AKADEMIA
OBRONY
NARODOWEJ

KIERUNKI ROZWOJU SYSTEMÓW ROZPOZNANIA WOJSK LĄDOWYCH

Praca naukowo-badawcza
Kryptonim „ROZPOZNANIE"
kod pracy: II.2.4.2

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 59133
II
Akademii Obrony Narodowej

WARSZAWA 2005

AKADEMIA OBRONY NARODOWEJ
WYDZIAŁ WOJSK LĄDOWYCH
INSTYTUT ZARZĄDZANIA I DOWODZENIA

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 59133
II
Akademii Obrony Narodowej

KIERUNKI ROZWOJU SYSTEMÓW ROZPOZNANIA WOJSK LĄDOWYCH

Praca naukowo - badawcza

Kryptonim „ROZPOZNANIE"

kod pracy: II.2.4.2

WARSZAWA **2005**

Recenzent: płk dr hab. Mariusz WIATR

Opracował zespół autorski w składzie:

1.	Płk dr hab. inż. Janusz KRĘCIKIJ	kierownik zespołu - wstęp; - zakończenie;
2.	Ppłk dr inż. Andrzej NOWAK	- rozdział: 1; 3; . oraz załączniki: 13;
3.	Ppłk dr inż. Marek WRZOSEK	rozdział 2; oraz załączniki: 1-12;

SPIS TREŚCI

Wstęp 5

1. Teoretyczne podstawy działań rozpoznawczych w operacjach. 18

1.1. Ewolucja myśli wojskowej 20

1.2. Modyfikacja techniczna środków walki 32

1.3. Koncepcja operacji XXI wieku 37

1.4. Działania rozpoznawcze w operacjach 46

2. Struktura systemu rozpoznania wojsk lądowych 54

2.1. Struktura rozpoznania ogólnowojskowego 55

2.1.1. Efekty poznawcze 66

2.2. Struktura systemu rozpoznania specjalistycznego 68

2.2.1. System rozpoznania artyleryjskiego 69

2.2.2. System rozpoznania inżynieryjnego 77

2.2.3. System rozpoznania skażeń 81

2.2.4. System rozpoznania powietrznego 86

2.2.5. System rozpoznania elektronicznego 94

2.3. Wyniki analizy struktury systemu rozpoznania 99

3. Prognoza rozwoju systemu rozpoznania XXI wieku 113

3.1. Koncepcja nowego systemu rozpoznania 114

3.1.1 Wsparcie systemu rozpoznania dla operacji informacyjnych. 118

3.1.2. Rozpoznanie w nowych technologiach informacyjnych 127

3.2. Działalność rozpoznawcza w nowym wieku 147

3.2.1. Robotyzacja w środkach rozpoznawczych 157

3.2.2. Środki przekazywania informacji 159

3.2.3. Tendencje zmian w rozpoznaniu patrolowym 161

3.2.4 Perspektywiczne środki rozpoznania elektronicznego 165

3.3. Projekt sił rozpoznawczych 171

3.3.1 Kierunki rozwoju systemu rozpoznania 181

Zakończenie 187

Bibliografia 193

Załączniki 196

WSTĘP

Pierwsze lata XXI stulecia jednoznacznie dowiodły, iż niedawny rozpad dwubiegunowego świata polityczno – militarnego nie przyniósł ze sobą całkowitej likwidacji zagrożeń dla pokoju zarówno w skali regionalnej jak i globalnej. Chociaż pełnoskalowy konflikt zbrojny z użyciem broni jądrowej, jakiego obawiano się przez lata zimnej wojny, oddalił się na czas nieokreślony, jego miejsce zajęły nowe zagrożenia, stanowiące poważną przeszkodę na drodze do zorganizowania skutecznego światowego systemu bezpieczeństwa. Konflikty asymetryczne, proliferacja broni masowego rażenia, stosowanie terroryzmu dla osiągania celów politycznych na niespotykaną dotąd skalę postawiły siły zbrojone przed wyzwaniami stanowiącymi niebezpieczną i trudną kombinację poszerzonych dotychczasowych zadań oraz tych wynikających z nowych zagrożeń.

Polska od lat realizuje swoje zobowiązania sojusznicze wynikające zarówno z przynależności do NATO, jak i do innych organizacji oraz koalicji - jak choćby koalicji antyterrorystycznej. Działania wynikające z tego rodzaju zobowiązań, a wyrażające się chociażby naszą obecnością wojskową na Bałkanach, w Afganistanie czy Iraku, oznaczają dla polskich Sił Zbrojnych poważne wyzwania. Nowe rodzaje zadań stawiane Siłom Zbrojnym to także nowe zadania dla szeroko rozumianego rozpoznania, którego znaczenia w dobie działań informacyjnych nie sposób przecenić. Zadania te są tym trudniejsze, że wymagają osiągnięcia zdolności do działania zarówno warunkach konfliktu pełnoskalowego, związanego z obowiązującą cały czas zasadą kolektywnej obrony Sojuszu, jak i w sytuacji różnego rodzaju kryzysów, czy wreszcie uczestnictwa w konfliktach asymetrycznych.

Tymczasem rzeczywistość systemu rozpoznania sił zbrojnych RP wskazuje, iż jest on ciągle nastawiony na wykonywanie zadań w warunkach klasycznych konfliktów pomiędzy porównywalnymi potencjałami zbrojnymi, głównie na terenie Europy Środkowej. Możliwości tego systemu w aspekcie

sygnalizowanych nowych zagrożeń są symboliczne i w minimalnym stopniu spełniają potrzeby wojsk lądowych w tym zakresie.

Zaakcentowane powyżej fakty skutkowały ujawnieniem sytuacji problemowej, zapoczątkowując w ten sposób pierwszy etap badań naukowych.

Bazując na dotychczasowej wiedzy oraz wynikach badań wstępnych, zespół autorski zdefiniował **cel główny pracy** jako ***zidentyfikowanie i sprecyzowanie kierunków rozwoju systemów rozpoznania funkcjonujących na potrzeby wojsk lądowych***.

Taki sposób sformułowania celu głównego determinował określenie szeregu celów cząstkowych, prowadzących do jego osiągnięcia. Cele takie sprecyzowane zostały następująco:

1. Usystematyzować istniejący teoretyczny dorobek aspekcie działań rozpoznawczych w działaniach wojsk lądowych.
2. Określić stan systemu rozpoznania wojsk lądowych Sił Zbrojnych RP.
3. Wskazać potencjalne kierunki rozwoju systemów rozpoznania prowadzące do osiągnięcia zdolności do działania w nowych uwarunkowaniach.

Obszarem badań był **system rozpoznania,** który zdefiniowany został jako „... rozwinięty w przestrzeni (na lądzie, na morzu, w powietrzu i kosmosie) potencjał rozpoznawczy, wewnętrznie powiązany i skoordynowany jednolitymi więzami organizacyjnymi (hierarchicznymi, funkcjonalnymi, informacyjnymi i technicznymi), działający na rzecz zdobywania, gromadzenia, opracowywania (przetwarzania) i przekazywania informacji o terenie i przeciwniku, w odniesieniu do którego są lub będą planowane, organizowane i prowadzone działania bojowe. System rozpoznania wojskowego jest częścią składową ogólnego systemu działań bojowych, a skuteczność jego funkcjonowania determinuje, w sposób zasadniczy, powodzenie tych działań (działań bojowych). Skuteczny system rozpoznania wojskowego pozwala w znacznej mierze

rekompensować przewagę przeciwnika w podstawowych siłach i środkach walki"[1].

Ze struktury systemu rozpoznania wynika, że składa on się z podsystemów: kierowania rozpoznaniem, realizacji zadań rozpoznawczych oraz informacyjnego.

Za **podsystem rozpoznania** przyjęto wyróżnioną ze względu na określone odniesienie ściśle określoną część systemu rozpoznania, charakteryzującą się własnymi powiązaniami organizacyjnymi. Na przykład w systemie rozpoznania dywizji zmechanizowanej WP występują takie podsystemy jak: rozpoznania elektronicznego, rozpoznania ogólnowojskowego (ogólnego), rozpoznania powietrznego, artyleryjskiego, inżynieryjnego, skażeń. Idąc dalej, biorąc pod uwagę najważniejsze sposoby pozyskiwania danych rozpoznawczych, w systemie rozpoznania dywizji można wyróżnić podsystemy: obserwacji (wzrokowej naziemnej i powietrznej, radioelektronicznej i radiolokacyjnej,) pomiarów dźwiękowych, rozpoznania bojowego (walka, napad, wypad, zasadzka) czy patrolowania.

Wspomniane powyżej dane rozpoznawcze zdobywane są przez elementy ugrupowania rozpoznawczego i elementy rozpoznawcze.

Element ugrupowania rozpoznawczego zdefiniowano jako etatowo lub czasowo zorganizowane siły i środki do samodzielnego wykonywania określonych zadań rozpoznawczych. Element ugrupowania rozpoznawczego funkcjonuje w podsystemie rozpoznania (niekiedy w systemie rozpoznania) jako odrębna całość organizacyjno - przestrzenna. Dostosowany jest do długotrwałego i samodzielnego działania w oderwaniu od sił głównych, zmieniania swego położenia i zachowania podstawowych warunków samoobrony oraz bytowych dla stanu osobowego i techniki bojowej. W przestrzeni stanowi sobą obiekt powierzchniowy bądź punktowy. W zależności od składu przyjmuje nazwę: patrol rozpoznawczy (PR), posterunek rozpoznania i namierzania radiowego, rubież obserwacji, grupa specjalna (GS), stacja pomiarów dźwiękowych, itp.

---

[1] M. Łokociejewski (red.), Rozpoznanie wojskowe, cz. I, Podstawy teoretyczne, Warszawa 2003, s. 25-27.

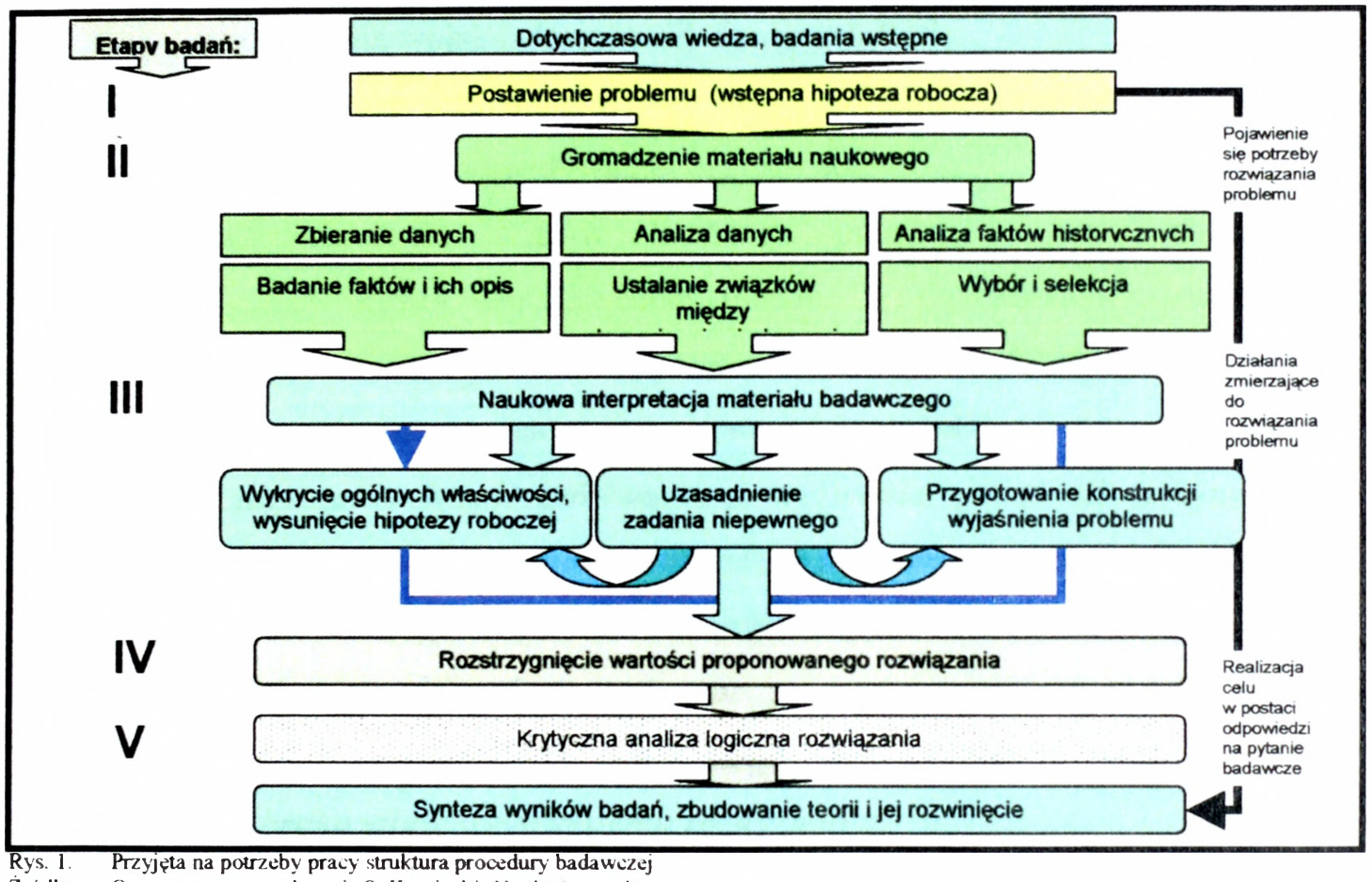
Jako **element rozpoznawczy** w pracy rozumiany jest pojedynczy środek rozpoznania wraz z obsługą (niekiedy grupa środków), który jest częścią elementu ugrupowania rozpoznawczego, niekiedy również podsystemu rozpoznania, (np. posterunek obserwacyjny – PO, jest częścią podsystemu obserwacji). Element rozpoznawczy jest dostosowany do krótkotrwałego działania w niewielkim oderwaniu od sił głównych i nie ma możliwości zachowania podstawowych warunków samoobrony, bytowych oraz eksploatacyjnych. W przestrzeni element rozpoznawczy jest obiektem punktowym, w zależności od składu przyjmuje nazwę: patrol rozpoznawczy (PR), posterunek obserwacyjny, samolot (śmigłowiec) rozpoznawczy, drużyna patrolowa, grupa wypadowa (GW), inżynieryjny posterunek fotografowania (IPF), aparatownia radioodbiorcza, stacja zakłóceń radiowych itp.

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

- teoretycznych aspektów działań rozpoznawczych,
- działalności rozpoznawczej w nowych uwarunkowaniach,
- struktury organizacyjnej sił rozpoznania.
- potencjalnego rozwoju systemu rozpoznania.

Już w trakcie badań wstępnych (zgodnie z przyjętą procedurą badawczą zobrazowaną na rys. 1) zespół autorski zmierzyć się musiał z problemem dotyczącym zakresu możliwości i zdolności perspektywicznego systemu rozpoznania do korzystania i współpracy z analogicznymi systemami sił sojuszniczych/koalicyjnych. Analiza trendów panujących w Sojuszu Północnoatlantyckim oraz poświęcającej coraz więcej uwagi swoim militarnym możliwościom Unii Europejskiej pozwoliła na konstatację, iż wielonarodowość jednostek organizacyjnych wojsk lądowych na poziomie korpusu jest faktem. Prawdziwe zatem wydaje się twierdzenie, iż narodowym szczeblem prowadzenia działań w ramach NATO lub innej, doraźnie tworzonej koalicji w najbliższej perspektywie pozostanie dywizja, brygada lub batalion (batalionowa grupa bojowa) – co potwierdzają wyniki analiz doświadczeń operacji stabilizacyjnej w Iraku. Jednocześnie zapoczątkowany, na razie w aspekcie planistycznym,

proces tworzenia „zbrojnego ramienia" Unii Europejskiej spowoduje, iż już na bardzo niskich szczeblach dowodzenia przyszłościowy system rozpoznania będzie musiał być zdolny do współpracy z analogicznymi systemami państw sojuszniczych czy koalicyjnych.



Rys. 1. Przyjęta na potrzeby pracy struktura procedury badawczej
Źródło: Opracowano na podstawie S. Kaminski, *Nauka i metoda*

W toku dalszej pracy, dążąc do osiągnięcia zakreślonych wcześniej celów, zespół autorski sformułował problem badawczy w postaci pytania:

W jakich kierunkach ewoluować będą systemy rozpoznania wojsk lądowych w XXI wieku?

Kolejny, drugi etap badań, będący *de facto* etapem badań porównawczych, stanowił w głównej mierze ciąg analiz, porównań i analogii oraz dalsze, dogłębne studiowanie dostępnej literatury przedmiotu. W konsekwencji tych badań zespół autorski utwierdził się w przekonaniu o konieczności podziału głównego problemu naukowego na kilka mniejszych, ograniczonych w zakresie rozpatrywanych zagadnień. W ten sposób zostały zidentyfikowane i wyodrębnione następujące problemy szczegółowe:

1. Jakie wnioski, w kontekście rozwoju systemów rozpoznania, wynikają z teoretycznego i praktycznego dorobku działań rozpoznawczych w operacjach?
2. Jak przedstawia się stan i możliwości współczesnego systemu rozpoznania wojsk lądowych Sił Zbrojnych RP?
3. Jakie zmiany nastąpią w organizacji i funkcjonowaniu systemu rozpoznania w przewidywalnej przyszłości?

Rezultaty dalszych studiów literatury przedmiotu oraz wnioski z doświadczeń będących konsekwencją udziału w ćwiczeniach stanowiły podstawę sformułowania **hipotezy wstępnej**. Bazując na posiadanej wiedzy oraz wynikach poprzedniego etapu badań, zespół autorski założył, że:

Nowe zagrożenia bezpieczeństwa oraz wyzwania wobec sił zbrojnych (w tym wojsk lądowych) w sposób jednoznaczny podnoszą znaczenie ciągłego, dokładnego i terminowego rozpoznania. Zarówno typowe działania zbrojne na dużą skalę, jak i przedsięwzięcia związane ze zwalczaniem terroryzmu czy operacjami stabilizacyjnymi nie będą mogły być skutecznie realizowane w warunkach braku właściwego systemu rozpoznania.

Istniejący w wojskach lądowych Sił Zbrojnych RP system rozpoznania nie spełnia w wystarczającym stopniu istniejących i przewidywanych wymagań i powinien ulec daleko idącym przeobrażeniom.

W perspektywicznym systemie rozpoznania wojsk lądowych istotną rolę odgrywać będą środki rozpoznania elektronicznego (ELINT) oraz obrazowego (IMINT). Utrzymana zostanie także rola i znaczenie rozpoznania sygnałowego (SIGINT). Rozpoznanie osobowe (HUMINT) pozostanie istotnym czynnikiem uzupełniających inne środki, szczególnie podczas działań w otoczeniu utrudniającym realizację rozpoznania innymi środkami. Szczególnego znaczenia nabierze funkcjonowanie systemu rozpoznania na rzecz działań informacyjnych, zaś system rozpoznania będzie musiał być zdolny do skutecznego działania w ramach operacji stabilizacyjnych i pokojowych. Oczekiwać należy robotyzacji środków rozpoznawczych oraz dalszego rozwoju technologicznego środków transmisji danych rozpoznawczych.

Kolejny, trzeci etap badań zobligował autorów do zastosowania szeregu metod badawczych prowadzących do rozwiązania określonych uprzednio problemów szczegółowych. Specyfika zidentyfikowanych problemów badawczych rzutowała bezpośrednio na fakt, iż wśród użytych metod znalazły się zarówno metody teoretyczne jak i, w ograniczonym zakresie, empiryczne.

Z metod teoretycznych we wszystkich etapach badań znalazły zastosowanie: analiza, synteza, wnioskowanie, porównanie, analogia oraz uogólnienie.

Analiza zastosowana została przede wszystkim w badaniach literatury dotyczącej problematyki systemu rozpoznania, w celu identyfikacji stanu obecnego i możliwych kierunków zmian w rozpatrywanym obszarze.

Syntezie poddane zostały wnioski z badań teoretycznych i empirycznych, porównywane następnie z przyjętymi założeniami.

W wydobywaniu podobieństw i różnic w rozwiązaniach z zakresu systemu rozpoznania w różnych siłach zbrojnych państw członkowskich NATO szczególnie pomocne było wykorzystanie **porównania**.

Poszukiwanie podobieństw badanych procesów i tendencji ułatwione zostało przez zastosowanie metody **wnioskowania,** przede wszystkim **wnioskowania zawodnego**.

Z kolei, biorąc pod uwagę kryteria rodzaju zdań stanowiących przesłanki oraz zdań będących konkluzjami, wnioskowanie (zawodne) realizowane było głównie przez **analogię**.

Uogólnienie wykorzystane zostało w trakcie badań do ujawnienia cech i zjawisk powtarzalnych, a przez to do formułowania zasad uniwersalnych dotyczących systemu rozpoznania.

W zakresie metod empirycznych szczególne znaczenie miała **obserwacja** ćwiczeń dowódczo - sztabowych. Przedmiotem obserwacji były:

- ćwiczenia dowódczo - sztabowe Akademii Obrony Narodowej: ZIMA i MAZURY 2004 oraz PIERŚCIEŃ 2004 i PIERŚCIEŃ 2005,
- ćwiczenie dowódczo – sztabowe CAPABLE WARRIOR 2004 (Wielonarodowy Korpus Północ – Wschód).

Wyniki obserwacji wymienionych ćwiczeń pozwoliły autorom dokonać weryfikacji zasadności przyjętych założeń w zakresie potencjalnych kierunków rozwoju systemów rozpoznania.

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

Dobrze realizowane działania rozpoznawcze, możliwe tylko w warunkach posiadania właściwego systemu rozpoznania, warunkują powodzenie każdej operacji. Twierdzenie to pozostaje aktualne, pomimo zmian wprowadzanych w dziedzinie organizacji, uzbrojenia i wyposażenia wojsk rozpoznawczych oraz zasad prowadzenia działań zbrojnych. Zarówno klasyczne działania na dużą skalę, jak i wszelkiego rodzaju przedsięwzięcia o charakterze militarnym, związane ze zwalczaniem terroryzmu, konfliktami asymetrycznymi czy operacjami stabilizacyjnymi nie będą mogły być skutecznie realizowane w warunkach braku właściwego systemu rozpoznania. System ten nie traci na znaczeniu również w trakcie przygotowania i prowadzenia działań zgodnie z najnowszymi koncepcjami działań sieciocentrycznych (network centric warfare – NCW). Co więcej, NCW stawia przed takim systemem nowe wymagania, rozszerzając znaczenie elementu rozpoznawczego zgodnie z zasadą every soldier is a sensor (każdy żołnierz jest „sensorem").

Wyniki badań pozwalają na konkluzję, iż pożądany system rozpoznania wojsk lądowych musi zapewnić w każdym rodzaju działań militarnych prowadzenie działań rozpoznawczych, czyli określonych czynności prowadzących do uzyskania, w drodze bezpośredniej obserwacji lub wykorzystania innych metod wykrywania, danych (informacji) o działaniach i środkach przeciwnika lub potencjalnego przeciwnika, oraz danych meteorologicznych, hydrograficznych lub geograficznych określonego obszaru.

W takim aspekcie system rozpoznania wojsk lądowych sił zbrojnych RP charakteryzuje się szeregiem niedomagań, szczególnie w zakresie:

- *efektywności sieci informacyjnej systemu rozpoznania, bazującej głównie na sprzęcie analogowym o zróżnicowanym czasie eksploatacji, co skutkuje stosunkowo długim czasem przekazu danych,*
- *powiązanego z powyższym braku zaawansowanego systemu komputerowego wspomagania pracy komórek rozpoznawczych w organach dowodzenia,*
- *rozpoznania specjalnego na szczeblach taktycznych (które w praktyce zanikło),*
- *braku sił i środków rozpoznawczych w strukturach batalionów zmechanizowanych i czołgów, co zmniejsza możliwości rozpoznania i napływ aktualnych informacji o przeciwniku i środowisku pola walki na najniższych szczeblach dowodzenia,*
- *przestarzałego technicznie sprzętu rozpoznania na szczeblu oddziałów i związków taktycznych.*
- *niewielkich możliwości rozpoznania na rzecz rażenia ogniowego (ogniem artylerii i śmigłowców), w tym braku środków precyzyjnej lokalizacji celów i natychmiastowej transmisji pozyskiwanych danych, w myśl koncepcji walki sieciocentrycznej,*
- *ograniczonych możliwości rozpoznania elektronicznego, głównie ze względu na fakt, iż pododdziały radioelektroniczna ZT nie posiadają środków do rozpoznawania i obezwładniania relacji radiowych z rozproszonym widmem (emisji typu frequency hopping – FH). Stąd istotnego znaczenia w prowadzeniu walki elektronicznej przez ZT nabiera problem stosowania innych środków, jak np. uderzenia nadajnikami zakłóceń jednorazowego użytku. Ponadto brak nowoczesnych środków łączności radiowej zapewniających pracę sieci rozpoznania, namierzania i zakłócania powoduje, że wydłużeniu ulega czas przekazu i przetwarzania danych pozyskiwanych w podsystemie rozpoznania radioelektronicznego,*
- *dużych dysproporcji w zakresie możliwości pozyskiwania danych na potrzeby prowadzenia ognia w stosunku do możliwości oddziaływania*

ogniowego środków rażenia - aktualnie środki rozpoznania artyleryjskiego mogą prowadzić rozpoznanie jedynie na potrzeby artylerii wykonującej zadania bezpośredniego wsparcia ogniowego (na głębokość od 5 do 7 km, a wyjątkowych warunkach do 10 km),

- *braku (w zakresie taktycznego systemu rozpoznania skażeń) wyposażenia elementów strukturalnych systemu w urządzenia do automatycznego wykrywania i określania parametrów wybuchów jądrowych, w tym również powietrznych, a także przyrządów umożliwiających automatyczne wykrywanie większej liczby środków toksycznych, w tym także przemysłowych,*
- *pozbawienie związku taktycznego organicznych pododdziałów rozpoznania powietrznego (śmigłowców i środków bezpilotowych), co zmniejsza stopień wiarygodności pozyskiwanych danych,*
- *stosunkowo maej samodzielności dowódców pododdziałów rozpoznawczych, głównie ze względu na nadmierną szczegółowość stawianych im zadań.*

Na podstawie wyników badań założyć można, iż system rozpoznania XXI wieku będzie zdolny do realizacji zadań, opartych na błyskawicznym zdobywaniu, opracowywaniu i rozpowszechnianiu informacji. Doskonalona wciąż będzie technika skanowania za pomocą urządzeń optoelektronicznych i radiolokacyjnych. Dalsze prace prowadzone będą w obszarze czterech technik: fotografii, techniki infralokacji (termolokacja), telewizji i radiolokacji. Należy spodziewać się kontynuacji realizacji programów budowy nowych bezzałogowych aparatów latających, opracowanych pod kątem spełnienia wymagań, stawianych podsystemom rozpoznawczym w nowoczesnej przestrzeni walki.

Przyszły system rozpoznania musi być w stanie tworzyć dokładny, zwięzły o dużej wierności wirtualny obraz obszaru działań, a ponadto łączyć te informacje z ogólną sytuacją, pogodą i danymi terenu (o dużej rozdzielczości) dając podstawę do przedstawiania dowódcy rzeczywistej sytuacji. Ten wspólny obraz pomagał będzie dowódcy w szybkim przygotowywaniu i podejmowaniu optymalnych decyzji. Można zatem stwierdzić, iż istotnym wyznacznikiem

rozwoju systemu rozpoznania będzie daleko idąca integracja ze zautomatyzowanymi systemami wspomagania dowodzenia, jako zasadniczy sposób zapewnienia dowódcom i sztabom jednolitej świadomości przestrzeni walki w czasie rzeczywistym lub niemal rzeczywistym.

Założyć można, że przyszłościowy system rozpoznania powinien zapewnić realizację następujących funkcji:

- *zdobywania, opracowywania, korelowania i zobrazowywania danych/informacji rozpoznawczych,*
- *oceny danych/informacji rozpoznawczych,*
- *nadzorowania płynnej sytuacji przestrzeni walki, uwzględniając przeciwdziałające czynniki, takie jak ataki przeciwnika, walka elektroniczna, zmęczenie, warunki pogodowe i terenowe,*
- *przekazywania lub otrzymywania rozkazów, informacji w czasie rzeczywistym.*

W zakresie rozpoznania patrolowego bojowe wozy rozpoznawcze nowej generacji umożliwią wykonywanie trzech zasadniczych zadań:

- *rozpoznania walką (wóz silniej opancerzony i uzbrojony, wykorzystywany do rozpoznania i głębokiego obchodzenia pozycji wojsk przeciwnika);*
- *dalekiego rozpoznania (wóz lżejszy, przystosowany do skrytego przenikania w głąb ugrupowania bojowego przeciwnika, w celu rozpoznania rejonów, obiektów i ewentualnej pomocy w kierowaniu ogniem własnych środków rażenia);*
- *ubezpieczenia bojowego (wóz silniej opancerzony i uzbrojony, który mógłby ogniem wstrzymać podchodzące pododdziały przeciwnika w czasie rozwijania lub wykonywania manewru przez wojska własne).*

W rozpoznaniu elektronicznym oczekiwać należy rozwiązania następujących problemów:

- *rozszerzenia przechwytywanego pasma częstotliwości, z możliwością wykrywania emisji na listkach bocznych;*

- *możliwości odbierania, namierzania, oraz identyfikacji radiolokatorów stosujących przemienność częstotliwości i przeszukiwanie elektroniczne, modulację przestrzenną, kompresję impulsów, technikę dopplerowską, technikę szerokopasmową;*
- *możliwości działania w zatłoczonym eterze, przy występowaniu zakłóceń wspólnokanałowych i interferencyjnych;*
- *zwiększenia dokładności namierzania;*
- *budowy małych, lekkich urządzeń do instalowania na bezzałogowych aparatach latających;*
- *integracji urządzeń rozpoznania radioelektronicznego z czujnikami różnych typów i możliwością sterowania ich pracą.*

Przyszłościowe środki rozpoznania radiolokacyjnego najprawdopodobniej będą zmierzać w kierunku zwiększenia zabezpieczenia przed szumami, zmniejszenia ciężaru i gabarytów stacji, zwiększenia ilości wykonywanych funkcji, dokładności a także wiarygodności uzyskiwanych informacji. Urządzenia optoelektroniczne umożliwią prowadzenie rozpoznania bez względu na porę doby, czy też warunki atmosferyczne. Nowe urządzenia wykorzystywać będą cały zakres promieniowania podczerwonego, oraz być sprzężone z laserami lub radiolokatorami pracującymi w zakresie fal milimetrowych.

Potwierdzona została teza, iż w perspektywicznym systemie rozpoznania wojsk lądowych istotną rolę odgrywać będą środki rozpoznania elektronicznego oraz obrazowego, a także utrzymana zostanie rola i znaczenie rozpoznania sygnałowego. Rozpoznanie osobowe również pozostanie istotnym czynnikiem uzupełniających inne środki.

Należy przyjąć, iż przyszły „system rozpoznania XXI wieku" ***odegra zasadniczą rolę w osiąganiu przewagi informacyjnej***.

Kolejny, czwarty etap badań polegał na weryfikacji hipotezy w celu jej ostatecznego uzasadnienia i sprawdzenia. Istotną rolę odegrały w tym zakresie opinie zebrane techniką wywiadu bezpośredniego, wyrażone przez oficerów szeregu państw NATO, dysponujących odpowiednim doświadczeniem

w zakresie planowania rozwoju systemów rozpoznania zarówno w układzie narodowym, jak i sojuszniczym.

Piąty, ostatni etap prac obejmował podsumowanie wyników badań, ich uogólnienie i syntezę. Zespół autorski przyjął określoną, wiarygodną interpretację rozwiązania problemu badawczego, która przedstawiona została w pisarskim opracowaniu wyników badań.

Struktura niniejszej pracy obejmuje wstęp, trzy rozdziały oraz zakończenie.

We **wstępie** zaprezentowano metodologiczne aspekty badań oraz konstrukcję opracowania pisarskiego pracy. Uzasadniono w nim także wybór tematu i przedstawiono przyjętą procedurę badawczą.

Rozdział pierwszy obejmuje wyniki badań dotyczących teoretycznych podstaw systemu rozpoznania wojsk lądowych.

Rozdział drugi zawiera wyniki badań w zakresie struktury, stanu i możliwości systemu rozpoznania wojsk lądowych Sił Zbrojnych RP.

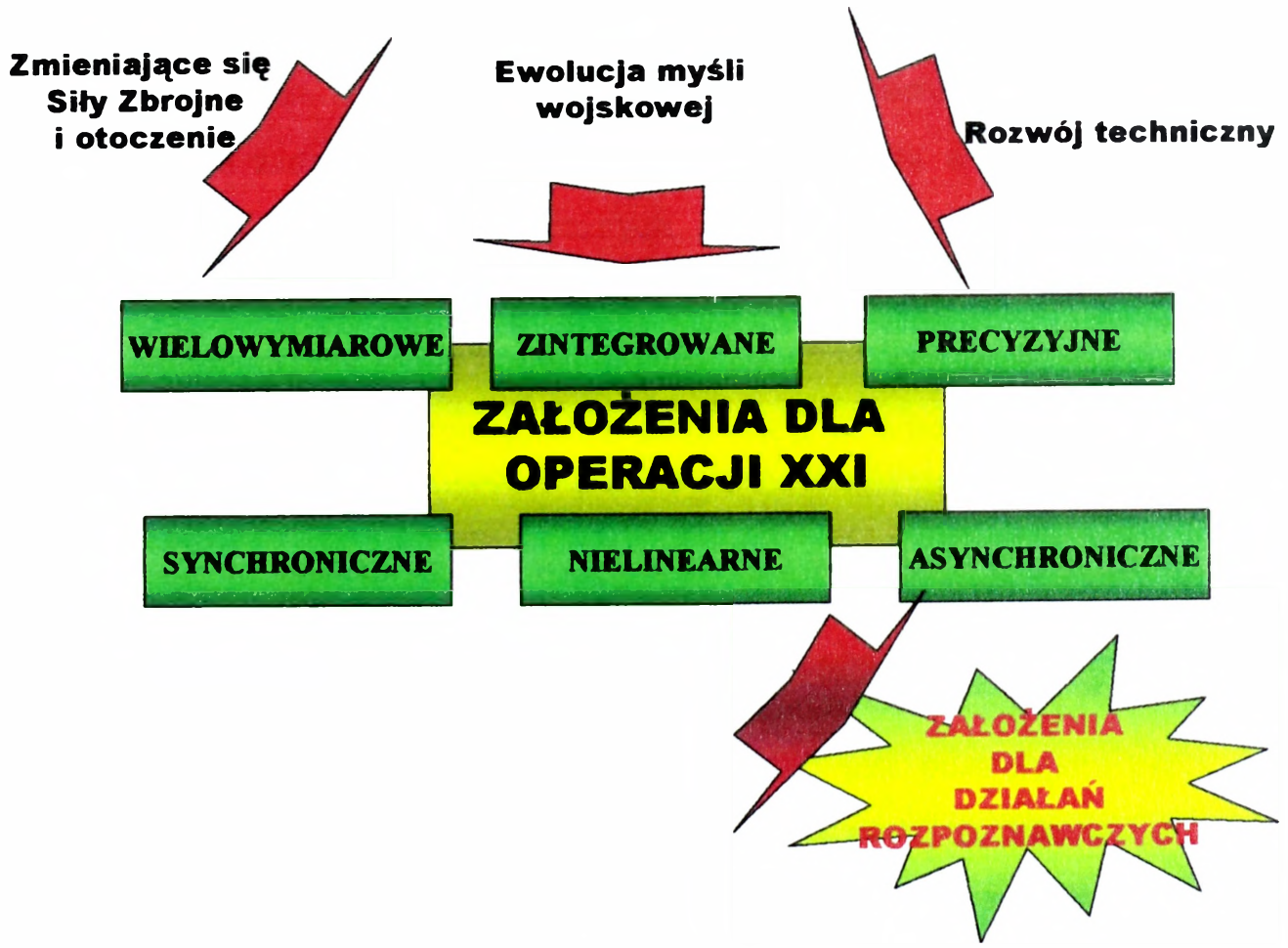
Treści **rozdziału trzeciego** stanowią podsumowanie całości procesu badawczego dotyczącego prognozy rozwoju systemu rozpoznania XXI wieku.

Pracę uzupełniają załączniki poszerzające zakres informacji dotyczących istotnych, zdaniem autorów, problemów.

Opracowane przez zespół autorski i zaprezentowane w rozdziale 3. wyniki badań w zakresie potencjalnego rozwoju systemu rozpoznania stanowić może podstawę do dalszych prac w tym zakresie. Powinny być one ukierunkowane na wszechstronne, praktyczne sprawdzenie przedstawionych rezultatów w jednostkach rozpoznawczych wojsk lądowych oraz w dalszej kolejności, modyfikacji i aktualizacji treści dokumentów doktrynalnych dotyczących problematyki rozpoznania w Wojskach Lądowych Sił Zbrojnych RP.

1. TEORETYCZNE PODSTAWY DZIAŁAŃ ROZPOZNAWCZYCH W OPERACJACH

Na pierwszy plan w rozwoju dzisiejszych Sił Zbrojnych wysuwają się przeobrażenia między innymi w myśli wojskowej, spowodowane w dużej części przez rewolucję techniczną. Bardzo złożone środowisko pola walki, będące skutkiem tych wydarzeń będzie miało znaczące implikacje dla przyszłych operacji a tym samym i dla działań rozpoznawczych (rys. 1.1).



Rys. 1.1. Założenia dla operacji XXI wieku

Ostatnie operacje w Południowej Azji, Panamie, Somalii, Rwandzie, Haiti, Bośni oraz Iraku wpływają na obraz koniecznych zmian. Oznacza to wykreowanie „operacji dalekiego zasięgu" jakie siły zbrojne (w przewidywanej przyszłości) będą

zmuszone prowadzić. Przytoczone powyżej przykłady to obraz średnio intensywnych konfliktów, a nie tradycyjnych wielkich bitew (oprócz Iraku).

Precyzyjne określenie trendów rozwojowych Sił Zbrojnych zarówno w bliższej, jak i dalszej przyszłości jest niezmiernie trudne. Prognozowanie utrudnia nie tylko fakt, że dotyczy ono ciągłych przemian, ale również to, że rozwój technologii i ich wojskowych zastosowań jest wyznaczany przez wiele różnorodnych uwarunkowań.

Stanisław Lem we wstępie do „Okamgnienia" przywołał wydaną w 1993 r. w Niemczech przez Federalne Ministerstwo do Spraw Badań i Technologii pracę pt.: „Technologie XXI stulecia". Z przekąsem zauważył, że jest rzeczą godną uwagi to, iż o rewolucji w dziedzinie ogólnoświatowej łączności (*world wide web*), czy też o biotechnologii, które stawały się niejako na oczach autorów, nie ma w niej ani jednego słowa, nie mówiąc już o poświęceniu temu tematowi osobnego rozdziału.

Przykład ten, podobnie jak inne, choćby z historii, wskazuje na to, jak niewdzięcznym zadaniem jest prognozowanie, zwłaszcza w odniesieniu do zjawisk cywilizacyjnych i kulturowo-społecznych. Niewdzięcznym, ale jakże frapującym. Bodajże generał Mac Arthur powiedział, że dobry żołnierz – niezależnie od tego czy dowodzi plutonem, czy armią – musi oglądać się w tył, patrzeć na boki i w przód, ale myśleć powinien tylko o przyszłości. Dobrze więc, że nasze myślenie nie kończy się na latach 2006–2008, lecz wybiega daleko w przód. Jest przy tym w prognozowaniu, zwłaszcza 25–30 letnim, pewien walor, który nie występuje w pracach nad planami średnio- i krótkoterminowymi. Ograniczone środki na realizację planów oraz korzystniejsza sytuacja geostrategiczna Polski jako członka NATO powodują, że z jednej strony ta bliska przyszłość sił zbrojnych jest postrzegana przez pryzmat niemożności – „nie stać nas na to", z drugiej zaś mniejsze zagrożenie skłania do traktowania sił zbrojnych jako efektownego, ale niezbyt przydatnego narzędzia. Wspomniany walor to komfort wynikający z tak odległej perspektywy, jak 25 lat. Pozwala bowiem na podejście typu: „wszystko się może zdarzyć". I choć nie upoważnia do fantazjowania, to jednak skłania do optymizmu, także w aspekcie finansowym.

Uwzględniając dotychczasowe burzliwe tempo postępu technicznego w świecie, można stwierdzić, że XXI wiek będzie wiekiem walki o informacje

i wszelkie podejmowane działania będą temu podporządkowane. Utworzenie we wszystkich rodzajach Sił Zbrojnych wspólnych, zbiorowych i sieciowych struktur dowodzenia, rozpoznania i walki elektronicznej powinno zagwarantować dominację informacyjną na polu walki.[3]

Prognozy owe są jednak obarczone wieloma niedoskonałościami, błędami różnego rodzaju, z elementarnymi włącznie. Błędem najbardziej rzucającym się w oczy jest skłonność do projektowania przyszłości jako ciągu linearnie dokonujących się zmian, ignorowanie obecnych w każdym procesie załamań rozwoju, regresów nawrotów[4] itp. Najbardziej niebezpieczna zaś może okazać się skłonność do upraszczania, co najczęściej wyraża się w absolutyzacji czynnika postępu technologicznego. Groźny może się też okazać militarno-wojenny populizm z jego tanią futurystyką, ekspozycją wojen wirtualnych, fascynacją możliwą skutecznością przyszłych systemów walki (niszczenia)[5] itd.

1.1. Ewolucja myśli wojskowej

W dziedzinie wojskowości wciąż priorytetowym tematem pozostaje kwestia związana z charakterem przyszłych operacji. Przysparza ona trudności zarówno teoretykom, jak i praktykom, którzy wybiegając w przyszłość pragną znaleźć odpowiedź na pytanie: jaki może być charakter przyszłych operacji? Jakie cechy i własności będą się składać na ich obraz? Jakie główne czynniki mogą determinować ich kształt? Czy zasadniczo będą się różnić od stanu, który dziś możemy obserwować? Które kierunki rozwoju wydają się na tyle trwałe, by w na ich podstawie można było wypowiadać się na ten temat? Czy nagle nie wystąpi jakieś szczególnie istotne zdarzenie, które w diametralny sposób zmieni nasz dotychczasowy pogląd, zakłóci zakładany kierunek rozwoju i tym samym zniweczy nasze prognozy? Powyższe problemy wydają się być kluczowe w prowadzonym obszarze badań, zaś ich interdyscyplinarny charakter nakłada obowiązek zachowania szczególnej ostrożności i uwagi w trakcie ich rozwiązywania.

---

[3] Zob. Materiały z warsztatów poświęconych przyszłości SZ, Sztab Generalny 6 czerwca 2001 r.
[4] B. Balcerowicz, *Wojny współczesne. Wojny Przyszłe*, Myśl wojskowa 2003, nr 5, s. 131.
[5] J. Black dostrzega wpływ popularnych (populistycznych) wyobrażeń o wojnach XXI wieku na niektóre doktryny militarne (w:) *War Post. Present and Future, Sulton Publishing*, London 2000, s. 284-287.

Mówiąc o charakterze przyszłych operacji, mamy na myśli zespół cech, które będą orzekać o nim, a więc będą opisywać, jaki może być w przyszłości. Powinny złożyć się na niego cechy i własności, które w zasadniczy sposób będą odróżniały jego obecny stan od stanu prognozowanego. Na obraz ten może, ponadto składać się wiele złożonych i różnorodnych czynników. Oddziaływać może na niego chociażby poziom rozwoju cywilizacyjnego, cele polityczne i zasobność podmiotów biorących w nich udział, system ich wartości czy też poziom morale, stopień rozwoju techniczno-technologicznego oraz warunki geograficzne.

Pomimo tak wielkiej różnorodności determinantów warunkujących charakter przyszłych operacji, wydaje się, iż uprawnieni jesteśmy do postawienia tezy, że **charakter przyszłych operacji będzie odzwierciedlał ogólny charakter przyszłego świata**. Z tego też względu nie będzie on czymś wyalienowanym, czy oderwanym od otaczającej go rzeczywistości, lecz właśnie będzie się dokładnie w nią wkomponowywał. Nie będzie mógł być inny, ponieważ charakter operacji nie jest i nie może być samodzielnym, innym bytem, lecz musi mieścić się w realiach rozpatrywanego okresu i co więcej, odzwierciedlać najistotniejsze jego cechy. Stąd też nasuwają się następne pytania: jakie to najistotniejsze cechy złożą się na naturę przyszłego świata a następnie będą się przekładać na charakter przyszłych operacji? Jakie to potężne „siły" mogą w istotny i trwały sposób je formować?

W teoretycznych opracowaniach akademickich nietrudno dostrzec skłonność do generalizowanej identyfikacji przyszłych wojen i konfliktów do wyspecyfikowania wszystkich ich cech. Stwarza się przy tym wrażenie, że problem można zredukować do jednego, ogólnego modelu. Na przykład C. Rutkowski znajduje 24 takie właściwości[6].

---

[6] C. Rutkowski, *Problemy bezpieczeństwa i sił zbrojnych XXI wieku*, Myśl Wojskowa 2001, nr 2 (613), s. 5-27. Dowodzi on, po pierwsze, że: groźba wojny pozostanie realna, utrzyma się niskie prawdopodobieństwo konfliktów wielkiej skali, gwałtownie będzie wzrastać natomiast liczba konfliktów ograniczonych w skali, celach i formach; podstawowym wyznacznikiem cech konfliktu będzie poziom rozwoju technologicznego i zasobność ekonomiczna stron; działania militarne będą coraz częściej służyły wykorzystywaniu szans, a nie przeciwdziałaniu zagrożeniom; procesy kierowania, rażenia będą realizowane w czasie realnym; kierowanie (dowodzenie) wojskami będzie zastępowane kierowaniem wojną i walką zbrojną; wzrastać będzie oddziaływanie na pozabojowe punkty ciężkości, maleć - na elementy bojowe; problemy odstraszania, walki informacyjnej, specjalnej itp. przenosić się będą na wyższy, polityczny szczebel; wzrośnie integracja działań cywilnych i wojskowych; działania militarne inne niż wojna staną się podstawowym obszarem działań sił zbrojnych; działania wojenne i inne niż wojna będą z reguły działaniami połączonymi w wymiarach: narodowo-międzynarodowym, cywilno-wojskowym, bojowo-niebojowym oraz RSZ; będzie maleć rola i zmieniać się charakter wojsk lądowych; technologie i zdolności do działań w kosmosie w coraz większym stopniu będą determinować możność, sprawność i charakter działań w innych sferach. Po drugie, że **walka zbrojna**

Odnoszą się one jednak - co należy podkreślić - nie do jednego generalnego modelu wojny (operacji), lecz do całego spektrum możliwych konfliktów zbrojnych.

Nadchodzącą erę już dawno nazwano „informacyjną". Erze informacyjnej powinny więc odpowiadać „wojny (operacje) w sferze informacyjnej".

Należałoby się zastanowić nad tym, czy ta przyszła wojna (operacje), prowadzona za pomocą najnowocześniejszych środków (wojna (operacja) ery informacyjnej) nie będzie się toczyć również według ogólnych klasycznych reguł?

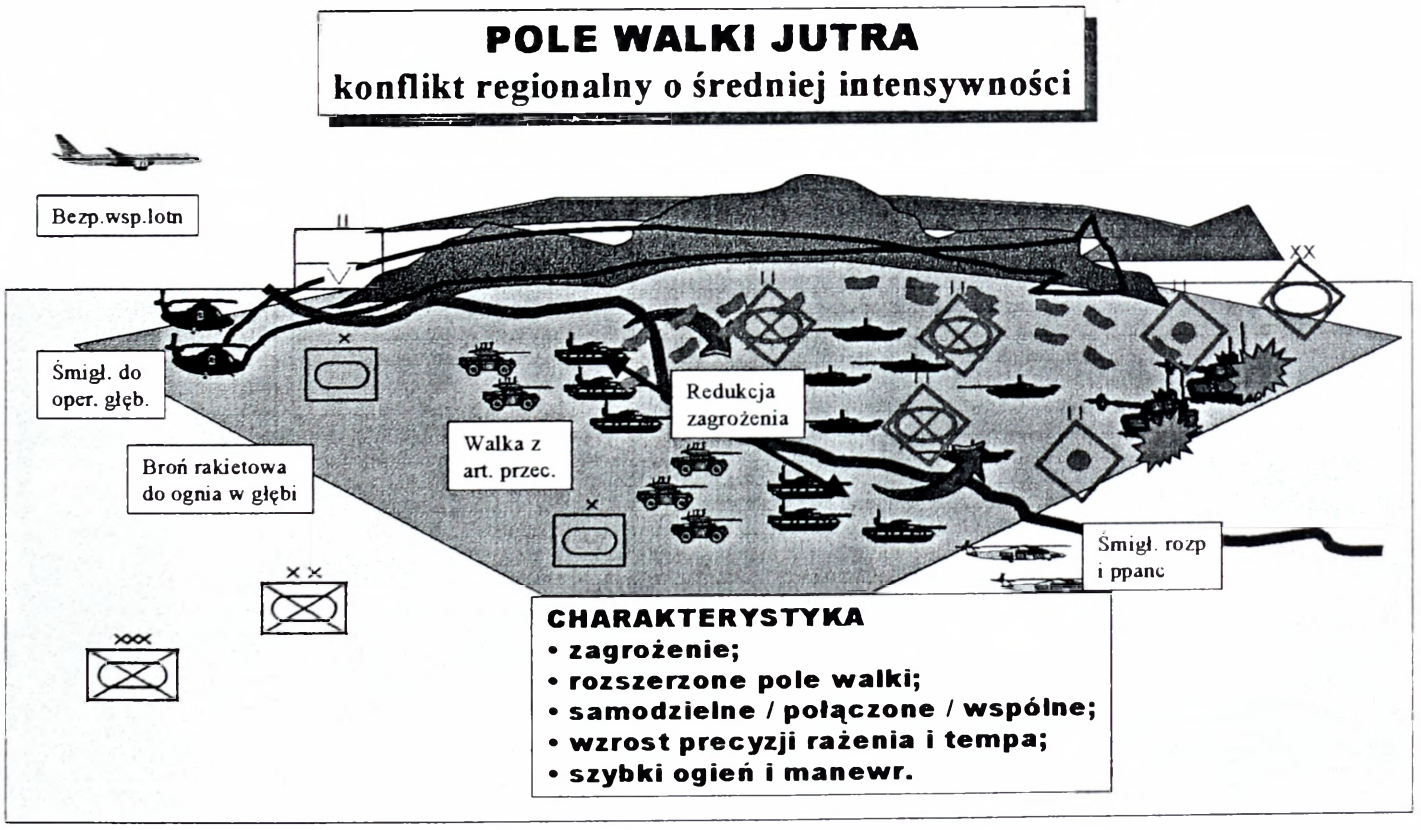
Zwraca na to uwagę J. Barnett w swojej książce *Future Warfare* (Przyszłe działania wojenne) przy okazji analizy wojny (walki) informacyjnej. Wymienia on kilka właściwości charakterystycznych dla wszystkich wojen, w tym i dla wojen (operacji) przyszłych, co do których przewiduje, że:

1. Zastosowanie walki informacyjnej będzie w nich warunkiem koniecznym do osiągnięcia zwycięstwa. Tak jak dotychczas zwycięstwo było możliwe tylko przy uzyskaniu przewagi na lądzie, morzu i w powietrzu, to w przyszłości będzie wątpliwe osiągnięcie zwycięstwa bez przewagi informacyjnej.
2. Wojna (walka) informacyjna może być zjawiskiem autonomicznym, ale może też być komponentem wspierającym działania militarne bądź działaniem głównym, wspieranym działaniami militarnymi.
3. Tak jak w przypadku wszystkich form wojen, wojna (walka) informacyjna będzie zawierać elementy ofensywne i defensywne. Strony (wojska) będą równocześnie używać informacji jako swoistej broni zaczepnej oraz bronić się przed użyciem jej przez przeciwnika.

---

w przyszłości będzie: właściwa społeczeństwu i cywilizacji informacyjnej, wykorzystującym jej możliwości; pełniej podporządkowana geopolityce i geoekonomii; częściej będzie środkiem realizacji i interesów ekonomicznych; w mniejszym stopniu będzie gwarantowała trwałe rozwiązania polityczne, stabilizację bezpieczeństwa; toczyć się będzie również między podmiotami niepaństwowymi lub w ich interesie; będzie coraz bardziej złożona, wielowymiarowa, zróżnicowana w formach, coraz bardziej będą złożone kombinacje środków i narzędzi; rzadziej będzie planowym środkiem polityki, częściej natomiast efektem eskalacji w sytuacjach nieskuteczności środków pozamilitarnych; będzie coraz bardziej asymetryczna i pośrednia; jeszcze bardziej zaskakująca i trudna do prognozowania, planowania scenariuszowego; będzie się toczyć w nowych ośrodkach, których znaczenie wzrośnie (kosmos, infosfera, nowe formy energii); pojawią się nowe formy i wymiary odstraszania; wzrośnie rola BMZ, bezpieczeństwa systemów; walka zbrojna będzie rodzić nowe, inne problemy i dylematy kierownicze, wykonawcze, moralne (z panelu dyskusyjnego polsko-ukraińskiego nt.: „Tendencje rozwoju walki zbrojnej").

4. Wojna (walka) informacyjna będzie prowadzona na wszystkich poziomach: strategicznym, operacyjnym i taktycznym. Normalnym obowiązkiem dowódców i sztabów (gremiów decyzyjnych) na każdym z tych szczebli będzie organizacja i koordynacja informacyjnych akcji i kampanii. Będą to uderzenia (ataki) na infrastrukturę informacyjną zarówno w wymiarze państw, teatrów działań, jak i jednostek wojskowych.
5. Wojska (siły zbrojne) muszą być zdolne do działań także w warunkach skutecznych uderzeń informacyjnych przeciwnika. Nierealna bowiem może się stać pełna osłona przed przeciwnikiem tylko przez oddziaływanie informacyjne.



Rys. 1.2. Konflikt regionalny

Szereg wizji, przewidywań, prognoz dotyczących wojen (operacji) przyszłości, wojen (operacji) XXI wieku zdaje się sugerować, że można mówić o ich jednym, ogólnym modelu. To złudzenie. Zapewne pojawią się nowe formy wojen (operacji), tak jak

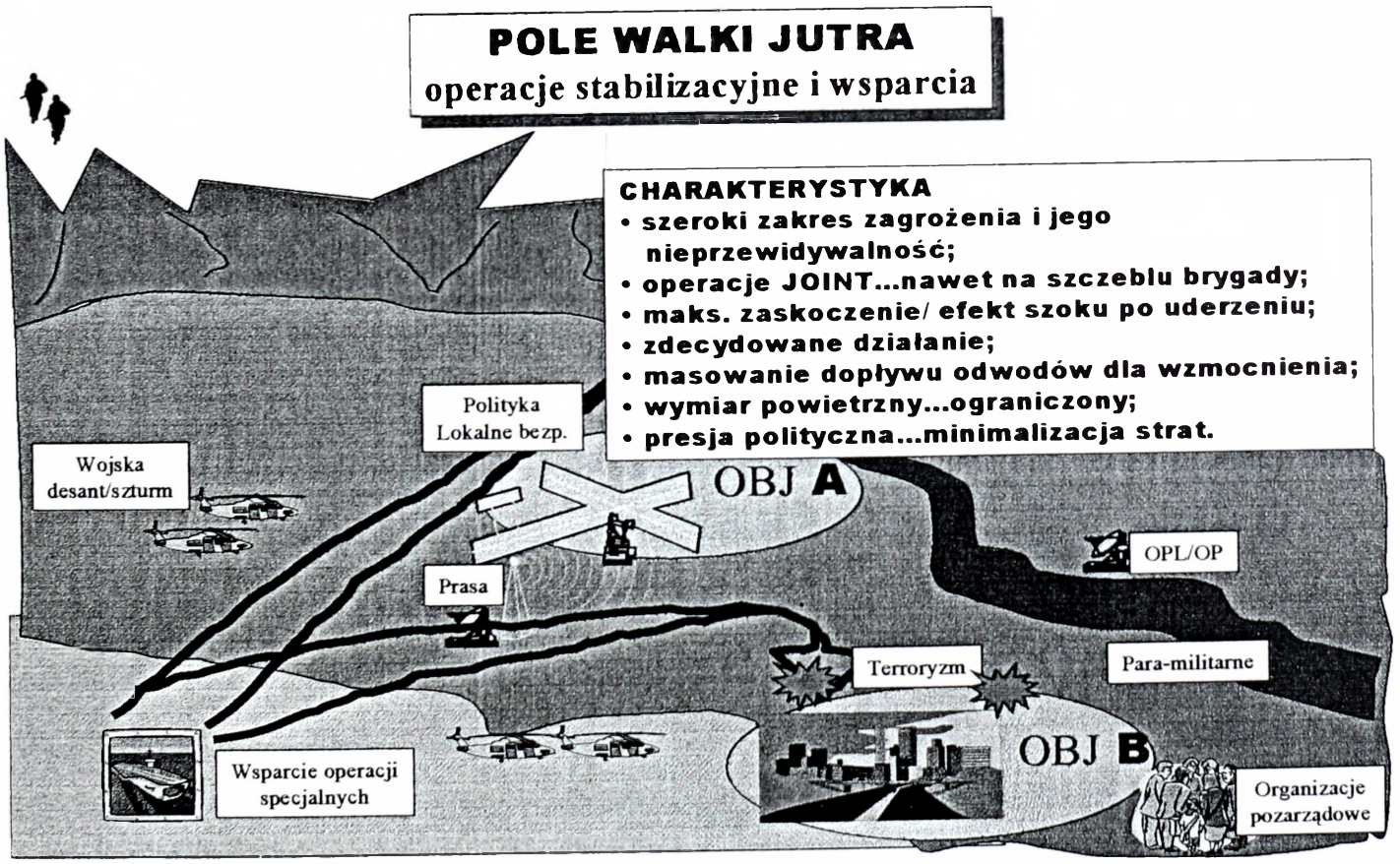
się pojawiły na przełomie XX i XXI wieku; stare jednak długo nie zanikną. Nowych zaś form może być kilka (zobacz rys. 1.2 i 1.3).

Z myślą o przyszłości rodzi się pytanie: jak długo jeszcze może dominować (może być obecny) taki właśnie typ wojen (operacji), konfliktów?

Biorąc pod uwagę fakt, że proces globalizacji dopiero nabiera dynamiki, może on nie zaniknąć, nie zejść na dalszy plan przez co trwać najmniej kilka dziesięcioleci.

Opierając się (bezpośrednio lub pośrednio) na teorii fal cywilizacyjnych „świata podzielonego na troje", poszczególnym kręgom przypisuje się niekiedy mocno zgeneralizowany w jego opisie „typ" wojny. I tak:

- kręgowi pierwszemu - „wojny XXI wieku", wojny ery informacyjnej;
- kręgowi drugiemu - „wojny XX wieku", wojny ery industrialnej;
- kręgowi trzeciemu - „wojny średniowieczne", wojny ery przedindustrialnej.



Rys. 1.3. Nowe formy działań

Ta uproszczona klasyfikacja ma czysto teoretyczne i zazwyczaj problematyczne znaczenie. Należy więc mieć na uwadze, że wtedy gdy mówimy o wojnach (operacjach) ery informacyjnej, to poruszamy się wciąż w obrębie futurystyki. Takich wojen

(operacji) jeszcze w istocie nie doświadczono, choć najnowsza historia dostarczyła ostatnio kilku symptomatycznych prób. W rzeczywistości nie wykształtowały się jeszcze społeczeństwa informacyjne. Należy jednak mieć na względzie to, że dzisiaj najbardziej technologicznie zaawansowane społeczeństwa funkcjonują w rozdwojonym porządku gospodarczym. Wciąż po części opiera się on na masowej produkcji, a po części na technologiach i usługach trzeciej fali. A ponieważ formy wojen (operacji) odpowiadają formom cywilizacji, formom produkcji, to możemy w dzisiejszych konfliktach zbrojnych dostrzec wymieszane ze sobą cechy wojen (operacji), drugiej i trzeciej fali. I tak to pozostanie zapewne przez co najmniej kilka dziesięcioleci XXI wieku. W wojnach (konfliktach), które mogą toczyć między sobą państwa kręgu industrialnego, prawdopodobnie znajdą zastosowanie technologie i systemy awangardowe. To (między innymi) sprawi, że owe konfrontacje będą przejmować pewne cechy wojen ery informacyjnej.

Pomieszanie cech wojen (operacji) różnych fal cywilizacyjnych występowało już wyraźnie w trzech symptomatycznych konfliktach przełomu XX i XXI wieku: w wojnie w rejonie Zatoki Perskiej, w wojnie o Kosowo, a także w wojnie (kampanii antyterrorystycznej) w Afganistanie i Iraku. W każdym z tych konfliktów po jednej stronie walczyły (walczą) armie najnowocześniejsze, po drugiej armie i organizacje tkwiące w epoce industrialnej, a nawet przedindustrialnej.

W przewidywaniach dotyczących przyszłych wojen, między innymi opartych na tofflerowskiej koncepcji „świata podzielonego na troje", nie należy zapominać o potwierdzonej historycznie prawdzie, że jeżeli pojawiają się nowe formy wojen (operacji), stare formy długo jeszcze nie znikną. Zwiększy się zatem ich różnorodność.

Obok koncepcji „świata podzielonego na troje" w ośrodkach (amerykańskich) przyjmuje się jeszcze kilka innych[7]. Na szczególną uwagę - w moim przekonaniu - zasługuje koncepcja skupiająca uwagę na możliwym renesansie ideologii. Według tej koncepcji, podziały w świecie mogą być zdominowane przez konkurujące, zwaśnione między sobą ideologie. Wiele konfliktów zbrojnych mogłoby wtedy mieć podłoże religijne, mogłyby niekiedy przybierać charakter swoistych krucjat.

---

[7] F. Heisbourg: *Wojny,* Warszawa 1998, s. 23-38.

Spośród podejść pragmatycznych (z przewidywanych modeli przyszłych interwencji zbrojnych) chciałbym przedstawić, te prezentowane jeszcze w roku 1998 przez F. Heisbourga. Zakłada on, że w ciągu najbliższych dwudziestu pięciu lat możemy być świadkami wojen w czterech następujących, szerokich kategoriach[8]:

1. Wojny podejmowane przez złośliwe antyzachodnie dyktatury, mające dostęp do broni masowego rażenia - wojny „państw - złoczyńców". Należy przewidywać, że ten typ konfliktu może pojawić się w obszarze rozciągającym się od północnej Afryki po Afganistan.
2. Wojny sukcesyjne, prowadzone o władzę w obrębie niegdyś istniejących, a dziś rozpadających się państw. Prawdopodobnymi teatrami tego typu wojen pozostaną Bałkany, niektóre obszary byłego Związku Radzieckiego, subkontynent indyjski i Afryka subsaharyjska.
3. Wojny „rozrywające", w których obce i rodzime grupy zaatakują uporządkowane podstawy funkcjonowania istniejących społeczeństw za pomocą tak różnych środków, jak terror, destrukcja systemów informatycznych, finansowych i innych. Ten rodzaj wojen grozi przede wszystkim krajom najbardziej rozwiniętym.
4. Wojny klasyczne, w których klasyczne (dziewiętnastowieczne) cele będą osiągane metodami XXI wieku. Tego typu wojny mogą zaistnieć przede wszystkim we wschodniej Azji.

Wymienione powyżej kategorie wojen – interwencji zbrojnych będą w różnym stopniu odzwierciedlać poziom zaawansowania rozwoju społeczeństw - jest to więc wizja komplementarna do wizji „świata podzielonego na troje".

W tej klasyfikacji brakuje ***wojen - interwencji zbrojnych***, prowadzonych przez państwa najbardziej rozwinięte tam, gdzie:

- zostaną naruszone ich interesy;
- będą tego wymagać względy humanitarne;
- będzie zagrożone bezpieczeństwo międzynarodowe lub bezpieczeństwo tych państw.

---

[8] Chodzi (głównie) o amerykański zespół „*Strategie Study Institute*", zajmujący się projektem „Army After Next".

Po historycznym zwrocie lat dziewięćdziesiątych - jak pisze gen. G. Gudera[9], generalny inspektor sił zbrojnych Niemiec - zakres zadań sił zbrojnych na naszym kontynencie został również zwielokrotniony i znacznie zróżnicowany. Obejmują one coraz większy obszar, od działań służących kształtowaniu partnerstwa i kooperacji po pomoc humanitarną - z jednej strony oraz od operacji służących przywracaniu pokoju po obronę kraju - z drugiej. W związku z tym niezbędne stało się rozpoczęcie gruntownych zmian w siłach zbrojnych. Zmiany te zostały zintensyfikowane i znacznie poszerzone na skutek wydarzeń z 11 września 2001 roku.

Uznano, że siły zbrojne przyszłości nie mogą być dalej jednostronnie ukierunkowywane na prowadzenie - jak to nazwał gen. G. Gudera - **„dużych operacji"**.

Oprócz nich muszą one, w celu przeciwdziałania konfliktom i likwidowania kryzysów - jak to ma miejsce w byłej Jugosławii - być zdolne do prowadzenia **„średnich operacji"** (siłami około 10 000 ludzi) - i to dość długo.

Ponadto, w celu realizacji operacji ewakuacyjnych i ratowniczych oraz ochrony własnych wojsk przed grupami terrorystycznymi, siły zbrojne muszą być zdolne do prowadzenia **„małych operacji"**, nawet na obszarach daleko położonych od własnego kraju.

Najbardziej prawdopodobne operacje (średnie i małe) wymagają konsekwentnego i zupełnie nowego ukierunkowania sił zbrojnych i związanego z tym dostosowania ich możliwości i struktur. Reasumując, siły zbrojne muszą być zdolne do realizowania nowych zadań, a więc **prowadzenia operacji rozstrzygających, misji stabilizacyjnych oraz operacji specjalnych**.

Oznacza to również, że siły zbrojne muszą mieć możliwość wydzielania odpowiedniej części do działania w ramach sił międzynarodowych, muszą więc być zdolne do wypełniania zobowiązań międzynarodowych odpowiednich do nowych zadań. Istota tych reform musi tkwić w strukturalnym ukierunkowaniu na realizację przewidywanych zadań. Ich spełnienie wymaga, by siły zbrojne były dyspozycyjne, a więc zdolne do działania w bardzo krótkim czasie, w wyniku czego można

---

[9] G. Gudera, Das Heer auf dem Weg in die Zukunft, Europäische Sicherheit, nr 10/2000 s. 14-21.

zwiększyć zakres ich działania. Ponadto muszą one być mobilne i bardziej uniwersalne niż obecnie.

Inną koncepcję konfliktów w XXI wieku przedstawił płk Peter FABER [10] - w zarysie programu szkolenia - a mianowicie uważa on, „...że w tradycyjnych konfliktach wojownicy musieli kształtować walkę, by dopasować ją do dostępnego uzbrojenia. W konfliktach jutra posłużą się „bronią", która będzie kształtować walkę, wtedy „powiążą" atuty broni. Dlatego należy skupić się na umiejętnym wykorzystaniu posiadanej wiedzy i manipulowaniu nią, zamiast uciekać się do stosowania tradycyjnych metod (wzmacniać siły, nadzorować terytorium itd.)". Ponadto – autor stwierdza - że należy odrzucać strategię liniową lub strategię następujących po sobie operacji prowadzonych przez pojedyncze rodzaje sił zbrojnych lub ich komponenty. Trzeba raczej przewidywać duże rozproszenie obrońców, w wymiarze operacji równoległych, „skrojonych" na miarę „**zintegrowanych modułów sił**". Te wrażliwe na wymiar czasowy operacje pozwolą na użycie siły rozstrzygającej, nie zaś miażdżącej, na „zdemontowanie" przeciwnika, a nie jego starcie z powierzchni ziemi i wreszcie, umożliwią przestrzeganie trzech zasad (opartego na RMA[11] konfliktu): **1) wiedzieć więcej niż twój przeciwnik, 2) ubiec go, 3) unikać starć, kiedy ryzyko jest zbyt wysokie.**

A oto przykłady konfliktów ery RMA:

- wojny 4 generacji
- wojna asymetryczna[12]
- wojna sieciocentryczna[13]
- dominacja cyklu decyzyjnego
- szybka dominacja
- dominujący manewr
- strategiczne zapobieganie
- strategiczne uderzenia uprzedzające

---

[10] Zob. P. Faber, *Rewolucja w dziedzinie wojskowości (proponowany zarys programu szkolenia*), Zeszyt Naukowy AON 2003, nr 4 (53) s. 125.

[11] *Revolution in Military Affairs* - Rewolucja (transformacja)w Sprawach Wojskowych zob. wykład admirała Edmunda Giambastaniego przeprowadzonego 20 października 2003 r. w AON.

[12] Jej istota polega na tym, że w starciu dwóch stron - z której jedna jest niewspółmiernie słabsza pod względem militarnym od drugiej - słabszy chwyta się metod absolutnie niekonwencjonalnych, osiągając zarazem przy minimum środków maksimum efektu (także politycznego).

[13] Koncepcja wojny sieciocentrycznej stanowi teoretyczną podstawę dla transformacji sił zbrojnych USA. Wojna sieciocentryczna definiowana jest jako opierająca się na przewadze informacyjnej koncepcja prowadzenia operacji, według której wzrost siły bojowej jest generowany przez połączenie w sieć informacyjną sensorów, decydentów i systemów walki w celu osiągnięcia wspólnej świadomości, zwiększenia szybkości dowodzenia oraz tempa operacji, zwiększenia skuteczności uzbrojenia, wzrostu odporności na uderzenia przeciwnika oraz zwiększenia stopnia synchronizacji działań.

- wojna równoległa (lub hiperwojna)
- kontrola strategiczna
- wojna przybrzeżna
- siły lądowe przyszłości
- dominacja w całym spektrum działań
- szybkie operacje rozstrzygające
- gwałtowne zatrzymanie
- szok i przerażenie
- potęga 21
- taktyka roju
- wojna kombinacyjna

Jednocześnie, wszelkie zdolności w zakresie bezpieczeństwa powinny zostać połączone, tworząc system. Wewnątrz tego systemu poszczególne organizacje (podsystemy) powinny być sterowane raczej „poziomo" niż „pionowo". Innymi słowy, organizacje te powinny być płaskie, tak bardzo jak to możliwe. Ich rozbudowana struktura powinna być jak najbardziej pozioma.

Z przedstawionych rozważań wynika, że wiek XXI znacznie bardziej - nawet wręcz rewolucyjnie - zmienia i najprawdopodobniej będzie zmieniał współczesne bezpieczeństwo w porównaniu ze stanem, który istniał w wieku ubiegłym. Staje się ono obecnie coraz bardziej różnorodne, kompleksowe i znacznie trudniejsze do przewidzenia. Zwiększa się liczba podmiotów, które mogą w nim brać udział. Klasyczny międzypaństwowy wariant wojny staje się coraz mniej prawdopodobny.

Równocześnie, nowe wymagania zmieniają krajobraz przyszłych działań. Ich uczestnicy oraz ich struktury mogą być w skali dotychczas nieznanej - nie tylko wzajemnie powiązani, lecz także w różnorodny sposób uwikłani w wydarzenia międzynarodowe. Coraz widoczniejsze stają się również rozmiary związków między Północą, a Południem, gdyż zaczynają coraz skuteczniej pomagać w rozstrzyganiu problemów pojawiających się w podzielonym i zróżnicowanym świecie.

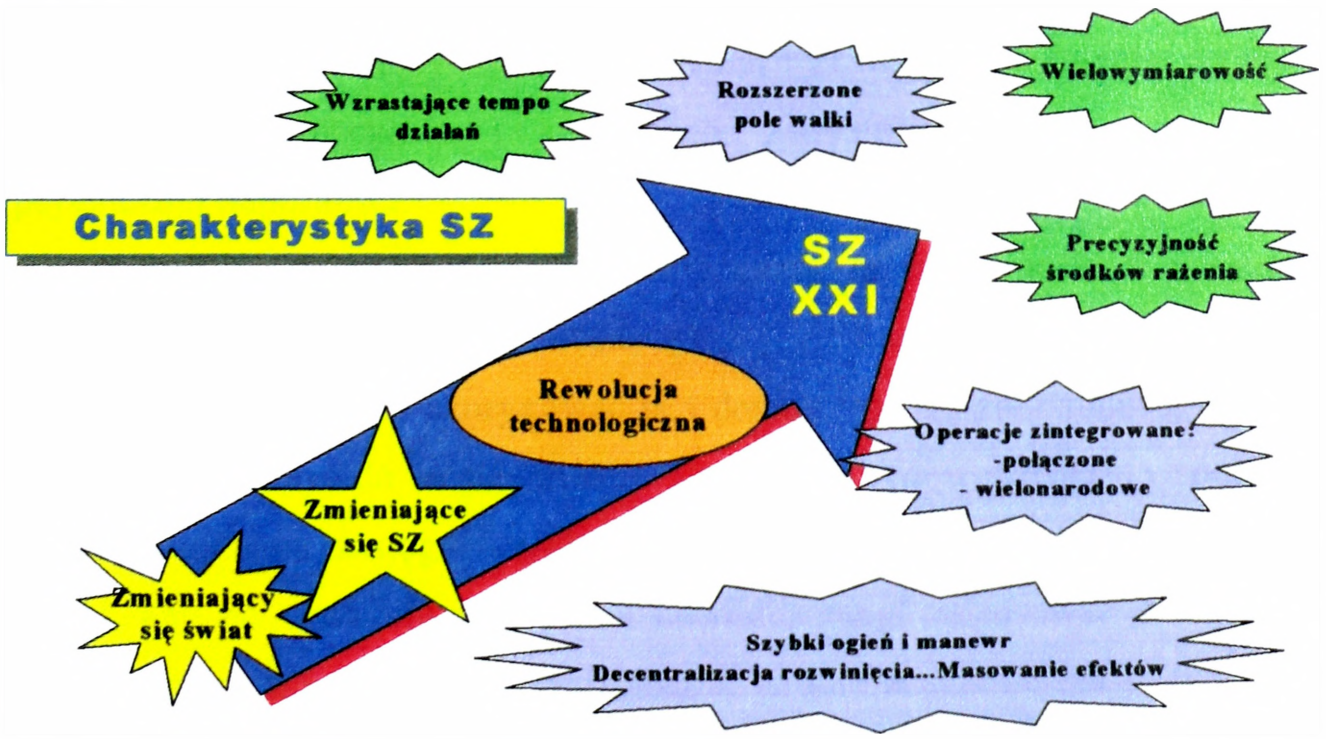
Wszystkie te czynniki mają decydujący wpływ na kształt przyszłych operacji. Wymagają, by rozumieć je jako zjawisko obejmujące wszystkie, a przynajmniej prawie wszystkie dziedziny życia. Wymagają również uznania:

- wielowymiarowego pojmowania kryzysów i konfliktów oraz niezbędności udzielenia odpowiedzi na wszystkie współczesne wyzwania polityki, bezpieczeństwa (a przynajmniej na ich większość);
- prewencji jako zjawiska niepodzielnego.

Na przykład, w walce z terroryzmem niezbędna okazała się współpraca międzynarodowa, umożliwiająca skuteczne, a zarazem wspólnie uzgodnione rozwiązanie pojawiających się wyzwań.

Szczególnie ważna stała się również współpraca pomiędzy najważniejszymi organizacjami, gdyż sprzyja prowadzeniu skutecznej polityki bezpieczeństwa.

Należy sobie także zdawać sprawę, że również obecna reforma sił zbrojnych jest znacznie głębsza aniżeli wszystkie dotychczasowe i bynajmniej nie sprowadza się do zmian strukturalnych. To nowe ukierunkowanie sił zbrojnych oznacza, że chodzi o głęboką transformację, która będzie trwać stosunkowo długo, być może ponad 10 lat. Chodzi bowiem przede wszystkim o zmiany mentalności i koncepcji, zmiany taktyczno - operacyjne, personalne, strukturalne i technologiczne. Zakładanym celem tego procesu jest osiągnięcie takiego stopnia doskonałości sił zbrojnych, by móc w przyszłości lepiej realizować skomplikowane zadania.



Rys. 1.4. Charakterystyka Sił Zbrojnych XXI wieku

Zmiany te są i prawdopodobnie nadal będą wykonywane w trakcie wypełniania przez część wojska różnorodnych zadań (misji). Oznacza to, że

równolegle przebiegają (i należy przypuszczać – że nadal będą przebiegać) trzy procesy: udział w operacjach, przekształcanie oraz doskonalenie. Dlatego - z czego trzeba sobie zdawać sprawę - siły zbrojne realizują te zadania w bardzo skomplikowanych warunkach. Uwzględniając powyższe, można sądzić, że w najbliższych latach siły zbrojne nadal będą zmuszone doskonalić kwalifikacje, zapewnić należytą realizację obecnych i przewidywanych działań (operacji), przeprowadzić zaplanowaną restrukturyzację sprawnie i w sposób zorganizowany (rys. 1.4).

W konkluzji można stwierdzić że, struktura sił zbrojnych mogłaby uwzględniać cztery lub pięć rodzajów sił zbrojnych, tj. **Wojska Lądowe, Siły Powietrzne, Marynarkę Wojenną, Wojska Specjalne i Informacyjne**, podporządkowane jednemu dowództwu operacyjnemu na czas kryzysu lub wojny. Z kolei jednostki wojskowe, szczególnie te, które mogą być użyte w pierwszej kolejności, powinna cechować stała gotowość do jak najszybszej realizacji różnorodnych zadań, umiejętność rozpoznawania na czas zaistniałej i dość często zmieniającej się sytuacji oraz sprawnego realizowania zadań i częstej ich zmiany. Stawia to przed siłami zbrojnymi większe niż dotychczas wymagania w zakresie wyszkolenia, wyposażenia, uzbrojenia, zabezpieczenia i wszelkiego zaopatrywania, a także fizycznej i psychicznej odporności.

Realizacja tych zadań wymaga, aby każdy dowódca posiadał wiedzę, która pozwoli mu na szybką i właściwą ocenę sytuacji oraz optymalne podjęcie decyzji, by w razie potrzeby potrafił skorygować ją i dostosować do zmieniającej się sytuacji, a więc był zdolny do elastycznego kierowania (dowodzenia) współczesnymi działaniami. Zatem zasięg i szybkość działań rozpoznawczych powinien być tak głęboki, aby po wykryciu zagrożenia dowódca mógł zastosować z odpowiednim wyprzedzeniem skuteczne przeciwdziałanie. Istotne znaczenie ma w tym wypadku także fakt, że siły zbrojne mogą być obecnie wykorzystywane do realizacji znacznie szerszego zakresu zadań niż to miało miejsce w minionym, industrialnym okresie.

1.2. MODYFIKACJA TECHNICZNA ŚRODKÓW WALKI

Duży wpływ na rozwój technologii wykorzystywanych przez wojsko mają doświadczenia z ostatnich wojen i lokalnych konfliktów zbrojnych oraz prognozy w zakresie przyszłościowego pola walki. Wykorzystywane są doświadczenia z wojny w Zatoce Perskiej i z konfliktów lokalnych w Afganistanie, byłej Jugosławii i Czeczenii. Najwięcej jednak doświadczeń wyniesiono z wojny w rejonie Zatoki Perskiej, którą można nazwać wojną dwóch generacji technologicznych. Udowodniła ona zdecydowaną wyższość technologii wykorzystywanych przez państwa koalicji nad technologiami lat siedemdziesiątych i osiemdziesiątych będących w dyspozycji Iraku. Wyposażenie (technologie) państw koalicji pozwalało na prowadzenie działań w nocy, obieg informacji rozpoznawczej (między innymi do środków rażenia) był w czasie zbliżonym do rzeczywistego a ponadto umożliwiało precyzyjne niszczenie wybranych celów oraz omijanie stref rażenia broni Iraku. W wojnie tej na szeroką skalę zostały zastosowane nowe technologie w kompleksowym ujęciu systemowym we wszystkich rodzajach sił zbrojnych, znane jako - C4I[14] - niekiedy nazywany jako „Kompleksowy system wspomagania dowodzenia". Między innymi wykorzystano systemy (technologie) kosmiczne, komputerowe, laserowe, stealth, mikroelektroniki, optoelektroniki oraz informatyczne.

Analiza przydatności poszczególnych egzemplarzy techniki (środków walki) w powiązaniu z prognozą rozwoju, umożliwia planowanie przyszłego pola walki i określenie roli poszczególnych rodzajów środków walki, np. rakiet balistycznych i manewrujących, samolotów i śmigłowców, czołgów, artylerii, broni plot, ppanc, rozpoznawczych, całemu arsenałowi z przedrostkiem cyber-, itd. Jednocześnie daje nowy impuls w odwiecznej walce między systemami ofensywnego i defensywnego oddziaływania.

Tempo rozwoju technicznego w XX w., zwłaszcza rozwój elektroniki, mikroelektroniki, optroniki, automatyki, technik komputerowych, laserowych, a także możliwość wytwarzania nowych materiałów, przyczyniły się do wzrostu dynamiki

---

[14] *Command, Control, Communications, Computers and Intelligence*

i znaczenia rozwoju, technologicznego, a w konsekwencji do wzrostu możliwości wojsk.

W największym stopniu dotyczy to:

- stymulowanej potrzebami programów kosmicznych inżynierii materiałowej;
- mikroelektroniki napędzanej postępem w dziedzinie fizyki ciała stałego;
- techniki komputerowej;
- telekomunikacji;
- optroniki.

W zakresie innowacji główną uwagę skierowano na techniki sterowania oraz automatyzacji. Wraz ze wzrostem postępu w mikro- i w nanotechnologii zarysowały się możliwości wykorzystania ich w większości dziedzin wojskowych. Dotyczy to również innowacji odnoszących się do przetwórstwa surowców, techniki, produkcji oraz do wytwarzania komponentów. Rozwój ten zwiększył możliwości poszczególnych systemów uzbrojenia w rozpoznaniu (identyfikacji), przenoszeniu ładunków oraz precyzji trafienia głównie dzięki zastosowaniu odpowiednich technik napędowych i wykorzystaniu bardziej wydajnej sensoryki. Osiągnięcia te kompleksowo zostały wykorzystane w technice komputerowej, informatyce, elektronice i telekomunikacji, co w znacznej mierze przyczyniło się do zwiększenia szybkości i pojemności zbierania, przetwarzania i wykorzystania informacji.

Najnowsze osiągnięcia technologiczne umożliwiły tworzenie sieciowych powiązań komunikacyjnych w obszarze dowodzenia, rozpoznania i prowadzenia walki. Przykładem mogą być działania państw koalicji podczas wojny w rejonie Zatoki Perskiej, w których na podstawie danych z rozpoznania kosmicznego, lotniczego, agenturalnego i specjalnego (w czasie rzeczywistym) podejmowano decyzje, a te przez linie łączności (komunikacyjne) były przesyłane do środków walki (samolotów, okrętów, środków opl, artylerii itp.).

W siłach lądowych osiągnięto większą odporność czołgów i bojowych wozów opancerzonych (BWO) na zniszczenie oraz zwiększono skuteczność środków ppanc., w niszczeniu środków opancerzonych. Większość systemów broni przystosowano do prowadzenia działań w nocy i w różnych warunkach pogodowych. Zastosowanie w artylerii amunicji samonaprowadzającej się w połączeniu

z pociskami manewrującymi (OUI, RAAM) zdecydowanie zwiększyło jej możliwości bojowe. Wykorzystano też technologie laserowe do naprowadzania pocisków na cel *(Copperhead* - USA i *Krasnopol* - Rosja) oraz w systemach kierowania ogniem artylerii.

Wprowadzenie do wyposażenia wojsk, elektronicznych systemów dowodzenia i kierowania oraz nowoczesnych środków walki powietrznej, zwłaszcza pocisków manewrujących i rakietowych pocisków balistycznych, zmusiło specjalistów do rozpoczęcia prac nad wdrożeniem nowych technologii do przeciwlotniczych systemów dalekiego zasięgu *(Patriot* - USA, *S-300* - Rosja). W systemach tych dzięki wprowadzeniu nowych rozwiązań i technologii należy oczekiwać poprawy takich parametrów, jak:

- odporność na środki przeciwdziałania radioelektronicznego przeciwnika;
- skrócenie czasu reakcji;
- zwiększenie zasięgu umożliwiającego zwalczanie zarówno pocisków manewrujących, jak i taktycznych oraz operacyjno-taktycznych balistycznych pocisków rakietowych;
- zwiększenie współczynnika prawdopodobieństwa trafienia celu;
- polepszenie możliwości manewrowych;
- zwiększenie możliwości jednoczesnego śledzenia i zwalczania wielu celów, niezależnie od tego, na jakiej wysokości działają

W systemach dowodzenia i łączności szeroko została zastosowaną technika cyfrowa, światłowodowa i komputerowa, co w znacznym stopniu zwiększyło szybkość i objętość przekazywanych informacji oraz znacznie poprawiło warunki utajniania przesyłanych wiadomości. Nowe systemy dowodzenia i łączności umożliwiają współpracę różnych rodzajów wojsk wykorzystujących własne urządzenia nawet w układach koalicyjnych.

Powyższe systemy są wyposażone w urządzenia do zobrazowania pola walki, urządzenia szyfrujące do kodowania i przesyłania danych (informacji) z bardzo dużymi prędkościami. W dużym zakresie wykorzystuje się jedną z technologii kosmicznych, jaką jest system nawigacji satelitarnej - GPS[15], który umożliwia dokładne określenie miejsca położenia. Obecnie jest on w indywidualnym

[15] GPS – *Global Positioning System* (globalny system pozycjonowania)

wyposażeniu żołnierza, a także wozów bojowych, samolotów i okrętów oraz stanowi ważny element pocisków artyleryjskich i rakietowych. Osiągnięcia w przedstawionych technologiach przyczyniły się do znacznego zwiększenia możliwości środków walki wszystkich rodzajów sił zbrojnych, zarówno tych wcześniej produkowanych poprzez ich modernizację, jak i nowych.

Najwięcej zmian wprowadzono w samolotach bombowych i myśliwsko-bombowych. W szczególności dotyczy to systemów uzbrojenia, nawigacji, dowodzenia i łączności oraz obrony indywidualnej. Największe osiągnięcia w tej dziedzinie mają Stany Zjednoczone, Francja i Wielka Brytania.

W systemach uzbrojenia doskonalono sposoby naprowadzania rakiet powietrze-ziemia, powietrze-powietrze zarówno z wykorzystaniem technologii laserowych, jak i radiolokacyjnych, optycznych i telewizyjnych. Dużą uwagę przywiązywano do modernizacji i rozwoju bomb kasetowych oraz ślizgowych zasobników bombowych i bomb paliwowo-powietrznych, wykorzystywanych przez lotnictwo bezpośredniego wsparcia poła walki.

W nowoczesnych zasobnikach bombowych do najważniejszych elementów należą układy kierowania i naprowadzania, które w decydującym stopniu zwiększają precyzję trafienia. Bardzo duże znaczenie dla zachowania „żywotności" i zwiększenia możliwości bojowych lotnictwa odgrywa wykorzystanie technologii *stealth.* Dzięki tej technologii możliwe jest wykorzystanie do budowy samolotów, materiałów pochłaniających promieniowanie radiolokacyjne, konstruowanie samolotu o określonych kształtach, co pozwala ustawiać go w pozycji najmniej widocznej dla stacji radiolokacyjnej, a więc czyni samolot niewidzialny, gdyż ten ma wówczas bardzo małe pole powierzchni odbicia fal radiolokacyjnych. Technologię stealth włączono również do badań przy produkcji okrętów, samolotów-pocisków, pocisków manewrujących i czołgów.

Ale to już było, a co nas czeka w dającej się przewidzieć przyszłości? Dzisiaj modne terminy to: **cyberatak, cyberdefensywa, bomba elektromagnetyczna**, itp. – to hasła, które jeszcze niedawno zaliczano do kategorii science fiction. Obecnie w walce bardziej skuteczne od pancerza i żołnierskich bagnetów stają się wirusy

komputerowe stworzone w wojskowych laboratoriach, mogące paraliżować działania każdego rodzaju sił zbrojnych.

Według opinii CIA - powszechnie cytowanych choćby w internecie - Izraelowi udało się wykraść z sieci informacje o pociskach „*Patriot*". Takie boczne wejścia informatyczne, mogące stanowić wręcz zagrożenie dla systemów, mają też tworzyć sobie Indie oraz Rosja. Specjaliści tego kraju pracują obecnie nad planami wojen informatycznych, zarówno ofensywnych, jak i defensywnych. Kuba i Bułgaria mają rzekomo pracować nad bronią opartą na wirusach komputerowych. Nowoczesna technologia, stosowana w wielu rodzajach broni, w coraz większym stopniu oparta jest na technice komputerowej sprzężonej ze środkami łączności satelitarnej. Dysponent tej broni może w każdej chwili, nawet już po rozpoczęciu ataku, dokonać korekty zaprogramowanych celów, zmienić parametry nawigacyjne, czy chociażby rodzaj i siłę rażenia.

Nieuchronnie zbliża się czas połączenia telefonii, informatyki i telewizji w dowodzeniu i kierowaniu wojskami oraz masowego wykorzystania w działaniach bojowych środków walki elektronicznej. W przyszłych działaniach - co udowodniły przedstawione wcześniej konflikty lokalne - w które zaangażowane były wojska NATO, dostęp do informacji, jej błyskawiczne opracowanie i przekazanie będzie sprawą kluczową. Informacje o polu walki z automatycznych baz danych będzie uzyskiwał nawet pojedynczy żołnierz, a cyfrowa sieć zobrazowania pola walki będzie wykorzystywana do natychmiastowego przekazywania ich dowódcom oraz walczącym wojskom. Cyfrowa obróbka danych będzie umożliwiała jednoczesne korzystanie z informacji przez wszystkich zainteresowanych. Ze wspólnej bazy, w której gromadzone będą aktualne dane, każdy dowódca będzie mógł wybrać niezbędne informacje do podjęcia optymalnej decyzji.

Zapewnienie dopływu tak dużej ilości informacji nie będzie możliwe, jeśli nie zapewni się należytej ochrony własnych pasm częstotliwości, uniemożliwiając jednocześnie przeciwnikowi ich zakłócania. Dlatego w perspektywicznych działaniach kluczową rolę wyznacza się środkom walki elektronicznej, stosowanym do dezorganizacji systemów rozpoznania, dowodzenia i łączności przeciwnika oraz osłony własnych systemów dowodzenia i kierowania ogniem. Według ekspertów,

walka elektroniczna może stać się jednym z kluczowych czynników prowadzących do uzyskania przewagi na przyszłym polu walki.

Skoro na współczesnym polu walki tak duże znaczenie odgrywa informacja oraz systemy komputerowe, najskuteczniejszą formą ataku staje się przechwycenie danych i uszkodzenie infrastruktury informatycznej przeciwnika. Specjaliści wojskowi twierdzą więc, że o sukcesie w przyszłej wojnie decydować będą informatycy, a bronią stanie się maszyna cybernetyczna.

W koncepcji działań zbrojnych w XXI wieku, opracowanej na potrzeby armii sojuszniczych, nacisk kładzie się m.in. na takie zagadnienia, jak precyzja uderzenia cyfrowego w centra analityczne przeciwnika oraz jego urządzenia rozpoznawcze, szybkość uzyskiwania informacji o ruchach przeciwnika, możliwych zagrożeniach i przekazanie ustaleń do wojsk oraz cyberdefensywę – ochronę własnych danych i przeciwdziałanie zakłóceniom w ich przekazywaniu.

Uogólniając omawiane zagadnienie, można przyjąć, że znajdujące się obecnie w wyposażeniu wojsk uzbrojenie i pozostały sprzęt techniczny są systematycznie zamieniane nowymi wzorami, których właściwości zwiększają lub zwielokrotniają dotychczasowe możliwości. Cechą charakterystyczną nowych systemów uzbrojenia jest szybsze rozpoznanie i zniszczenie określonego celu z większej odległości niż to będzie mógł wykonać potencjalny przeciwnik. We wszystkich liczących się państwach zauważalny nacisk położono na zdobywanie informacji, jej przetwarzanie i dystrybucję w czasie rzeczywistym.

1.3. Koncepcja operacji XXI wieku

Wnioski z analizy założeń w podrozdziałach 1.1 i 1.2 uprawniają zespół do stwierdzenia, że przyszłe operacje (operacje XXI wieku), będą się cechowały niespotykanym jak dotąd rozmachem i dynamiką w układzie wielowymiarowym (lądy, morza, powietrze, kosmos, cyberprzestrzeń) oraz wielonarodowym. Głównie będą to operacje prawdopodobnie poniżej progu wojny - o charakterze prewencyjnym bądź wymuszającym pokój. Już teraz, w operacjach tego typu daje się zaobserwować tendencje integracyjne niektórych rodzajów sił zbrojnych (np. w wymiarze

powietrzno-lądowym). Proces ten może postępować stosunkowo szybko. Zacierające się różnice pomiędzy rodzajami sił zbrojnych mogą w rezultacie ewoluować na rzecz komponentów połączonych, zorganizowanych i funkcjonujących w obrębie określonych misji lub operacji.

Dotychczas rozpoznane trendy rozwoju wskazują, że na polu walki jutra: dowódcy[16] będą mieli do swojej dyspozycji precyzyjniejsze niż dziś i o większej sile destrukcji i ruchliwsze systemy walki oraz elastyczniejsze struktury organizacyjne. Zmasowanie potencjalnych możliwości może pozwolić przyszłym dowódcom na:

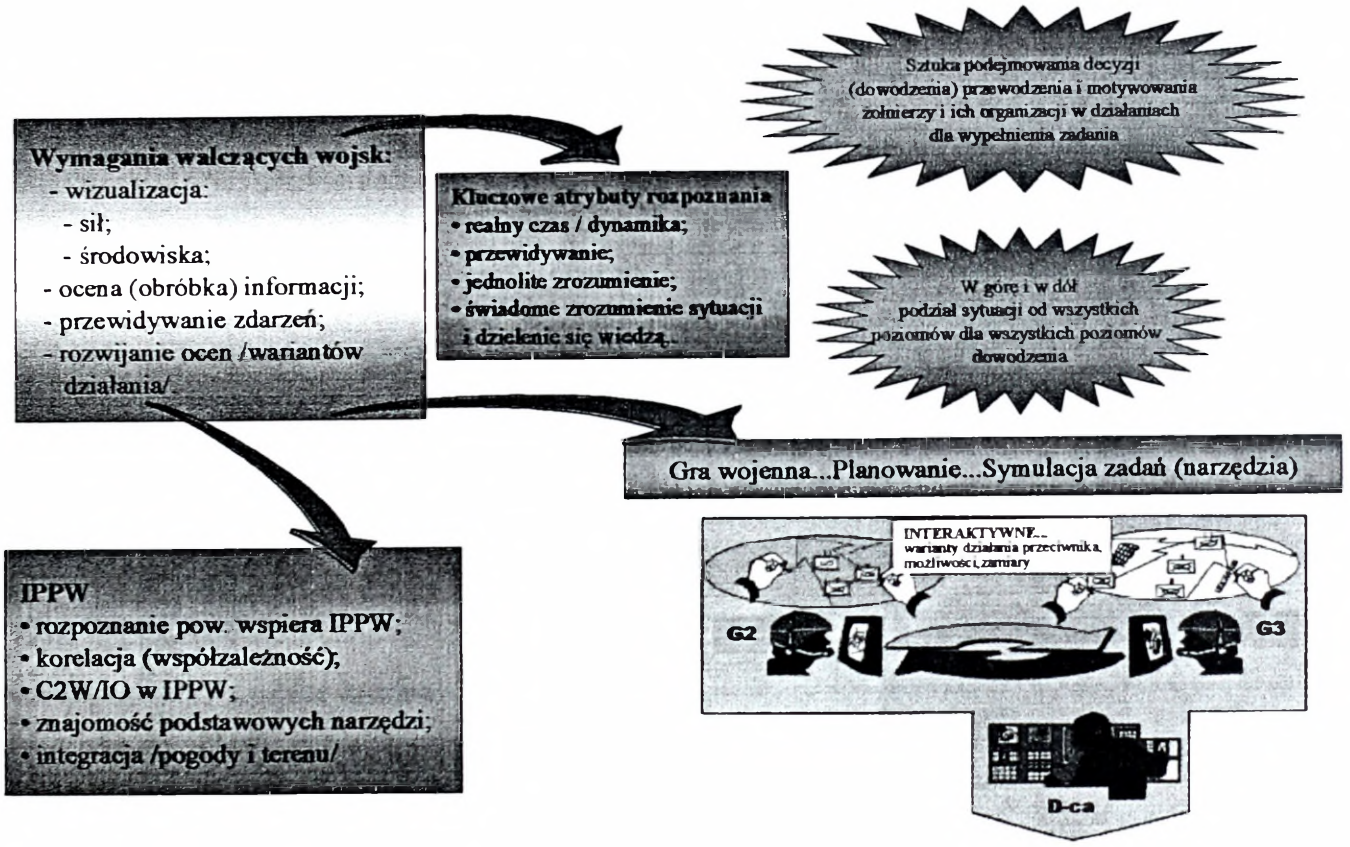
- prowadzenie wielowymiarowych, równoczesnych operacji;
- postrzeganie pola walki w realnym lub zbliżonym do realnego czasie;
- pionowe i poziome zobrazowanie sytuacji w wojskach własnych i przeciwnika;
- precyzyjną lokalizację w czasie i przestrzeni „wariantów" ataku celów wysokoopłacalnych i wysokowartościowych, zarówno środkami niszczącymi jak i bronią nieniszczącą;
- szeroką ochronę wojsk własnych w czasie całej operacji;
- kierowanie operacjami połączonymi i wielonarodowymi, z szeregiem dodatkowych komponentów jak: agencje rządowe i pozarządowe, stowarzyszenia międzynarodowe, organizacje humanitarne itp.

Koniecznym warunkiem prognozy „Operacji XXI w." będzie uzyskanie o niej wiedzy i możliwości zaspokojenia zapotrzebowań informacyjnych. W centrum zainteresowania będą kwalifikacje zarówno dowódców, żołnierzy jak i pracowników cywilnych (operacje humanitarne). Oznacza to, że należy wszystkich w/w przygotować do tworzenia na potrzeby podejmowania decyzji, dokładnych i terminowych komputerowych (wirtualnych) prezentacji sytuacji pola walki. Prezentacje powinny umożliwić zobrazowanie środowiska operacyjnego, terenu i warunków pogodowych, położenia przeciwnika i wojsk własnych, możliwych jego wariantów działania, własnej reakcji itd. Sytuacja taka będzie możliwa dzięki obsługującym źródłowe elementy systemów, zsynchronizowane w całość i wspierające działania bojowe. Wyposażenie stanowić będą wielospektrowe źródła

---

[16] Zob. Programy TRADOC 525-5, *Chief Staff albo Army Vision dla 21st Century.*

danych o wysokich możliwościach technologicznych ukazujących działanie w czasie rzeczywistym. Operacje będą wspierane przez przekazywanie danych metodą „*smart push*"[17] lub „*smart pull*"[18]. Końcowym efektem będzie wsparcie zbrojnych i niezbrojnych ataków wybranych celów i prowadzenie poprzez synchronizację głębokich operacji informacyjnych łączących dowodzenie i kontrolę elektroniczną oraz uderzenia (atak) C2 i obronę C2 (rys.1.5).



Rys. 1.5. Dowodzenie na przyszłym polu walki

Można zatem założyć, że w ewentualnej przyszłej operacji liczyć się będą przede wszystkim „wojska napadu elektronicznego" i „wojska informatyczne". Po irackiej operacji „*Desert Forx*" i po wojnie z Serbią nazywaną operacją „*Allied Force"*, coraz powszechniej słychać głosy nawołujące do zmiany sztuki operacyjnej i taktyki prowadzenia współczesnych operacji wojskowych. Dziś widać już jednoznacznie, że w przyszłości będziemy mieli do czynienia z konfliktami nowego

---

[17] Automatyczne wprowadzanie informacji do baz danych na podstawie zapotrzebowań.
[18] Automatyczny, elektroniczny dostęp do baz danych na podstawie klucza.

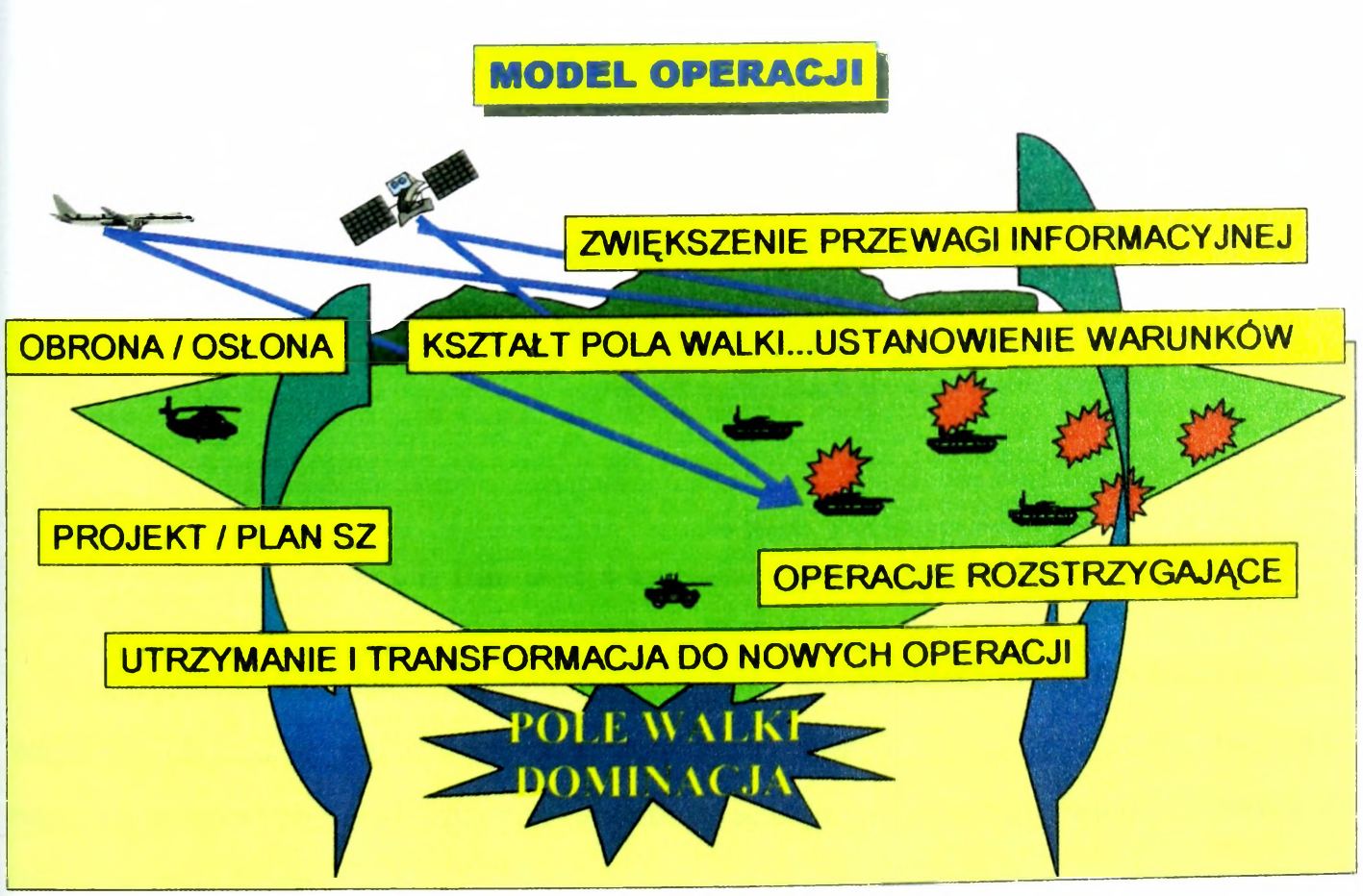
typu, diametralnie różniącymi się od tego, co było dotąd – powiedział, występując przed kamerami amerykańskiej telewizji, „człowiek, który wygrał wojnę w Zatoce", emerytowany generał Norman Schwarzkopf. Analitycy, powołując się na przykłady doświadczeń z walk w Zatoce i wojny czeczeńskiej, są zdania, że wszystkie przyszłe konflikty, nawet lokalne, muszą być prowadzone z jak najszerszym wykorzystaniem środków elektronicznych. Dlatego, według ich założeń, w pierwszym etapie działań, jeszcze przed zniszczeniem infrastruktury obrony powietrznej przeciwnika, niezbędne jest zniszczenie jego potencjału i systemu teleinformatycznego, pokawałkowanie łączności, zakłócenie dowodzenia podczas włamań do sieci komputerowych i celowe fałszowanie danych oraz zagłuszanie transmisji i przekazów informatycznych. Teoria tego typu działań ma być jak najszybciej opracowana. Według amerykańskich wojskowych w trakcie najnowszych ćwiczeń prowadzonych w USA, przedsięwzięcia z zakresu wojny informatycznej przeniesione zostały na wyższy szczebel – z taktycznego na strategiczny. W armii amerykańskiej dojrzała też myśl o powołaniu nowego rodzaju broni. Byłyby to specjalne oddziały walki teleinformatycznej, do zadań których należałoby niszczenie przy pomocy swoistych bomb informatycznych struktur sieci elektronicznych przeciwnika. Według tychże informacji już obecnie szkoli się w tym celu wojskowych radiotechników i informatyków. Dzisiaj wizja przemian technologicznych, wykorzystywanych do celów wojskowych, jeszcze szokuje. Trzeba jednak zdawać sobie sprawę, że nie da się tego uniknąć. Społeczeństwa i wojskowi, podejmując próbę pozostania przy dotychczasowych przyzwyczajeniach i zachowaniach, szybko znajdą się na marginesie. Także najwyżsi dowódcy w Wojsku Polskim prognozują, że walka elektroniczna, będąca obecnie jednym z elementów działań bojowych, w najbliższej przyszłości stanie się samodzielnym środkiem walki, decydującym w znacznym stopniu o zwycięstwie w ewentualnym konflikcie.

W podsumowaniu „Operacje XXI w" powinny być projektowane, wyposażane oraz przygotowywane do spotkania przyszłych operacji i sprostaniu wymogom przyszłego pola walki. Muszą być elastyczne, posiadać układ komponentowy o możliwościach szybkiego rozwinięcia do działania we wspólnych i koalicyjnych

działaniach. Aby do tego doszło, muszą być zintegrowane komplementarnie i wysoce wyspecjalizowane z ogólnym systemem:

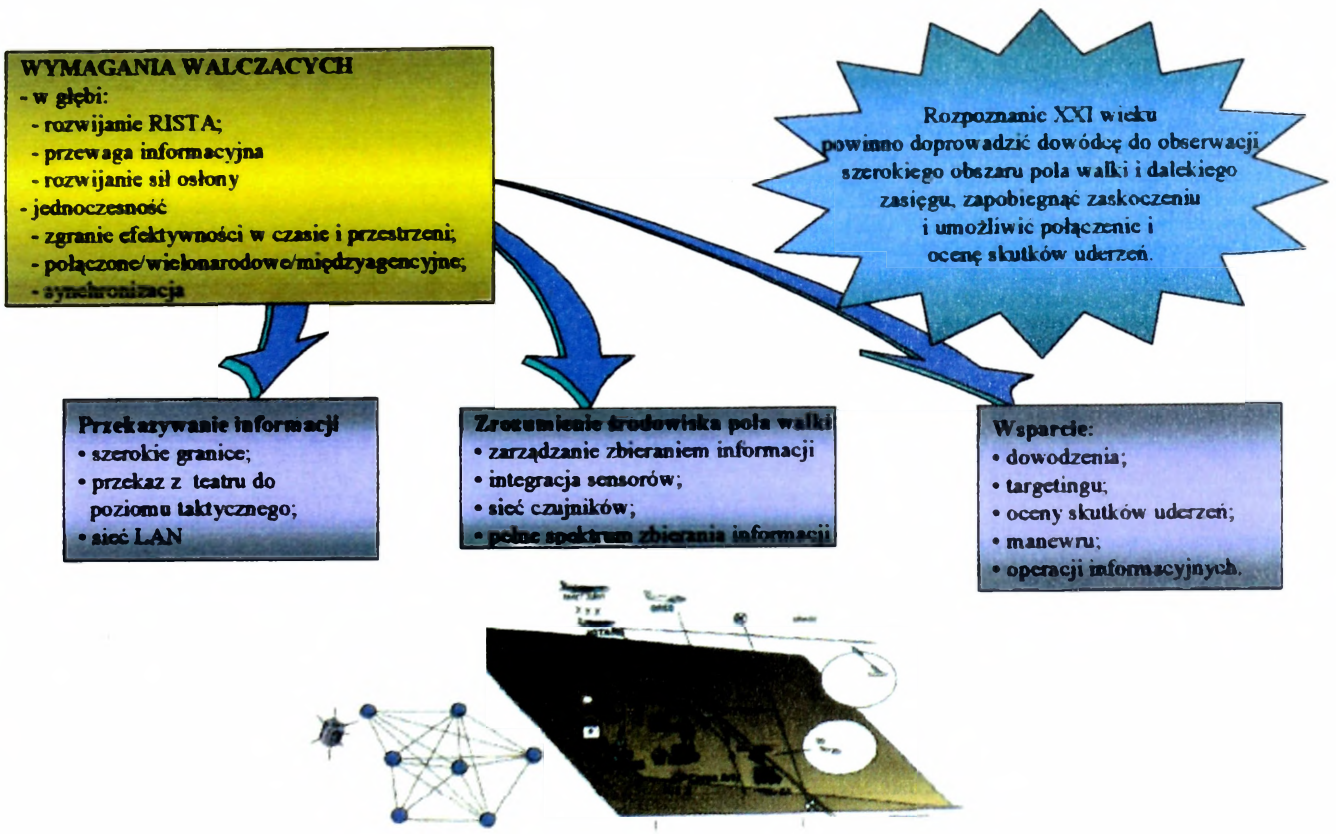
- narodowe agencje (ABW, WSI itd.);
- centra dowodzenia oraz centra dowodzenia rozpoznaniem;
- jednostki operacyjne i taktyczne;
- komponenty aktywne (rozwinięte jednostki bojowe) i rezerwowe;
- połączone wielonarodowe siły zbrojne.

W opinii ekspertów myśli wojskowej (podrozdział 1.1 oraz rys 1.6) rysuje się przyszły model operacji, które powinny być charakteryzowane przez: równoczesność, wielowymiarowość, nielinearność w przestrzeni pola walki i prowadzonych przez jednostki połączone i wielonarodowe w działaniach w rozproszeniu i odizolowaniu, wykorzystujące szybki manewr, ogień i osiąganie decydujących efektów. Mogą one również być charakteryzowane przez znaczący wzrost tempa operacyjnego, zapewnienie ochrony wojskom własnym i umiejętne użycie środków rażenia (niszczących i nieniszczących).



Rys. 1.6. Model operacji

Konkludując, można stwierdzić, że SZ XXI wieku mogą realizować operacje wg następującego wzoru: nie będzie fazowości czy też sekwencyjności walki, jedynie płynne przejście między planowaniem, wykonaniem i odtworzeniem zdolności bojowej. Nie będzie ważne gdzie przyszły konflikt lub operacja wojskowa będzie miała miejsce. SZ będą dysponować takimi możliwościami operacyjnymi w zakresie tworzenia zgrupowania z poszczególnych komponentów, że problem przestrzeni i odległości nie powinien odgrywać znaczącej roli, ważna natomiast będzie dominacja na rozszerzonym polu walki (rys. 1.7).



Rys. 1.7. Dominacja na rozszerzonym polu walki

Logistyka SZ - zabezpieczenia techniczne i materiałowe prowadzonych operacji wojskowych będzie realizowane w szerokim zakresie w oparciu o system mobilnych baz materiałowych, realizujących zadania logistyczne na zamówienie dowódców wieloma sposobami.

Kształt pola walki - będzie określony warunkami prowadzenia operacji. Będzie miał wpływ na głębokość zadań, czas trwania oraz zasady rozmieszczania wojsk sąsiadów i koalicjantów.

Operacje rozstrzygające – działania prowadzone przez siły i środki niezbędne do osiągnięcia sukcesu tj. zniszczenia przeciwnikowi środków walki i zminimalizowania strat własnych. Powinno to być uzyskiwane we współdziałaniu z zapewnieniem przewagi informacyjnej, dużego tempa działań, manewru, oraz precyzyjnego rażenia.

Pozostając w nurcie rozważań nad przyszłymi zmianami pola walki należy określić scenariusz prawdopodobnej interwencji zbrojnej. Nowy konflikt według prognostów wojskowych rozpocznie się od serii wybuchów w atmosferze przypominających grzmoty. Jednak na skutek wybuchów nic nie wyleci w powietrze, nie będzie odłamków ani fali uderzeniowej, tylko po chwili przestaną działać wszystkie urządzenia techniczne i systemy elektroniczne. Takie skutki spowoduje eksplozja bomby elektromagnetycznej (e-bomby). Zdetonowanie e-bomby wyzwoli promieniowanie mikrofalowe. Mikrofale przenikać będą do wnętrza budynków przez przewody wentylacyjne i anteny, paraliżując urządzenia w rejonie wybuchu. Wybuch unieszkodliwi systemy komputerowe w ośrodkach i centrach dowodzenia. Nalot nie niszczy budynków, nie będzie ofiar wśród ludzi. Sztaby i dowództwa jednostek pozbawione łączności będą „ślepe i głuche". Niezdolne do dowodzenia a nawet automatycznego odpalenia zdalnie sterowanych środków rażenia. Zamilknie radio i telewizja, w eter nie popłynie żadna informacja. Eksplodująca bomby grafitowe zniszczą również sieć energetyczną i urządzenia elektryczne[19].

Jednak zanim nastąpi pierwsza eksplozja bomby na terenach przyszłej operacji pojawią się siły specjalne. To one będą poszukiwały i wskazywały rozmieszczenie podziemnych stanowisk dowodzenia wojskami i rządowych ośrodków kierowania. W tym czasie zespoły dywersyjno-rozpoznawcze będą lokalizowały i niszczyły mobilne wyrzutnie rakiet i pocisków samonaprowadzających. Inne grupy specjalne podejmą próby destabilizacji systemu państwowego poprzez organizację działań

---

[19] Zob. Tygodnik „*Wprost*", Nr 1055 (16 lutego 2003).

partyzanckich. Nowym zadaniem sił specjalnych będzie także poszukiwanie i ujęcie przywódców reżimu lub głównych przedstawicieli totalitarnego ustroju w państwie.

Rozwijając wizję przyszłej operacji można założyć, że w pierwszym etapie przyszłych działań na opanowanym przez siły specjalne lotnisku pojawią się samoloty transportowe, z których wytoczy się taktyczna grupa rozpoznawczo-bojowa wyposażona w kołowe transportery opancerzone. Będą wśród nich wozy załogowe, ale zdecydowaną większość stanowić będą inteligentne roboty i specjalistyczne automaty. Najpierw rozpełzną się szybkie, małe, lekkie bezzałogowe pojazdy rozpoznawcze - szperacze. Ich podstawowym zadaniem będzie zlokalizowanie i naniesienia na cyfrowe mapy pozycji bojowych przeciwnika oraz określenie położenia odwodów, rozmieszczonych w pobliżu lotniska a zagrażających dalszym etapom operacji. Jeśli odwody przeciwnika zostaną wprowadzone do działania będą zaatakowane - związane walką przez bezzałogowe wozy bojowe, uzbrojone w automatyczne środki rażenia ogniowego. Dowódcy będą kierować operacją ukryci w zintegrowanych stanowiskach dowodzenia i łączności – pojazdach wyposażonych w automatyczne systemy obrony przed pociskami różnego typu i zakłóceniem elektronicznym.

W drugim etapie operacji na lądowisko przybędzie kolejna, taktyczna grupa uderzeniowa. Z pokładów samolotów transportowych wyjadą większe bezzałogowe pojazdy bojowe, wyposażone we własne „owady" zwiadowcze i latające platformy bojowe oraz środki wsparcia artyleryjskiego z kasetowymi wyrzutniami precyzyjnych pocisków rakietowych. Dzięki zintegrowanym systemom rozpoznania połączone zostaną wyniki rozpoznawcze pierwszej i drugiej fali desantu i ten sposób obszar rozpoznania sił przeciwnika zostanie rozszerzony tworząc dla sztabu operacji, cyfrowy obraz obszaru zainteresowania. Na ekranach operatorów pojawią się kolorowe znaki wskazujące pozycje wojsk własnych (niebieskie) i sił wroga (czerwone). Szybkość i precyzja działania wojsk interwencyjnych zmuszą potencjalnego przeciwnika do zajęcia terenów zapewniających ukrycie i maskowanie, sprzyjających przegrupowaniu sił i odtworzeniu zdolności bojowej. Będą to obszary zurbanizowane, górzyste lub porośnięte gęstą roślinnością. Tam z kolei wojskom interwencyjnym znakomicie

przydadzą się miniaturowe roboty wywiadowcze, także te przeznaczone do walki w zamkniętych pomieszczeniach[20].

Tak według prognoz może wyglądać błyskawiczna operacja interwencyjna (wymuszania pokoju) w XXI wieku bazująca na teorii „wojny sieciocentrycznej". Operacja przeprowadzona zostanie za pomocą zautomatyzowanych, kołowych pojazdów opancerzonych nowego typu, samolotów bezpilotowych i specjalnej formacji piechoty. Wszyscy uczestnicy operacji działać będą w sieciowym systemie przesyłania danych, wymiany informacji taktycznych i dowodzenia, co zapewni przewagę informacyjną i bezpieczeństwo atakującym (nie będzie ofiar spowodowanych ogniem własnej artylerii czy lotnictwa).

Powracając na grunt rzeczywistości należy wspomnieć jeszcze jeden aspekt konfliktów zbrojnych. Na początku lat 90-tych minionego wieku w kontekście rewolucyjnych różnic w technologii wojskowej armii amerykańskiej i jej europejskich partnerów pojawiło się pojęcie - wojny asymetrycznej (*asymmetric warfare*). Określa się ją jako konflikt zbrojny, w ramach, którego państwo i jego siły zbrojne konfrontowane są z przeciwnikiem, którego cele, organizacja (formacje partyzanckie, struktury podziemne) i środki walki oraz metody działania (np. terroryzm) nie mieszczą się w konwencjonalnym pojęciu wojny. Strona walcząca w konflikcie asymetrycznym nie podejmuje bezpośredniej konfrontacji na polu walki z wojskami przeciwnika. Zatem dążąc do zadania agresorowi dotkliwego ciosu posługuje się metodami niekonwencjonalnymi, takimi jak: terroryzm (z wykorzystaniem broni masowego rażenia), działania psychologiczne (deprecjonowanie liderów, obniżanie morale społeczeństwa i żołnierzy przeciwnika oraz propaganda) a także elementy walki informacyjnej (zakłócenia a nawet atak informatyczny).

Tak więc, asymetryczne działania jako skutek różnicy technologicznej walczących stron prowadzą do aktów terrorystycznych, sabotażu, dywersji. Nie ma dnia, aby środki masowego przekazu nie informowały o stratach wśród żołnierzy sił interwencyjnych (np. Irak) spowodowanych działaniami niekonwencjonalnymi. Zatem otwarte pozostaje pytanie czy armia wyposażona w najnowsze osiągnięcia techniki będzie w stanie obronić się przed prymitywnymi narzędziami walki. W tej sytuacji

---

[20] Por. W. Łuczak, *Zrobotyzowana US army XXI wieku*. Raport – wto, 9/2002.

ważnym problemem pozostaje ochrona kontyngentów działających w rejonach niestabilnych. Podejmowane przedsięwzięcia mają na celu zapewnienie bezpieczeństwa wojskom zarówno w bazie (obozie) jaki w czasie realizacji zadań mandatowych. Nie należy zapominać, że tego typu zagrożenie może także wystąpić na terenie kraju – państwa, uczestnika misji wsparcia lub utrzymania pokoju (zamachy terrorystyczne, napady na wartowników, itp.).

1.4. Działania rozpoznawcze w operacjach

Historia dostarcza wiele przykładów świadczących o znaczeniu działań rozpoznawczych. Wybitnym wodzom (dowódcom), sprawnie działające rozpoznanie zawsze pomagało w odniesieniu zwycięstwa. Mimo prymitywnych środków walki dowódcy nie mogli sobie pozwalać na ryzyko przystępowania do bitwy bez minimum podstawowych informacji o przeciwniku. Chiński wódz Sun-tzy domagał się nawet, aby znajomość przeciwnika była równie dobra, jak znajomość sił własnych, bo tylko wtedy można być pewnym zwycięstwa:

„Jeżeli nie znasz nieprzyjaciela, a znasz siebie, możesz przegrać lub wygrać, a jeżeli nie znasz ani nieprzyjaciela, ani siebie, możesz być pewny przegranej".

W polskiej myśli wojskowej także znajdujemy dowody, że od zarania rozwoju rzemiosła wojskowego zwracano dużą uwagę na problem działań rozpoznawczych. Pisze o tym L. Kaltenbergh, przytaczając, wskazówki hetmana Tarnowskiego. Tenże w taki oto sposób upomina ówczesnych wodzów-hetmanów: „Hetman ma też o tym wielką pieczę mieć, aby zawsze o nieprzyjacielu wiedzieć mógł, gdzie jest albo jak daleko..."[21]

Dobrze realizowane działania rozpoznawcze warunkują powodzenie w operacji. Teza ta jest ciągle aktualna, pomimo zmian wprowadzanych w dziedzinie organizacji, uzbrojenia i wyposażenia wojsk rozpoznawczych oraz zasad prowadzenia działań bojowych. Można by zaryzykować stwierdzenie, że prowadzenie działań rozpoznawczych stanowi imperatyw dla każdego pododdziału, niezależnie od sytuacji, rodzaju działań i warunków współczesnego pola walki.

---

[21] L. Kalenbergh, Za wolność naszą i waszą, Warszawa 1968, s. 39

Każdy żołnierz ma ostatecznie obowiązek obserwowania przedpola i przestrzeni powietrznej, zamaskowania swojej pozycji oraz meldowania swoich spostrzeżeń bez specjalnego polecenia. Tę działalność można również uznać za działania rozpoznawcze.

Nietrudno zorientować się, że używam pojęcia „działania rozpoznawcze" a nie „działalność rozpoznawcza". W literaturze przedmiotu pojęcia te używane są niekiedy jako synonimy. Czy tak jest naprawdę?

W każdym języku przyporządkowuje się poszczególnym wyrażeniom sens, czyli znaczenie. Różnie bywa ono określane przez logików. Nie wchodząc w szczegóły i w dyskusje, można powiedzieć, że sens wyrażenia przysługujący mu w jakimś języku jest to sposób rozumienia przypisany temu wyrażeniu przez reguły danego języka. Znaczenie wyrażenia będącego nazwą[22] nazywają niektórzy logicy pojęciem. W poniższych rozważaniach wygodnie będzie używać takiego semiotycznego sposobu określenia pojęcia.

W celu uniknięcia nieporozumień każde wyrażenie winno mieć w języku jedno znaczenie, czyli być jednoznaczne, a każda nazwa - jedno dające się jednoznacznie określić pojęcie. Z różnych względów zdarza się jednak inaczej. Istnieją wyrażenia wieloznaczne (różnoznaczne), czyli tzw. homonimy, oraz wyrażenia częściowo wieloznaczne, czyli o znaczeniach zasadniczo różnych, lecz pod pewnym względem takich samych (pojęcia analogiczne)[23]. Wieloznaczność danego wyrazu rozpatrywanego w oderwaniu, czyli tzw. wieloznaczność potencjalna, nie jest jeszcze wadliwością logiczną, może być bowiem usunięta przez kontekst, w którym ten wyraz aktualnie występuje. Stąd nawet w języku naukowym nie dąży się za wszelką cenę do usunięcia wszystkich wyrazów potencjalnie wieloznacznych. Wywody winno się tam formułować w taki sposób, żeby różne możliwe sensy wyrazów nie odgrywały żadnej roli w ocenie poznawczych wartości całych sformułowań, a zwłaszcza w rozstrzyganiu

---

[22] Nazwa to wyrażenie, które nadaje się na podmiot (lub orzecznik) w zdaniu prostym, inaczej mówiąc, wyrażenie, które pełni funkcję oznaczenia.

[23] Gdy mówi się o pojęciu analogicznym, ma się zazwyczaj na myśli właściwie nie jedno ścisłe pojęcie, ale wiele pojęć, nie tylko jednak związanych wspólną nazwą, lecz także stanowiących relatywną jedność zakresową, która polega na tym, że o wszystkich desygnatach pojęcia analogicznego orzeka się treść w pewnych proporcjach relatywnie taką samą, choć formalnie i zasadniczo różną. Pojęcie analogiczne różni się przeto od pojęcia mętnego, które charakteryzuje się tym, że ma nie dość ostro zdeterminowany zakres (pojęcie niejasne, czyli nieostre) lub niedostatecznie wyznaczoną treść (pojęcie niewyraźne).

prawdziwości wypowiedzi i waloru zawartych w nich argumentacji[24]. Logicznie szkodliwa jest dopiero wieloznaczność aktualna, jak np. ekwiwokacja, czyli użycie tego samego wyrazu w jednym układzie zdań w różnych znaczeniach albo w taki sposób, że nie wiadomo, o jakie spośród potencjalnych znaczeń chodzi (o ile oczywiście poprawność sformułowania tego układu zdań wymaga takiego samego albo jednoznacznie określonego sensu). Aby zapobiec błędom ekwiwokacji i chwiejności znaczenia, należy zdawać sobie sprawę z różnych sensów, jakie mają wyrazy wieloznaczne, a więc znać poszczególne znaczenia, a nawet umieć odróżniać możliwe odcienie tych znaczeń. Taka sytuacja powstaje właśnie w odniesieniu do terminu *„działalność oraz działanie”,* które są niewątpliwie potencjalnie wieloznaczne. Niewiele przeszkadza to w języku potocznym, razi natomiast w ściśle technicznym posługiwaniu się tymi terminami. Niektórzy uważają że wieloznaczność ta istnieje tylko wtedy, gdy bierzemy pod uwagę sposób rozumienia wyrazów *„działalność” oraz „działanie”*. Wydaje się jednak, że wieloznaczność ta ze względu na rozmaitość ujęć potocznych i obiegowych samej teorii działalności i działań występuje nawet w jednym typie myślenia.

W celu pokazania różnych, choćby podobnych, znaczeń wyrazu *działalność* przedstawię kilka jego definicji. Da to jakby przybliżoną definicję tego terminu.

Jako przykład niech posłuży następująca: „Pod pojęciem działalności rozpoznawczej należy rozumieć zespół przedsięwzięć (działań) obejmujący zdobywanie, przetwarzanie i rozpowszechnianie danych o przeciwniku i obszarze działań, niezbędnych do przygotowania i prowadzenia walki lub innego rodzaju działań wojskowych”[25]. Tamże czytamy dalej: celem działalności rozpoznawczej, na każdym poziomie dowodzenia Sił Zbrojnych RP, w czasie pokoju, kryzysu i wojny jest zapewnienie kierownictwu MON, dowódcom i sztabom wiedzy o aktualnym lub potencjalnym zagrożeniu, obszarze działań i warunkach klimatyczno-atmosferycznych.

---

[24] Można nawet wskazać pewne pozytywne wartości potencjalnej wieloznaczności wyrażeń. Pozwala ona zmniejszyć liczbę wyrazów w języku oraz krótko wysłowić myśli i wnioskowania opierające się na podobieństwie i przenośniach.

[25] Rozpoznanie wojskowe. Doktryna połączona. Szt. Gen. 1531/2001 s. 7

W regulaminie działań rozpoznawczych wojsk lądowych *działalność rozpoznawcza* definiowana jest jako „zespół czynności zmierzający do gromadzenia i rozpowszechnienia niezbędnej wiedzy o przeciwniku z wyłączeniem tzw. działań operacyjnych, operacyjno - rozpoznawczych (agenturalnych) w szczególności na własnym terytorium i w stosunku do obywateli własnego kraju."[26]

Działalność w słowniku języka polskiego[27] określana jest: **1.** «zespół czynności, działań, podejmowanych w jakimś celu, zakresie, czynny udział w czym; działanie, praca» Działalność artystyczna, dyplomatyczna, literacka, konspiracyjna, polityczna. Działalność w dziedzinie albo w zakresie czegoś. Przejawiać, podejmować, rozwinąć działalność. **2.** «wpływ, oddziaływanie, rola» Działalność wulkaniczna, rafotwórcza. Działalność Słońca.

Słownik poprawnej polszczyzny[28] konkretyzuje, że *działalność* prowadzimy w zakresie czegoś (nie: czymś) to znaczy działalność rozpoznawcza, literacka, sportowa a nie w rozpoznaniu, literaturze, sporcie. Jednocześnie określa, że *działalność* prowadzimy w celu uzyskania czegoś (nie w kierunku czegoś).

Drugim terminem jest *działanie*, które jest łączone z *działalnością* np. w regulaminie działań rozpoznawczych wojsk lądowych czytamy:"...w opracowaniu nie używa się już określenia *prowadzenia rozpoznania* które zastąpiono pojęciem *działalności rozpoznawczej*"[29].

Natomiast *działanie* wg. słownika języka polskiego to: **1.** rzecz. od działać zakres, zasięg, metody działania. Pobudki działania. Mieć pole do działania. Niszczące działanie morza. **2.** zwykle w *lm* «walki zbrojne, ruchy wojsk» Działania wojenne. Działania zaczepne, odporne. Działania lotnictwa, czołgów. **3.** *mat.* «wyznaczanie liczby a. przedmiotu matematycznego przyporządkowanego w sposób jednoznaczny innym liczbom na podstawie określonego prawa» Działanie arytmetyczne. Działanie na liczbach.

---

[26] Działania rozpoznawcze, Tymczasowa instrukcja, DWLąd. Wewn. 17/2002, Warszawa 2002, s. 7
[27] Słownik Języka Polskiego, PWN, Warszawa1978, tom I,s. 496
[28] Słownik Poprawnej Polszczyzny, PWN, Warszawa 1980 s. 141
[29] Działania rozpoznawcze, Tymczasowa instrukcja, DWLąd. Wewn. 17/2002, Warszawa 2002, s. 5

Słownik poprawnej polszczyzny natomiast konkretyzuje, że działanie to; zakres, metoda działania; działanie czego – na co «oddziaływanie, wpływ czegoś na coś». Np. działanie elementów rozpoznawczych na obiekty.

Na podstawie przedstawionych wyżej definicji nietrudno zauważyć, że posiadają one cechy pod pewnym względem spójne. Stąd wieloznaczność tego wyrazu nie jest zupełna. Nasuwa się pytanie: jaki jest główny sens (znaczenie) wyrazu działalność? Odpowiedź może być następująca: wyrazem działalność posługujemy się, najogólniej mówiąc, dla oznaczenia pewnego rodzaju czynności (działań) podejmowanych w określonym celu.

Na zakończenie można pokusić się o zdefiniowanie „działalności rozpoznawczej".

Działalność rozpoznawcza to zespól czynności (działań) podejmowanych w czasie pokoju, kryzysu i wojny w celu zdobycia (uzyskania) informacji(a nie tylko danych) dotyczących działalności i możliwości prowadzenia walki przez aktualnego lub potencjalnego przeciwnika, obszaru prowadzenia działań oraz warunków klimatycznych i atmosferycznych.

Przyjmując do dalszych rozważań taką definicję, należy stwierdzić, że w tej sytuacji zakres działalności rozpoznawczej (zespół czynności, działań) to nie tylko: zdobywanie, przetwarzanie i rozpowszechnianie danych (informacji) o przeciwniku i obszarze działań, niezbędnych do przygotowania i prowadzenia walki lub innego rodzaju działań ale także *kierowanie tymi działaniami.*

Natomiast *działania rozpoznawcze to: czynności podejmowane w celu uzyskania, w drodze bezpośredniej obserwacji lub wykorzystania innych metod zdobywania, danych (informacji) o działaniach i środkach przeciwnika lub potencjalnym przeciwnika, albo danych meteorologicznych, hydrograficznych lub geograficznych określonego obszaru, itp..*

Przy takim podejściu do problemu, można przyjąć, iż **prowadzenie działań rozpoznawczych to istota działalności rozpoznawczej polegająca na podejmowaniu określonych czynności w celu uzyskania, w drodze bezpośredniej obserwacji lub wykorzystania innych metod wykrywania, danych (informacji) o działaniach i środkach przeciwnika lub potencjalnego przeciwnika, oraz danych**

meteorologicznych, hydrograficznych lub geograficznych określonego obszaru, itp.[30]. Są to najważniejsze ale nie jedyne czynności prowadzenia działań rozpoznawczych, które wraz z ich przygotowaniem tworzą zamknięty, nawzajem się przenikający cykl rozpoznawczy[31].

Nie tylko dzisiaj, ale zawsze - w każdym okresie rozwoju sztuki wojennej - działaniom rozpoznawczym (rozpoznawaniu) przyznawano odpowiednio wysoką rangę. Jest więc pewna nieścisłość w utartym twierdzeniu, że w warunkach współczesnych operacji wzrosła ich rola. Wzrost ten jest procesem ciągłym, wynikającym z rozwoju środków walki, których jakość powoduje, że przed działaniami rozpoznawczymi stawia się coraz wyższe wymagania. Każde niedopatrzenie czy opóźnienie w zdobyciu danych (informacji) staje się groźniejsze w skutkach. Działania rozpoznawcze, podobnie jak walka, pogłębiają swój zasięg, rozszerzają swoje zainteresowania i obligowane są do dostarczania informacji o przeciwniku i terenie szybciej, aby stworzyć dowódcom i sztabom możliwości podejmowania decyzji w zmieniających się nieustannie sytuacjach bojowych. Jeżeli więc teraz operacje nabierają większego rozmachu w wielu środowiskach, to także z większym rozmachem muszą być prowadzone działania rozpoznawcze. Muszą one nie tylko dorównać tempu prowadzonych operacji, ale nawet je wyprzedzać. Nowe środki walki, o nie spotykanej dotychczas sile niszczenia, niezwykle manewrowe, starannie przez przeciwnika maskowane muszą być rozpoznane w sposób dokładny, precyzyjny i szybki.

Wspomnieliśmy już, że w każdym okresie historycznym działania rozpoznawcze były odpowiednio ważne. Zawsze oficerów rozpoznania nurtowały podobne pytania: kto, gdzie, co i kiedy może? Pytania te nie straciły nic ze swej aktualności, ale w miarę rozwoju sposobów prowadzenia operacji ten „ktoś" (przeciwnik) stale zmienia się, staje się jakościowo inny, bardziej ruchliwy, groźniejszy pod względem możliwości bojowych. I chociaż pytania pozostały te same, to odpowiedz na nie musi być odpowiednio szybsza i trafniejsza.

---

[30] Nowak A. Działalność rozpoznawcza na szczeblach taktycznych, AON Warszawa 2002, s. 8.
[31] Zob. Nowak A. Działalność rozpoznawcza na szczeblach taktycznych, AON Warszawa 2002, s. 22.

Działania rozpoznawcze powinny być prowadzone możliwie „najściślej", tzn. że na obszarze działań bojowych, nie powinny występować luki w rozpoznawaniu.

Zgodnie z „koncepcją podziału rozpoznania", działania rozpoznawcze prowadzone są na szczeblu: strategicznym, operacyjnym i taktycznym. Jednak reasumując wyniki dotychczasowych analiz, wszystko wskazuje na to, że w przyszłości podział ten może być następujący: *działania o (globalnym) zasięgu, dalekie działania rozpoznawcze oraz działania rozpoznawcze w rejonach operacji.*

W działaniach rozpoznawczych o globalnym zasięgu, jako nośnik, występować powinien satelitarny system radarowy, który we współdziałaniu z podsystemem rozpoznania elektronicznego powinien zapewnić ciągły dopływ informacji. Musi on ściśle współpracować z innymi systemami - włączenie z systemami europejskich partnerów- i być przykładem skutecznej, militarnej kooperacji na europejskim szczeblu.

W dalekich działaniach rozpoznawczych, pierwszeństwo powinien otrzymać wysoko latający, bezzałogowy, charakteryzujący się długim czasem lotu aparat powietrzny, oraz siły zdolne do prowadzenia działań rozpoznawczych w głębi operacyjnej.

Natomiast uzupełnieniem działań rozpoznawczych o globalnym zasięgu i dalekich działań rozpoznawczych będą działania rozpoznawcze prowadzone w rejonach operacji przez siły i środki poszczególnych jednostek (kontyngentów). Z uwagi na ich specyfikę, możliwości zdobycia aktualnych i bardzo szczegółowych informacji, zdobyte dane wykorzystywane będą nie tylko przez poszczególne kontyngenty lecz stanowić mogą ważne źródła informacji dla komórek rozpoznawczych szczebla państwowego.

Wnioski z analizy literatury wskazują, że działania rozpoznawcze w poszczególnych obszarach powinny być prowadzone w ścisłej współpracy ze sobą i wzajemnie się uzupełniać, a informacje przez nie zdobywane, muszą być wykorzystywane na bieżąco lub też gromadzone w Banku Informacji.

Powyższe wnioski pozwalają na ogólne stwierdzenie, że *działania rozpoznawcze zależą od wielu czynników. Można tu wymienić tak oczywiste czynniki jak charakter wykonywanego zadania bojowego, szczebel dowodzenia, stopień wyszkolenia i zgrania osób funkcyjnych czy ilości czasu posiadanego na przygotowanie działań rozpoznawczych. Czynnikiem często pomijanym jest czynnik*

ludzki w rozumieniu indywidualnego podejścia – dowódcy – jeśli chodzi o prowadzenie działań rozpoznawczych.

Przedstawiony przegląd problemów, dotyczących prowadzenia działań rozpoznawczych, nie stanowi zbioru zamkniętego. Jednak ze względu na wiele poruszanych problemów może nie tylko przyczynić się do ustalenie pewnych pojęć i wyjaśnienia niektórych zagadnień, ile do wzbudzenia nowych wątpliwości i trudności w dziele rozpoznawania. Może to wywołać przynajmniej zainteresowanie *działaniami rozpoznawczymi w operacjach* oraz coraz bardziej prawdopodobne, aktualizującą się problematyką walki informacyjnej.

2. STRUKTURA SYSTEMU ROZPOZNANIA WOJSK LĄDOWYCH

Wyniki analizy literatury przedmiotu wskazują, że system rozpoznania wojsk lądowych został wyodrębniony ze względu na środowisko prowadzenia działań rozpoznawczych. System rozpoznania wojsk lądowych jest częścią składową ogólnego systemu rozpoznania sił zbrojnych, a celowość jego funkcjonowania determinuje, w sposób zasadniczy, powodzenie działań militarnych na lądzie. Skuteczny system rozpoznania wojsk lądowych pozwala w znacznej mierze rekompensować przewagę przeciwnika w podstawowych siłach i środkach walki.

Przez otoczenie systemu należy rozumieć zbiór wszystkich obiektów nie należących do systemu, których właściwości oddziałują na system i zarazem ulegają zmianom pod wpływem działania tego systemu. W tym kontekście w skład otoczenia systemu rozpoznania wojsk lądowych wchodzą systemy rozpoznania powietrznego i marynarki wojennej.

Organizowanie systemu rozpoznania realizuje się z wyprzedzeniem w stosunku do zasadniczych przedsięwzięć przygotowania działań militarnych. W tym zakresie zasadą jest, aby system rozpoznania zdolny był do funkcjonowania jeszcze w czasie wypracowania decyzji i mógł dostarczać niezbędnych aktualnych informacji rozpoznawczych dowódcy oraz szefom rodzajów wojsk do trafnej oceny przeciwnika i środowiska oraz zaplanowania i użycia podległych sił i środków. System ten winien być tak zorganizowany, by w toku działań wojsk lądowych skutecznie nadzorować obszar starcia zbrojnego oraz zdobywać niezbędne informacje do planowania kolejnych operacji.

System rozpoznania wojsk lądowych określonego poziomu dowodzenia jest tworzony na bazie potencjału rozpoznawczego występującego etatowo w strukturze organizacyjnej (wojska rozpoznawcze podporządkowane funkcjonalnie szefowi komórki rozpoznawczej G2, wojska rozpoznawcze

podporządkowane dowódcom rodzajów wojsk), potencjału rozpoznawczego sił wzmocnienia i wsparcia, innych jednostek rozpoznawczych, które mogą być czasowo włączone w skład systemu rozpoznania np. sił OT i rozpoznania specjalnego.

Ze struktury systemu rozpoznania wynika, że składa on się z podsystemów. Podsystem rozpoznania, jak wskazują wyniki analizy literatury to wyróżniona ze względu na określone cechy ściśle określona część systemu rozpoznania charakteryzująca się własnymi powiązaniami organizacyjnymi. Uogólniając, zatem dotychczasowe wnioski można stwierdzić, że w systemie rozpoznania wojsk lądowych wyróżnia się wymienione powyżej podsystemy, a w podsystemach elementy (ugrupowania rozpoznawczego i rozpoznawcze). System rozpoznania bazuje na strukturze organizacyjnej wojsk lądowych, a więc składa się ze specjalistycznych pododdziałów rozpoznawczych rodzajów wojsk, które stanowią elementy ugrupowania bojowego.

2.1. STRUKTURA SYSTEMU ROZPOZNANIA OGÓLNOWOJSKOWEGO

Dokonując analizy struktury rozpoznania wojsk lądowych, należy poznać otoczenie i uwarunkowania, w jakich funkcjonuje przedmiot badań. Prowadzenie analizy wymaga założenia, że funkcjonowanie systemu realizowane jest w strukturach wojsk lądowych a więc system spełnia rolę usługową w stosunku do użytkowników i w związku z tym stanowi określony element systemu wyższego rzędu, bowiem Wojska Lądowe są komponentem systemu obronnego państwa. System ten definiowany jest w literaturze przedmiotu jako skoordynowany wewnętrznie zbiór elementów organizacyjnych, ludzkich i materiałowych wzajemnie powiązanych i działających na rzecz obrony państwa[1]. Struktura systemu rozpoznania ogólnowojskowego

Batalion (pododdział zmechanizowany, czołgów, desantowy, szturmowy) jest podstawowym szczeblem organizacyjnym zdolnym realizować podstawowe zadania rozpoznawcze. W skład potencjału rozpoznawczego

---

[1] *Leksykon Wiedzy Wojskowej*, Warszawa, MON 1979, s. 425.

batalionu wchodzi sekcja rozpoznania (S-2) oraz wydzielone z pododdziałów elementy rozpoznawcze[2]. Za działalność rozpoznawczą ponosi odpowiedzialność kierownik S - 2, który odpowiada za:

- przygotowanie i realizację przedsięwzięć rozpoznawczych i przeciwrozpoznawczych w batalionie;
- szkolenie dowództwa batalionu z zakresu problematyki rozpoznania;
- właściwe wykorzystanie elementów rozpoznawczych batalionu

Komórka rozpoznawcza batalionu (S-2) wchodzi w skład grupy dowodzenia, a jej kierownik podlega bezpośrednio szefowi sztabu batalionu. Do jego podstawowych obowiązków należy:

- przygotowanie systemu rozpoznania batalionu do działania i kierowanie elementami rozpoznania w toku walki;
- zbieranie i analiza danych rozpoznawczych z rejonu rozpoznania batalionu;
- opracowanie meldunków rozpoznawczych i przesyłanie ich zgodnie z procedurami operacyjnymi
- zapewnienie bezpieczeństwa systemowi rozpoznania;
- analiza zdobytych dokumentów bojowych oraz wzorów uzbrojenie i sprzętu wojskowego;
- prowadzenie dokumentacji rozpoznawczej zgodnie z obowiązującymi procedurami.

Możliwości wydzielania elementów rozpoznawczych w batalionie i zasady ich użycia są zależne od struktury organizacyjnej i wyposażenia batalionu (zmechanizowanego, czołgów, powietrznodesantowego, itd.). Pozwalają między innymi na wydzielenie: posterunków obserwacyjnych (PO) lub ruchomych posterunków obserwacyjnych (RPO), posterunków obserwacji

---

[2] Każda kompania posiada przygotowany do prowadzenia działań rozpoznawczych pluton.

przestrzeni powietrznej i skażeń oraz pieszych lub bojowych patroli rozpoznawczych.

Potencjał rozpoznawczy (oddziału) brygady zmechanizowanej (pancernej) umożliwia prowadzenie rozpoznania w jej strefie odpowiedzialności. W strukturze organizacyjnej systemu rozpoznania brygady znajdują się: sekcja rozpoznania (S-2), kompania rozpoznawcza, pododdziały rozpoznawcze artylerii, saperów, obrony przeciwlotniczej oraz rozpoznania skażeń.

W brygadzie komórką sztabową zajmującą się zagadnieniami rozpoznania i przeciwrozpoznania jest sekcja S - 2. Odpowiada ona za: przygotowanie i prowadzenie działań rozpoznawczych, szkolenie dowództw, brygady i pododdziałów z problematyki rozpoznania, przeciwdziałania rozpoznaniu przeciwnika oraz organizacji sił zbrojnych armii innych państw będących obiektem zainteresowania. Funkcjonalnie S-2 planuje w imieniu dowódcy wykorzystanie zgodnie z przeznaczeniem systemu rozpoznawczego brygady.

Kierownik sekcji S-2 podlega bezpośrednio szefowi sztabu brygady i odpowiada za:

- przygotowanie i prowadzenie działań rozpoznawczych;
- przepływ danych rozpoznawczych i informacji o przeciwniku od walczących wojsk do wyższego poziomu dowodzenia;
- zapewnienie bezpieczeństwa elementom rozpoznania oraz systemowi informacyjnemu brygady;
- współpracę z kierownikami sekcji S-2 batalionów, jednostek wzmocnienia i wsparcia, z zespołami artylerii, saperów, naprowadzania lotnictwa;
- terminowe przygotowanie i przesłanie meldunków;
- prowadzenie mapy sytuacyjnej i informowanie dowódcy oraz sztabu o położeniu i działaniu sił przeciwnika;
- przejmowanie jeńców oraz przekazanie ich do sztabu przełożonego;

- przygotowanie stosownych informacji do części głównej rozkazu operacyjnego dowódcy brygady;
- opracowanie stosownie do sytuacji i potrzeb załącznika „*Rozpoznanie*" wraz z koniecznymi uzupełnieniami;
- organizowanie i utrzymanie współdziałania oraz zabezpieczenia działań rozpoznawczych.

W zakresie planowania i kierowania rozpoznaniem do obowiązków S-2 należy:

- opracowanie planu zbierania informacji;
- podział rejonu rozpoznania brygady pomiędzy wykonawców zadań rozpoznawczych;
- zapewnienie bezpieczeństwa własnym elementom rozpoznawczym oraz elementom przełożonego w rejonie odpowiedzialności brygady;
- uzupełnianie dokumentów bojowych (rozkaz operacyjny) o treści wynikające z planowania rozpoznania;

W zakresie oceny przeciwnika i prognozowania zagrożenia kierownik S-2 odpowiada za:

- opracowanie wariantów zagrożenia, wskazywanie celów wysoko opłacalnych i wysokowartościowych;
- pozyskiwanie, gromadzenie i opracowanie informacji o potencjalnym przeciwniku z rozpoznania studyjnego i bezpośredniego;
- zbieranie meldunków o przeciwniku i warunkach terenowych z rozpoznania osobowego i elektronicznego;
- wymianę informacji o przeciwniku ze specjalistami rodzajów wojsk;
- pozyskiwanie danych rozpoznawczych na potrzeby działań ogniowych artylerii i śmigłowców wsparcia, w tym koordynacja ważności celów, przekazywanie współrzędnych obiektów rażenia dla koordynacji wsparcia ogniowego;

- rozpowszechnianie opracowanych informacji rozpoznawczych pozyskanych w toku działań rozpoznawczych;
- przesłuchiwanie zbiegów, rozmowy z ludnością cywilną;
- terminowe przedstawianie dowódcy prawdopodobnych wariantów działania przeciwnika;
- przesyłanie na SD przełożonego osobowych i rzeczowych źródeł informacji (jeńcy, dezerterzy, egzemplarze broni, sprzętu bojowego i wyposażenia).

Przepływ informacji rozpoznawczych w oddziale organizowany jest zasadniczo w oparciu o radiowe środki łączności. Gromadzenie informacji rozpoznawczych w S-2 realizowane jest kanałami formalnymi o strukturze hierarchicznej oraz kanałami funkcjonalnymi. Meldunki rozpoznawcze od patroli rozpoznawczych brygady przyjmowane są przez dowódcę kompanii rozpoznawczej. Okresowo dowódca kompanii przekazuje (ważne natychmiast) zebrane zbiory w postaci meldunku na stanowisko dowodzenia do sekcji kierowania rozpoznaniem. Na stanowisku dowodzenia zbiory informacyjne pozyskiwane od rozpoznania specjalistycznego (rodzajów wojsk) gromadzone są cyklicznie przez oficera sekcji rozpoznania. Ich wykorzystanie następuje w procesie oceny przeciwnika oraz dla zapewnienia bezpieczeństwa elementom rozpoznania osobowego. Następnie zgromadzone zbiory informacyjne z sekcji rozpoznania brygady po ich uprzednim przetworzeniu (uogólnieniu) kierowane są w formie okresowych meldunków (graficznych i pisemnych) rozpoznawczych do wydziału rozpoznawczego związku taktycznego.

Kompania rozpoznawcza brygady przeznaczona jest do zdobywania i dostarczania dowódcy brygady terminowych i wiarygodnych informacji o ugrupowaniu, składzie i działalności sił przeciwnika, przemieszczaniu odwodów oraz zmianach w terenie powstałych na skutek prowadzenia walki w rejonie odpowiedzialności rozpoznawczej brygady. W skład kompanii wchodzą następujące pododdziały:

- grupa dowodzenia, która składa się z dowódcy kompanii, szefa kompanii, technika kompanii, dwóch kierowców (kierowca

WD dowódcy kompanii i kierowca samochodu ciężarowo-terenowego), sanitariusza oraz radiotelegrafisty;

- cztery plutony rozpoznawcze - każdy składa się z drużyn rozpoznawczych, (w pierwszej drużynie jest to jednocześnie dowódca plutonu), na wyposażeniu drużyny znajduje się kołowy transporter rozpoznawczy z taktycznym radarem pola walki; ponadto w każdym plutonie jest grupa motocyklowa dysponująca dwoma motocyklami czterokołowymi (TRX).

Kompania do prowadzenia działań rozpoznawczych organizuje stosowne elementy rozpoznawcze, których podstawę stanowią etatowe plutony i drużyny. W oparciu o organiczne pododdziały organizowane są stosowne do warunków operacyjno-taktycznych: PO, RPO, PR, GW a także zasadzki, napady i wypady.

Działalność rozpoznawcza związku taktycznego (dywizji) opiera się na funkcjonowaniu wydziału rozpoznania i walki elektronicznej (G-2), oraz specjalistycznych jednostek rozpoznawczych, do których należą: batalion rozpoznawczy, kompania radioelektroniczna oraz pododdziały rozpoznawcze rodzajów wojsk.

Całokształtem działalności rozpoznawczej na szczeblu dywizji zajmuje się G-2. W tym względzie odpowiada on za: przygotowanie i prowadzenie rozpoznania, przeciwrozpoznanie i bezpieczeństwo informacji, W ramach kompetencji G-2 pozostaje szkolenie dowództwa dywizji z problematyki rozpoznania i walki elektronicznej, oraz prawidłowe wykorzystanie zgodnie z przeznaczeniem jednostek rozpoznawczych.

G-2 w strukturze organizacyjnej posiada specjalistyczne sekcje realizujące zadania funkcjonalne. Doraźnie w skład G-2 wchodzą przedstawiciele artylerii, wojsk inżynieryjnych, lotnictwa wojsk lądowych i innych specjalności stosownie do potrzeb. Zespół G-2 rozmieszcza się na Centrum Dowodzenia. Poprzez oficerów poszczególnych sekcji współpracuje z innymi komórkami stanowiska dowodzenia. Szef G-2 podlega bezpośrednio szefowi sztabu i ponosi odpowiedzialność za:

- ewidencję wszelkich zmian położenia oraz składu przeciwnika;
- opracowanie meldunków oraz komunikatów rozpoznawczych;
- przygotowanie planu zbierania informacji;
- przygotowanie i przedstawienie dowódcy wariantów oceny zagrożenia;
- uzgodnienie zadań i kierowanie działalnością przeciwrozpoznawczą w dywizji;
- udział w przesłuchiwaniu jeńców, zbiegów i osób cywilnych;
- bezpieczeństwo wojsk;
- ocenę i właściwą dystrybucję zebranych informacji rozpoznawczych;
- przygotowanie i realizację zadań WE;
- przygotowanie oceny warunków terenowych i stanu pogody;
- zorganizowanie współdziałania i zabezpieczenia działań rozpoznawczych.

G-2 w zakresie planowania rozpoznania ponosi odpowiedzialność za:

- opracowanie planu rozpoznania i planu zbierania informacji;
- wybór punktów i rejonów szczególnego zainteresowania w strefie działania ZT;
- podział pasa działania i wyznaczenie linii koordynacji działań rozpoznawczych między rozpoznaniem dywizyjnym i brygadowym;
- opracowanie załącznika Rozpoznanie do rozkazu operacyjnego w części dotyczącej zadań rozpoznania;
- gromadzenie informacji o stanie wojsk rozpoznawczych dywizji;
- udzielanie pomocy podwładnym w zakresie realizacji zadań rozpoznawczych;

- utrzymywanie współpracy z poszczególnymi sekcjami wydziału G - 2;
- utrzymywanie współdziałania w ramach sztabu dywizji i zapewnienie bezpieczeństwa elementom rozpoznawczym;
- prowadzenie dokumentacji rozpoznawczej.

W zakresie planowania rozpoznania powietrznego odpowiada za:

- opracowanie planu zbierania informacji środkami rozpoznania powietrznego (śmigłowce rozpoznawcze, bezzałogowe samoloty rozpoznawcze);
- dokonywanie uzgodnień co do terminów i rubieży (kierunków) działań LWLąd. korpusu (komponentu lądowego) oraz sił powietrznych;
- opracowanie części załącznika „Rozpoznanie" w zakresie zadań rozpoznawczych dla śmigłowców i BSR;
- prowadzenie dokumentacji sprawozdawczej.

W zakresie oceny i prognozowania zagrożenia G-2 ponosi odpowiedzialność za:

- opracowanie wariantów zagrożenia, wskazywanie celów wysokoopłacalnych i wysokowartościowych dla artylerii i śmigłowców wsparcia;
- pozyskiwanie, gromadzenie i opracowanie danych o potencjalnym przeciwniku z rozpoznania studyjnego i bezpośredniego;
- zbieranie meldunków rozpoznawczych o przeciwniku i warunkach terenowych z rozpoznania osobowego i elektronicznego;
- pozyskiwanie informacji o przeciwniku od jednostek OT i układu pozamilitarnego;
- wymianę informacji o przeciwniku z oficerami rodzajów wojsk, jednostkami współdziałającymi i sąsiadami;

- pozyskiwanie danych rozpoznawczych na potrzeby działań ogniowych artylerii i lotnictwa - określenie ważności celów, przekazywanie współrzędnych obiektów rażenia do ośrodka koordynacji wsparcia ogniowego;
- rozpowszechnianie przetworzonych danych rozpoznawczych i materiałów pozyskanych w toku działań rozpoznawczych;
- udział w przesłuchiwaniu jeńców, zbiegów, uchodźców oraz ludności miejscowej;
- stałą aktualizację mapy informacyjnej, terminowe przedstawianie dowódcy prawdopodobnych wariantów działania przeciwnika;
- dostarczanie na SD przełożonego osobowych i rzeczowych źródeł informacji (jeńcy, dezerterzy, egzemplarze broni, sprzętu bojowego
i wyposażenia);
- koordynację przedsięwzięć sztabu w zakresie oceny i wartościowania zagrożenia.

W zakresie WE komórka G-2 realizuje następujące zadania:

- ocena sytuacji (zagrożenia) RE;
- planowanie i kierowanie rozpoznaniem RE;
- planowanie i kierowanie zakłóceniami RE;
- dystrybucja danych z rozpoznania RE;
- koordynacja przedsięwzięć z zakresu obrony RE.

W obszarze problematyki bezpieczeństwa wojsk G-2 odpowiada za:

- przygotowanie planu i eliminację działań rozpoznawczych przeciwnika;
- zapobieganie działaniom destabilizującym sytuację w tyłowej strefie dywizji;
- bezpieczeństwo i ochronę tajemnicy w sztabie dywizji;
- udział w przesłuchaniu jeńców, zbiegów, dezerterów i ludności miejscowej;

- maskowanie i sposoby ochrony najważniejszych elementów systemu rozpoznania ZT;
- przygotowanie propozycji bezpieczeństwa operacji;
- opracowanie stosownych dokumentów dowodzenia.

Batalion rozpoznawczy jest jednostką przeznaczoną do prowadzenia działań rozpoznawczych na szczeblu związku taktycznego. Jego zadanie polega na dostarczaniu dowódcy dywizji wiarygodnych informacji niezbędnych do planowania walki, podjęcia decyzji, celowego wykorzystania środków rażenia i kierowania manewrem wojsk. Batalion rozpoznawczy ze względu na różnorodność posiadanych środków można wykorzystywać w ugrupowaniu wojsk własnych jak i w ugrupowaniu przeciwnika. Podstawowym kryterium mającym wpływ na sposób wykorzystania potencjału rozpoznawczego batalionu jest:

- rodzaj działań operacyjnych (taktycznych);
- miejsce i rola związku taktycznego w ugrupowaniu operacyjnym;
- możliwości prowadzenia rozpoznania (warunki środowiska).

Batalion rozpoznawczy związku taktycznego w zmodernizowanej strukturze składa się z dowództwa, sztabu, grupy analizy danych i trzech kompanii rozpoznawczych oraz kompanii radioelektronicznej. Pierwsza kompania wyposażona jest w kołowe transportery rozpoznawcze, druga, o składzie mieszanym, posiada bojowe wozy rozpoznawcze oraz kołowe transportery rozpoznawcze ze stacjami radiolokacyjnymi, trzecia, lekka kompania o mieszanym składzie, wyposażona jest w samochody osobowo-terenowe i motocykle. W składzie batalionu znajdują się pododdziały logistyczne – plutony: zaopatrzenia, remontowy i medyczny. Na potrzeby zabezpieczenia łączności i dowodzenia w strukturze batalionu jest także pluton łączności.

Kompania radioelektroniczna przeznaczona jest do rozpoznawania i obezwładniania zakłóceniami RE, ultrakrótkofalowej łączności radiowej (naziemnej i lotniczej) przeciwnika. Kompania jest organicznym elementem ugrupowania bojowego dywizji. Struktura organizacyjna kompanii jest następująca:

- dowództwo kompanii oraz grupa kierowania (GK);
- pluton rozpoznania radiowego UKF;
- pluton namierzania radiowego UKF;
- pluton zakłóceń radiowych UKF (lądowych i lotniczych);
- drużyna logistyczna.

Jej możliwości rozpoznawczo-bojowe wynikają głównie z ilości posiadanego sprzętu, jego parametrów taktyczno-technicznych, przyjętego sposobu wykonania zadań oraz stopnia wyszkolenia i przygotowania stanu osobowego do działań na polu walki. Możliwości wskazują na zdolność w zakresie prowadzenia rozpoznania i obezwładniania radioelektronicznego. Do prowadzenia zakłóceń relacji radiowych UKF, dywizja może otrzymać nadajniki zakłócające jednorazowego użytku.

Przepływ informacji rozpoznawczych realizowany jest za pomocą radiowych i przewodowych środków łączności oraz z wykorzystaniem komputerowego wspomagania pracy sztabowej.

Informacje napływające od elementów rozpoznawczych batalionu przesyłano jako zbiorczy meldunek do wydziału rozpoznawczego. W G-2 dane o przeciwniku przenoszone są na mapę informacyjną, natomiast położenie elementów rozpoznawczych na plan rozpoznania.

Zbiory informacyjne uzyskane przez elementy rozpoznawcze rodzajów wojsk gromadzone są w G-2, poprzez skierowanie oficera łącznikowego do odpowiednich komórek funkcjonalnych stanowiska dowodzenia związku taktycznego.

Eskadra rozpoznania powietrznego przekazuje dane z rozpoznania powietrznego za pośrednictwem oficera lotnictwa włączonego w strukturę G-2 jako oficera łącznikowego dowódcy eskadry. Dodatkowo w całym systemie rozpoznania prowadzono bezpośredni odbiór meldunków z pokładu śmigłowca.

Pozyskane przez podsystem rozpoznania elektronicznego zbiory informacyjne pozyskiwane są bezpośrednio, z wykorzystaniem łączności radiowej do G-2.

Gromadzenie informacji rozpoznawczych pozyskiwanych od jeńców, zbiegów i miejscowej ludności pozostawiono w zakresie kompetencji żandarmerii wojskowej oraz innych zainteresowanych przedstawicieli komórek sztabu, w tym oczywiście także rozpoznania.

Połączenia funkcjonalne – bezpośrednie w sieci rozpoznania realizowane są tylko w przypadku zdobycia przez elementy rozpoznawcze wyjątkowo istotnych informacji. Stąd też częstym rozwiązaniem, w praktycznej działalności szkoleniowej, dla skrócenia obiegu informacji jest włączanie w struktury G-2 przedstawicieli sztabu batalionu, natomiast w skład sekcji rozpoznania brygady dowódcy kompanii[3].

2.1.1. Efekty poznawcze

W okresie ostatnich lat w związku ze zmianą uwarunkowań polityczno-wojskowych siły zbrojne uległy transformacji. Zmiany organizacyjne objęły również organa i jednostki rozpoznawcze szczebla taktycznego, a w tym szczególnie bataliony rozpoznawcze związków taktycznych i kompanie rozpoznawcze brygad zmechanizowanych i pancernych (szczegółowa struktura została przedstawiona w załącznikach). Diagnoza organizacyjna nowych struktur oraz wnioski wynikające z obserwacji procesu szkolenia i ćwiczeń z wojskami pozwalają na szereg uogólnień.

Po pierwsze batalion rozpoznawczy w zmodyfikowanej strukturze pozbawiony został kompanii specjalnej, co ograniczyło możliwości prowadzenia rozpoznania przez związek taktyczny. Powstałą „lukę informacyjną" wypełnia się trzecią kompanią rozpoznawczą, której mieszany skład (samochody osobowo-terenowe i motocykle) umożliwia prowadzenie działań rozpoznawczych w obszarze zajętym przez przeciwnika. Jednak jak wskazują wnioski z ćwiczeń, czas dotarcia elementów rozpoznawczych do wyznaczonych rejonów jest dłuższy niż w przypadku przerzutu grup specjalnych śmigłowcem, a zabezpieczenie logistyczne i bojowe elementów rozpoznawczych trudniejsze.

---

[3] Przedstawione rozwiązania budzą szereg zastrzeżeń zarówno w kwestii teoretycznej jak i praktycznej.

Wprowadzenie na szczeble taktyczne motocykli znacznie zwiększyło możliwości przestrzenne podsystemu zdobywania danych, brak jest jednak odpowiednich środków łączności, umożliwiających swobodę działania patrolom motocyklowym. Wnioski z praktyki szkoleniowej wskazują, że powyższy problem rozwiązywany jest poprzez tworzenie mieszanych patroli rozpoznawczych (transportery rozpoznawcze i motocykle).

Po drugie przeniesienie rozpoznania specjalnego aż na szczebel strategiczny praktycznie uniemożliwia wzmocnienie elementami rozpoznania specjalnego związku taktycznego realizującego priorytetowe zadania bojowe.

Po trzecie - wprowadzenie w struktury jednostek rozpoznania pododdziałów rozpoznania skażeń stworzyło nowy problem opracowywania napływających specjalistycznych danych o sytuacji skażeń chemicznych i promieniotwórczych oraz zagrożeń powstałych w wyniku uwolnienia toksycznych środków przemysłowych. Aktualnie przeniesiono siły i środki rozpoznania skażeń natomiast oficerowie – specjaliści, pracujący na zbiorach informacyjnych pozyskiwanych przez specjalistyczne elementy rozpoznawcze, pozostali w strukturach wojsk obrony przeciwchemicznej.

Przeprowadzone zmiany strukturalne w elementach rozpoznawczych oddziałów i związków taktycznych nie wpłynęły na jakość danych pozyskiwanych na potrzeby rażenia ogniowego, dalej odczuwalne są braki wyposażenia technicznego umożliwiającego z pożądaną dokładnością określanie położenia celów.

Nie uległ również zmianie system dowodzenia i kierowania elementami rozpoznawczymi. Brak jest samodzielności dowódców w zakresie podejmowanych decyzji do prowadzenia rozpoznania, szczególnie na szczeblu kompania i batalion rozpoznawczy.

Zmiany strukturalne nie spowodowały jakościowej poprawy posiadanych środków rozpoznawczych. Mała ilość środków radiolokacyjnych i optoelektronicznych redukuje zasięg i skuteczność rozpoznania w warunkach ograniczonej widoczności.

Z powyższych faktów wynika, że funkcjonowanie systemu rozpoznania nie jest zadowalające. Potwierdzają to również wyniki badań. W związku z tym celowa jest ponowna analiza strukturalna komórek sztabowych, oddziałów i pododdziałów rozpoznawczych w celu poszukiwania rozwiązań zwiększających efektywność działania badanego obiektu.

2.2. STRUKTURA SYSTEMU ROZPOZNANIA SPECJALISTYCZNEGO

Przyjmowane dotychczas podziały rodzajów rozpoznania nie są często zbyt precyzyjne, gdyż trudno się dopatrzyć określonego kryterium tych podziałów. Nie uwzględnia się przy tym wszystkich cech szczególnych dla odmiennych rodzajów rozpoznania. Pewnym rozwiązaniem tego problemu jest podział przyjmujący za kryterium użyte do zdobywania informacji siły i środki oraz sposób działania elementów rozpoznawczych. W tym aspekcie wyróżniamy rozpoznanie bezpośrednie (elementy rozpoznawcze będące w kontakcie z przeciwnikiem np.: wzrokowym lub bojowym) i rozpoznanie pośrednie (elementy rozpoznawcze wykorzystujące źródła informacji przeciwnika – np.; jego korespondencję radiową). Innym kryterium podziału rozpoznania jest przeznaczenie pozyskiwanych informacji rozpoznawczych. W tym aspekcie wyróżnia się rozpoznanie na potrzeby sytuacji (tzw. ogólnowojskowe) i rozpoznanie specjalistyczne (rodzajów wojsk). Należy jednak nadmienić, że w wielu sytuacjach taktyczno-operacyjnych organizuje się zintegrowane elementy rozpoznawcze. Idea włączania w patrole rozpoznawcze elementów rozpoznania specjalistycznego (np.: inżynieryjnego lub skażeń) nie jest nowa i przez wiele lat funkcjonowała w wojskach lądowych. Jednak coraz większa specjalizacja zadań i rozwój techniki, a także nowe zjawiska w procesie dowodzenia (np.: targeting, bezpośrednie wsparcie powietrzne, działania aeromobilne) wymusiły inną organizację systemu rozpoznania. Każdy zdobywa informacje ze swoich źródeł i każdy jest zobowiązany udostępnić ją zainteresowanym użytkownikom. Stąd też zmiana w nazwie dokumentów planistycznych taktycznego systemu rozpoznania – wprowadzono plan

zdobywania informacji. Bowiem informacje się zdobywa, a nie tylko oczekuje na ich napływ i wyniki bezpośrednich działań rozpoznawczych. W związku z powyższym rozpoznanie sytuacji (ogólnowojskowe) umożliwia określenie potencjalnego ugrupowania bojowego przeciwnika, natomiast rozpoznanie specjalistyczne (rodzajów wojsk) określa położenie i działanie jego sił i środków (np.; rozmieszczenie zapór inżynieryjnych przeciwnika, stanowisk ogniowych artylerii, systemu dowodzenia). Warto jeszcze nadmienić, że w nowych strukturach sztabów i stanowisk dowodzenia powstały zintegrowane zespoły rozpoznania. Bowiem zamiarem organizacyjnym jest budowa jednego spójnego systemu informacyjnego (zintegrowanego), zdolnego gromadzić, przetwarzać i rozpowszechniać informacje rozpoznawcze na potrzeby określonych użytkowników (manewr lądowy i powietrzny, rażenie ogniowe, obezwładnianie elektroniczne).

2.2.1. System rozpoznania artyleryjskiego

Podstawowym źródłem danych (o wymaganym stopniu dokładności) o przeciwniku pod kątem zabezpieczenia działalności ogniowej artylerii związku taktycznego jest rozpoznanie artyleryjskie. Wykonuje ono zadania na potrzeby własnych pododdziałów, a jednocześnie jest ważnym źródłem informacji dla współpracujących z nim innych rodzajów rozpoznania. Rozpoznanie artyleryjskie jest działaniem bojowym, którego celem jest zdobywanie danych o położeniu obiektów w ugrupowaniu przeciwnika oraz o terenie i warunkach meteorologicznych. Jest zatem procesem, w którym następuje zdobywanie i opracowywanie informacji o potencjalnym lub rzeczywistym przeciwniku i terenie oraz stanie atmosfery, niezbędnym do właściwego użycia wojsk rakietowych i artylerii w działaniach taktycznych i operacyjnych. Rozpoznanie artyleryjskie sprzęgnięte z systemem dowodzenia i kierowania ogniem powinno, zatem zapewnić artylerii pełną skuteczność rażenia sił i obiektów przeciwnika. Prowadzi się je z wykorzystaniem technicznych środków rozpoznania radiolokacyjnego i dźwiękowego oraz za pomocą przyrządów optyczno-mierniczych rozpoznania wzrokowego.

W zależności od stosowanych środków rozpoznawczych, rozpoznanie na rzecz ognia artylerii dzieli się na: wzrokowe, dźwiękowe (akustyczne), radiolokacyjne i powietrzne.

Rozpoznanie wzrokowe prowadzą grupy (pododdziały) rozpoznawcze jednostek artylerii (wysunięci obserwatorzy), z punktów obserwacyjnych (dowódczo-obserwacyjnych) za pomocą przyrządów optycznych i optoelektronicznych, a ponadto obserwatorzy artyleryjscy z pokładów śmigłowców rozpoznawczych[4]. Analiza możliwości rozpoznania wzrokowego pozwala na stwierdzenie, że ogień skuteczny z wykorzystaniem danych pochodzących ze źródła rozpoznania wzrokowego możliwy jest na odległość 5-7 km. Natomiast korzystając z punktów obserwacyjnych rozmieszczonych na wyniosłościach terenowych w sprzyjających warunkach atmosferycznych i dobrej widzialności obiektów nawet do 10 i więcej kilometrów. Rozpoznanie wzrokowe[5] pozwala na pozyskanie danych o 50-60 obiektach punktowych w ciągu jednej godziny z jednego źródła informacji (punktu obserwacyjnego), zaś wykorzystując dwuboczną obserwację 10-12 obiektów, w zależności od stosowanych technicznych urządzeń obserwacyjnych. W warunkach ograniczonej widoczności (mgła, dym, deszcz, śnieg, noc) możliwości źródeł rozpoznania bazujących na wzrokowym pozyskiwaniu danych mogą wynosić 3-5 km.

Rozpoznanie dźwiękowe (akustyczne) umożliwia wyznaczenie współrzędnych obiektów będących źródłem fal dźwiękowych. Przeznaczone jest do rozpoznania strzelających środków artyleryjskich i na tej podstawie określenia położenia pododdziałów artylerii przeciwnika. Rozpoznanie dźwiękowe umożliwia również poprzez określenie położenia miejsc wybuchów pocisków własnej artylerii korygowanie jej ognia.

---

[4] Na korzyść artylerii może być prowadzone rozpoznanie wzrokowe przez siły i środki rozpoznania patrolowego pod warunkiem uzyskania wymaganego stopnia dokładności określania współrzędnych obiektów.

[5] Praktyczne ćwiczenia potwierdzają możliwości rozpoznania wzrokowego por. M. Nowsza, *System rozpoznania – część systemu ognia artylerii*, Przegląd Wojsk Lądowych 1999, nr 1(475), s. 53-57.

Rozpoznanie radiolokacyjne prowadzą stacje radiolokacyjne wykrywania naziemnych i nawodnych celów ruchomych oraz określają współrzędne wybuchów pocisków własnej artylerii. Analiza możliwości stacji SNAR-10 jako źródła rozpoznania na lądzie wskazuje, że może ona prowadzić rozpoznanie we wskazanym sektorze na głębokość – obiektu pojedynczego do 18 km, wyznaczanie współrzędnych wybuchów artylerii powyżej 120 mm wynoszą 4-10 km. Na wodzie natomiast z powodu innego środowiska i warunków obserwacji jej możliwości wzrastają i wynoszą do obiektu nawodnego 25-30 km, a w zakresie określania współrzędnych wybuchów pocisków własnej artylerii do 14 km.

Rozpoznanie powietrzne pozyskuje dane o położeniu obiektów w odległości 8-20 kilometrów z wykorzystaniem przyrządów obserwacyjnych (3-8 km bez środków optycznych). Korytarz lotu śmigłowca wynosi 10-15 kilometrów. Ogólny czas określenia współrzędnych od wykrycia celu (1-3 minut) waha się do 5 do 10 minut. Przyjmując powyższe kalkulacje, możliwości rozpoznania śmigłowca sprowadzają się do określenia (wcięcia celu) położenia 3 celów w ciągu godziny. Stąd wynika wniosek, że śmigłowiec nie może być wykorzystywany jako efektywny środek rozpoznania artyleryjskiego w ograniczonym zakresie. Niemniej jednak jest on cennym źródłem danych o ogólnym działaniu przeciwnika i może być punktem korygowania ognia artylerii. Rozpoznanie powietrzne prowadzone przez załogi śmigłowców jest realizowane jako rozpoznanie wzrokowe (obserwacja – nadzorowanie sytuacji na polu walki) lub fotograficzne z wykorzystaniem aparatów do wykonywania zdjęć pionowych i skośnych. Taktyka działania śmigłowca zakłada[6], ze wykonuje on lot koszący z okresowym, gwałtownym wznoszeniem do wysokości 100-300 m. Ponadto należy pamiętać, że fotografowanie lotnicze w zasadzie nie może być wykonywane w rejonach silnej obrony przeciwlotniczej ze względu na parametry techniczne śmigłowca.

---

[6] Lot na większych wysokościach nie może być wykonywany po prostej, a czas jego trwania powinien być krótszy niż czas otwarcia ognia przez środki obrony przeciwlotniczej przeciwnika.

Prowadzone ćwiczenia dowódczo-sztabowe wskazują, że w przypadku niewystarczających możliwości pododdziałów rozpoznawczych artylerii przesyłane jest, do wydziału rozpoznawczego związku taktycznego, zapotrzebowanie na wiadomości. Dotyczy ono danych o określonych obiektach przewidywanych do rażenia ogniowego lub zakłócania, a znajdujących się poza zasięgiem własnych środków rozpoznania. Jednak należy pamiętać, że dane z rozpoznania ogólnowojskowego, radiotechnicznego i lotniczego przy obecnym poziomie techniki rozpoznawania mogą być wykorzystane przez jednostki artylerii jedynie do planowania użycia wsparcia ogniowego w walce związku taktycznego. Ze względu na ich małą dokładność (rozpoznanie ogólnowojskowe) lub zbyt długi czas przetwarzania (rozpoznanie lotnicze) mogą stanowić tylko podstawę do wykonania uderzeń ogniem artylerii do celów stacjonarnych i do dużych obiektów powierzchniowych.

Zasadniczym zadaniem sił i środków rozpoznania na rzecz wsparcia ogniowego wojsk w walce jest pozyskiwanie, odpowiednio dokładnych, terminowych i wiarygodnych danych o obiektach przeciwnika, umożliwiających skuteczne rażenie. W tym celu na wszystkich poziomach dowodzenia organizuje się stosownie do charakteru działań taktycznych właściwy system rozpoznania artyleryjskiego. Umożliwia on realizację zadań w zakresie zdobywania, opracowania i przekazywania danych o obiektach przeciwnika.

Organicznym pododdziałem wsparcia ogniowego batalionu (nie dotyczy bcz) jest kompania wsparcia. Dysponuje ona dwoma plutonami moździerzy, drużyną dowodzenia i sekcją wysuniętych obserwatorów. Sekcja wysuniętych obserwatorów wyposażone jest w przyrządy optyczno-miernicze pozwalające na prowadzenie rozpoznania wzrokowego i wykrycie celów w zasięgu widoczności. Posiadane środki łączności (radiowe i przewodowe) umożliwiają przekazywanie informacji rozpoznawczych oraz kierowanie ogniem.

W brygadzie etatowym pododdziałem realizującym wsparcie ogniowe jest dywizjon artylerii samobieżnej. W swojej strukturze posiada baterię dowodzenia składająca się z trzech plutonów wysuniętych obserwatorów. Każdy pluton umożliwia organizację rozpoznania artyleryjskiego na potrzeby batalionu.

Stąd w przypadku, gdy w brygadzie występują cztery bataliony to w baterii dowodzenia powinny być także cztery plutony wysuniętych obserwatorów. Pluton składa się z trzech sekcji wysuniętych obserwatorów (SWO). Zadaniem plutonu jest prowadzenie rozpoznania wzrokowego przeciwnika i obsługiwania strzelania[7]. Sekcje są zasadniczym źródłem informacji o wykrytych obiektach rażenia ogniowego. Wykorzystanie elementów rozpoznania artyleryjskiego realizowane jest poprzez skierowanie plutonów wysuniętych obserwatorów do batalionów, a podległe im sekcje wysuniętych obserwatorów (SWO) przydzielane zostają do poszczególnych kompanii. Zasadniczo w kompaniach czołgów dowódcy SWO pełnią funkcję koordynatorów wsparcia ogniowego, natomiast w kompaniach zmechanizowanych współdziałają z dowódcami plutonów moździerzy, którzy są koordynatorami ognia w batalionie. Rola kompanijnych koordynatorów wsparcia ogniowego sprowadza się do planowania i nadzorowania wykonywania zadań przez artylerię polową według potrzeb stosownych dowódców pododdziałów[8].

Rozpoznanie wzrokowe prowadzone przez SWO odbywa się w określonym sektorze rozpoznania. Sektor ten może mieć różną szerokość i zależeć od realizowanego zadania przez kompanię i warunków środowiska walki, w tym szczególnie ukształtowania terenu. Zasięg rozpoznania uzależniony jest od rzeźby i pokrycia terenu oraz warunków atmosferycznych. Wywiera to istotny wpływ na głębokość rozpoznania. Ponieważ szerokość kompanijnego punktu oporu nie przekracza dwóch km, jeden PO może prowadzić rozpoznanie przed frontem działania kompanii zmechanizowanej[9]. Należy jednak zaznaczyć, że biorąc pod uwagę szerokość działań bojowych brygady w obronie (15-20 km) i wykorzystanie w pierwszym rzucie dwóch batalionów (sześć kompanii, czyli sześć SWO), rozpoznaniem artyleryjskim pokryte będzie około 60-80 % ogólnej

---

[7] Pluton wysuniętych obserwatorów do prowadzenia rozpoznania posiada: dalmierz laserowy (LPR-1, DAK-2)
i stereoskopowy, kątomierz-busolę PAB-2A, lornetkę peryskopową AST, radiostacje przenośne UKF oraz lornetki 7x45.

[8] Zob. szerzej K Czajka., P. Malinowski, Rozpoznanie na rzecz wsparcia ogniowego wojsk lądowych. Warszawa 2002.

[9] W złożonych warunkach taktycznych i terenowych (teren lesisto-jeziorny i zurbanizowany) rozpoznanie może być prowadzone jedynie w punkcie ciężkości jej działań.

strefy odpowiedzialności ogniowej[10]. Podobne problemy występują w przypadku prowadzenie działań opóźniających. Natomiast w natarciu rozpoznaniem wzrokowym można pokryć cały pas natarcia oddziału. Bowiem pas natarcia batalionu i ilość wykorzystywanych do walki pododdziałów zapewniają prowadzenie rozpoznania artyleryjskiego[11] w toku prowadzenia działań zaczepnych.

W dywizjonie artylerii za całokształt działalności rozpoznawczej odpowiada oficer rozpoznania. Do jego zasadniczych obowiązków należy między innymi:

- określenie kolejności i sposobów zbierania danych z rozpoznania (od jednostek rozpoznawczych i podległych sztabów),
- uzgodnienie z oficerem S-2 brygady sposobu wymiany danych o przeciwniku,
- opracowanie i rozpowszechnianie zdobytych danych z rozpoznania artyleryjskiego.

W pułku artylerii podległym dowódcy związku taktycznego odpowiedzialnym za gromadzenie i przetwarzanie danych napływających ze źródeł rozpoznania artyleryjskiego jest kierownik sekcji rozpoznawczej pułku. Elementem strukturalnym sieci rozpoznawczej pułku jest pluton rozpoznania dźwiękowego w pułku artylerii oraz bateria rozpoznania dźwiękowego w samodzielnym dywizjonie rozpoznania artyleryjskiego. W wyposażeniu tych pododdziałów znajdują się dwa typy sprzętu, zestaw PZK-19W w plutonie rozpoznania dźwiękowego oraz w baterii rozpoznania dźwiękowego zestaw AZK-5.

W skład zestawu PZK wchodzi: punkt centrali CP1 punkt pracy dowódcy, CP2, które umieszczono na specjalnych nadwoziach dwóch samochodów GAZ-66. Trzy podstawy pomiarowe, których placówki dźwiękowe rozmieszczono na nadwoziach samochodów UAZ 452 lub UAZ 452-T2.

---

[10] Por. K Czajka., P Malinowski., *Rozpoznanie...*, wyd. cyt.
[11] Por. K Czajka., P Malinowski., *Rozpoznanie* ...wyd. cyt.

Natomiast AZK-5, jest ilościowo mniejszy. Trzy punkty pomiarowe są zamontowane na nadwoziach samochodów ZIŁ 131. Centralę zestawu oraz łączność rozmieszczono na nadwoziach dwóch kolejnych samochodów ZIŁ 131. Posterunek uprzedzający jest na nadwoziu samochodu GAZ-66. Pododdział rozpoznania dźwiękowego rozwija od dwóch do trzech punktów (podstaw pomiarowych) zależnie od sytuacji operacyjno-taktycznej oraz posiadanego czasu.

Podstawę ugrupowania bojowego pododdziału rozpoznania dźwiękowego stanowią placówki dźwiękowe. W ugrupowaniu pododdziału wyposażonego w zestaw PZK, rozmieszczone są one w przybliżeniu na łuku koła, w odległości 2-3 km od linii styczności walczących wojsk. Pododdział wyposażony w zestaw AZK-5 rozwija swoje placówki (sześć) w linii prostej (w miarę możliwości terenu) na odcinku około 8-10km, w odległości 2-4 km od linii styczności.

Rozpoznanie dźwiękowe posiada możliwości skutecznej realizacji zadań rozpoznawczych na głębokość pierwszorzutowych brygad przeciwnika z ograniczoną możliwością w zakresie liczby i rodzaju wykrywanych obiektów w jednostce czasu[12].

W aktualnie funkcjonującym systemie rozpoznania artyleryjskiego podstawowymi dokumentami gromadzenia i opracowywania informacji rozpoznawczych są:

- na wszystkich punktach obserwacyjnych, w pododdziałach rozpoznania dźwiękowego i radiolokacyjnego – dziennik rozpoznania i obsługiwania strzelania;
- w punktach kierowania rozpoznaniem – dziennik zarządzeń i meldunków oraz dziennik ewidencji danych z rozpoznania,
- w punktach kierowania rozpoznaniem (PKR) pododdziałów artylerii – mapa rozpoznawcza. Na mapie rozpoznawczej umieszcza się dane o przeciwniku, wszystkie wykryte obiekty,

---

[12] Wynika to z możliwości zabezpieczenia ciągłości rozpoznania oraz niezawodności jego systemu.

z podaniem źródeł i terminów ich pozyskania, a także ugrupowanie bojowe sił i środków rozpoznania artyleryjskiego.

Jest to rozwiązanie analogiczne do stosowanego przez sztabowe komórki rozpoznania ogólnego.

Dokumentami sprawozdawczo-informacyjnymi w zakresie ewidencji celów są:

- w dywizjonie artylerii – szkic rozpoznawczy, dziennik celów, meldunek bojowy wraz ze szkicem i wykazem współrzędnych celów;
- w oddziałach (związkach taktycznych) artylerii – szkic celów (mapa), dziennik celów, meldunek rozpoznawczy;

W perspektywie dokumenty te będą zastąpione odpowiednio oprogramowanymi terminalami systemów komputerowych[13] (również „mapy elektroniczne"). Pozyskane zbiory danych na każdym poziomie dowodzenia nanosi się na mapę i analizuje na potrzeby prowadzenia ognia. Wyniki z rozpoznania przekazywane są bezpośredniemu przełożonemu w formie meldunków okresowych (od dwóch do czterech na dobę) oraz doraźnych niezwłocznie po wykryciu ważnych obiektów – celów. Otrzymywane meldunki podlegają weryfikacji w zakresie ich przydatności dla ognia artylerii. W przypadku spełnienia wymogów przewidzianych dokumentami normatywnymi (instrukcjami) podejmowane są stosowne decyzje o zwalczaniu wykrytych celów. Decyzje te w formie komend ogniowych kierowane są do pododdziałów ogniowych. Komendy ogniowe „spływają w dół" poprzez kolejne szczeble hierarchicznej sieci informacyjnej aż do wykonawców zadań ogniowych.

Wyniki rozpoznania artyleryjskiego są wykorzystywane do prowadzenia walki ogniowej oraz przekazywane odpowiednim komórkom dowodzenia jako elementy ogólnego położenia wojsk. Natomiast wyniki rozpoznania studyjnego, sprecyzowane wnioski z oceny zagrożenia oraz prognoza prawdopodobnego charakteru przyszłych działań, stanowią podstawę do wypracowania sposobów zdobywania danych niezbędnych do działalności ogniowej artylerii. Prognoza

---

[13] System TOPAZ

zagrożenia umożliwia określenie celów wysokoopłacalnych i wysokowartościowych. Na bazie uzyskanych danych następuje określenie ilości obiektów przewidzianych do rażenia.

Aktualnie środki rozpoznania artyleryjskiego mogą prowadzić rozpoznanie jedynie na potrzeby artylerii wykonującej zadania bezpośredniego wsparcia ogniowego (na głębokość od 5 do 7 km, a wyjątkowych warunkach do 10 km). Przy obecnym technicznym wyposażeniu nie mają one żadnych organicznych możliwości rozpoznania obiektów położonych w głębi operacyjno-taktycznej. Natomiast możliwości rozpoznania powietrznego i elektronicznego nie spełniają zakładanych przez artylerię wymagań w zakresie określenia położenia celów z wymaganą dokładnością i w związku z powyższym pozyskiwane dane nie mogą zostać wykorzystane do rażenia ogniowego. Tymczasem doświadczenia konfliktów lokalnych pozwalają na postawienie tezy, że środki rozpoznania artyleryjskiego powinny umożliwiać penetrację ugrupowania przeciwnika na głębokość dwu- a nawet trzykrotnie większą od zasięgu środków rażenia danego szczebla dowodzenia. Uzyskany w ten sposób czas operacyjny może zostać wykorzystany na zaplanowanie kolejnych uderzeń ogniowych.

Na koniec należy wskazać, że w kontekście procesu targetingu podsystem rozpoznania artyleryjskiego powinien stanowić organiczny i samowystarczalny układ pozyskiwania danych o obiektach przeciwnika przewidzianych do rażenia ogniowego. Układ ten powinien być zasilany informacyjnie w zakresie specjalistycznym, z zewnętrznych źródeł zasilania.

2.2.2. System rozpoznania inżynieryjnego

Rozpoznanie inżynieryjne jest to zespół przedsięwzięć studyjnych, planistyczno-organizacyjnych i wykonawczych, realizowanych przez dowódców wszystkich szczebli, sztaby i wojska w celu zdobycia (uzyskania) wiarygodnych wiadomości inżynieryjnych o przeciwniku i terenie, niezbędnych do podjęcia decyzji do działań taktycznych i zorganizowania zabezpieczenia inżynieryjnego

oraz realizacji zadań inżynieryjnych[14]. Indukując treści zawarte w powyższej definicji, dostrzegać należy dwa zasadnicze elementy składowe rozpoznania inżynieryjnego:

- zdobywanie wiadomości inżynieryjnych dotyczących przeciwnika i terenu w zakresie umożliwiającym przygotowanie i prowadzenie działań taktycznych,
- pozyskiwanie danych inżynieryjnych na potrzeby specjalistycznego zabezpieczenia inżynieryjnego i realizacji zadań inżynieryjnych.

Rozpoznanie inżynieryjne prowadzone przez pododdziały i oddziały rodzajów wojsk (np.:. das, pa, paplot, br) w zakresie potrzebnym do samodzielnego wykonywania zadań zabezpieczenia inżynieryjnego organizują dowódcy, wydzielając stosowne elementy rozpoznawcze. Natomiast wojska inżynieryjne prowadzą rozpoznanie specjalistyczne, wykorzystując w tym celu odpowiednio wyszkolone i wyposażone pododdziały rozpoznawcze. Stąd wniosek, że rozpoznanie inżynieryjne jest stałym składnikiem zabezpieczenia inżynieryjnego walki. Wobec powyższego posiada własną organizację (odrębną strukturą, wyposażenie techniczne oraz zasoby informacyjne), będącą częścią jedynie funkcjonalną taktycznego systemu rozpoznania wojsk lądowych.

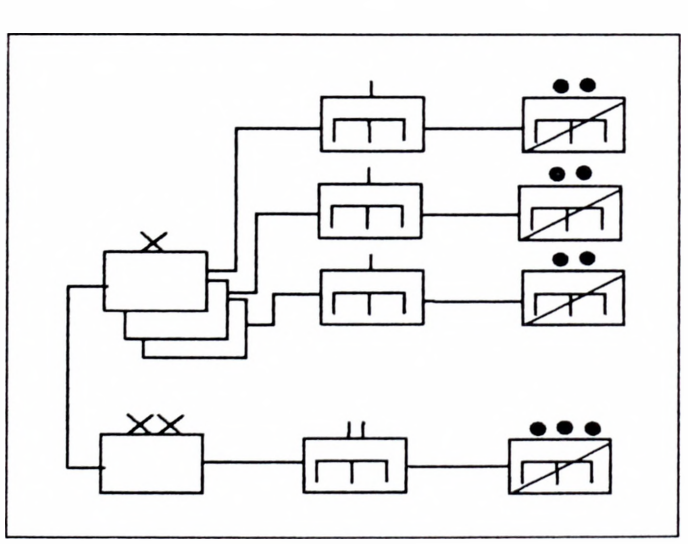
Zdobywanie danych o przeciwniku i terenie podsystem rozpoznania inżynieryjnego realizuje poprzez: obserwację, podsłuchiwanie, fotografowanie, wypad, zasadzkę, badanie dokumentów, sprzętu i uzbrojenia. Zatem przedstawione sposoby działania elementów rozpoznawczych są analogiczne jak w rozpoznaniu ogólnym. Reasumując wnioski w tym zakresie, należy stwierdzić, że rozpoznanie inżynieryjne realizuje zadania samodzielnie bądź w składzie elementów rozpoznawczych innych rodzajów wojsk.

W przyszłych działaniach bojowych niezwykle istotne znaczenie dla rozpoznania inżynieryjnego ma szczegółowe poznanie terenu. Stąd też właściwe rozpoznanie studyjne umożliwia zarówno pełniejsze wykorzystanie właściwości terenu jak i pozwala również z większym prawdopodobieństwem ocenić

---

[14] J. Parzewski, Rozpoznanie inżynieryjne w działaniach taktycznych, Warszawa, AON 1995, s. 7.

możliwości potencjalnego przeciwnika w zakresie inżynieryjnym. Z powyższego faktu wynikają wspólne obszary zainteresowania dla rozpoznania inżynieryjnego i ogólnego. Zaliczyć do nich należy: teren i przeciwnika. Stąd też konieczna jest ścisła współpraca informacyjna i analogicznie dalej konieczność posiadania dostępu do sieci informacyjnej obu podsystemów rozpoznania. Należy także stwierdzić, że w ramach rozpoznania przesyłane powinny być dane związane z koncepcyjną pracą komórek sztabowych w zakresie prognozy zagrożenia, właściwości taktycznych terenu i warunków atmosferycznych oraz przyszłego działania elementów rozpoznawczych. Powyższa koordynacja pracy sztabowej znajduje swe odzwierciedlenie w praktyce szkoleniowej, bowiem wielokrotnie w skład zespołów G-2 i S-2 wchodzą oficerowie wojsk inżynieryjnych. Procedura pracy sztabowych komórek wojsk inżynieryjnych (osób funkcyjnych) w zakresie rozpoznania jest analogiczna (w obszarze gromadzenia, przetwarzania i dystrybucji danych) jak w podsystemie rozpoznania ogólnego.



Rys. 1. Struktura taktycznego systemu rozpoznania inżynieryjnego

Praktyka prowadzonych ćwiczeń wskazuje, że istnieje również tendencja tworzenia w początkowym etapie pracy sztabu, wydzielonej komórki analizy i oceny terenu obejmującej oficerów o specjalności: rozpoznanie, wojska inżynieryjne, radioelektronika, logistyka, obrona powietrzna. Zespół ten

funkcjonalnie realizuje zadania w komórce G-2 (S-2), a efekty jego pracy udostępniane są wszystkim zainteresowanym oficerom sztabu.

W rozpoznaniu inżynieryjnym podstawowym kanałem informacyjnym jest łączność radiowa. W radiostację UKF wyposażone są transportery rozpoznania inżynieryjnego oddziałów i związków taktycznych. Alternatywnym rozwiązaniem jest stosowanie na posterunkach obserwacyjnych radiostacji przenośnych.

Dowódca kompanii saperów utrzymuje z podległymi dowódcami plutonów oraz dowódcą drużyny rozpoznania inżynieryjnego w sieci radiowej za pomocą radiostacji UKF. Łączność z dowódcą drużyny rozpoznania inżynieryjnego utrzymywana jest w S/R KF kierownika sekcji rozpoznania brygady za pomocą radiostacji pokładowej KF z WD.

Powyższe fakty wskazują, że przesyłanie danych o terenie i przeciwniku odbywa się z wykorzystaniem funkcjonalnych kanałów informacyjnych. Stosowane rozwiązania wynikają zawsze z określonej sytuacji operacyjno-taktycznej oraz rodzaju prowadzonych działań taktycznych. Zadania rozpoznawcze można ująć w następujących wariantach wykorzystania taktycznego rozpoznania wojsk inżynieryjnych:

- w okresie przygotowania obrony do prowadzenia rozpoznania inżynieryjnego we własnym ugrupowaniu z zadaniem ustalenia rubieży dogodnych do rozbudowy rejonów i pozycji obronnych oraz zabezpieczenia potrzeb manewru wojsk własnych. Następnie w koordynacji z G-2 (S-2) prowadzenie rozpoznania składu i wyposażenia wojsk inżynieryjnych przeciwnika w aspekcie podejmowanych działań przygotowawczych do pokonania systemu zapór inżynieryjnych;
- w natarciu zasadniczym zadaniem rozpoznania jest ustalenie możliwości i sposobu rozbudowy rejonów przeznaczonych do rozmieszczenia wojsk oraz dróg marszu do rubieży wejścia do walki, a następnie ustalenie stopnia rozbudowy fortyfikacyjnej punktów oporu, rubieży i pozycji obronnych przeciwnika, w tym przygotowanych niszczeń.

Rozpoznanie inżynieryjne realizuje w pierwszej kolejności zadania związane z realizacją poszczególnych elementów zabezpieczenia inżynieryjnego a następnie rozpoznania działalności przeciwnika w aspekcie inżynieryjnym. Wniosek z tego, że koordynując działania rozpoznawcze konieczne jest uwzględnienie specyfiki rozpoznania inżynieryjnego tak zakresie pozyskiwanych informacji, jak i w charakterze realizowanych zadań rozpoznawczych.

Planowaniem rozpoznania inżynieryjnego, na szczeblach taktycznych, zajmują się kierownicy sztabowych komórek wojsk inżynieryjnych, którzy koordynują wysiłki rozpoznawcze w tym zakresie z oficerami S-2/G-2. Dokumenty planistyczne zabezpieczenia inżynieryjnego ujmują działalność rozpoznawczą w „Planie zabezpieczenia inżynieryjnego", gdzie nanoszone są obiekty rozpoznania, elementy rozpoznania i kierunki ich działania. W batalionie saperów związku taktycznego i kompanii saperów oddziału opracowuje się stosowne dokumenty dowodzenia (np.: Tabelę zadań oraz użycia sił i środków rozpoznania inżynieryjnego).

2.2.3. System rozpoznania skażeń

Sprawą o zasadniczym znaczeniu dla prowadzenia rozpoznania skażeń, a szerzej rzecz traktując, dla działalności całego systemu rozpoznania jest fakt, że w ostatnich latach zmieniła się ocena zagrożeń militarnych państwa, a koncepcja rozwiązywania potencjalnych konfliktów z użyciem broni masowego rażenia ma coraz mniej zwolenników (lub jest całkowicie pomijana).

Jednak fakt istnienia broni masowego rażenia jest już wystarczającym dowodem na poparcie tezy o możliwości rozwiązywania konfliktów lokalnych z użyciem BMR, nawet broni jądrowej (Indie – Pakistan?), a więc powstania rozległych stref skażeń[15]. Utrzymywanie w dużych ilościach ładunków BMR i środków jej przenoszenia w arsenałach mocarstw atomowych każe widzieć nie tylko potencjalne zagrożenie[16].

---

[15] W 1979 roku w okolicach Świerdłowska (obecnie Jekaterynburg) z laboratorium wojskowego, w którym produkowano broń biologiczną, wydostało się na zewnątrz kilka tysięcznych grama płynu z żywymi kulturami wąglika. W męczarniach zginęło 96 pracowników.

[16] Podczas operacji „Pustynna Burza" kilkadziesiąt razy ogłaszano alarm chemiczny.

Jeszcze innego wymiaru rozpoznanie skażeń nabiera w aspekcie potencjalnych działań terrorystycznych[17] oraz w sytuacjach, kiedy to broń biologiczna może zostać użyta w lokalnych konfliktach narodowościowych. Reasumując powyższe fakty stwierdzić należy, że w dającej się przewidzieć przyszłości raczej niemożliwe będzie jednoznaczne rozstrzygnięcie zasadności i realności zastosowania BMR w walce zbrojnej[18].

Wobec powyższego stanu faktów tylko jako prawdopodobna może być uwzględniana perspektywa selektywnego (ograniczonego) użycia BMR w działaniach taktycznych[19]. Przyjęcie nakreślonego powyżej modelu zagrożenia BMR może w konsekwencji wpłynąć na istotne zmiany zadań w zakresie rozpoznania. Zwiększeniu ulegnie liczba zadań związanych z rozpoznaniem skażeń chemicznych, wywołanych zwłaszcza przez toksyczne środki przemysłowe (TSP)[20] oraz obiekty energetyki jądrowej[21].

Głównym zadaniem systemu rozpoznania skażeń jest zapewnienie dowódcom i sztabom danych o faktach i skutkach użycia broni masowego rażenia oraz awariach obiektów energetyki jądrowej i przemysłu chemicznego. Ponadto dokonanie oceny zaistniałych zdarzeń i na tej podstawie przedstawienie wniosków i propozycji działań mających na celu minimalizację ich skutków. Pododdziały rozpoznania skażeń są przeznaczone do działania zarówno w okresie pozyskiwania (pododdziały), jak i weryfikacji danych (SOAS). Źródłami rozpoznania są urządzenia zamontowane na samochodach opancerzonych BRDM-2 rs. Z ich wykorzystaniem możliwe jest uzyskanie na potrzeby podsystemu rozpoznania skażeń, następujących informacji rozpoznawczych:

---

[17] W marcu 1995 roku japońska sekta religijna – Aum Shinrikyo, użyła sarinu w środkach komunikacji miejskiej w Tokio, zginęło niemal 200 osób, a skutki działania gazu odczuło około 5000 mieszkańców.
[18] W czasie wojny w Zatoce Perskiej wojska Saddama Husajna wpompowały ogromne ilości ropy do Zatoki Perskiej – jest to przykład realnych zagrożeń trudnych do przewidzenia.
[19] Por. S. Prądzyński, Kierunki doskonalenia obiegu informacji systemu wykrywania skażeń w aspekcie zmian strukturalnych sił zbrojnych, Myśl Wojskowa 1997 nr 6, s. 57-66.
[20] W 1984 roku w Bhopalu (Indie) wyciek z amerykańskich zakładów chemicznych spowodował śmierć 6954 osób.
[21] Awaria elektrowni atomowej w Czarnobylu.

- warunki panujące w przyziemnych warstwach atmosfery (kierunek i prędkość wiatru, pionowa stateczność atmosfery, temperatura gleby oraz na wysokości 0,5 m i 2 m, stan zachmurzenia),
- parametry naziemnych wybuchów jądrowych (moc wybuchu, czas, azymut i odległość od posterunku, kierunek przemieszczania się obłoku promieniotwórczego),
- azymut i odległość od powietrznego wybuchu jądrowego,
- rozkład mocy dawki ekspozycyjnej w terenie skażonym promieniotwórczego,
- rodzaj użytego bojowego środka trującego (w zakresie ograniczonym do grup związków fosforoorganicznych, parzących, duszących i ogólnotrujących),
- stopień skażenia uzbrojenia, sprzętu bojowego oraz środków materiałowych.

Ponadto załogi samochodów opancerzonych BRDM-2 rs mogą pobierać skażone próbki do analizy w laboratoriach. Pozyskane dane rozpoznawcze są przekazywane radiowym kanałem informacyjnym, jako jawne meldunki, do komórek specjalistycznych, a następnie w strukturze hierarchicznej na kolejne szczeble dowodzenia. Zatem organizacja rozpoznania skażeń powoduje, że pozyskiwane dane rozpoznawcze są zbierane przez pododdziały rozpoznania skażeń. Następnie są przykazywane w postaci jawnych meldunków kanałami łączności radiowej poprzez kolejne szczeble dowodzenia do stacji obliczeniowo-analitycznej skażeń (SOAS) związku taktycznego. Specjalistyczne drużyny rozpoznania skażeń znajdują się w plutonach przeciwchemicznych brygady.

System wykrywania skażeń dysponuje siłami i środkami umożliwiającymi określanie parametrów uderzeń bronią masowego rażenia, monitoring skażeń oraz odtwarzanie rzeczywistej sytuacji skażeń chemicznych i promieniotwórczych, powstałej w wyniku uderzeń chemicznych, jądrowych oraz zniszczeń (awarii) obiektów przemysłowych. W stałej gotowości bojowej funkcjonują tylko wybrane elementy systemu zwane systemem wczesnego wykrywania (SWW). Pozostałe elementy rozwijane są w miarę wzrostu poziomu

zagrożenia. Do zasadniczych elementów strukturalnych systemu rozpoznania skażeń należy zaliczyć:

- posterunki (patrole) naziemnego rozpoznania skażeń, organizowane przez pododdziały rozpoznania skażeń;
- patrole powietrznego rozpoznania skażeń, organizowane na bazie kluczy śmigłowców rozpoznania skażeń;
- specjalistyczne jednostki organizacyjne, przeznaczone do prowadzenia analiz.

Podsystem rozpoznania skażeń tworzą obecnie elementy, rozmieszczone głównie w sztabach związków taktycznych, oddziałów i pododdziałów. Są one połączone za pośrednictwem stosownych kanałów informacyjnych. W systemie rozpoznania skażeń możemy wyszczególnić następujące źródła rozpoznania:

- w specjalistycznych pododdziałach rozpoznania skażeń – posterunki i patrole naziemnego rozpoznania skażeń oraz patrole powietrznego rozpoznania skażeń, dokonujące pomiarów z użyciem przyrządów pomiarowych znajdujących się w samochodach do rozpoznania skażeń BRDM-2rs i śmigłowcach Mi-2 rs;
- w pozostałych pododdziałach – posterunki obserwacyjne (w batalionach) i obserwatorzy (w kompaniach).

W systemie rozpoznania skażeń szczególne znaczenie dla jakości procesów informacyjnych ma algorytm przetwarzania danych, a więc metoda otrzymywania informacji na podstawie zbioru danych rozpoznawczych. Na bazie uzyskanych informacji oficer obrony przeciwchemicznej, korzystając z odpowiednich tabel, wykreśla na mapie prognozowaną lub rzeczywistą sytuację skażeń, a następnie – porównując położenie stref skażeń z położeniem własnych obiektów militarnych – ocenia straty oraz opracowuje propozycje działań minimalizujących skutki uderzeń bronią masowego rażenia. Prognozowanie zagrożeń polega na przetworzeniu zbioru danych uzyskanych ze źródeł przy pomocy specjalistycznych metodyk pracy oficerów obrony przeciwchemicznej dotyczących:

- oceny sytuacji chemicznej po skażeniach toksycznymi środkami przemysłowymi (TSP),
- oceny sytuacji promieniotwórczej po awarii elektrowni jądrowej,
- oceny sytuacji promieniotwórczej w terenie,
- oceny sytuacji chemicznej,
- oceny strat w rejonach uderzeń bronią jądrową.

W obecnie funkcjonującym systemie rozpoznania skażeń wszystkie dane wejściowe systemu wykrywania skażeń są uzyskiwane za pomocą stosunkowo prostych przyrządów pomiarowych (źródeł rozpoznania). Do głównych wad tak zorganizowanego systemu wejść informacyjnych należy zaliczyć:

- identyfikację przez przyrządy pomiarowe tylko nielicznej grupy środków toksycznych (wyłącznie grupa związków fosforoorganicznych, iperyt, luizyt, cyjanowodór, chlorocyjan, fosgen i dwufosgen);
- niski poziom automatyzacji pomiarów meteorologicznych, detekcji środków toksycznych i określania parametrów naziemnych wybuchów jądrowych i małą wiarygodność oceny parametrów wybuchów naziemnych oraz niemożliwość określenia parametrów powietrznych wybuchów jądrowych;
- możliwość zakłócania informacyjnego w czasie transmisji meldunków drogą radiową.

Wydaje się, że jakość sieci informacyjnej taktycznego systemu rozpoznania skażeń można poprawić poprzez wyposażenie elementów strukturalnych systemu w urządzenia do automatycznego wykrywania i określania parametrów wybuchów jądrowych, w tym również powietrznych. Dostrzegać należy także konieczność wprowadzenia do wyposażenia pododdziałów rozpoznania skażeń przyrządów umożliwiających automatyczne wykrywanie większej liczby środków toksycznych, w tym także przemysłowych.

Ze względu na to, że czynności wykonywane podczas przetwarzania danych mają charakter rutynowy, a obliczenia – charakter ściśle formalny, rozwój systemu wykrywania skażeń powinien zmierzać w kierunku opracowania oprogramowania umożliwiającego automatyzację działania. Konieczne wydaje

się stworzenie sieci komputerowej, w której informacje dotyczące uderzeń bronią masowego rażenia, skażeń chemicznych i promieniotwórczych oraz awarii obiektów zawierających toksyczne środki przemysłowe lub materiały promieniotwórcze byłyby przekazywane za pomocą łączy modemowych do centralnego węzła informacyjnego – stacji/bazy, dokonującego aktualizacji zasobów informacyjnych.

W celu zapewnienia niezawodności systemu rozpoznania skażeń wskazane wydaje się połączenie informacyjne jego struktur również w układzie niemilitarnym, z możliwością wzajemnego przejmowania niektórych zadań w razie awarii technicznych lub zniszczeń istotnych jego elementów. W okresie pokoju system rozpoznania skażeń powinien ściśle współdziałać z Państwowym Monitoringiem Środowiska i tworzyć bazę danych o stanie ochrony środowiska w jednostkach i instytucjach wojskowych, a także o zagrożeniach ekologicznych ze strony obiektów przemysłowych, transportu kołowego, kolejowego i wodnego.

2.2.4. System rozpoznania powietrznego

Rozpoznanie powietrzne to całokształt przedsięwzięć na ziemi i w powietrzu mających na celu zdobywanie informacji o przeciwniku, terenie i warunkach atmosferycznych za pomocą aparatów latających w przestrzeni powietrznej do wysokości 30 000 m[22]. Rozpoznanie powietrzne jest organizowane i prowadzone w celu zdobycia nowych informacji rozpoznawczych o obiektach przeciwnika oraz dla potwierdzenia wiadomości pozyskanych z innych źródeł. Dodatkowo rozpoznanie powietrzne służy do określenia skutków własnych uderzeń ogniowych. Powietrzne działania rozpoznawcze prowadzone są w ścisłej koordynacji z innymi rodzajami rozpoznania. Taktyczne rozpoznanie powietrzne prowadzi się w celu zdobycia informacji o przeciwniku, niezbędnych do prowadzenia działań taktycznych. Przyjmuje się, że taktyczne rozpoznanie powietrzne prowadzone jest na

---

[22] K. Jóźwiak, *Rozpoznanie powietrzne*, Warszawa 1996.

głębokość około 80 – 150 km. Jest to związane przede wszystkim ze strefą działania i zainteresowania oddziału i związku taktycznego wojsk lądowych. W odniesieniu do potrzeb planowania i użycia środków rażenia (lotniczych i lądowych) rozpoznanie powietrzne dzieli się na wstępne, bezpośrednie i kontrolne[23].

Lotnictwo związku taktycznego wojsk lądowych stanowi eskadra śmigłowców rozpoznawczo-łącznikowych. Eskadra ta składa się z dwóch kluczy śmigłowców. Klucz rozpoznawczy w składzie czterech śmigłowców rozpoznawczych i klucz łącznikowy w składzie dwóch śmigłowców (łącznikowy i powietrzny punkt dowodzenia). W okresie pokoju eskadry tworzą grupę śmigłowców związków taktycznych, która organizacyjnie wchodzi w skład pułku śmigłowców bojowych. W ramach pułku realizuje szkolenie lotnicze, natomiast szkolenie taktyczne najczęściej w ramach ćwiczeń taktycznych wojsk lądowych. Wydzielone eskadry w okresie zagrożenia i wojny są podporządkowywane dowódcom związków taktycznych.

Do głównych zadań rozpoznania powietrznego eskadry śmigłowców rozpoznawczo-łącznikowych związku taktycznego wojsk lądowych należy:

- rozpoznanie składu, ugrupowania i systemu dowodzenia przeciwnika i ustalenie rozmieszczenia jego wybranych środków ogniowych, a także stopnia rozbudowy inżynieryjnej;
- ustalenie rozmieszczenia środków elektronicznych przeciwnika;
- wykrywanie i rozpoznawanie oraz ciągłe śledzenie manewru odwodów przeciwnika;
- wykrywanie i rozpoznawanie rejonów rozmieszenia elementów i urządzeń logistycznych oraz dozorowanie dróg i mostów;
- kierowanie ogniem artylerii oraz naprowadzanie na cel śmigłowców bojowych i samolotów działających w ramach bezpośredniego wsparcia sił lądowych.

---

[23] Zob. szerzej: M., Łokociejewski (red.) *Rozpoznanie wojskowe* cz. III, wyd. cyt.

Śmigłowce rozpoznawcze w określonych sytuacjach mogą wykonywać także zadania transportowe, przerzucając w szczególnie newralgiczne rejony niewielkie zespoły zwiadowców wraz z niezbędnym wyposażeniem i motocyklami, a także grupy dalekiego rozpoznania.

Na podstawie badań empirycznych określono, że załoga śmigłowca rozpoznawczego w ciągu doby może wykonać 2-3 loty długotrwałe do 2 godzin lub 6-9 lotów krótkotrwałych po 20-30 minut[24]. Natomiast analiza możliwości pozyskiwania danych wskazuje, że w jednym wylocie załoga śmigłowca może wykonać tylko jedno z następujących zadań rozpoznawczych:

W dzień:

- prowadzenie obserwacji 1-2 rejonów o powierzchni 10-25 km^2 na głębokość 4-8 km oraz określenie rodzaju obiektu, charakteru jego działalności i współrzędnych,
- prowadzenie obserwacji pola walki w pasie bezpośrednio przyległym do rubieży styczności bojowej o szerokości 6 km na głębokość 4-8 km i przekazanie informacji z pokładu śmigłowca na SD ZT,
- rozpoznanie wzrokowo-fotograficzne 1-2 odcinków dróg o łącznej długości do 100 km lub odcinka rzeki do 50 km,
- rozpoznanie skażeń przemysłowych w 1-2 rejonach,
- rozpoznanie bezpośrednie 1-2 obiektów znajdujących się na głębokości 4-8 km z określeniem współrzędnych i przekazanie informacji na SD ZT,
- poprawianie i kontrola ogni artylerii do 1–2 celów stałych lub jednego ruchomego znajdujących się na głębokości 4-8 km,
- rozpoznanie 2-3 rejonów rozwinięcia własnych pododdziałów artylerii polowej lub rakietowej,
- przewóz pasażerów w ramach lotów łącznikowych lub grupy rozpoznawczej (4-5 żołnierzy) na głębokość do 30 km,

W nocy:

---

[24] W. Michalak, S. Suchora, Użycie śmigłowców rozpoznawczych w działaniach bojowych wojsk, Warszawa, AON 1995, s. 45.

- prowadzenie obserwacji pola walki w pasie bezpośrednio przyległym do rubieży styczności wojsk o szerokości 4-6 km na głębokość 2-4 km, przy oświetleniu terenu,
- rozpoznanie w jasną noc 1-2 odcinków dróg nad własnym terenem o łącznej długości do 100 km,
- prowadzenie rozpoznania bezpośredniego z wykorzystaniem aparatury do rozpoznania w podczerwieni na głębokość 3-4 km od rubieży styczności wojsk,
- poprawianie ognia artylerii polowej do jednego celu stałego oświetlonego pociskami artyleryjskimi,
- przerzut grupy rozpoznawczej na głębokość do 30 km.

Przedstawione powyżej fakty wskazują na konieczność posiadania określonych jednostek śmigłowców rozpoznawczych. Aktualne możliwości klucza w składzie 4 maszyn wskazują, że nie jest on w stanie prowadzić rozpoznania, z zachowaniem ciągłości. Bowiem każdy obiekt powinien być rozpoznawany 4-6 razy w ciągu doby. Zatem jedynie 8-12 obiektów może być rozpoznanych przy lotach krótkotrwałych, a jeszcze mniej (o połowę) przy lotach długotrwałych. Przeprowadzona analiza możliwości rozpoznawczych wskazuje, że klucz śmigłowców może zaspokoić potrzeby informacyjne ZT w zakresie 16-24% ogólnej liczby obiektów, natomiast w przypadku skupienia priorytetu rozpoznania jedynie na obiektach ważnych 32-48%[25]. Powyższe kalkulacje powinny również uwzględniać prawdopodobieństwo wykonania zadania, które w głównej mierze zależy od efektywności rozpoznania oraz poziomu obezwładnienia obrony przeciwlotniczej przeciwnika. Przeprowadzone badania praktyczne, a także doświadczenia z ćwiczeń i konfliktów wskazują, że w zależności od rodzaju obiektów i możliwości rozpoznania, współczynnik efektywności kształtuje się na poziomie 0,7. Oznacza to, że wskazany procent

---

[25] W pasie obrony dywizji (na głębokości 10-30 km) może być rozmieszczonych około 280 różnych obiektów przeciwnika. O. Horak, *Jakie zadania należałoby postawić rozpoznaniu wojskowemu*, Zeszyty Naukowe AON 1994, nr 2 (15), s. 78.

zaspokojenia potrzeb informacyjnych ZT wojsk lądowych przez śmigłowce będzie jeszcze mniejszy[26].

Doświadczenie wskazują, że nieuzbrojonym okiem można rozpoznać obiekty (np. czołgi, transportery, artylerię) z odległości 4-6 km w warunkach dobrej widoczności z wysokości 50-300 m. Wobec tego rozpoznawanie musi być prowadzone na podstawie widoku obiektów z jednej strony – rzut boczny lub czołowy. Celowe jest, zatem wyposażenie śmigłowców w aparaturę do obserwacji wzrokowej oraz aparaturę rozpoznania obrazowego wyróżniającą się odpowiednio wysoką zdolnością rozdzielczą i ostrością zobrazowania. Do pozyskiwania danych w warunkach ograniczonej widoczności konieczne jest wyposażenie śmigłowców rozpoznawczych w urządzenia pozwalające na rozpoznawanie celów i ich identyfikację bez konieczności widzialności wzrokowej. Obecne systemy termalne, zdaniem ekspertów, nie spełniają oczekiwanych wymagań w tym zakresie, natomiast może je spełnić radar zakresu milimetrowego. Szczególnie złożone problemy istnieją w obszarze pozyskiwania danych w warunkach nocnych. Dla zapewnienia właściwego oświetlenia i ustawienia punktów orientacyjnych, według których załoga śmigłowca będzie określała położenie obiektów w ugrupowaniu przeciwnika, konieczne jest oświetlenie terenu za pomocą bomb lub specjalnych rakiet oświetlających. Wyniki obserwacji w warunkach optycznych przekłamań świetlnych obniżają wartość pozyskiwanych danych w aspekcie ich wiarygodności. Poprawy istniejącego stanu rzeczy szukać należy w wyposażeniu śmigłowców rozpoznawczych w aparaturę elektroniczną, umożliwiającą załodze wykonywanie zadań bez spełnienia warunku optycznej widzialności obiektu.

Użycie śmigłowców na rzecz artylerii i ich bojowego wykorzystania na potrzeby kierowania ogniem wskazuje, że może być ono realizowane jedynie w warunkach obserwacji wzrokowej. Obserwacja wzrokowa z wykorzystywaniem mapy 1:25 000 lub zdjęć fotograficznych, umożliwia określenie uchyleń wybuchów od celu z dokładnością zapewniającą przejście do

---

[26] W. Michalak, S. Suchora, *Użycie śmigłowców rozpoznawczych,* s. 47.

ognia skutecznego. Jednak działanie takie nie jest efektywne, ponieważ w większości przypadków określenie współrzędnych charakteryzuje się dużym błędem kołowym. Składa się na to szereg przyczyn, a do głównych można zaliczyć: poziom wyszkolenia nawigatora, dokładność mapy i jej aktualność (zgodność z terenem), charakter obszaru działania – obecność punktów terenowych umożliwiających załodze dowiązanie się do terenu, warunki obserwacji (wysokość, widoczność, odległość obserwacji). Ponadto sumaryczny czas wykrycia, rozpoznania celu i jego identyfikacji oraz wypracowania danych do strzelania pozwala na prowadzenie ognia z wykorzystaniem śmigłowców do obiektów stałych lub o niewielkiej manewrowości. W perspektywie przyszłych działań manewrowych i dynamicznego pola walki taki stan rzeczy jest nie do przyjęcia. Konieczne jest wprowadzenie automatycznego systemu przekazywania danych z urządzeń rozpoznawczych śmigłowca na stanowiska ogniowe artylerii.

Przedstawione fakty wskazują, że prowadzenie rozpoznania przez śmigłowce może być realizowane jedynie dla potrzeb oceny sytuacji w strefie taktycznej i to nie na całą jej głębokość. Wiąże się to przede wszystkim ze słabym wyposażeniem śmigłowców rozpoznawczych, które nie pozwala na precyzyjne określenie położenia poszczególnych elementów ugrupowania bojowego przeciwnika. Ponadto obserwacja może być prowadzona w zasadzie tylko znad ugrupowania wojsk własnych (w bezpiecznej odległości od linii styczności wojsk) co z kolei ogranicza jego zasięg. Należy domniemywać, że w przyszłych działaniach, gdzie priorytetowym obszarem zmagań walczących stron, będzie walka informacyjna, śmigłowce rozpoznawcze powinny stanowić ważny element pozyskiwania całego spektrum informacji rozpoznawczych o sytuacji w strefie taktycznej.

Fotografowanie jest jednym z ważniejszych źródeł pozyskiwania danych. Do zasadniczych zadań wykonywanych za pomocą aparatury fotograficznej należy rozpoznawanie rejonów obrony przeciwnika, inżynieryjnej rozbudowy terenu, stanu technicznego dróg, mostów, węzłów komunikacyjnych.

Warunki wykonywania tych zdjęć obligują do zastosowania kamer panoramicznych o dużych możliwościach technicznych.

Zebrane wnioski praktyczne pozwalają na stwierdzenie, iż zasadniczymi problemami w pozyskiwaniu terminowych i wiarygodnych danych są: długi czas opracowania wyników rozpoznania, niska jakość materiału fotograficznego, niski współczynnik wykonania zadania (zależny głównie od widzialności i struktury obrony przeciwlotniczej przeciwnika) oraz zasięg rozpoznania śmigłowca.

Analiza współczesnych typów śmigłowców rozpoznawczych wybranych państw NATO, wskazuje, że posiadają one w zakresie środków łączności 2-5 radiostacji KF i UKF przeznaczonych do współpracy z wojskowymi organami ruchu lotniczego, ośrodkami dowodzenia różnych rodzajów wojsk oraz na potrzeby kierowania ogniem. Wyposażenie wybranych zachodnich śmigłowców rozpoznawczych stanowią między innymi: zautomatyzowane systemy nawigacyjne, łączności i transmisji danych obrazowych, komputery pokładowe wspomagające pracę pilota i obserwatora, systemy ostrzegania.

Wprowadzenie na szczebel związku taktycznego organicznych pododdziałów rozpoznania powietrznego (śmigłowców i środków bezpilotowych) zwiększy wydajność informacyjną systemu i przyczyni się do wzrostu poziomu wiarygodności pozyskiwanych danych poprzez porównanie wyników rozpoznania pozyskiwanych z różnych źródeł powietrzno-lądowego systemu zdobywania danych. Tym bardziej, że zarówno praktyka ćwiczeń (armii zachodnich) jak i rozważania teoretyczne wskazują na potrzebę włączenia jednostek śmigłowców rozpoznawczych w strukturę organizacyjną związków taktycznych. Najczęściej spotykaną formą organizacyjną są eskadry śmigłowców rozpoznawczych w oddziałach śmigłowców związków taktycznych wojsk lądowych (WB, Francja, Niemcy). W USA natomiast śmigłowce rozpoznawcze zorganizowane są w kompanię rozpoznania powietrznego batalionu rozpoznawczego.

Ważne miejsce w aktualnych koncepcjach prowadzenia działań rozpoznawczych znalazły bezzałogowe aparaty rozpoznawcze[27] (BAR). W perspektywie zakłada się zastąpienie śmigłowców i samolotów załogowych przez BAR w sytuacjach złożonych i niebezpiecznych, a do tej grupy należą zadania rozpoznawcze. Bezzałogowe aparaty latające charakteryzujące się prostotą obsługi, małymi powierzchniami odbicia radiolokacyjnego, niskim poziomem promieniowania podczerwonego i hałasu mają większe możliwości przetrwania i wykonania zadań rozpoznawczych w ugrupowaniu potencjalnego przeciwnika. Postęp w elektronice wprowadził nową jakość w dziedzinie rozpoznania. W najnowszych konstrukcjach BAR tradycyjne aparaty fotograficzne zastępowane są przez czujniki elektroniczne, które umożliwiają prowadzenie rozpoznania niezależnie od warunków atmosferycznych i pory doby oraz przesyłanie zdobytych danych w czasie rzeczywistym lub ich cyfrową rejestrację na nośniku magnetycznym. Obraz cyfrowy dostarczany przez elektroniczne czujniki charakteryzuje się dużą szczegółowością, łatwością w przetwarzaniu elektronicznym i teletransmisji. Cyfrowe dane pozyskanego obrazu przetwarza się w taki sposób, ażeby uwypuklić lub skorygować wybrane elementy lub obiekty będące przedmiotem rozpoznania.

Szansę w rozwoju rozpoznania powietrznego poprzez zastosowanie najnowszych osiągnięć techniki, zwłaszcza z dziedziny elektroniki, mechaniki precyzyjnej, materiałów i technologii do wytwarzania produkcji bezzałogowych aparatów latających dostrzegło wiele państw.

2.2.5. System rozpoznania elektronicznego

Rozpoznanie elektroniczne (wykrywanie, przechwytywanie, śledzenie oraz namierzanie) organizuje się w skali samodzielnego pododdziału – kompanii radioelektronicznej związku taktycznego[28]. W procesie zdobywania danych o przeciwniku istota ich pozyskiwania sprowadza się do wykorzystania

---

[27] Termin ten obejmuje samoloty oraz śmigłowce bezzałogowe a także konstrukcje wolnolatające z aparaturą rozpoznawczą (np.: balony obserwacyjne, szybowce, paralotnie).

[28] Pomimo zmiany nazwy w WRE na WE nazwa pododdziału pozostała, bowiem większość zadań realizowane jest s zakresie radiowym.

wszelkich dostępnych sił i środków, aby zgromadzić jak najwięcej prawdziwych danych o położeniu faktycznym i zamiarach przeciwnika. Stosownie do tego na bazie dostępnych narzędzi tworzy się podsystem rozpoznania dostosowany do realizacji określonego zadania[29]. Kompania radioelektroniczna stojące przed nią zadania walki elektronicznej realizuje na korzyść związku taktycznego, a więc uczestniczy we wszystkich rodzajach działań taktycznych. Zakres realizowanych zadań specjalistycznych uzależniony będzie, zatem od zadań walki elektronicznej podjętych i realizowanych przez dowództwo związku taktycznego. Głównym celem walki elektronicznej w działaniach taktycznych jest:

1) wykrycie emisji elektromagnetycznych (sygnałów) przeciwnika,
2) zabezpieczenie efektywnego wykorzystania energii elektromagnetycznej wojskom własnym,
3) zapobieżenie użyciu energii elektromagnetycznej przez przeciwnika.

Taktyczny system rozpoznania elektronicznego obejmuje następujące źródła rozpoznania:

1) posterunki rozpoznania radioelektronicznego – są to posterunki namierzania radiowego oraz posterunki rozpoznania systemów radiolokacyjnych. W czasie pracy bojowej posterunki tworzą stosowne systemy rozpoznania elektronicznego;
2) posterunki namierzania radiowego – dostarczają danych umożliwiających lokalizację źródeł rozpoznania (pracujących radiostacji).

Namiary dokonywane są zarówno na źródła wykryte w celu ustalenia miejsca ich rozmieszczenia, a także na źródła przechwytywane i śledzone dla potwierdzenia bądź uaktualnienia danych o ich położeniu. Niezależnie od sposobu prowadzenia namierzania, praca posterunku polega na dostrojeniu urządzeń stanowiska namierzania do częstotliwości pracy środków radiowych przeciwnika i identyfikacji źródła. Następnie dokonywany jest namiar na obiekt elektroniczny, a uzyskany wynik przekazywany jest kanałem informacyjnym na stanowisko kierowania namiarem;

---

[29] Por. L. Ciborowski, *Walka informacyjna*, Toruń 2002, s. 78.

3) posterunki rozpoznania systemów radiolokacyjnych – zdobywają dane rozpoznawcze samodzielnie, ściśle współpracując ze sobą podczas lokalizacji źródeł. Współpraca polega na wzajemnym naprowadzaniu się na wykryte obiekty oraz wymianie danych umożliwiających identyfikację źródeł przeciwnika;

4) posterunki zakłóceń radiowych – są elementem wykonawczym zadań obezwładniania radiowego. Ciągła praca posterunku, ze względów bezpieczeństwa, w reżimie aktywnego zakłócania realizowana jest przez okres około 1 godziny. Po tym czasie posterunek należy przemieścić na pozycję zapasową. Podsystem zakłóceń jest najbardziej manewrowym elementem systemu walki elektronicznej.

Do zasadniczych elementów warunkujących terminowe wykonanie zadań rozpoznawczych należą:

- zakres wykorzystania przestrzeni elektromagnetycznej przez przeciwnika, a w tym intensywność pracy namierzanych obiektów elektronicznych,
- właściwości namierników wykonujących namiar,
- pojemność kanału informacyjnego w zakresie przekazywania zadań i gromadzenia wyników namierzania,
- potencjał obrony elektronicznej przeciwnika w tym szczególnie intensywność oddziaływania elektronicznego na system zdobywania danych,
- poziom obsady etatowej obsług i zakres ich wyszkolenia.

Praktyczne wnioski uzyskane w toku prowadzonych ćwiczeń dowodzą, że z danych rozpoznania elektronicznego tylko treść jawnej korespondencji przekazywanej w kanałach łączności może zawierać treści informacyjne o działalności przeciwnika do bezpośredniego wykorzystania. Pozostałe dane dotyczące pracy systemów elektronicznych wymagają szczegółowej analizy w celu przetworzenia ich na pożądane zbiory informacyjne. Analizy tej dokonuje

zespół funkcjonalny na podstawie zgromadzonych zasobów informacyjnych obejmujących:

1. Parametry techniczne:

- częstotliwości i czas pracy, czas trwania impulsów, okresy ich powtarzania oraz okresy obrotów anten źródeł rozpoznania,
- cechy identyfikujące obiekt stanowiący źródło rozpoznania,
- indywidualne cechy rozpoznawcze radiotelegrafistów obsługujących radiostacje,
- intensywność pracy źródeł,
- azymuty (namiary) pracujących obiektów rozpoznania pozyskane z posterunków rozpoznania elektronicznego.

2. Właściwości organizacyjne:

- struktura sieci i kierunków radiowych,
- sposoby i częstotliwość zmian danych radiowych,
- kryptonimy, znaki rozpoznawcze, znaki służbowe, umowne frazy (skróty) i kody używane w korespondencji radiowej,
- natężenie ruchu w relacjach radiowych przeciwnika.

Wyszczególnione powyżej parametry stanowią bazę informacyjną do identyfikacji źródeł z obiektami rozpoznania, określenia ich położenia i składu. Pozyskane dane stanowią podstawę do odtworzenia elektronicznych aspektów sytuacji pola walki w obszarze odpowiedzialności. Uzyskanie pożądanych efektów w procesie przetwarzania danych możliwe jest tylko dzięki wcześniejszemu zgromadzeniu odpowiedniej ilości treści informacyjnych rozpoznania studyjnego[30].

Na podstawie zbioru pozyskanych informacji zmiana dyżurna grupy kierowania prowadzi na bieżąco, jako graficzny obraz pola walki o spektrum elektromagnetyczne, mapę informacyjną. Najczęściej nanoszone są następujące obiekty elektroniczne przeciwnika:

---

[30] Szerzej zob. J. Jańczak (red.), W. Scheffs, *Walka radioelektroniczna w działaniach taktycznych*, Warszawa 1999.

- stanowiska dowodzenia związków taktycznych, oddziałów i pododdziałów,
- punkty i ośrodki kierowania artylerią polową i przeciwlotniczą,
- wysunięte punkty naprowadzania lotnictwa,
- punkty (stanowiska) kierowania rozpoznaniem i walką elektroniczną,
- inne obiekty elektroniczne nakazane przez przełożonego.

Końcowym wynikiem procesu analizy jest zbiór danych przesyłanych do G-2 związku taktycznego, zawierający graficzno-tekstowy opis odtworzonych fragmentów sytuacji pola walki w rozpoznawanym obszarze.

Dla potrzeb dowodzenia i kierowania pracą bojową organizowana jest sieć informacyjna kompanii radioelektronicznej oparta na łączności radiowej, radioliniowej i przewodowej.

Ugrupowanie bojowe kompanii radioelektronicznej organizowane jest z całości posiadanych sił i środków na pozycjach bojowych, nie pozostawiając żadnych środków w odwodzie. Rozmieszczenie elementów podsystemu warunkowane jest szeregiem czynników, do których zalicza się:

- sytuację operacyjno-taktyczną, w tym szczególnie rodzaj działań taktycznych,
- sytuację w przestrzeni elektromagnetycznej obszaru walki,
- zakres zadań kompanii,
- rozmieszczenia rozpoznawanych obiektów elektronicznych, w tym środków łączności radiowej podlegających zakłócaniu,
- warunki terenowe i atmosferyczne wpływające na rozprzestrzenianie się fal elektromagnetycznych.

Na możliwości namierzania zasadniczy wpływ mają: techniczne parametry stosowanych urządzeń rozpoznawczych oraz wyszkolenie obsług. Istotnym czynnikiem decydującym o możliwościach bojowych kompanii radioelektronicznej, w tym głównie w zakresie rozpoznania i obezwładniania radioelektronicznego, jest sytuacja elektroniczna po stronie przeciwnika, a szczególnie intensywność pracy jego środków radiowych, ich podatność na

rozpoznanie i zakłócanie oraz związane z tym sposoby i zakres prowadzenia obrony informacyjnej.

Transformacja struktury organizacyjnej pododdziału na funkcjonalny podsystem rozpoznania i zakłócania, prowadzi do utworzenia następujących elementów ugrupowania bojowego (wariant.):

1. Punktu dowodzenia (PD) kompanii,
2. Radiowego centrum rozpoznawczego (RCR),
3. Podsystemu namierzania radiowego UKF (SN) złożonego z trzech posterunków namierzania radiowego (PN),
4. Podsystemu rozpoznania i namierzania radiolokacyjnych środków pola walki (SNRLok) złożony z trzech posterunków wykrywania środków i systemów radiolokacyjnych,
5. Grupy środków zakłóceń (GSZ) – posterunków zakłóceń radiowych (PZ).

Punkt dowodzenia kompanii, rozmieszcza się w centrum ugrupowania taktycznego, za pozycjami bojowymi grup stacji zakłóceń radiowych na głębokości 4-6 km od linii styczności wojsk. Punkt dowodzenia kompanii złożony jest ze stanowiska dowódcy kompanii oraz stanowiska grupy kierowania, które rozwijane są w oparciu o wozy sztabowe[31].

Radiowe centrum rozpoznawcze rozwija się w strefie taktycznej, zawsze w centrum ugrupowania kompanii radioelektronicznej w pobliżu centralnie rozmieszczonego posterunku namierzania (wariantowo w pobliżu punktu dowodzenia kompanii). Przewiduje się również rozwinięcie w pobliżu siebie wszystkich trzech elementów jednocześnie.

Pluton zakłóceń radiowych w ugrupowaniu bojowym[32] rozmieszcza się grupami stacji zakłóceń (w każdej grupie po jednej stacji zakłóceń UKF i jednej UKF pasma lotniczego) w odległości np. 3-6 km od linii styczności wojsk

---

[31] Zob. J Janczak, (red.) W. Walka elektroniczna w działaniach związku taktycznego, AON, Warszawa 2000.

[32] Jako warianty przewiduje się rozmieszczanie grup środków zakłóceń z większym lub mniejszym rozproszeniem lub też pojedynczych stacji zakłóceń (np. przy konieczności rozmieszczenia stacji zakłóceń łączności lotniczej na kierunkach spodziewanych uderzeń lotnictwa taktycznego, nie pokrywających się z rejonem rozmieszczenia kompanii).

i z zachowaniem odległości między grupami 5-10 km. Przy czym warunki pracy określają, że odległość stacji zakłóceń w grupie powinna być nie mniejsza niż 300 m. Kolejnym ograniczeniem w tworzeniu ugrupowania jest konieczność zapewnienia warunków bezpieczeństwa pracy własnych systemów. Stąd wniosek, że w pobliżu nie mogą pracować węzły łączności (WŁ) wykorzystujące łączność UKF oraz środki rozpoznania radioelektronicznego UKF.

Pluton namierzania radiowego w ugrupowaniu bojowym kompanii radioelektronicznej rozwija dwa systemy (namierzania radiowego UKF po trzy posterunki każdy oraz rozpoznania i namiaru systemów radiolokacyjnych) w pasie 4-6 km od linii styczności wojsk i z zachowaniem odległości co najmniej 7-10 km pomiędzy sąsiednimi posterunkami (baza namierzania systemu złożonego z trzech posterunków wynosi 15-20 km i więcej).

Jako wariant standardowy realizowane jest często tworzenie zespołów funkcjonalnych na pozycjach bojowych. W tym celu rozmieszcza się razem posterunki namierzania radiowego i radiolokacyjnego. Zalecana odległość między stacjami (posterunkami), może wynosić 100-300 m.

2.3. Wyniki analizy struktury systemu rozpoznania

System rozpoznania w ciągu ostatnich lat znacznie poprawił swoje możliwości pozyskiwania informacji poprzez zwiększenie ilości źródeł danych. Jednak przeprowadzone badania wskazują, że efektywność systemu nie wzrosła w zakresie umożliwiającym zaspokojenie potrzeb użytkowników systemu, dotyczy to szczególnie przesyłania treści informacyjnych.

Perspektywiczny system rozpoznania to system mieszany osobowo-elektroniczny i powietrzno-lądowy o dużych możliwościach zdobywania informacji, jej przetwarzania oraz rozpowszechniania w systemach informatycznych oraz zdolny do realizacji zadań obrony informacyjnej. Przeprowadzone badania nad funkcjonowaniem sieci pozwoliły poznać zależności pomiędzy strukturą sieci informacyjnej taktycznego systemu

rozpoznania wojsk lądowych i jakością przepływu danych. Wśród negatywnych aspektów działania sieci informacyjnej wskazać należy brak:

a) środków automatyzacji pracy sztabowej,

b) sprawnych kanałów przysyłania danych,

c) urządzeń elektronicznego obrazowania sytuacji.

W rezultacie przeprowadzonych badań stwierdzono następujące fakty:

a) sieć informacyjna taktycznego systemu rozpoznania stanowi element składowy podsystemu rozpoznania wojsk lądowych, stąd jak wykazały badania, jako wydzielony element całości systemu determinuje jego funkcjonowanie;

b) modyfikacja struktur organizacyjnych w aspekcie potrzeb użytkowników poprawi efektywność systemu rozpoznania wojsk lądowych;

c) wystarczalność informacyjną użytkowników zapewni rozdzielenie strumienia informacyjnego oraz połączenie autonomicznych baz danych w jedną sieć informacyjną systemu rozpoznania wspartą technicznymi urządzeniami wspomagającymi;

d) wiarygodność i terminowość przesyłanych treści informacyjnych wzrośnie po wprowadzeniu technicznych środków przetwarzania danych.

Przeprowadzone badania wykazały również, że efektywność obiektu badań uwarunkowana jest szeregiem czynników. Do najważniejszych z nich zaliczono: strukturę organizacyjną systemu rozpoznania, otoczenie, dostępny system łączności (liczba i jakość kanałów informacyjnych), potrzeby informacyjne użytkowników, wyposażenie techniczne wspierające realizację procesów informacyjnych, zbiory danych oraz poziom merytorycznego przygotowania personelu.

Rezultatem pracy badawczej są opracowane i przedstawione w formie opisowej wnioski zmierzające do zwiększenia efektywności działania taktycznego systemu rozpoznania w następujących obszarach:

I. Modyfikacja struktur organizacyjnych

System rozpoznania wojsk lądowych stanowią, w aspekcie technicznym, dwa podsystemy: podsystem łączności i podsystem przetwarzania danych. Stworzenie silnej i zintegrowanej sieci informacyjnej wymaga przebudowy istniejących struktur oraz kompleksowego zabezpieczenia technicznego. Nowa architektura sieci informacyjnej umożliwi sprawniejsze kierowanie systemem rozpoznania taktycznego, co w konsekwencji poprawi jego skuteczność w zakresie pozyskiwania wiarygodnych i terminowych treści informacyjnych.

Narzędziem umożliwiającym spełnianie zadań przez rozpoznanie jest zautomatyzowany system zdobywania, przetwarzania i przesyłania danych, obsługiwany przez wyspecjalizowany kadrowy zespół wykorzystujący sprawne kanały transmisji danych. Zebrane w czasie obserwacji fakty świadczą, że w związku ze wzrastającą ilością danych ich zbieraniem powinny zajmować się odpowiednie elementy funkcjonalne zintegrowanego zespołu rozpoznania, zdolne do przetwarzania otrzymywanych zbiorów informacyjnych. Napływające dane mogą być dostarczane w różnej formie (graficznej, pisemnej, słownej) konieczne więc jest wyposażenie stosownych komórek w specjalistyczny sprzęt techniczny.

Przeprowadzone badania wykazały również, że aby uzyskać potrzebne dane z wewnętrznych i zewnętrznych źródeł rozpoznania w wyznaczonych strefach, należy posiadać odpowiednią ilość elementów zbierania informacji (dysponujących odpowiednimi urządzeniami pozyskiwania danych o dużym stopniu wiarygodności i dokładności). Ilość elementów rozpoznawczych powinna być zwiększana proporcjonalnie do stopnia zagrożenia lub poziomu intensyfikacji działań przez wojska potencjalnego przeciwnika. W zakresie gromadzenia zbiorów informacyjnych o przeciwniku celowe jest zorganizowanie komórki specjalistycznej, która będzie się zajmowała ich dystrybucją. Otrzymane rezultaty badań wskazują na potrzebę stworzenia jednolitego podsystemu dystrybucji danych o przeciwniku dla różnych użytkowników (rażenie, zakłócanie, obezwładnianie) w czasie zapewniającym właściwe wykorzystanie posiadanych zasobów informacyjnych.

Wyniki badań potwierdzają tezę, że aby zintegrowany system rozpoznania był skuteczny, konieczna jest ścisła koordynacja między operacyjnymi i taktycznymi poziomami dowodzenia oraz ośrodkami kierowania rozpoznaniem rodzajów wojsk. Przestrzeganie zasady współdziałania różnych poziomów dowodzenia (aspekt pionowy) i zasad współpracy równorzędnych (aspekt poziomy), powinno być zawarte w dokumentach normatywnych.

II. System łączności:

Możliwości systemu rozpoznania wojsk lądowych nie można rozpatrywać w oderwaniu od struktury systemu łączności. Nieodzowny dla dowodzenia rozpoznaniem jest ciągły dopływ danych realizowany przez nowoczesne systemy łączności. Na współczesnym polu walki, ogromnej liczby danych niezbędnych w procesie podejmowania decyzji nie można już przekazywać sposobem tradycyjnym. Dynamika działań będzie wymagać szybszego przekazywania dużych zbiorów, a więc decydującą rolę będzie odgrywać czynnik czasu. Stąd też wynika konieczność komputerowego sterowania strumieniem danych w automatycznym systemie łączności. Wprawdzie słowna wymiana treści informacyjnych będzie praktykowana także w przyszłości, to jednak będzie to miało miejsce wyłącznie na wyższych szczeblach, w celu wymiany poglądów i osobistego informowania dowódcy. Natomiast jak wykazały badania, zbiory danych istotne dla procesu dowodzenia będą wyrażane w formie alfanumerycznej lub graficznej na wskaźnikach zobrazowania elektronicznego.

Nie mniej istotne jest zapewnienie skrytości przekazywania danych. Dzięki zastosowaniu techniki cyfrowej obniżeniu ulegną koszty utajniania. Zebrane fakty wskazują, że wzrośnie efektywność transmisji danych oraz odporność na zakłócanie toru informacyjnego. Jak wykazano w procesie badań, większość europejskich państw NATO wprowadziła już do wyposażenia swoich wojsk systemy o podobnej technice lub rozpoczęła ich modernizację. Głównym jednak problemem jest zapewnienie kompatybilności systemów łączności, która pozwoli uniknąć w przyszłości dodatkowych kosztów ponoszonych na urządzenia zapewniające połączenia z sieciami partnerskimi. Zmienione

i rozszerzone spektrum zadań dla wojsk rozpoznawczych wymaga posiadania uniwersalnych sieci łączności zdolnych do szybkiej zmiany swojej struktury, a przede wszystkim sieci zdolnych do współpracy z systemami pracującymi według innych standardów, zapewniających dowodzenie podsystemami rozpoznania na małych, średnich, dużych i bardzo dużych odległościach.

Szybki rozwój technologiczny powoduje zwiększenie przepustowości kanałów łączności, co w konsekwencji umożliwia przetwarzanie i korzystanie z większej liczby danych, w krótkim czasie. Przeprowadzone badania wskazują na konieczność ustalenia szczegółowych reguł i zasad regulujących zarówno napływ danych, jak też odpowiednie wyposażenie węzłów informacyjnych w środki ich transmisji i przetwarzania. Wprowadzenie zmian technicznych w systemie łączności, wpłynie na sprawność analizy i syntezy danych szczegółowych, a w efekcie przygotowanie treści informacyjnych użytecznych do podejmowania decyzji. Taki uogólniony wniosek, w aspekcie rozpoznania, pokazuje rozmiary zadań, jakie muszą realizować sieci informacyjne, aby mogły sprostać wszystkim potrzebom taktycznego systemu rozpoznania.

Tworząc technicznie nową sieć informacyjną z zastosowaniem systemów informatycznych, powinno się dążyć do tworzenia wielokanałowego systemu łączności. Badania wskazują, że nie bez wpływu na jakość sygnału informacyjnego pozostaje niezawodność łączy, obciążenie sieci i charakterystyka techniczna kanałów przesyłowych, stąd też przyszłościowa sieć informacyjna powinna być zdolna przesyłać zdobyte dane w postaci zakodowanych sygnałów na duże odległości bez zniekształceń i w czasie zbliżonym do rzeczywistego.

Zebrane fakty potwierdzają, że największym problemem w zapewnieniu łączności w systemie rozpoznania jest przekazywanie danych zdobytych przez elementy rozpoznawcze natychmiast po ich pozyskaniu. Konieczne jest, aby do jednego węzła informacyjnego spływały zbiory danych od różnych źródeł. Tymczasem wyniki badań wskazują, że każdy element rozpoznawczy wojsk lądowych dysponuje środkiem łączności o zbliżonych parametrach technicznych, co utrudnia sprawną komunikację.

W rezultacie przeprowadzonych badań stwierdzono, że system łączności jest rozbudowany organizacyjnie. Tworzą go w zdecydowanej większości kanały radiowe oraz przewodowe. Ze względu na duże odległości działania elementów rozpoznawczych konieczne jest wykorzystywanie łączności KF i łączności radioliniowej. Do zapewnienia utajnionej łączności wielokanałowej służyć ma zespół radiostacji zapewniających naziemną i lotniczą wymianę danych. Wiele problemów w zakresie łączności wynika również ze specyfiki terenu, w jakim prowadzone są działania rozpoznawcze, z jego ukształtowania, pokrycia roślinnością oraz zakresem urbanizacji.

W problematyce badań dotyczących systemu łączności uwzględniono także wozy dowodzenia na potrzeby rozpoznania, które obecnie nie spełniają wymagań użytkowników. Oczekują oni małego, mobilnego i funkcjonalnego terminalu rozpoznawczego zamontowanego na pojeździe terenowym lub transporterze opancerzonym. Mobilne węzły informacyjne taktycznego systemu rozpoznania pozwolą na pełne kontrolowanie sytuacji bojowej na polu walki i natychmiastowe reagowanie na zmiany w ugrupowaniu bojowym przeciwnika.

Prowadzone w armii amerykańskiej eksperymenty potwierdziły realność tych oczekiwań i przydatność tego typu węzłów informacyjnych w czasie ćwiczeń[33]. Działanie eksperymentalnego, rozpoznawczego węzła informacyjnego obserwowano po zainstalowaniu wyposażenia w brygadowym wozie dowodzenia rozwiniętym w polowych warunkach w Fort Benning. W czasie ćwiczeń nowy wóz dowodzenia, zapewniał duże możliwości transferu danych na szczebel brygady. Według opinii ekspertów amerykańskich w przeciwieństwie do dotychczasowych rozwiązań wzrosła sprawność informacyjna ćwiczącej brygady. Eksperymentalny moduł informacyjny korzystał z mobilnego systemu łączności radiowej, systemu radiostacji do łączności ze środkami powietrznymi oraz z satelity taktycznego.

III. Wyposażenie techniczne:

---

[33] Zob. *Military Intelligence*, 1994, nr 7-9, s. 25-27.

Wiedza i doświadczenie oficerów rozpoznania mają duże znaczenie. Jednak nie mniej istotne jest wykorzystanie odpowiednich narzędzi wspomagających prowadzone prace na informacjach.

Przeprowadzone badania potwierdzają tezę, że wprowadzenie urządzeń technicznych wpłynie na sprawniejsze przekazywanie pomiędzy elementami sieci informacyjnej taktycznego systemu rozpoznania posiadanych i pozyskiwanych zbiorów danych. Zastosowanie elektronicznych przetworników danych w sieci informacyjnej podniesie poziom obsługi użytkowników poprzez:

- zwiększenie efektywności przepływu danych stosownych do potrzeb użytkownika,
- podniesienie poziomu wiarygodności treści informacyjnych uzyskane dzięki aktualizacji baz danych,
- obniżenie kosztów ekonomicznych przesyłania dużych zbiorów danych w ciągu krótkiego czasu

Dla sprawnego funkcjonowania taktycznej sieci informacyjnej niezbędne jest zapewnienie wewnętrznej i zewnętrznej zgodności gromadzenia i dystrybucji treści informacyjnych, służących zaspokojeniu potrzeb użytkowników. Każdy węzeł informacyjny, posiadając własną bazę danych, dostosowaną do potrzeb użytkownika, może zwiększyć efektywność sieci informacyjnej poprzez szybsze w czasie i, co za tym idzie, aktualniejsze przesyłanie danych. W związku z tym konieczne jest przyjęcie jednolitych zasad gromadzenia i przekazywania zbioru danych do różnych węzłów informacyjnych. Problem ten może stanowić przedmiot dalszych badań.

W procesie prowadzonych badań stwierdzono ponadto, że zapewnienie właściwej pracy sieci informacyjnej może nastąpić również w wyniku elektronicznego śledzenia efektów oraz potrzeb użytkowników. Jak wynika z przeprowadzonych badań, utrzymanie spójności systemu w każdej fazie przetwarzania danych staje się warunkiem koniecznym do uzyskania zamierzonego efektu końcowego. Jednym z technicznych warunków skuteczności działania sieci informacyjnej taktycznego systemu rozpoznania jest

wykorzystanie elektronicznych systemów przetwarzania. Przetwarzanie danych w nowoczesnych systemach elektronicznych umożliwia[34]:

- automatyczną identyfikację i klasyfikację sygnału informacyjnego,
- automatyczne utajnianie przesyłanych w sieci komputerowej danych,
- małe opóźnienie informacyjne w strukturze systemu,
- komputerowe zobrazowanie sytuacji pola walki z wykorzystaniem cyfrowej mapy terenu,
- rozbudowane procedury i algorytmy do szacowania sytuacji taktycznej w rozpoznawanym terenie oraz zobrazowania wyników z różnym stopniem szczegółowości rozpoznania na ekranie monitora (graficznego lub alfanumerycznego),
- automatyczne przesyłanie w sieci komputerowej (w postaci zakodowanej) do uprawnionych użytkowników rozkazów, meldunków i komunikatów,
- dublowanie funkcji z pominięciem określonego szczebla w przypadku wyeliminowania jednego z uczestników walki

Przeprowadzone badania wskazują, że złożoność procesu modyfikacji systemu rozpoznania wojsk lądowych jest uwarunkowana szeregiem czynników. Na podstawie otrzymanych wyników, za szczególnie ważne w zapewnieniu właściwego funkcjonowania sieci informacyjnej uznać należy poniższe problemy:

a) w sferze organizacyjnej:

- Utworzenie jednolitego systemu rozpoznania osobowego i elektronicznego, zapewniającego współpracę z analogicznymi systemami funkcjonującymi w państwach NATO.
- Normatywne regulacje prawne z zakresu techniki, sposobu i terminów przekazywania zasobów organicznych baz danych (jednostek operacyjnych wojska, obrony terytorialnej, układu pozamilitarnego) do wykorzystania na potrzeby współdziałania i oceny zagrożenia.

---

[34] Microelectronics digital communications handbook, MITEL Corporation, Canada 1993.

- Poprawa efektywności sieci informacyjnej rozpoznania poprzez połączenie organizacyjne komórek sztabowych dokonujących oceny zagrożenia i prognozujących przyszły charakter działania potencjalnego przeciwnika. Dotyczy to szczególnie komórek specjalistycznych rodzajów wojsk i rodzajów sił zbrojnych.
- Zintegrowanie, w ramach sieci informacyjnej, wszystkich przydatnych źródeł rozpoznania.
- Zapewnienie wzajemnej wymiany informacji między współdziałającymi komórkami sztabowymi w zakresie: realizowanych zadań, położenia własnych elementów rozpoznawczych, sytuacji w wojskach przeciwnika.

b) w sferze technicznej:

- Automatyzacja procesu operacji na zbiorach danych.
- Upowszechnienie nowej sformalizowanej dokumentacji rozpoznawczej.
- Wprowadzenie specjalistycznych programów użytkowych z możliwością przekazywania treści informacyjnych w postaci tekstowej, graficznej i tabelarycznej, przeznaczonych dla określonych odbiorców w jak najkrótszym czasie operacyjnym.
- Zastosowanie automatycznych systemów utajniających przesyłanie danych w sieci rozpoznania taktycznego.

2.4. Wnioski ogólne

Efektywność sieci informacyjnej systemu rozpoznania zależna jest nie tylko od ilości użytkowników, lecz także od nowoczesnych technicznych środków rozpoznania, łączności oraz przetwarzania danych, opartych na osiągnięciach współczesnej techniki, telekomunikacji i informatyki. Tymczasem sprzęt łączności, będący w wyposażeniu taktycznego systemu rozpoznania wojskowego, jest sprzętem analogowym o zróżnicowanym czasie eksploatacji. Ze względu na wysokie koszty zakupu, musi być eksploatowany zgodnie z normami zużycia, co utrudnia wprowadzenie w jego miejsce nowych egzemplarzy i powoduje konieczność szukania rozwiązań alternatywnych –

tymczasowych, bazujących na zakupionych sposobem gospodarczym środkach łączności ogólnie dostępnych na rynku np.: radio CB i Motorola. Konieczne jest wykorzystywanie urządzeń dupleksowych opartych wyłącznie na systemie cyfrowym, z możliwością wymiany danych przez ich szyfrowanie w ruchu telefonicznym, telegraficznym i telekopiowym już od szczebla pododdziału rozpoznawczego. W pododdziałach rozpoznawczych ze względu na czas przekazu danych celowe jest wprowadzenie urządzeń telefonicznych z wybieraniem bezpośrednim pozwalającym na realizację połączeń priorytetowych. Podniesienie efektywności funkcjonowania sieci informacyjnej może nastąpić poprzez wprowadzenie nowoczesnego, odpornego na zakłócenia sprzętu łączności, nawigacji, wskazywania celów i naprowadzania środków rażenia do podstawowych elementów rozpoznawczych podsystemu rozpoznania ogólnowojskowego

Pododdziały rozpoznawcze na poziomie taktycznym powinny być szkolone i wyposażone do działania w ugrupowaniu przeciwnika na zasadach grup dalekiego rozpoznania, jakie funkcjonują w strukturach jednostek NATO. Dlatego dążyć należy jednocześnie do przywrócenia rozpoznania specjalnego, dostrzegając w tym rozwiązaniu wiele istotnych zalet wpływających na poprawę funkcjonowania systemu rozpoznania.

Konieczne jest posiadanie sił i środków rozpoznawczych w strukturach batalionów zmechanizowanych i czołgów. Pozwoli to na zwiększenie możliwości rozpoznania i zapewni stały napływ aktualnych informacji o przeciwniku i środowisku pola walki.

Poprawę możliwości funkcjonowania systemu rozpoznania w aspekcie rażenia ogniowego (ogniem artylerii i śmigłowców) należy upatrywać w rozwoju infrastruktury technicznej poszczególnych źródeł rozpoznania i sztabowych zespołów przetwarzających informacje. Nadrzędną zasadą powinno być przekazywanie informacji do zainteresowanych dysponentów środków rażenia w autonomicznej sieci informacyjnej. Urzeczywistnienie tej tezy wymaga wyposażenia pododdziałów rozpoznawczych w środki precyzyjnej lokalizacji

celów i natychmiastowej transmisji pozyskiwanych danych, w myśl koncepcji walki sieciocentrycznej.

Skuteczność funkcjonowania systemu rozpoznania można poprawić poprzez zwiększenie samodzielności dowódców pododdziałów rozpoznawczych. Drogą ku temu jest unikanie nadmiernej szczegółowości stawianych zadań do określenia rejonu działania pododdziałów rozpoznawczych (stref, kierunków lub obiektów) oraz rodzaju i czasu pozyskania określonych wiadomości o przeciwniku i terenie.

W zakresie rozpoznania radioelektronicznego należy wskazać, że na możliwości namierzania zasadniczy wpływ mają: techniczne parametry stosowanych urządzeń rozpoznawczych oraz wyszkolenie obsług. Istotnym czynnikiem decydującym o możliwościach bojowych kompanii radioelektronicznej, w tym głównie w zakresie rozpoznania i obezwładniania radioelektronicznego, jest sytuacja elektroniczna po stronie przeciwnika, a szczególnie intensywność pracy jego środków radiowych, ich podatność na rozpoznanie i zakłócanie oraz związane z tym sposoby i zakres prowadzenia obrony informacyjnej. Tymczasem kompania radioelektroniczna ZT nie posiada środków do rozpoznawania i obezwładniania relacji radiowych z rozproszonym widmem (emisji typu frequency hopping – FH). Stąd istotnego znaczenia w prowadzeniu walki elektronicznej przez ZT nabiera problem stosowania innych środków, jak np. uderzenia nadajnikami zakłóceń jednorazowego użytku. Brak nowoczesnych środków łączności radiowej zapewniających pracę sieci rozpoznania, namierzania i zakłócania powoduje, że wydłużeniu ulega czas przekazu i przetwarzania danych pozyskiwanych w podsystemie rozpoznania radioelektronicznego

Przeprowadzona analiza stanu jakościowego i ilościowego sił i środków rozpoznania artyleryjskiego na szczeblu oddziału, wskazuje na dużą dysproporcję w zakresie możliwości pozyskiwania danych na potrzeby prowadzenia w stosunku do możliwości oddziaływania ogniowego środków rażenia. Wyniki badań dowodzą, że aktualnie środki rozpoznania artyleryjskiego mogą prowadzić rozpoznanie jedynie na potrzeby artylerii wykonującej zadania

bezpośredniego wsparcia ogniowego (na głębokość od 5 do 7 km, a wyjątkowych warunkach do 10 km). Przy obecnym technicznym wyposażeniu nie mają one żadnych organicznych możliwości rozpoznania obiektów położonych w głębi operacyjno-taktycznej. Ponadto możliwości rozpoznania powietrznego i elektronicznego nie spełniają zakładanych przez artylerię wymagań w zakresie określenia położenia celów z wymaganą dokładnością i w związku z powyższym pozyskiwane dane nie mogą zostać wykorzystane do rażenia ogniowego. Doświadczenia wojen i konfliktów lokalnych pozwalają na postawienie tezy, że siły i środki rozpoznania artyleryjskiego powinny umożliwiać penetrację ugrupowania przeciwnika na głębokość dwu- a nawet trzykrotnie większą od zasięgu środków rażenia danego szczebla dowodzenia. Uzyskany w ten sposób czas operacyjny zostanie wykorzystany na zaplanowanie kolejnych uderzeń ogniowych. Pożądanym kierunkiem zmian jest wprowadzenie do użytku bezpilotowych środków rozpoznania, nowych stacji radiolokacyjnych i radarów obserwacji pola walki.

Wydaje się, że jakość sieci informacyjnej taktycznego systemu rozpoznania skażeń można poprawić poprzez:

- wyposażenie elementów strukturalnych systemu w urządzenia do automatycznego wykrywania i określania parametrów wybuchów jądrowych, w tym również powietrznych;
- wprowadzenie do wyposażenia pododdziałów rozpoznania skażeń przyrządów umożliwiających automatyczne wykrywanie większej liczby środków toksycznych, w tym także przemysłowych;
- automatyzację pomiarów meteorologicznych;
- stworzenie sieci zintegrowanych, zautomatyzowanych i mobilnych stacji pomiarowych, umożliwiających równoległe wykonywanie pomiarów oraz automatyzację transmisji danych do nadrzędnych elementów systemu.

Wprowadzenie na szczebel związku taktycznego organicznych pododdziałów rozpoznania powietrznego (śmigłowców i środków

bezpilotowych) zwiększy wydajność informacyjną sieci i przyczyni się do wzrostu stopnia wiarygodności pozyskiwanych danych poprzez porównanie wyników rozpoznania pozyskiwanych z różnych źródeł powietrzno-lądowego systemu zdobywania danych. Wyniki analizy współczesnych typów śmigłowców rozpoznawczych wybranych państw NATO, wskazuje, że posiadają one w zakresie środków łączności 2-5 radiostacji KF i UKF przeznaczonych do współpracy z wojskowymi organami ruchu lotniczego, ośrodkami dowodzenia różnych rodzajów wojsk oraz na potrzeby kierowania ogniem[35]. Praktyka ćwiczeń i rozważania teoretyczne wskazują na potrzebę włączenia jednostek śmigłowców rozpoznawczych w strukturę organizacyjną związków taktycznych. Najczęściej spotykaną formą organizacyjną są eskadry śmigłowców rozpoznawczych w oddziałach śmigłowców związków taktycznych wojsk lądowych (WB, Francja, Niemcy). W USA natomiast śmigłowce rozpoznawcze zorganizowane są w kompanię rozpoznania powietrznego batalionu rozpoznawczego.

Autorzy pracy zdają sobie sprawę, że wiele interesujących problemów zostało tylko zasygnalizowanych, niektóre zjawiska tylko oszacowane i wymagają dalszych badań. Ze względu na trwający proces restrukturyzacji wojsk rozpoznawczych, zespół autorski ma również świadomość zmienności kontekstu badań. Zmienności, która uniemożliwia zakładanie trwałości uzyskanych wyników i sformułowanych wniosków. Kontynuacja dalszych badań w zakresie rozpoznania wojsk lądowych, koncentrować się powinna na opracowaniu:

a) systemu komputerowego wspomagania pracy komórki G-2,
b) wsparcia informatycznego w procesie przekazywania danych,
c) technicznej modernizacji kanałów informacyjnych,
d) pojazdu sztabowego na potrzeby taktycznego systemu rozpoznania.

---

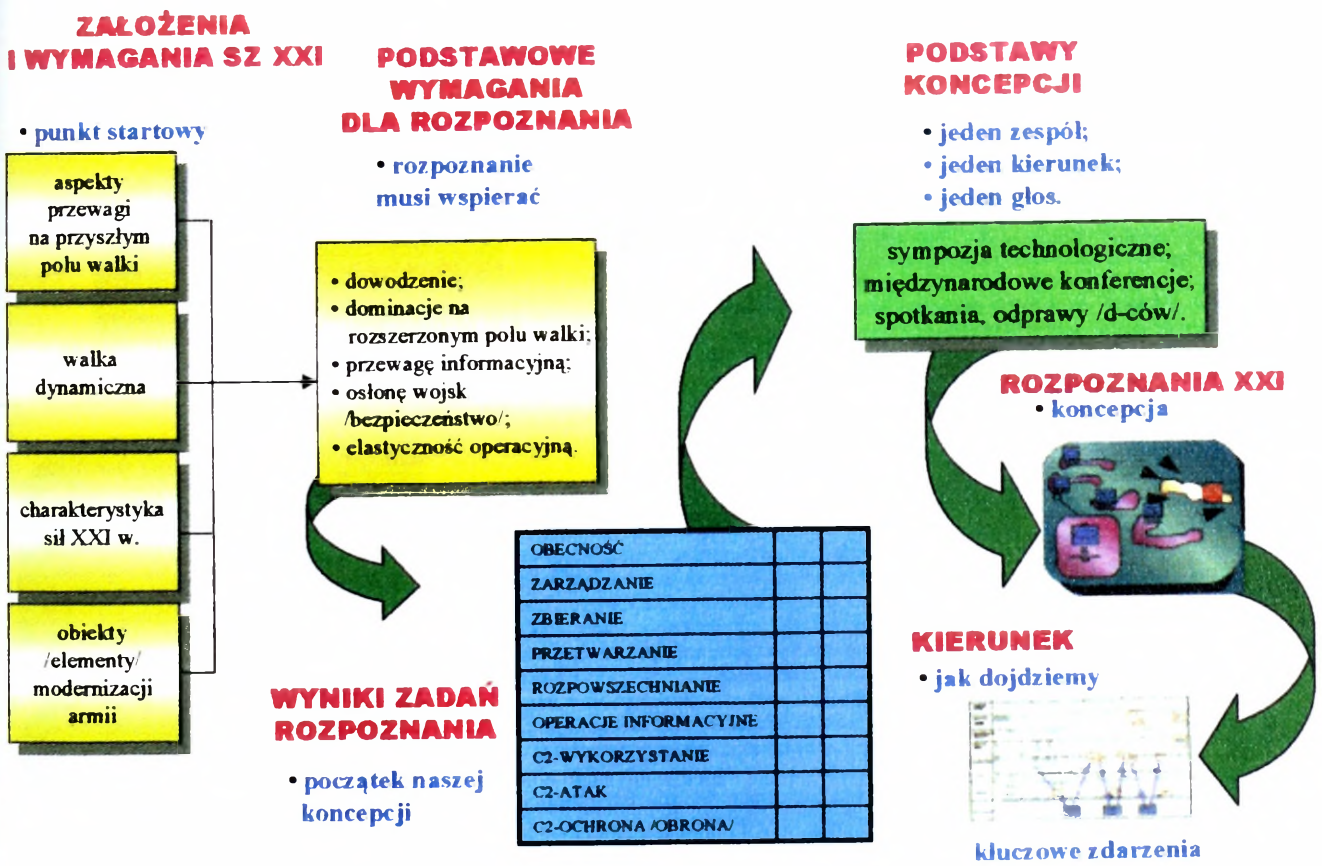
[35] Specjalistyczne śmigłowce rozpoznawcze to: OH–6A, OH–58A, Gazelle, BO–105M.

Uzupełnienia i pogłębienia wymaga problematyka wpływu procesu przygotowania kadry do realizacji zadań w nowych strukturach organizacyjnych. Należy również zastanowić się nad potrzebą i możliwością opracowania i stosowania standardów edukacyjnych dostosowanych do stanowisk służbowych, stworzenia systemu zapewniającego jakość kształcenia zawodowego oraz możliwością wykorzystania doświadczeń szkolnictwa wojskowego państw NATO.

Wnioski z badań mogą być wykorzystane w procesie modernizacji taktycznego systemu rozpoznania oraz w działalności dydaktycznej. Autorzy pracy mają nadzieję, że przedstawiony materiał będzie kolejnym elementem w tworzeniu nowoczesnego systemu rozpoznania. Wyniki badań mogą być w przyszłości przyczynkiem zmian racjonalizujących funkcjonowanie systemu rozpoznania oraz przyczynią się do upowszechnienia poruszanej problematyki wśród kadry pionu rozpoznania wojskowego.

3. PROGNOZA ROZWOJU SYSTEMU ROZPOZNANIA XXI WIEKU

Z przeprowadzonych rozważań (w rozdziale pierwszym i drugim) wynika, że decydujący wpływ na tworzenie perspektywicznego systemu rozpoznania mają założenia i wymagania dotyczące Sił Zbrojnych[1] XXI wieku oraz przewidywane modele działań (operacji) (rys. 3.1). Z nich to właśnie wynika główny cel a tym samym podstawowe założenia i wymagania oraz koncepcja systemu rozpoznania wojskowego.



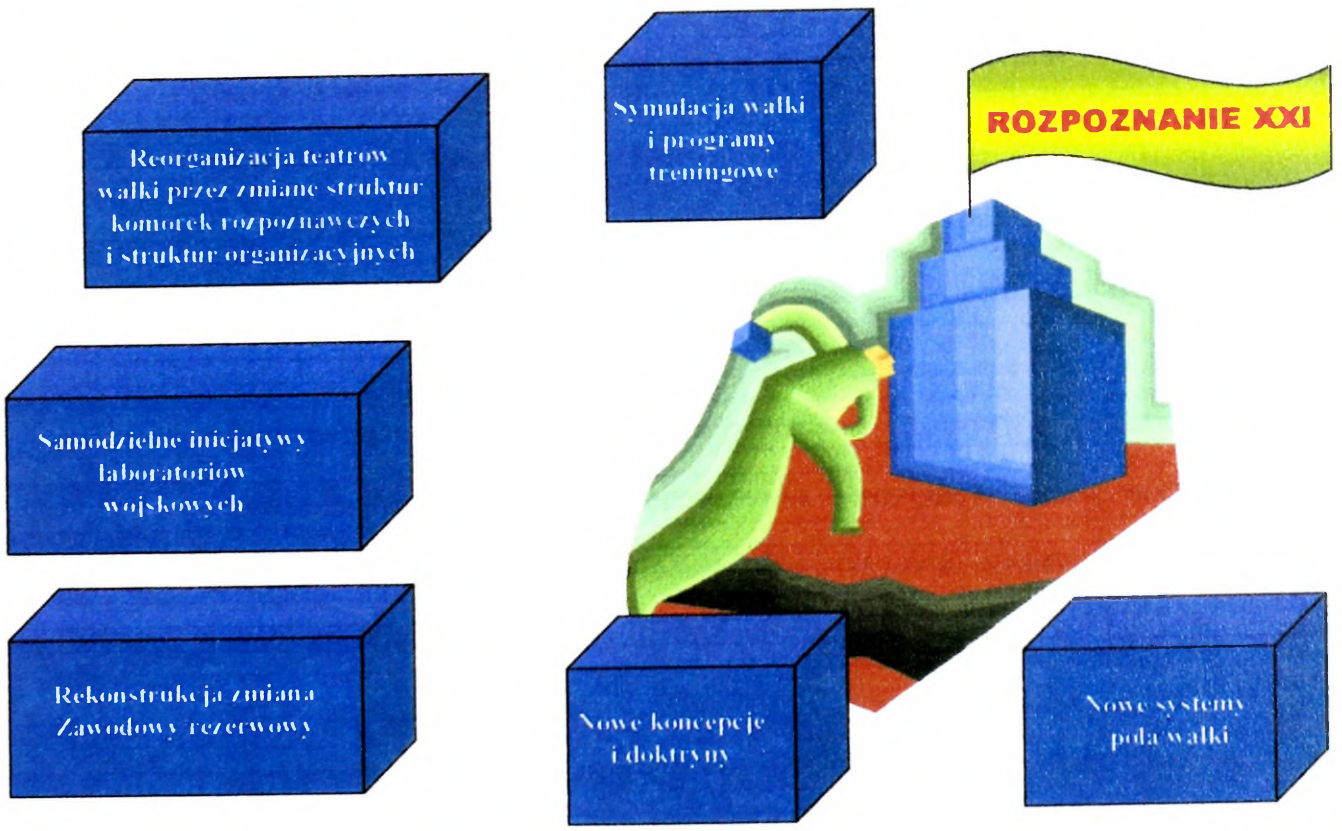
Rys. 3.1. Założenia rozpoznania wojskowego XXI wieku

[1] Są to wymagania zawarte w Koncepcji Strategicznej Sojuszu oraz decyzje Praskiego szczytu NATO o kierunkach transformacji sojuszu, jak również decyzje kopenhaskiego szczytu Unii Europejskiej o dalszych reformach i rozwoju tożsamości Unii jak również „Strategii bezpieczeństwa narodowego RP" z 22 lipca 2003 roku, uzupełniona Strategią wojskową RP a ponadto „Programem rozwoju SZ na lata 2005-2010".

3.1 KONCEPCJA NOWEGO SYSTEMU ROZPOZNANIA

Aktualnie istniejący system rozpoznania wojskowego jest skutkiem tworzenia (to znaczy planowania i organizowania) w okresie ostatnich dziesięcioleci. Jest on zdolny do pozyskiwania danych (informacji) dla wojsk z bardzo ograniczonymi możliwościami, musi jednak posłużyć jako baza dla ewolucyjnego rozwoju systemu rozpoznania wojskowego dla potrzeb SZ XXI wieku. Pełny sukces może być osiągnięty poprzez realizację następujących przedsięwzięć (rys. 3.2):

- powstanie całej rodziny nowoczesnych interoperacyjnych systemów, (rozpoznania, nadzorowania obszaru działań, określania położenia celów wysokoopłacalnych, wysokowartościowych itp.);



Rys. 3.2. Tworzenie systemu rozpoznania wojskowego XXI wieku

- integracji innych systemów z systemem rozpoznania dla pozyskania większych możliwości zdobywania danych (informacji) i pełnej interoperatywności systemu;
- przygotowania systemu rozpoznania wg nowej koncepcji prowadzenia działań (operacji);
- doskonalenie współpracy między czynnym stanem osobowym rozpoznania wojskowego a rezerwami przewidywanymi do jego wzmocnienia;
- reorganizacji teatru działań poprzez organizację wielopoziomowych baz danych i poziomów rozpoznania;
- opracowanie problematyki zagrożeń wojną informacyjną wynikającymi z narodowej doktryny informacyjnej państwa (musi być opracowana);
- tworzenie nowych symulacyjnych systemów treningowych w wersji indywidualnej, zespołowej lub całych jednostek, w ramach operacji (działań) połączonych, wielonarodowych itp., jednocześnie realistyczne przedstawianie tego, co może, a czego nie może osiągnąć rozpoznanie w obecnym i przyszłym kształcie.

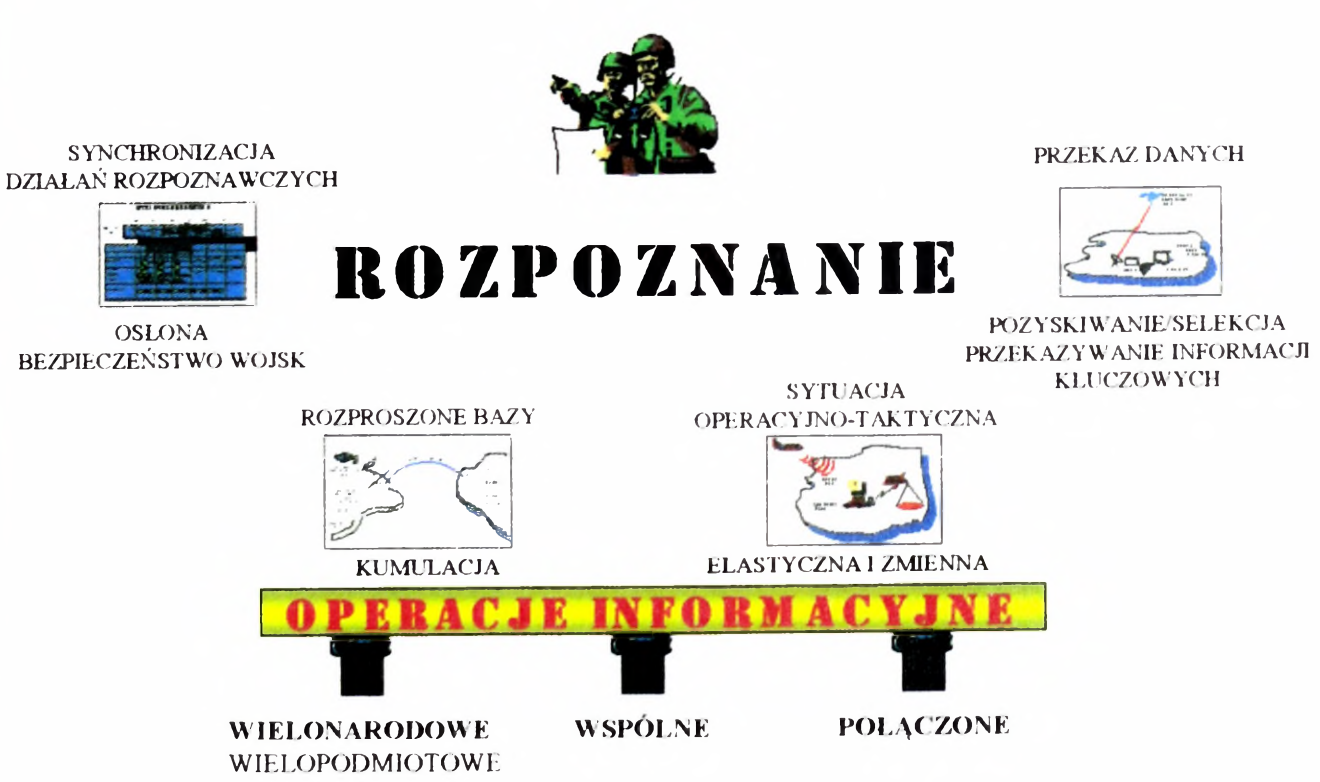
Ponadto, system ten powinien być zgodny z wytycznymi naszej aktualnej doktryny rozpoznawczej[2] oraz Sojuszu a ponadto powinien kierować się następującymi kryteriami (rys.3.3):

1. ***Dowódca kieruje rozpoznaniem*** - dowódca musi zdefiniować „Zasadnicze Potrzeby Informacyjne Dowódcy[3]", cele wysokoopłacalne oraz terminy a także przewidzieć wysiłek systemu rozpoznania we wszystkich elementach ugrupowania bojowego (rzutach). Rozpoznanie musi ponadto poznać i zrozumieć system walki przeciwnika, jego możliwości, ograniczenia, zasady wykorzystania systemu ognia, manewru itp.
2. ***Synchronizacja rozpoznania*** - powoduje nowy sposób zarządzania cyklem rozpoznania. Sprowadza się ona do potrzeb dowódcy - co, gdzie i kiedy potrzebuje on wiedzieć, aby mógł zrealizować swoje zadanie

---

[2] *Rozpoznanie Wojskowe*, Szt. Gen. 1531/2001, Warszawa 2001
[3] Tamże, s. 8.

(koncepcję). Dowódca i zwiadowcy muszą zrozumieć plan działań przełożonego a w nim widzieć kontekst przeprowadzenia operacji informacyjnych. Zwiadowcy muszą także przewidzieć kiedy dowódca będzie potrzebował specjalnych informacji do przeprowadzenia ataku na cele specjalne. Aby uzyskać sukces powinni także znać możliwości i ograniczenia sił i środków systemu rozpoznania, nadzorowania obszaru działań i określania celów wysokoopłacalnych w zakresie realizacji priorytetowych potrzeb rozpoznawczych dowódcy. Jednocześnie należy zaznaczyć że, przy szybko zmieniających się wymaganiach współczesnego obszaru działań, *zwinność i ruchliwość* to klucz dla systemu rozpoznania aby mógł szybko dokonać przegrupowania sił i środków.



Rys. 3.3. Kryteria doktrynalne rozpoznania wojskowego

3. ***Modułowa baza operacyjna*** - jest trzecim elementem doktryny. W strukturze sił projektowanych działań, szybkość jest zasadą pozyskiwania efektów. Dowódca musi tak rozmieścić elementy rozpoznawcze aby pokryły główny ciężar działań - kierunek głównego wysiłku. Rozpoznanie powinno być elastyczne i gotowe do pozyskiwania danych źródłowych w realnym czasie po czym schronienia się w przygotowanym miejscu. Organizacja rozpoznania w działaniach (operacjach) powinna zabezpieczyć umiejętne skoncentrowanie sił a następnie ich rozproszenie.
4. ***Taktyczne ugrupowanie*** - jest rozwinięciem koncepcji działań (operacji) realizowanych na poziomie modułu (zespołu rozpoznawczego). Możliwości modułu powinny być zmienne w zależności od rozmiaru i składu, oraz czasu trwania działań bojowych. Podstawowym elementem, który wpływa na możliwości rozpoznawcze ugrupowania bojowego jest wg nazwy doktrynalnej Patrol Rozpoznawczy[4] i często obejmuje on organiczne jak i nieorganiczne siły.
5. ***Przekazywanie danych rozpoznawczych*** to 5 kryterium, zawierająca w sobie dwa kluczowe działania:
    a. bezpośrednią transmisję nieobrobionych danych/informacji pozyskiwanych z wielu źródeł i czujników ograniczoną tylko do zasadniczych potrzeb dowódcy;
    b. łatwy dostęp do informacji rozpoznawczych i bazy danych wymaga wykwalifikowanego personelu, wyposażonego i wspartego systemami zapewniającymi automatyczną i bezpieczną komunikację.

Aby przedstawione kryteria mogły się urzeczywistnić, system musi posiadać następujące możliwości:

- prowadzenie w szerokich obszarach wielospektralnego nadzorowania obszaru działań (ląd, morze, powietrze, kosmos, cyberprzestrzeń);

---

[4] *Działania rozpoznawcze*, Tymczasowa instrukcja, DWLąd. Wewn. 17/2002, Warszawa 2002, s. 23

- zespolenie w jeden system działań rozpoznawczych „od podstawy po szczyt" ugrupowania przeciwnika;
- wizualne zobrazowanie sytuacji na obszarze działań;
- określanie, lokalizację i identyfikację celów wysokoopłacalnych i wysokowartościowych;
- interoperacyjny dostęp do informacji w czasie prowadzenia operacji połączonych lub wielonarodowych;
- działania z zakresu walki w obszarze dowodzenia (C2W);
- prowadzenie działalności wspierającej siły zabezpieczające działania (operacje);
- udział w poszukiwaniu zaginionych itp.

3.1.1 WSPARCIE SYSTEMU ROZPOZNANIA DLA OPERACJI INFORMACYJNYCH

Działania na informacji zawsze były czynnikiem, który warunkował osiągnięcie powodzenia w prowadzonych działaniach. Jej znaczenie dostrzegli i dostrzegają wszyscy teoretycy, począwszy od Sun Tzu[5] (VI w. p.n.e.), poprzez generałów epoki napoleońskiej, aż do współczesnych dowódców i historyków. Jednak tylko niektórzy z nich nazywają ją w ten sposób : operacje informacyjne (*Information Operation*) lub wojna informacyjna (*Information Warfare*).

Dziś wiele się mówi o operacjach informacyjnych lub wojnie informacyjnej, choć nie zawsze specjaliści z tej dziedziny definiują ją tak samo. Niemiecki analityk wojskowy kmdr Niels Möller-Gulland[6] uważa, że obejmuje ona szeroki zakres poglądów: od bardzo futurystycznych wyobrażeń o tym, że wojna cybernetyczna (*Cyber War*) lub wojna w systemach sieciowych (*Net War*) mogłaby zastąpić wojnę niosącą cierpienia i śmierć, aż po konserwatywne - dowodzące, że przedsięwzięcia te można by zaliczyć do form tradycyjnej wojny, po zmodyfikowaniu ich odpowiednio do rozwoju technologicznego.

---

[5] Sun Tzu w traktacie Sztuka wojny (s. 8) pisał: „Poznaj siebie i poznaj wroga, dopiero wtedy twoje zwycięstwo nie będzie zagrożone. Poznaj warunki terenu i pogody, wtedy twoje zwycięstwo będzie całkowite". Chociaż w zapisie tym Sun Tzu nie używa pojęcia „operacje informacyjne" czy też „walka Informacyjna", to jednak pod względem merytorycznym wymienia jej wszystkie komponenty.

[6] Müller N., *Krieg im Informationszeitalter. Was ist neu?* w: „Schweizer Soldat" 1995, nr 11, s. 19.

Natomiast pracownik National Defence University w Waszyngtonie Martin Libicki[7] twierdzi z kolei: „*Jestem w stanie różne formy występowania Information Warfare pokroić w kosteczki, podzielić je, ugotować i upiec – zawsze jednak powstanie z tego rozmokłe (papkowate) danie jednogarnkowe. Informacja może obejmować wszystko - od pogłosek do superkomputerów a wojna obejmuje wszystkie ludzkie czynności - od poprawnego współzawodnictwa do śmiertelnego konfliktu.*". Można spotkać jeszcze inne definicje, np.: „*Operacjami informacyjnymi nazywamy działania, które mają doprowadzić do przewagi w dziedzinie informacyjnej przez ograniczenie dopływu informacji, dezorganizację działań podejmowanych na ich podstawie oraz oddziaływanie na systemy informatyczne przeciwnika. Z drugiej strony mają ochraniać własne systemy informacyjne, transmisję danych oraz zapewnić właściwą na ich bazie działalność dowództw.*[8]"

W doktrynie połączonej, „Rozpoznanie wojskowe[9]" (s. 33), operacje informacyjne definiowane są jako: „*przedsięwzięcia mające wpływ na podejmowanie decyzji politycznych i wojskowych poprzez oddziaływanie na informacje, podstawowe procesy informacyjne, systemy dowodzenia, kierowania, łączności i informatyki przeciwnika, a także chroniące własne informacje, procesu i systemy informacyjne*". Definicje ta zawierają tylko wojskowe aspekty. Ale i one nie wyczerpują wszystkich wariantów określenia „operacji informacyjnych".

W wojnie o Kuwejt (1991 r.) takich elementów działań zbrojnych nie traktowano jeszcze stricte jako operacji informacyjnych. Ich zastosowanie miało przede wszystkim zwiększyć skuteczność broni przeznaczonej do fizycznej likwidacji przeciwnika. Szacuje się, że prawdziwych operacji informacyjnych można oczekiwać dopiero w drugiej dekadzie XXI wieku.

Martin Libicki, mimo wątpliwości, podzielił operacje informacyjne na 7 form (elementów): *Command and Control War (C2W), Intelligence-Based War, Electronic War, Hacker War, Economic Information War, Cyber or Net War* oraz *Psychological Operations.*

---

[7] M. Libicki, *What is Information Warfare*, Washington 1995 r. passim.
[8] Tamże.
[9] Wyd. cyt...*Rozpoznanie wojskowe,* s. 33.

Command and Control War (C2W), czyli wojna w obszarze dowodzenia, z militarnego, punktu widzenia jest uważana za dominujący komponent operacji informacyjnych. Obejmuje wszelkie działania przeciwko centrom dowodzenia i urządzeniom kierowania na wszystkich szczeblach, z fizyczną ich likwidacją włącznie (niszczeniem). Jej celem jest pozbawienie przeciwnika zdolności dowodzenia, tzn. uzyskanie takiego stanu, w którym dowództwo przeciwnika zostanie pozbawione informacji lub otrzyma tylko fragmentaryczne dane o wojskach, które z kolei nie będą w stanie zrozumieć podejmowanych przez dowództwo decyzji.

W historii wojen oddziaływanie na dowództwa nie jest niczym nowym. Już w czasach antycznych wodzowie dążyli do tego, by pojmać wodza (najczęściej króla) obcego państwa lub unieszkodliwić go w inny sposób. Pod Trafalgarem hiszpański strzelec wyborowy trafił śmiertelnie admirała Horatio Nelsona (1756–1805). Japońska flota została pozbawiona dowódcy – admirała Isoroku Yamamoto (1884–1943), kiedy Amerykanie zestrzelili jego samolot nad Bougainville podczas bitwy o Wyspy Salomona. Po zadaniu ciosu egipskim strukturom dowodzenia 5 czerwca 1967 r. wojska izraelskie w ciągu czterech dni opanowały półwysep Synaj.

Ale i na tym odcinku zanotowano niepowodzenia. Były wielkie trudności z wyeliminowaniem z życia politycznego przywódcy Organizacji Wyzwolenia Palestyny Jasira Arafata, czy też libijskiego władcy Mu'ammara al-Kaddafiego lub dyktatora Kuby Fidela Castro. Uniknął likwidacji somalijski generał Muhammed Furah Aidid. Nie udało się zlikwidować w 2001 r. w Afganistanie największego terrorysty – Osamy bin Ladena. Dyktator Iraku Saddam Husajn został ujęty dopiero po upływie 8 miesięcy od zakończeniu działań wojennych w Iraku (2003r.).

Przez pojęcie *Intelligence-Based War (IBW)* rozumie się przedsięwzięcia, które służą optymalnemu zebraniu, zarejestrowaniu i przetworzeniu informacji niezbędnych do oceny sytuacji oraz do skutecznego użycia sił własnych. W formie pasywnej obejmuje ona sprzężenie wszystkich możliwych sensorów i źródeł informacji. Zalicza się do niej także tradycyjną formę zdobywanie wiadomości – szpiegostwo. Aktywne formy tej wojny obejmują przedsięwzięcia manipulacyjne sensorami przeciwnika, ich dezinformację oraz fizyczne niszczenie. Martin Libicki przewiduje w nich udział: satelitów, sensorów akustycznych i sejsmicznych (*far stand-off sensors*); aparatów

bezzałogowych, naziemnych stacji radiolokacyjnych, pław morskich itp. (*near stand-off sensors*) oraz czujników akustycznych, grawimetrycznych, optycznych i biochemicznych (*in-place sensors*). Zalicza też do nich tzw. *weapon sensors - reflected radar, light-detection* itp.

Electronic Warfare według Nielsa Möllera-Gullanda - to nic innego, jak wojna elektroniczna skierowana przeciwko wrogim środkom oraz systemom dowodzenia i łączności z jednoczesną ochroną własnych środków elektronicznych. Ma on na uwadze przede wszystkim elektromagnetyczne spektrum środków przekazu poszerzone o systemy dowodzenia i informacji oraz przetwarzania danych. Martin Libicki rozgranicza *Electronic Warfare* od *Command and Control War i Intelligence-Based War*. Uważa również, że *Electronic Warfare* dotyczy przede wszystkim technik operacyjnych: elektronicznej i kryptograficznej. Jako istotny obszar uznaje też wojnę systemów radiolokacyjnych (*search and target, jamming and counterjamming*).

Economic Information Warfare, czyli ekonomiczna wojna informacyjna, obejmuje przedsięwzięcia wywierające wpływ na gospodarkę w szerokim tego słowa znaczeniu. Na przykład, manipulacja indeksami giełdowymi lub zmiennymi kursami walut mogłaby doprowadzić do krachu system bankowy danego państwa. Komputerowe transakcje giełdowe mogą spowodować tak szybki odpływ gotówki, że banki i instytucje nadzoru bankowego nie będą w stanie w porę im zapobiec. Innymi elementami oddziaływania *Economic Information Warfare* mogą stać się urządzenia energetyczne, system transportowo-komunikacyjny, system kontroli ruchu powietrznego lub system komunikacji kolejowej (np. nastawnie kolejowe). Scenariusz takich wydarzeń przetestowano podczas strategicznych ćwiczeń dowódczo-sztabowych pod kryptonimem „*The Day After*" w Szwajcarii (listopad 1997).

Hacker War, albo wojna piratów komputerowych, jest skierowana na wnikanie do cywilnych i wojskowych systemów informatycznych i manipulowanie nimi lub ich zniszczenie w celu przerwania transmisji danych. Ten komponent wojny elektronicznej najczęściej przynosi wymierne efekty. Rozróżnia się hakerów (*Hacker*) i krakerów (*Cracker*). *Haker* wnika do systemu, ale nie czyni mu uszczerbku, choć często pozostawia w nim swoją, wizytówkę, aby pokazać słabe punkty systemu. *Kraker* natomiast włamuje się do systemu, by poczynić w nim szkody. Pewnemu

specjaliście od przetwarzania danych udało się wejść do jednego z komputerów amerykańskiego krążownika typu „*Aegis*", który był powiązany z systemem dowodzenia okrętu. Istniało duże prawdopodobieństwo podania jednostce błędnych danych nawigacyjnych. W latach 90-tych grupa rosyjskich *hakerów* włamała się do niejawnych dokumentów szwajcarskiego Departamentu Uzbrojenia, czyniąc internet narzędziem szpiegowskim. W 1997 r. *hakerzy* amatorzy z Chorwacji złamali kod zabezpieczenia bazy danych Pentagonu i wykradli dane dwóch baz rakietowych oraz centrali obsługującej satelity wojskowe. *Hakerzy* rozkodowali niejawne dane z programu NASA (*National Aeronautics and Space Administration*).

Cyber War albo *Net War* (wojna cybernetyczna albo wojna w systemach sieciowych) obejmuje pojęcia, zgodnie z którymi część działań bojowych zostanie przeniesiona w wirtualny świat systemów i sieci komputerowych, jednocześnie zostanie zredukowane użycie siły fizycznej (ludzkiej). Trzeba sobie jednak zdawać sprawę z tego, że nie wszystko, co wirtualne będzie mogło być zrealizowane, że część pozostanie długo jeszcze w sferze fikcji naukowej). Niels Möller-Gulland sądzi, że mogłyby znaleźć zastosowanie np. roboty ze sztuczną inteligencją zastępujące ludzi lub satelitarne urządzenia rozpoznawcze powiązane z przetwarzaniem danych lub wreszcie dość często przywoływane tzw. cyfrowe pole walki (*das digitale Gefechtsfeld*).

Szwajcar Christoph Abegglen ze Szkoły Dowodzenia w Pfaffhausen w 1996 r. przyjął następującą klasyfikację: Net War jest ukierunkowana przede wszystkim na społeczeństwo i jego infrastrukturę informacyjną, natomiast *Cyber War* zajmuje się siłami zbrojnymi przeciwnika i odnosi się do operacji militarnych. Publicysta „*Österreichische Militärische Zeitschrift*" Erich Vad[10] widzi pewną szansę we wczesnym użyciu środków walki informacyjnej, twierdząc, że „bezkrwawe metody wojny informacyjnej umożliwiają rozstrzygnięcie konfrontacji technologicznej przewyższającymi siłami jeszcze przed zastosowaniem klasycznej przemocy zbrojnej."

---

[10] Zob. E. Vad, *Operative Führung. Grundlagen, Merkmale und Perspektiven*, „Österreichische Militärische Zeitschrift" 1998, nr 2.

Psychological Operations zajmują się ludzkim czynnikiem wojny informacyjnej i oddziałują na siłę woli i świadomość przeciwnika. Oddziaływanie psychologiczne może objąć całą ludność wroga lub być skierowane tylko na jego siły zbrojne. Do tego celu wykorzystuje się media własne i obce. Martin Libicki rozróżnia: operacje przeciwko narodowej świadomości przeciwnika, dowództwom wojskowym, wojskom i kulturze. Szczególnie ważne są działania psychologiczne przeciwko wojskom przeciwnika. Wymagają one jego dobrej znajomości i posiadania danych o nim. Libicki zaleca kierować je przeciwko konkretnym jednostkom przeciwnika w formie uprzedzeń i gróźb zniszczenia (rozbicia), co zawsze w jakiś sposób wpływa na morale ludzi, którzy na ogół nie kwapią się, by znaleźć się w sytuacjach zagrożeń.

Reasumując, można stwierdzić, że istotą Operacji Informacyjnych jest integracyjna funkcja wszystkich (lub możliwie wszystkich) aspektów informacji w obszarze działania cywilnego lub wojskowego. Natomiast głównym celem będzie dążenie do uzyskania przewagi (dominacji) informacyjnej.

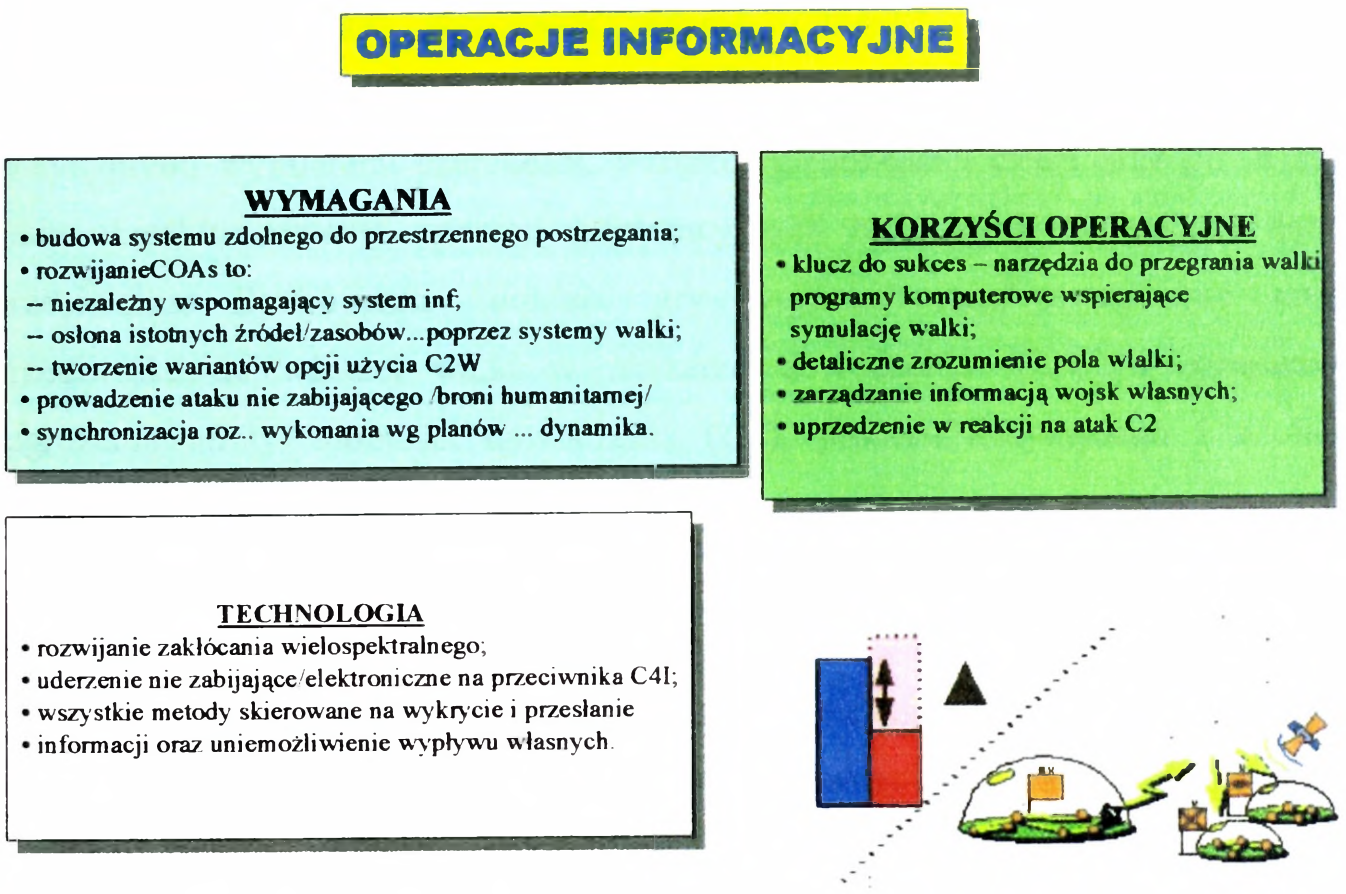
Dominacja informacyjna będzie uzyskana, kiedy zrozumienie obszaru działań przez dowódcę znacząco przewyższy poziom zaskoczenia, zyskuje on wtedy czas na reakcje i przestrzeń do działania. Dowódca będzie prowadził walkę informacyjną, by osiągnąć wszystkie korzyści wynikające z przewagi informacyjnej. Natomiast wsparcie systemu rozpoznania dla walki informacyjnej powinno zawierać: możliwość zrozumienia jak działa system informacyjny przeciwnika przez identyfikowanie i umieszczanie jego kluczowych punktów węzłowych i miejsc wrażliwych (C2[11] *Exploit*); umożliwiających atak (C2[12] *Attack*) i ponowną ocenę skutków uderzenia dla ustalenia jak działa system informacyjny przeciwnika po wykonanym ataku, by zidentyfikować, własne kluczowe punkty węzłowe i miejsca wrażliwe (C2 *Protect*[13]) (rys 3.4).

By skutecznie zaatakować, dowódca będzie wymagał gruntownego zrozumienia struktury dowodzenia przeciwnika i jego decyzji. Założenie tego zrozumienia, stanowić będzie analiza szczegółów prowadzona w okresie pokoju i aktualizowana podczas pełnego spektrum konfliktu. Dlatego system rozpoznana musi wspierać

---

[11] Wykorzystanie systemu dowodzenia (rozpoznania i WE).
[12] Uderzenie na system dowodzenia i kierowania
[13] Osłona systemu dowodzenia – obrona informacyjna.

przygotowanie i walkę w obszarze dowodzenia przez efektywne wykorzystanie sił i środków, utrzymanie ochrony bazy danych wojsk własnych oraz przeprowadzenie ataku na bazę danych przeciwnika. Gruntowne zrozumienie *Wojskowego Środowiska Informacyjnego* jest podstawą dla rozwijania i wykonywania efektywnych działań ofensywnych w obszarze dowodzenia, by zniszczyć, przeszkodzić, zaprzeczyć, albo zdegradować sieci informacyjne przeciwnika, jego systemy dowodzenia, dane i źródła rozpoznania oraz proces wypracowania decyzji.



Rys. 3 .4. Rozpoznawcze wsparcie dla operacji informacyjnych

To uświadomienie, umożliwia efektywną ochronę własnych systemów dowodzenia, by wykluczyć przeciwnika od skutecznego przeprowadzenia ataku przeciwko nam. Pełny atak może nastąpić poprzez zrozumienie, że proces decyzyjny przeciwnika pozwala na dokładne oszacowanie potencjalnych celów w ramach naszego ugrupowania i wspiera efektywnie prowadzenie operacji informacyjnych przeciwko istotnym punktom węzłowym. Rozpoznanie ma zidentyfikować jak przeciwnik będzie porażony przez określoną walkę w obszarze dowodzenia, jaka jest

istota celów *HVT*[14] i *HPT*[15] oraz przewidzieć jego odpowiedź kiedy systemy dowodzenia i kierowania będą zaatakowane.

Dla realizacji zadań rozpoznawczych muszą zostać użyte takie same technologie jakie są wykorzystywane w systemie dowodzenia, chociaż może się zdarzyć, że będą wymagane jakieś nowe techniki wspomagające. Informacyjne Przygotowanie Pola Walki musi dostarczyć narzędzi potrzebnych dla wsparcia operacji informacyjnych. Ponadto musi wesprzeć „grę wojenną", planowanie działań i ich realizację oraz dostarczyć narzędzi do „przegrania" w działaniu alternatywnym sposobów postępowania wykonania zadania (*COAs*)[16]. Te narzędzia (programy symulacyjne) walki w obszarze dowodzenia, umożliwią dowódcy „myśleć" poza tradycyjnymi wymiarami szerokości, wzrostu, głębokości i czasu oraz przewidzieć, jakie określone obiekty operacji informacyjnych będą miały wpływ na decyzję przeciwnika. Dynamiczna zdolność gry wojennej musi symulować reakcje przeciwnika do własnej walki w obszarze dowodzenia (*C2W*) i przedstawiać zagrożenia utraty zdolności dowodzenia (*C2*), procesu decyzyjnego i zdolności gromadzenia informacji.

Wykorzystanie systemów dowodzenia i kierowania, pozwali wojskom operacyjnym w pełni zrozumieć zamiar przeciwnika i określić jego zdolność. Jego operacyjna wartość dostarczy dowódcy dokładnego obrazu i wizualizacji, żeby mógł wybrać czynniki, wykorzystując w pełni większe tempo działania i zdolność rażenia, a tym samym osiągnąć założony cel. Dowódca będzie teraz wiedział, kiedy, gdzie i jak zaatakować system dowodzenia przeciwnika.

Ofensywna forma walki w obszarze dowodzenia zawiera zarówno sposoby „niszczącego" jak i „nieniszczącego" wpływania na proces decyzyjny przeciwnika, aby zapobiec efektywnemu dowodzenia przez zaprzeczanie jego informacji, mylenie albo niszczenie jego systemu dowodzenia lub dostarczanie mu fałszywej lub zniekształconej informacji. Zdolność, by gruntownie zrozumieć i graficznie

---

[14] Cele wysokowartościowe (*High-Value Target - HVT*) to ważne obiekty w ugrupowaniu bojowym przeciwnika, spełniające kluczową rolę w wykonaniu zadania bojowego a których porażenie znacznie obniży jego wartość bojową, natomiast wykaz obiektów/celów w literaturze anglojęzycznej jest nazywany „listą"

[15] Cele wysokoopłacalne (*High-Payoff Target - HPT*) są tymi celami, które muszą zostać zaatakowane, by wykonać zadanie.

[16] **COA** - *Course of Action.*

przedstawić pole walki w aspekcie informacji jest podstawą dla pomyślnego ataku na system dowodzenia. Wyrafinowane, „nieśmiertelne" opcje ataku, by mylić, przeszkodzić, przekręcić albo zniszczyć informację powinny być planowane i wykonywane przez elementy rozpoznawcze jako część ataku na system dowodzenia przeciwnika. Opcje ataku mogą zmienić się od chirurgicznego zagłuszania spektrum częstotliwości do wtargnięcia do systemów dowodzenia i kierowania, by uszkodzić lub zmanipulować danymi. Ocena skutków uderzenia na system dowodzenia przeciwnika jest podstawą w szacowaniu efektów ataku i utrzymywaniu dominacji informacyjnej. Jednakże, analiza sposobu, by prowadzić ocenę skutków uderzeń na cele, które były nie - śmiertelnie atakowane to znaczące wyzwanie do przyszłego doradztwa technicznego komórek rozpoznawczych. Efektywna ocena skutków uderzeń jest istotna w ramach IPPW i w uaktualnianiu warunków skuteczności. Jednocześnie proces oceny skutków uderzeń (ataku) na system dowodzenia będzie wymagał określenia prawdopodobieństwa wykonania ataku i macierzy, opartej na algorytmach, używając zbiorów danych, oraz wnioskowania i analizy reakcji, jaką przewiduje przeciwnik.

W rezultacie można uznać że, wartość operacyjna ataku na system dowodzenia, umożliwi dowódcy oddalić zagrożenie i uniemożliwić stosowną reakcję do własnego działania. Dominacja informacyjna pozwoli własnym wojskom, zakłócić percepcje przeciwnika i wykonać operacje mylenia przez wstawianie danych do systemu przeciwnika bez ruszania pojedynczego zbioru. Ponadto atak na system dowodzenia dostarczy dowódcy możliwości by zaangażować się do decydujących działań i stworzyć warunki - które opracował jego sztab - dla realizacji zadań operacji informacyjnych.

Obrona informacyjna (OI) może być ofensywna albo defensywna. Ofensywna obrona systemów dowodzenia, używa elementów podstawowych by zmniejszyć zdolność przeciwnika, do zaatakowania własnego systemu dowodzenia. Obronna forma redukuje podatności własnego systemu dowodzenia na atak przeciwnika przez wykorzystanie odpowiedniego fizycznego i elektronicznego działania. OI musi ponadto zostać włączona do systemów SZ jako zaplanowane, działanie. Niepowodzenie, spowoduje zagrożenie systemu dowodzenia. Zdolność, aby

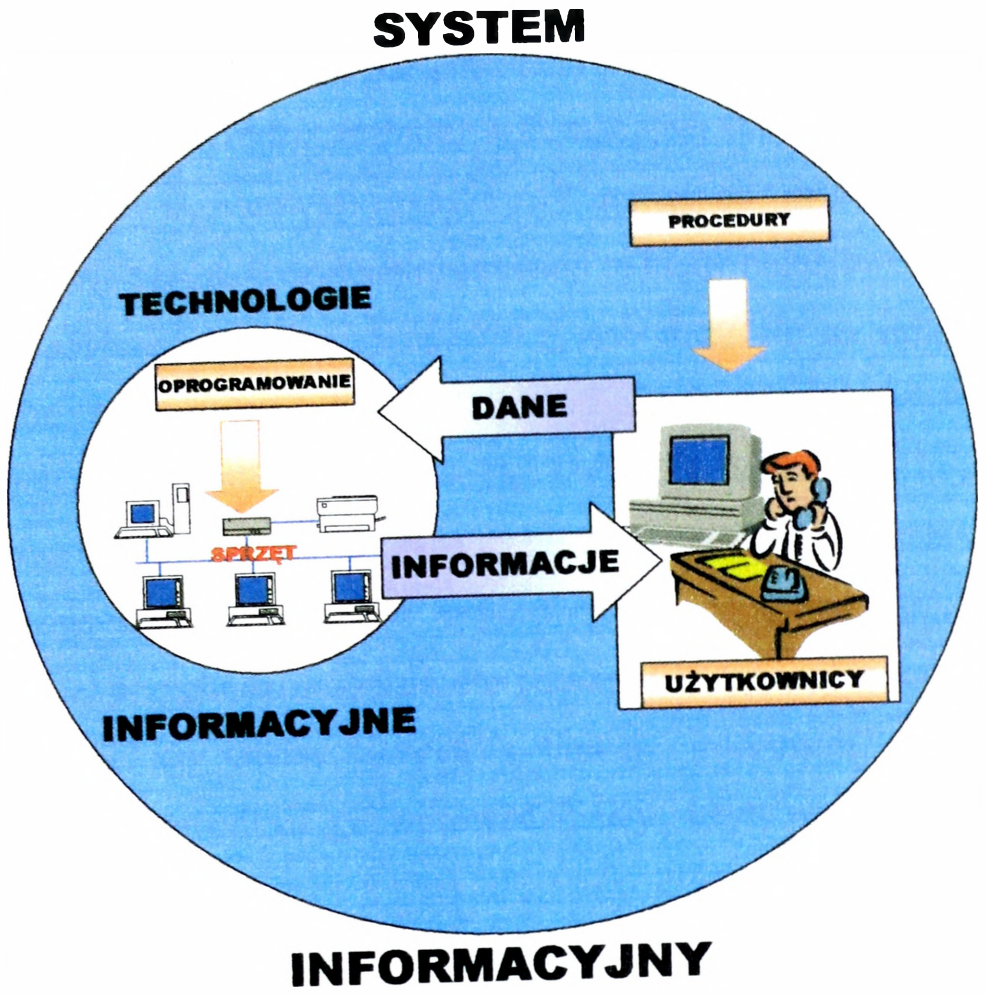
gruntownie zrozumieć i graficznie przedstawić obszar działań w aspekcie informacji jest podstawą, ponieważ sprawny system dowodzenia ochrania działania. Narzędzia są potrzebne, by pomóc w dostrzeganiu nieupoważnionych prób włamania, by uzyskać dostęp do informacji i elektronicznie wyśledzić intruza. Gra wojenna musi pokazać skutki ataku przeciwnika na system dowodzenia.

Operacyjna wartość OI dostarcza obronę przeciw zagrożeniu atakiem na systemy dowodzenia. Utrzymywanie zdolności wojsk operacyjnych w tym zakresie umożliwia sprawne dowodzenie i kontrole wojsk poprawia możliwości przetrwania na polu walki i podnosi tempo działania.

3.1.2 Rozpoznanie w nowych technologiach informacyjnych

W teorii sztuki wojennej w szkoleniu wojsk, a także w działalności edukacyjnej i naukowo-badawczej pojawia się nowy obszar zainteresowań związany z nowymi technologiami informacyjnymi. Obszar ten ma duże znaczenie zarówno dla teoretyków jak i praktyków - kadr dowódczo-sztabowych.

W ich ramach pojawiają się różne terminy i bogate znaczeniowo pojęcia (rys.3.5.). Maja one związek nie tylko z modyfikacją tradycyjnych zachowań i procesów, ale również z innymi dyscyplinami naukowymi. Często spotykanym i równie wieloznacznym pojęciem są „system informacyjny", „system informatyczny" czy też „technologie informacyjne czy informatyczne?". Kłopot polega bynajmniej nie na tym, że nikt nie wie, co należy rozumieć przez te pojęcia, lecz wprost przeciwnie - zbyt wielu ludzi nadaje tym pojęciom zbyt wiele znaczeń. W tej części analiz terminologicznych warto zwrócić uwagę, że posługiwanie się terminem „system informacyjny i/lub informatyczny" czy „nowoczesne technologie i techniki informacyjne" budzi wiele zastrzeżeń. Wynika to z gwałtownego rozwoju technologii i braku trafniejszego określenia. Podjęta analiza podstawowych pojęć nie ma charakteru uniwersalnego i z metodologicznego punktu widzenia jest i długo jeszcze będzie przedmiotem dyskusji. Wymienione kategorie, choć ciągle się zmieniają, są ze sobą funkcjonalnie i strukturalnie powiązane.



Rys. 3.5. System informacyjny a technologie informacyjne

Użytkownik potrzebuje informacyjnego wspomagania procesów po to, by dodać wartości produktom i usługom oraz działaniom, w których rezultacie one powstają. Informatyk oferuje mu rozwiązania, które niekoniecznie przydają wartości użytkownikowi, ale wciąż dobrze sprzedają się. Użytkownikowi mówi: *organizacja to nie moja sprawa, ja znam się na informatyce i jej narzędzia sprzedaję; twoja sprawa, jak to wykorzystasz*. Problem w tym, że użytkownik za słabo wciąż zna się na dowodzeniu a na informatyce w ogóle. Bo i po co ma się znać na informatyce? Jeśli informatyk mówi, że nie musi się znać na taktyce, działaniach operacyjnych czy cyklu pracy, to dlaczego od np. zwiadowcy wymagamy znajomości narzędzi?

Czasami zastanawiam się, dlaczego forsujemy pojęcie systemy informatyczne lub ... systemy zautomatyzowane. Przecież *zautomatyzowany* oznacza: wykonywany bez interwencji człowieka[17]. A informatykę wprowadza się nie po to, by eliminować najważniejszy składnik organizacji - człowieka - ale by zwiększyć jego możliwości.

---

[17] Jakaś czynność wykonywana automatycznie (za pomocą urządzeń technicznych).

śmiem twierdzić, że przyczyną omijania określenia: *system informacyjny* jest chęć odwrócenia uwagi od prawdziwych problemów informacyjnych (czyt.: dowodzenia) i jej skierowania na narzędzia techniki informacyjnej (czyt.: gadżety). Same pojęcia wskazują, co należy akcentować: czym? i jak? zamiast co? mamy zrobić i po co?

Już w fazie szeroko rozumianej edukacji te błędy pojęciowe dezorientują adepta zawodu. W powszechnym rozumieniu ktoś, kto uczy się na informatyka, ma być technologiem, programistą. Potem ci specjaliści widzą niewiele poza coraz nowocześniejszą i wspanialszą technologią. Twierdzą, że trzeba ją kupić i zastosować, chociaż wciąż nie wiedzą po co? i do czego? Ten zachwyt udziela się decydentom, którzy zgadzają się na propozycje wyposażenia w najnowocześniejszą technologię. Dopiero później przychodzi refleksja. Po co nam ten system zautomatyzowany, skoro nie wykorzystuje się lawiny danych a brakuje informacji? Po co nam system informatyczny, skoro odkąd go wprowadziliśmy, użytkownik czeka na informację dwa-trzy razy dłużej?

Warto zaznaczyć, że nie ma jeszcze ostatecznych ustaleń terminologicznych w zakresie systemów czy technologii. W ostatnich latach obserwujemy niezwykle dynamiczny rozwój ilościowy i jakościowy elektroniki powszechnego użytku, zwłaszcza techniki telewizyjnej i komputerowej. Wszystkie one bardzo szybko wkraczają do różnych dziedzin i form komunikowania się. Praktyka wyprzedza teorię i z tego też powodu występują trudności z nazewnictwem i jednoznaczną interpretacją pojęć. Nowe sposoby gromadzenia, utrwalania, przetwarzania i przesyłania nie miały nie tylko swych teoretyków, ale nawet wizjonerów. Tymczasem tworzenie nowych wyrażeń jest procesem długotrwałym. O przyswojeniu nowych terminów powinna decydować ich komunikaty zaś struktura pojęć powinna być podporządkowana normom polszczyzny. Dziś nie ulega najmniejszej wątpliwości, że nowa terminologia elektroniczna i informatyczna - chociażby ze względu na swój społeczny aspekt- wymaga stałej troski: normowania, selekcji i eliminacji niewolniczych kalek z języków.

Dlatego zakładam, że pojęcie *systemu informatycznego* prawdopodobnie zniknie. Od dawna nie mówi się pralka, lodówka, żelazko czy oświetlenie *elektryczne*. Tak jak zasilanie elektryczne jest czymś naturalnym, tak narzędzie informatyczne

powinno być już czymś ewidentnym w sferze systemów informacyjnych (bo nie informatycznych).

Poprzez analogię można by przeprowadzić analizę dotyczącą technologii informacyjnych czy też informatycznych. W konkluzji można przyjąć że, **system informacyjny** – stanowi zespół określonej technologii informacyjnej, korzystających z niej użytkowników oraz procedur działania mającego na celu realizację zadania polegającego na uzyskaniu informacji lub na jej przetworzeniu do pożądanego formatu natomiast **technologia informacyjna** – to sposób wykorzystywania i współdziałania sprzętu, oprogramowania i zadań niezbędnych do zrealizowania operacji na informacjach.

Technologie informacyjne, ze względu na swoje funkcje mają powszechne zastosowanie, także w wojsku mogą wspomóc realizację wielu zadań typowych dla walki. Najnowsze technologie umożliwiają tworzenie (generowanie) informacji, ich przekazywań przechowywanie, selekcję, udostępnianie, wykorzystywanie w postaci słowa, obrazu, dźwięków, znaków symbolicznych. Szczególne znaczenie ma zobrazowanie sytuacji, w ramach której zjawiska mogą być prezentowane w sposób dynamiczny, a działania symulowane. Techniczne możliwości technologii informatycznych pozwalają m.in. na:

- natychmiastowy przekaz informacji;
- wzajemne ich uzupełnianie;
- stosunkowo rzetelne i wierne ich odtwarzanie;
- szybkie przetwarzanie informacji;
- zwolnione bądź przyśpieszone analizowanie sytuacji;
- podejmowanie decyzji obarczonych niewielkim ryzykiem błędu.

Jednym z elementów współczesnej technologii informacyjnej jest Internet. Dotychczas nie udzielono jednak pełnej odpowiedzi na pytanie, czym on jest. Bardzo trafne jest stwierdzenie Stanisława Lema: „Internet jest odpowiedzią na pytanie, które nie zostało jeszcze postawione". Trzeba przyznać, że największe zachwyty nad siecią wygłaszają twórcy jej struktury technicznej i rosnących w zawrotnym tempie zasobów danych oraz odnoszący z tego największe korzyści, przede wszystkim finansowe. Można by nawet pokusić się o stwierdzenie, że powstaje społeczeństwo sieciowe -

znaczna część jego egzystencji będzie się toczyć w wirtualnym świecie, w którym zanikną odległości, oś czasu, potrzeba fizycznej realizacji człowieczeństwa, i tylko informacja będzie ważna.

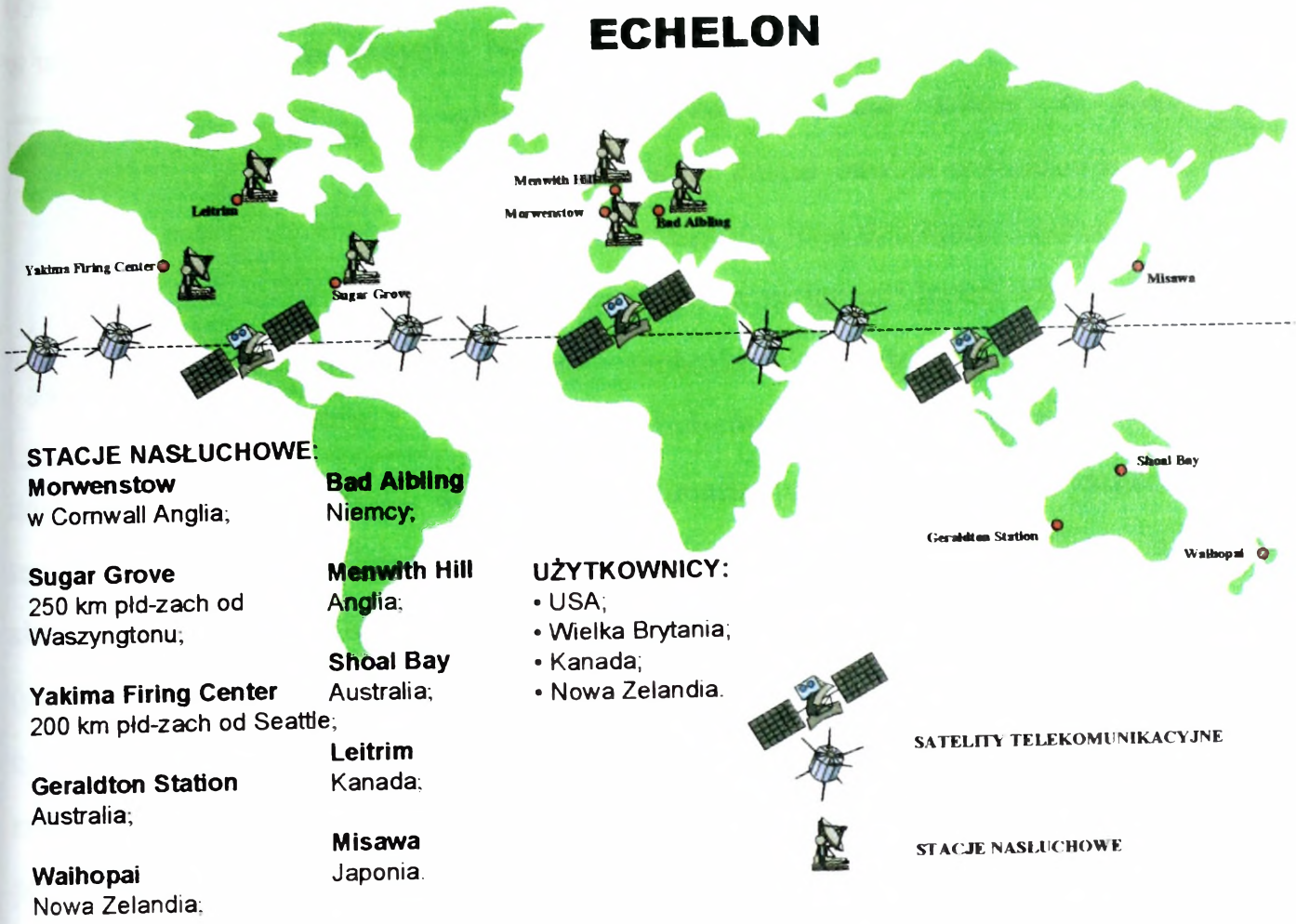
3.1.2.1 Echelon

Co jakiś czas dowiadujemy się o kolejnych przykładach naruszenia prywatności. Pogłoska o tym, jakoby służby specjalne podsłuchiwały i rejestrowały wszystkie przesyłane informacje, poszukując w nich przy pomocy specjalnego oprogramowania pewnych „wrażliwych" słów, takich jak „bomba" czy „narkotyki", jest niemal tak stara, jak samo komunikowanie się. Zwykle rewelacji owych nikt nie traktował poważnie, biorąc je po prostu za jedną z wielu krążących „miejskich legend". Jednak doniesienia, które od kilku lat pojawiają się w prasie i różnych serwisach informacyjnych, pozwalają w coraz większym stopniu sądzić, że w tym przypadku mamy do czynienia z czymś więcej niż tylko legendą. Powyższe przypadki mogą jednak okazać się nic nie znaczącymi drobiazgami w porównaniu z operacją prowadzoną na iście globalną skalę przez amerykańską *National Security Agency (NSA)*. O ile oczywiście prawdą jest to, co coraz częściej z różnych źródeł słyszy się na temat projektu o kryptonimie *Echelon*.[18]

Początku historii tego systemu można dopatrywać się w roku 1947, kiedy to pomiędzy NSA i jej brytyjskim odpowiednikiem zajmującym się wywiadem elektronicznym - *Government Communication Headquarters (GCHQ)* - zawarte zostało tajne porozumienie „Wielka Brytania-Stany Zjednoczone" („*United Kingdom - United States" - UKUSA*), które w późniejszym czasie rozszerzono także o odpowiednie agencje wywiadowcze Kanady, Australii i Nowej Zelandii. Pierwotnie porozumienie UKUSA miało służyć współpracy w zakresie „klasycznego" wywiadu - a więc pozyskiwania informacji wojskowych, dyplomatycznych itp. - głównie dotyczących ZSRR i innych państw późniejszego Układu Warszawskiego. Jednak wraz z zakończeniem zimnej wojny agencje współpracujące w ramach UKUSA w coraz większym stopniu zaczęły zmieniać obszar swoich zainteresowań w kierunku szpiegostwa przemysłowego i gospodarczego (rys3.6).

---

[18] http://www.echelonwatch.org/



Rys. 3.6 Echelon

Zmieniły się też metody ich działania. Tradycyjny wywiad elektroniczny polegał na podsłuchu wybranych kanałów łączności - np. linii telefonicznych należących do placówek dyplomatycznych, czy częstotliwości radiowych używanych przez wojsko - i przechwytywaniu przesyłanych tymi kanałami informacji. Uruchomiony prawdopodobnie we wczesnych latach siedemdziesiątych (a więc będący niemal „rówieśnikiem" Internetu...) system *Echelon* wychodził zupełnie z innego założenia - podsłuchiwać „hurtem" wszystko, co tylko da się podsłuchać, i przy pomocy komputerów z odpowiednim oprogramowaniem wyszukującym wyławiać z tej masy informacji wiadomości, które mogą być przydatne dla wywiadu[19].

Prawdopodobnie pierwotna wersja systemu *Echelon* służyła analizowaniu danych przechwyconych przez dwie stacje nasłuchowe, zbudowane w celu podsłuchiwania transmisji przesyłanych przez system satelitów telekomunikacyjnych Intelsat - jedna z tych stacji znajdowała się w miejscowości Morwenstow w Anglii

[19] Zob. http://www.hr/mprofaca/echelon.html

(rys. 3.7), druga w Yakima na północnym zachodzie USA. Skuteczność systemu w wyławianiu interesujących NSA informacji okazała się większa, niż się spodziewano: zdecydowano zatem o rozbudowie systemu. Echelon został bardzo rozbudowany w latach 80-tych. Rozszerzono jego działanie o nowe funkcje tak, by mógł nadążyć za zmianami technicznymi jeśli chodzi o nowe techniki łączności (mikrofale, łączność satelitarna). Echelon rozrósł się o nowe urządzenia nasłuchowe i nowe ośrodki komputerowe, analizujące przechwycone dane; i rozwój ten trwa do dnia dzisiejszego. Urządzenia te to m.in. specjalne stacje naziemne, służące podsłuchiwaniu sygnałów przesyłanych przez satelity telekomunikacyjne (stacje te często stanowią niemal wierne kopie „prawdziwych" stacji naziemnych używanych przez systemy łączności satelitarnej, takie jak np. Intelsat - rys.3.8). Są również specjalne satelity szpiegowskie, wykonujące zadanie niejako odwrotne: przechwytujące z kosmosu sygnały emitowane przez naziemne systemy łączności, takie jak np. popularne w telekomunikacji radiolinie działające w paśmie mikrofalowym, radiotelefony, czy telefony komórkowe. Z uwagi na właściwości tych środków łączności ich skuteczne podsłuchiwanie na ziemi możliwe jest tylko w stosunkowo ograniczonym obszarze geograficznym, niedaleko od nadajnika; natomiast odbiór ich sygnałów z kosmosu nie przedstawia większego problemu. Przypuszcza się, iż obecnie system ten jest zdolny do przechwytywania i analizowania większości (według niektórych nawet 90%) połączeń telefonicznych, teleksowych, faksowych i internetowych w ruchu międzynarodowym, a być może w niektórych państwach także połączeń krajowych.



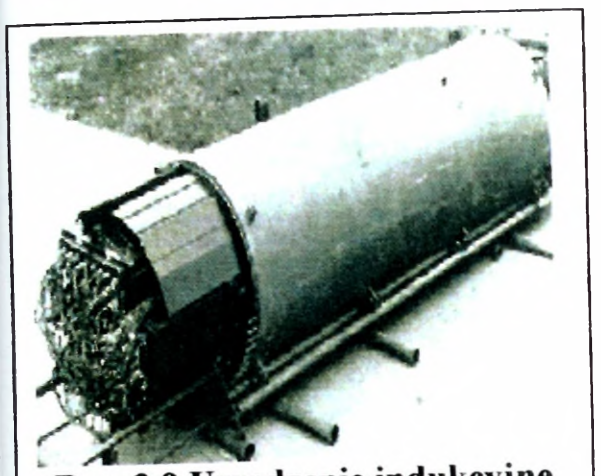
Rys. 3.7 Morwenstow



Rys.3.8 Misawa - Japonia

Podsłuchiwane są także, za pomocą specjalnych urządzeń indukcyjnych instalowanych przez łodzie podwodne, podmorskie kable telefoniczne (rys.3.9). Są, a raczej były - gdyż obecnie ta metoda podsłuchu coraz bardziej traci na znaczeniu,

z uwagi na powszechne zastępowanie kabli miedzianych światłowodami, które nie dają się podsłuchiwać (jedyną metodą podsłuchu łącza światłowodowego jest jak dotąd podłączenie się do tzw. repeatera, czyli urządzenia wzmacniającego sygnały przesyłane światłowodami - o ile takowy na danym łączu jest zainstalowany). Wreszcie nie należy pomijać podsłuchu realizowanego typowymi metodami - poprzez instalowanie „bocznych furtek" w centralach telefonicznych (w Stanach Zjednoczonych NSA prowadziła taką działalność od 1945 r. pod kryptonimem SHAMROCK - sprawa wyszła na jaw dopiero w 1975 r. przy okazji słynnej afery *Watergate*), czy też oprogramowania przechwytującego dane na głównych routerach szkieletowych Internetu.



Rys. 3.9 Urządzenie indukcyjne

Dane uzyskane z podsłuchu łączy telekomunikacyjnych stanowią wielką mieszaninę sygnałów, składającą się z szeregu różnych transmisji przesyłanych jednocześnie. Specjalne urządzenia, produkowane na zlecenie NSA przez szereg firm amerykańskich, służą do rozdzielenia tej mieszaniny na indywidualne kanały telekomunikacyjne i zidentyfikowania rodzaju prowadzonej w każdym z nich łączności (telefon, teleks, faks, transmisja danych). Przykładowo, urządzenie o nazwie SNAPPER produkowane przez firmę *Applied Signal Technology* może analizować i rozdzielać na pojedyncze kanały dane przechwycone z łącza o przepustowości 2,5 Gbps - to więcej, niż najszybsze łącza długodystansowe istniejące obecnie. Wyodrębnione już transmisje mogą być rejestrowane na taśmach magnetofonowych, twardych dyskach lub przekazywane bezpośrednio do systemów komputerowych celem dalszej analizy. System Echelon zorientowany jest przede wszystkim na analizę transmisji o charakterze tekstowym (faksów, teleksów, e-maili) z uwagi na to, że dane tego rodzaju łatwo poddają się maszynowemu przeszukiwaniu (przechwycone faksy wcześniej przetwarzane są przy pomocy programów OCR do postaci tekstu ASCII). Mniej uwagi poświęca się rozmowom telefonicznym, z uwagi na to, że nie istnieje jak dotąd oprogramowanie pozwalające w sposób niezawodny identyfikować słowa w sygnale mowy (aczkolwiek agencje współpracujące w ramach Echelona i wynajęte

przez nie firmy software'owe podejmowały wielokrotnie próby stworzenia takiego oprogramowania, jednak kończyły się one zawsze niepowodzeniem). Jednak według niektórych źródeł, w systemie Echelon również masowo nagrywa się rozmowy telefoniczne, jednak taśmy są odsłuchiwane jedynie wyrywkowo; większości z nich nikt nigdy nie słucha i po kilku miesiącach są kasowane - chyba że dany numer telefonu znajdzie się akurat z innych powodów w kręgu zainteresowań wywiadu[20].

Najlepszym jak dotąd źródłem informacji o funkcjonowaniu Echelona jest książka Nicky Hagera „*Secret Power*"[21]. Według przedstawionego przez niego opisu, „serce" systemu Echelon stanowi zespół komputerów znajdujących się w stacjach nasłuchowych, wyposażonych w oprogramowanie znane pod nazwą *Dictionary*. *Dictionary* jest typowym oprogramowaniem wyszukującym teksty, identycznym pod względem zasady działania do chociażby wyszukiwarek internetowych. W dostarczanym z urządzeń podsłuchowych strumieniu informacji Dictionary wychwytuje słowa czy frazy znajdujące się na wprowadzanej przez agencje wywiadowcze liście „słów kluczowych"[22]. Jeżeli któreś z tych słów zostanie znalezione, cała wiadomość, w którym występowało (teleks, faks, e-mail) opatrywana jest odpowiednim kodem, zawierającym datę, czas i miejsce przechwycenia oraz rodzaj kanału telekomunikacyjnego, którym wiadomość była przesyłana (publiczny, dyplomatyczny, wojskowy itp.) i przekazywana do dalszej analizy przez ludzi. Tak oto opisuje ich pracę Hager: „Każdego ranka analitycy wywiadu elektronicznego logują się na swoich terminalach w Waszyngtonie, Ottawie, Cheltenham, Canberrze i Wellington (miasta, w których znajdują się siedziby agencji wywiadowczych uczestniczących w porozumieniu UKUSA - przyp. AN). Otrzymują wykaz różnych kategorii przechwyconych wiadomości, każdą oznaczoną czterocyfrowym kodem. Na przykład 1911 może oznaczać japońskie depesze dyplomatyczne z Ameryki

---

[20] http://www.echelon.wiretapped.net/

[21] http://www.fas.org/irp/eprint/sp/

[22] Przykładowa lista takich słów: „MOSSAD NASA MI5 ONI CID AK47 M16 C4 MALCOLM X REVOLUTION CHEROKEE HILLARY BILL CLINTON AL GORE GEORGE BUSH WACKENHUT TERRORIST TASK FORCE 160 SPECIAL OPS 12TH GROUP 5TH GROUP SF ATF DOD WACO RUBY RIDGE OKC OKLAHOMA CITY MILITIA GUN HANDGUN MILGOV ASSAULT RIFLE TERRORISM BOMB DRUG HORIUCHI KORESH PROMIS MOSSAD DAVIDIAN KAHL POSSE COMITATUS WEAVER VICKIE WEAVER SPECIAL FORCES LINDA THOMPSON SPECIAL OPERATIONS GROUP SOG SOF DELTA FORCE CONSTITUTION BILL OF RIGHTS WHITEWATER POM PARK ON METER ARKANSIDE IRAN CONTRAS OLIVER NORTH VINCE FOSTER PROMIS" z http://jya.com/cryptout.htm echelon

Łacińskiej, 3848 informacje polityczne z i o Nigerii, a 8182 jakiekolwiek wiadomości dotyczące rozpowszechniania technologii kryptograficznych. Wybierają swoją kategorię, otrzymują informację o tym, ile wiadomości w tej kategorii zostało przechwyconych przez Echelon i rozpoczyna się dzień pracy. Analitycy przeglądają ekran po ekranie przechwycone faksy, e-maile itp. i gdy pojawia się wiadomość warta uwagi, wybierają ją do dalszego opracowania. Jeżeli nie jest ona po angielsku, zostaje następnie przetłumaczona, po czym zapisana w standardowym formacie raportów wywiadowczych stosowanym w całej sieci UKUSA, albo w całości jako „raport", albo w postaci streszczenia lub „wyciągu".

O skali działania systemu może świadczyć wypowiedź byłego dyrektora NSA, Williama Studermana, cytowana przez Campbella[23] w raporcie *„Interception Capabilities 2000*": „tylko jeden (nie wymieniony z nazwy) system podsłuchowy[24] może dostarczyć miliona wiadomości w ciągu pół godziny. Z tego miliona filtry pozostawiają jedynie 6500; tylko 1000 spełnia kryteria przekazania do dalszej obróbki; analitycy wybierają dziesięć, z których wytwarzany jest zaledwie jeden raport - takie są typowe statystyki".

Ciekawy jest sposób, w jaki komputery należące do poszczególnych agencji współpracują w ramach Echelona. Wszystkie instalacje pracujące w ramach UKUSA połączone są własną rozległą siecią komputerową - sieć ta, pracująca w oparciu o internetowy protokół TCP/IP, stanowi prawdopodobnie jeden z największych na świecie intranetów (na początku lat osiemdziesiątych - jak podaje Duncan Campbell - była ona większa od ówczesnego Internetu!). Korzystając z tej sieci, każda z agencji może zadawać kategorie informacji do wyszukiwania oraz odbierać przechwycone wiadomości z każdej stacji Echelona na świecie. Komputery wykonujące przeszukiwanie działają przy tym równocześnie na rzecz każdej agencji z osobna - każda z nich, niezależnie od pozostałych, może zdalnie wprowadzać własne słowa kluczowe do wyszukiwania, a wyszukany materiał jest bezpośrednio przesyłany do

---

[23] http://jya.com/echelon-dc.htm i http://www.iptvreports.mcmail.com/stoa_cover.htm lub http://www.gn.apc.org/duncan/stoa.htm

[24] W USA opracowano system USSID18 (United States Signals Intelligence Directive 18), którego zadaniem jest zbieranie informacji na temat osób mających obywatelstwo amerykańskie oraz innych przebywających czasowo lub tylko odwiedzających USA. System ten wchodzi w skład większego o nazwie USSS (United States Signals Intelligence System). Jednym z setek systemów, które go tworzą jest także Echelon.

„zamawiającej" go agencji z pominięciem lokalnego personelu obsługującego system. Teoretycznie każda z pięciu agencji jest w systemie równorzędna i żadna nie ma dostępu do danych zbieranych przez pozostałe. Ponieważ jednak cały sprzęt i oprogramowanie dostarczone zostały przez NSA, nie pozbawione podstaw może być przypuszczenie, iż w systemie istnieją „boczne furtki", faworyzujące amerykańską agencję, która być może ma możliwość dostępu do danych pozostałych partnerów.

Do 1990 roku Internet nie był właściwie obiektem szczególnego zainteresowania programu Echelon - ruch internetowy przechwytywano niejako „przy okazji" ogółu sygnałów płynących podsłuchiwanymi łączami telekomunikacyjnymi. Jednak znaczny wzrost ilości informacji przesyłanych za pośrednictwem Internetu skłonił NSA na początku lat dziewięćdziesiątych do rozbudowy arsenału stosowanych metod podsłuchu o metody specyficznie internetowe, jak *sniffing*[25] sieci. Znany jest fakt zainstalowania przez NSA w 1995 r. oprogramowania typu *sniffer*, przechwytującego wszystkie przesyłane pakiety danych, w dziewięciu głównych węzłach szkieletu amerykańskiego Internetu. Wśród nich znalazły się dwa najbardziej znane węzły firmy *MCI*, *MAE-East i MAE-West*, przez które w owym czasie przechodziła znaczna część ruchu internetowego przebiegającego do, z lub poprzez USA. Obecnie większość amerykańskich operatorów Internetu rozbudowała strukturę połączeń alternatywnych, omijających owe węzły - nie tyle ze względu na fakt zainstalowania w nich *snifferów* NSA, co na ich tragiczne wręcz przeciążenie - podówczas jednak przechwycenie ruchu na tych węzłach oznaczało faktyczne przechwycenie większości ruchu międzynarodowego w Internecie.

Czy zatem rzeczywiście - jak głoszą powtarzane od lat w Internecie pogłoski - wszystkie informacje przepływające przez Internet są podsłuchiwane i rejestrowane? Po pierwsze, warto zauważyć, że ogromnej większości informacji przesyłanych przez Internet wcale nie trzeba podsłuchiwać, gdyż są one ogólnie dostępne! Do listów przesyłanych w grupach dyskusyjnych, czy zawartości stron WWW może mieć dostęp każdy użytkownik Internetu - w tym, oczywiście, również agencje wywiadowcze. Nie

---

[25] Sniffing to działalność polegająca na monitorowaniu i rejestrowaniu identyfikatorów i haseł używanych w czasie logowania się autoryzowanych użytkowników do sieci chronionych, aby uzyskać do nich dostęp. Służy temu specjalne oprogramowanie śledzące ruch w Sieci i przechwytujące dane transmitowane między komputerem autoryzowanego użytkownika a serwerem, spośród których wyłapuje ono identyfikator i hasło.

ma wątpliwości co do tego, że z dostępu tego robią one użytek; udostępniane w Internecie informacje są przez nie rejestrowane i szczegółowo analizowane. Wiadomo na przykład, że brytyjska agencja DERA (*Defense Evaluation and Research Agency*) posiada centrum komputerowe z dyskami o pojemności 1 TB (terabajta), zawierające archiwum wszystkich wiadomości z grup dyskusyjnych Usenetu z ostatnich 90 dni. To „prywatne DejaNews" nie służy z pewnością rozrywce pracowników wspomnianej agencji. Wiadomo też, że NSA posiada własne wyszukiwarki - „roboty" internetowe, które wędrują po stronach WWW w poszukiwaniu informacji w analogiczny sposób, jak czynią to „roboty" komercyjnych wyszukiwarek typu Altavista. Ślady ich odwiedzin znajdują się w logach wielu serwerów WWW, szczególnie zawierających materiały dotyczące prywatności, kryptografii, wolności obywatelskich itp.

Ta cześć ruchu internetowego, która wymaga podsłuchu, ogranicza się zatem do komunikacji prywatnej - głównie w postaci e-maila oraz danych przesyłanych w wirtualnych sieciach prywatnych (VPN), utworzonych w obrębie Internetu. Przechwytywanie większości tego ruchu - głównie w relacjach międzykontynentalnych - jest, biorąc pod uwagę techniczne możliwości systemu bardzo możliwe.

W istocie jednak, rzeczywistą bronią przeciwko Echelonowi i podobnym działaniom jest stosowanie oprogramowania szyfrującego, które obecnie bez problemu dostępne jest dla każdego użytkownika Internetu. Właśnie rozpowszechnienie się tego oprogramowania stanowi obecnie główną przeszkodę dla działalności wywiadu elektronicznego. Nic więc dziwnego, że NSA stara się wszelkimi dostępnymi sobie sposobami ograniczyć rozpowszechnianie „silnej" kryptografii. Wydaje się jednak, że amerykańskie czynniki rządowe coraz bardziej nabierają przekonania, że walka z szyfrowaniem skazana jest na przegraną. Sygnałem tej zmiany postawy może być choćby niedawne złagodzenie obowiązujących przez wiele lat restrykcji na eksport z USA oprogramowania szyfrującego z długimi kluczami. Kryptografowie działają w końcu nie tylko w USA, a użytkownicy nie mogąc legalnie używać amerykańskiego oprogramowania szyfrującego, zwrócą się w kierunku produktów pochodzących z innych krajów, odbierając amerykańskim producentom zyski.

Można się natomiast spodziewać, że NSA będzie starała się wpływać na producentów oprogramowania szyfrującego, aby wbudowywali w swoje produkty „tylne wejścia", pozwalające NSA odczytywać zakodowane transmisje. Przypadek taki wykryto już w systemie bezpiecznej poczty elektronicznej pakietu Lotus Notes: program wysyłał klucz sesji zakodowany nie tylko kluczem publicznym odbiorcy, ale również... kluczem publicznym NSA! Odkodowanie tak zaszyfrowanej transmisji nie przedstawiało zatem dla NSA żadnego problemu. Na szczęście proceder taki jest znacznie trudniejszy - o ile nie niemożliwy - do przeprowadzenia w przypadku programów *open source*, których kod źródłowy jest publicznie dostępny, jak chociażby *GNU Privacy Guard*.

3.1.2.2 Carnivore i Magic Lantern

W Quantico, w stanie Wirginia, w laboratorium badawczo-konstrukcyjnym Akademii FBI stworzono mechanizm do przeglądania korespondencji przesyłanej pocztą internetową. Ludzie, którzy odwiedzali Akademię FBI w Quantico w stanie Wirginia, porównują nastrój panujący w tym kompleksie, składającym się z 21 rozrzuconych po lesie schludnych budynków, do małego śpiącego miasteczka uniwersyteckiego ze środkowego zachodu lub szpitala. Wrażenie to psuje nieco fakt, że akademię otacza płot z kolczastego drutu i zwykle docierają tu odgłosy kanonady z pobliskiego poligonu. Jest ona bowiem położona na terenie bazy *Marine Corps.*, znajdującej się 40 mil od Waszyngtonu. Jeden z budynków akademii, w którym mieści się *Engineering and Research Facility* (laboratoria badawczo-konstrukcyjne), jest miejscem pracy Marcusa Thomasa, aktualnie około czterdziestoletniego szefa grupy specjalnych agentów, pod którego kierunkiem stworzony został mniej więcej przed ośmioma laty system inwigilacji przesyłanej przez Internet poczty elektronicznej. Nazwa, jaką nadała swemu systemowi grupa Thomasa, licząca dziś około 90 agentów, świadczy, że nawet policjanci mają może nieco specyficzne poczucie humoru. Program jest znany oficjalnie jako Carnivore, czyli „Mięsożerca" (oficjalna nazwa: DCS1000), a symbolizuje go ikona przedstawiająca potwora z zakrwawionymi zębami pożerającego pasmo zero-jedynkowych bitów. W połowie lipca ubiegłego roku Carnivore, wbrew intencjom swych twórców, zyskał szeroką sławę, stając się przedmiotem gorącej kontrowersji i publicznej debaty, która nieprędko się zakończy.

Prace nad pierwszą wersją systemu (pod nazwą Omnivore) FBI rozpoczęto jeszcze w lutym 1997. Wówczas planowano skorzystać z komputerów Solaris. Począwszy od czerwca 1999 r Omnivore zastąpiony został przez sieć Carnivore pracującą pod kontrolą Windows NT. Według dość ogólnikowych informacji podanych do publicznej wiadomości przez FBI, mechanizm funkcjonowania opracowanego w laboratoriach Biura systemu podsłuchu korespondencji elektronicznej jest następujący: FBI, działając w porozumieniu z dostawcą usług internetowych (providerem), instaluje swą „czarną skrzynkę" na wyjściu serwera. FBI wraz z dostawcą starają się następnie ustalić źródło (access point), z którego pochodzi cała korespondencja osoby zidentyfikowanej w nakazie sądowym, a także możliwie niewielką ilość nie związanej z tą osobą informacji. Tylko ta część „elektronicznego ruchu" kierowana jest do Carnivore, który kopiuje wszystkie uzyskane dane, nie zakłócając przepływu komunikacji. Skopiowane informacje przepuszczane są na następnym etapie przez filtr, którego zadaniem jest wydobycie ze strumienia danych jedynie tej ich części, na której przechwycenie zezwala nakaz sądowy. „Przecedzone" informacje są następnie rejestrowane i po rekonstrukcji kompletnych przekazów z przesyłanych pakietów „plombowane", tak że dostęp do ich treści mają tylko osoby prawnie do tego upoważnione. Carnivore, jak twierdzi FBI, został zbudowany przy użyciu ogólnie dostępnych aplikacji Windows 2000. Ten uproszczony opis działania systemy elektronicznej inwigilacji nie zadowala krytyków, którzy twierdzą, że bez ujawnienia wszystkich szczegółów jego kodu nie mogą oni być pewni, że Carnivore nie jest w stanie monitorować całej przechodzącej przez serwery komunikacji. Podobnymi systemami dysponują także tajne służby innych krajów; m.in. Wielkiej Brytanii (MI-5), Holandii (BVD) oraz Rosji (FSB).

Dzięki funkcjonowaniu tego systemu, Federalne Biuro Śledcze miało dostęp do wszelkich informacji zawartych w elektronicznej poczcie. Co najważniejsze, okazało się, że przechwytywane przez „Drapieżnika" dane były szyfrowane i z tego powodu są zupełnie bezużyteczne.

I tak narodził się nowy projekt stworzenia „Magic Lantern" (Magiczna Latarnia), rozszerzonego programu Carnivore, który pozwoli na łamanie lub omijanie

kodów, którymi zabezpieczone są dane zapisane na twardych dyskach komputerów należących do przestępców lub podejrzanych.

Aktualnie jeszcze nie wiadomo, jak działałby ten system, jednak nie wyklucza się np. możliwości stworzenia konia trojańskiego, który byłby niepostrzeżenie instalowany na komputerze podejrzanego. Program ten cały czas monitorowałby działanie komputera przy czym określone informacje, jak np. hasła dostępu do zakodowanych danych byłyby wysyłane do FBI.

3.1.2.3 RIP - Regulation of Investigatory Powers

W Wielkiej Brytanii w czerwcu 2000 roku parlament zatwierdził ustawę dotyczącą systemu RIP (*Regulation of Investigatory Powers*). RIP[26] zostało stworzone, by ścigać internetowych przestępców, w tym pedofili. Określa ono procedurę postępowania przedstawicieli prawa przy przechwytywaniu poczty elektronicznej wysyłanej przez podejrzanych i podczas śledzenia ich działalności w Internecie. Według niej wszyscy dostawcy muszą wysyłać w czasie rzeczywistym kopie danych do najbliższej jednostki policji. W odróżnieniu od Rosji, w Wielkiej Brytanii dopuszczalne jest chronienie prywatności poprzez szyfrowanie wiadomości. W obu krajach w ręce policjantów trafiają wszystkie dane - zarówno korespondencja podejrzanych o popełnienie przestępstw, jak i zwykłych obywateli. Według brytyjskiego *Sunday Times*, królewski kontrwywiad M15 rozpocznie budowę gmachu, w którym przeprowadzana będzie analiza przechwytywanych listów elektronicznych. Budowa GTAC (*Government Technical Assistance Centre*) pochłonie 25 milionów funtów. Do tego dochodzą jeszcze koszty śledzenia, które oszacowano na 30 milionów funtów rocznie. Nadmiar zgromadzonych danych doprowadzi prawdopodobnie do zmiany regulacji mówiącej o obowiązku przechowywania ich przez siedem lat.

3.1.2.4 SORM

Od kilku lat znana jest sprawa programu SORM (*Sistiema Opieratiwno-Rozysknych Mieropriatij*), używanego przez rosyjskie służby bezpieczeństwa do inwigilacji korespondencji elektronicznej. W 1998 roku wydany został dekret dotyczący systemu mającego umożliwić inwigilację internetową obywateli Rosji -

---

[26] http://www.fipr.org/rip

SORM-2[27] (System for *Operational Research Actions on the Documentary Telecommunication Networks*). Ministerstwo Sprawiedliwości zobowiązało rosyjskich dostawców Internetu (w tym firmy dostawcy usług ISP – *Internet Services Provider*) do przekazywania Rosyjskiej Federalnej Służbie Bezpieczeństwa (FSB), będącej spadkobierczynią KGB, kopii całości informacji przesyłanych z i do sieci. Gdy jeden z dostawców nie zgodził się z tym dekretem zagrożono, że jego licencja zostanie cofnięta.

Gdyby wydano to w formie ustawy, musiałaby ona być przegłosowana przez rosyjską Dumę. W ten sposób uniknięto niepewności co do wyników głosowania. SORM-2 ma jeszcze jedną „przewagę" nad programem amerykańskim. W Rosji wymagana jest zgoda sądu lub prokuratury do założenia podsłuchu telefonicznego, jednak aby ułatwić sobie życie szefowie Ministerstwa Sprawiedliwości oraz Służby Bezpieczeństwa podali sobie ręce i stwierdzili, że dotychczasowe przepisy nie odnoszą się do nowego zjawiska, jakim jest poczta elektroniczna przesyłana Internetem. Zgoda sądu lub prokuratury do jej przeglądania nie jest zatem wymagana. Oto jak prosto poradzono sobie z tym problemem. Aby jeszcze bardziej ułatwić życie tym, którzy dbają o to, aby naród nie był mądrzejszy od władzy i nie przerywał jej błogostanu, w 2000 roku prezydent Putin wprowadził przepis, na mocy którego SORM-2 może być używany także przez inne służby, np. celne lub podatkowe. Użytkownicy internetu mogą chronić się przed takimi niecnymi praktykami, używając programów typu PGP, czyli szyfrujących przekazywane dane, ale w Rosji są one zakazane, jeżeli nie mają certyfikatu przyznanego przez FSB. Na razie nie mają, a będą go mieć wtedy, gdy specjaliści od kryptologii umożliwią służbom federalnym łamanie algorytmów szyfrujących.

SORM-2 różni się od Carnivore'a tym, że do podsłuchiwania nie jest potrzebne uzyskanie ani zgody sądu ani prokuratora. Kolejna różnica dotyczy finansowania całego przedsięwzięcia. W Rosji wszystkie koszty związane z wprowadzaniem wspomnianego dekretu w życie ponoszą dostawcy usług internetowych. Ważne jest orzeczenie Sądu Najwyższego, według którego dekret regulujący sprawy związane z SORM-2 nie jest ustawą, gdyż nie został uchwalony przez Dumę.

---

[27] http://jedi.konsnet.ru/sorm lub http://ipsec.pl/opsec/article/171

Na Ukrainie prezydent Kuczma planował we wrześniu 1999 roku wprowadzenie rozwiązania opartego na systemie SORM-2. Propozycja ta została jednak odrzucona przez parlament. Niemniej jednak kontrola przeprowadzona miesiąc wcześniej wśród dostawców usług internetowych wykazała, że system ten był wykorzystywany już przez niektórych z nich.

3.1.2.5 Rozporządzenie Ministra Infrastruktury z 24 stycznia 2003 r.

W grudniu 2000 roku Ministerstwo Spraw Wewnętrznych i Administracji złożyło projekt nowego rozporządzenia „w sprawie szczegółowych wymagań i sposobu wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego”[28]. To rozporządzenie wydane miałoby być przez ministra łączności. Projekt ten przedstawiał w skrócie, jak mają postępować operatorzy telekomunikacyjni, by umożliwić realizację zadań na rzecz obronności państwa.

Wiele punktów tego projektu budziło poważne zastrzeżenia zwłaszcza ze strony dostawców usług internetowych. Projekt nie określał jednoznacznie kto jest uprawniony do otrzymywania informacji pochodzących z podsłuchu. Poza tym operatorzy telekomunikacyjni musieli „ponosić koszty związane z zakupem systemów, ich instalacją, uruchomieniem, eksploatacją i utrzymaniem”. Oznaczało to, że musieli by pokrywać wszelkie koszty aż do czasu pełnego zautomatyzowania. Wprowadzenie tego projektu w życie oznaczało by wydatki nie tylko na sprzęt, ale również na opracowanie odpowiedniego oprogramowania. Dostawcy usług internetowych szacowali, że poniosą koszty od kilku do kilkunastu tysięcy złotych miesięcznie. Poza tym koszty obejmowały by również sfinansowanie łączy od siedziby dostawców usług internetowych aż do organów wymienionych w artykule 40 ust 2. Prawo Telekomunikacyjne[29].

---

[28] http://www.isoc.org.pl/2001/rozporzadzenie_mswia/projekt.pl.html

[29] Obowiązek, o którym mowa w ust. 1, dotyczy zapewnienia, na koszt operatora, technicznych i organizacyjnych możliwości wykonywania w sieci telekomunikacyjnej eksploatowanej przez operatora zadań na rzecz prokuratury, sądów, a także uprawnionych jednostek organizacyjnych podporządkowanych Ministrowi Obrony Narodowej, uprawnionych jednostek organizacyjnych podległych ministrowi właściwemu do spraw wewnętrznych, ministrowi właściwemu do spraw finansów publicznych oraz Szefowi Urzędu Ochrony Państwa, począwszy od dnia rozpoczęcia eksploatowania tej sieci, jeżeli Prezes URT nie ustali, na wniosek zainteresowanego operatora, późniejszego terminu.

Dodatkowym utrudnieniem było wymaganie, by informacje przekazywane były w postaci niezaszyfrowanej, jeśli operator szyfruje dane. Ponadto niejasnym punktem był okres archiwizowania danych, co wiązało się z utrzymaniem odpowiednio dostosowanych systemów przechowywania danych.

Przeciwko proponowanemu przez MSWiA projektowi rozporządzenia protestowali właściwie wszyscy - dostawcy Internetu, zwykli jego użytkownicy, prasa. Negatywne stanowisko zajęła też Polska Izba Informatyki i Telekomunikacji[30], której MSWiA przekazało projekt do zaopiniowania, uzasadniając, że wprowadzenie go w życie sprawiłoby, że byliby podsłuchiwani nie tylko przestępcy, ale każdy obywatel. Pod znakiem zapytania stanęłaby poufność tajemnic handlowych, które przesyłane są za pomocą Internetu. Nie istniałaby również kwestia prywatności korespondencji.

Wszelkie dyskusje na ten temat zakończyło „Rozporządzenie Ministra Infrastruktury z 24 stycznia 2003 roku opublikowane w Dz. U. z dnia 7 lutego 2003 roku".

Rozporządzenie określiło, iż każda firma internetowa musi zainstalować sterowany z zewnątrz system, pozwalający organom bezpieczeństwa na dostęp w dowolnym momencie do dowolnych przesyłanych danych; co więcej, system ten musi także archiwizować cały ruch przechodzący przez sieć firmy przez bliżej nieokreślony czas.

Całkowicie odrębną, a niezwykle istotną sprawą jest kwestia naruszania przez proponowane rozwiązanie praw obywatelskich - m.in. tajemnicy komunikowania się, która zgodnie z Konstytucją RP może być ograniczona jedynie w przypadkach określonych w ustawie. W proponowanym rozwiązaniu służby specjalne mogłyby podsłuchiwać ruch w sieci wedle własnego uznania i bez jakiejkolwiek kontroli; nikt nie wiedziałby o tym, czy jest podsłuchiwany i dlaczego.

Wnioski ogólne.

Z powyższych rozważań wynika, że prognozując system rozpoznania XXI wieku powinniśmy założyć, iż musi się on kierować racjonalnymi działaniami, opartymi na błyskawicznym zdobywaniu, opracowywaniu i rozpowszechnianiu

---

[30] http://ipsec.pl/ipsec/article/291

informacji. Dla nikogo przecież nie ulega wątpliwości, że ilość i jakość informacji dostarczona przez system rozpoznania ma i będzie miała bezpośredni wpływ na dowodzenie i jego efekty.

Osiągnięcia naukowo-techniczne spowodowały jakościowy skok w rozwoju niektórych środków rozpoznania, ale przede wszystkim nowych sposobów zdobywania, opracowywania i przekazywania zdobytych informacji. W tej dziedzinie, obok rozwoju fotografii (możliwości w tym zakresie ogromnie wzrosły), pojawiła się i wciąż jest doskonalona technika skanowania za pomocą urządzeń optoelektronicznych i radiolokacyjnych. Ponadto w rozpoznaniu obrazowym prace badawcze prowadzone są w obszarze czterech technik: fotografii, techniki infralokacji (termolokacja), telewizji i radiolokacji.

Według ocen specjalistów wojskowych z dziedziny rozpoznania lotniczego, najbliższe lata mają być okresem prac nad realizacją programów budowy nowych bezzałogowych aparatów latających. Obecnie aparaty rozpoznawcze zostały opracowane pod kątem spełnienia podstawowych wymagań, stawianych systemom na przyszłym polu walki. Przyszłościowymi ich zaletami ma być: uniwersalność, niski koszt budowy i eksploatacji, łatwość obsługi i krótki czas przygotowania do startu.

Efekty rozpoznania zobrazowane mają być na cyfrowej mapie wojskowej, a doskonalenie polegać ma na rozwiązaniu problemów wynikających z ograniczeń sprzętu używanego do wyświetlania. Istnieje możliwość wprowadzenia mechanizmów pozwalających na uproszczenie użytkowania map indywidualnych (tematycznych) na stanowisku pracy użytkownika. W tym celu proponuje się dwustopniową procedurę na oddzieleniu generowania map cyfrowych od ich użytkowania w systemie.

Nowe możliwości zobrazowania sytuacji na mapie wojskowej mają być udoskonalane dzięki rozwojowi grafiki komputerowej (zwłaszcza udoskonaleniu jakości generowanych obrazów), budowaniu złożonych systemów w czasie rzeczywistym (np. systemów wizualizacji dla potrzeb działań zbrojnych), a także - co wymaga podkreślenia - dzięki metodom symulacji rzeczywistości. Wynika stąd twierdzenie, że obszar zastosowań grafiki komputerowej wykroczy daleko poza metody prezentacji danych w postaci różnego rodzaju wykresów czy animacji dla potrzeb gier symulacyjnych.

W przyszłości systemy dowodzenia wykorzystywać muszą systemy łączności szerokopasmowej oraz łączność satelitarną. Generalnie dąży się do funkcjonalnej integracji i unifikacji systemów łączności i informatyki, czyli do utworzenia jednej platformy systemowej dla wszystkich rodzajów usług. Praktycznie użytkownicy będą mieli dostęp do wszystkich niezbędnych systemów i podsystemów informacyjnych, używając jednego komputera. Ponadto są prowadzone prace nad rozszerzeniem zdolności transmisyjnych sieci oraz nad zwiększeniem mobilności systemów łączności i informatyki.

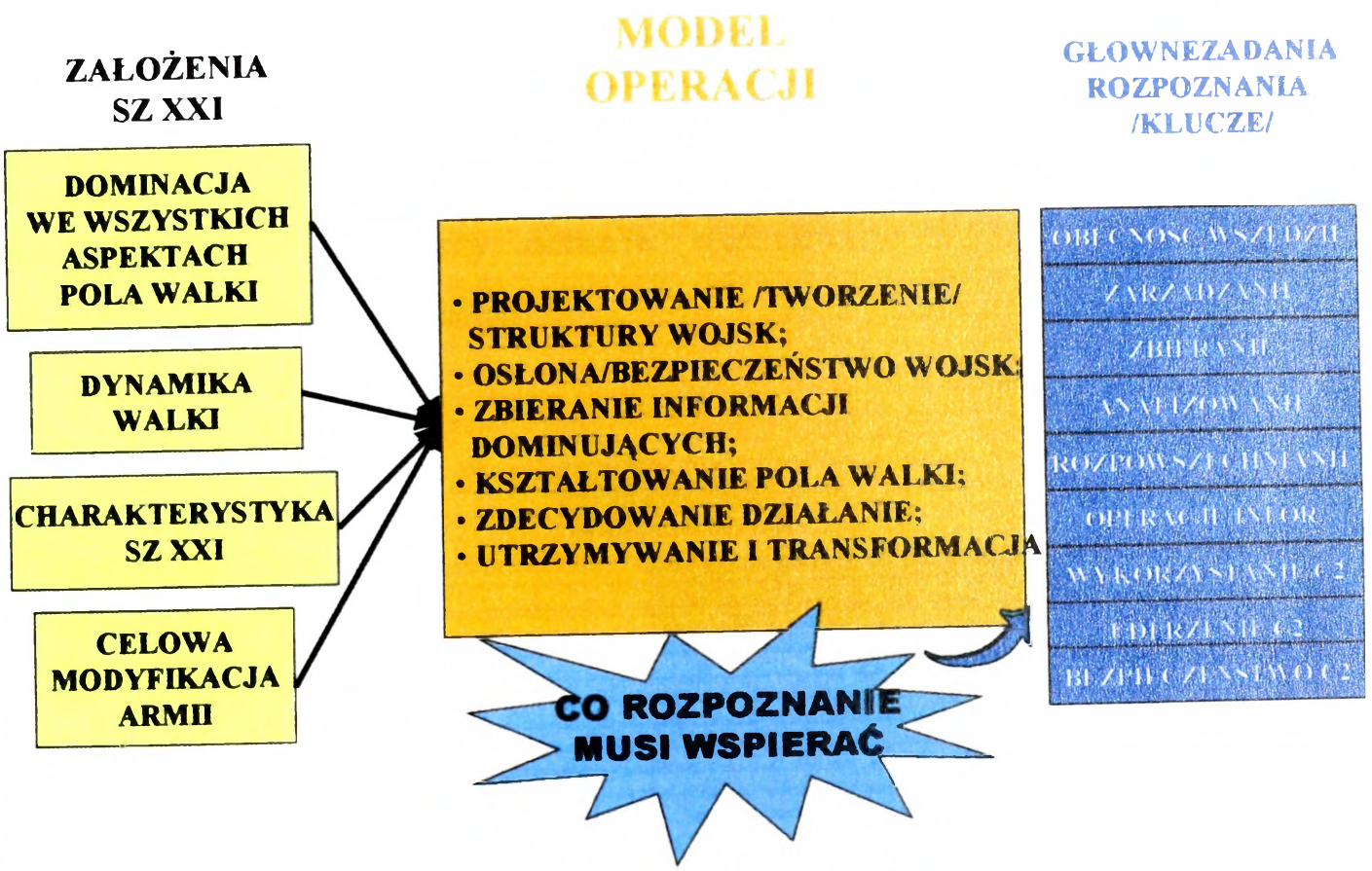
Ponadto w niektórych państwach w dalszym ciągu prym wieść będą systemy rozpoznania satelitarnego, dzięki którym zapewni się systematyczną kontrolę ogromnej ilości informacji pod względem militarnym, gospodarczym, stanu środowiska, pogody itp., co w konsekwencji doprowadzi do globalnego rozpoznania. Różnorodne urządzenia rozpoznawcze, w połączeniu z komputerami oraz dokładnymi danymi, pozwolą na maksymalne odciążenie użytkowników.

Dla skrócenia czasu upływającego od rozpoznania do zniszczenia przeciwnika buduje się systemy rozpoznawczo-uderzeniowe, które mają być podstawowymi środkami walki. Potwierdzeniem może być amerykański program robotyzacji pola walki. Przewiduje się, że rozwiązania z tego zakresu wykorzystywane będą m.in. do realizacji zadań związanych z rozpoznaniem, wyszukaniem celu, rozmieszczeniem czujników pomiarowych itp.

Właściwe (tj. szybkie i sprawne) wykorzystanie nowych technologii informacji może przyczynić się do zdobycia kluczowych informacji niezbędnych do realizacji zadań. Nowoczesne technologie informowania oraz sprzęt użyty do ich nadzorowania są w stanie przeobrazić świat w „globalną wioskę", ale przy splocie szczególnych sytuacji możemy otrzymać mieszankę „spamu". Informatyzacja społeczeństwa zrodziła tzw. „efekt CNN", co oznacza, że ilość informacji oraz coraz krótsze cykle przekazywania wiadomości redukują czas przeznaczony na ich przetworzenie.
Już choćby z tego pobieżnego opisu wynika, że działalność uczestniczących w konflikcie stron, wymaga korzystania z wielu różnorodnych zasobów informacyjnych zdolnych do efektywnego ich pozyskiwania, przechowywania, przetwarzania i rozpowszechniania.

3.2 DZIAŁALNOŚĆ ROZPOZNAWCZA W NOWYM WIEKU

Można założyć że, działalność rozpoznawcza w XXI wieku będzie realizowana przez wykonywanie zadań przedstawionych na rysunku 3.10.



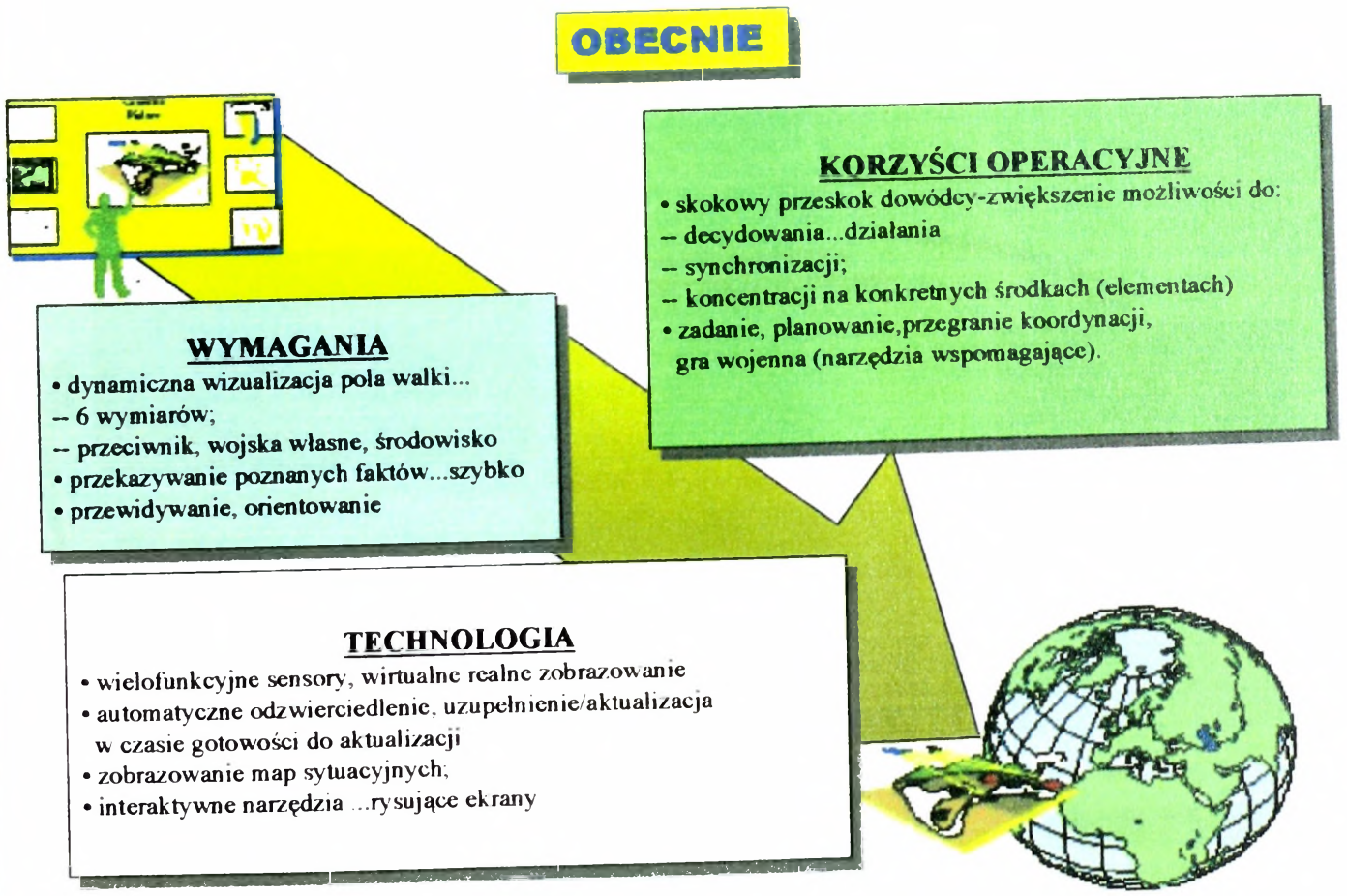
Rys. 3.10. Zadania rozpoznania

Określając założenia dla przyszłościowego systemu rozpoznania zaczęliśmy od analiz wymagań SZ XXI wieku. Wymagania te zostały wyprowadzone jako efekty analiz dokonanych w ramach prac naukowo badawczych i ćwiczeń, przez autorytety w zakresie myśli wojskowej, poszukiwano odpowiedzi jak walczyć, jakie dostarczyć „zdolności" dowódcy by mógł prowadzić działania (operacje) rozstrzygające (rys.3.11).

Przedstawiono, że aktualny system rozpoznania nie spełnia wymagań, pełnej percepcji różnych czynników obszaru działań i zrozumienia wszystkiego, co „przedstawiają" źródła/środki informacji. Ustalono, że obecnie wiedza dowódcy -

oparta na zrozumieniu obszaru działań i sytuacji przeciwnika - jest głównie uzyskiwana z obrazu obszaru działań jaki dostarczy system rozpoznania.

Ponadto, wyartykułowano zdolności dowódcy, który przewiduje trudne decyzje oraz analizuje opcje aby zmniejszyć niepewność działania w czasie kiedy decyzje są opracowywane. Podczas działań dynamicznych jego percepcja jest powiązana z prognozowaniem wariantów działania oraz rozpoznaniem obecnych działań przeciwnika, jego zamiarów w czasie i przestrzeni. Przedstawianie tych obu działań (własnych i przeciwnika) podczas procesu gry wojennej, jak również podczas rozwijania działań, dostarczy obrazów wirtualnych, by otrzymać dynamiczny połączony obraz obszaru działań.

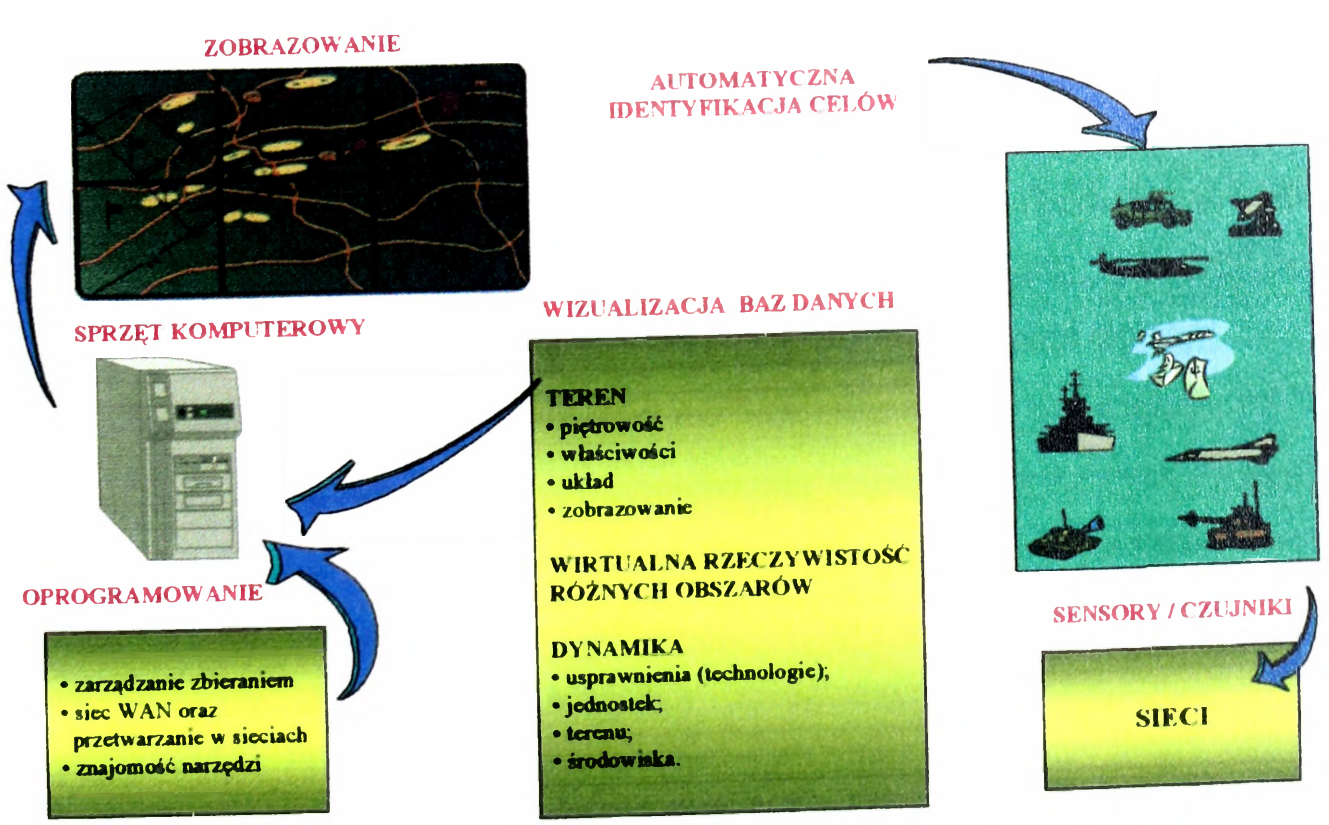


Rys. 3.11. Wymagania SZ w zakresie rozpoznania

System rozpoznania musi być w stanie, tworzyć dokładny, zwięzły o dużej wierności wirtualny obraz obszaru działań a ponadto łączyć to z ogólną sytuacją, pogodą i danymi terenu (o dużej rozdzielczości) dając podstawę, do projektowania

obrazu dla dowódcy. Ten wspólny obraz, musi pomóc dowódcy w natychmiastowym zrozumieniu aktualnej i przyszłej sytuacji musi on więc „widzieć" obszar działań i przygotować optymalne (inteligentne) decyzje. To jest klasyczny cykl rozpoznawczy oraz kierowanie wymaganiami i zdolnościami zgodnie z otrzymanym zadaniem. Przedstawiona „prezentacja" powinna być przygotowana przez zespół wysoko wykwalifikowanych, dobrze wyszkolonych żołnierzy operatorów/zwiadowców, którzy potrafią i umieją analizować zagrożenie, pogodę i teren w kontekście określonej sytuacji a nie tylko wymagań dowódcy.

Taka „prezentacja obszaru działań jutra" powinna się ewoluować od mapy do cyfrowego ekranu ukazującego graficzne i tekstowe meldunki rozpoznawcze, sprawozdania - ilustrując cyfrowy pokaz wirtualnej rzeczywistości, który przynosi obszar działań (rys. 3.12).



Rys. 3.12. Technologia wizualizacji obszaru działań

Elektroniczne oleaty muszą być uaktualniane dynamicznie, by dodać zmiany w sytuacji (zmienią wartość albo usuną informację) i ukazywać wpływ pogody, bazując na właściwościach terenu zapisanych elektronicznie (***DTED*** - *Digital Terrain and Elevation Data*) oraz wszystkie dane przesyłać w czasie realnym. Informacje powinny być zobrazowane (np. na płaskim panelu 2D lub 3D), zdolnym do przekazu wizualnego, obrazów graficznych i filmów wideo oraz obrazów wirtualnych z wielokrotnymi zdolnościami pokrycia ekranu różnymi informacjami - każdy fragment ekranu pokazuje inną funkcję multimedialną.

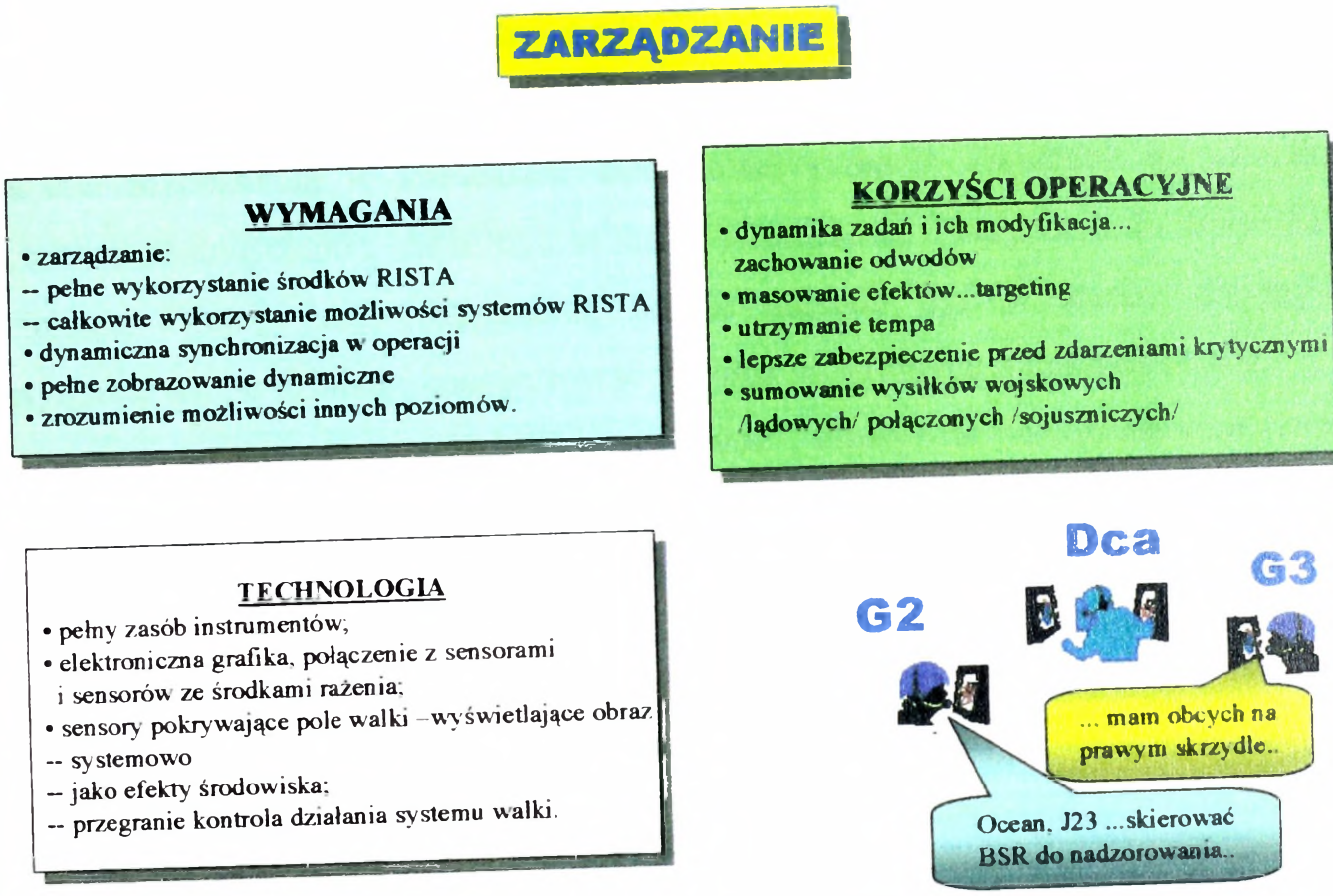
Dźwiękowe i wizualne informacje tzw. audio-informacje i współpracujące narzędzia (tablice elektroniczne) powinny być używane, by dynamicznie odtworzyć i skoordynować „prezentację" dla pełniejszego zrozumienia. Ponadto automatyczna aktualizacja będzie alarmować oficera/operatora, jeśli obraz będzie uaktualniany/zmieniany. Technologia „prezentacji" powinna wspierać planowanie zadań, grę wojenną, treningi i zapewni sprawne wykonanie zadań.

Przyszłe zdolności systemu „Rozpoznania XXI wieku" w dziedzinie „prezentacja" muszą reprezentować „milowy" skok w możliwości dowódcy, by zdecydowanie wesprzeć działania i racjonalnie wykorzystać posiadane siły. Wartość rzeczywista będzie zrozumiana pełniej, gdy dowódca/użytkownicy utwierdzą się w przekonaniu, że dzięki systemowi rozpoznania utrzymują stałe tempo działań, mają lepsza skuteczność rażenia i poprawione zdolności w przetrwaniu wojsk.

Zakładam, że operatorzy systemów rozpoznawczych obowiązujących w XXI wieku, będą wymagać pełnego oprogramowania, narządzi użytkowych do korzystania z bogatych zasobów informacji o charakterze organicznym, połączonym, narodowym i wielonarodowym itp.

Wejścia od wszystkich sensorów (załogowych i bezzałogowych) z obszaru odpowiedzialności i zainteresowania, muszą zostać połączone i być odpowiednio zarządzane, by dostarczyć w realnym czasie, dokładnego wspólnego obrazu obszaru działań. W konsekwencji, „działalność rozpoznawcza" musi wyjść poza tradycyjną działalność opartą na przetwarzaniu informacji i brać pod uwagę wszystkie wyniki działań rozpoznawczych z różnych źródeł informacji, stąd też wzrost roli rozpoznania celów, nadzorowania obszaru działań itp.

Aby powyższe założenia mogły zostać osiągnięte każdy z (uprawnionych) operatorów systemu musi widzieć sytuację i miejsca rozmieszczenia elementów - źródeł informacji w aspekcie poziomym i pionowym (powietrzno-lądowym) umożliwiając tym samym skuteczną koordynacje i synchronizację zadań (rys. 3.13).



Rys. 3.13. Zarządzanie

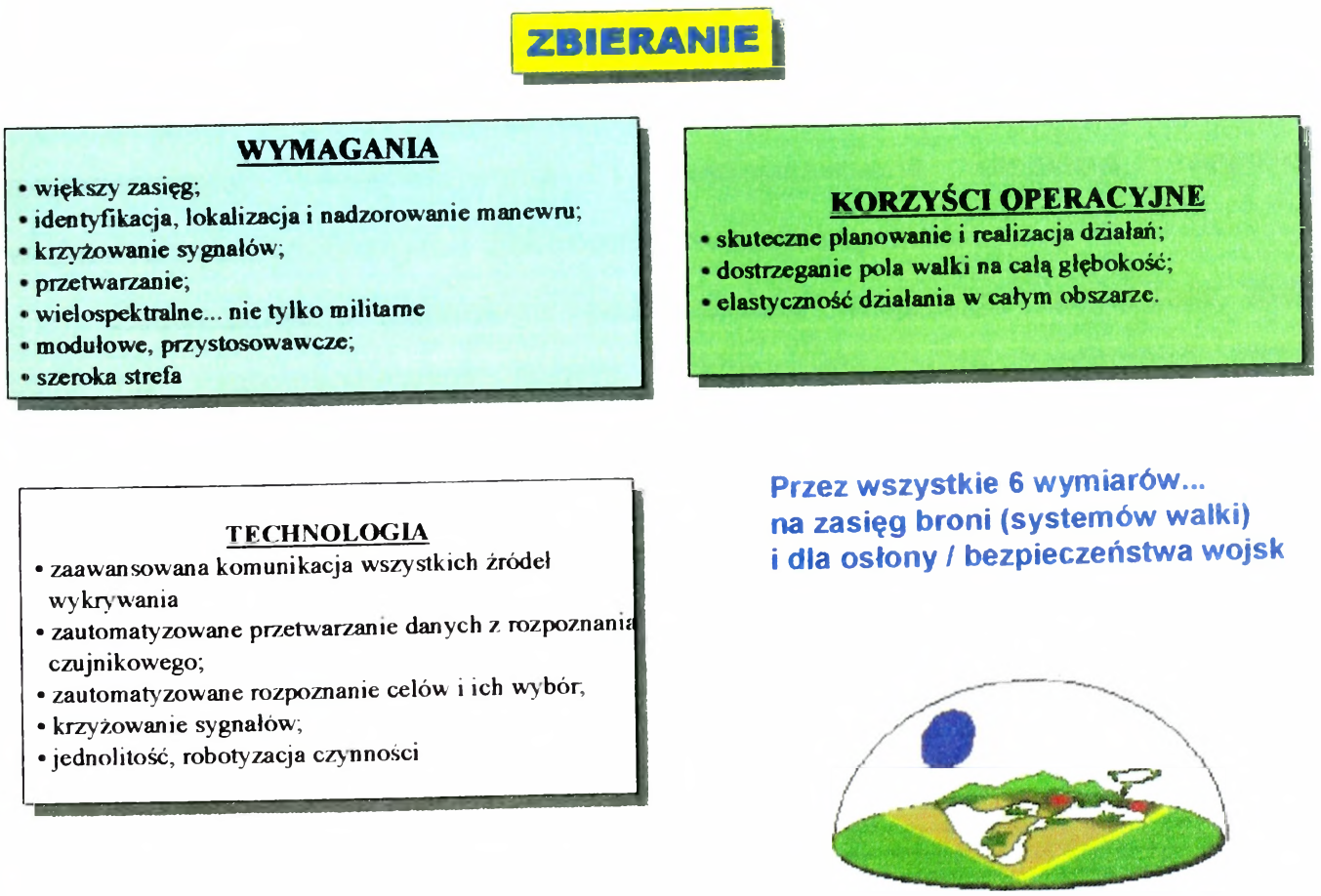
Żeby skutecznie zarządzać systemem i jego podsystemami RSTA[31] w przyszłości, operatorzy megasystemu muszą być w stanie dynamicznie planować, koordynować i synchronizować systemy rozpoznania używając wizualnych pokazów, wykorzystując narzędzia oraz automatyzowane macierze synchronizacji. Ponadto, muszą być w stanie widzieć w rzeczywistym czasie wykonywanie zadań rozpoznawczych w działaniach i analizować wiadomości postrzegane przez sensory. Muszą też być w stanie widzieć i łączyć informacje w relacji sensor do sensora i sensor do wykonawcy, wykonawca do wykonawcy. Ponadto muszą wiedzieć jak

[31] **RSTA** - *Reconnaissance, Surveillance, and Targeting Acquisition*

utrzymać obszar pod nadzorem systemu rozpoznania i mieć pokrycie na wszystkich obiektach poziomo i pionowo. Z takimi możliwościami, operatorzy rozpoznania będą w stanie dynamicznie reorganizować system i przecelowywać zadania oraz przesuwać skupienie wysiłku rozpoznania, aktualizując pokrycie obszaru sensorami a tym samym mogą skuteczniej lokalizować i śledzić istotne cele.

Dynamiczne działania wymagają, by dowódca miał prawdziwy obraz realizowanych działań rozpoznawczych. Taka „nowa walka" powinna pokazywać graficznie rozpoznanie i obiekty/cele RSTA, ponieważ dowódca musi postrzegać zadania rozpoznania w kontekście całościowej sytuacji. Dowódca w przyszłości (z takimi zdolnościami), może być w stanie skuteczniej i bezpośrednio wpływać na działania. Dlatego też, rozpoznanie będzie musiało być w stanie utrzymywać optymalne tempo działań i koncentrować wysiłek na istotnych obiektach/celach.

Sensory powinny „widzieć" i „rozumieć", dlatego w wielofunkcyjne sensory muszą być zaopatrzone wozy bojowe, samoloty (załogowe i bezzałogowe) oraz żołnierze na ziemi, powietrzu, morzu i przestrzeni (np. kosmicznej) (rys.3.14).



Rys. 3.14. Zbieranie

Trend w naszych przyszłych systemach zbiorów informacji powinien zmierzać do modułowego i węzłowego systemu. Moduły powinny być w pełni automatyczne, o szerokim obszarze działania i gromadzenia danych/informacji oraz określonej precyzji lokalizacji. Projektowanie architektury otwartej, by wspólną technologią zewrzeć środowisko użytkowe powinno pozwolić takim systemom, rozwinąć swoje możliwości. Przyszłe systemy muszą ponadto dostarczyć wielospektralnego wizerunku dla pokładowego przetwarzania. Bezzałogowe aparaty i sensory naziemne oparte na robotach i mikroelektronicznych maszynach, powinny działać razem, by zrealizować pokrycie w obszarach niedostępnych do konwencjonalnych środków rozpoznawczych. Pojedyncze platformy powinny być w stanie nosić, wielokrotne typy modułów sensorów i wspierać szybkie wykorzystanie inteligentnych i doskonałych systemów broni.

System zbiorów danych w rozpoznaniu XXI wieku, powinien umożliwić dowódcy zobaczyć i uchwycić całkowity (globalny) obszar działania z dużą wiernością. Dlatego rozpoznanie musi dostarczyć dowódcy informacji, których potrzebuje, aby zrozumieć określone pole walki i rozmieścić swoje wojska oraz zidentyfikować i wyśledzić istotne obiekty/cele.

Przyszłe systemy rozpoznania, ponadto powinny wymagać automatycznego rozpoznawania, identyfikowania i umiejscawiania obiektów rozpoznania w akustycznym, widocznym i elektromagnetycznym spektrum.

Zaawansowane technologie przetwarzania wstępnego, zawierające techniki takie jak zautomatyzowany system wskazywania celów (obiektów) (ATR)[32], wykrywanie zmiany sytuacji i określanie poszczególnych rodzajów obiektów przeciwnika zdejmując ich elektroniczne odciski palców muszą zostać skierowane do sensorów i procesorów, by szybko zidentyfikować i wyśledzić istotne cele. Będą też wymagane nowe technologie sensorów skierowanych na wykrywanie rozwiniętego kamuflażu przeciwnika i urządzenia do ukrycia oraz maskowania wojsk własnych. Wszystkie narzędzia mogą być wykorzystane we wsparciu HUMINT[33] (osobowych źródeł informacji).

---

[32] **ATR** - *Automated Target (object) Recognition.*
[33] **HUMINT** – *Human Intelligence*, por. *Rozpoznanie Wojskowe*, Doktryna Połączona, Szt. Gen. 1531/2001, Warszawa 2001, s. 18.

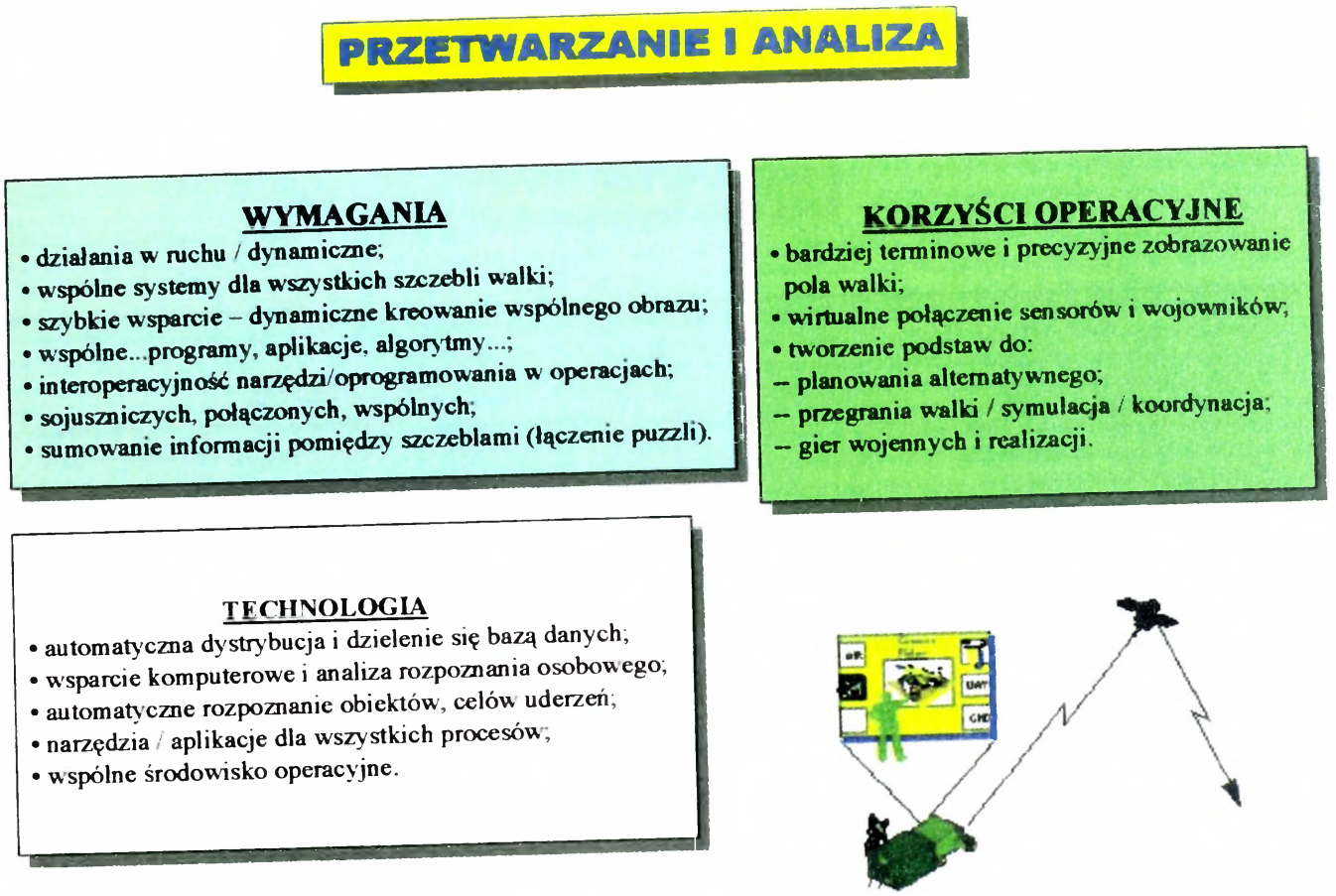
Zdolność, by gruntownie zrozumieć i zobaczyć pole walki, pozwoli sztabom, skuteczniej zaplanować i wykonać operacje decydujące. Jednakże, to wymaga dużego spektrum sensorów - opisanych powyżej - po to aby zebrać dane potrzebne dowódcom i sztabom oraz właściwie zwizualizować i zrozumieć ich przestrzeń działania.

Przetwarzanie i analiza przemienia dane z obszaru działań na informację do zrozumienia i ostatecznie do efektywnego opracowania decyzji. Ponieważ wzrasta dynamika obszaru działań rośnie również ilość i szybkość operacji realizowanych na informacjach. Dlatego, rozpoznanie XXI wieku, musi rozwinąć systemy wspólne do wszystkich poziomów dowodzenia, w celu szybkiego przetwarzania, analizy i przepustowości danych/informacji oraz jednocześnie skupić agregację informacji oraz zapewnić wnioskowanie uprzedzające od góry na dół do poziomu brygady/batalionu. Właściwości systemu muszą ponadto uwzględniać przetwarzanie i analizę danych/informacji rozpoznawczych w ruchu (rys. 3.15).

Zdolność do szybkiego przetwarzania i analizy danych wymaga systemu, który dostarczy połączenia wirtualnego między źródłami rozpoznawczymi a „centrum dowodzenia" ze skutecznym filtrowaniem, by zapobiec zatorom informacyjnym. Stąd też rozproszone przetwarzanie danych i ich analiza musi być porównywana z wynikami w bazie centralnej, do której dostęp musi być gwarantowany stosownym akcesem. Aplikacje i algorytmy muszą być standaryzowane przez wielopoziomowe bezpieczne systemy informatyczne znajdujące się na wszystkich poziomach. Ponadto systemy muszą zoptymalizować wykorzystanie użytkowych danych dotyczących środowiska oraz wspólnych aplikacji programowych, aby dostrzegać poziomy i pionowy wymiar zagrożenia. Aby powyższe możliwości mogły być zrealizowane wymagane są określone narzędzia współdziałania, by zapewnić szybki przepływ danych z baz i transfer grafiki z wielonarodowych źródeł rozpoznawczych.

Przyszłe przetwarzanie i zdolności analizy muszą ponadto zapewnić szybkie i dynamiczne tworzenie wspólnego obrazu dowódcy. Analitycy muszą być w stanie ustawiać zautomatyzowane alarmy i używać automatycznych procedur dla uzyskiwania dostępu do odległych baz danych. By pomóc analitykom w określaniu znaczenia poszczególnych informacji z materiału analizowanego, wymagane są narzędzia sztucznej inteligencji, które umożliwiają automatyczne rozpoznanie

przedmiotów, istot, albo obiektów/celów oraz pozwolą analitykom dynamicznie zmienić określone parametry albo zestawy reguł. Wreszcie, analitycy muszą być w stanie odwzorować sytuację przeciwnika „na żywo" żeby dowódca mógł szybko zrozumieć i przystąpić do działania według czegoś co „widzi i rozumie".

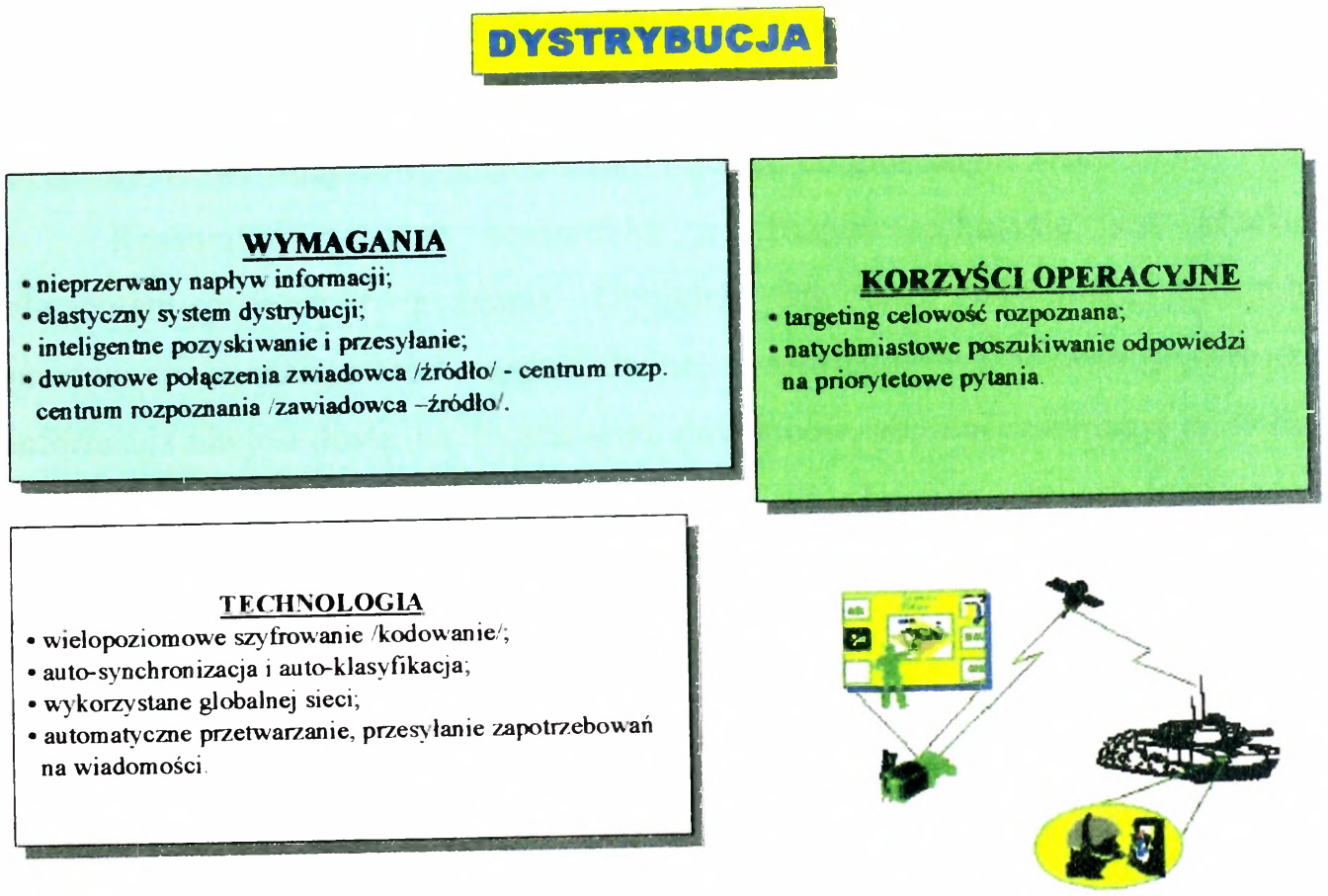


Rys. 3.15. Przetwarzanie i analiza danych/informacji

Wartość informacji w określonym czasie będzie związana z dokładną wizualizacją obszaru działania. To umożliwi dowódcy zdolność, by poznać i zrozumieć możliwości zagrożenia, w stosunku do terenu, pogody i aktualnej sytuacji. Zjawisko to przekształci informację w zrozumienie, żeby dowódca mógł skuteczniej prowadzić decydujące działania. Założenie dla działania jest następujące: planowanie, gra wojenna, kontrola i wykonanie, dlatego wsparcie informatyczne musi być stosowne do zabezpieczenia wszystkich faz działań dla pokoju, kryzysu i wojny.

Rozproszenie sił i tempo działań będzie nakazywało, dostarczyć prowadzącym działania nieprzerwanego strumienia informacji w ruchu. Ponieważ siły (biorące udział w działaniach) rozpraszają się i prowadzą rozproszone działania, elastyczne

rozpowszechnianie informacji staje się istotnym wymogiem. Bez tego rozpoznanie XXI wieku nie będzie w stanie, dostarczać dowódcy koniecznej wizualizacji jego przestrzeni działania. Technologia powinna być wykorzystywana, by zapewnić automatyczne rozpowszechnianie informacji na w różnych poziomach jej klasyfikacji i wśród użytkowników (rys. 3.16).



Rys. 3.16. Dystrybucja danych/informacji

Wielowariantowe sposoby (technologie) przesyłania informacji typu: „*Smart Push*"[34] – „*Smart Pull*[35]" umożliwią, żeby informacja przekazana przez prowadzących działania była automatycznie aktualizowana w bazie w oparciu o założone kryteria. Ponadto, automatyczne przetwarzanie „zapotrzebowania na informacje" przyspieszy

[34] *Smart push* /eleganckie wtłaczanie/- automatyczne przesyłanie przez przełożonego do podległych jednostek wojskowych danych rozpoznawczych według oceny i potrzeb.
[35] *Smart pull* /zręczne pozyskiwanie/ - możliwość poszczególnych jednostek wojskowych automatycznego dojścia pocztą elektroniczną do baz danych przełożonych, w zakresie otrzymania wymaganych informacji rozpoznawczych.

proces odpowiadania na PPR (PIR)[36] dowódcy. Jeśli informacja nie będzie natychmiast dostępna, stosowne narzędzia muszą określić priorytet poszukiwania odpowiedzi na zapotrzebowanie w trybie automatycznym. Nowe technologie muszą umożliwić dostępność baz danych bez przeciążania systemu komunikacji.

Zdolności systemu łączności (komunikacji) muszą zostać skonfigurowane tak, by umożliwić rozpowszechnianie danych ze źródeł bojowych takich jak czołgi, walcząc pojazdy, odległe bezzałogowe sensory, zwiadowcy, śmigłowce i systemy rozpoznania rodzajów wojsk. Wymagania rozpowszechniania zawierają: szerokość pasma na żądanie, dostęp według klucza, wielopoziomowy dostęp bezpieczeństwa, bezprzewodowe miejscowe sieci obszaru i dostęp do globalnych sieci.

Reasumując, można stwierdzić, że rozpowszechnianie jest kluczowym elementem procesu rozpoznania. Obojętnie jak dużo informacji jest zebrane, przetworzone, analizowane i zgromadzone, rozpoznanie jest bezwartościowe dopóki informacja nie jest dostępna, by wspierać dowódców, gdy oni potrzebują jej w formie, którą rozumieją. Wartość rozpowszechniania jest właściwa gdy rozpoznanie ma na celu dostarczenie do prowadzących działania informacji które zwiększają tempo działania, skuteczność rażenia i możliwości przetrwania.

3.2.1. Robotyzacja w środkach rozpoznawczych

Zakładam, że przyszłościowy system (systemy) rozpoznania powinien zapewnić realizację następujących funkcji:

- zdobywania, opracowywania, korelowania i zobrazowywania danych/informacji rozpoznawczych;
- oceny danych/informacji rozpoznawczych;
- nadzorowania płynnej sytuacji pola walki, w obecności przeciwdziałających czynników takich jak ataki przeciwnika, walka elektroniczna, zmęczenie, warunki pogodowe i terenowe;
- przekazywania lub otrzymywania rozkazów, informacji w czasie rzeczywistym.

---

[36] PIR - *Priority Intelligence Requirement.*

Aby powyższe funkcje mogły zostać zrealizowane, w koncepcjach nowych Sił Zbrojnych wprowadza się roboty wspierające zwiadowców. Systemy robotów to rozwiązanie perspektywiczne i korzystne z punktu widzenia bezpieczeństwa zwiadowcy a co się z tym wiąże obniżeniem poziomu strat w działaniach. Oprócz zakładanej możliwości realizacji niebezpiecznych zadań rozpoznawczych mają one zastąpić zwiadowców w wykonywaniu różnych czynności od zaopatrywania wysuniętych posterunków do działań rozpoznawczych i wyszukiwania obiektów/celów. W istocie chodzi o zminimalizowanie, a nawet wykluczenie, bezpośredniego niebezpieczeństwa powstania strat bezpowrotnych wśród zwiadowców.

Niektóre modele wojowniczych robotów (zwiadowców) przeszły już chrzest bojowy w Afganistanie. Małe pojazdy, wyposażone w wysuwane ramię i hydrauliczny podnośnik z kamerami telewizyjnymi pozwalają operatorom na prowadzenie wielospektralnej obserwacji. Takie pojazdy podczas wojny z Talibami zapuszczały się do jaskiń, skąd za pośrednictwem kamer przekazywały obraz do centrum dowodzenia.

Inne pojazdy-roboty wyposażone w aparaturę do wykrywania substancji chemicznych penetrowały obiekty położone w strefie zagrożenia. Konstrukcja robotów umożliwia podniesienie się po wywrotce, pozwala także pływać, wdrapywać się na schody, przedzierać przez śnieg i piasek. Rozpoznawcze automaty potrafią także samodzielnie trafić do bazy wykorzystując system nawigacji satelitarnej.

Konstruktorzy robotów pomni wniosków z walk na Bałkanach i w miastach Iraku budują urządzenia do najtrudniejszych działań bojowych toczonych na obszarach zurbanizowanych. Do działań w mieście opracowano projekt jednego z najmniejszych bezzałogowców rozpoznawczych - SUBOT (*Smalt Unit Robot*). Pragnąc rozpoznać sytuację za załomem muru, czy wzgórzem, zwiadowca rzuca złożonym SUBOT-em jak piłką w powietrze. Ten po osiągnięciu celu opada a uderzając o grunt zwalnia system blokujący i pojazd rozkłada się na dwie półkule, pełniące rolę kół jezdnych, wysuwa się stabilizujący ogon, uruchamia się kamera oraz inne urządzenia rozpoznawcze.

Amerykanie planują, aby lądowe pojazdy bezzałogowe mogły w przyszłości dostarczyć więcej informacji niż obecne bezpilotowe środki rozpoznania powietrznego

używane już powszechnie w działaniach. Dlatego też, dla równowagi rozpoznania bezzałogowego powietrznego i lądowego przewidziano budowę aż 7 typów bezzałogowych wozów bojowych o masie 16–18 ton w wersji rozpoznawczej a także transportujących bezpilotowe statki latające. Specjalną uwagę poświęcono 6-tonowemu cichemu robotowi-szperaczowi na 4 kołach, który w pierwszej fazie walki ma wykrywać rozmieszczenie sił lądowych potencjalnego przeciwnika. We wrześniu 2001r. na poligonie amerykańskim przetestowano już półtoratonowego, automatycznego szperacza - czterokotłowego, który w trudnym terenie, w misji rozpoznawczej osiągnął szybkość 35 km/h. Docelowo ma być jeszcze dwukrotnie szybszy.

Rodzinę super-robotów tworzą także różne typy latających bezpilotowców rozpoznawczych, dostarczane w rejon operacji przez bezzałogowe transportery. Mają to być aparaty przenoszące uzbrojenie i gotowe samodzielnie zaatakować wskazane cele, ale także mikro-roboty rozpoznawcze wlatujące do pomieszczeń, schronów, bunkrów i podziemnych ośrodków dowodzenia, wyszukujące środki rażenia, niszczące elementy systemów łączności.

Z technicznego punktu widzenia najciekawsze i najbardziej niezwykłe są kroczące automaty rozpoznawczo-ogniowe, które będą przypominać maszyny znane z filmowych scenariuszy wojen kosmicznych. Według planów FCS[37] stworzone zostaną trzy typy takich konstrukcji: logistyczny, bojowy i rozpoznawczy. Możliwości trakcyjne sprawią, że kroczące roboty towarzyszyć będą żołnierzom nawet w terenie górzystym[38]. Niektóre będą się mogły samodzielnie bronić, gdy zostaną zaatakowane przez przeciwnika.

3.2.2.Środki przekazywania informacji.

Newralgicznym elementem każdego systemu, od którego zależy jego sprawność i niezawodność jest komunikacja/łączność. Konieczność całkowitej kompatybilności środków zdobywania informacji ze środkami przekazywania

---

[37] *Future Combat System.*
[38]Konstrukcje przewidują połączenie pojazdu gąsienicowego jako stopy robota i systemu dźwigni – odpowiednika nogi człowieka.

informacji, oraz wymagania stawiane przepustowości (ilości przesyłanych bitów informacji w jednostce czasu), to podstawowe problemy do rozwiązania we współczesnych systemach dowodzenia i rozpoznania.

Podstawowymi czynnikami warunkującymi pracę systemów łączności są między innymi:

- wzrost liczby użytkowników (mobilna komunikacja);
- zapotrzebowanie na nowe usługi telekomunikacyjne;
- postęp w rozwoju mikroelektroniki;
- narzędzia do kontroli systemów rozpoznawczych.

Czynniki te charakteryzują się systematycznym wypieraniem tradycyjnych środków łączności analogowej i zastępowaniem ich bardziej rozbudowanymi systemami łączności cyfrowej.

Systemy łączności cyfrowej tworzą na ogół strukturę sieciową, składającą się z węzłów i wielokanałowych łączy. Zapewniają one łączność foniczną, transmisję informacji, bezpieczeństwo i zabezpieczenie danych/informacji, przekazywanie obrazów z rozpoznania itd. Tak szeroki zakres usług telekomunikacyjnych wymaga stosowania łączy o coraz większej przepustowości, co z kolei wymusza konieczność przechodzenia w łączności na coraz wyższe zakresy częstotliwości.

Przekazywanie drogą radiową i w czasie rzeczywistym obrazów telewizyjnych wykonanych w zakresach podczerwieni lub radiolokacyjnym wymaga zapewnienia szerokiego pasma częstotliwości oraz dużej szybkości transmisji, a tym samym i wysokich częstotliwości pracy.

Innym bardzo ważnym problemem w działalności rozpoznawczej jest przetworzenie i przekazywanie informacji. Informacje, uzyskane za pomocą wysokoczułych czujników, są wartościowe, mają jednak znaczenie tylko wtedy, gdy możliwe jest szybkie ich przetworzenie i przekazanie. Natomiast przetworzenie i przekazanie zdobytych informacji odbiorcom (znajdującym się na ziemi lub w powietrzu) w czasie bliskim rzeczywistemu będzie możliwe jedynie w zintegrowanym i zautomatyzowanym systemie gromadzenia, przetwarzania i przekazywania informacji.

Zmiany zachodzące w strategii, sztuce operacyjnej i taktyce narzucają, jak nigdy dotychczas konieczność uzyskiwania bardzo dokładnych, wiarygodnych i aktualnych informacji. Wzrost znaczenia rozpoznania i stawianie mu coraz wyższych wymagań stwarza z kolei potrzebę ciągłego rozwoju środków rozpoznawczych oraz doskonalenia organizowania i sposobów jego prowadzenia. Wzrasta zapotrzebowanie na supernowoczesne, systemy i środki rozpoznawcze, w których będą znajdować zastosowanie najnowsze osiągnięcia techniczne.

Reasumując, można stwierdzić, że pierwszoplanowego znaczenia nabiera obecnie ścisła współpraca oraz połączenie i koordynacja wysiłku w dziedzinie rozwoju zintegrowanych systemów dowodzenia, a w nich systemu (systemów) rozpoznania.

3.2.3. TENDENCJE ZMIAN W ROZPOZNANIU PATROLOWYM.

Ostatnie konflikty lokalne, a szczególnie wojna w Zatoce Perskiej spowodowały większe zapotrzebowanie na bojowe wozy rozpoznawcze (bwr), spełniające wymagania współczesnego i przyszłego pola walki. Podstawowe wymogi stawiane nowoczesnym (bwr) to możliwość przerzutu drogą powietrzną, zdolność do prowadzenia działań w ciągu całej doby i w każdych warunkach atmosferycznych (klimatycznych), wyższa ruchliwość i siła ognia oraz możliwość automatycznego określania swojej pozycji i przekazywania danych/informacji z posiadanych sensorów w czasie rzeczywistym.

Bojowe wozy rozpoznawcze nowej generacji powinny zezwalać na wykonywanie trzech zasadniczych zadań:

- rozpoznania walką (wóz silniej opancerzony i uzbrojony, wykorzystywany do rozpoznania i głębokiego obchodzenia pozycji wojsk przeciwnika);
- dalekiego rozpoznania (wóz lżejszy, przystosowany do skrytego przenikania w głąb ugrupowania bojowego przeciwnika, w celu rozpoznania rejonów, obiektów i ewentualna pomoc w kierowaniu ogniem własnych środków rażenia);
- ubezpieczenia bojowego (wóz silniej opancerzony i uzbrojony, który mógłby ogniem wstrzymać podchodzące pododdziały przeciwnika w czasie rozwijania lub wykonywania manewru przez wojska własne).

Z zadań tych wynika, że bwr nowej generacji powinien być pojazdem wyposażonym w następujące elementy:

- pancerz modułowy, umożliwiający demontowanie lub montowanie przez załogę dodatkowych jego elementów w warunkach polowych;
- automatyczne działko z precyzyjnym i szybkim systemem kierowania ogniem, która umożliwi prowadzenie ognia do celów naziemnych i powietrznych;
- automatyczne urządzenia obronne (czujniki do wykrywania opromieniowania i przeciwpancernych pocisków na torze lotu oraz pasywne i aktywne środki obrony);
- urządzenia identyfikujące „swój-obcy";
- najnowsze elektrooptyczne, radiolokacyjne i inne czułe sensory/urządzenia rozpoznawcze (umieszczone na wysuwanym wysięgniku), pozwalające na prowadzenie rozpoznania w każdych warunkach dnia i nocy, dokładne i szybkie określanie współrzędnych bwr i obiektów oraz w czasie rzeczywistym przekazywanie tych informacji do ośrodków zbierania informacji (np. amerykański SABRE).

Z badań przeprowadzonych przez Amerykanów w czasie wojny w rejonie Zatoki Perskiej wynika, że o sprawności bojowej zwiadowcy na przyszłym polu walki będzie w dużym stopniu decydowało m. in. indywidualne wyposażenie elektroniczne. Będzie ono miało duży wpływ na prawidłowe przygotowanie się zwiadowcy do działań oraz sprawne i precyzyjne jego działanie w czasie wykonywania zadania.

Prace nad zintegrowanym wyposażeniem osobistym żołnierza - zwiadowcy są najbardziej zaawansowane w Stanach Zjednoczonych. Program wybiega daleko w przyszłość oraz charakteryzuje się kompleksowością i możliwością jego wdrażania etapami (uzupełnienie istniejących elementów - nowymi). Realizacja programu przebiega w dwóch etapach: pierwszy - zakłada opracowanie zintegrowanego zestawu ochronnego, a drugi - zintegrowanie zestawu zabezpieczającego.

W skład zestawu ochronnego wchodzą moduły: ochraniający głowę, odzieży ochronnej oraz zasilający i klimatyzacyjny.

Moduł ochraniający głowę składa się z hełmu z maską przeciwgazową i plastycznym ochraniaczem twarzy przed odłamkami i promieniowaniem laserowym oraz z urządzeń do pobierania płynów, ponadto na hełmie jest montowania kamera niskich poziomów oświetlenia i wskaźnik przeziernikowy.

Nowy mundur zapewnia ciągłe monitorowanie funkcji życiowych każdego żołnierza i błyskawiczną ocenę jego zdolności bojowej. Kombinezon wojownika przyszłości powinien sam dopasowywać się barwami ochronnymi do otoczenia, zapewniając stosowny do środowiska walki kamuflaż. Taki mundur przyszłości pozwoli również przeżyć w terenie skażonym, bowiem chronić będzie przed bronią masowego rażenia stanowiąc rodzaj klimatyzowanego pomieszczenia dla ludzkiego organizmu. Dzięki wbudowanym w kombinezon detektorom będzie automatycznie ostrzegał użytkownika przed minami i pułapkami czyhającymi pod ziemią. A przede wszystkim zagwarantuje przyłączenie każdego żołnierza do globalnej przestrzeni informatycznej. Dzięki temu, na swoim indywidualnym wyświetlaczu będzie on mógł w każdej chwili zapoznać się z wykrytymi, uaktualnianymi na bieżąco danymi o przeciwniku. Żołnierz otrzyma w ten sposób wielowymiarowy obraz budowany przez superkomputery integrujące dane z wielu źródeł rozpoznawczych, w tym także z rozpoznania satelitarnego. Urządzenia do przetwarzania danych i systemy łączności, łącznie z antenami i zasilaniem umieszczone w okolicach torsu żołnierza zapewnią komunikację z bazą i posłużą również jako ochrona istotnych życiowo organów.

W skład modułu zasilającego i klimatyzacyjnego wejdzie lekkie źródło zasilania, które zabezpieczy w energię układ ochładzający i filtrujący, zapewniając odparowanie i ochładzanie powietrza oraz utrzymywanie nadciśnienia pod odzieżą.

Zestaw ochronny ma zabezpieczyć warunki sprawnego działania żołnierza - zwiadowcy w odzieży przez 36-48 godzin.

Zintegrowany zestaw zabezpieczający ma składać się z wyposażenia elektronicznego, środków łączności i uzbrojenia, które stanowić będzie kompozytowa ultralekka, precyzyjna broń o różnych rodzajach amunicji.

Głównym elementem wyposażenia elektronicznego jest komputer osobisty o bardzo małych wymiarach, z nośnikiem danych o dużej pojemności, przeznaczony do:

- gromadzenia i przetwarzania informacji;
- graficznego zobrazowania informacji;
- kierowania łącznością (szyfrowanie i deszyfrowanie przekazywanej informacji);
- określania pozycji w terenie;
- głosowego sterowania elementami wyposażenia osobistego, łączności i uzbrojenia;
- dowodzenia na polu walki.

W pamięci komputera będą przechowywane informacje o przeciwniku i terenie, które zwiadowca wykorzysta w czasie przygotowania się do wykonania zadania. Komputer będzie przedstawiał na wskaźniku przeziernikowym mapę cyfrową terenu z zaznaczonymi pozycjami przeciwnika oraz na bieżąco je uaktualniał w miarę napływu informacji rozpoznawczych z komputerowej sieci łączności. Zwiadowca będzie miał możliwość ustalania kolejności otrzymywanych i przekazywanych informacji (czyli określać, jakie dane komputer powinien podawać w pierwszej kolejności a jakie w kolejnej). Potrzebne informacje będą wyświetlane na małym nahełmowym wielofunkcyjnym wskaźniku przeziernikowym (zamontowanym przed oczami). Urządzenie to o masie około 60 g, zasilane prądem małej mocy, oprócz funkcji przedstawiania informacji komputerowej będzie wykorzystywane do wyświetlania obrazu (np. w nocy z celownika termowizyjnego umieszczonego na broni osobistej). Komputer umożliwi również nakładanie na obraz termowizyjny innych informacji, np. danych o wykrytym celu. Poprzez sieć łączności komputerowej obraz ten może być także transmitowany do innych zwiadowców, np. z drużyny.

Dla osób postronnych nie znających realiów i wymagań przyszłego pola walki taki obraz to fikcja. Tymczasem w świadomości ludzi zainteresowanych perspektywami rozwoju armii już od dłuższego czasu pojawiają się nowe szerokie terminy znaczeniowe jak wojownik przyszłości (*Future Warrior*) czy przyszły system walki wojsk lądowych – FCS (*Future Combat System*). Wymienione tylko dwa charakterystyczne „słowa-klucze" wskazują na zasadnicze kierunki przemian w rozpoznaniu XXI wieku. Futurystyczna jednostka już istnieje (w ograniczonym wymiarze) i prowadzi ćwiczenia zgrywające. Praktyczne wykorzystanie lekkich sił

manewrowych w ramach ćwiczenia *„Arrowhead Lighting II"* z udziałem 3 brygady 2 dywizji amerykańskiej wykazało przydatność bojową tego typu formacji (lekkie wsparte technologią informatyczną). Ćwiczenia przeprowadzono na obiektach poligonu Fort Polk gdzie brygadowy zespół bojowy złożony z 3600 żołnierzy i wyposażony w kołowe transportery *Stryker* prowadził regularne i nieregularne działania bojowe. Ćwiczenie poprzedzone zostało kombinowanym przerzutem pododdziałów samolotami C-17 i C-130, transportem kolejowym oraz morskim. Pozytywne oceny za ćwiczenie uzyskano dzięki skutecznemu systemowi rozpoznania, łączności i dowodzenia oraz wysokiej dynamice działań[39].

3.2.4. PERSPEKTYWICZNE ŚRODKI ROZPOZNANIA ELEKTRONICZNEGO

Rozpoznanie elektroniczne będzie również w przyszłości jednym z podstawowych sposobów zdobywania informacji. Sam proces zbierania informacji będzie miał charakter pasywny (bierne prowadzenie rozpoznania przeciwnika). Jego zasięg rozpoznania powinien przekraczać zasięg efektywnego działania środków rozpoznania radiolokacyjnego (aktywnego rozpoznania przeciwnika).

Perspektywiczne środki rozpoznania elektronicznego powinny być modernizowanie, głównie w zakresie zwiększenia ich zasięgu, precyzji rozpoznania oraz operatywności. W tym czasie mogą pojawić się nowe urządzenia, wykorzystujące znacznie szersze zakresy fal radiowych pasma milimetrowego które dzisiaj nie jest wykorzystywane.

Kluczem do poprawnego działania rozpoznania elektronicznego może być rozwiązanie następujących problemów:

- rozszerzenie przechwytywanego pasma częstotliwości, z możliwością wykrywania emisji na listkach bocznych;
- możliwość odbierania, namierzania, oraz identyfikacji radiolokatorów stosujących przemienność częstotliwości i przeszukiwanie elektroniczne, modulację przestrzenną, kompresję impulsów, technikę dopplerowską, technikę szerokopasmową;

---

[39] Zob. RAPORT-wto nr 7/2003, str.51.

- możliwość działania w zatłoczonym eterze, przy występowaniu zakłóceń wspólnokanałowych i interferencyjnych;
- zwiększenie dokładności namierzania;
- budowy małych, lekkich urządzeń do instalowania na bezzałogowych aparatach latających;
- integracji urządzeń rozpoznania radioelektronicznego z czujnikami różnych typów i możliwością sterowania ich pracą.

W dającej się przewidzieć przyszłości rozwój technologii radarowych będzie miał dla rozpoznania istotne znaczenie (rozpoznanie radiotechniczne – *RADINT*). Radar, stwarza możliwość aktywnego nadzorowania „przeglądania" znacznych obszarów terenu, niezależnie od warunków atmosferycznych, pory doby i roku. Mogą tu znaleźć zastosowanie dwa różne rozwiązania: radiolokatory wykrywania celów nieruchomych i radiolokatory wykrywania celów ruchomych.

Analiza aktualnego stanu oraz tendencji rozwojowych aktywnych radiolokacyjnych środków obserwacji pola walki pozwala sformułować następujące uogólnione wnioski:

- najbardziej rozpowszechnione do wykrywania obiektów pola walki są i będą stacje r/lok pracujące w zakresie 3 cm (8-12 GHz), np. francuski system rozpoznania r/lok „*ORCHIDEE*", lub brytyjski „*ASTOR*";
- najnowszy sprzęt lotniczy jest wyposażony w stacje r/lok pracujące w zakresie 3 i 2 cm (8 - 20 GHz) i tendencja ta może się utrzymać w konstrukcjach perspektywicznych, np. włoski „*CRESO*"; amerykański AN/APG-66 z modyfikacją AN/APQ-164 czy też angielski *FOXHUNTER*;
- stacje r/lok wykorzystywane do rozpoznania i kierowania ogniem wykorzystują zakres fal o długości 1 cm /34 - 36 GHz/ i należy się w przyszłości spodziewać szerszego stosowania sprzętu pracującego w tym zakresie np. AN/TPQ 36 i 37[40];
- moce stacji r/lok powinny być dostosowane do potrzeb w zakresie głębokości rozpoznawania;

---

[40] Stacje te wykorzystywane były przez pododdziały artylerii w czasie „Pustynnej Burzy" określając położenie obiektów z dokładnością do 10 m, oraz przesyłając informację do Brygadowego Ogniwa Wsparcia Ogniowego /FSE/ w czasie kilka sekund.

- optymalizacja ze względu na dokładność określania położenia celu i przekazu informacji w czasie rzeczywistym lub bliskim rzeczywistemu.

Oprócz wymienionych uogólnionych wniosków, należy dodatkowo zaznaczyć, że w literaturze przedmiotu można znaleźć wzmianki rozpoczęcia prac nad radarami pasywnymi, wykrywającymi obiekty (cele) na podstawie ich własnego promieniowania w paśmie mikrofalowym. Typowe okna wykorzystywane w radiolokacji pasywnej to 30 - 35 GHz, 75 - 95 GHz.

W technice wojskowej znalazło zastosowanie całe widmo fal radiowych (łączność, radionawigacja) mikrofale w radiolokacji, kierowaniu pociskami i wielu innych dziedzinach. Sięgają one aż do fal milimetrowych (zwykle 8 mm).

Fale submilimetrowe (milimetrowe) są (umownie) widmem leżącym w zakresie długości 1000 -100 μm. Właściwości fal milimetrowych (10mm do 1mm) zbliżają się do znanych własności klasycznych mikrofal a więc cechuje je dobra propagacja prawie w dowolnych warunkach atmosferycznych i duże anteny.

Fale o długości zbliżonej do 10 mm mają własności zbliżone do znanych z optyki zakresu widzialnego ich propagacja silnie uzależniona jest od warunków atmosferycznych. Anteny (soczewki, reflektory) są niezwykle małe. Aktualnie (z wyjątkiem pasma „8mm", gdzie już istnieją urządzenia radiolokacyjne) inne pasma fal milimetrowych i submilimetrowych mają zastosowanie jeszcze w modelach badawczych.

Do najważniejszych środków rozpoznania pracujących na falach milimetrowych należy zaliczyć radary. Częstotliwości pracy radarów związane są z oknami transmisji w atmosferze i wynoszą: 35, 60, 94, 140 i 220 GHz. Wyjątek stanowi częstotliwość 60 GHz.

Do zalet radarów pracujących na falach milimetrowych można zaliczyć:

- wąską wiązkę i duży zysk kierunkowy uzyskiwany przy pomocy anten o małych apreturach;
- szersze pasmo do obróbki sygnałów, dużą rozróżnialność w zasięgu oraz niskie prawdopodobieństwo wykrycia;
- dużą częstotliwość zjawiska Dopplera;

- tłumienie w atmosferze umożliwiające utajnienie w ograniczonym zasięgu przesyłanych informacji;
- lepszą penetrację przez mgłę, dym, pył w porównaniu z układami na podczerwień i optycznymi.

Ale możemy się spotkać i z wadami oraz ograniczeniami takimi jak:

- tłumienie atmosferyczne ograniczające zasięg;
- absorbcję i odbicia ograniczające zasięg podczas deszczu;
- ograniczoną penetrację podłoża (drzewa, liście itp.);
- duży koszt elementów i podzespołów, małą wydajność i aktywność źródeł.

Przyszłościowe środki rozpoznania radiolokacyjnego najprawdopodobniej będą zmierzać w kierunku zwiększenia zabezpieczenia przed szumami, zmniejszenia ciężaru i gabarytów stacji, zwiększenia ilości wykonywanych funkcji, dokładności a także wiarygodności uzyskiwanych informacji. Uwzględniając wrażliwość stacji radiolokacyjnych i niektórych innych technicznych środków rozpoznawczych, należy opracować nowe urządzenia rozpoznawcze. Powinny to być kompleksowe urządzenia rozpoznawcze, które łączyłyby zastosowanie techniki telewizyjnej, termowizyjnej[41], podczerwieni, radiolokacyjnej i laserowej. Umieszczenie ich na naziemnych i powietrznych nosicielach umożliwi wykrywanie nawet zamaskowanych celów w dowolnej porze doby i skomplikowanych warunkach atmosferycznych.

Urządzenia optoelektroniczne umożliwiają prowadzenie rozpoznania bez względu na porę doby, czy też warunki atmosferyczne. W skład tych urządzeń wchodzą różnego rodzaju czujniki, lasery, termowizory i układy światłowodowe. Należy liczyć się, że w przyszłości rozwój urządzeń zostanie ukierunkowany na ich miniaturyzację. Nowe urządzenia powinny wykorzystywać cały zakres promieniowania podczerwonego, oraz być sprzężone z laserami lub radiolokatorami

---

[41] W skład urządzeń termowizyjnych wchodzą również układy optyczne, skomplikowane i zminiaturyzowane układy elektroniczne obróbki sygnału, a w niektórych przypadkach mechaniczno-optyczne skanery do wybierania obrazu. W ostatnich latach coraz częściej stosowane są układy półprzewodnikowe z tzw. sprzężeniem ładunkowym /CCD/. Na przykład: firma Texas Instrument, produkuje układy detekcyjne dla II okna atmosferycznego zawierające 2048x2048 elementów. Układy te mogą współpracować z różnymi monitorami i urządzeniami do zapisu magnetycznego obrazu. Przewiduje się, że systemy termowizyjne będą wykorzystywane na coraz większą skalę, w tym również do nocnej obserwacji pola walki na dużych odległościach przez wysuniętych obserwatorów lub z wozów bojowych /np. termowizory AN/TAS-6 lub AN/TAS-4.

pracującymi w zakresie fal milimetrowych. Natomiast w celu uodpornienia ich na zakłócenia powinny być zbudowane na bazie techniki światłowodowej.

Na szczególną uwagę w rozwoju środków rozpoznawczych (w zakresie rozpoznania obrazowego realizowanego w polu elektromagnetycznym) zasługują czujniki wykorzystujące długofalową część promieniowania ultrafioletowego, zakres widzialny, podczerwień bliższą, podczerwień termalną w pierwszym (2,76,3 mm) i drugim (8 - 14 mm) oknie atmosferycznym[42] oraz radiolokację w tym aspekcie, który dotyczy możliwości przedstawienia wyników rozpoznania w postaci obrazu.

Istnieje potrzeba wprowadzenia urządzeń, które by miały możliwość prowadzenia rozpoznania w rozważanym fragmencie pola elektromagnetycznego mieszczącego się w zakresie od 0,20 mm w części ultrafioletu do około 14 mm w części termalnej oraz w zakresie radiolokacyjnym od około 1mm do 1m, (ograniczamy się tylko do tych właściwości tego pola, które są przedmiotem rozpoznania).

Mogą to być:

- pasywne urządzenia optoelektroniczne (np. systemu TV) do wielospektralnej rejestracji informacji w zakresie widzialnym i podczerwieni bliższej połączonego z mikroprocesorem zapewniającym możliwość analizy informacji w oparciu o widmowe współczynniki odbicia;
- urządzenia termalne zapisujące informacje w co najmniej dwóch kanałach w połączeniu z kanałem widzialnym.

Oddzielną grupę środków rozpoznawczych, stanowią czujniki wykorzystywane do wykrywania ruchów wojsk lub sprzętu bojowego. Są już opracowane czujniki pracujące w zakresie podczerwieni, a także czujniki magnetyczne oraz czujniki akustyczne i sejsmiczne przy użyciu których istnieje możliwość wykrycia i precyzyjnego odróżnienia pojazdów kołowych od gąsienicowych. Ponadto istnieje możliwość określenie dokładnej liczby wykrytych celów. Czujniki włączają się do pracy automatycznie w momencie pojawienia się obiektu w zasięgu wykrywania,

---

[42] Wykorzystywane promieniowanie (szczególnie II zakresu) jest w małym stopniu pochłaniane i rozpraszane przez dym i pyły. Jest również znacznie słabiej rozpraszane przez mgłę. Dzięki temu wzrasta zasięg rozpoznania w porównaniu z rozpoznaniem w paśmie widzialnym (noc, zła pogoda) i bliska podczerwień.

w tym samym czasie uruchamiany jest nadajnik do transmisji informacji na stanowisko kontroli. Zastosowana w nadajniku modulacja szerokopasmowa lub skokowe zmiany częstotliwości w czasie nadawania praktycznie uniemożliwiają wykrycie nadajnika metodami radio-elektronicznymi.

Większość wymagań stawianych środkom rozpoznawczym mogą spełnić jedynie powietrzne systemy rozpoznania elektronicznego, stanowiące trzon systemu rozpoznania wojskowego zarówno w okresie pokoju, jak i w czasie wojny[43].

Obok załogowych powietrznych środków rozpoznawczych coraz większego znaczenia w rozpoznawaniu nabierać będą bezzałogowe aparaty latające[44].Mogą one w wielu sytuacjach z powodzeniem uzupełnić samoloty rozpoznawcze.

Obecnie, postęp techniczny umożliwia skonstruowanie bardzo małych i lekkich skanerów termicznych, kamer elektro-optycznych, radiolokatorów obserwacji bocznej, lotniczych aparatów fotograficznych, układów sterowania i układów transmisji informacji, które można wykorzystać do opracowania nowej generacji BSR. Aktualnie prowadzone są prace nad następującymi BSR: mikro np. *Black Widow*, *Delta Bee* lub *Bat CIT*, bardzo krótkiego zasięgu /30-50 km/ np. UAV-CR; krótkiego zasięgu /do 150 km/ np. UAV-SR; średniego zasięgu /650 km/ np. UAV-MR; oraz długotrwałego lotu np. *UAV-Endurance*.

Doświadczenia zdobyte podczas konfliktów zbrojnych wykazują, że bardzo wysoką efektywność rozpoznawania obiektów i rejonów uzyskały kompleksowe systemy rozpoznawcze, w których skład wchodziły załogowe i bezzałogowe środki rozpoznawcze.

---

[43] Np. amerykański zautomatyzowany, zintegrowany system dystrybucji informacji taktycznych JTIDS (*Joint Tactical Information Distribution System*).

[44] Konflikt w Zatoce Perskiej potwierdził wartość bezzałogowych aparatów latających. Jednak w czasie konstruowania tych aparatów z przeznaczeniem dla wszystkich możliwości użytkowników nie należy zapominać, że aby być przydatnym do wskazywania celów wszystkie informacje musi zbierać bardzo dokładnie oraz w czasie rzeczywistym lub prawie rzeczywistym przesłać je do organów dowodzenia (środków ogniowych). Jest to pewnik nie podlegający dyskusji że aparat powinien być zoptymalizowany ze względu na dokładność określania położenia celu (obiektu) oraz mieć możliwość bezpośredniego połączenia się z systemem przeciwdziałania ogniowego.

3.3 PROJEKT SIŁ ROZPOZNAWCZYCH

Strategia bezpieczeństwa narodowego RP[45] definiuje następujące zadania dla Wojska Polskiego: (1) odpowiednie przygotowanie swoich sił i środków do przeciwdziałania wszelkiego rodzaju zagrożeniom dla bezpieczeństwa państwa oraz ochrony interesów Polski; (2) udział w realizacji zobowiązań sojuszniczych oraz w zapewnianiu bezpieczeństwa zbiorowego w Europie; (3) współdziałanie w zapewnieniu bezpieczeństwa w sytuacji zagrożenia atakami terrorystycznymi na terytorium Polski oraz udział w działaniach koalicji antyterrorystycznej na obszarze NATO i poza nim. Zgodnie z zapisami dokumentu siły zbrojne RP uczestniczyć mogą także w ramach operacji stabilizacyjnych prowadzonych przez ONZ, OBWE, NATO i UE, a także koalicji ad hoc.

Określa ponadto, iż podstawowym zadaniem polityki i systemu obronnego państwa jest przeciwdziałanie polityczno-militarnym zagrożeniom, w tym przede wszystkim obrona terytorium Polski przed ewentualną agresją zbrojną oraz zapewnienie nienaruszalności granic, ochrona organów państwowych i instytucji publicznych oraz zapewnienie możliwości ich ciągłego funkcjonowania, ochrona ludności oraz zapewnienie jej warunków przetrwania w sytuacji kryzysu lub konfliktu. Na system obronny Polski nałożono także odpowiedzialność za wykrywanie zagrożeń, kierowanie przygotowaniami obronnymi w czasie pokoju, reagowanie na zagrożenia kryzysowe, obronę państwa i udział we wspólnej sojuszniczej obronie zgodnie z art. 5. traktatu waszyngtońskiego z kwietnia 1949 r., który jest aktem konstytucyjnym Sojuszu Północnoatlantyckiego.

Ważnym elementem nowej strategii są także stwierdzenia o stopniowym zastępowaniu sił statycznych (mających na celu obronę terytorialną) przez nowoczesne, mobilne, wysoce wyspecjalizowane jednostki. Z charakteru nowych zagrożeń wynikać będzie także konieczność rozwoju współpracy wojska ze strukturami cywilnymi w zakresie reagowania na zagrożenia pozamilitarne. Dokument zawiera ponadto inne nowe i interesujące dla wojskowych elementy. Stwierdza np. że zdefiniowaniu potrzeb obronnych państwa, a także adaptacji wojska do zmieniających

---

[45] Zatwierdzona przez Radę Ministrów RP 22 lipca 2003 roku a podpisana przez Prezydenta RP 8 września na posiedzeniu Rady Bezpieczeństwa Narodowego

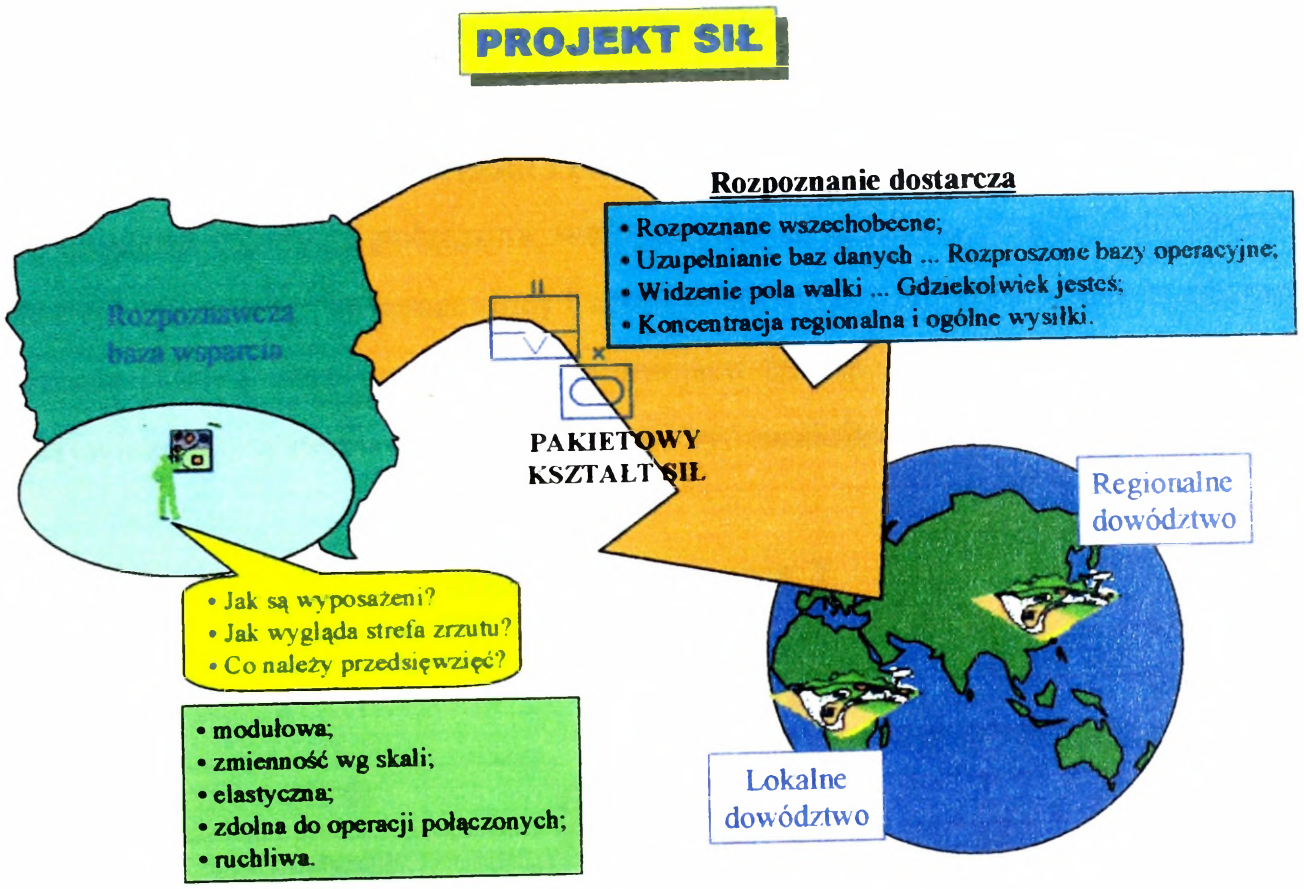
się sytuacji i nowych wyzwań, służyć będą strategiczne przeglądy obronne przeprowadzane w zależności od potrzeb.

Natomiast, zgodnie z „*Programem rozwoju SZ na lata 2005-2010*" ogłoszonym przez MON 1 października 2004 jednostki składać się będą z kompatybilnych ze sobą modułów (segmentów) określonych sił oraz środków. Oddziały zapakowane zostaną jakby do kilku modułów - „worków", z których będzie można, wybierając konieczne segmenty, budować niczym z puzzli jednostki kierowane zarówno do Sił Odpowiedzi NATO, struktur wojskowych Unii Europejskiej czy działań (operacji) stabilizacyjnych. W jednym z tych „worków" mają się znaleźć dowództwa oraz wspierające je pododdziały (oddziały) rozpoznawcze. W kolejnym - nowoczesne, w pełni rozwinięte i profesjonalne jednostki bojowe. W następnym - wszystko, co wiąże się z logistyką. Chodzi o „skonstruowanie" pododdziału, który w swoich strukturach organizacyjnych pomieściłaby niezbędne środki i wyposażenie dla zapewnienia pełnej samodzielności tworzonych grup zadaniowych w ramach oddziału.

Strategia jak i program powinny mieć decydujący wpływ na perspektywiczny system rozpoznania i jednocześnie na możliwości taktyczne zgrupowań, dlatego, że każdy moduł musi posiadać własną bazę rozpoznawczą, która zapewni mu realizację zadania czy też zadań, umożliwi także prowadzenie działań w każdym zakątku świata. Dlatego, szczególną uwagę należy przywiązywać do integrowania możliwości różnych systemów rozpoznawczych w ramach działań połączonych oraz wielonarodowych. Ponadto dowódcy, muszą przygotować i rozwinąć zintegrowany wartościowy informacyjnie system. System ten powinien mieć charakter modułowy, elastyczny w tworzeniu oraz wysoce kompleksowy, o zmiennych właściwościach i strukturach.

W przyszłych działaniach dowódcy powinni dysponować możliwościami budowy systemu, który wspiera (dostarcza informacji) bazy informacyjne podczas kolejnych działań. Bazy muszą być lokalizowane w ośrodkach prowadzących rozpoznanie i zapewniających rozwinięcie sił w czasie wszystkich faz działań. Włączając w to ugrupowanie sił i środków, nadzorowania w okresie wstępnego rozwijania sił, aż do momentu uzyskania przewagi informacyjnej. Bazy informacyjne powinny być: narodowe - połączonych rodzajów wojsk i wielonarodowe

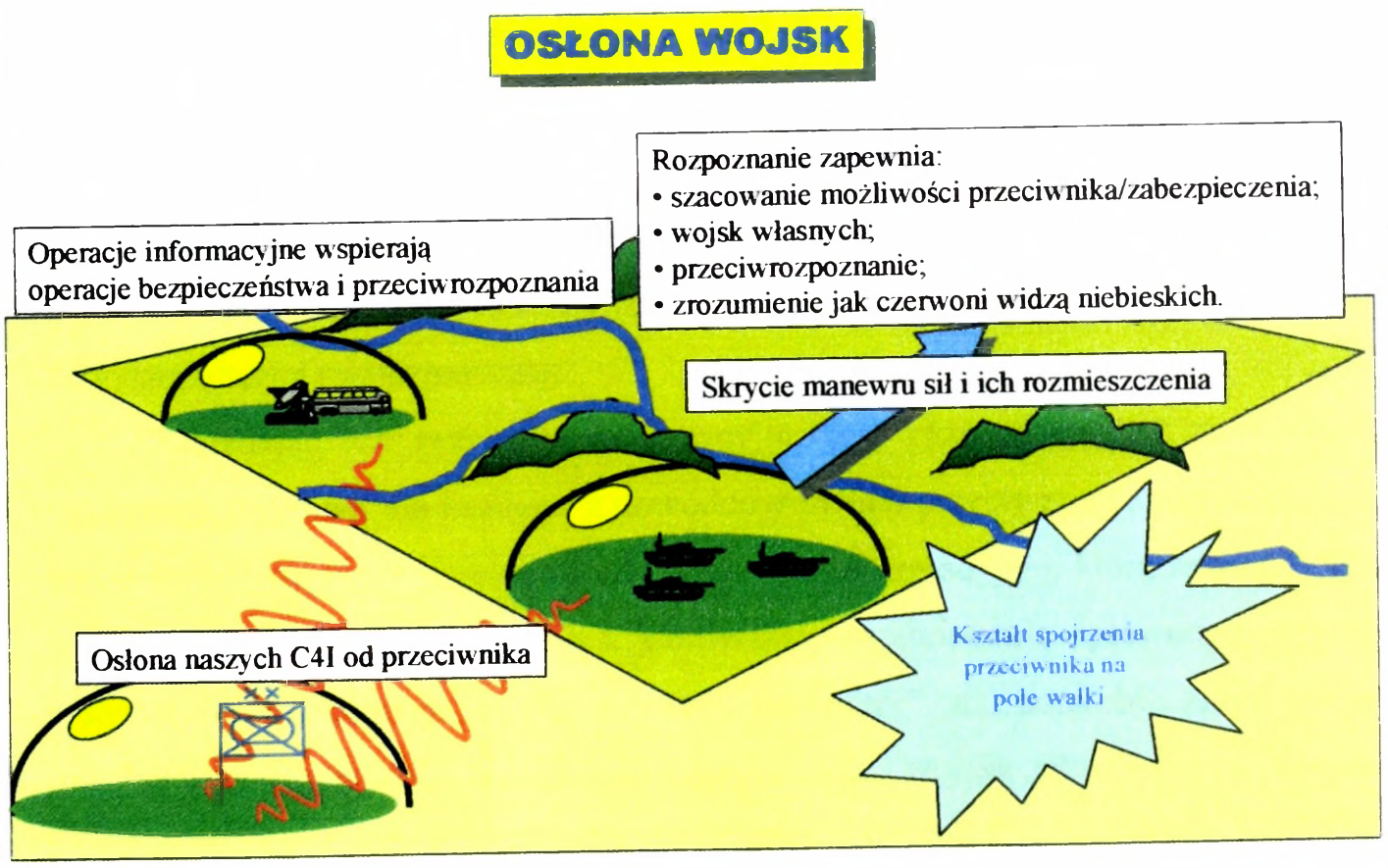
z możliwością rozwinięcia swoich jednostek rozpoznawczych w okresie przygotowania działań, oraz budowania obszaru teatru działań (rys 3.17).



Rys. 3.17. Projekt sił

Dowództwo Operacyjne (Centrum rozpoznawcze) powinno odgrywać główną rolę w osłonie sił. Możliwości takich systemów jak rozpoznanie informatyczne, lądowe, morskie, powietrzne lub specjalne muszą być zwielokrotnione przez dostęp do lokalnych baz danych - umożliwi to wymianę informacji w czasie kierowania działaniami. Ponadto dowództwo musi dostarczać informacji operacyjnym elementom rozpoznania, zlokalizowanym we wszystkich komponentach operacyjnego ugrupowania włączając w to narodowe możliwości baz danych. W przyszłości (należy założyć), że żaden rzut bojowy nie będzie mógł funkcjonować samodzielnie, bowiem sytuacja będzie wymagała aby pozyskiwał dane z systemu, którego on sam będzie składową (ogniwem). Dowództwo operacyjne będzie tym samym jednym wielkim systemem informacyjnym o wielu współpracujących ogniwach.

W zakresie łączności koniecznym jest wprowadzenie na wyposażenie jednostek rozpoznawczych jednoosobowych kanałów łączności satelitarnej i wyprowadzenie końcówek do zdalnego sterowania stacjami łączności. Ten krok może być także przykładem specjalizacji zespołów „wsparcia rozpoznania" jednostek narodowych. Powinny one być wyposażone w możliwość otrzymywania informacji z powietrza, morza i lądu i kosmosu. Od chwili kiedy tylko dowódca otrzyma rozkaz do podjęcia działań, natychmiast przybywa moduł i rozwija system rozpoznawczy w zależności od potrzeb działania (operacja połączona, wielonarodowa, stabilizacyjna itp.) do wsparcia informacyjnego, osłony informacyjnej i obrony informacyjnej oraz walki w obszarze dowodzenia (*C2W*). Raz jeszcze w tym miejscu trzeba podkreślić, że kluczem do perspektywicznego systemu rozpoznania musi być modułowość.



Rys. 3.19. Osłona wojsk

Siły Zbrojne przyszłości będą narażone we wszystkich fazach działań i w każdym rzucie bojowym na oddziaływanie konwencjonalnej broni dalekiego zasięgu, terrorystów, wirusów komputerowych i połączenia różnych niszczących

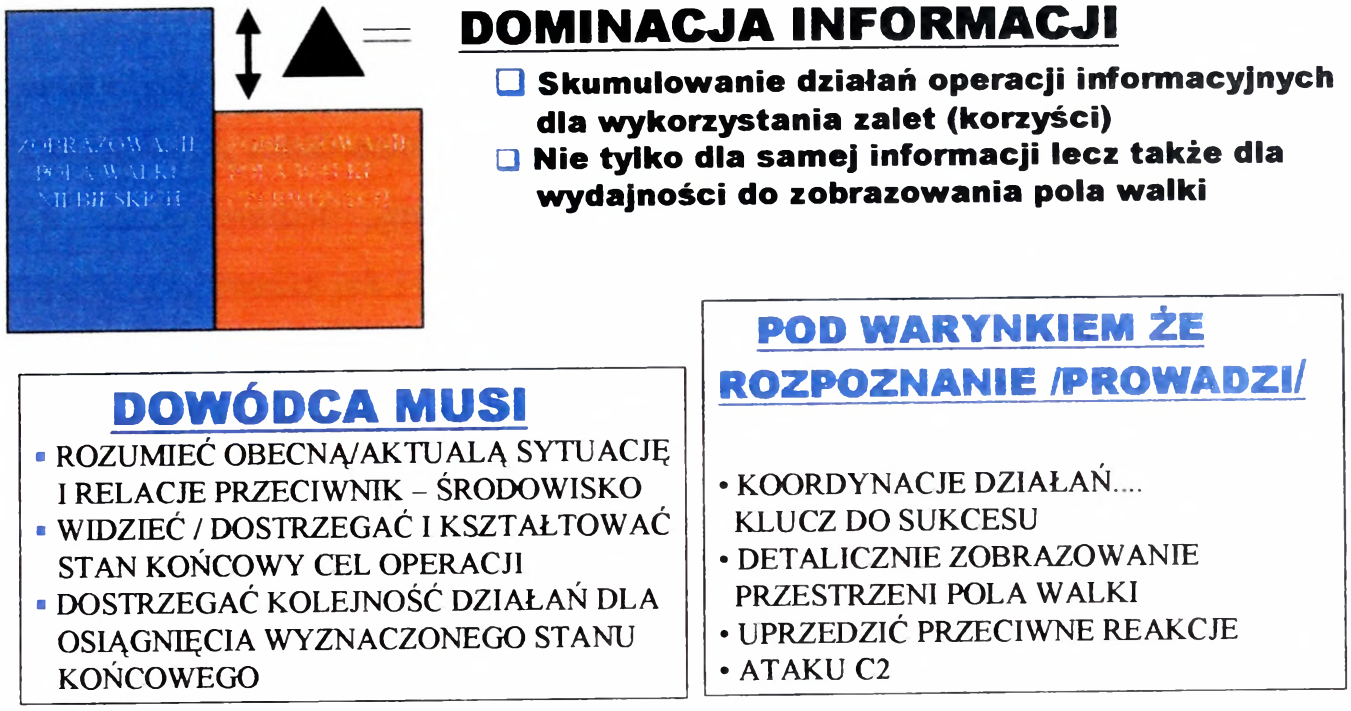
i nieniszczących broni (rys. 3.19). Zagrożenie będzie wielowymiarowe o potencjalnych możliwościach bardzo precyzyjnych uderzeń i dużej sile rażenia. Dlatego osłona sił musi zapewnić przeciwdziałanie atakom na *C4I* jak również środki przeciw *C2W*, a także osłonę od typowych uderzeń konwencjonalnych. Z tego wynika, że dowódcy przyszłych działań muszą znać zagrożenie w pełnym zakresie, wskazywać priorytety w osłonie oraz posiadać klucz dostępu do źródłowych informacji z danego obszaru[46]. W osłonie wojsk wymagane jest także aby system rozpoznania rozróżniał w dynamicznym układzie sił strony konfliktu "czerwoną" i „niebieską", wszystko po to aby można było efektywnie prowadzić symulacje komputerowe. Wykorzystując rezerwy technologiczne jakie tkwią w IPPW dowódca może analizować nowe czynniki determinujące aktywne i pasywne warianty działania przeciwnika oraz w stosunku do nich podejmować działania zapobiegawcze. Działalność rozpoznawczych sił zabezpieczenia działań, powinna się koncentrować na przeciwdziałaniu zasadzkom, zaskoczeniu, prowadzeniu działań przeciwrozpoznawczych i *C2W* dla zapewnienia przewagi informacyjnej. Ponieważ osiągnięcie przewagi informacyjnej w odpowiednim miejscu i czasie (rys. 3.20) pozwoli wspierać przeciwrozpoznawcze działania czyniąc je integralną częścią każdej fazy działalności rozpoznawczej.

Zakładając, że przewaga informacyjna jest różnicą między zrozumieniem informacji dostępnej dla każdego z dowódców dwóch przeciwnych stron konfliktu, to jej cel będzie osiągany przez prowadzenie walki informacyjnej, która zawiera: osłonę własnych systemów dowodzenia i kierowania, ustanowienia sprawnego, pewnego systemu informacyjnego (*C4I*) a także „Infosfery" na potrzeby przedstawienia informacji z zakresu obszaru działań (rozpoznanie, wojska własne i inne stosowne informacje), by poprawić wizualizację przestrzeni walki i zaspokajać zasadnicze potrzeby informacyjne dowódcy (*CCIR*)[47]. Dlatego, aby osiągnąć dominację informacyjną, dowódca musi ochronić własne systemy informacyjne, niszcząc albo obezwładniając systemy przeciwnika (*C4I/RSTA*), używając połączenia ognia

---

[46] Zob. Strefowe bazy danych (SBD) – pojęcie to oraz jego szczegółowa interpretacja, w odniesieniu do systemu rozpoznawczego, w polskiej myśli wojskowej po raz pierwszy zostało sformułowane w 1994 roku w cytowanej już publikacji ... R. Kwećka, A. Nowak, *Budowa modelu...*, wyd. cyt, AON, Warszawa 1994, rozdział czwarty.
[47] **CCIR** - *Commander's Critical Information Requirements.*

i maskowania, zakłócania jego systemów rozpoznania oraz kierowania w ramach tzw. nie „śmiertelnego" ataku. Dominacja informacyjna może być także kształtowana jednostkowo lub kompleksowo dla określonego miejsca i wybranego czasu.



Rys. 3.20. Dominacja informacji

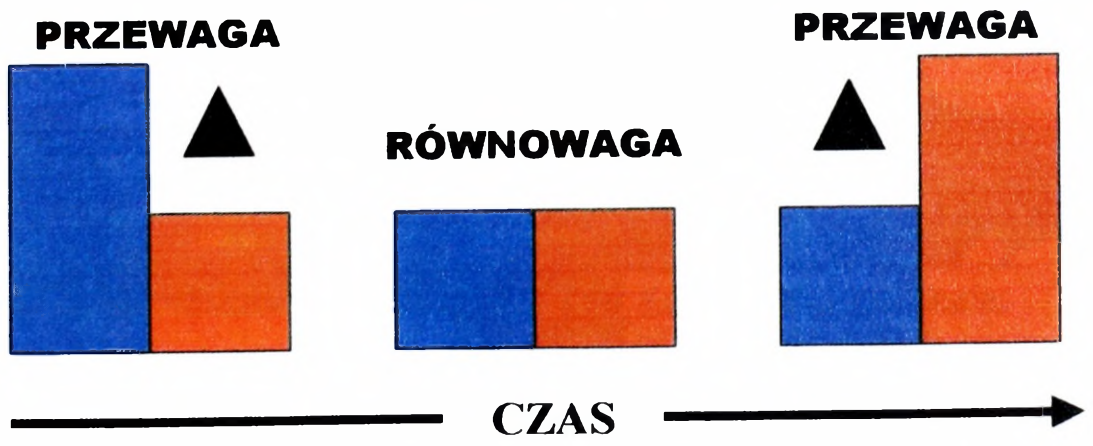
Jednocześnie zespół autorski zakłada, że „System rozpoznania XXI wieku" odegra zasadniczą rolę w osiąganiu dominacji informacyjnej. Siły rozpoznawcze będą zbierać, analizować posiadaną informację o przeciwniku, pogodzie, terenie, itd. w ten sposób dostarczając dowódcy możliwości, aby zwizualizować zdobyte informacje dotyczące obszaru działań. We wsparciu informacyjnym w procesie realizacji celu działania, analitycy oszacują obiekty do rażenia i obezwładnienia oraz określą *C4I/RSTA* a ponadto, możliwości wykonania uderzenia i podatność na działania środków WE. Planiści działań rozpoznawczych będą kontynuowali planowanie, koordynację i synchronizację w celu zintegrowanego użycia elektronicznych możliwości. W ten sposób „System rozpoznania XXI wieku" pozwoli dowódcy

skuteczniej skupić możliwości zarówno rażenia jak i obezwładnienia środkami elektronicznymi, by osiągnąć decydujący efekt.

Aby kształtować pole walki, dowódca musi mieć wirtualny, zbliżony do czasu realnego - ciągły obraz sytuacji w stosunku do zakładanego stanu końca działań. Musi też być w stanie, dokładnie umiejscowić się w systemie walki (działań), określić sposób działania i wtedy wiązać z walką obiekty przeciwnika w czasie działań w głębi z rozmaitym sposobem oddziaływania bezpośredniego, rażenia (fizycznego) lub elektronicznego, zakłócania ewentualnie maskowania własnej sytuacji. On i jego sztab muszą przeprowadzić „grę wojenną" w różnych opcjach i zrozumieć zarówno działania przeciwnika jak i określić zdolności wojsk własnych (zamiary) i przewidzieć wpływ czynników środowiska z zakresu pogody i terenu. Oni muszą też skoordynować wykorzystanie zdolności połączonych sił wielonarodowych (rys. 3.21).

POZIOM OPERACYJNY — **Nie jest możliwa bez ustanowienia przewagi informacyjnej jako warunku dla operacji militarnych /podobnie jak zamiar wywalczenia przewagi w powietrzu/**

POZIOM TAKTYCZNY —
- **Przewaga informacyjna jest normalnym/zasadniczym tymczasowym warunkiem (zbiór warunków/możliwości)**
- **Proces zbierania / gromadzenia informacji dla przewagi informacyjnej musi przenikać działania taktyczne (kształt sił, kształt pola walki i zdecydowane wsparcie)**



Rys. 3.21. Przewaga informacyjna

Kształtując pole walki, wojska muszą zostać wsparte przez siły rozpoznawcze, które mogą korzystać z zasobów informacyjnych środków rozpoznania przeznaczonych do działania w głębi obszaru działania (np.: *JSTARS, U2*), zdolnych dokładnie wyśledzić i zlokalizować HPT (np.: środki bezpilotowe, naziemnych systemów czujnikowych itp.), prowadzić WE oraz wesprzeć działania głębokie mając na celu pozyskiwanie ciągłych i dokładnych danych. Ponadto w systemie tym, muszą pracować dobrze wyszkoleni analitycy rozpoznania i operatorzy wysoce mobilnych systemów pozyskiwania danych, aby skutecznie wspierali stosowne decyzje i chronili kanały łączności. To musi zostać zorganizowane w taki sposób, by łączyć różne informacje dotyczące rozpoznania, określania i wskazywania celów oraz nadzorowania obszaru działań pochodzące od rozmaitych organicznych (własnych) oraz połączonych i wielonarodowych systemów rozpoznania.

W końcu, system ten musi uzyskać zdolność, by przewidzieć działania przeciwnika, oszacować teren i określić poprawnie pogodowe warunki dla uderzenia w czasie działania wojsk własnych, pozwalając dowódcom i sztabom gruntownie analizować kolejne działania w ramach gier wojennych (rys.3.22).



Rys. 3.22. Kształt obszaru działań (pola walki)

Zakładając, że działania (operacje) rozstrzygające będą wymagały dokładnego obrazu przestrzeni obszaru działań. To z kolei wymaga skoordynowanego projektu by działania były jednoczesne, w aspekcie uderzenia. Ponadto, jest wymagana dokładna ocena skutków uderzeń, by zapewnić pomyślne zakończenie każdej fazy przed przechodzeniem do następnej a to z kolei wymaga dokładnej identyfikacji miejsca i pozycji walczących wojsk.

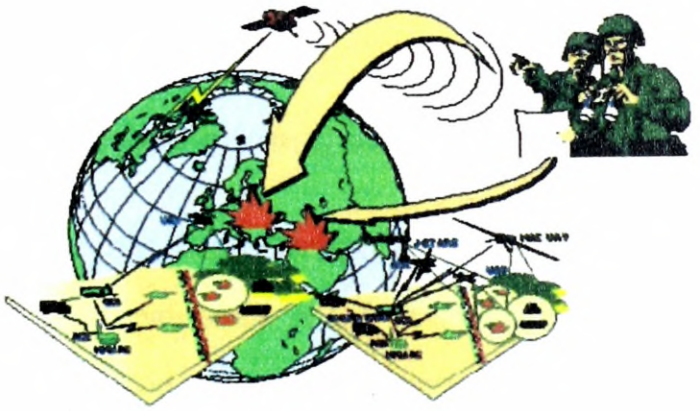
Gęstość różnych obiektów/celów i poziom zaangażowania wojsk wzrośnie, gdy jednostki będą w kontakcie bojowym a czas reakcji zostanie bardzo skrócony. Z tego wynika, że struktura systemu rozpoznania wspierającego działania (operacje) decydujące musi być wyjątkowo elastyczna i zdolna dostarczać stosownych rezultatów rozpoznania na potrzeby własnego dowódcy. System musi być zdolny nie tylko do zbierania, ale i przetwarzania informacji oraz posiadać zdolność przekazu - komunikowania się z ośrodkami centralnymi. System musi też dostarczać, dowódcy informacji w ramach działań (operacji) rozstrzygających umożliwiających wsparcie ataku elektronicznego w postaci modułowej na poszczególne obiekty przeciwnika (rys.3.23).



Rys. 3.23. Działania (operacje) rozstrzygające

Warianty działania i plany alternatywne pomogą dowódcy utrzymać tempo działania, kiedy działania przechodzą od jednej fazy do następnej. Natomiast zintegrowany wysiłek rodzajów wojsk będzie osiągnięty - tylko i wyłącznie - przez utrzymanie i ochronę systemu logistycznego.

Działania rozpoznawcze będą ciągłe, zaprojektowane tak, by uniknąć zaskoczenia i ochronić jednostki - elementy rozpoznawcze. Powinny składać się z systemów, które mogą zostać utrzymane w gotowości i sprawnie dostarczone oraz rozmieszczane w krótkim czasie w rejonie działania. To założenie będzie wymagało nowatorskiego podejścia do systemu rozpoznania dla jednostek wsparcia bojowego i logistycznego. Działania rozpoznawcze wymagają ponadto przygotowania dowódców do przyszłych działań (rys 3.24).



DOWÓDCA MUSI:
- utrzymywać tempo operacji;
- osłaniać dopływ zasobów (odwody, logistyka).

POD WARUNKIEM ŻE ROZPOZNANIE:
- wspiera operacje bieżące;
- nadzoruje obszar regionalny i globalny;
- podkreśla zrozumienie rozpoznania;
- posiada siły zdolne do przetrwania.

Rys. 3.24. Dowódca a rozpoznanie

Dostrzegając uwarunkowania technologiczne prowadzenia walki należy wskazać, że kwestia transformacji systemu do nowego wymiaru musi być rozpatrywana w kontekście zmiany koncepcji prowadzenia działań (*Revolution in*

Military Affairs). W zgodnej opinii wielu specjalistów największym beneficjantem nadchodzących zmian będzie system przekazywania i opracowywania informacji, w tym rozbudowany system dowodzenia (*C4I*). W śmiałych koncepcjach przyszłych działań zakłada się, że system dowodzenia i rozpoznania wojsk nie będzie tylko rodzajem banku danych, ale będzie miał możliwość tworzenia wiedzy[48], czyli będzie w stanie przekazać opracowany produkt na potrzeby użytkowników przyszłych działań militarnych.

Drogą ku temu ma być powstanie tzw. sił (wojsk) sieciocentrycznych, opierających możliwości operacyjne i przewagę nad przeciwnikiem na informacji. Wojska nowego typu będą miały nieporównywalnie większą świadomość operacyjną (wiedzę o obszarze działania oraz położeniu i działaniu sił własnych i przeciwnika), bowiem jednostki bojowe będą w stanie płynnie wymieniać posiadane zasoby informacyjne[49]. Zatem w konsekwencji będą mieć zdolność do samoregulacji systemu bojowego - automatycznej synchronizacji uderzeń i manewru.

3.3.1 KIERUNKI ROZWOJU SYSTEMU ROZPOZNANIA

Na początku XXI wieku, po ustąpieniu bezpośredniego zagrożenia ze strony państw sąsiednich, określamy się sami jako państwo, przed którym jest coraz mniej wyzwań i zagrożeń. Narastające konflikty, nawet te odległe, miały jednak bezpośredni wpływ na sytuację nie tylko w Polsce, ale również na całym obszarze europejskim.

Rozwijające się nowe formy konfliktów, takie jak: spory wewnętrzne, wojny domowe oraz międzynarodowy terroryzm nie mogą pozostać nie zauważone, a siły i środki wydzielone w ramach Paktu Północnoatlantyckiego i UE do działań, muszą być w stałej gotowości.

Wzrastająca skala rozprzestrzeniania się środków masowego rażenia, wzrastający ciągle zakres ich możliwości oraz fakt, że mogą być one w posiadaniu czynników innych niż państwowe, stwarza możliwość wywołania konfliktów na niewyobrażalną dotąd skalę. Do tego dochodzą jeszcze nowe teatry działań wojennych,

---

[48] Rozpoznanie to wiedza, produkt końcowy opracowywania szeregu danych rozpoznawczych do postaci wiadomości użytecznych dla uczestników walki.
[49] Obecnie nie jest to możliwe, bowiem każda armia a czasami nawet rodzaj sił zbrojnych stosuje inny format zapisu danych.

które mogą wpływać na życie naszego społeczeństwa oraz nasz rozwinięty, skomputeryzowany i wysoce utechniczniony świat. Pojęcie „wojny informacyjnej" przestało już być pojęciem utopijnym.

Przedstawione fakty skłaniają do wniosków, że wyobrażenie „klasycznego sporu" pomiędzy dwoma suwerennymi państwami zastępowane jest przez różnorakie formy konfliktu, charakteryzujące się „asymetrycznością" jego prowadzenia. Tożsamość działających w koalicjach lub pojedynczo, państwowych lub niepaństwowych, wojskowych lub cywilnych „aktorów" wojny, staje się przy tym coraz mniej przejrzysta.

Wnioskując z analizy literatury stwierdzam, że pojęcia „zagrożenie" i „bezpieczeństwo" ulegają ciągłym zmianom, a ich znaczenie jest ciągle uaktualniane (dopasowywane do rzeczywistości). Dlatego też nowoczesny system rozpoznania, chcący sprostać ciągle zmieniającym się wymaganiom i warunkom, musi zachować ciągłą zdolność do działania oraz elastyczność swoich struktur.

Bierzemy czynny udział w międzynarodowych przedsięwzięciach, mających na celu utrzymanie pokoju na świecie. Użycie naszych jednostek w operacjach ratunkowych, pomocy, ewakuacyjnych oraz operacjach zapobiegania konfliktom i ich likwidacji (wygaszania) - to realizm dzisiejszych i przyszłych dni. Do tego potrzebne są siły rozpoznawcze, które są w stanie sprostać szerokiemu spektrum zadań rozpoznawczych, realizowanych w poszczególnych operacjach.

Zakładając, że głównym zadaniem (rolą) systemu rozpoznania, obok jak najwcześniejszego wykrycia rejonów nowych ognisk zapalnych i ich monitorowania, musi być możliwie najszersze wsparcie informacyjne jednostek, przewidzianych do działania w tych rejonach lub już w nich działających.

To system musi pełnić - między innymi – następujące funkcje: informacyjną, ostrzegającą i ochronną. Jednocześnie musi być również zdolny do realizacji innych zadań takich jak:

1. informowanie kierownictwa politycznego (rządowego) i wojskowego o sytuacji na świecie oraz wyprzedzające wskazywanie ewentualnych zagrożeń;
2. zidentyfikowanie dla jednostek przygotowujących się do działania lub już działających jako kontyngenty:
   - wszelkich dostępnych informacji o rejonie działania;

- możliwych wariantów działania stron konfliktu i wynikającego stąd ryzyka (zagrożeń) dla jednostek;
- zaleceń w zakresie ochrony ludzi i sprzętu;

3. Ocena sytuacji bezpieczeństwa jednostek na terenie kraju i w rejonach i użycia.

W celu realizacji tego „profilu zdolności", w ramach „ Planu modernizacji SZ na lata 2005-2010", zostały zapoczątkowane nowe uwarunkowania systemu rozpoznania.

Najistotniejszymi obszarami zainteresowania tego procesu są:

- *stan osobowy* - odbudowa jakościowa i ilościowa stanu osobowego, uwzględniająca nowe „ spektrum zadaniowe";
- *struktury* - budowa „przyszłościowych" struktur organizacyjnych, zdolnych do samodzielnego funkcjonowania i w układzie koalicyjnym;
- *technika* - techniczna rozbudowa możliwości rozpoznawczych, szczególnie w ZO (ZT) powstałych na bazie różnych Rodzajów Sił Zbrojnych.

W wyniku analizy powyższych faktów zespól autorski uważa, że baza wojskowego „profilu zdolności" jest bardziej rozległa. Coraz większego znaczenia nabierają zdolności: przewidywania, dokonywania właściwej oceny a przede wszystkim zapewnienia dopływu dokładnych i aktualnych informacji. „Świat" nie zapewni nam bezpieczeństwa dziś, ani w najbliższej przyszłości, i dlatego od perspektywicznego systemu rozpoznania musimy wymagać:

1. skrupulatnej i sumiennej „pracy u podstaw", zapewniającej stworzenie stabilnej bazy informacyjnej.
2. elastycznego doboru środków, metod i sposobów zdobywania informacji, zapewniających „dotrzymanie kroku" szybko rozwijającym się sytuacjom kryzysowym.

Wymogi personalne, strukturalne i materiałowe zostały już określone, a ich wprowadzenie w czyn - rozpoczęte. Jednakże, rozpoczęta obecnie realizacja nowych uwarunkowań systemu rozpoznania może okazać się tylko „krokiem pośrednim" toczącego się właśnie procesu zmian.

Z przeprowadzonych obserwacji w czasie ćwiczeń, treningów wynika, że w naturze systemu rozpoznania leży jednak to, że musi on ciągle odnawiać i dopasowywać swój „profil zdolności". Nie dzieje się to jednak bez powodu. W dobie szybkich zmian i coraz

doskonalszej techniki, system rozpoznania musi sprostać coraz to innym wyzwaniom (w innych obszarach problemowych).

„Klucze" do rozwiązania tych problemów leżą w ilości środków finansowych, inwencji twórczej, zdolności innowacji i stopniu fachowości stanu osobowego systemu rozpoznania. Nakłady finansowe, zainwestowane w system rozpoznania, będą wydatkami „opłacalnymi". Pozwolą na jego prawidłowe funkcjonowanie, a zdobyte aktualne i dokładne informacje pozwalają na podjęcie trafnych, „najekonomiczniejszych" decyzji. Tym samym, zmniejszą się zagrożenia dla stanów osobowych kontyngentów wojskowych i zostaną stworzone optymalne warunki do realizacji stojących przed nimi zadań.

Analiza założeń teoretycznych, wnioski z praktyki szkoleniowej oraz doświadczenia z wojen i konfliktów lokalnych, pozwalają na ogólne stwierdzenia dotyczące efektywnego zbudowania systemu rozpoznania (SR), jako najbardziej technologicznie zaawansowanej formy wspomagania procesu dowodzenia z wykorzystaniem najnowszej technologii który wymaga spełnienia określonych uwarunkowań.

Zestaw najważniejszy można ująć następująco:

- realizacja SR, rozumiana jako całokształt działań przygotowawczych, organizacyjnych i wykonawczych, a obejmujący pełen cykl życia systemu informacyjnego, musi być rozpatrywana w kategorii złożonego przedsięwzięcia informacyjnego, traktowanego jako inwestycja strategiczna;
- cel wdrożenia systemu i jego zakres funkcjonalny muszą jednoznacznie wynikać ze strategii SZ, jako dokumentu pochodnego względem misji i strategii jego funkcjonowania;
- wdrożenie SR wymaga pełnego zaangażowania najwyższego kierownictwa SZ i zagwarantowania odpowiednich zasobów ludzkich, finansowych i materiałowych wykorzystywanych zgodnie z najnowszymi zdobyczami wiedzy i doświadczeń w tym zakresie.

Ponadto należy zaznaczyć, że złożoność realizacji SR wynikać będzie z kilku podstawowych czynników:

- organizacyjnego - uwzględnia zmiany w otoczeniu SZ i w nich samych, pracę zespołową, komunikację między zespołami wykonawczymi a przyszłymi użytkownikami SR, koordynację różnych działań itp.;
- technicznego - zapewnia zachowanie koniecznego współdziałania między elementami struktury realizacyjnej SR przy uwzględnianiu dynamiki zmian w infrastrukturze informatycznej, będących pochodną rozwoju środków technicznych;
- technologicznego - uwzględnia zależności określonych etapów i faz prowadzonych działań, socjo-psychologicznego - obejmuje postawy i zachowania ludzi (przyszłych użytkowników wdrażanego systemu i jego realizatorów) w grupie i ich interakcje.

Natomiast do kluczowych uwarunkowań organizacyjnych w realizacji SR można zaliczyć:

- prawidłowe przygotowanie i przeprowadzenie prac w zakresie zdefiniowania zadania projektowego, inicjującego właściwe działania projektowo-wdrożeniowe;
- dokonanie wyboru systemu spośród oferowanych gotowych standardów światowych (jako platformy);
- formalne powołanie zespołu projektowo-wdrożeniowego o strukturze i składzie osobowym, uwzględniającym specyfikę organizacyjno-techniczną SZ i wdrażany system, który przygotuje szczegółową koncepcję rozwiązania łącznie z analizą jego ryzyka, harmonogramem i budżetem;
- konsekwentne realizowanie przyjętych ustaleń wykonawczych zgodnie z przyjętą metodyką prac przy zachowaniu wymogów jakościowych całego przedsięwzięcia.

Na zakończenie, można się pokusić o kilka praktycznych rad dla przyszłych twórców SR, które mogą być następujące:

- całość prac projektowo-wdrożeniowych powinna przebiegać zgodnie z przyjętą metodyką postępowania;
- tworzenie SR musi poprzedzić identyfikacja i modelowanie jego głównych i pomocniczych procesów informacyjnych wraz

z dostosowaniem całej infrastruktury do wymagań proponowanych rozwiązań. Działania te, powinny być wspomagane pełnym cyklem metodycznym, czyli zastosowaniem odpowiednich metod i narzędzi informatycznych;

- na etapie wyboru systemu spośród gotowych standardów światowych konieczne jest takie określenie zadania projektowego, aby realizowany SR spełniał oczekiwania jego użytkowników końcowych, a nie zaspakajał wizje inżynierskie jego realizatorów, przyszli jego użytkownicy muszą rozumieć zapowiadane korzyści i wyraźnie się z nimi identyfikować;
- powodzenie realizacji SR zależy będzie od struktury, składu osobowego i organizacji prac zespołu projektowo-wdrożeniowego, którego powołanie i określenie kompetencji oraz odpowiedzialności powinno być usankcjonowane formalnym dokumentem kierownictwa SZ, w pracach takiego zespołu konieczny jest udział kluczowych użytkowników systemu, a jednym z jego kierowników powinna być osoba ze ścisłego kierownictwa SZ, zespół taki musi mieć charakter interdyscyplinarny o odpowiedniej hierarchicznej strukturze z komitetem sterującym na czele, należy sprawnie i kompleksowo przeprowadzić szkolenia kierownictwa i wszystkich przyszłych użytkowników oraz traktować je jako element pełnego cyklu życia rozwiązania informatycznego;
- rezultaty końcowe realizacji SR powinno uzyskiwać się na zasadzie efektu synergii, co oznacza, że zadowolenie użytkowników systemu nie będzie tylko prostą sumą użyteczności zastosowanych komponentów, stąd tak dużą uwagę należy przykładać do zakresu i jakości działań integratora prac projektowo-wdrożeniowych, który powinien obejmować całość wiedzy teoretycznej i doświadczeń praktycznych z zakresu SR oraz dynamicznie dokonującego się rozwoju narzędzi i technologii informatycznej;
- z uwagi na duży ciężar finansowy całego przedsięwzięcia należy pamiętać, że istnieje ścisły związek między kondycją finansową SZ a powodzeniem w realizacji SR.

ZAKOŃCZENIE

Przedstawione w pracy wyniki badań pozwalają na przyjęcie tezy, iż prowadzenie działań rozpoznawczych to istota działalności rozpoznawczej polegająca na podejmowaniu określonych czynności w celu uzyskania, w drodze bezpośredniej obserwacji lub wykorzystania innych metod wykrywania, danych (informacji) o działaniach i środkach przeciwnika lub potencjalnego przeciwnika, oraz danych meteorologicznych, hydrograficznych lub geograficznych określonego obszaru. Są to najważniejsze ale nie jedyne czynności prowadzenia działań rozpoznawczych, które wraz z ich przygotowaniem tworzą zamknięty, nawzajem się przenikający cykl rozpoznawczy.

Nie tylko obecnie, ale w każdym okresie rozwoju sztuki wojennej działaniom rozpoznawczym (rozpoznawaniu) przyznawano odpowiednio wysoką rangę. Istnieje więc pewna nieścisłość w utartym twierdzeniu, że w warunkach współczesnych wzrosła ich rola. Wzrost ten jest procesem ciągłym, wynikającym z rozwoju środków walki, których jakość powoduje, że przed działaniami rozpoznawczymi stawia się coraz wyższe wymagania. Pogłębiają one, podobnie jak walka, swój zasięg, rozszerzają obszar zainteresowania i obligowane są do dostarczania informacji o przeciwniku i terenie coraz szybciej, aby stworzyć dowódcom i sztabom możliwości podejmowania decyzji w zmieniających się nieustannie sytuacjach. Jeżeli współczesne operacje nabierają większego rozmachu w wielu środowiskach, to także z większym rozmachem muszą być prowadzone działania rozpoznawcze.

Efektywność systemu rozpoznania zależna jest nie tylko od ilości użytkowników, lecz także od nowoczesnych technicznych środków rozpoznania, łączności oraz przetwarzania danych, opartych na osiągnięciach współczesnej techniki, telekomunikacji i informatyki. W pododdziałach rozpoznawczych ze względu na czas przekazu danych celowe jest wprowadzenie urządzeń telefonicznych z wybieraniem bezpośrednim pozwalającym na realizację połączeń priorytetowych. Podniesienie efektywności funkcjonowania sieci informacyjnej może nastąpić także poprzez wprowadzenie nowoczesnego,

odpornego na zakłócenia sprzętu łączności, nawigacji, wskazywania celów i naprowadzania środków rażenia do podstawowych elementów rozpoznawczych podsystemu rozpoznania ogólnowojskowego

Pododdziały rozpoznawcze na poziomie taktycznym powinny być szkolone i wyposażone do działania w ugrupowaniu przeciwnika na zasadach grup dalekiego rozpoznania, jakie funkcjonują w strukturach jednostek NATO. Dlatego dążyć należy jednocześnie do przywrócenia rozpoznania specjalnego, dostrzegając w tym rozwiązaniu wiele istotnych zalet wpływających na poprawę funkcjonowania systemu rozpoznania.

Konieczne jest posiadanie sił i środków rozpoznawczych w strukturach batalionów zmechanizowanych i czołgów. Pozwoli to na zwiększenie możliwości rozpoznania i zapewni stały napływ aktualnych informacji o przeciwniku i środowisku pola walki.

Poprawę możliwości funkcjonowania systemu rozpoznania w aspekcie rażenia ogniowego (ogniem artylerii i śmigłowców) należy upatrywać w rozwoju infrastruktury technicznej poszczególnych źródeł rozpoznania i sztabowych zespołów przetwarzających informacje. Nadrzędną zasadą powinno być przekazywanie informacji do zainteresowanych dysponentów środków rażenia w autonomicznej sieci informacyjnej. Urzeczywistnienie tej tezy wymaga wyposażenia pododdziałów rozpoznawczych w środki precyzyjnej lokalizacji celów i natychmiastowej transmisji pozyskiwanych danych.

Skuteczność funkcjonowania systemu rozpoznania można poprawić poprzez zwiększenie samodzielności dowódców pododdziałów rozpoznawczych. Drogą ku temu jest unikanie nadmiernej szczegółowości stawianych zadań do określenia rejonu działania pododdziałów rozpoznawczych oraz rodzaju i czasu pozyskania określonych wiadomości o przeciwniku i terenie.

W zakresie rozpoznania radioelektronicznego należy wskazać, że na możliwości namierzania zasadniczy wpływ mają: techniczne parametry stosowanych urządzeń rozpoznawczych oraz wyszkolenie obsług. Istotnym czynnikiem decydującym o możliwościach bojowych kompanii radioelektronicznej, w tym głównie w zakresie rozpoznania i obezwładniania

radioelektronicznego, jest sytuacja elektroniczna po stronie przeciwnika, a szczególnie intensywność pracy jego środków radiowych, ich podatność na rozpoznanie i zakłócanie oraz związane z tym sposoby i zakres prowadzenia obrony informacyjnej. Tymczasem kompania radioelektroniczna ZT nie posiada środków do rozpoznawania i obezwładniania relacji radiowych z rozproszonym widmem (emisji typu frequency hopping – FH). Stąd istotnego znaczenia w prowadzeniu walki elektronicznej przez ZT nabiera problem stosowania innych środków, jak np. uderzenia nadajnikami zakłóceń jednorazowego użytku. Brak nowoczesnych środków łączności radiowej zapewniających pracę sieci rozpoznania, namierzania i zakłócania powoduje, że wydłużeniu ulega czas przekazu i przetwarzania danych pozyskiwanych w podsystemie rozpoznania radioelektronicznego

Przeprowadzona analiza stanu jakościowego i ilościowego sił i środków rozpoznania artyleryjskiego na szczeblu oddziału, wskazuje na dużą dysproporcję w zakresie możliwości pozyskiwania danych na potrzeby prowadzenia w stosunku do możliwości oddziaływania ogniowego środków rażenia. Przy obecnym technicznym wyposażeniu nie mają one żadnych organicznych możliwości rozpoznania obiektów położonych w głębi operacyjno-taktycznej. Ponadto możliwości rozpoznania powietrznego i elektronicznego nie spełniają zakładanych przez artylerię wymagań w zakresie określenia położenia celów z wymaganą dokładnością i w związku z powyższym pozyskiwane dane nie mogą zostać wykorzystane do rażenia ogniowego. Doświadczenia wojen i konfliktów lokalnych pozwalają na postawienie tezy, że siły i środki rozpoznania artyleryjskiego powinny umożliwiać penetrację ugrupowania przeciwnika na głębokość dwu- a nawet trzykrotnie większą od zasięgu środków rażenia danego szczebla dowodzenia. Uzyskany w ten sposób czas operacyjny zostanie wykorzystany na zaplanowanie kolejnych uderzeń ogniowych. Pożądanym kierunkiem zmian jest wprowadzenie do użytku bezpilotowych środków rozpoznania, nowych stacji radiolokacyjnych i radarów obserwacji pola walki.

Wydaje się, że jakość sieci informacyjnej taktycznego systemu rozpoznania skażeń można poprawić poprzez:

- wyposażenie elementów strukturalnych systemu w urządzenia do automatycznego wykrywania i określania parametrów wybuchów jądrowych, w tym również powietrznych;
- wprowadzenie do wyposażenia pododdziałów rozpoznania skażeń przyrządów umożliwiających automatyczne wykrywanie większej liczby środków toksycznych, w tym także przemysłowych;
- automatyzację pomiarów meteorologicznych;
- stworzenie sieci zintegrowanych, zautomatyzowanych i mobilnych stacji pomiarowych, umożliwiających równoległe wykonywanie pomiarów oraz automatyzację transmisji danych do nadrzędnych elementów systemu.

Wprowadzenie na szczebel związku taktycznego organicznych pododdziałów rozpoznania powietrznego (śmigłowców i środków bezpilotowych) zwiększy wydajność informacyjną sieci i przyczyni się do wzrostu stopnia wiarygodności pozyskiwanych danych poprzez porównanie wyników rozpoznania pozyskiwanych z różnych źródeł powietrzno-lądowego systemu zdobywania danych. Praktyka ćwiczeń i rozważania teoretyczne wskazują na potrzebę włączenia jednostek śmigłowców rozpoznawczych w strukturę organizacyjną związków taktycznych.

Autorzy pracy zdają sobie sprawę, że wiele interesujących problemów zostało tylko zasygnalizowanych, niektóre zaś zjawiska tylko oszacowane i jako takie wymagają dalszych badań. Ze względu na trwający proces restrukturyzacji wojsk rozpoznawczych, zespół autorski ma również świadomość zmienności przedmiotu badań, która stawia pod znakiem zapytania trwałość uzyskanych wyników i sformułowanych wniosków. Można jednak przyjąć, iż kontynuacja dalszych badań w zakresie systemu rozpoznania wojsk lądowych koncentrować się powinna na opracowaniu:

- systemu komputerowego wspomagania pracy komórki G-2,

- wsparcia informatycznego w procesie przekazywania danych,
- technicznej modernizacji kanałów informacyjnych,
- pojazdu sztabowego na potrzeby taktycznego systemu rozpoznania.

Istniejący obecnie system rozpoznania wojskowego stanowi rezultat tworzenia (to znaczy planowania i organizowania) w okresie ostatnich dziesięcioleci. Jest on zdolny do pozyskiwania danych (informacji) dla wojsk z bardzo ograniczonymi możliwościami, musi jednak posłużyć jako baza dla ewolucyjnego rozwoju systemu rozpoznania wojskowego dla potrzeb wojsk lądowych XXI wieku. Założyć można, iż sukces w tym aspekcie może być osiągnięty poprzez realizację między innymi następujących przedsięwzięć:

- powstanie całej rodziny nowoczesnych interoperacyjnych systemów,;
- integracji innych systemów z systemem rozpoznania dla pozyskania większych możliwości zdobywania danych (informacji) i pełnej interoperatywności systemu;
- przygotowania systemu rozpoznania wg nowej koncepcji prowadzenia działań (operacji);
- tworzenie nowych symulacyjnych systemów treningowych w wersji indywidualnej, zespołowej lub całych jednostek, w ramach operacji (działań) połączonych, wielonarodowych itp., jednocześnie realistyczne przedstawianie tego, co może, a czego nie może osiągnąć rozpoznanie w obecnym i przyszłym kształcie.

Z całą pewnością uzupełnienia i pogłębienia wymaga problematyka wpływu procesu przygotowania kadry do realizacji zadań w nowych strukturach organizacyjnych. Należy również zastanowić się nad potrzebą i możliwością opracowania i stosowania standardów edukacyjnych dostosowanych do stanowisk służbowych, stworzenia systemu zapewniającego jakość kształcenia zawodowego oraz możliwością wykorzystania doświadczeń szkolnictwa wojskowego państw NATO.

Wnioski z badań mogą być wykorzystane w procesie modernizacji systemu rozpoznania wojsk lądowych oraz w działalności dydaktycznej. Autorzy pracy mają nadzieję, że przedstawiony materiał będzie kolejnym elementem

w tworzeniu nowoczesnego systemu rozpoznania. Wyniki badań mogą być w przyszłości przyczynkiem zmian racjonalizujących funkcjonowanie systemu rozpoznania oraz upowszechnienia poruszanej problematyki wśród kadry pionu rozpoznania wojskowego.

BIBLIOGRAFIA

Literatura przedmiotu:

1. Black J., War Post. Present and Future, Sulton Publishing, London 2000.
2. Ciborowski L., Kierowanie obroną państwa i dowodzenie wojskami, Warszawa 1998.
3. Ciborowski L., Walka informacyjna, Toruń 1999.
4. Clausewitz C., O wojnie, Warszawa 1995.
5. Czajka K., Malinowski P., Rozpoznanie na rzecz wsparcia ogniowego wojsk lądowych, Warszawa 2002.
6. Dęga Cz., Uzbrojenie i pole walki wojsk lądowych do 2020 roku, Warszawa 1995.
7. Grzelak Cz., Stańczyk S., Zwoliński S. Bez możliwości wyboru, Warszawa 1993 r.
8. Heisbourg F., Wojny, Warszawa 1998.
9. Jakubczak R., Marczak J., Obrona Terytorialna Polski na progu XXI wieku, Warszawa 1998.
10. Jakubczak R., Wojska Obrony terytorialnej, Warszawa 2002.
11. Jańczak J., Walka elektroniczna w działaniach taktycznych, Warszawa 1999.
12. Jóźwiak K., Rozpoznanie powietrzne, Warszawa 1996.
13. Kaczmarek W., Ścibiorek Z., Przyszła wojna - jaka?, Warszawa 1995.
14. Kalenbergh L., Za wolność naszą i waszą, Warszawa 1968
15. Kamiński S., Pisma wybrane. Tom IV. Nauka i metoda, pojęcie nauki i klasyfikacja nauk, wyd. IV, Lublin, KUL 1992.
16. Kawka W., Kowalkowski S., Struktury organizacyjne wojsk inżynieryjnych, Warszawa 2002.
17. Kisiel J., Rozpoznanie wojskowe (podstawy teoretyczne). Warszawa AON, 1998. S/3916
18. Koziej S., Teoria sztuki wojennej, Warszawa 1993.
19. Kulczyński S., Organizacja, działania i szkolenie pododdziałów specjalnych w siłach zbrojnych wybranych państw, Warszawa 1992.
20. Kwećka R., Nowak A. Budowa modelu systemu rozpoznania wojskowego w aspekcie organizacyjnym i informacyjnym, rozprawa doktorska, AON. Warszawa 1994.
21. Libicki M., What is Information Warfare, Washington 1995.
22. Łokociejewski M.(red.), Rozpoznanie wojskowe, cz. I, Podstawy teoretyczne, cz. II Działalność informacyjna, cz. II Prowadzenie działań rozpoznawczych, Warszawa 2003.
23. Michalak W., Suchora S., Użycie śmigłowców rozpoznawczych w działaniach bojowych wojsk, Warszawa 1995.

24. Michniak J., Wisz A., Bezpieczeństwo i ochrona informacji w wojskowych sieciach telekomunikacyjnych i zautomatyzowanych systemach dowodzenia, Warszawa 2000.
25. Nowak A. (red.) Planowanie, organizowanie i prowadzenie działań rozpoznawczych, Warszawa AON, 2003
26. Nowak A., Działalność rozpoznawcza na szczeblach taktycznych, AON, Warszawa 2002.
27. Parzewski J., Rozpoznanie inżynieryjne w działaniach taktycznych, Warszawa 1995.
28. Scheffs W., Batalion walki radioelektronicznej w działaniach operacyjnych, Warszawa 2002
29. Scheffs W.: Możliwości bojowo-rozpoznawcze pododdziałów walki elektronicznej, AON, Warszawa 2003
30. Szmyd R., Motocyklowy zwiad w Wojsku Polskim, Warszawa 1999.
31. Sztuka wojenna sił zbrojnych uczestniczących w wojnach lokalnych i ważniejszych konfliktach zbrojnych po II wojnie światowej, Warszawa 1997.
32. Toffler A. i H., Trzecia fala, Warszawa 1997.
33. Toffler A. i H., Wojna i antywojna, Warszawa 1997.
34. Wrzosek M., Działania rozpoznawcze na obszarze kraju, AON, Warszawa 2003.
35. Wrzosek M., Taktyczny system rozpoznania wojsk lądowych, Warszawa 2004.
36. Ziółkowski L., Rubaj T., Organizacja, uzbrojenie, możliwości bojowe i kierunki rozwoju wojsk rakietowych i artylerii, Warszawa 2002.

Encyklopedie i słowniki:

1. Słownik Języka Polskiego, PWN, tom I Warszawa1978.
2. Słownik Poprawnej Polszczyzny, PWN, Warszawa 1980.

Artykuły:

1. Balcerowicz B., Wojny współczesne. Wojny Przyszłe, Myśl Wojskowa nr 5/2003.
2. Faber P., Rewolucja w dziedzinie wojskowości (proponowany zarys programu szkolenia), Zeszyt Naukowy AON nr 4 (53) 2003.
3. Gudera G., Das Heer auf dem Weg in die Zukunft, Europäische Sicherheit, nr 10/2000.
4. J. L. Bezpieczeństwo Stanów Zjednoczonych w świetle walki informacyjnej, Wojskowy Przegląd Zagraniczny 3/99.
5. K. B. Tendencje rozwojowe bojowych wozów rozpoznawczych, Wojskowy Przegląd Zagraniczny nr 2/97.
6. Łuczak W., Zrobotyzowana US army XXI wieku, Raport – wto, 9/2002.
7. Müller N., Krieg im Informationszeitalter. Was ist neu? w: „Schweizer Soldat" nr 11/1995.
8. Prądzyński S., Kierunki doskonalenia obiegu informacji systemu wykrywania skażeń w aspekcie zmian strukturalnych sił zbrojnych, Myśl Wojskowa nr 6/97.
9. Rutkowski C., Problemy bezpieczeństwa i sił zbrojnych XXI wieku, Myśl Wojskowa nr 2 (613)/2001.

10. Stokalski A., Tendencje rozwojowe w dziedzinie automatyzacji dowodzenia i kierowania środkami walki wojsk lądowych, Myśl Wojskowa 2, Warszawa 1992 Skrzypczak W., Operacja kombinowana, Polska Zbrojna 21 (331) Maj 2003.
11. Wojna w Iraku, oceny naszych ekspertów. Biuletyn AON nr 2 (14)/2003.
12. Wrzosek M., Struktura strumienia informacyjnego w taktycznym systemie rozpoznania wojsk lądowych, ZN AON nr 2 (cz. I), 3-4 (cz. II), Warszawa 2002.

Opracowania o charakterze normatywnym:

1. NATO AAP-6 (2003).
2. Program TRADOC 525-5, Chief Staff Army "Vision for 21st Century"
3. Regulamin działań wojsk Lądowych, Warszawa 1999.
4. Rozpoznanie wojskowe, Doktryna połączona, Szt.Gen.1531/2001, Warszawa 2001
5. FM-34-1, Intelligence and electronic warfare operations, Headquorters Departments of the Army, Washington DC 1994.
6. FM-34-130, Intelligence Preparation of the Battlefield, Headquorters Departments of the Army, Washington DC 1994.
7. FM-34-60, Counterintlligence, Headquorters Departments of the Army, Washington DC 1994.
8. FM-5-105, Topographic Operations, Headquorters Departments of the Army, Washington DC 1993.
9. Działania rozpoznawcze, Tymczasowa instrukcja, DWLąd.Wewn.17/2002, Warszawa 2002

Strony internetowe:

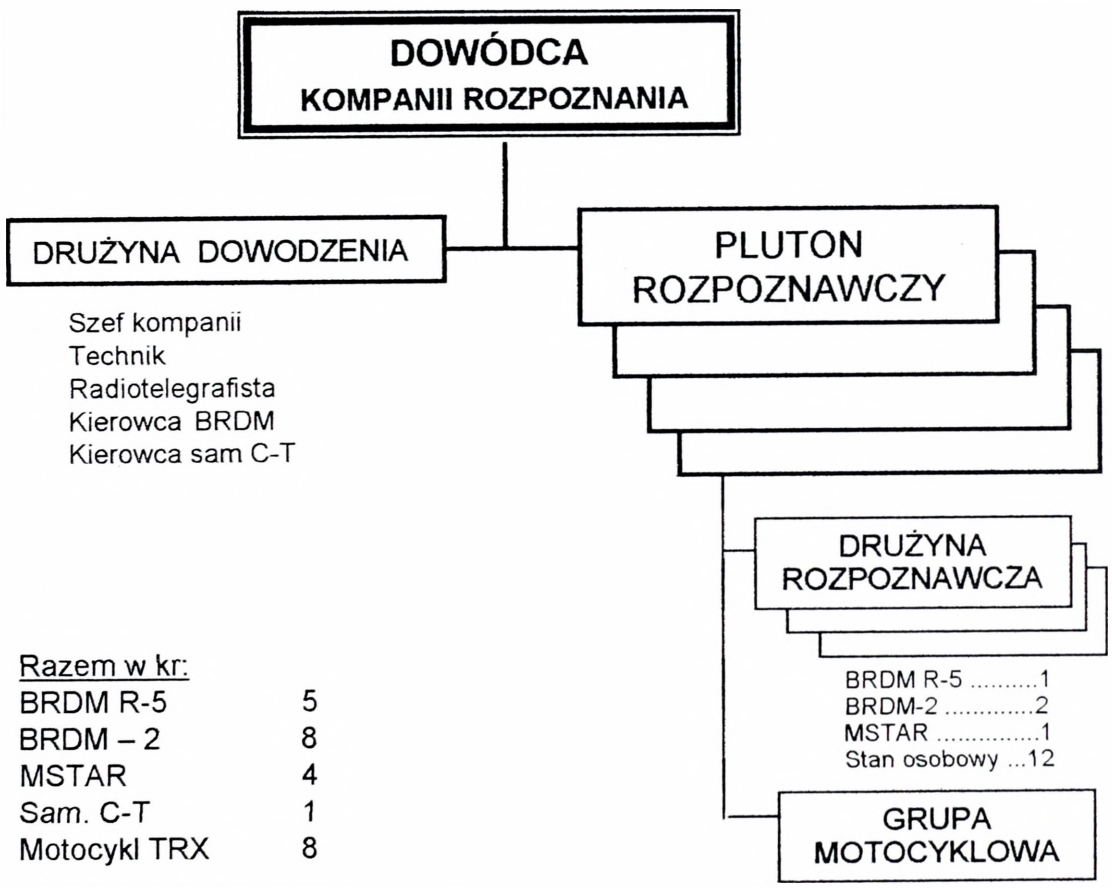
- http://www.echelonwatch.org/
- http://www.hr/mprofaca/echelon.html
- http://www.echelon.wiretapped.net/
- http://www.fas.org/irp/eprint/sp/
- http://jya.com/cryptout.htm echelon
- http://jya.com/echelon-dc.htm
- http://www.iptvreports.mcmail.com/stoa_cover.htm
- http://www.gn.apc.org/duncan/stoa.htm
- http://www.fipr.org/rip
- http://jedi.konsnet.ru/sorm
- http://ipsec.pl/opsec/article/171
- http://www.isoc.org.pl/2001/rozporzadzenie_mswia/projekt.pl.html
- http://ipsec.pl/ipsec/article/291

ZAŁĄCZNIKI

1. Struktura organizacyjna kompanii rozpoznawczej oddziału
2. Struktura organizacyjna batalionu rozpoznawczego
3. Struktura organizacyjna kompanii rozpoznania radioelektronicznego
4. Struktura organizacyjna eskadry śmigłowców rozpoznawczo-łącznikowych
5. Struktura organizacyjna kompanii rozpoznawczej OT
6. Struktura organizacyjna pododdziałów rozpoznania artyleryjskiego w brygadzie
7. Struktura organizacyjna pododdziałów rozpoznania artyleryjskiego w dywizji
8. Pododdziały rozpoznania inżynieryjnego na poziomie taktycznym
9. Pododdziały rozpoznania skażeń na poziomie taktycznym
10. Przepływ informacji rozpoznawczych w G-2
11. Jednostki rozpoznawcze w strukturze organizacyjnej wojsk lądowych na poziomie taktycznym
12. Arkusz obserwacji
13. Kwestionariusz opinii eksperta

Załącznik 1

STRUKTURA ORGANIZACYJNA KOMPANII ROZPOZNANIA ODDZIAŁU

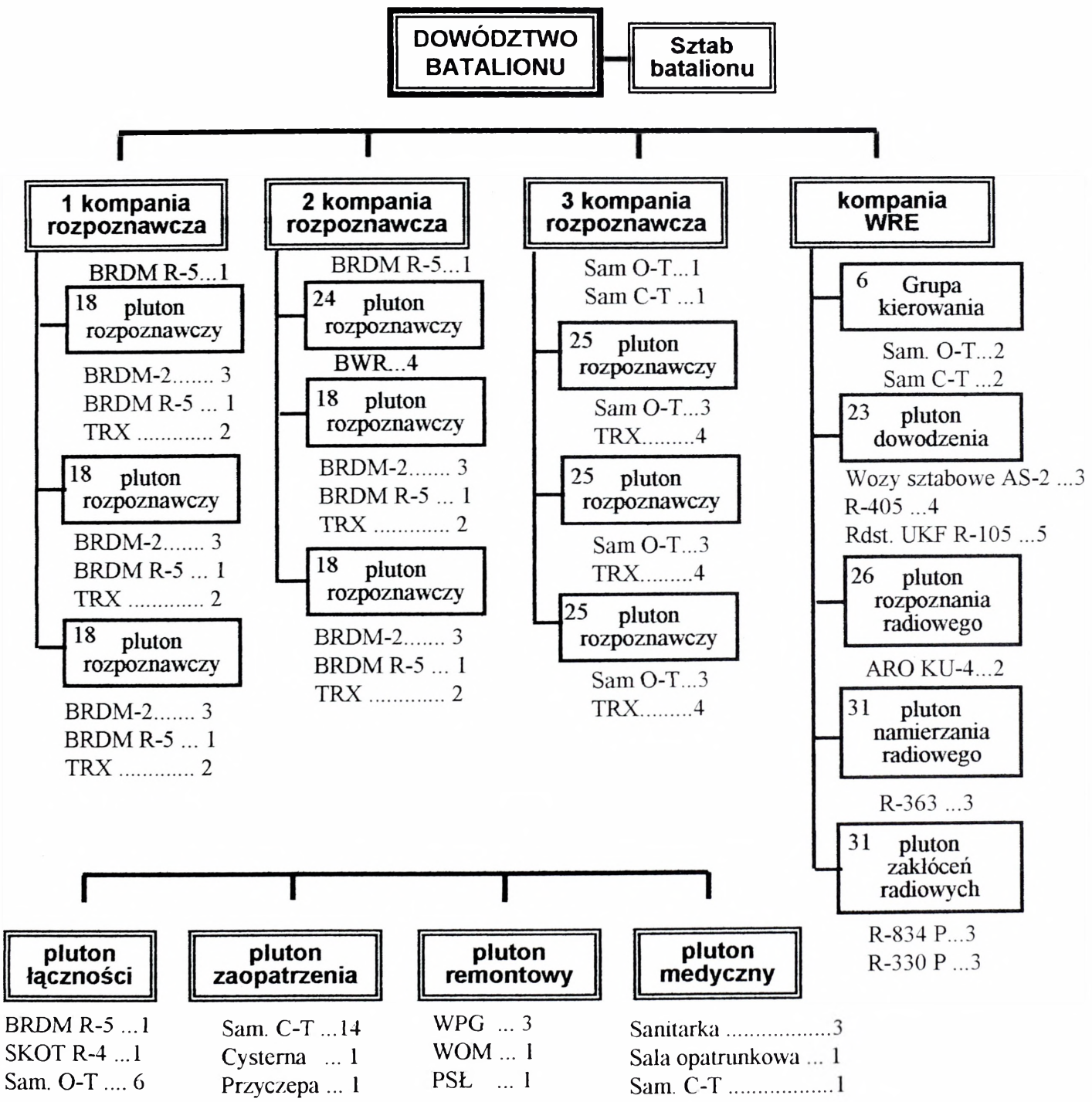


Razem w kr:	
BRDM R-5	5
BRDM – 2	8
MSTAR	4
Sam. C-T	1
Motocykl TRX	8

Załącznik 2

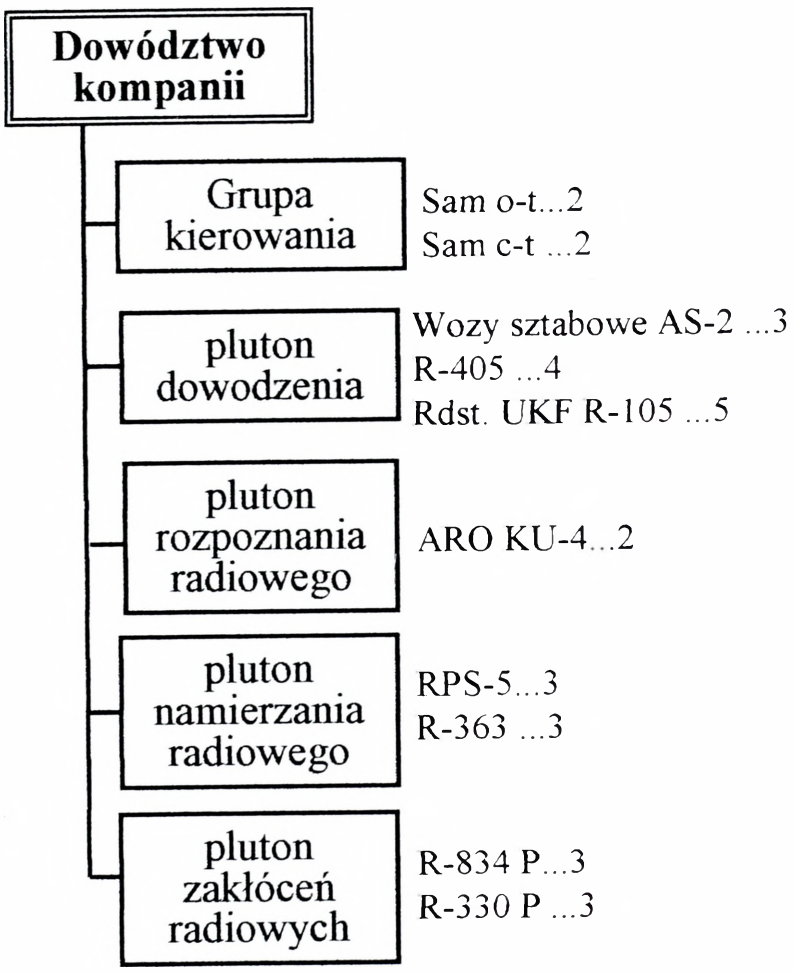
STRUKTURA ORGANIZACYJNA BATALIONU ROZPOZNAWCZEGO

(wariant)



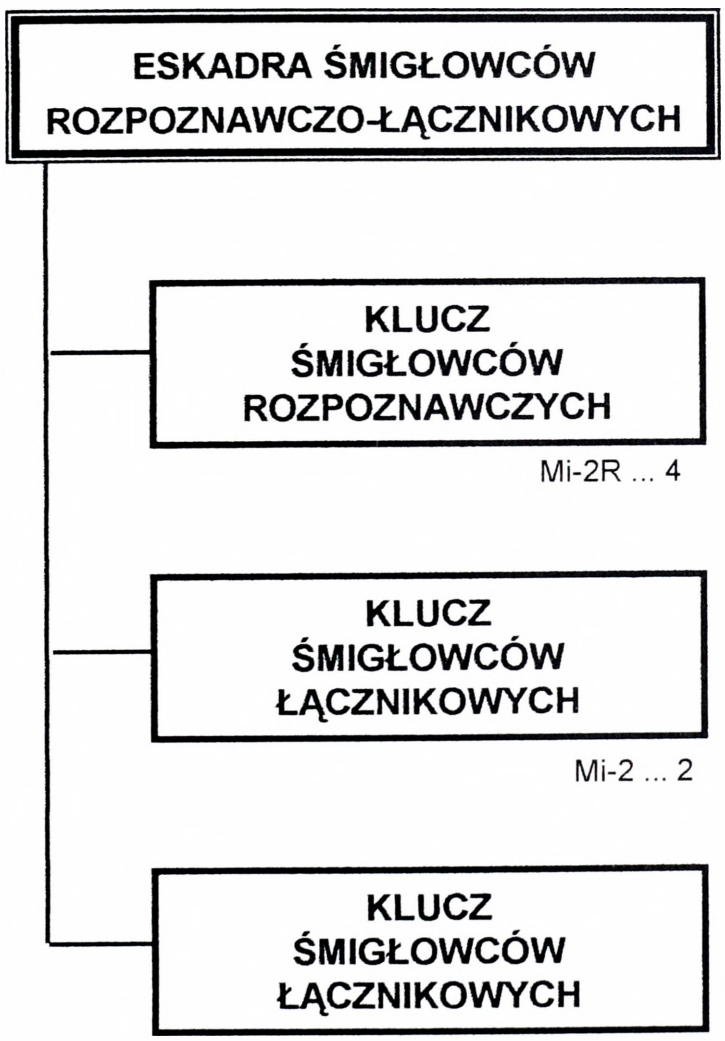
Załącznik 3

STRUKTURA ORGANIZACYJNA KOMPANII ROZPOZNANIA RADIOELEKTRONICZNEGO



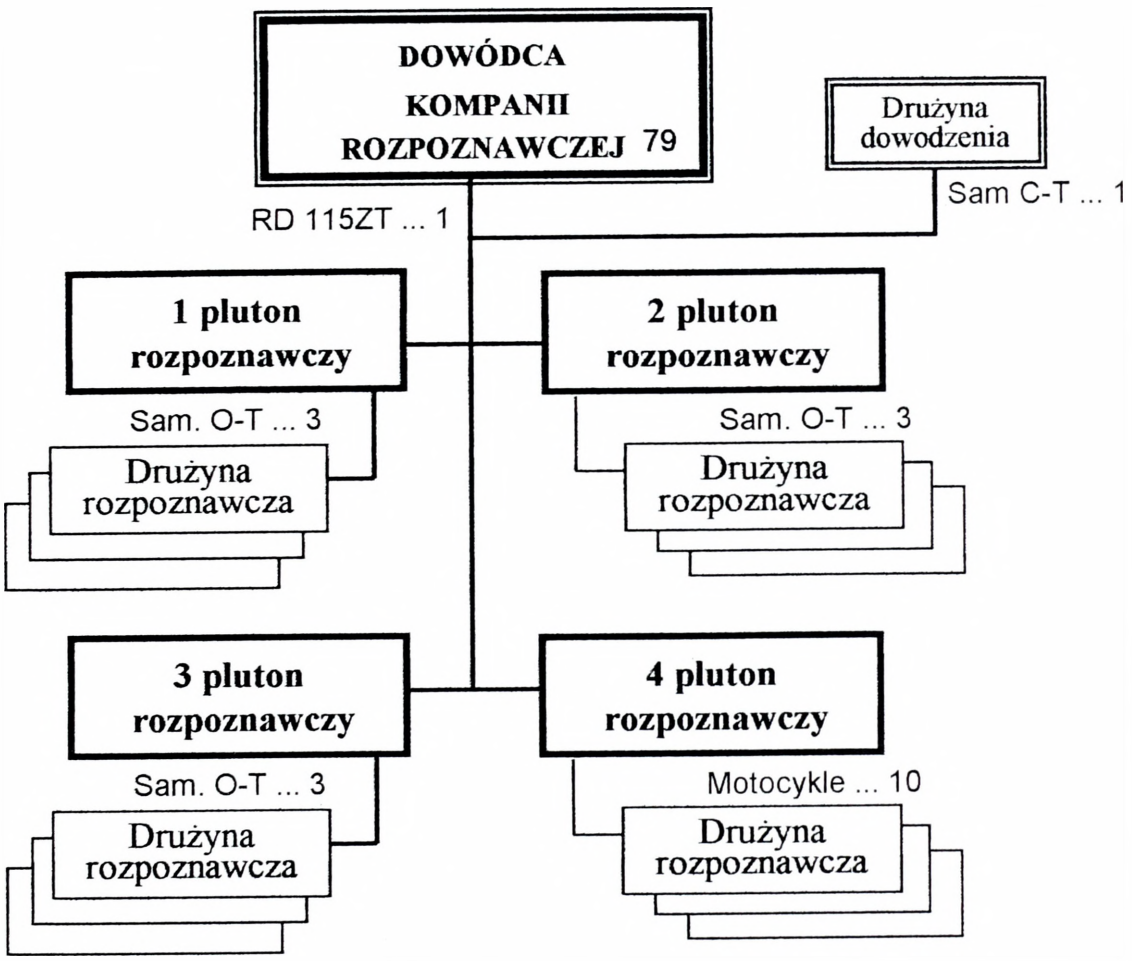
Załącznik 4

STRUKTURA ORGANIZACYJNA ESKADRY ŚMIGŁOWCÓW ROZPOZNAWCZO-ŁĄCZNIKOWYCH



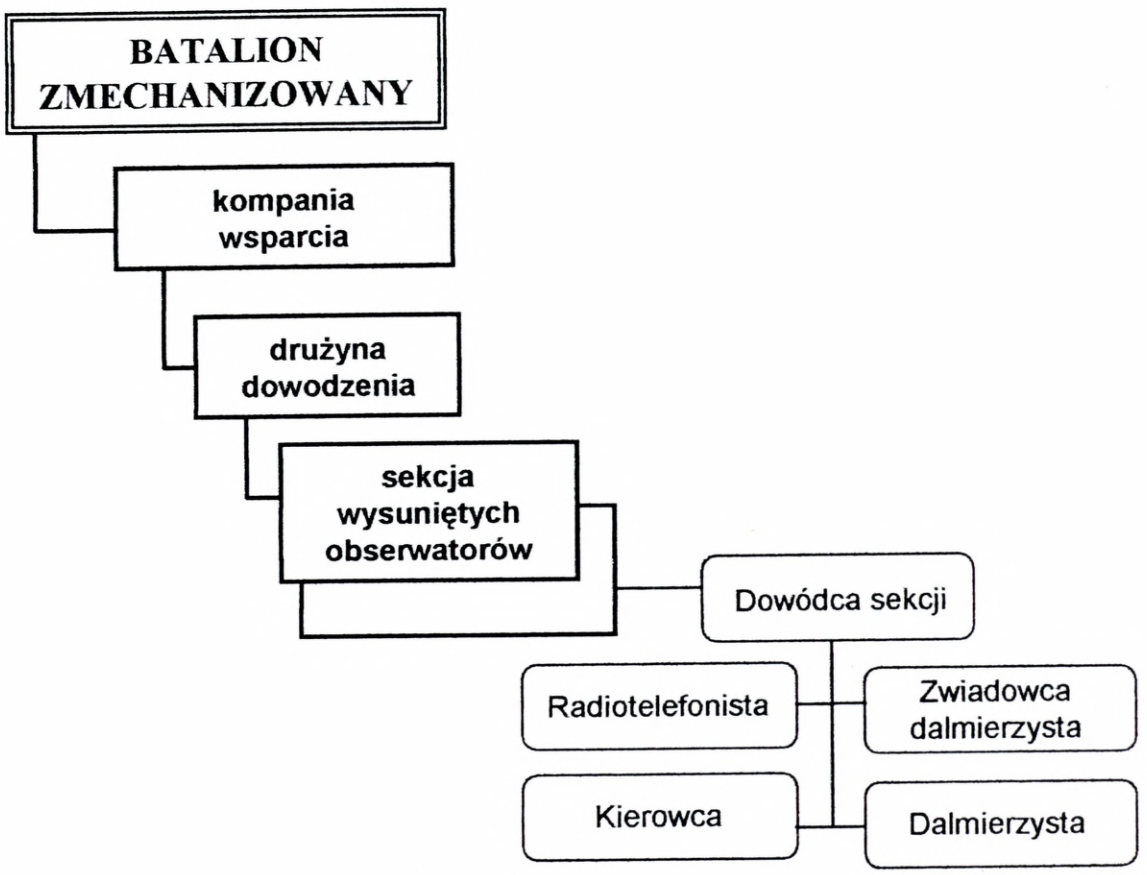
Załącznik 5

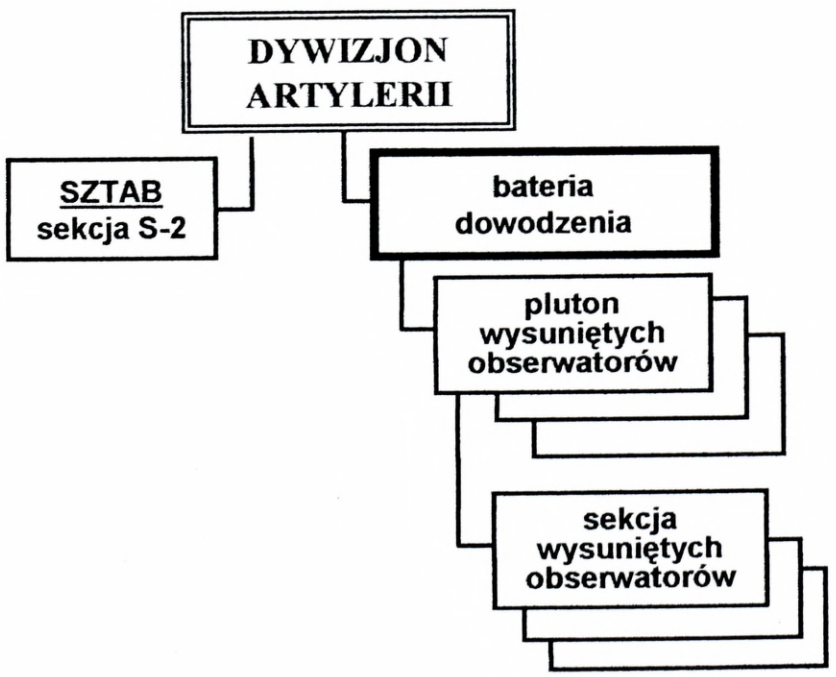
STRUKTURA ORGANIZACYJNA KOMPANII ROZPOZNAWCZEJ OT



Załącznik 6

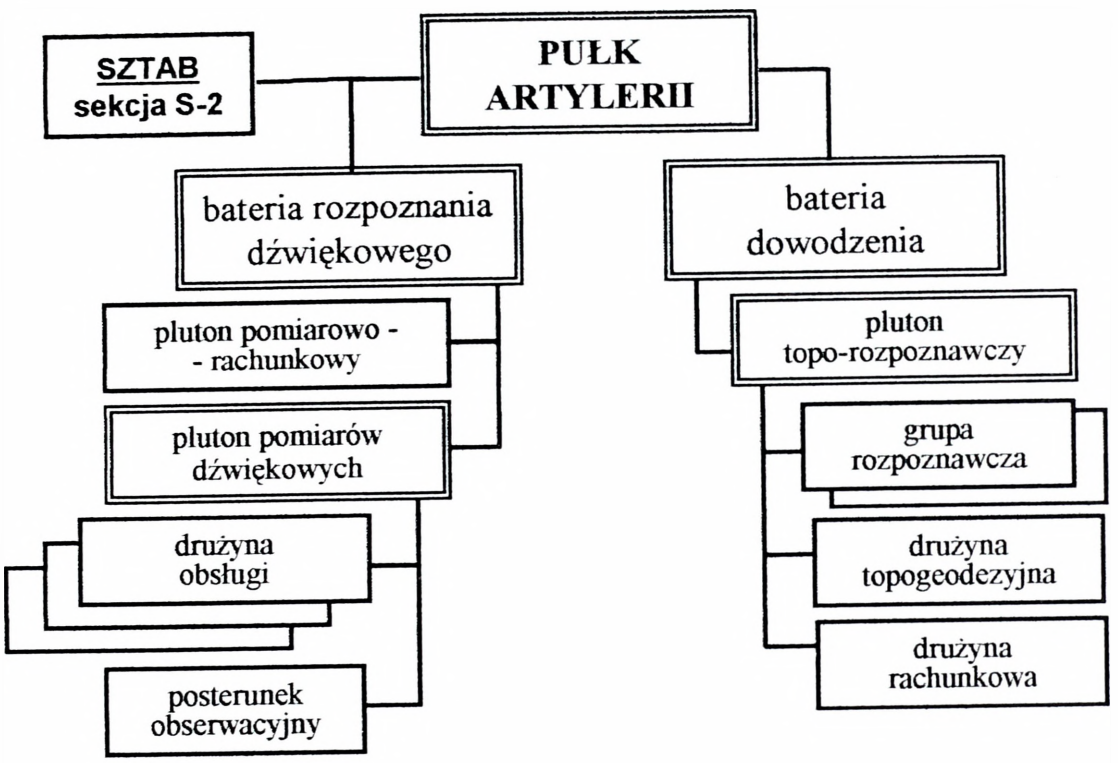
STRUKTURA ORGANIZACYJNA PODODDZIAŁÓW ROZPOZNANIA ARTYLERYJSKIEGO W BRYGADZIE

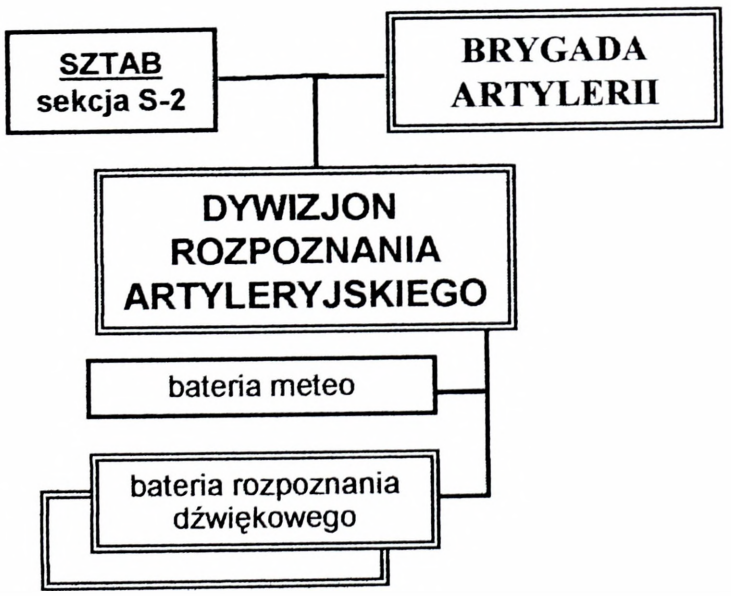




Załącznik 7

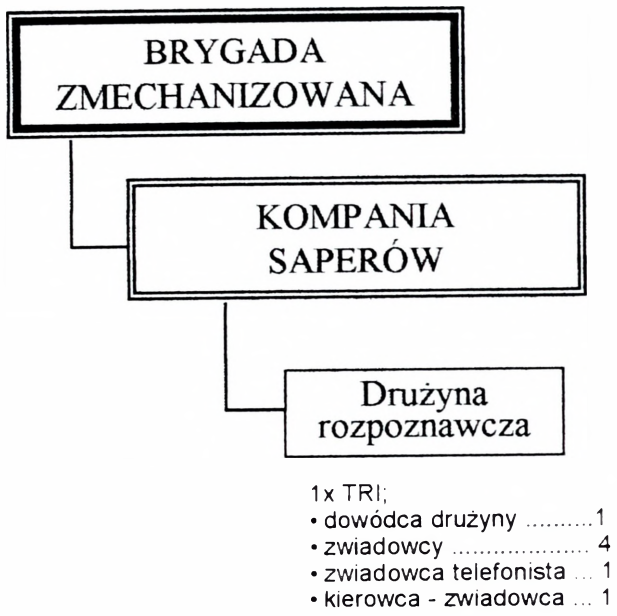
STRUKTURA ORGANIZACYJNA PODODDZIAŁÓW ROZPOZNANIA ARTYLERYJSKIEGO W DYWIZJI

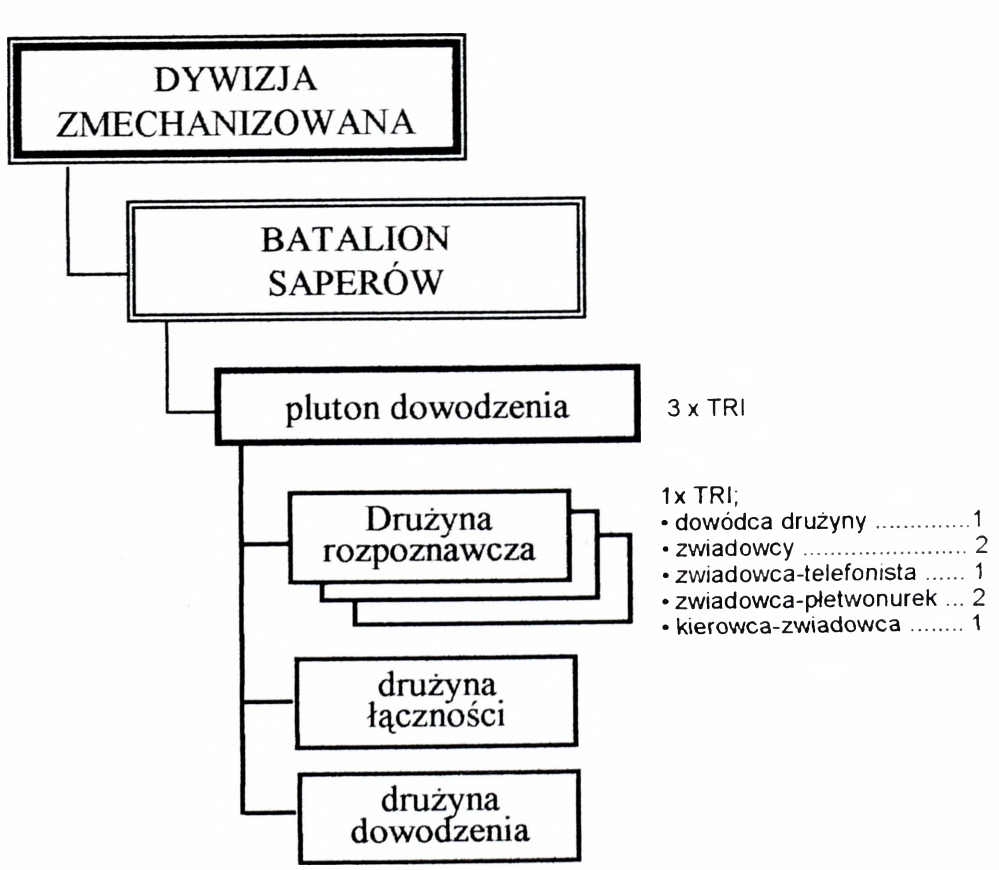




Załącznik 8

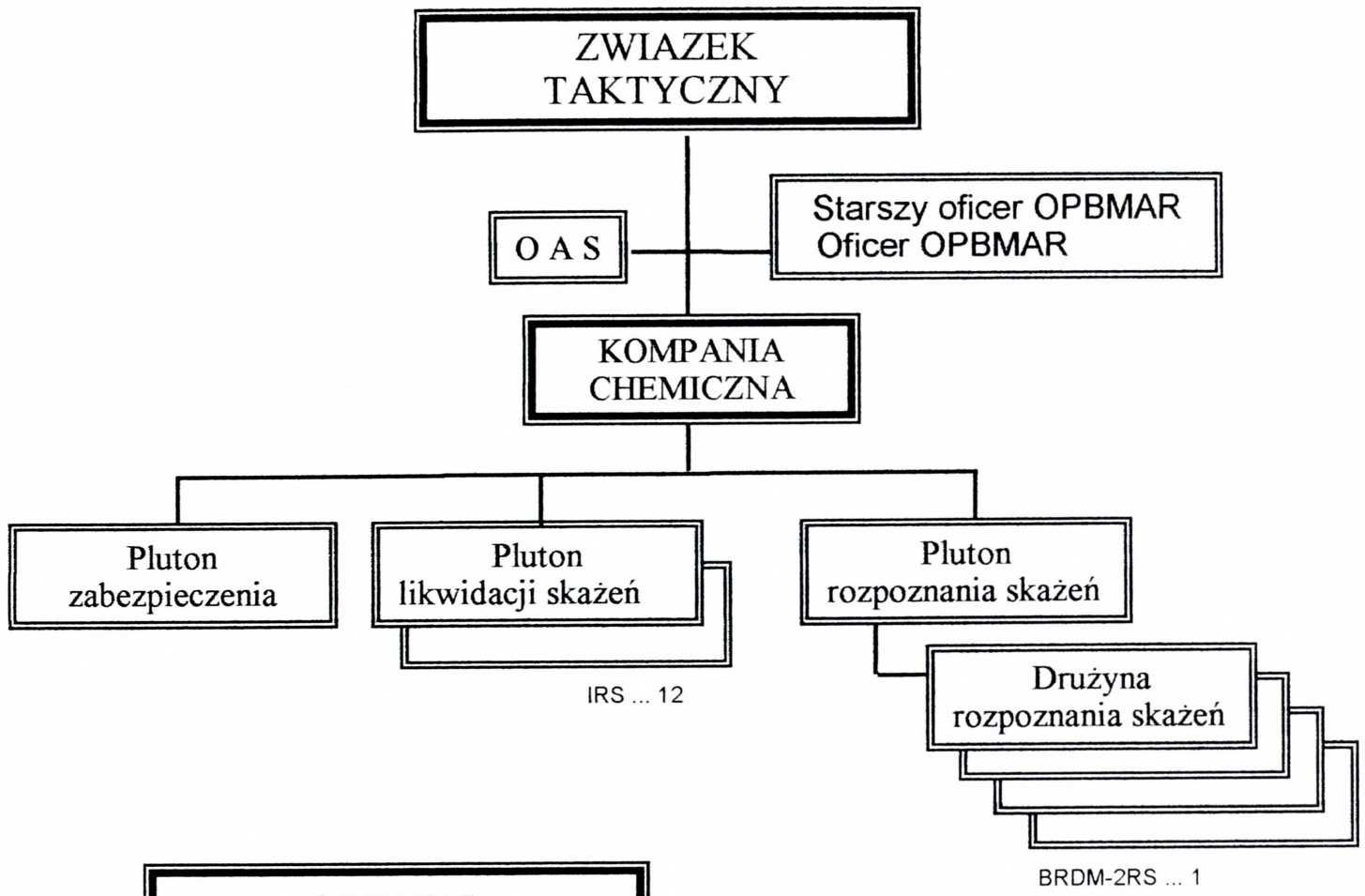
PODODDZIAŁY ROZPOZNANIA INŻYNIERYJNEGO NA POZIOMIE TAKTYCZNYM

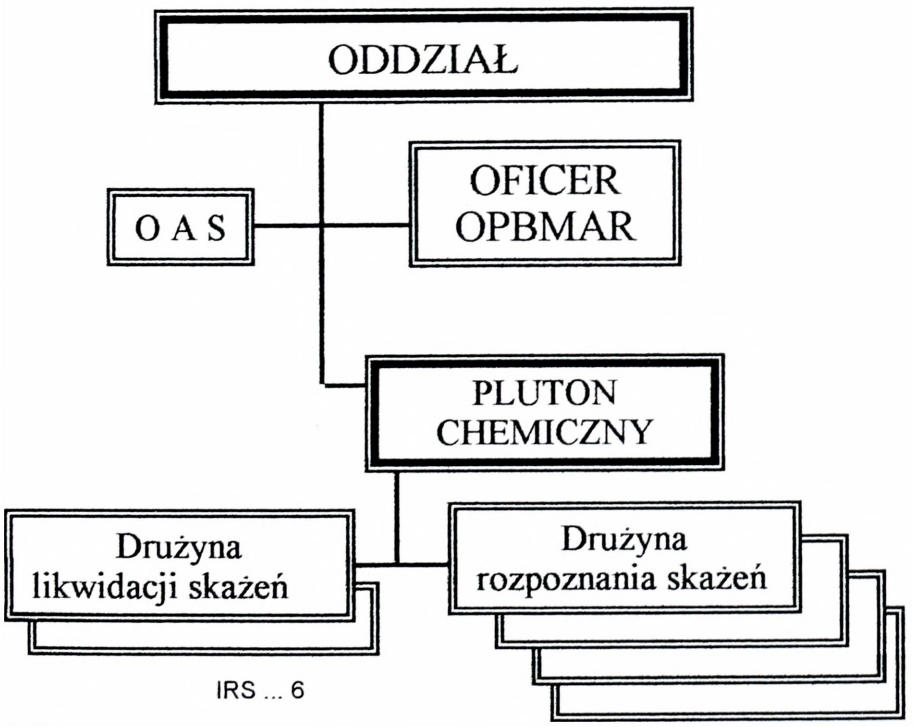




Załącznik 9

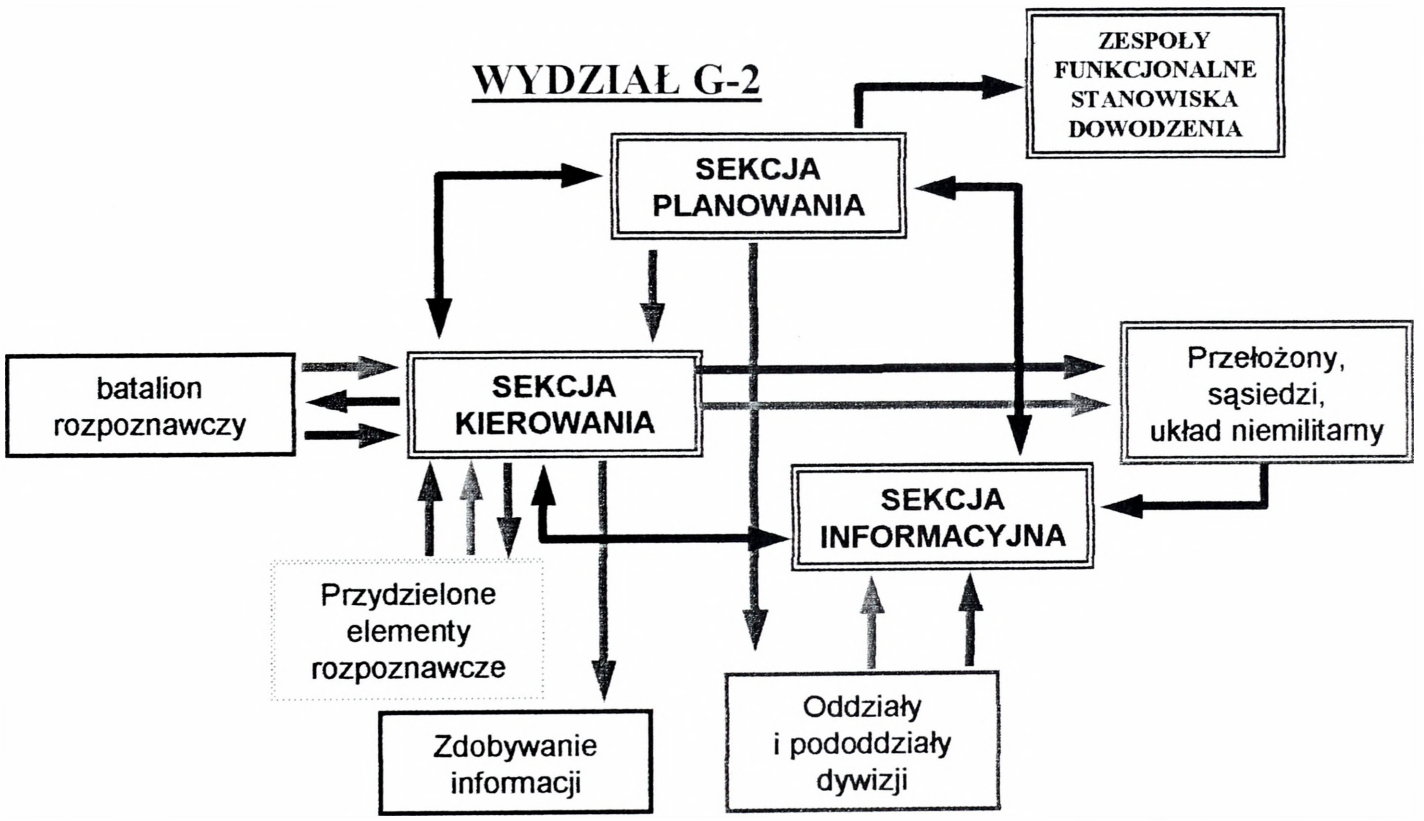
PODODDZIAŁY ROZPOZNANIA SKAŻEŃ NA POZIOMIE TAKTYCZNYM





Załącznik 10

PRZEPŁYW INFORMACJI ROZPOZNAWCZYCH W G-2



Legenda:

- Zadania rozpoznawcze
- Meldunki rozpoznawcze
- Wymiana informacji
- Zapotrzebowanie na informacje

JEDNOSTKI ROZPOZNAWCZE W STRUKTURZE ORGANIZACYJNEJ WOJSK LĄDOWYCH NA POZIOMIE TAKTYCZNYM

Wyszczególnienie	Związek taktyczny	Oddział	Pododdział
Rozpoznanie sytuacyjne (ogólnowojskowe)			
Wojska zmechanizowane i pancerne	• Wydział Rozpoznawczy (G-2) • batalion rozpoznawczy	• sekcja rozpoznawcza (S-2) • kompania rozpoznania	• sekcja rozpoznawcza (S-2) • nieetatowy pluton rozpoznania
Rozpoznanie specjalistyczne (rodzajów wojsk)			
Artyleria	**pułk artylerii** • S-2 • **bateria rozpoznania dźwiękowego**: pluton pomiarowo-rachunkowy pluton pomiarów dźwiękowych ▪ **bateria dowodzenia**: pluton topograficzno-rozpoznawczy	**dywizjon artylerii samobieżnej** • S-2 • bateria dowodzenia (trzy plutony wysuniętych obserwatorów)	**kompania wsparcia** • drużyna dowodzenia (dwie sekcje wysuniętych obserwatorów)
Wojska inżynieryjne	**batalion saperów** • pluton dowodzenia /3 x drrinż/	**kompania saperów** • drrinż	
Wojska opchem	**St. oficer OPBMAR/G-3** Oficer OPBMAR **Kompania przeciwchemiczna** • pluton rozpoznania skażeń (pięć drużyn rozpoznania skażeń) • **OAS** (batalion dowodzenia)	**Oficer OPBMAR/S-3** **pluton chemiczny** (cztery drużyny rozpoznania skażeń, OAS)	
Lotnictwo Wojsk Lądowych	**Eskadra śmigłowców rozpoznawczo-łącznikowych**		

Załącznik 12

ARKUSZ OBSERWACJI

Obiekt obserwacji: .....

Rodzaj obserwacji: .....

Data .....

ELEMENTY PODLEGAJĄCE OBSERWACJI:

1. Struktura systemu rozpoznania.
2. Siły i środki wydzielane przez ćwiczących do prowadzenia rozpoznania w poszczególnych etapach operacji/walki.
3. Podział obowiązków funkcyjnych w komórkach stanowiska dowodzenia w zakresie realizacji przedsięwzięć planistycznych i wykonawczych w ramach rozpoznania.
4. Potrzeby systemu rozpoznania w zakresie zdobywania informacji.
5. Wymiana informacji rozpoznawczych w ćwiczących sztabach.
6. koordynacja działań rozpoznawczych w ramach ćwiczących poziomów dowodzenia.
7. Inne spostrzeżenia.

Załącznik 13

Narzędzia badawcze stosowanie w procesie badań naukowych
Kwestionariusz opinii eksperta

AKADEMIA OBRONY NARODOWEJ
WYDZIAŁ WOJSK LĄDOWYCH

KWESTIONARIUSZ OPINII EKSPERTA

Celem przeprowadzanych badań jest poznanie opinii doświadczonych oficerów w zakresie prognozy rozwoju systemu rozpoznania w dającej się przewidzieć przyszłości.

Wyniki badań uzyskane tą drogą wzbogacą wiedzę z zakresu rozpatrywanego problemu oraz stanowić będą jedno z istotnych źródeł opracowania wniosków zawartych w pracy naukowo badawczej na temat: „Kierunki rozwoju systemów rozpoznania Wojsk Lądowych".

Serdecznie dziękuję za współpracę

ppłk Andrzej NOWAK

Warszawa **2005**

Wyniki badań dotyczące przyszłych operacji Sił Zbrojnych upoważniają mnie do stwierdzenia że na pierwszy plan w rozwoju dzisiejszych Sił Zbrojnych wysuwają się przeobrażenia między innymi w myśli wojskowej, spowodowane w dużej części przez rewolucję techniczną. Ponadto, bardzo złożone środowisko pola walki, będące skutkiem tych wydarzeń ma znaczące implikacje dla przyszłych operacji a tym samym i dla tworzenia nowego systemu rozpoznania.

Ostatnie operacje w Południowej Azji, Panamie, Somalii, Rwandzie, Haiti, Bośni oraz Iraku wpływają na obraz koniecznych zmian. Oznacza to wykreowanie „operacji dalekiego zasięgu" jakie siły zbrojne (w przewidywanej przyszłości) będą zmuszone prowadzić. Przytoczone powyżej przykłady to obraz średnio intensywnych konfliktów, a nie tradycyjnych wielkich bitew (oprócz Iraku).

Precyzyjne określenie trendów rozwojowych Sił Zbrojnych (a tym samym i systemu rozpoznania) zarówno w bliższej, jak i dalszej przyszłości jest niezmiernie trudne. Prognozowanie utrudnia nie tylko fakt, że dotyczy ono ciągłych przemian, ale również to, że rozwój technologii i ich wojskowych zastosowań jest wyznaczany przez wiele różnorodnych uwarunkowań.

Stanisław Lem we wstępie do „Okamgnienia" przywołał wydaną w 1993 r. w Niemczech przez Federalne Ministerstwo do Spraw Badań i Technologii pracę pt.: „Technologie XXI stulecia". Z przekąsem zauważył, że jest rzeczą godną uwagi to, iż o rewolucji w dziedzinie ogólnoświatowej łączności (*world wide web*), czy też o biotechnologii, które stawały się niejako na oczach autorów, nie ma w niej ani jednego słowa, nie mówiąc już o poświęceniu temu tematowi osobnego rozdziału.

Przykład ten, podobnie jak inne, choćby z historii, wskazuje na to, jak niewdzięcznym zadaniem jest prognozowanie, zwłaszcza w odniesieniu do zjawisk cywilizacyjnych i kulturowo-społecznych. Niewdzięcznym, ale jakże frapującym. Bodajże generał Mac Arthur powiedział, że dobry żołnierz – niezależnie od tego czy dowodzi plutonem, czy armią – musi oglądać się w tył, patrzeć na boki i w przód, ale myśleć powinien tylko o przyszłości. Dobrze więc, że nasze myślenie nie kończy się na latach 2006–2008, lecz wybiega daleko w przód. Jest przy tym w prognozowaniu, zwłaszcza 25–30 letnim, pewien walor, który nie występuje w pracach nad planami średnio- i krótkoterminowymi. Ograniczone środki na realizację planów oraz korzystniejsza sytuacja geostrategiczna Polski jako członka NATO powodują, że z jednej strony ta bliska przyszłość sił zbrojnych jest postrzegana przez pryzmat niemożności – „nie stać nas na to", z drugiej zaś mniejsze zagrożenie skłania do traktowania sił zbrojnych jako efektownego, ale niezbyt przydatnego narzędzia. Wspomniany walor to komfort wynikający z tak odległej perspektywy, jak 25 lat. Pozwala bowiem na podejście typu: „wszystko się może zdarzyć". I choć nie upoważnia do fantazjowania, to jednak skłania do optymizmu, także w aspekcie finansowym.

Uwzględniając dotychczasowe burzliwe tempo postępu technicznego w świecie, można stwierdzić, że XXI wiek będzie wiekiem walki o informacje i wszelkie podejmowane działania będą temu podporządkowane. Utworzenie we wszystkich rodzajach Sił Zbrojnych wspólnych, zbiorowych i sieciowych struktur dowodzenia, rozpoznania i walki elektronicznej powinno zagwarantować dominację informacyjną na polu walki.

Prognozy owe są jednak obarczone wieloma niedoskonałościami, błędami różnego rodzaju, z elementarnymi włącznie. Błędem najbardziej rzucającym się w oczy jest skłonność do projektowania przyszłości jako ciągu linearnie dokonujących się zmian, ignorowanie obecnych w każdym procesie załamań rozwoju, regresów nawrotów itp. Najbardziej niebezpieczna zaś może okazać się skłonność do upraszczania, co najczęściej wyraża się w absolutyzacji czynnika postępu technologicznego. Groźny może się też okazać militarno-wojenny populizm z jego tanią futurystyką, ekspozycją wojen wirtualnych, fascynacją możliwą skutecznością przyszłych systemów walki (niszczenia) itd.

Pomimo tak wielkiej różnorodności determinantów warunkujących charakter przyszłych operacji, wydaje się, iż uprawnieni jesteśmy do postawienia tezy, że **charakter przyszłych operacji będzie odzwierciedlał ogólny charakter przyszłego świata**. Z tego też względu nie będzie on czymś wyalienowanym, czy oderwanym od otaczającej go rzeczywistości, lecz właśnie będzie się dokładnie w nią wkomponowywał. Nie będzie mógł być inny, ponieważ charakter operacji nie jest i nie może być samodzielnym, innym bytem, lecz musi mieścić się w realiach rozpatrywanego okresu i co więcej, odzwierciedlać najistotniejsze jego cechy. Stąd też nasuwają się następne pytania: jakie to najistotniejsze cechy złożą się na naturę przyszłego świata a następnie będą się przekładać na charakter przyszłych operacji? Jakie to potężne „siły" mogą w istotny i trwały sposób je formować?

Uznano, że siły zbrojne przyszłości nie mogą być dalej jednostronnie ukierunkowywane na prowadzenie - jak to nazwał gen. G. Gudera - **„dużych operacji"**.

Oprócz nich muszą one, w celu przeciwdziałania konfliktom i likwidowania kryzysów - jak to ma miejsce w byłej Jugosławii - być zdolne do prowadzenia **„średnich operacji"** (siłami około 10 000 ludzi) - i to dość długo.

Ponadto, w celu realizacji operacji ewakuacyjnych i ratowniczych oraz ochrony własnych wojsk przed grupami terrorystycznymi, siły zbrojne muszą być zdolne do prowadzenia **„małych operacji"**, nawet na obszarach daleko położonych od własnego kraju.

Najbardziej prawdopodobne operacje (średnie i małe) wymagają konsekwentnego i zupełnie nowego ukierunkowania sił zbrojnych i związanego z tym dostosowania ich możliwości i struktur. Reasumując, siły zbrojne muszą być zdolne do realizowania nowych zadań, a więc **prowadzenia operacji rozstrzygających, misji stabilizacyjnych oraz operacji specjalnych**.

Inną koncepcję konfliktów w XXI wieku przedstawił płk Peter FABER - w zarysie programu szkolenia - a mianowicie uważa on, „...że w tradycyjnych konfliktach wojownicy musieli kształtować walkę, by dopasować ją do dostępnego uzbrojenia. W konfliktach jutra posłużą się „bronią", która będzie kształtować walkę, wtedy „powiążą" atuty broni. Dlatego należy skupić się na umiejętnym wykorzystaniu posiadanej wiedzy i manipulowaniu nią, zamiast uciekać się do stosowania tradycyjnych metod (wzmacniać siły, nadzorować terytorium itd.)". Ponadto – autor stwierdza - że należy odrzucać strategię liniową lub strategię następujących po sobie operacji prowadzonych przez pojedyncze rodzaje sił zbrojnych lub ich komponenty. Trzeba raczej przewidywać duże rozproszenie obrońców, w wymiarze operacji równoległych, „skrojonych" na miarę „**zintegrowanych modułów sił**". Te wrażliwe na

wymiar czasowy operacje pozwolą na użycie siły rozstrzygającej, nie zaś miażdżącej, na „zdemontowanie" przeciwnika, a nie jego starcie z powierzchni ziemi i wreszcie, umożliwią przestrzeganie trzech zasad (opartego na RMA konfliktu): **1) wiedzieć więcej niż twój przeciwnik, 2) ubiec go, 3) unikać starć, kiedy ryzyko jest zbyt wysokie.**

Z przedstawionych rozważań wynika, że wiek XXI znacznie bardziej - nawet wręcz rewolucyjnie - zmienia i najprawdopodobniej będzie zmieniał współczesne bezpieczeństwo w porównaniu ze stanem, który istniał w wieku ubiegłym. Staje się ono obecnie coraz bardziej różnorodne, kompleksowe i znacznie trudniejsze do przewidzenia. Zwiększa się liczba podmiotów, które mogą w nim brać udział. Klasyczny międzypaństwowy wariant wojny staje się coraz mniej prawdopodobny.

Równocześnie, nowe wymagania zmieniają krajobraz przyszłych działań. Ich uczestnicy oraz ich struktury mogą być w skali dotychczas nieznanej - nie tylko wzajemnie powiązani, lecz także w różnorodny sposób uwikłani w wydarzenia międzynarodowe. Coraz widoczniejsze stają się również rozmiary związków między Północą, a Południem, gdyż zaczynają coraz skuteczniej pomagać w rozstrzyganiu problemów pojawiających się w podzielonym i zróżnicowanym świecie.

Wszystkie te czynniki mają decydujący wpływ na kształt przyszłych operacji. Wymagają, by rozumieć je jako zjawisko obejmujące wszystkie, a przynajmniej prawie wszystkie dziedziny życia. Wymagają również uznania:

- wielowymiarowego pojmowania kryzysów i konfliktów oraz niezbędności udzielenia odpowiedzi na wszystkie współczesne wyzwania polityki, bezpieczeństwa (a przynajmniej na ich większość);
- prewencji jako zjawiska niepodzielnego.

Na przykład, w walce z terroryzmem niezbędna okazała się współpraca międzynarodowa, umożliwiająca skuteczne, a zarazem wspólnie uzgodnione rozwiązanie pojawiających się wyzwań.

W konkluzji można stwierdzić że, struktura sił zbrojnych mogłaby uwzględniać cztery lub pięć rodzajów sił zbrojnych, tj. **Wojska Lądowe, Siły Powietrzne, Marynarkę Wojenną, Wojska Specjalne i Informacyjne**, podporządkowane jednemu dowództwu operacyjnemu na czas kryzysu lub wojny. Z kolei jednostki wojskowe, szczególnie te, które mogą być użyte w pierwszej kolejności, powinna cechować stała gotowość do jak najszybszej realizacji różnorodnych zadań, umiejętność rozpoznawania na czas zaistniałej i dość często zmieniającej się sytuacji oraz sprawnego realizowania zadań i częstej ich zmiany. Stawia to przed siłami zbrojnymi większe niż dotychczas wymagania w zakresie wyszkolenia, wyposażenia, uzbrojenia, zabezpieczenia i wszelkiego zaopatrywania, a także fizycznej i psychicznej odporności.

Realizacja tych zadań wymaga, aby każdy dowódca posiadał wiedzę, która pozwoli mu na szybką i właściwą ocenę sytuacji oraz optymalne podjęcie decyzji, by w razie potrzeby potrafił skorygować ją i dostosować do zmieniającej się sytuacji, a więc był zdolny do elastycznego kierowania (dowodzenia) współczesnymi działaniami. Zatem zasięg i szybkość działań rozpoznawczych powinien być tak głęboki, aby po wykryciu zagrożenia dowódca mógł zastosować z odpowiednim wyprzedzeniem skuteczne przeciwdziałanie. Istotne znaczenie ma w tym wypadku

także fakt, że siły zbrojne mogą być obecnie wykorzystywane do realizacji znacznie szerszego zakresu zadań niż to miało miejsce w minionym, industrialnym okresie.

W wyniku powyższych rozważań można założyć, że przyszłe operacje (operacje XXI wieku), będą się cechowały niespotykanym jak dotąd rozmachem i dynamiką w układzie wielowymiarowym (lądy, morza, powietrze, kosmos, cyberprzestrzeń) oraz wielonarodowym. Głównie będą to operacje prawdopodobnie poniżej progu wojny - o charakterze prewencyjnym bądź wymuszającym pokój. Już teraz, w operacjach tego typu daje się zaobserwować tendencje integracyjne niektórych rodzajów sił zbrojnych (np. w wymiarze powietrzno-lądowym). Proces ten może postępować stosunkowo szybko. Zacierające się różnice pomiędzy rodzajami sił zbrojnych mogą w rezultacie ewoluować na rzecz komponentów połączonych, zorganizowanych i funkcjonujących w obrębie określonych misji lub operacji.

Dotychczas rozpoznane trendy rozwoju wskazują, że na polu walki jutra: dowódcy będą mieli do swojej dyspozycji precyzyjniejsze niż dziś i o większej sile destrukcji i ruchliwsze systemy walki oraz elastyczniejsze struktury organizacyjne. Zmasowanie potencjalnych możliwości może pozwolić przyszłym dowódcom na:

- prowadzenie wielowymiarowych, równoczesnych operacji;
- postrzeganie pola walki w realnym lub zbliżonym do realnego czasie;
- pionowe i poziome zobrazowanie sytuacji w wojskach własnych i przeciwnika;
- precyzyjną lokalizację w czasie i przestrzeni „wariantów" ataku celów wysokoopłacalnych i wysokowartościowych, zarówno środkami niszczącymi jak i bronią nieniszczącą;
- szeroką ochronę wojsk własnych w czasie całej operacji;
- kierowanie operacjami połączonymi i wielonarodowymi, z szeregiem dodatkowych komponentów jak: agencje rządowe i pozarządowe, stowarzyszenia międzynarodowe, organizacje humanitarne itp.

Biorąc pod uwagę przedstawione powyżej informację oraz uwzględniając zalecenia sojusznicze i wnioski wynikające z praktyki dowodzenia uprzejmie proszę Pana o ustosunkowanie się do następujących problemów:

1. *Kierunki rozwoju systemu rozpoznania są determinowane rozwojem naukowo-technicznym w zakresie zdobywania, opracowania i przekazywania informacji;*
2. *Ze względu występowanie w obszarze przyszłych operacji dużej ilości obiektów do rozpoznania - w różnych środowiskach prowadzenia działań bojowych – przyszłościowy system rozpoznania musi być systemem zintegrowanym, wielopłaszczyznowym;*
3. *graficzne zobrazowanie pola walki umożliwi świadomość operacyjną dowódcy, skróci czas planowania i jednocześnie czas reakcji;*
4. *dla zapewnienia sprawnego działania systemu rozpoznania musi być technicznie doskonały system wymiany informacji zdolny do przesyłania dużych pakietów informacji na znaczące odległości;*
5. *istotną rolę w procesie planowania działań rozpoznawczych posiada dowódca , który określa zasadnicze potrzeby informacyjne, potrzeby realizacji zadań rozpoznawczych oraz kieruje działaniami rozpoznawczymi*

Uogólnienie wyników badań opinii ekspertów

Wyniki badań opinii ekspertów potwierdziły tezy postawione przez autora pracy dotyczące perspektywicznego systemu rozpoznania.

Perspektywiczny system, musi się kierować racjonalnymi działaniami, opartymi na błyskawicznym zdobywaniu, opracowywaniu i rozpowszechnianiu informacji. Dla nikogo przecież nie ulega wątpliwości, że ilość i jakość informacji dostarczona przez system rozpoznania ma i będzie miała bezpośredni wpływ na dowodzenie i jego efekty.

Osiągnięcia naukowo-techniczne spowodowały jakościowy skok w rozwoju niektórych środków rozpoznania, ale przede wszystkim nowych sposobów zdobywania, opracowywania i przekazywania zdobytych informacji. W tej dziedzinie, obok rozwoju fotografii (możliwości w tym zakresie ogromnie wzrosły), pojawiła się i wciąż jest doskonalona technika skanowania za pomocą urządzeń optoelektronicznych i radiolokacyjnych. Ponadto w rozpoznaniu obrazowym prace badawcze prowadzone są w obszarze czterech technik: fotografii, techniki infralokacji (termolokacja), telewizji i radiolokacji.

Według ocen specjalistów wojskowych z dziedziny rozpoznania lotniczego, najbliższe lata mają być okresem prac nad realizacją programów budowy nowych bezzałogowych aparatów latających. Obecnie aparaty rozpoznawcze zostały opracowane pod kątem spełnienia podstawowych wymagań, stawianych systemom na przyszłym polu walki. Przyszłościowymi ich zaletami ma być: uniwersalność, niski koszt budowy i eksploatacji, łatwość obsługi i krótki czas przygotowania do startu.

Efekty rozpoznania zobrazowane mają być na cyfrowej mapie wojskowej, a doskonalenie polegać ma na rozwiązaniu problemów wynikających z ograniczeń sprzętu używanego do wyświetlania. Istnieje możliwość wprowadzenia mechanizmów pozwalających na uproszczenie użytkowania map indywidualnych (tematycznych) na stanowisku pracy użytkownika. W tym celu proponuje się dwustopniową procedurę na oddzieleniu generowania map cyfrowych od ich użytkowania w systemie.

Nowe możliwości zobrazowania sytuacji na mapie wojskowej mają być udoskonalane dzięki rozwojowi grafiki komputerowej (zwłaszcza udoskonaleniu jakości generowanych obrazów), budowaniu złożonych systemów w czasie rzeczywistym (np. systemów wizualizacji dla potrzeb działań zbrojnych), a także - co wymaga podkreślenia - dzięki metodom symulacji rzeczywistości. Wynika stąd twierdzenie, że obszar zastosowań grafiki komputerowej wykroczy daleko poza metody prezentacji danych w postaci różnego rodzaju wykresów czy animacji dla potrzeb gier symulacyjnych.

W przyszłości systemy dowodzenia wykorzystywać muszą systemy łączności szerokopasmowej oraz łączność satelitarną. Generalnie dąży się do funkcjonalnej integracji i unifikacji systemów łączności i informatyki, czyli do utworzenia jednej platformy systemowej dla wszystkich rodzajów usług. Praktycznie użytkownicy będą mieli dostęp do wszystkich niezbędnych systemów i podsystemów informacyjnych, używając jednego komputera. Ponadto są prowadzone prace nad rozszerzeniem zdolności transmisyjnych sieci oraz nad zwiększeniem mobilności systemów łączności i informatyki.

Ponadto, w dalszym ciągu prym wieść będą systemy rozpoznania satelitarnego, dzięki którym zapewni się systematyczną kontrolę ogromnej ilości informacji pod względem militarnym, gospodarczym, stanu środowiska, pogody itp., co w konsekwencji doprowadzi do globalnego rozpoznania. Różnorodne urządzenia rozpoznawcze, w połączeniu z komputerami oraz dokładnymi danymi, pozwolą na maksymalne odciążenie użytkowników.

Dla skrócenia czasu upływającego od rozpoznania do zniszczenia przeciwnika buduje się systemy rozpoznawczo-uderzeniowe, które mają być podstawowymi środkami walki. Potwierdzeniem może być amerykański program robotyzacji pola walki. Przewiduje się, że rozwiązania z tego zakresu wykorzystywane będą m.in. do realizacji zadań związanych z rozpoznaniem, wyszukaniem celu, rozmieszczeniem czujników pomiarowych itp.

Właściwe (tj. szybkie i sprawne) wykorzystanie nowych technologii informacji może przyczynić się do zdobycia kluczowych informacji niezbędnych do realizacji zadań. Nowoczesne technologie informowania oraz sprzęt użyty do ich nadzorowania są w stanie przeobrazić świat w „globalną wioskę", ale przy splocie szczególnych sytuacji możemy otrzymać mieszankę „spamu". Informatyzacja społeczeństwa zrodziła tzw. „efekt CNN", co oznacza, że ilość informacji oraz coraz krótsze cykle przekazywania wiadomości redukują czas przeznaczony na ich przetworzenie.

Już choćby z tego pobieżnego opisu wynika, że działalność uczestniczących w konflikcie stron, wymaga korzystania z wielu różnorodnych zasobów informacyjnych zdolnych do efektywnego ich pozyskiwania, przechowywania, przetwarzania i rozpowszechniania.

Wnioski z badań opinii ekspertów doprowadziły ostatecznie autora do przyjęcia na potrzeby pracy głównych założeń systemu jako odzwierciedlenia przedsięwzięć zawierających działalności rozpoznawczej w nowym wieku, co znalazło swoje odzwierciedlenie w pracy.

Rezultaty dalszych badań opinii ekspertów wykazały również, że przedstawiony projekt sił rozpoznawczych jest spójny i czytelny.

W takiej sytuacji, bazując na wynikach badań, autor przyjął w zaproponowanej koncepcji następujące założenia:

1. ***Dowódca kieruje rozpoznaniem*** - dowódca musi zdefiniować „Zasadnicze Potrzeby Informacyjne Dowódcy", cele wysokoopłacalne oraz terminy a także przewidzieć wysiłek systemu rozpoznania we wszystkich elementach ugrupowania bojowego (rzutach). Rozpoznanie musi ponadto poznać i zrozumieć system walki przeciwnika, jego możliwości, ograniczenia, zasady wykorzystania systemu ognia, manewru itp.
2. ***Synchronizacja rozpoznania*** - powoduje nowy sposób zarządzania cyklem rozpoznania. Sprowadza się ona do potrzeb dowódcy - co, gdzie i kiedy potrzebuje on wiedzieć, aby mógł zrealizować swoje zadanie (koncepcję). Dowódca i zwiadowcy muszą zrozumieć plan działań przełożonego a w nim widzieć kontekst przeprowadzenia operacji informacyjnych. Zwiadowcy muszą także przewidzieć kiedy dowódca będzie potrzebował specjalnych informacji do przeprowadzenia ataku na cele specjalne. Aby uzyskać sukces powinni także znać możliwości i ograniczenia sił i środków systemu rozpoznania, nadzorowania obszaru

działań i określania celów wysokoopłacalnych w zakresie realizacji priorytetowych potrzeb rozpoznawczych dowódcy. Jednocześnie należy zaznaczyć że, przy szybko zmieniających się wymaganiach współczesnego obszaru działań, *zwinność i ruchliwość* to klucz dla systemu rozpoznania aby mógł szybko dokonać przegrupowania sił i środków.

3. ***Modułowa baza operacyjna*** - jest trzecim elementem doktryny. W strukturze sił projektowanych działań, szybkość jest zasadą pozyskiwania efektów. Dowódca musi tak rozmieścić elementy rozpoznawcze aby pokryły główny ciężar działań - kierunek głównego wysiłku. Rozpoznanie powinno być elastyczne i gotowe do pozyskiwania danych źródłowych w realnym czasie po czym schronienia się w przygotowanym miejscu. Organizacja rozpoznania w działaniach (operacjach) powinna zabezpieczyć umiejętne skoncentrowanie sił a następnie ich rozproszenie.
4. ***Taktyczne ugrupowanie*** - jest rozwinięciem koncepcji działań (operacji) realizowanych na poziomie modułu (zespołu rozpoznawczego). Możliwości modułu powinny być zmienne w zależności od rozmiaru i składu, oraz czasu trwania działań bojowych. Podstawowym elementem, który wpływa na możliwości rozpoznawcze ugrupowania bojowego jest wg nazwy doktrynalnej Patrol Rozpoznawczy i często obejmuje on organiczne jak i nieorganiczne siły.
5. ***Przekazywanie danych rozpoznawczych*** to 5 kryterium, zawierająca w sobie dwa kluczowe działania:
   a. bezpośrednią transmisję nieobrobionych danych/informacji pozyskiwanych z wielu źródeł i czujników ograniczoną tylko do zasadniczych potrzeb dowódcy;
   b. łatwy dostęp do informacji rozpoznawczych i bazy danych wymaga wykwalifikowanego personelu, wyposażonego i wspartego systemami zapewniającymi automatyczną i bezpieczną komunikację.

Aby przedstawione kryteria mogły się urzeczywistnić, system musi posiadać następujące możliwości:

- prowadzenie w szerokich obszarach wielospektralnego nadzorowania obszaru działań (ląd, morze, powietrze, kosmos, cyberprzestrzeń);
- zespolenie w jeden system działań rozpoznawczych „od podstawy po szczyt" ugrupowania przeciwnika;
- wizualne zobrazowanie sytuacji na obszarze działań;
- określanie, lokalizację i identyfikację celów wysokoopłacalnych i wysokowartościowych;
- interoperacyjny dostęp do informacji w czasie prowadzenia operacji połączonych lub wielonarodowych;
- działania z zakresu walki w obszarze dowodzenia (C2W);
- prowadzenie działalności wspierającej siły zabezpieczające działania (operacje);
- udział w poszukiwaniu zaginionych itp.

S/6343
21,40