametry pracy systemu teleinformatycznego (np. wilgotność, temperatura)
- ☐ Błędy popełnione przez użytkowników
- ☐ Kradzież lub uszkodzenie sprzętu
- ☐ Instalacja nielegalnego oprogramowania (wirusy)
- ☐ Inne .....

5. Które, Pana/Pani zdaniem, przedsięwzięcia zapewnienia bezpieczeństwa systemom teleinformatycznym, są realizowane w operacji wielonarodowej?
Proszę wskazać rangę niżej przedstawionych odpowiedzi: (1-bardzo często,2- często, 3- rzadko, 4-czasami, 5- nigdy, 6- nie mam zdania.)

- ☐ Identyfikacja i uwierzytelnianie
- ☐ Kontrola dostępu
- ☐ Śledzenie odpowiedzialności
- ☐ Badanie (audyt) stanu bezpieczeństwa
- ☐ Ochrona współdzielonych zasobów
- ☐ Dokładność ochrony
- ☐ Niezawodność ochrony
- ☐ Ochrona komunikacji
- ☐ Inne .....

6. Czy, Pana/Pani zdaniem, zabezpieczenia fizyczne i elektroniczne zasobów informacyjnych w operacji wielonarodowej są wystarczające?
Proszę postawić znak „X" przy wybranej odpowiedzi.

- ☐ Jest na bardzo dobrym poziomie
- ☐ Jest na dobrym poziomie
- ☐ Jest na dostatecznym poziomie
- ☐ Jest na poziomie niedostatecznym
- ☐ Nie mam zdania.

7. Czy, Pana/Pani zdaniem, stosowanie różnego rodzaju sprzętu gromadzącego, przetwarzającego i przesyłającego informacje jest przyczyną obniżenia bezpieczeństwa w operacji wielonarodowej?
   Proszę postawić znak „X" przy wybranej odpowiedzi.

   - ☐ Tak
   - ☐ Raczej tak
   - ☐ Raczej nie
   - ☐ Nie
   - ☐ Nie mam zdania.

8. Czy, Pana/Pani zdaniem, struktury wielonarodowe sprzyjają zapewnieniu bezpieczeństwa fizycznego i elektronicznego operacji wielonarodowej?
   Proszę postawić znak „X" przy wybranej odpowiedzi.

   - ☐ Tak
   - ☐ Raczej tak
   - ☐ Raczej nie
   - ☐ Nie
   - ☐ Nie mam zdania.

9. Czy, Pana/Pani zdaniem, żołnierze mają świadomość zapewnienia bezpieczeństwa fizycznego i elektronicznego w trakcie udziału w operacji wielonarodowej?
   Proszę postawić znak „X" przy wybranej odpowiedzi.

   - ☐ Tak
   - ☐ Raczej tak
   - ☐ Raczej nie
   - ☐ Nie
   - ☐ Nie mam zdania.

10. Czy spotkał się Pan/Pani w swojej działalności służbowej z próbą ingerencji w systemy teleinformatyczne wykorzystywane w SZ?
    Proszę postawić znak „X" przy wybranej odpowiedzi.

    - ☐ Często
    - ☐ Czasami
    - ☐ Rzadko
    - ☐ Nigdy
    - ☐ Nie mam zdania

11. Które, Pana/Pani zdaniem, zabezpieczenia fizyczne warunkują niezakłóconą pracę w obiektach stacjonarnych wykorzystywanych przez wojska w trakcie prowadzenia operacji wielonarodowych?
    Proszę postawić znak „X" przy wybranej odpowiedzi.

    - ☐ Bramy ochronne
    - ☐ Furtki, kołowroty
    - ☐ System przepustkowy
    - ☐ Monitoring
    - ☐ Inne .....
    - ☐ .....

12. Które, Pana/Pani zdaniem, zabezpieczenia fizyczne powinny być realizowane podczas organizowania patroli (interwencyjnych, rutynowych, itp.) w operacjach międzynarodowych?
Proszę postawić znak „X" przy wybranej odpowiedzi.

- ☐ Konwoje
- ☐ Osłona śmigłowcowa
- ☐ Monitoring realizowany przez BAL
- ☐ Działania HUMINT i/lub wywiadu wojskowego
- ☐ Inne .....
- ☐ .....

13. Jakie, Pana/Pani zdaniem, zabezpieczenia fizyczne powinny być stosowane na SD sił wielonarodowych?
Proszę postawić znak „X" przy wybranej odpowiedzi.

- ☐ Posterunki wartownicze
- ☐ Patrole żołnierskie
- ☐ Furtki, kołowroty
- ☐ System przepustkowy
- ☐ Monitoring
- ☐ Inne .....
- ☐ .....

14. Jakie może Pan/Pani wymienić uwarunkowania ochrony fizycznej.

.....
.....
.....
.....
.....
.....
.....

15. Jakie może Pan/Pani wymienić uwarunkowania ochrony elektronicznej.

.....
.....
.....
.....
.....
.....
.....

16. W którym etapie, Pana/Pani zdaniem, operacji wielonarodowej występują zagrożenia?
Proszę uszeregować względem poziomu zagrożenia: 1-nie występują, 2-występują rzadko, 3-występują czasami, 4-zawsze występują.

- ☐ Planowanie operacji wielonarodowej
- ☐ Przygotowanie operacji wielonarodowej
- ☐ Przegrupowanie sił w obszar operacji wielonarodowej
- ☐ Prowadzenie operacji
- ☐ Przegrupowanie sił po zakończeniu operacji

Metryczka

1. *Stopień wojskowy*
   - ☐ Podoficer
   - ☐ Oficer młodszy
   - ☐ Oficer starszy

2. *Wiek*
   - ☐ Do 30 lat
   - ☐ 30-35 lat
   - ☐ 35-40 lat
   - ☐ Powyżej 40 lat

3. *Staż służby*
   - ☐ Do 5 lat
   - ☐ 5-10 lat
   - ☐ 10-15 lat
   - ☐ 15-20 lat
   - ☐ Powyżej 20 lat

4. *Udział w działaniach wielonarodowych*
   - ☐ Nie był
   - ☐ Jeden raz
   - ☐ Dwa razy i więcej

5. *Rodzaj jednostki wojskowej*
   - ☐ Specjalna
   - ☐ Zmechanizowana/pancerna
   - ☐ Wsparcia
   - ☐ Logistyczna

Załącznik 2

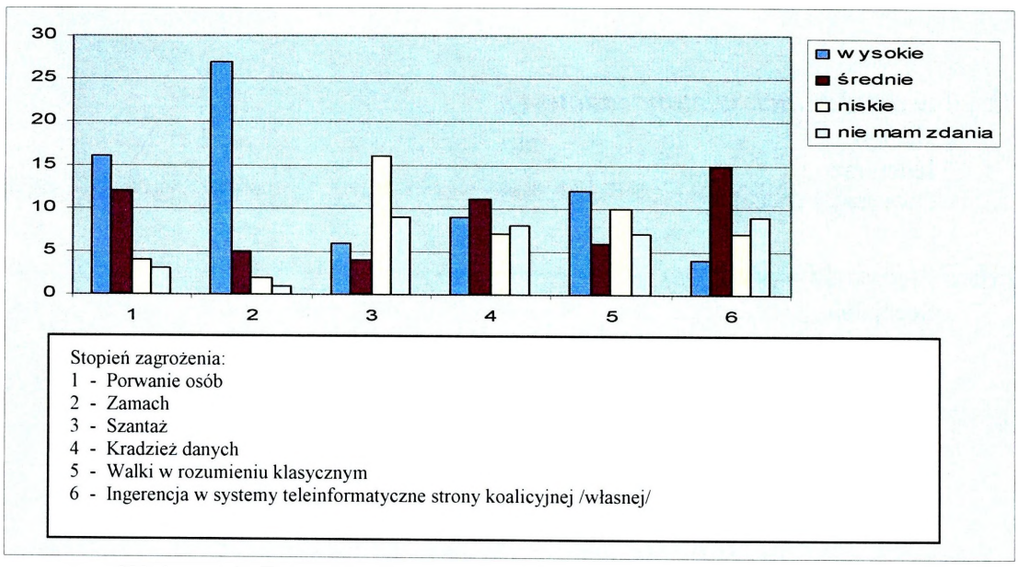
OPRACOWANE WYNIKI ANKIETY

Na podstawie zgromadzonego materiału, zespół autorski opracował uogólnione wyniki ankiety. Rezultaty poznawcze stanowiły podstawę do weryfikacji założeń teoretycznych obejmujących problematykę bezpieczeństwa fizycznego i elektronicznego operacji wielonarodowych.

1. Jakie, Pana/Pani zdaniem, zagrożenia występują w operacjach wielonarodowych?

Proszę wskazać rangę niżej przedstawionych odpowiedzi: (1-wysoki,2- średni, 3- niski, 4-nie mam zdania.)

- ☐ Porwanie osób
- ☐ Zamach
- ☐ Szantaż
- ☐ Kradzież danych
- ☐ Walki w rozumieniu klasycznym
- ☐ Ingerencja w systemy teleinformatyczne strony koalicyjnej /własnej/
- ☐ Inne .....



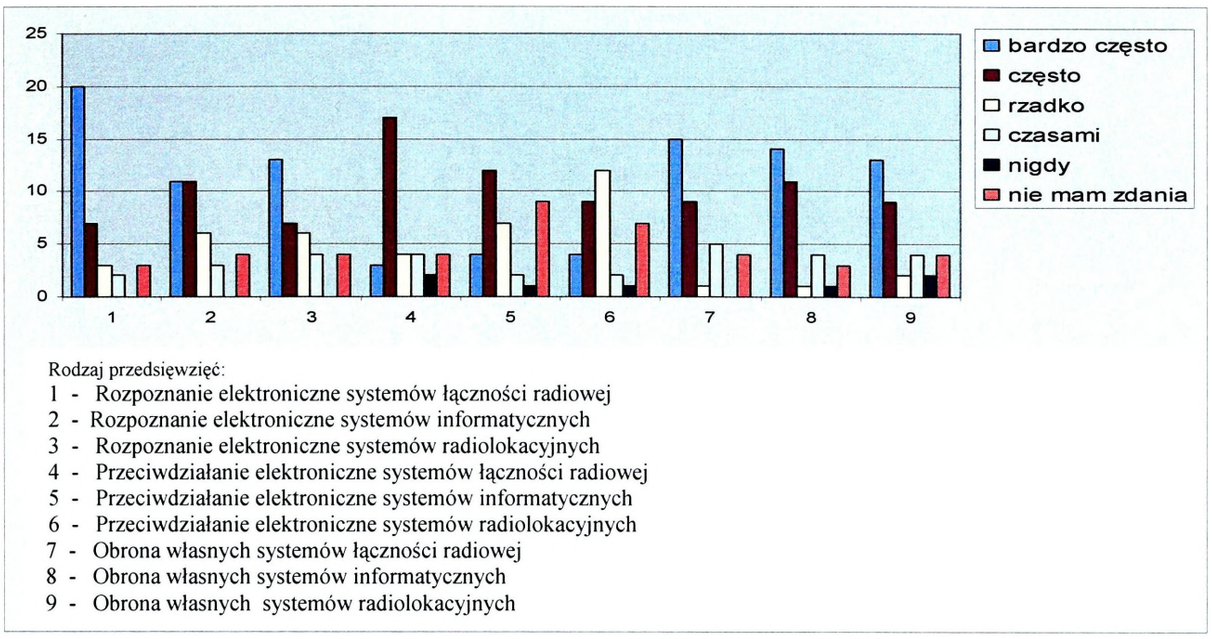
Wykres 1. Zagrożenia występujące w operacji wielonarodowej

Na podstawie otrzymanych wyników można wnioskować, że wśród zagrożeń wskazanych przez zespół autorski, najwyższy stopień zagrożenia dla sił wielonarodowych stanowią zamachy. Respondenci nie wykluczyli jednak innych rodzajów zagrożeń. Wymienili również porwania i walki w rozumieniu klasycznym jako średni stopień zagrożenia. Wyniki badań potwierdziły dociekania zespołu autorskiego oraz mają potwierdzenie w wydarzeniach w działaniach wielonarodowych w Afganistanie.

2. Które, Pana/Pani zdaniem, przedsięwzięcia walki elektronicznej są realizowane przez stronę przeciwną w operacji wielonarodowej?

Proszę wskazać rangę niżej przedstawionych odpowiedzi: (1-bardzo często,2- często, 3- rzadko, 4-czasami, 5- nigdy, 6- nie mam zdania.)

- ☐ Rozpoznanie elektroniczne systemów łączności radiowej
- ☐ Rozpoznanie elektroniczne systemów informatycznych
- ☐ Rozpoznanie elektroniczne systemów radiolokacyjnych
- ☐ Przeciwdziałanie elektroniczne systemów łączności radiowej
- ☐ Przeciwdziałanie elektroniczne systemów informatycznych
- ☐ Przeciwdziałanie elektroniczne systemów radiolokacyjnych
- ☐ Obrona własnych systemów łączności radiowej
- ☐ Obrona własnych systemów informatycznych
- ☐ Obrona własnych systemów radiolokacyjnych



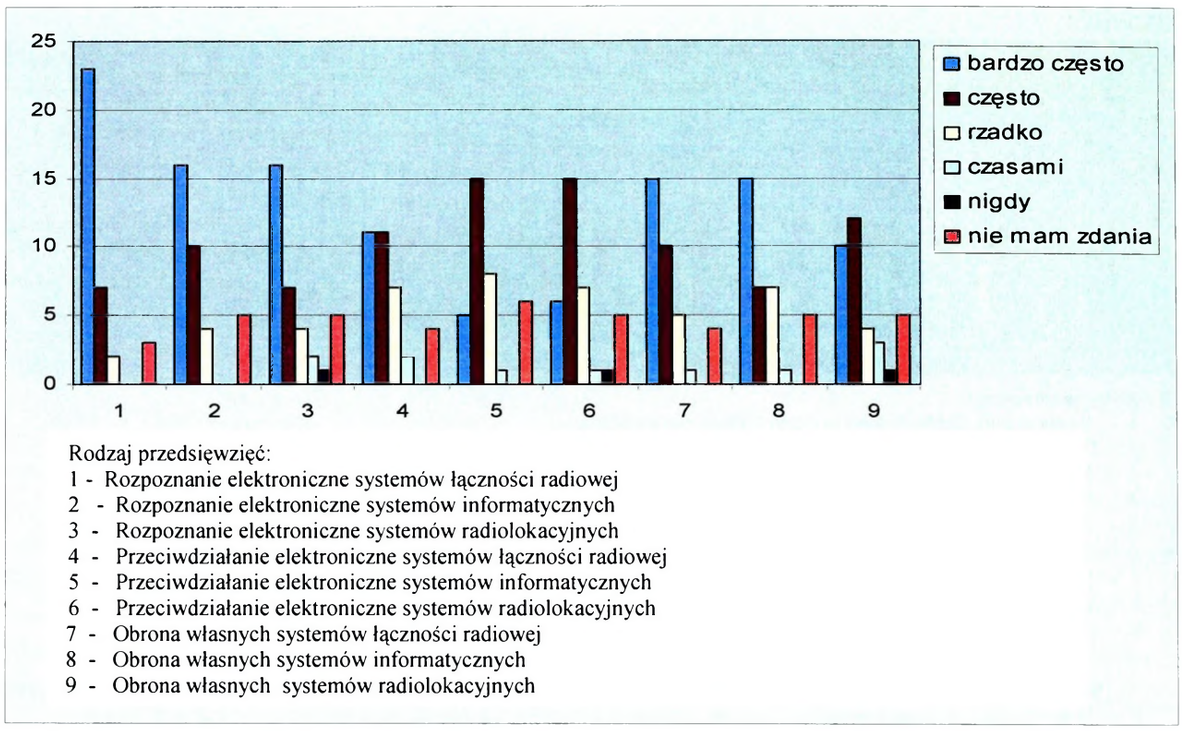
Wykres 2. Przedsięwzięcia walki elektronicznej realizowane przez stronę przeciwną w operacji wielonarodowej

W zakresie przedsięwzięć walki elektronicznej (WE) realizowanych przez stronę przeciwną w operacjach wielonarodowych ankietowani wskazali jako najczęściej realizowane rozpoznanie elektroniczne systemów łączności oraz obronę własnych systemów. Pozostałe przedsięwzięcia WE nie zostały wykluczone, jednak wskazano na mniejszą ich intensywność. Wynika z powyższego, że siły wielonarodowe muszą brać pod uwagę zagrożenie elektroniczne realizowane przez stronę przeciwną. Wskazanie na przeciwdziałanie elektroniczne, jako często realizowane oznacza, że przeciwnik wykorzystuje w szerokim zakresie urządzenia do tego przeznaczone. Należy jednak zaznaczyć, że dotychczasowe doświadczenia z działań wielonarodowych nie potwierdzają opinii badanych. Brak jest przesłanek do stwierdzenia, że przeciwdziałanie elektroniczne jest, bądź będzie szeroko realizowane przez przeciwnika. Nie należy jednak całkowicie tego wykluczyć.

3. Które, Pana/Pani zdaniem, przedsięwzięcia walki elektronicznej są realizowane przez stronę koalicyjną w operacji wielonarodowej?

Proszę wskazać rangę niżej przedstawionych odpowiedzi: (1-bardzo często,2- często, 3- rzadko, 4-czasami, 5- nigdy, 6- nie mam zdania.)

- ☐ Rozpoznanie elektroniczne systemów łączności radiowej
- ☐ Rozpoznanie elektroniczne systemów informatycznych
- ☐ Rozpoznanie elektroniczne systemów radiolokacyjnych
- ☐ Przeciwdziałanie elektroniczne systemów łączności radiowej
- ☐ Przeciwdziałanie elektroniczne systemów informatycznych
- ☐ Przeciwdziałanie elektroniczne systemów radiolokacyjnych
- ☐ Obrona własnych systemów łączności radiowej
- ☐ Obrona własnych systemów informatycznych
- ☐ Obrona własnych systemów radiolokacyjnych



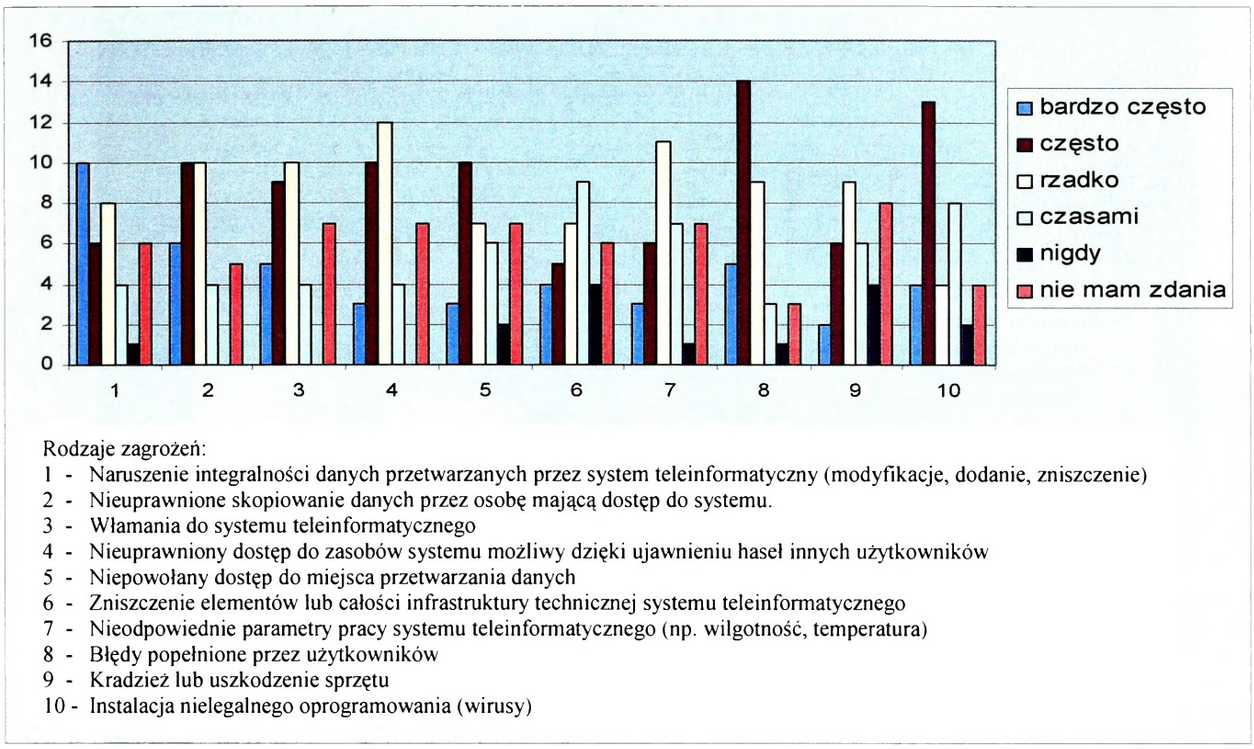
Wykres 3. Przedsięwzięcia walki elektronicznej realizowane przez stronę koalicyjną w operacji wielonarodowej

Na postawie zebranych danych można stwierdzić, że do zasadniczych przedsięwzięć walki elektronicznej w operacjach wielonarodowych zalicza się rozpoznanie elektroniczne oraz obrona własnych systemów elektronicznych. Realizacja wyżej wymienionych przedsięwzięć ma na celu lokalizację sił przeciwnika na podstawie: wymiany radiowej, prowadzonego rozpoznania radiolokacyjnego pola walki oraz zapewnienie niezakłóconych warunków pracy dla własnych systemów. Ankietowani wskazali również, że często realizowane jest przeciwdziałanie elektroniczne wykorzystywane do uniemożliwienia inicjowania ładunków wybuchowych drogą radiową.

4. Które, Pana/Pani zdaniem, zagrożenia systemów informatycznych występują w operacji wielonarodowej?

Proszę wskazać rangę niżej przedstawionych odpowiedzi: (1-bardzo często,2- często, 3- rzadko, 4-czasami, 5- nigdy, 6- nie mam zdania.)

- ☐ Naruszenie integralności danych przetwarzanych przez system teleinformatyczny (modyfikacje, dodanie, zniszczenie)
- ☐ Nieuprawnione skopiowanie danych przez osobę mającą dostęp do systemu.
- ☐ Włamania do systemu teleinformatycznego
- ☐ Nieuprawniony dostęp do zasobów systemu możliwy dzięki ujawnieniu haseł innych użytkowników
- ☐ Niepowołany dostęp do miejsca przetwarzania danych
- ☐ Zniszczenie elementów lub całości infrastruktury technicznej systemu teleinformatycznego
- ☐ Nieodpowiednie parametry pracy systemu teleinformatycznego (np. wilgotność, temperatura)
- ☐ Błędy popełnione przez użytkowników
- ☐ Kradzież lub uszkodzenie sprzętu
- ☐ Instalacja nielegalnego oprogramowania (wirusy)
- ☐ Inne .....



Rodzaje zagrożeń:
1 - Naruszenie integralności danych przetwarzanych przez system teleinformatyczny (modyfikacje, dodanie, zniszczenie)
2 - Nieuprawnione skopiowanie danych przez osobę mającą dostęp do systemu.
3 - Włamania do systemu teleinformatycznego
4 - Nieuprawniony dostęp do zasobów systemu możliwy dzięki ujawnieniu haseł innych użytkowników
5 - Niepowołany dostęp do miejsca przetwarzania danych
6 - Zniszczenie elementów lub całości infrastruktury technicznej systemu teleinformatycznego
7 - Nieodpowiednie parametry pracy systemu teleinformatycznego (np. wilgotność, temperatura)
8 - Błędy popełnione przez użytkowników
9 - Kradzież lub uszkodzenie sprzętu
10 - Instalacja nielegalnego oprogramowania (wirusy)

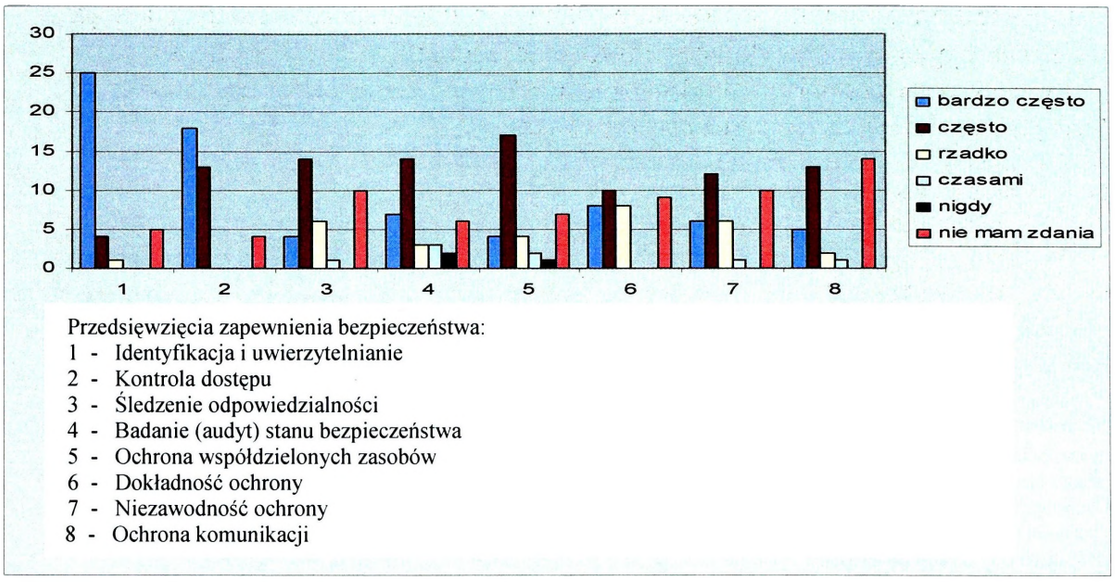
Wykres 4. Zagrożenia systemów informatycznych występujące w operacji wielonarodowej

Z uzyskanych wyników wynika, że zagrożenia dla systemów informatycznych sił wielonarodowych związane są z wirusami komputerowymi i błędami popełnionymi przez użytkowników. Należy więc stwierdzić, że jednym z istotnych warunków bezpieczeństwa systemów informatycznych jest właściwy dobór personelu oraz duża jego świadomość o istniejących zagrożeniach. Wielonarodowość sił nie sprzyja tego typu rozwiązaniom, dlatego więc ważnym jest stosowanie zabezpieczeń technicznych i programowych, które zostały przedstawione w rozdziale czwartym.

5. Które, Pana/Pani zdaniem, przedsięwzięcia zapewnienia bezpieczeństwa systemom teleinformatycznym, są realizowane w operacji wielonarodowej?

Proszę wskazać rangę niżej przedstawionych odpowiedzi: (1-bardzo często,2- często, 3- rzadko, 4-czasami, 5- nigdy, 6- nie mam zdania.)

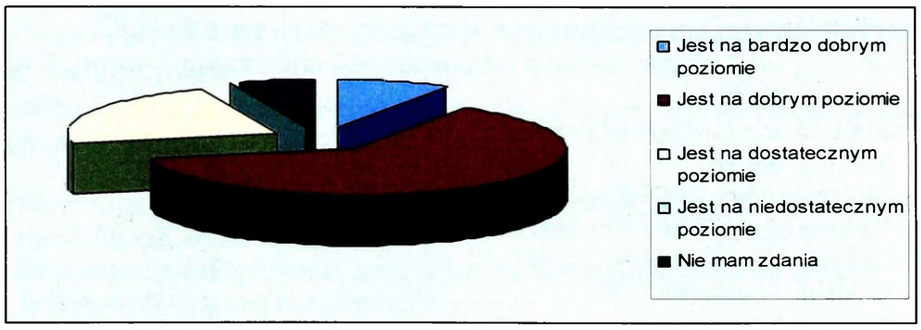
- ☐ Identyfikacja i uwierzytelnianie
- ☐ Kontrola dostępu
- ☐ Śledzenie odpowiedzialności
- ☐ Badanie (audyt) stanu bezpieczeństwa
- ☐ Ochrona współdzielonych zasobów
- ☐ Dokładność ochrony
- ☐ Niezawodność ochrony
- ☐ Ochrona komunikacji
- ☐ Inne .....



Wykres 5. Przedsięwzięcia zapewnienia bezpieczeństwa systemom teleinformatycznym

Uzyskane wyniki, dotyczące przedsięwzięć zapewnienia bezpieczeństwa systemom informatycznym, potwierdzają słuszność wniosków uzyskanych w pytaniu 4. Za najczęściej realizowane w operacjach wielonarodowych badani wskazali identyfikację i uwierzytelnianie oraz kontrolę dostępu. W działaniach wielonarodowych dużą wagę przywiązuje się do kontroli personelu obsługującego sprzęt komputerowy.

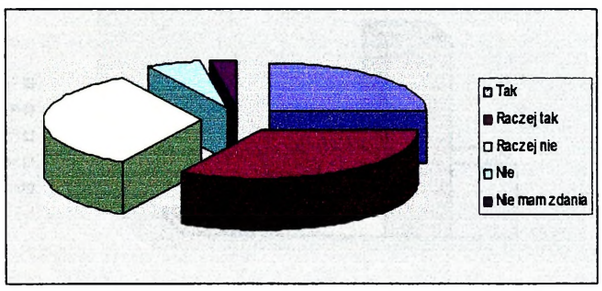
6. Czy, Pana/Pani zdaniem, zabezpieczenia fizyczne i elektroniczne zasobów informacyjnych w operacji wielonarodowej są wystarczające?
   Proszę postawić znak „X" przy wybranej odpowiedzi.
   - ☐ Jest na bardzo dobrym poziomie
   - ☐ Jest na dobrym poziomie
   - ☐ Jest na dostatecznym poziomie
   - ☐ Jest na poziomie niedostatecznym
   - ☐ Nie mam zdania.



Wykres 6. Poziom zabezpieczeń fizycznych i elektronicznych zasobów informacyjnych w operacji wielonarodowej

Ze zgromadzonych faktów wynika, że zabezpieczenia fizyczne i elektroniczne są na bardzo dobrym i dobrym poziomie. Świadczy to o tym, że w ramach działania sił wielonarodowych dużą rangę osiąga realizacja przedsięwzięć mających na celu bezpieczeństwo wojsk. Wykorzystywanie różnorodnego sprzętu z przeznaczeniem zwiększania poczucia bezpieczeństwa wynika ze świadomości istnienia zagrożeń, a co za tym idzie zwiększa bezpieczeństwo sił.

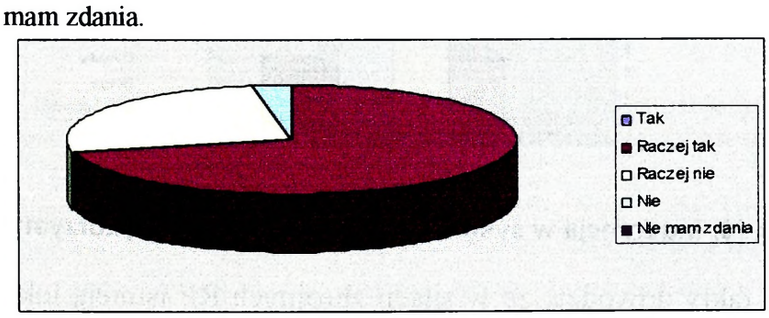
7. Czy, Pana/Pani zdaniem, stosowanie różnego rodzaju sprzętu gromadzącego, przetwarzającego i przesyłającego informacje jest przyczyną obniżenia bezpieczeństwa w operacji wielonarodowej?
Proszę postawić znak „X" przy wybranej odpowiedzi.
   - ☐ Tak
   - ☐ Raczej tak
   - ☐ Raczej nie
   - ☐ Nie
   - ☐ Nie mam zdania.



Wykres 7. Stosowanie różnego rodzaju sprzętu gromadzącego, przetwarzającego i przesyłającego informacje jako przyczyna obniżenia bezpieczeństwa w operacji wielonarodowej

Uzyskane fakty świadczą, że wykorzystywanie sprzętu narodowego przez siły z różnych państw jest przyczyną obniżenia bezpieczeństwa w operacji wielonarodowej. Związane jest to z niekompatybilnością sprzętową. Poszczególne egzemplarze sprzętu nie współpracują ze sobą. Jest to asumpt do tworzenia sprzętu według określonych standardów, zapewniających wymianę informacji pomiędzy różnymi rodzajami sprzętu wykorzystywanego przez siły z państw biorących udział w operacji wielonarodowej.

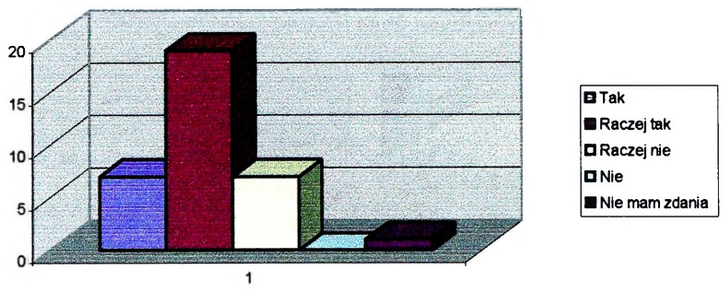
8. Czy, Pana/Pani zdaniem, struktury wielonarodowe sprzyjają zapewnieniu bezpieczeństwa fizycznego i elektronicznego operacji wielonarodowej?
Proszę postawić znak „X" przy wybranej odpowiedzi.
   - ☐ Tak
   - ☐ Raczej tak
   - ☐ Raczej nie
   - ☐ Nie
   - ☐ Nie mam zdania.



Wykres 8. Wpływ struktur wielonarodowych na zapewnienie bezpieczeństwa fizycznego i elektronicznego operacji wielonarodowej

Ze zgromadzonych faktów wynika, że siły wielonarodowe wpływają pozytywnie na zapewnienie bezpieczeństwa fizycznego i elektronicznego, co jest wynikiem legitymizacji działań przez społeczność międzynarodową. Realizacja zadań przez wiele państw powoduje, że strona przeciwna nie identyfikuje wroga w postaci jednego narodu.

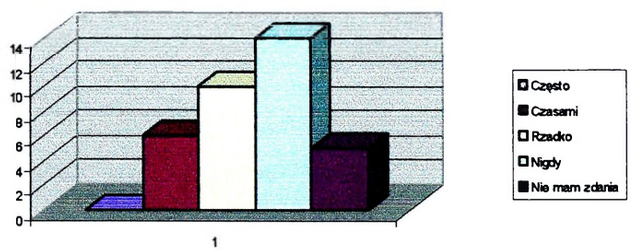
9. Czy, Pana/Pani zdaniem, żołnierze mają świadomość zapewnienia bezpieczeństwa fizycznego i elektronicznego w trakcie udziału w operacji wielonarodowej?
Proszę postawić znak „X" przy wybranej odpowiedzi.
   - ☐ Tak
   - ☐ Raczej tak
   - ☐ Raczej nie
   - ☐ Nie
   - ☐ Nie mam zdania.



Wykres 9. Świadomość zapewnienia bezpieczeństwa fizycznego i elektronicznego w trakcie udziału w operacji wielonarodowej

Dostarczone dane świadczą o dobrym przygotowaniu sił zbrojnych RP do udziału w operacja wielonarodowych w zakresie świadomości zapewnienia bezpieczeństwa zarówno fizycznego jak i elektronicznego.

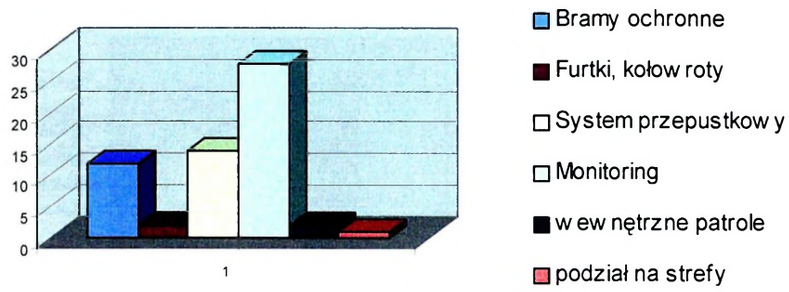
10. Czy spotkał się Pan/Pani w swojej działalności służbowej z próbą ingerencji w systemy teleinformatyczne wykorzystywane w SZ?
Proszę postawić znak „X" przy wybranej odpowiedzi.
   - ☐ Często
   - ☐ Czasami
   - ☐ Rzadko
   - ☐ Nigdy
   - ☐ Nie mam zdania



Wykres 10. Ingerencja w systemy teleinformatyczne wykorzystywane w SZ

Uzyskane fakty dowodzą, że w siłach zbrojnych RP istnieją luki w zabezpieczeniach systemów teleinformatycznych.

11. Które, Pana/Pani zdaniem, zabezpieczenia fizyczne warunkują niezakłóconą pracę w obiektach stacjonarnych wykorzystywanych przez wojska w trakcie prowadzenia operacji wielonarodowych?
Proszę postawić znak „X" przy wybranej odpowiedzi.
   - ☐ Bramy ochronne
   - ☐ Furtki, kołowroty
   - ☐ System przepustkowy
   - ☐ Monitoring
   - ☐ Inne .....
   - ☐ .....



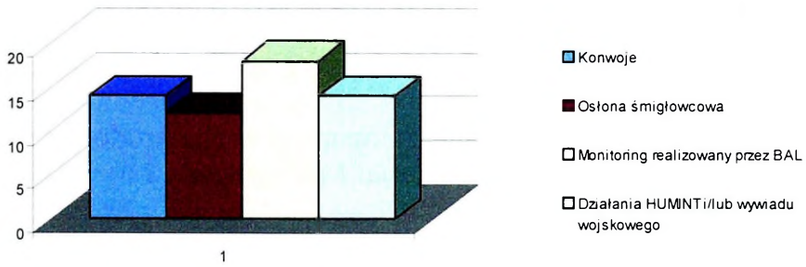
Wykres 11. Zabezpieczenia fizyczne warunkujące niezakłóconą pracę w obiektach stacjonarnych wykorzystywanych przez wojska w trakcie prowadzenia operacji wielonarodowych

Ze zgromadzonych faktów wynika, że warunkiem koniecznym warunkującym niezakłóconą pracę w obiektach stacjonarnych jest zorganizowanie systemu przepustkowego na bramach ochronnych i ciągły monitoring. Ankietowani wskazali najczęściej monitoring, co świadczy o potrzebie szerokiego stosowania sprzętu optronicznego w zapewnieniu bezpieczeństwa.

12. Które, Pana/Pani zdaniem, zabezpieczenia fizyczne powinny być realizowane podczas organizowania patroli (interwencyjnych, rutynowych, itp.) w operacjach międzynarodowych?

Proszę postawić znak „X" przy wybranej odpowiedzi.

- ☐ Konwoje
- ☐ Osłona śmigłowcowa
- ☐ Monitoring realizowany przez BAL
- ☐ Działania HUMINT i/lub wywiadu wojskowego
- ☐ Inne .....
- ☐ .....



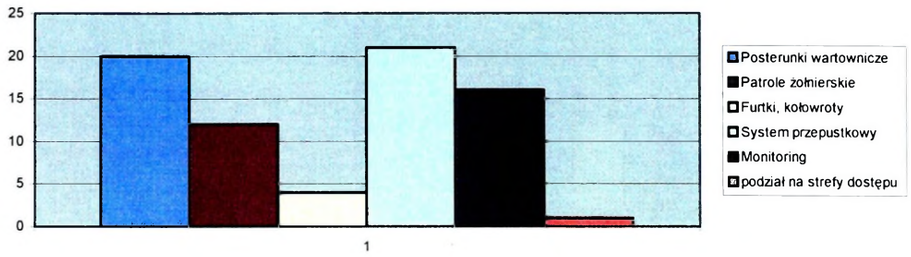
Wykres 12. Zabezpieczenia fizyczne realizowane podczas organizowania patroli (interwencyjnych, rutynowych, itp.) w operacjach międzynarodowych

Brak jednoznacznego wskazania na określony rodzaj zabezpieczenia fizycznego podczas organizowania patroli świadczy, że należy stosować wszystkie rodzaje zabezpieczeń, które wzajemnie się uzupełniają i zapewniają wielopłaszczyznowy napływ informacji o zagrożeniach dla sił będących poza bazą.

13. Jakie, Pana/Pani zdaniem, zabezpieczenia fizyczne powinny być stosowane na SD sił wielonarodowych?

Proszę postawić znak „X" przy wybranej odpowiedzi.

- ☐ Posterunki wartownicze
- ☐ Patrole żołnierskie
- ☐ Furtki, kołowroty
- ☐ System przepustkowy
- ☐ Monitoring
- ☐ Inne .....
- ☐ .....



Wykres 13. Zabezpieczenia fizyczne stosowane na SD sił wielonarodowych

Ze zgromadzonych faktów wynika, że zabezpieczenia wykorzystywane na SD sił wielonarodowych to: zorganizowanie systemu przepustkowego, organizacja posterunków wartowniczych i ciągły monitoring.

14. Jakie może Pan/Pani wymienić uwarunkowania ochrony fizycznej

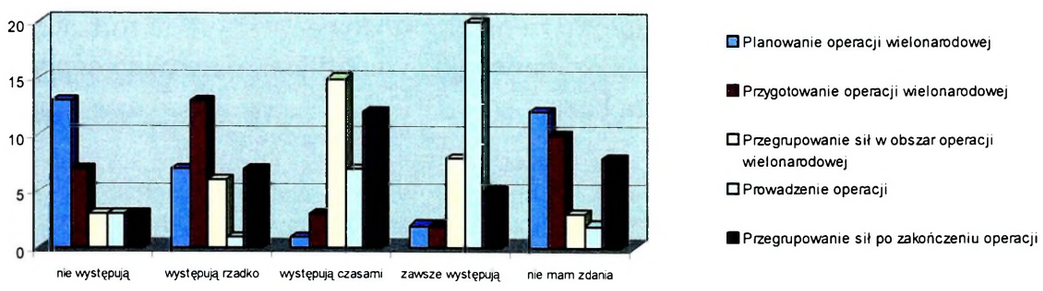
Ankietowani wymieniali różne uwarunkowania ochrony fizycznej. Łączono ochronę fizyczną z zasadami prowadzenia działań wielonarodowych, ze szkoleniem sił, z właściwą organizacją systemu rozpoznania, organizacją stref bezpieczeństwa i systemem dostępu do informacji, rodzaj i wielkość obiektu podlegającego ochronie. Główne wskazania dotyczyły organizacji ochrony fizycznej realizowanej przez pododdziały wartownicze.

15. Jakie może Pan/Pani wymienić uwarunkowania ochrony elektronicznej

Ankietowani wskazali przede wszystkim uwarunkowania sprzętowe i programowe, dobór kadr do obsługi urządzeń, właściwą organizację ochrony elektronicznej poprzez masowe stosowanie urządzeń elektronicznych, zasady prowadzenia działań wielonarodowych jak również ochronę elektromagnetyczną systemów przechowywania, przetwarzania i dystrybucji informacji.

16. W którym etapie, Pana/Pani zdaniem, operacji wielonarodowej występują zagrożenia?
Proszę uszeregować względem poziomu zagrożenia: 1-nie występują, 2-występują rzadko, 3-występują czasami, 4-zawsze występują.

- ☐ Planowanie operacji wielonarodowej
- ☐ Przygotowanie operacji wielonarodowej
- ☐ Przegrupowanie sił w obszar operacji wielonarodowej
- ☐ Prowadzenie operacji
- ☐ Przegrupowanie sił po zakończeniu operacji



Wykres 14. Występowanie zagrożeń w poszczególnych etapach operacji wielonarodowej

Uzyskane dane świadczą, że największe zagrożenia dla sił wielonarodowych występuje w czasie prowadzenia operacji wielonarodowej. Należy się również liczyć z zagrożeniami podczas przegrupowania sił w obszar operacji wielonarodowej jak również w czasie przegrupowania po zakończeniu operacji.

Metryczka

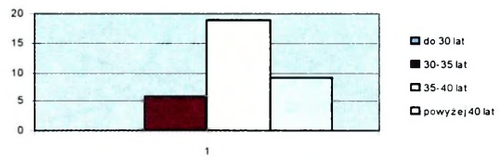
Stopień wojskowy

- ☐ Podoficer
- ☐ **Oficer młodszy**
- ☐ Oficer starszy

Ankieta została przeprowadzona wśród oficerów młodszych.

Wiek

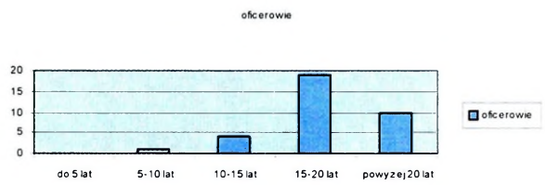
- ☐ Do 30 lat
- ☐ 30-35 lat
- ☐ 35-40 lat
- ☐ Powyżej 40 lat



Wykres 15. Rozkład ankietowanych ze względu na wiek

Staż służby

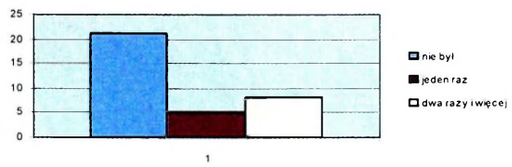
- ☐ Do 5 lat
- ☐ 5-10 lat
- ☐ 10-15 lat
- ☐ 15-20 lat
- ☐ Powyżej 20 lat



Wykres 16. Rozkład ankietowanych ze względu staż służby

Udział w działaniach wielonarodowych

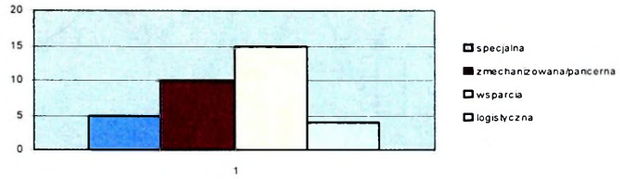
- ☐ Nie był
- ☐ Jeden raz
- ☐ Dwa razy i więcej



Wykres 17. Rozkład ankietowanych ze względu na udział w operacjach wielonarodowych

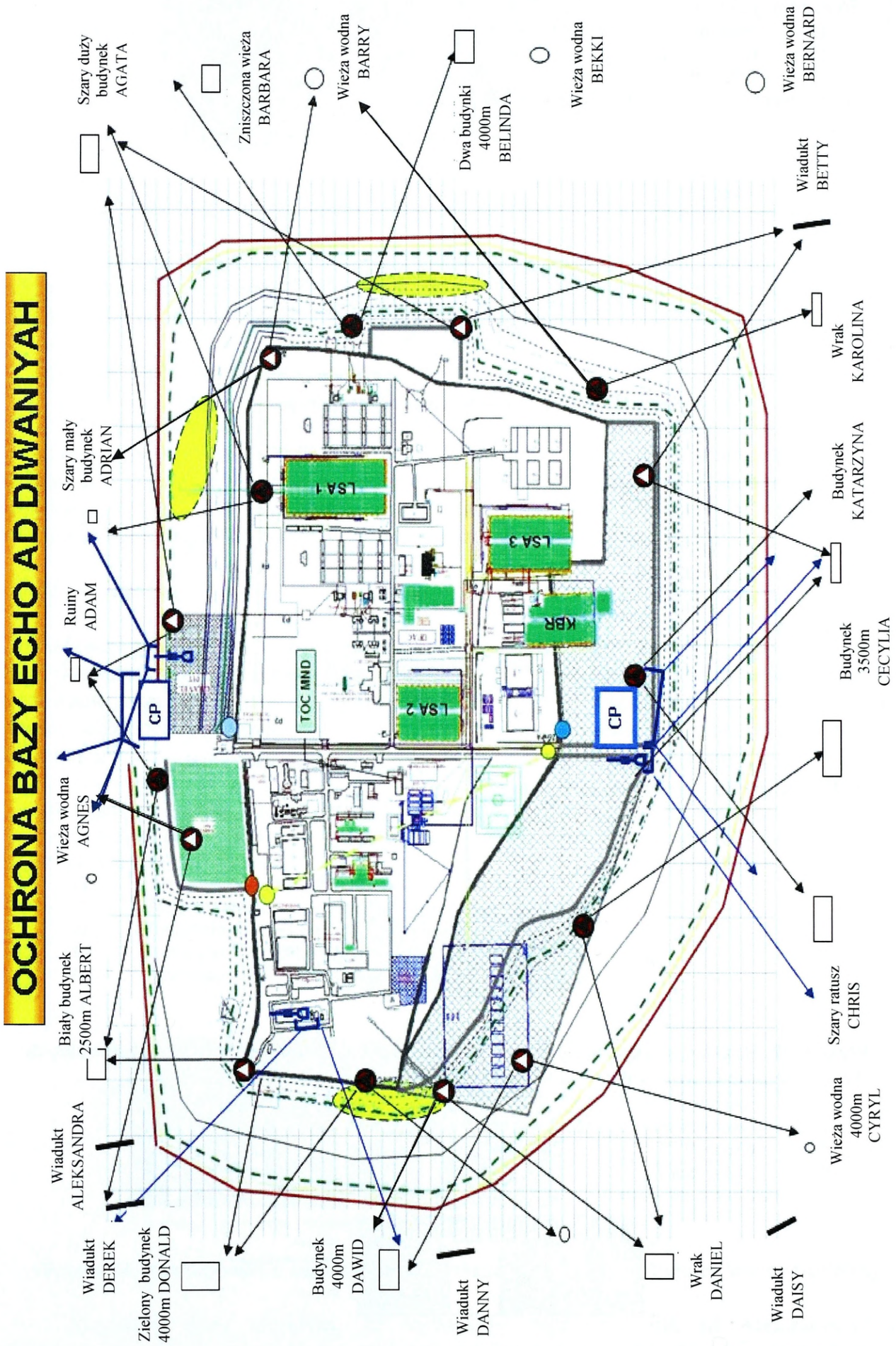
Rodzaj jednostki wojskowej

- ☐ Specjalna
- ☐ Zmechanizowana/pancerna
- ☐ Wsparcia
- ☐ Logistyczna



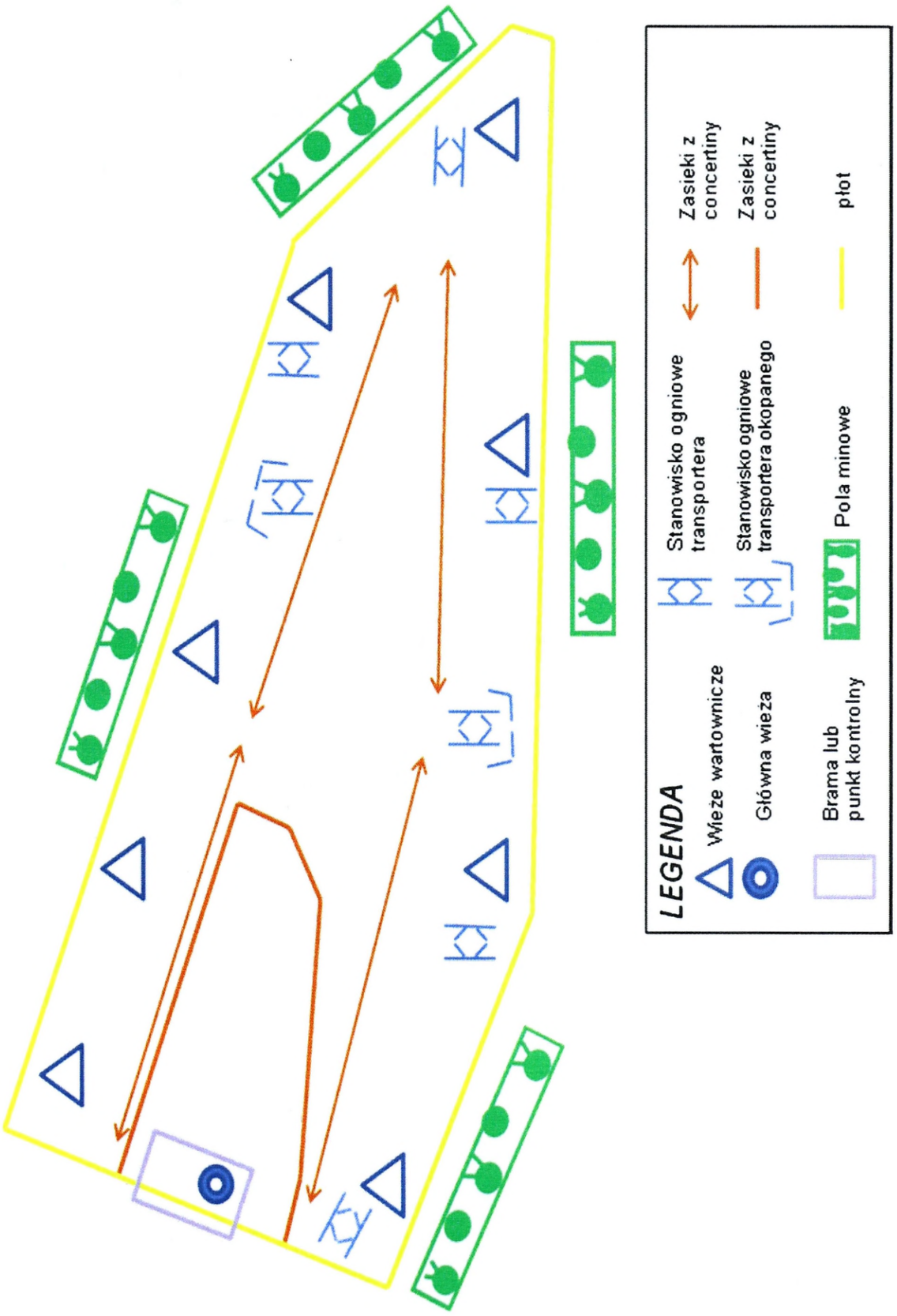
Wykres 18. Rozkład ankietowanych ze względu na rodzaj jednostki macierzystej

SYSTEM OCHRONY BAZY ECHO – AD DIWANIYAH /IRAK/



Załącznik 4

SYSTEM OCHRONY BAZY SHARANA /AFGANISTAN/

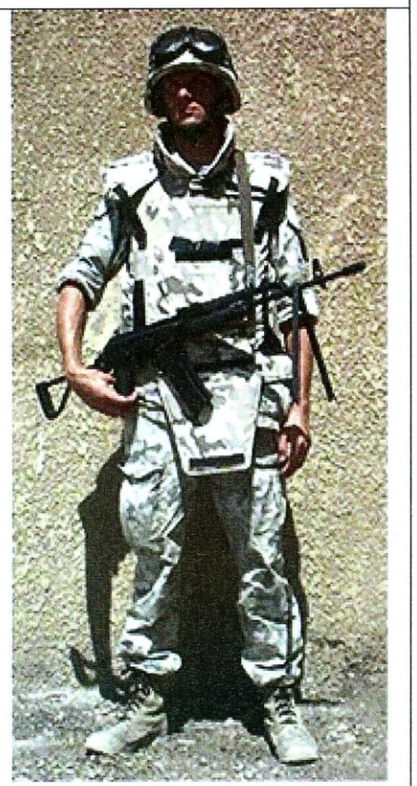


Załącznik 5

STANY ALARMOWE – PKW IRAK

STANY ALARMOWE	ANALIZA ZAGROŻENIA
ALPHA	Brak widocznych sygnałów fizycznego zagrożenia przeciwko Siłom Koalicji lub współpracującym z nimi organizacjom. Organizacje ekstremistyczne/ terrorystyczne pozostają jako zagrożenie stałe.
BRAVO	Widoczne sygnały fizycznego zagrożenia w stosunku do Sił Koalicji - oddziałów lub współpracujących organizacji. Widoczne zamiary przeprowadzenia ataków jednak bez możliwości określenia czasu i miejsca. Wzrost możliwości wystąpienia działań terrorystycznych jednakże bez możliwości określenia czasu i miejsca.
CHARLIE	Wywiad i/ ub wydarzenia wskazują na to, że Siły Koalicji lub współpracujące z nimi organizacje zostaną lub już zostały zaatakowane. Służby wywiadowcze wskazują, że organizacje terrorystyczne zaatakują Siły Koalicji - oddziały lub współpracujące z nimi organizacje.
DELTA	Służby wywiadowcze i/lub wydarzenia dokładnie wskazują na cele, strefy odpowiedzialności, Siły Koalicji lub współpracujące z nimi organizacje, które zostaną lub już zostały zaatakowane.

KODY UBIORU – PKW IRAK

			
E	**F**	**G i H**	**I i J**
Mundur polowy i kapelusz, broń w bezpiecznym miejscu	**Mundur polowy i kapelusz, broń przy żołnierzu bez podpiętego magazynka**	**G - Mundur polowy i kapelusz, kamizelka i hełm dostępne w ciągu 10 minut, broń bez podpiętego magazynka; H – Mundur polowy i kapelusz, kamizelka i hełm dostępne w każdej chwili**	**I - Kamizelka i hełm na sobie, broń z podpiętym magazynkiem; J - Kamizelka i hełm na sobie, broń załadowana**

Załącznik 7

KODY RUCHU POJAZDÓW - PKW IRAK

KOD	INSTRUKCJE
VM – KOD 1	Wysyłanie konwojów – ograniczone do minimum Wysyłanie konwojów po zmroku – zabronione Ochrona konwoju – bezwzględnie wymagana
VM – KOD 2	Wysyłanie konwojów – ograniczone Wysyłanie konwojów po zmroku – zabronione Ochrona konwoju – bezwzględnie wymagana
VM – KOD 3	Wysyłanie konwojów – ograniczone Wysyłanie konwojów po zmroku – zabronione Ochrona konwoju – bezwzględnie wymagana
VM – KOD 4	Wysyłanie konwojów – bez ograniczeń Wysyłanie konwojów po zmroku – dopuszczalne Ochrona konwoju – bezwzględnie wymagana
VM – KOD 5	Wysyłanie konwojów – bez ograniczeń Wysyłanie konwojów po zmroku – dopuszczalne Ochrona konwoju – niewymagalna

Załącznik 8

STANY ZAGROŻENIA ALARMOWEGO – PKW AFGANISTAN

STANY ALARMOWE	OPIS
ALPHA	Ogólne ostrzeżenie przed możliwością przeprowadzenia akcji terrorystycznej, której zasięg jest trudny do określenia i okoliczności nie usprawiedliwiają wprowadzenia wyższego stanu alarmowego.
BRAVO	Wprowadza się w przypadku zwiększonej aktywności i bardziej przewidywalnej groźby akcji terrorystycznej, chociaż żaden szczególny cel nie był zidentyfikowany.
CHARLIE	Wprowadza się, w przypadku zaistnienia albo w momencie otrzymania od rozpoznania informacji o możliwości przeprowadzenia akcji terrorystycznej.
DELTA	Wprowadza się natychmiast po zaistnieniu zamachu terrorystycznego albo w momencie uzyskania od rozpoznania informacji o konkretnej lokalizacji prawdopodobnej akcji terrorystycznej. Normalnie ten stan alarmowy wprowadza się po zlokalizowaniu zagrożenia.

KODY UZBROJENIA

KODY UZBROJENIA **Personel ISAF będzie nosił broń cały czas w rejonie odpowiedzialności (AOR)**	
WU	Broń rozładowana bez magazynka w broni, bez naboju w komorze nabojowej, magazynki łatwo dostępne.
WL	Broń załadowana, magazynek w broni, bez naboju w komorze nabojowej.
WR	Broń gotowa, nabój w komorze nabojowej, zabezpieczona.

Zapory fortyfikacyjne stosowane w PKW

Wygląd					
Typ	ALASKA BARRIER	TEXAS BARRIER	SCUD BUNKER	HESCO BASTION	JERSEY BARRIER
Wysokość	3,70	1,77	1,50	1,30	0,85
Długość	1,40	2,00	3,00	1,10	3,00
Ciężar	0,30	0,40	2,00	1,20	0,30

KODY UBIORU – PKW AFGANISTAN

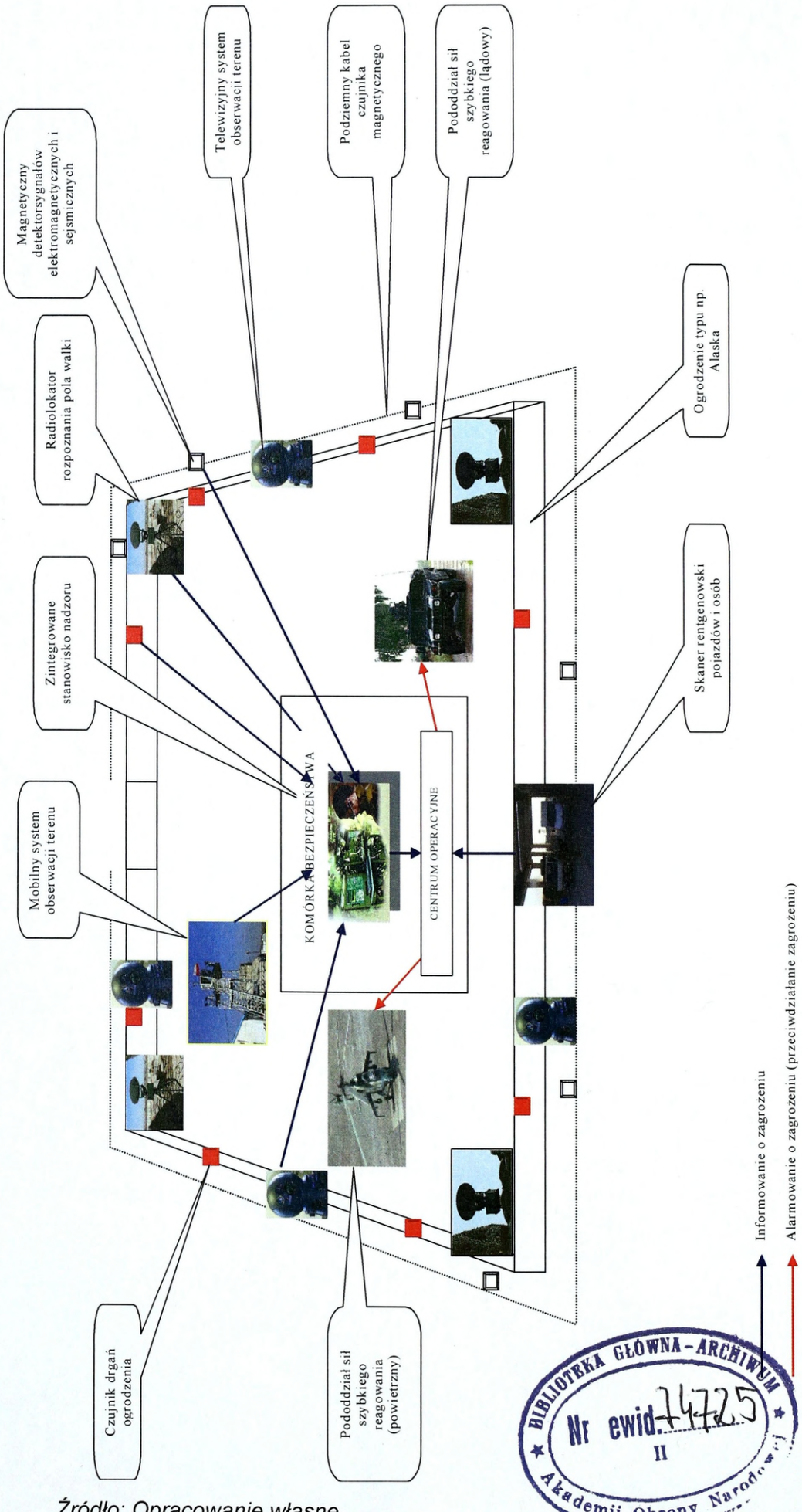
			
0	**1**	**2**	**3**
Mundur polowy i beret	**Kamizelka i hełm w zasięgu ręki**	**Kamizelka na sobie hełm w zasięgu ręki**	**Kamizelka i hełm na sobie**

KODY RUCHU POJAZDÓW – PKW AFGANISTAN

KODY RUCHU POJAZDÓW Dowódca ISAF zachowuje prawo by wprowadzić do użycia tylko pojazdy opancerzone.	
1	Minimum jeden pojazd i dwóch uzbrojonych żołnierzy *
2	Minimum dwa pojazdy i czterech uzbrojonych żołnierzy*
3	Minimum dwa pojazdy, 4 uzbrojonych żołnierzy. Łączność we wszystkich pojazdach. Ruch tylko w wyjątkowych sytuacjach.+

* Przynajmniej jeden pojazd wyposażony w łączność
+ Dodatkowe ograniczenia jak noszenie broni, specjalne upoważnienia do opuszczania zachowuje COS

System ochrony baz w działaniach wielonarodowych – wariant



Źródło: Opracowanie własne.