WALKA ELEKTRONICZNA W DZIAŁANIACH SIECIOCENTRYCZNYCH

Materiały z międzynarodowej konferencji naukowej

AKADEMIA OBRONY NARODOWEJ

WALKA ELEKTRONICZNA W DZIAŁANIACH SIECIOCENTRYCZNYCH

AKADEMIA OBRONY NARODOWEJ

WALKA ELEKTRONICZNA W DZIAŁANIACH SIECIOCENTRYCZNYCH

Materiały z międzynarodowej konferencji naukowej

WARSZAWA 2008

Recenzenci
prof. dr hab. Leopold CIBOROWSKI
dr hab. inż. Józef JANCZAK

Kierownik naukowy
płk dr hab. Marek WRZOSEK

Redakcja naukowa
ppłk dr inż. Waldemar SCHEFFS

Komitet naukowy
płk dr hab. Jarosław WOŁEJSZO
prof. dr hab. inż. Józef MICHNIAK
płk dr hab. inż. Marek WRZOSEK
płk dr hab. Henryk SPUSTEK
płk dr hab. Tomasz MAJEWSKI

Komitet organizacyjny
ppłk dr inż. Waldemar SCHEFFS
ppłk dr nawig. Grzegorz ROSŁAN
ppłk dypl. Piotr KALISZEWICZ

Projekt okładki
Genowefa MAJCHROWSKA

Skład i łamanie
Mirosława PRYMEK

Korekta
Jolanta PUCHALSKA

Opracowanie zawiera materiały wygłoszone podczas konferencji.
Forma przedstawienia materiałów odpowiada wersji przekazanej przez autorów.

ISBN 978-83-7523-055-0

Sygn. AON 5898/08

Skład, druk i oprawa: Wydawnictwo Akademii Obrony Narodowej
00-910 Warszawa, al. gen. A. Chruściela 103, tel. 681-40-55, tel./faks 681-37-52
Zam. nr 1385/2008

SPIS TREŚCI

We współczesnym świecie jedną z istotnych kwestii jest właściwe pojmowanie roli przekazu informacji. W dobie społeczeństwa informacyjnego szczególnego znaczenia nabierają więc sieci teleinformatyczne jako elektroniczna droga przekazu informacji. Nowoczesne społeczności oczekują szybkich, dobrych jakościowo, rzetelnych i obszernych informacji, których przekaz jest coraz bardziej istotny z punktu widzenia funkcjonowania państw i społeczeństw. Można pokusić się o stwierdzenie, iż dalszy rozwój cywilizacji jest dziś w znacznym stopniu uzależniony od elektronicznych form przekazu informacji. Zablokowanie przekazu lub jego zafałszowanie może prowadzić do wystąpienia różnych zagrożeń i perturbacji, na które narażone są przede wszystkim działania sieciocentryczne i rozwiązania na nich oparte – często będące newralgicznymi z punktu widzenia bezpieczeństwa państwa.

Problem ten jest dostrzegany przez instytucje państwowe, w tym Ministerstwo Spraw Wewnętrznych i Administracji, podmioty prywatne, struktury międzynarodowe, takie jak Unia Europejska czy NATO. W sposób naturalny największe potrzeby ochrony, a co za tym idzie – doświadczenie, posiadają podmioty wiodące dla poszczególnych sektorów bezpieczeństwa państwa. Warto tu wspomnieć o sektorach militarnym, finansowym, czy też bezpieczeństwa. Istotną rolę odgrywa również organ państwa realizujący zadania w ustawowo wyodrębnionym dziale administracji rządowej – informatyzacja poprzez działania strategiczne i koordynacyjne na poziomie kraju.

Wyzwania współczesności wymagają wzmożenia wysiłków nie tylko w zakresie identyfikowania zagrożeń dla sprawnych działań sieciocentrycznych, ale też skoordynowania wspólnych działań dotyczących zapobiegania oraz przeciwdziałania zagrożeniom.

Należy zatem uznać za cenne wszelkie kroki podejmowane w celu określenia aktualnych założeń działań sieciocentrycznych, modyfikacji systemu przeciwdziałania zagrożeniom oraz dyskusji nad działaniami systemowymi. Przejawem tych starań jest inicjatywa Wydziału Wojsk Lądowych dotycząca walki radioelektronicznej w działaniach sieciocentrycznych, której wyniki będą interdyscyplinarne i wartościowe dla wszystkich instytucji i podmiotów troszczących się o bezpieczeństwo obywateli i państwa.

Warszawa, 22 kwietnia 2008 roku

Witold Drożdż
MINISTERSTWO
SPRAW WEWNĘTRZNYCH i ADMINISTRACJI
PODSEKRETARZ STANU

Ppłk dr inż. Waldemar SCHEFFS
Sekretarz naukowy

WALKA ELEKTRONICZNA W DZIAŁANIACH SIECIOCENTRYCZNYCH

Konferencja naukowa w Zakładzie Rozpoznania i Walki Elektronicznej Instytutu Wojsk Lądowych

9 kwietnia 2008 r. w Instytucie Zarządzania i Dowodzenia[1] Akademii Obrony Narodowej odbyła się konferencja naukowa na temat: „Walka elektroniczna w działaniach sieciocentrycznych". Zamierzeniem organizatora konferencji była wymiana poglądów na temat określenia przydatności stosowanych obecnie procedur prognozowania zagrożeń w kontekście doświadczeń z przebiegu konfliktów zbrojnych oraz wykorzystania ich w wojskach lądowych. Obradom przewodniczyli prodziekan Wydziału Wojsk Lądowych[2] płk dr hab. Marek Wrzosek oraz kierownik Instytutu Zarządzania i Dowodzenia płk dr Jan Posobiec, obowiązki sekretarza naukowego pełnił ppłk dr inż. Waldemar Scheffs, a sekretarza organizacyjnego ppłk dr Grzegorz Rosłan.

W sympozjum uczestniczyli:

– przedstawiciele Zarządu Analiz Wywiadowczych i Rozpoznawczych – P2,
– przedstawiciele zarządów rozpoznania i walki elektronicznej wojsk lądowych i sił powietrznych,
– przedstawiciele attaché Francji, Węgier i Słowacji,
– przedstawiciel Ministerstwa Spraw Wewnętrznych i Administracji,
– przedstawiciele Wojskowych Zakładów Łączności nr 1 z Zegrza,
– prezes firmy Radiotechnika Marketing Sp. z o.o.,
– przedstawiciel Przemysłowego Instytutu Telekomunikacji SA,
– przedstawiciel Instytutu Techniki Wojsk Lotniczych,
– przedstawiciel Telekomunikacji Polskiej SA,
– dyrektor polskiego oddziału ACFCA,
– przedstawiciele z Akademii Obrony Narodowej, w tym Wydziału Wojsk Lądowych, Wydziału Wojsk Lotniczych i Obrony Powietrznej, Wydziału Strategiczno-Obronnego,
– dowódca 8. batalionu walki radioelektronicznej,
– szef zespołu analiz 2 Ośrodka Radioelektronicznego,

---

[1] Taka nazwa Instytutu obowiązywała do chwili reorganizacji AON i od 1 września nosi on nazwę Instytut Wojsk Lądowych.

[2] Podobnie jak Instytut Zarządzania i Dowodzenia, Wydział Wojsk Lądowych także został przekształcony w Wydział Zarządzania i Dowodzenia.

– studenci podyplomowych studiów obronno-strategicznych, podyplomowych studiów operacyjno-taktycznych i magisterskich studiów uzupełniających.

Dążenie do osiągnięcia zdolności sieciocentrycznych wymaga od wielu systemów sprawnego i skutecznego działania. Systemami będącymi podstawą działań wojsk w środowisku sieciocentrycznym są środki rozpoznania i łączności. Widzieć, wiedzieć i automatycznie przekazać informację o przeciwniku to połowa sukcesu. Jednak pozostały kwestie nadal otwarte, które są przedmiotem dalszych badań. Dotyczą one przydatności obecnie wykorzystywanych środków, procedur i metod działania we współczesnych konfliktach militarnych, przenoszonych w coraz większym zakresie do środowiska sieciocentrycznego.

Potrzeba wymiany opinii na temat problemów poruszanych podczas seminarium wynika z konieczności jednoznacznego postrzegania i rozumienia zagadnień związanych z wykorzystaniem środków i systemów walki elektronicznej w środowisku sieciocentrycznym.

Podjęty na seminarium temat jest szczególnie istotny, zwłaszcza teraz – w okresie gwałtownych zmian elektronicznych i informatycznych, jakie dokonują się w wielu dziedzinach życia, a tym bardziej w armiach świata. Informatyzacja życia wywiera coraz większy wpływ na człowieka. Ludzie uzależniają się od urządzeń – szczególnie elektronicznych. Proces ten daje się szeroko zaobserwować w środowisku zarówno cywilnym, jak i wojskowym. Wdrażanie nowych technologii elektronicznych do wojsk (ich wykorzystanie) powoduje jakościowo nowe spojrzenie na postrzeganie wielu nowych zjawisk, towarzyszących tak gwałtownemu rozwojowi. Modyfikacja sprzętu elektronicznego przeznaczonego do rozpoznania, przeciwdziałania czy obrony elektronicznej z jednoczesnym automatycznym przetwarzaniem i dystrybuowaniem informacji jest aktualnie standardem. Procesy te wywierają coraz większy wpływ na przebieg działań. Zachodzi więc konieczność usystematyzowania wielu zagadnień w tym istotnym obszarze działalności walki elektronicznej. Wiele kwestii, które już dawno powinny stać się przedmiotem badań, nadal pozostaje nierozwiązanych. Dotyczą one przydatności aktualnej teorii prowadzenia WE, obecnie wykorzystywanych systemów, sposobów wykorzystania sprzętu, analizy i przekazywania informacji. Aktualne i przyszłe pole walki jest tym stymulatorem poszukiwań nowych rozwiązań, który pozwala na opracowanie nowych metod prowadzenia walki elektronicznej w działaniach sieciocentrycznych.

Dążąc do możliwie szerokiego wyjaśnienia nieuregulowanych kwestii, organizatorzy zaprosili do udziału w dyskusji przedstawicieli Sztabu Generalnego WP, Dowództwa Wojsk Lądowych, Dowództwa Sił Powietrznych, jednostek rozpoznawczych, wybranych komórek organizacyjnych AON i oficerów zaprzyjaźnionych armii sojuszniczych a także instytucji oraz firm zainteresowanych omawianą problematyką.

Dyskusję utrzymano w nurcie rozważań nad następującymi kwestiami głównymi:

1. Aktualne założenia teoretyczne działań sieciocentrycznych:
   a) istota działań sieciocentrycznych,
   b) założenia walki elektronicznej w działaniach sieciocentrycznych,
   c) możliwości wykorzystania systemu walki elektronicznej w działaniach sieciocentrycznych,
   d) zarządzanie zasobami informacyjnymi w działaniach sieciocentrycznych.
2. Założenia modyfikacji sytemu walki elektronicznej w działaniach sieciocentrycznych.
3. Rozwiązania systemowe i sprzętowe.

Dla organizatorów konferencji zgromadzona w wyniku dyskusji wiedza będzie niezbędna przede wszystkim do właściwego przygotowania i realizacji procesu dydaktycznego. Rezultaty konferencji będą stanowić także podstawę do wyznaczenia kierunków modyfikacji obowiązujących procedur walki elektronicznej.

Zagadnienia i problemy poruszane przez referentów znalazły żywe odzwierciedlenie w dyskusji, w której głos zabrali: gen. bryg. w st. spocz. Witold Cieślewski, prof. dr hab. Józef Michniak (IZiD), dr hab. Tadeusz Bogusz (PIT), płk dr hab. Marek Wrzosek (prodziekan Wydziału Zarządzania i Dowodzenia), płk dr Jan Posobiec (dyrektor IWL), płk Christian Barthlen (attaché Francji), dr hab. Józef Janczak (AON).

Podsumowania dokonał kierownik naukowy płk dr hab. Marek Wrzosek, który stwierdził, że zarówno wystąpienia, jak i dyskusja mogą świadczyć o trafności oraz aktualności podjętej problematyki badawczej, a także o osiągnięciu celów, jaki wyznaczyli sobie organizatorzy konferencji.

Płk Christian BARTHLEN
Attaché Francji

UCYFROWIENIE POLA WALKI

Siły zbrojne Francji z początkiem XXI wieku rozpoczęły proces modernizacji swoich wojsk do standardów jednostek w pełni cyfrowych. Proces ten uwidocznił się głównie w wojskach lądowych. To wojska lądowe jako pierwsze stanowczo zaangażowały się w te działania, czego konkretnym wyrazem była decyzja szefa sztabu wojsk lądowych, rozkazująca ich przejście na cyfrowe urządzenia łączności, rozpoznania i kierowania do końca 2009 roku. Jednocześnie szef sztabu przewiduje, że uzbrojenie w pełni sterowane cyfrowo również będzie możliwe do przerzutu w roku 2009. Będą to wówczas ucyfrowionione siły, zdolne natychmiastowo podjąć walkę. Przewiduje się, że zostaną one utworzone z dwóch brygad ogólnowojskowych, wyspecjalizowanych brygad wsparcia (wojska inżynieryjne, artyleria, wywiad i lekkie lotnictwo wojsk lądowych) oraz dwóch brygad logistycznych. Pozostała część sił lądowych powinna osiągnąć zdolność do działań w środowisku sieciocentrycznym do roku 2015.

Po wydarzeniach z 11 września 2001 roku świat uległ zmianom, zmieniły się także warunki zaangażowania sił lądowych Francji. Przeszliśmy od sytuacji stosunkowo „komfortowej", kiedy to warunki zaangażowania były dobrze znane, a przeciwnik doskonale zidentyfikowany i na rozpoznanym terenie, do sytuacji, w której przeciwnik jest niekiedy bardzo trudny do zidentyfikowania wśród licznej populacji, w środowisku zurbanizowanym, gdzie indywidualne i zbiorowe akty przemocy mogą przybierać najróżniejsze formy.

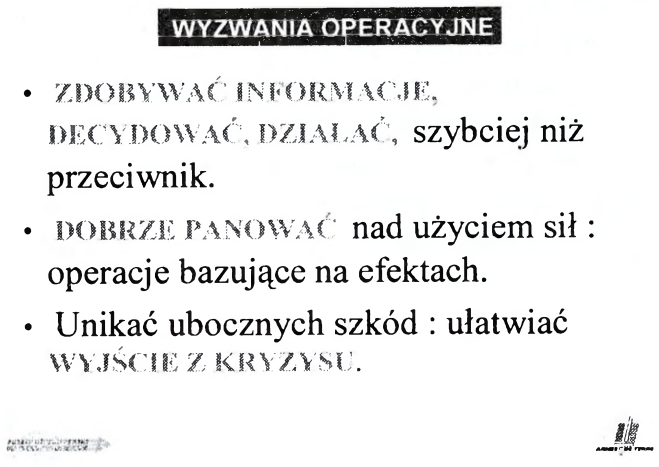
Imponujący rozwój nowych technologii informacji i komunikacji, którego przejawem jest m.in. Internet i postęp w nanotechnologiach, znalazł swoje odbicie także w obszarze wojskowym, gdzie systemy informacji i komunikacji uległy głębokim zmianom, wymuszając modyfikację naszego sposobu pracy. Ta rewolucja w dziedzinie informacji dała impuls, by przystąpić do realizacji ucyfrowienia sił lądowych. Z procesem tym wiąże się wielkie nadzieje, jeśli chodzi o płynność i precyzję wymienianych informacji. Przyspiesza on proces decyzyjny, a zyskany tym sposobem czas pozwala dowódcy poświęcić się jego zasadniczej funkcji, czyli dowodzeniu ludźmi. Zapewnia również większy komfort dowódcy, który może monitorować na swym ekranie sytuację wszystkich swoich podwładnych, sił sojuszników i sił przeciwnika oraz kluczowych elementów w danym środowisku, takich jak organizacje pozarządowe, szczególnie chronione obiekty infrastruktury itp.

Dowódca dysponuje ogółem potrzebnych mu informacji w wybranym przez siebie czasie i miejscu. Dzięki temu może opuścić główne stanowisko dowodzenia, by przenieść się tam, gdzie uzna swą obecność za konieczną. Zachowuje oczywi-

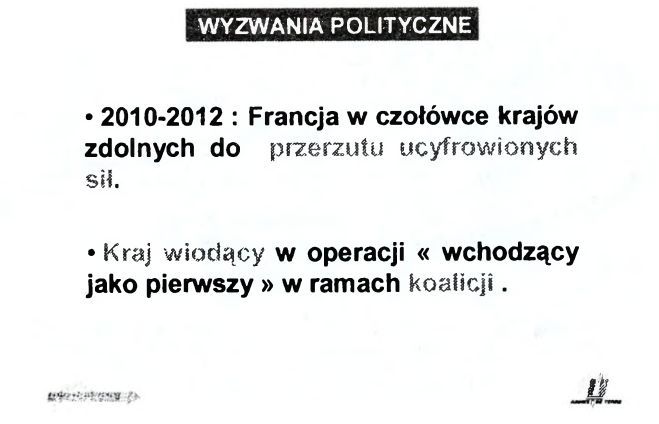
ście możliwość wydawania komend głosem: nic nigdy nie zastąpi głosu, a często i spojrzenia szefa, ale tu dochodzimy już do granic ucyfrowienia.

Główne wyzwania związane z ucyfrowieniem mają charakter polityczny, operacyjny i techniczny. Dzięki płynności i precyzji wymienianych informacji dowódca może podjąć decyzję szybciej niż przeciwnik i tym samym uzyskać nad nim przewagę. W stosownym czasie na jego monitorze wyświetlą się wszystkie potrzebne mu informacje i wiedza ta pozwoli mu zareagować szybko i dokładnie, tak jak wymaga tego sytuacja. To ścisłe dostosowanie natury i formatu środków do wyznaczonego celu przyczyni się do zoptymalizowania dostępnych zasobów, a także i do zmniejszenia ubocznych szkód. Tymczasem wiadomo, że od tego właśnie czynnika zależy powodzenie operacji mających na celu rozwiązanie kryzysu.

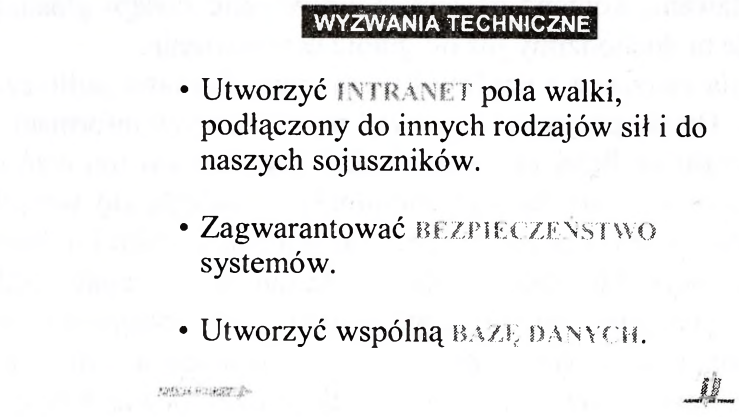
I wreszcie, ostatnie wyzwanie ma charakter techniczny. Wystarczy przenieść złożoność systemu Internetu, jakim codziennie się posługujemy, na Intranet pola walki, jaki właśnie tworzymy, by ocenić skalę tego zadania.



Rys. 1. Wymagania operacyjne dla ucyfrowionych sił zbrojnych Francji



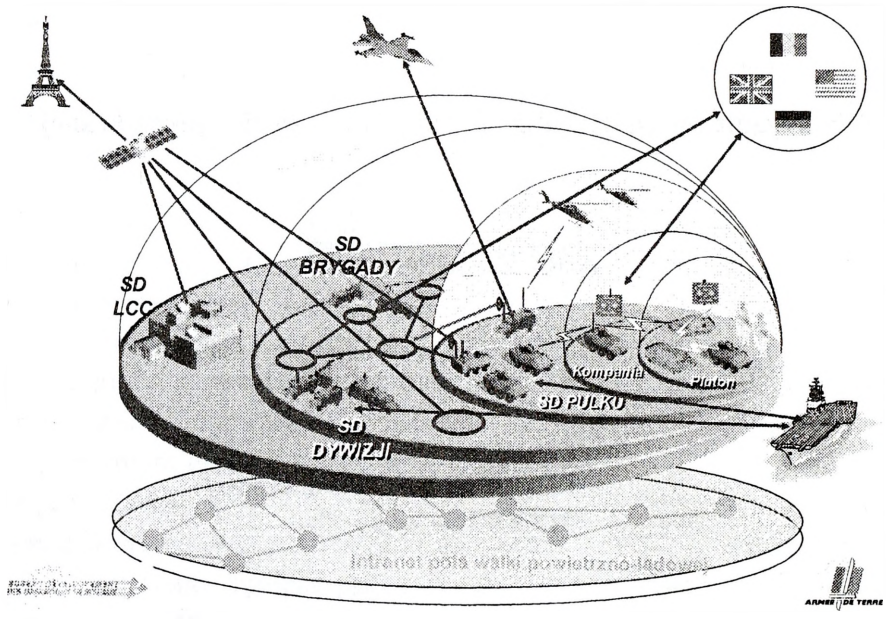
Rys. 2. Wymagania polityczne dla ucyfrowionych sił zbrojnych Francji



Rys. 3. Wymagania techniczne dla ucyfrowionych sił zbrojnych Francji

Siły lądowe Francji muszą być w stanie wymieniać wszystkie potrzebne informacje wewnątrz sił lądowych, z innymi rodzajami zaangażowanych sił i z sojusznikami, gwarantując bezpieczeństwo tej wymiany i integralność przekazywanych danych. Wymiana informacji musi być oczywiście zapewniona niezależnie od okoliczności, także w środowisku wrogim, w czasie konfliktu zbrojnego.

Wielka Brytania i Niemcy także rozpoczęły proces ucyfrowienia. Francja ze swej strony przewiduje, że w perspektywie lat 2010–2012 będzie w stanie pełnić rolę kraju wiodącego w ramach koalicji prowadzącej operację „wchodzący jako pierwszy".

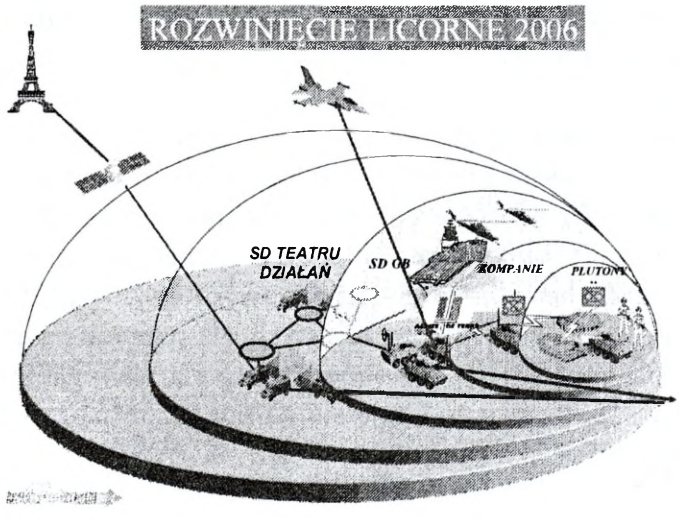


Rys. 4. Proces wdrażania systemów cyfrowych do wojsk lądowych

W górnej części rysunku 4 każda półkula odpowiada innemu szczeblowi dowodzenia. Siły zbrojne Francji przechodzą w ten sposób od plutonu, a nawet od pojedynczego żołnierza lub czołgu, do szczebla brygady i wyżej, a nawet do politycznych ośrodków decyzyjnych kraju. Cały system przejścia wojsk lądowych jest oczywiście podłączony do sieci wojsk lotniczych, marynarki oraz sił sojuszników Francji. Wszystkie te szczeble są między sobą połączone i mogą wymieniać się informacjami niezbędnymi do podjęcia decyzji i prowadzenia operacji. Jest to możliwe dzięki rozmieszczeniu w terenie całej sieci, której ogniwa są między sobą połączone, co przedstawiono w dolnej części rysunku 4. W chwili obecnej układ ten nie jest pełny, ale wojska lądowe Francji stopniowo, krok po kroku, uzupełniają go, na każdym z etapów sprawdzając doświadczalnie osiągnięcia. Takie działanie gwarantuje wojskom lądowym skuteczność przyjętego dla siebie wariantu i jego ogólną spójność w stosunku do:

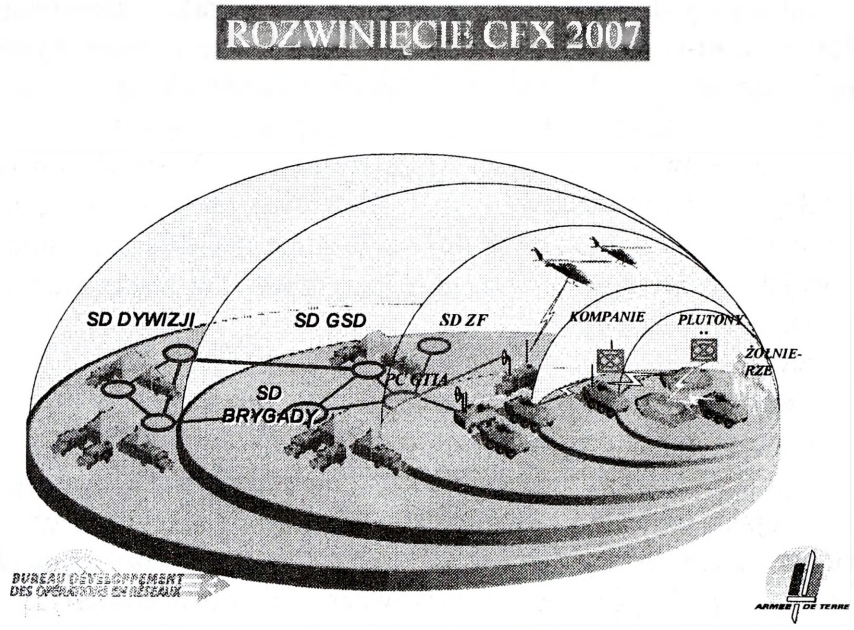
– dyspozycyjności sił,
– możliwości technicznych i finansowych,
– zdolności żołnierzy do nadążania za rozwojem systemów.

Działania wojsk lądowych Francji mają charakter jednocześnie operacyjny i taktyczny. Wojska lądowe Francji działania operacyjne rozpoczęły na dobre w 2004 roku wraz z eksperymentami w zakresie wymiany informacji na szczeblach plutonu, kompanii i pułku. Dostosowano wówczas cele doświadczeń operacyjnych do możliwości, jakie dawała ówczesna technika. Rok później postanowiono przetestować szczeble komplementarne do tych z roku 2004, koncentrując się na szczeblu brygady. Szczeble pułku i kompanii służyły tylko temu, by umożliwić funkcjonowanie wyższych szczebli. W roku 2006 po raz pierwszy eksperymentowano z całym ucyfrowionym systemem dowodzenia. Uwzględnione były wszystkie szczeble, nawet jeśli szczebel plutonu nie był w pełni wyposażony, jako że terminale są tam dopiero dostarczane.



Rys. 5. Utworzona architektura cyfrowego pola walki na dużych odległościach

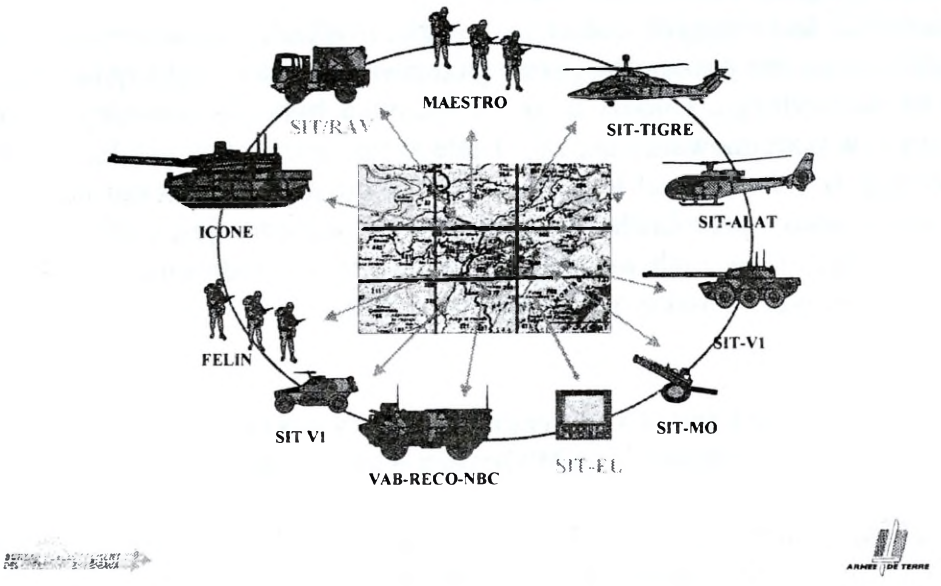
Prowadzono również doświadczenia z okrętem desantowym ORANE i z samolotem dozoru typu ATLANTIC 2. Na rysunku 6 doskonale widać rozwinięcie sił, jakie miało miejsce pod koniec ubiegłego roku (2007), kiedy to po raz pierwszy utworzono ucyfrowiony system/łańcuch dowodzenia między szczeblami 2 i 7.



Rys. 6. Kompletny obraz ucyfrowionego pola walki dla armii francuskiej

Działalność techniczna związana jest z poszczególnymi szczeblami dowodzenia, którym odpowiadają właściwe dla nich systemy informacji. Wynika to ze specyfiki każdego szczebla dowodzenia. Potrzeby w zakresie wymiany informacji dowódcy plutonu dysponującego terminalem SIT są całkiem inne, jeśli chodzi o ich charakter i objętość, od potrzeb pułkownika dowodzącego pułkiem przy użyciu systemu informacji pułkowej (SIR) lub od potrzeb generała, który posługuje się systemem informacji i dowodzenia sił (SICF).

System informacji pułkowej znajduje się w samym sercu systemu globalnego, jako że pułk jest właśnie takim sercem wojsk lądowych, zarówno w czasie pokoju, jak i w czasie operacji. Ta architektura opiera się na trzech systemach informacji w zależności od rozpatrywanego szczebla i na dwóch systemach komunikacji z wykorzystaniem, rzecz jasna, środków satelitarnych – ze względu na liczbę elementarnych systemów informacji przeznaczonych dla różnych czujników, dla różnych systemów uzbrojenia lub dla plutonów pełniących całą gamę funkcji operacyjnych, bez względu na to, czy znajdują się na pokładzie wozów bojowych, czy poruszają się pieszo.



Rys. 7. Łączenie systemów przekazu informacji

Na rysunku 7 pokazane są główne systemy, które trzeba włączyć do wojsk lądowych, które będą działały na rzecz technicznej interoperacyjności. Wiążą się z tym duże trudności, ponieważ wymogi systemu przeznaczonego na przykład dla śmigłowca TIGRE są bardzo różne od wymogów systemu dla żołnierza piechoty wyposażonego w FELIN lub dla logistyka, który musi zarządzać zaopatrzeniem.

Aby porzucić tę logikę programów, w 2005 roku rozpoczęto całościową operację SIC TERRE (system informacji i dowodzenia wojsk lądowych). W roku 2003 systemy wojsk lądowych Francji „rozmawiały" ze sobą tylko parami 2 : 2 – nie istniała między nimi żadna interoperacyjność. W chwili obecnej około dziesięciu systemów współpracuje ze sobą dzięki temu, że – mówiąc obrazowo – przerzucono między nimi wiele „kładek" do wymiany informacji. Natomiast celem jest zbudowanie wspólnej technicznej platformy, na której będą konstruowane wszystkie nowe systemy, które zostaną wprowadzone do wszystkich używanych obecnie systemów uzbrojenia.

W zadaniu postawionym przez szefa sztabu wojsk lądowych w 2005 roku czytamy:

- Ucyfrowić całe siły lądowe, które będą zdolne do przerzutu w dowolny rejon do roku 2015.
- Osiągnąć zdolność do przerzutu w 2009 roku, ucyfrowionych sił (ogólnowojskowa brygada) zdolnych natychmiastowo do walki. Siły utworzyć z dwóch brygad ogólnowojskowych wraz z ich wsparciem oraz jednym elementem logistycznym.

• Dostosować tempo procesu ucyfrowienia do możliwości szkolenia i uwzględnić ograniczenia techniczne oraz przemysłowe.

• Rozwinąć użycie narzędzi symulacji.

Zdolności technicznych żołnierzy na stanowiskach operacyjnych w żadnym wypadku nie można ograniczać, wręcz przeciwnie – należy człowieka włączyć do łańcucha decyzyjnego. Chodzi o to, by technika była dla dowódcy narzędziem pomocnym w podejmowaniu decyzji. Dlatego też dowódcy wojsk lądowych Francji uważają, iż szkolenie sił to jeden z kluczy do sukcesu procesu ucyfrowienia, który jest w toku i przeobraża wojska lądowe. Niezbędne jest dobre opanowanie użycia tych systemów i ich wdrożenie. Na nic zda się wydawanie milionów euro, jeśli nie będzie można maksymalnie ich wykorzystać.

Operacja wojsk lądowych Francji z wykorzystaniem ucyfrowionych jednostek na Wybrzeżu Kości Słoniowej

Możliwość rozważenia kilku hipotez zaangażowania sił wojskowych i szybkiego przygotowania odpowiednich rozkazów oraz ich natychmiastowe przekazanie bez uszczerbku na ich jakości z jednoczesnym ich zrozumieniem, połączone z ucyfrowieniem jednostek, pozwala znacznie zwiększyć szybkość reakcji i skuteczność sił. Ta zdolność zwiększa znaczenie elementów będących w odwodzie, gdyż sztab dysponuje potrzebnym czasem i środkami, by przygotować kilka możliwych hipotez ich zaangażowania. Pozwala na dostosowanie ich w ostatniej chwili i przejście natychmiast do działania. Nie można jednak zapominać, że istnieje ryzyko narzucenia jednostkom destabilizującego je rytmu poprzez zbyt szybkie zmiany gotowości.

Zdolność do geolokalizacji pozwala na lepsze zobrazowanie sił, a zatem i na lepszą ocenę wykonania misji, przez to samo oferuje większą zdolność do elastycznego działania z wyprzedzeniem. Ucyfrowienie pola walki (NEB) pozwala zmniejszyć odległości. Dla przykładu: ogólnowojskowa grupa bojowa (GTIA) 2 w Bouaké otrzymała zadanie kontroli strefy. Otrzymano FRAGO o godz. 15.00, a oddziały były na miejscu o 18.00. Użycie systemu informacji pułku (SIR) pozwoliło nie wzywać dowódców kompanii do stanowiska dowodzenia, lecz wysłać im bezpośrednio jasne rozkazy, pełne i od razu czytelne. Ucyfrowienie pola walki zwiększyło szybkość reakcji jednostki i pozwoliło jej w czasie akcji użyć środków w optymalny sposób.

SIOC przyczyniły się do tej zdolności przystosowawczej, odpowiadając na potrzeby SD ogólnowojskowych grup bojowych, a nawet pozwoliły, by bojowa podgrupa taktyczna podzieliła się na dwie części. Wystarczyło dorzucić jedno stanowisko pracy na przenośnym systemie informacji pułku. Te pozytywne stwierdzenia nie powinny nam przesłonić napotykanych trudności. Na przykład nieczytelny i ciężki IHM niemal uniemożliwiał szybkie zatwierdzanie rozkazów przez dowódcę. Poczta nie pozwala zameldować o takich sytuacjach, jak makabryczne odkrycia, kryjówki broni, różne wymuszenia. I wreszcie, wielki wysiłek wkłada się

obecnie w jakość kartograficznych narzędzi systemów. O ile interoperacyjność SIT-SIR (system informacji terminal – system informacji pułku) okazała się w pełni zadowalająca, to ograniczenia w wymianie informacji między SICF (system informacji i dowodzenia sił) a SIR niemal uniemożliwiły przepływ informacji z PCIAT (ogólnowojskowe stanowisko dowodzenia) do SIT ogólnowojskowej grupy bojowej.

Ppłk mgr Mariusz BLACH
Zarząd Analiz Wywiadowczych i Rozpoznawczych – P2

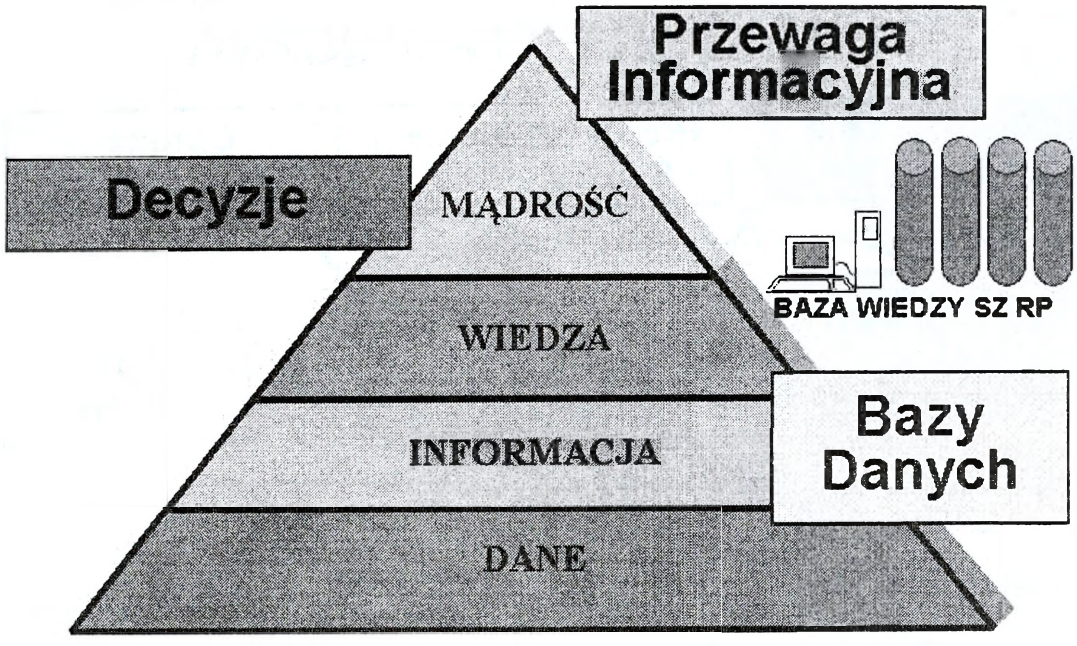
BAZY DANYCH ELEMENTEM SKUTECZNOŚCI ROZPOZNANIA ELEKTRONICZNEGO

Sukces w walce zbrojnej zdeterminowany jest potrzebą zdobycia przewagi nad przeciwnikiem. Sposobem realizacji tego celu jest dysponowanie informacjami wyprzedzającymi, dlatego też konieczność rozpoznania zamiarów przeciwnika jest tak stara, jak same działania wojenne. Można śmiało stwierdzić, że rozpoznanie zawsze warunkowało sukces na polu walki. Sprawne rozpoznanie jest niewątpliwie czynnikiem wzmacniającym potencjał wojsk oraz decydującym w dużej mierze o zwycięstwie na polu walki.

Do skutecznego prowadzenia rozpoznania konieczny jest szybki i niezawodny obieg kompleksowych informacji na wszystkich szczeblach dowodzenia. Umożliwia to generowanie wspólnego obrazu sytuacji operacyjnej oraz zapewnia przewagę informacyjną, a co za tym idzie – przewagę decyzyjną.

Aby działania wojsk były skuteczne, niezbędna jest pełna (w miarę możliwości) informacja o potencjalnym przeciwniku, zdobyta i potwierdzona przez różne źródła, skojarzona ze sobą i dystrybuowana do zainteresowanych w czasie zbliżonym do rzeczywistego. Należy tu zwrócić uwagę na fakt, że w języku potocznym pojęcia „informacji" i „danych" są często ze sobą utożsamiane i używane zamiennie, mimo że istnieje między nimi istotna różnica. Przede wszystkim informacja ze swej natury nie ma charakteru materialnego i nie jest rzeczą, lecz procesem zachodzącym pomiędzy umysłem człowieka i oddziałującym na niego środowiskiem zewnętrznym (bodźcami). Rolę owych bodźców mogą spełniać dane. Są one zapisem określonej informacji lub jej reprezentacją i przybierać mogą różną postać (np. literową, cyfrową, dźwiękową lub rysunkową). Dane są więc nośnikiem (medium) informacji. Informacją jest zaś to, co zdołamy z tego medium wywnioskować[3].

[3] Zobacz: *Recommendation of the Council of the OECD concerning Guidelines for Security of Information Systems*, OECD/GD (92), 10 Paris 1992. Aneks do *Wytycznych OECD w sprawie Bezpieczeństwa Systemów Informacyjnych* definiuje pojęcie danych i informacji w sposób następujący: „Dane" (data): przedstawienie faktów, pojęć lub poleceń w sposób sformalizowany i umożliwiający ich komunikowanie, interpretację lub przetwarzanie zarówno przez ludzi, jak i urządzenia (*automatic means*). „Informacja" (*information*): jest to znaczenie, jakie nadajemy danym za pomocą konwencji odnoszących się do tych danych (*is the meaning assigned to data by means of conventions applied to that data*).

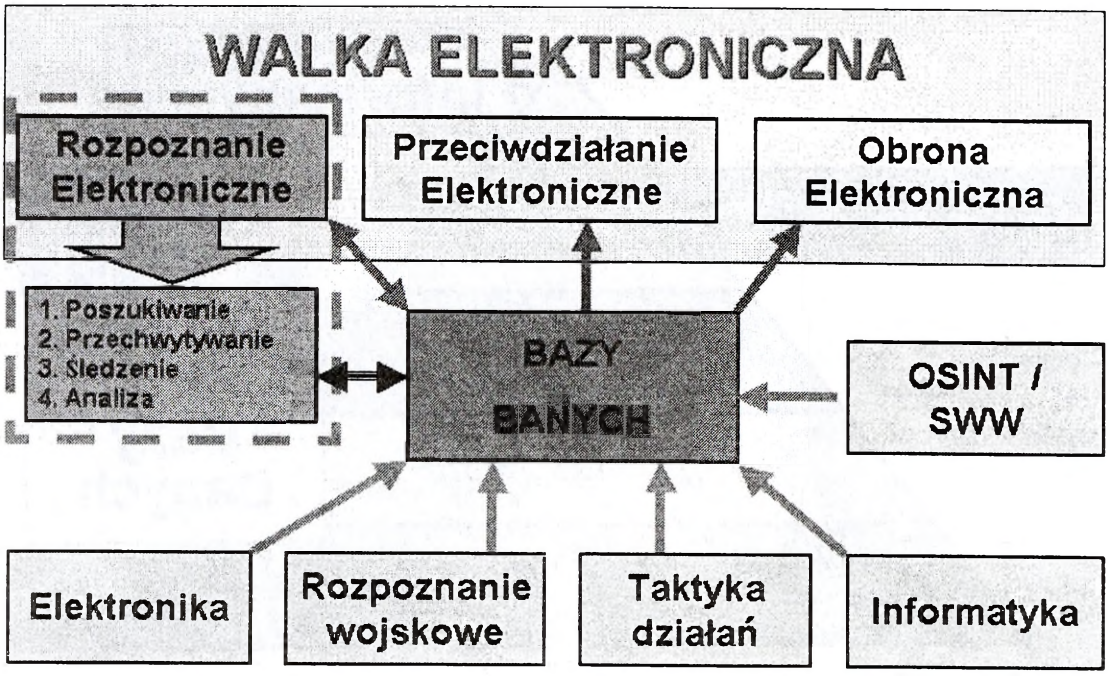


Rys. 1. Przewaga informacyjna a bazy danych

Posiadanie informacji ma kluczowe znaczenie w rozwiązywaniu problemów decyzyjnych, a w szczególności tych najbardziej złożonych. Informacja stanowi podstawę wiedzy, przy czym wiedzę rozumiemy jako ogół wiarygodnych informacji w rzeczywistości połączony z umiejętnościami ich wykorzystywania. To dzięki wiedzy jesteśmy skuteczni w działaniu, to wiedza usprawnia nasze myślenie i prowadzi do mądrości, a tym samym jest jednym z czynników umożliwiających osiągnięcie przewagi informacyjnej.

Realizacja tego zadania w Siłach Zbrojnych RP została już zapoczątkowana poprzez wdrażanie zautomatyzowanych systemów dowodzenia wykorzystujących bezpieczne sieci teleinformatyczne. Wszyscy bowiem mamy świadomość, że podstawę działań w środowisku sieciocentrycznym stanowi sprawna i niezawodna infrastruktura techniczna. Infrastruktura techniczna jest ważna, jednak zasadniczym elementem skuteczności działań jest aktualna i wiarygodna informacja, usystematyzowana w bazach danych.

Gromadzenie zbiorów danych, ich odpowiednie uporządkowanie i opracowanie jest procesem złożonym i czasochłonnym. Podstawowymi sposobami zdobywania danych z rozpoznania elektronicznego są: poszukiwanie, przechwytywanie, śledzenie oraz namierzanie. Proces ten opiera się na analizie, selekcji i redukcji informacji otrzymywanych z wielu innych, różnych dziedzin, np. rozpoznania wojskowego, taktyki ogólnowojskowej, informatyki i elektroniki.



Rys. 2. Źródła zasilania baz danych WE

Gromadzone i przetwarzane dane dotyczą nie tylko sił i środków bojowych przeciwnika, ale także danych o gospodarce, technice, nauce i polityce. W ten sposób gromadzone są dane mające wpływ na funkcjonowanie gospodarki kraju potencjalnego przeciwnika. Działanie takie pozwala na analizę możliwości użycia sił i środków militarnych oraz pozamilitarnych potencjalnego przeciwnika. Zgromadzone informacje pozwalają na zidentyfikowanie symptomów podnoszenia stanów gotowości bojowej, mobilizacji sił zbrojnych oraz gospodarki narodowej. Ograniczają one zaskoczenie systemu obronnego państwa w początkowym okresie konfliktu zbrojnego, a tym samym stają się jednym z pierwszych elementów wywalczenia przewagi informacyjnej na polu walki.

Współczesne założenia doktrynalne Rzeczypospolitej Polskiej oraz Sojuszu Północnoatlantyckiego wskazują na potrzebę utworzenia jednolitego systemu baz danych. Już od wielu lat priorytetem w tej dziedzinie są bazy danych źródeł promieniowania radiolokacyjnego. Zapotrzebowanie na informacje dotyczące danych radiolokatorów uwidoczniło się podczas udziału w misjach pokojowych, akcjach stabilizacyjnych i konfliktach lokalnych na całym świecie. Dane takie stanowią przede wszystkim element baz danych systemów obrony indywidualnej statków powietrznych (zarówno radiolokacyjnych, optycznych, jak i termicznych). Bazy takie wykorzystywane są także w systemach obrony okrętów (np. przeciwrakietowych). Dotyczy to także systemów obrony środków pancernych, a w przyszłości wykorzystywane będą również w bojowych wozach piechoty. Bazy takie stanowią również element systemu identyfikacji wojsk własnych zapobiegający uderzeniom

ogniowym na elementy własnego lub sojuszniczego ugrupowania (uzbrojenia)[4] poprzez udostępnienie informacji o emiterach używanych przez wojska własne. Aby działania takie (identyfikacja) były możliwe, należy wcześniej dysponować interoperacyjnymi bazami danych środków elektronicznych zarówno przeciwnika, jak i własnych (sojuszniczych) oraz właściwe je wykorzystywać. Dlatego tak ważne jest ich wcześniejsze przygotowanie i udostępnienie wszystkim tym, którzy powinni je otrzymać. Jest to problem tworzenia mapy sytuacji elektronicznej (EOB[5]) na podstawie danych dostarczanych przez bazy danych emisji elektromagnetycznych. Obecnie w NATO nie zdefiniowano ostatecznego formatu EOB, co powoduje utrudnienia w jej wykorzystaniu. Prace nad powyższym formatem są prowadzone w Grupie Roboczej ds. Rozpoznania i Wywiadu Elektronicznego – SEWWG[6].

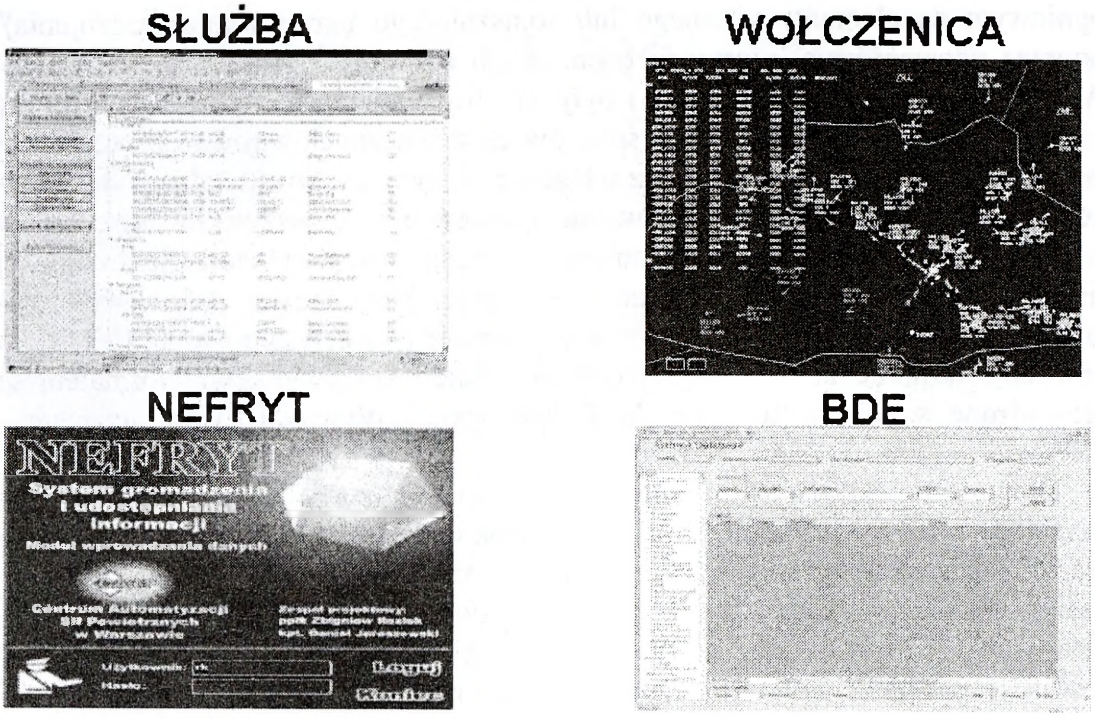
Dokument doktrynalny „Walka elektroniczna" (Sztab Gen. 1549/2003) obowiązujący w SZ RP już od 2003 roku podkreśla wagę systemu wymiany informacji oraz baz danych o obiektach elektronicznych. Podkreśla się w nim, że system wymiany informacji i danych o obiektach elektronicznych powinien zapewnić swobodny ich przepływ w relacjach: urządzenie rozpoznawcze – baza danych – użytkownik, a podstawę systemu stanowi odpowiednio skonfigurowana baza, umożliwiająca archiwizację informacji operacyjnych oraz parametrów technicznych obiektów elektronicznych, służących do prowadzenia analizy operacyjno-technicznej i określenia parametrów dla systemów przeciwdziałania i obrony elektronicznej, a także rażenia środkami ogniowymi.

W Siłach Zbrojnych RP system rozpoznania elektronicznego jest bardzo istotnym elementem zintegrowanego systemu rozpoznania wojskowego. Organizatorem tego systemu jest Zarząd Analiz Wywiadowczych i Rozpoznawczych P-2. W chwili obecnej wdrażane są (w różnym stopniu zaawansowania) cztery główne systemy wspomagające działanie rozpoznania elektronicznego. Są to:

1. Zautomatyzowany system wymiany informacji rozpoznawczych pracujący na rzecz Zintegrowanego Systemu Rozpoznania Sił Zbrojnych RP „SŁUŻBA";
2. System gromadzenia, archiwizowania i przetwarzania informacji „NEFRYT";
3. Zautomatyzowany system dowodzenia i kierowania rozpoznaniem elektronicznym „WOŁCZENICA";
4. System bazy danych źródeł promieniowania radiolokacyjnego „BDE" (Baza Danych Emiterów).

---

[4] Friendly Fire.
[5] Electronic Order of Battle.
[6] SIGINT/Electronic Warfare Working Group.



Rys. 3. Systemy wspomagające rozpoznanie elektroniczne

Do głównych zadań systemu „SŁUŻBA" należy:

- przyspieszenie procesu zbierania, przetwarzania (opracowywania) i przekazywania (obiegu) bieżących informacji wewnątrz zintegrowanego systemu rozpoznania oraz przesyłania do odbiorców zewnętrznych dokumentów informacyjnych i sprawozdawczych;
- utrzymywanie funkcjonowania centralnej bazy danych rozpoznawczych i zapewnienie dostępu do niej uprawnionym użytkownikom;
- usprawnienie archiwizacji oraz procesu wyszukiwania informacji według różnorodnych układów tematycznych, czasowych itp.;
- dostarczanie informacji rozpoznawczych do pozostałych zautomatyzowanych systemów dowodzenia.

System informatyczny „NEFRYT" ma za zadanie zautomatyzowanie procesu zbierania, archiwizowania i przetwarzania informacji o strukturze, bazowaniu, uzbrojeniu, składach osobowych, ćwiczeniach i szkoleniach sił zbrojnych państw leżących w operacyjnych obszarach zainteresowania (OOZ) i poza nimi. Oprogramowanie opracowane jest w oparciu o standardy zawarte w dokumentach AIntP-3 i ADatP-3, określające zasady przygotowania i zarządzania bazami danych w NATO. Powyższy system będzie wykorzystywał infrastrukturę SI „SŁUŻBA" (opcjonalnie SEC WAN).

Wdrożenie zautomatyzowanego systemu dowodzenia i kierowania rozpoznaniem elektronicznym „WOŁCZENICA" umożliwi:

- uzyskanie interoperacyjności z systemami rozpoznania i walki elektronicznej NATO poprzez wykorzystanie tych samych standardów transmisji danych;
- zautomatyzowane dowodzenie pododdziałami rozpoznania elektronicznego;
- dostarczenie danych z rozpoznania elektronicznego do systemu „DUNAJ" w celu utworzenia zintegrowanego rozpoznawczego obrazu sytuacji powietrznej (RAP)[7];
- kierowanie środkami rozpoznania pracującymi w ramach Zintegrowanego Systemu Rozpoznania SZ RP.

Następnym omawianym systemem jest system baz danych źródeł promieniowania radiolokacyjnego, nazywany też systemem baz danych emiterów (przy założeniu, że mówimy o emiterach niekomunikacyjnych). Potrzeba utworzenia systemu bazy danych źródeł promieniowania radiolokacyjnego wynikła z konieczności wdrożenia w Siłach Zbrojnych RP postanowień doktryny „Walka elektroniczna" (Sztab Gen. 1549/2003) gwarantujących bezzakłóceniową (bezpieczną) pracę systemów dowodzenia, walki elektronicznej, nawigacji i kierowania środkami rażenia, opartych na środkach radiolokacyjnych, w układzie narodowym, sojuszniczym i koalicyjnym.

Głównym celem utworzenia w resorcie obrony narodowej systemu bazy danych o źródłach promieniowania radiolokacyjnego jest uzyskanie zdolności do jednoznacznej identyfikacji przechwytywanych sygnałów radiolokacyjnych oraz powiązanie ich z systemami bojowymi lub platformami przenoszącymi środki radiolokacyjne. Jest to jeden z priorytetów walki elektronicznej. Celami pośrednimi uzyskanymi w związku z realizacją celu głównego są:

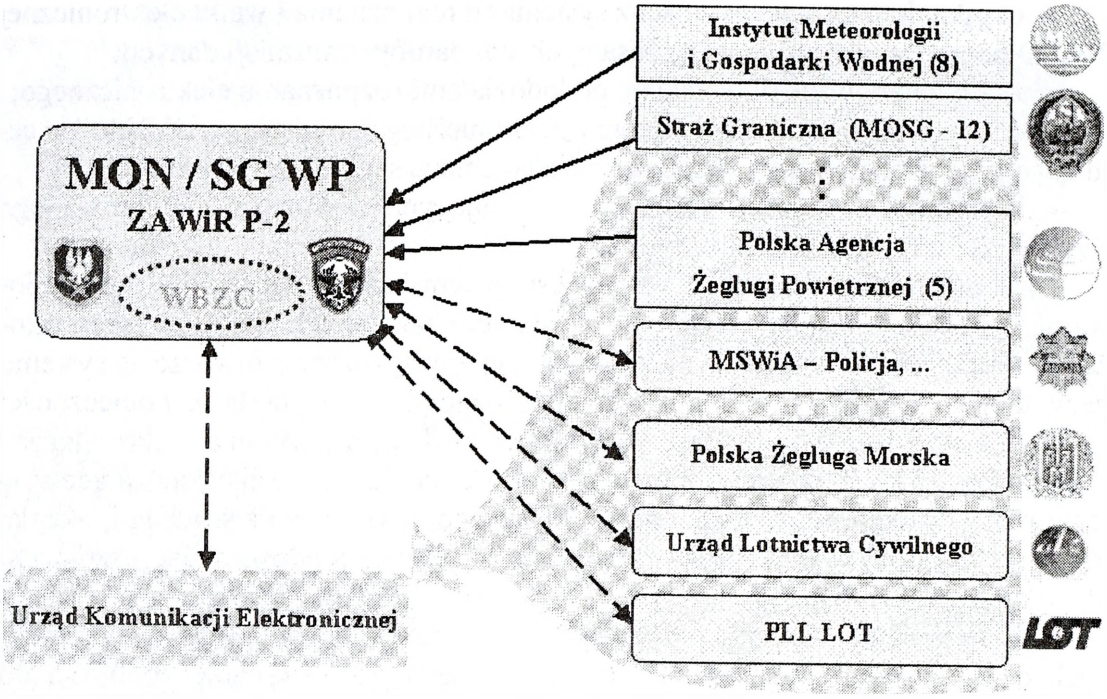
1. Utworzenie narodowej bazy danych źródeł promieniowania radiolokacyjnego wykorzystywanej w systemach obrony indywidualnej statków powietrznych i okrętów bojowych RP;
2. Posiadanie bazy danych obiektów elektronicznych potrzebnych do zapewnienia kompatybilności elektromagnetycznej w obszarze zainteresowania oraz wykorzystywanych do tworzenia mapy obiektów radiolokacyjnych (EOB);
3. Posiadanie kompatybilnej z państwami Sojuszu Północnoatlantyckiego bazy danych źródeł promieniowania radiolokacyjnego wykorzystywanej podczas pokoju, kryzysu i wojny;
4. Ujednolicenie formatów baz danych wykorzystywanych w urządzeniach rozpoznania elektronicznego.

Prawidłowe rozpoznanie emisji fal elektromagnetycznych może być jedynym sposobem rozpoznania celu, którego nie widać. Zapewnia ono dostarczenie systemowi dowodzenia istotnych informacji o przeciwniku, takich jak precyzyjne namiary oraz dane o jego możliwościach bojowych.

Tworzenie narodowej bazy danych o emiterach wymaga współpracy z innymi instytucjami spoza resortu obrony narodowej. W bazie danych powinny być gromadzone szczegółowe parametry sprzętu elektronicznego państw leżących w obszarach operacyjnego zainteresowania SZ RP oraz własnych urządzeń wojskowych i cywilnych.

---

[7] Recognised Air Picture.



Rys. 4. Wybrane instytucje spoza resortu ON wspomagające BDE

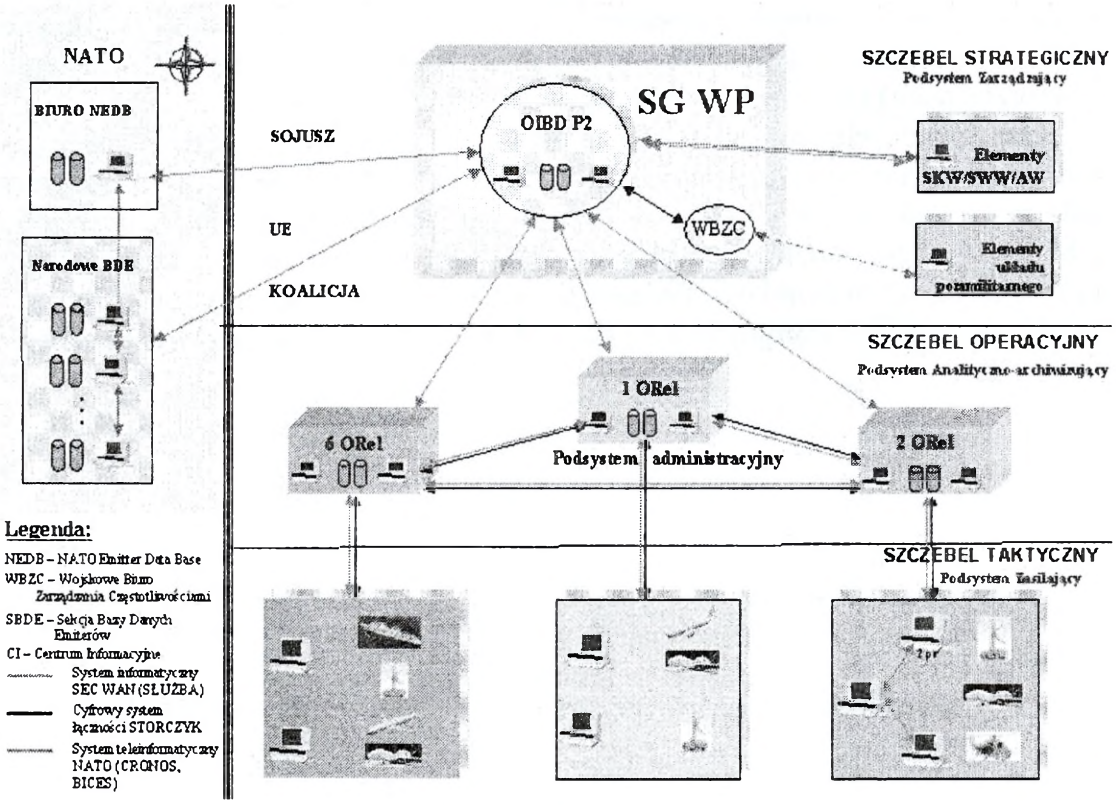
Realizacja tego zadania wymaga ścisłego współdziałania z Wojskowym Biurem Zarządzania Częstotliwościami, które na podstawie osobnych porozumień będzie przekazywało dane o urządzeniach radiolokacyjnych wykorzystywanych przez jednostki Ministerstwa Spraw Wewnętrznych i Administracji (Straży Granicznej, Policji), Agencji Ruchu Lotniczego, Polskiej Żeglugi Morskiej, Urzędu Lotnictwa Cywilnego oraz Instytutu Meteorologii i Gospodarki Wodnej.

Format gromadzonych danych został ściśle określony w Normie Obronnej „Baza danych źródeł promieniowania radiolokacyjnego. Wymagania" (NO-02A058) zatwierdzonej przez ministra obrony narodowej do stosowania w komórkach organizacyjnych MON oraz jednostkach organizacyjnych jemu podległych. W ten sposób wszystkie nowe urządzenia i systemy walki elektronicznej wprowadzane na wyposażenie SZ RP mają ściśle określone wymagania techniczne, dotyczące formatu danych wejściowych i wyjściowych.

Problematyką baz danych źródeł promieniowania radiolokacyjnego zajmuje się Oddział Rozpoznania Obrazowego i Baz Danych Zarządu Analiz Wywiadowczych i Rozpoznawczych P2, współpracując z przedstawicielami zarządów rozpoznania i walki elektronicznej rodzajów sił zbrojnych oraz innymi instytucjami MON. Jest to konsekwencją decyzji ministra obrony narodowej nr 210/MON z 18 maja 2007 r. (DzU MON nr 9 z 2007 r.) w sprawie powołania zespołu do przygotowania i wdrożenia w resorcie obrony narodowej systemu baz danych źródeł promieniowania radiolokacyjnego.

Opracowany i zatwierdzony przez szefa Sztabu Generalnego WP harmonogram wdrażania systemu w SZ RP zakłada zakończenie wdrażania głównych elementów systemu w 2009 roku. Termin ten jest w dużej mierze uzależniony od daty wdrożenia do eksploatacji w SZ RP systemu SEC-WAN, a także terminu podpisania dodatkowych porozumień z instytucjami spoza resortu ON.

Osobnym zagadnieniem jest zapewnienie wsparcia naukowego dla systemu, czyli powstanie specjalistycznego laboratorium, którego głównymi zadaniami będzie dokonywanie szczegółowej analizy przechwyconych sygnałów radiolokacyjnych, przekształcanie ich do formatu wykorzystywanego przez urządzenia ostrzegające przed opromieniowaniem radiolokacyjnym i opracowanie taktyki działań dla platform opromieniowanych sygnałem radiolokacyjnym.



Rys. 5. System baz danych źródeł promieniowania radiolokacyjnego. Model 2008

Już dzisiaj SZ RP dysponują szeroką gamą urządzeń dokonujących akwizycji sygnałów radiolokacyjnych. Są to m.in. stacje rozpoznania sygnałów radiolokacyjnych: Breń, Gunica, Procjon, NELS, MSR-W, Lena MD, RUO-10. Jednocześnie na ukończeniu są prace mające na celu pozyskanie mobilnej stacji rozpoznania i analizy sygnałów radiolokacyjnych.

Mobilny zestaw rejestracji i analizy sygnałów radiolokacyjnych (MZRiASR) będzie przeznaczony do prowadzenia rozpoznania sygnałów radiolokacyjnych,

analizy i syntezy danych rozpoznania sygnałów radiolokacyjnych generowanych przez urządzenia montowane na platformach naziemnych, morskich i powietrznych. Zadaniem tego zestawu będzie prowadzenie rozpoznania radioelektronicznego oraz monitorowanie sytuacji w pobliżu granic RP, rejonów ćwiczeń oraz w rejonach wykonywania misji polskich kontyngentów wojskowych w ramach operacji NATO i UE. Zestawy będą stanowiły wyposażenie komórek baz danych emiterów.

Podsumowanie

Jak dowodzą doświadczenia ostatnich lat, walka elektroniczna stała się niezbędnym i bardzo ważnym elementem wszelkich działań wojsk zarówno w czasie pokoju, wojny, jak i w sytuacjach kryzysowych. Widmo elektromagnetyczne (obok cyberprzestrzeni) jest kolejnym wymiarem współczesnego pola walki.

Rozpoznanie elektroniczne jako integralny element walki elektronicznej dostarcza siłom zbrojnym danych potrzebnych do uzyskania przewagi informacyjnej nad przeciwnikiem. Wszystkie te informacje są systematycznie gromadzone w bazach danych umożliwiających efektywne ich wykorzystanie przez wszystkich uprawnionych użytkowników. Zadania te realizowane są przez System Rozpoznania Wojskowego Sił Zbrojnych RP i są zgodne z wymaganiami sieciocentrycznego pola walki.

Ppłk dr inż. Piotr DELA
Zakład Systemów Teleinformatycznych
Instytutu Wojsk Lądowych Wydziału Zarządzania i Dowodzenia AON

SIECI INFORMATYCZNE W SYSTEMIE WALKI ELEKTRONICZNEJ

Wstęp

W niniejszym referacie przedstawiona została koncepcja wykorzystania sieci informatycznych na potrzeby systemu walki elektronicznej. Zawarte w referacie propozycje rozwiązań oparte zostały na kilkuletnich badaniach i doświadczeniach autora związanych z organizacją i eksploatacją mobilnych sieci informatycznych. Przedstawione rozwiązania uwzględniają szereg różnorodnych czynników wpływających na funkcjonowanie systemu walki elektronicznej, takich jak m.in.: bezpieczeństwo systemu (odporność na wykrycie i zakłócenia), szerokość dostępnego pasma, niezawodność, wymagania operacyjno-techniczne, dostęp do informacji. Celowo pominięto szczegóły techniczne proponowanych rozwiązań, skupiając się na idei wykorzystania sieci informatycznych.

Opisując charakterystykę sieci informatycznych (komputerowych), należy w pierwszej kolejności określić ich przeznaczenie. Otóż sieci te są rozwijane w celu zapewnienia wymiany informacji zarówno w ramach sieci lokalnej stanowiska dowodzenia. Może to być także sieć lokalna, np. na pojazdach, wozach, aparatowniach itp. (LAN – *Local Area Network*), jak i pomiędzy sieciami rozwiniętymi na innych stanowiskach dowodzenia (innych pojazdach, wozach, aparatowniach) poprzez sieci rozległe (WAN – *Wide Area Network*), do których podłączony jest dany element.

Sieci informatyczne powinny być wyposażane w następujące elementy:
- systemy przetwarzania,
- systemy przechowywania,
- systemy transmisji danych,
- układy połączeń kablowych i bezprzewodowych.

Systemy przetwarzania to m.in. zautomatyzowane systemy dowodzenia (kierowania, sterowania), których głównym zadaniem jest wspomaganie pracy operatorów w przetwarzaniu posiadanej informacji.

Systemy przechowywania to dedykowane serwery zdolne do przechowywania informacji opracowywanej na stanowisku dowodzenia (w zespole). Serwery te muszą się charakteryzować dużą niezawodnością i zapewniać ciągłą dostępność danych dla określonych operatorów. Z tego też względu niezbędne jest przechowywanie tej samej informacji w różnych miejscach.

Systemy transmisji danych i układy połączeń kablowych i bezprzewodowych to nic innego jak fizyczna realizacja sieci informatycznej. W skład każdej sieci, oprócz odpowiednich połączeń, wchodzą urządzenia aktywne (switche, routery, huby), zdolne do transmisji danych na ustalonych przez administratora sieci zasadach.

Istotnym wymaganiem stawianym sieciom informatycznym rozwijanym w warunkach polowych jest niski poziom emisji ujawniającej oraz jej odporność na zagrożenia elektromagnetyczne. Wymagania te zawarte są odpowiednio w normach NO-06-A200, NO-06-A500, (MIL Std 461D), MIL Std 188-125-2.

Sieci informatyczne mogą być budowane z wykorzystaniem wielu różnorodnych rozwiązań, tworzących spójny i kompletny system teleinformatyczny wspomagający pracę operatorów. Poszczególne elementy sieci mogą być wykorzystywane osobno, w zależności od zaistniałej sytuacji.

Sprzęt stosowany do tworzenia sieci informatycznych musi również spełniać surowe wymogi eksploatacyjne, co zagwarantuje jego niezawodną pracę przez wiele lat. Szybki rozwój nowoczesnych technologii w dziedzinie łączności i informatyki spowodował, że projektowanie systemów i urządzeń teleinformatycznych specjalnie dla wojska przestało być opłacalne[8]. Do tworzenia tych systemów przyjęto podejście zwane jako COTS (*commercial of the shelves*), czyli wykorzystanie urządzeń komercyjnych w wojsku. Z uwagi na to, że nie wszystkie urządzenia mogły być zastosowane bezpośrednio, upowszechniła się technologia „utwardzany COTS" (*hardened COTS*). Rozróżniane są trzy podstawowe poziomy utwardzania, a mianowicie V1, V2 i V3[9]. Poziom V1 to najniższy poziom utwardzenia, odpowiadający urządzeniom do zastosowań biurowo-przemysłowych. Poziom V2 dotyczy urządzeń wykorzystywanych na polowych stanowiskach dowodzenia i do zastosowań w pojazdach. Poziom V3 jest wykorzystywany do tworzenia systemów z pełną odpornością na wszelkiego rodzaju zagrożenia.

Technologia COTS pozwoliła na szybkie zastosowanie w urządzeniach wojskowych najnowszych technologii informatycznych. Dodatkową zaletą podejścia COTS jest możliwość uzyskania niższych kosztów wdrożenia wyrobów dla wojska ze względu na standaryzację wykorzystywanych technologii informatycznych.

Wymagania stawiane przed sieciami (systemami) informatycznymi

Przeprowadzone analizy pozwalają na stwierdzenie, że rejon, w którym prowadzone są działania związane z walką elektroniczną, wpływa bezpośrednio na funkcjonowanie i możliwości sieci informatycznych. Do czynników mających tu wpływ należy zaliczyć:

---

[8] Takie podejście wymusił szybki rozwój szeroko rozumianej teleinformatyki.

[9] M. Dras, *Systemy sprzętowe do budowy polowych sieci teleinformatycznych na stanowiskach dowodzenia*, materiały z sympozjum nt. „Sieci teleinformatyczne stanowisk dowodzenia wojsk lądowych szczebla taktycznego", AON, Warszawa 2005, s. 36.

– wielkość rejonu (obszaru),
– charakter rejonu (gęstość zabudowy),
– istniejącą infrastrukturę techniczną rejonu (w tym infrastrukturę teleinformatyczną).

Wielkość i charakter obszaru działań (obszaru kryzysu) determinuje m.in. warunki propagacji fal radiowych i w istotny sposób ogranicza zasięg fal radiowych. Obszary o gęstej zabudowie (gęsto zaludnione i o dużym stopniu uprzemysłowienia) charakteryzują się dużymi zakłóceniami elektromagnetycznymi[10].

Analizy wykazały, że istotnymi czynnikami, mającymi wpływ na sieci informatyczne, są także warunki klimatyczne, meteorologiczne i propagacyjne. Do ważnych czynników z tego zakresu należy zaliczyć odpowiednio:
– długość dnia i nocy,
– prognozę pogody oraz jej wpływ na istniejącą infrastrukturę (temperaturę, opady atmosferyczne, wilgotność powietrza),
– stan atmosfery, troposfery (zjawisko rozproszenia w troposferze fal UKF)[11] i jonosfery (propagację odbicia od warstw jonosfery)[12].

Wymienione czynniki mogą w istotnym stopniu zmniejszyć lub zwiększyć możliwości eksploatacyjne systemów informatycznych, a także wywierać pośredni wpływ na personel obsługujący te systemy.

W procesie kierowania walką elektroniczną posiadane (wykorzystywane) systemy informatyczne muszą zapewnić sprawne funkcjonowanie stworzonego systemu dowodzenia. Systemy te muszą umożliwić zachowanie istotnych właściwości stworzonego systemu kierowania, takich jak: jedność kierowania (*unity of command*), ciągłość kierowania (*continuity of command*), przejrzysta struktura systemu kierowania (*clear chain of command*), integracja kierowania (*integration of command*) oraz decentralizacja kierowania (*decentralization of command*).

Z analizy literatury wynika, że wymagania stawiane przed systemami (sieciami) informatycznymi można podzielić na dwie podstawowe grupy: wymagania operacyjne i wymagania techniczno-eksploatacyjne.

Wymagania operacyjne

Wymagania operacyjne wynikają w głównej mierze z faktu, że wykorzystywane systemy informatyczne są systemami złożonymi i działają w ramach funkcjonowania innych systemów informatycznych, zarówno podrzędnych, równorzędnych, jak i nadrzędnych. Wykorzystywane systemy powinny być ze sobą w pełni kompatybilne (mieć możliwość wymiany pomiędzy sobą informacji). Z tego względu można wyróżnić trzy podstawowe wymagania operacyjne, a mianowicie: terminowość, wierność i skrytość. Wynikają one przede wszystkim z zadań stawia-

[10] P. Daniluk, *Radiowa służba stała i ruchoma*, AON, Warszawa 2004, s. 35.
[11] Tamże, s. 148–153.
[12] Tamże.

nych przed stworzonym systemem kierowania walką elektroniczną i decydują o ich skuteczności operacyjnej[13].

Terminowość stanowi zdolność systemów informatycznych do przekazywania informacji (danych) w określonym czasie. Jest ona określana jako prawdopodobieństwo przesyłania informacji w czasie, który nie przekracza dopuszczalnych wartości dla ustalonych priorytetów przesyłanych informacji przy uwzględnieniu obciążenia systemów informatycznych. Z badań wynika, że systemy informatyczne powinny zapewnić dostęp do niezbędnych usług i informacji w czasie rzeczywistym lub zbliżonym do rzeczywistego (bazy danych, GIS, VoIP, SMTP, POP3)[14].

Wierność to zdolność systemów informatycznych do odtworzenia w urządzeniach (systemach) odbiorczych nadanych informacji z zadaną dokładnością, przy uwzględnieniu istniejących zakłóceń i zniekształceń. W nowoczesnych systemach cyfrowych miarą jakości sygnału jest prawdopodobieństwo wystąpienia elementarnej stopy błędu lub stopień zniekształcenia kodowego informacji. Wierność transmisji w systemach cyfrowych jest określana przez średnie prawdopodobieństwo wystąpienia błędów na poziomie stopy błędów. Istotnymi miarami wierności (jakości) w systemach cyfrowych jest bitowa stopa błędów BER (*bit error ratio*) oraz symbolowa stopa błędów Pe. Bitowa stopa błędów pozwala określić prawdopodobieństwo wystąpienia błędu w strumieniu przesyłanych informacji.

Skrytość to zdolność systemów informatycznych do przeciwstawienia się potencjalnym możliwościom podsłuchu przesyłanych (transmitowanych) danych. Skrytość dotyczy ochrony przesyłanych informacji, ochrony określonych relacji wymiany informacji oraz faktu i miejsca przekazu informacji. W klasycznych działaniach wojsk lądowych skrytość przekazywania informacji określana jest zazwyczaj poprzez trzy wskaźniki:

- współczynnik utajnienia kanałów (łączy) w systemach (sieciach) informatycznych,
- prawdopodobieństwo wykrycia obiektu systemu łączności,
- wartość oczekiwaną ilości wykrytych obiektów w systemie łączności.

W kierowaniu walką elektroniczną skrytość przekazu informacji może odegrać decydujące znaczenie dla możliwości przeprowadzenia odpowiednich operacji.

Wymagania techniczno-eksploatacyjne

Wymagania techniczno-eksploatacyjne stawiane przed systemami informatycznymi są związane ze sprawnością i właściwym funkcjonowaniem stworzonego, na potrzeby walki elektronicznej, systemu. Wymagania techniczno-eksploatacyjne definiują istotne właściwości wykorzystywanych środków informatycznych oraz zasady ich funkcjonowania. Z przeprowadzonych badań wynika, że do głównych wymagań techniczno-eksploatacyjnych systemu należy zaliczyć:

---

[13] *System łączności brygady*, praca zbiorowa pod kierunkiem J. Janczaka, AON, Warszawa 2004, s. 14.

[14] J. Michniak, *Dowodzenie i łączność*, AON, Warszawa 2005, s. 177.

– gotowość (dostępność),
– przepustowość,
– trwałość,
– mobilność,
– bezpieczeństwo.

Gotowość (dostępność) jest to zdolność systemu informatycznego do terminowego przejścia z jednego stanu do innego, niezbędnego do zapewnienia kierowania reagowaniem kryzysowym. Dostępność osiąga się poprzez stworzenie odpowiedniej struktury organizacyjno-funkcjonalnej systemu informatycznego, w skład której wchodzą także właściwe procedury oraz wyposażenie techniczne pozwalające na realizację wyznaczonych zadań. Do podstawowych wskaźników określających gotowość (dostępność) należy zaliczyć czas przejścia systemu informatycznego do stanu pełnej wydajności i prawdopodobieństwo terminowego wykonania zaplanowanych przedsięwzięć w określonym czasie. Należy zauważyć, że do osiągnięcia gotowości systemu informatycznego niezbędny jest wysoki poziom wyszkolenia personelu technicznego obsługującego (utrzymującego) ten system[15].

Przepustowość systemu dotyczy w głównej mierze sieci szkieletowych. Przepustowość sieci (systemu) określana jest przez potencjalne możliwości tych sieci w zakresie transmisji odpowiednich strumieni danych w jednostce czasu. Jest ona ustalana dla poszczególnych relacji wymiany informacji (pary węzłów, kanału łączności, linii telekomunikacyjnych). Ważne jest także zapewnienie niezbędnego pasma transmisji danych możliwie na najniższych szczeblach kierowania, co umożliwi pozyskiwanie informacji o zaistniałej sytuacji u samego źródła. Do podstawowych wskaźników określających przepustowość systemu informatycznego można zaliczyć: maksymalną szybkość transmisji, ilość podstawowych kanałów w relacji łączności, wartość oczekiwaną ilości kanałów w relacji łączności[16].

Trwałość systemu informatycznego to jego zdolność do pracy podczas oddziaływania różnorodnych czynników zewnętrznych, związanych w głównej mierze z niekorzystnym oddziaływaniem warunków meteorologicznych, terenowych, zakłóceń elektromagnetycznych itp. Odporność na zakłócenia systemu informatycznego definiuje się jako zdolność tego systemu do realizacji zamierzonych (zaplanowanych) zadań w warunkach oddziaływania wszystkich rodzajów zakłóceń. Niezawodność systemu informatycznego to nic innego jak zdolność do wykonania postawionych zadań przy zachowaniu odpowiednich wartości parametrów eksploatacyjnych.

Do podstawowych wskaźników określających trwałość systemu informatycznego należy m.in. zaliczyć: współczynnik sprawności, średni czas poprawnej pracy systemu teleinformatycznego, prawdopodobieństwo, że czas przerwy w pracy systemu nie przekroczy dopuszczalnej wartości[17].

---

[15] *System łączności brygady*, wyd. cyt., s. 16.
[16] Tamże, s. 17.
[17] Tamże.

Mobilność systemu informatycznego determinowana jest poprzez rodzaj środków w nim wykorzystywanych i stanowi właściwość systemu, która przejawia się zdolnością do prawidłowego i terminowego tworzenia podsystemu wymiany informacji. Mobilność można określić wskaźnikami: prawdopodobieństwem terminowego wykonania zadania w zakresie zmiany struktury i funkcjonalności systemu informatycznego, granicznym czasem wykonania zadań kierowania walką elektroniczną z określoną niezawodnością[18].

Bezpieczeństwo systemu informatycznego rozumiane jest jako zdolność tego systemu do przeciwstawienia się wszystkim rodzajom zagrożeń, w tym: podsłuchem, modyfikacją i odmową usługi[19]. Zapewnienie bezpieczeństwa systemu informatycznego (podsystemu wymiany informacji) należy do zadań najtrudniejszych i najbardziej skomplikowanych. Pod względem technicznym system informatyczny stworzony na potrzeby walki elektronicznej stanowić będzie środowisko złożone i różnorodne. Z tego też względu w celu projektowania, optymalizacji, eksploatacji oraz zarządzania systemami teleinformatycznymi należy posłużyć się odpowiednimi modelami matematycznymi i analitycznymi, dedykowanym oprogramowaniem (np. Comnet III, Opnet, NetView, HP OpenView itp.), a także wytycznymi zawartymi w dokumentach normatywnych. Stworzony system informatyczny (podsystem wymiany informacji) będzie systemem rozproszonym, charakteryzującym się odpowiednimi właściwościami, takimi jak:

- współdzieleniem zasobów,
- otwartością,
- współbieżnością,
- skalowalnością,
- przeźroczystością,
- tolerowaniem uszkodzeń.

Współdzielenie zasobów wynika z potrzeb uczestników procesu kierowania walką elektroniczną do współdzielenia informacji o aktualnej sytuacji. Cecha ta pozwala na równoległą pracę zespołową z wykorzystaniem tych samych obiektów informacji oraz usług systemowych. Zasoby informacyjne w rozproszonych systemach informatycznych powinny być umieszczone w określonych węzłach systemu. Dostęp do nich powinien być realizowany poprzez zdalną komunikację. Aktualnie wyróżniane są dwa podstawowe modele współdzielenia informacji w rozproszonych systemach informatycznych, a mianowicie: model oparty na architekturze klient–serwer i model bazujący na obiektach, np. w technologii CORBA (*Common Object Request Broker Architecture*)[20].

Otwartość systemu informatycznego charakteryzuje jego zdolność dodawania nowych usług systemu, bez konieczności zmiany lub zwielokrotniania usług już istniejących. Otwartość systemu zapewniana jest m.in. poprzez specyfikację i do-

---

[18] J. Michniak, *Dowodzenie i łączność*, wyd. cyt., s. 179.

[19] W. Stallings, *Ochrona danych w sieci i intersieci w teorii i praktyce*, Wydawnictwa Naukowo-Techniczne, Warszawa 1997, s. 19–20.

[20] J. Liberty, *C++ – Księga eksperta*, Wydawnictwo Helion, Gliwice 1999, s. 685–711.

kumentowanie protokołów i interfejsów komunikacyjnych, co umożliwia zapewnienie kompatybilności poszczególnych urządzeń i całych systemów[21].

Współbieżność systemu mówi o możliwości komunikowania się, w systemach rozproszonych, dużej liczby komputerów wyposażonych w jeden lub więcej układów mikroprocesorowych. Wykorzystanie w systemach informatycznych architektur nadmiarowych (redundancji) oraz wyposażenie komputerów w układy wieloprocesorowe pozwala na zwiększenie mocy obliczeniowych, skrócenie czasu realizacji zadań oraz zwiększenie niezawodności systemu.

Skalowalność systemu mówi o możliwości modyfikacji i rozbudowy struktury systemu teleinformatycznego w zakresie usług przez niego świadczonych. Jest to nic innego jak możliwość przyłączania i odłączania urządzeń świadczących konkretne usługi. Skalowalność związana jest bezpośrednio z utrzymaniem wysokiej wydajności i niezawodności pracy całego systemu informatycznego[22].

Przeźroczystość systemu to jego zdolność do ukrywania przed użytkownikami systemu jego struktury organizacyjno-funkcjonalnej. Pozwala to postrzegać system informatyczny jako jedną spójną całość. Przeźroczystość systemu w trakcie kierowania walką elektroniczną pozwala na bezpośredni i przejrzysty dostęp do aktualnej i wiarygodnej informacji. Można wyróżnić przeźroczystość: dostępu, położenia, współbieżności, zwielokrotniania, awarii, wędrówki, wydajności i skalowania[23].

Tolerowanie uszkodzeń to zdolność systemu informatycznego do realizacji postawionych zadań oraz nieprzerwanej pracy w różnorodnych warunkach, wywierających niekorzystny wpływ na funkcjonowanie systemu jako całości. Tolerowanie uszkodzeń przez system informatyczny można uzyskać poprzez:

– zastosowanie urządzeń wykonanych w odpowiedniej technologii (dedykowanej do postawionych wymagań),

– zastosowanie architektury redundantnej.

Tolerowanie uszkodzeń przez system informatyczny związane jest także z funkcjonowaniem w samym systemie określonych mechanizmów, takich jak[24]:

– autokonfiguracji,

– identyfikacji zaistniałych uszkodzeń,

– przywracania funkcjonalności systemu po awarii.

---

[21] G. Coulouris, J. Dollimore, T. Kindberg, *Systemy rozproszone – podstawy i projektowanie*, Wydawnictwa Naukowo-Techniczne, Warszawa 1998, s. 39–42.

[22] Tamże, s. 43–45.

[23] Tamże, s. 47–48.

[24] A. Silberschatz, P.B. Galvin, *Podstawy systemów operacyjnych*, Wydawnictwa Naukowo-Techniczne, Warszawa 2001, s. 707–762.

Koncepcja walki sieciocentrycznej

Innym wyzwaniem stojącym przed sieciami informatycznymi jest ich rola i znaczenie w koncepcji walki sieciocentrycznej. Pojęcie **walka sieciocentryczna** zostało zaprezentowane pierwszy raz szerszej publiczności w 1998 roku, w artykule „Network Centric Warfare – Its Origins and Future" zamieszczonym na łamach „Proce-edings"[25]. Przedstawiono w nim nowy sposób prowadzenia działań militarnych w erze społeczeństw informacyjnych.

Rozwój technologii informatycznych spowodował lawinowe narastanie nowych, nieznanych dotychczas możliwości komunikowania się oraz gwałtownie poszerzył obszary ich zastosowania. Technologie transmisji danych (wykorzystywane głównie w sieci Internet) dostosowane do potrzeb użytkowników cywilnych dały nowe możliwości systemom wykorzystywanym w wojsku. To pozwoliło na zwiększenie ich możliwości w zakresie przekazywania, przetwarzania i analizy danych. Wyzwaniem jest jednak sposób zorganizowania przekazu informacji w sieci oraz odpowiednie jej udostępnienie. Najważniejszą sprawą jest łączenie dostępnych w sieci informacji i tworzenie jednolitych obrazów sytuacji (COP – *Common Operational Picture*).

Na potrzeby koncepcji NCW (*Network Centric Warfare*) tworzona jest globalna sieć informacyjna (*Global Information Grind*), która ma stanowić fizyczną platformę telekomunikacyjną zapewniającą realne funkcjonowanie przyjętej koncepcji wojny. W systemach sieciocentrycznych należy wyróżnić trzy klasy wzajemnie powiązanych relacjami i współdziałających podsieci:

– sieć środków rozpoznania określane mianem sieci sensorów (*Sensor Grid*),

– sieć systemu stanowisk dowodzenia (*C2 Grid*),

– sieć systemów uzbrojenia, w której funkcjonują aktywne środki walki (*Shooter Grid*).

Architektura sieci informatycznych powinna zapewnić połączenie tych trzech podsystemów w jeden sprawnie funkcjonujący mechanizm.

Zapewnienie możliwości przesyłania odpowiedniej ilości danych związanych z obrazowaniem aktualnego obrazu przestrzeni walki wymaga wykorzystania różnego rodzaju sieci informatycznych o określonej przepustowości. Podstawowymi (nadrzędnymi) sieciami wykorzystywanymi w koncepcji NCW będą sieci komercyjne, resortowe i użytku publicznego. Będą to zarówno różnego rodzaju sieci komercyjne (np. POLPAK, TP SA, Netia, telefonia komórkowa), sieci resortowe (np. MILWAN, SECWAN, sieć teleinformatyczna Straży Granicznej), systemy łączności satelitarnej (np. EUTELSAT, INTELSAT, US SAT), jak i sieć Internet. Sieci te zapewnią odpowiedni transfer danych praktycznie w każdym zakątku kuli ziemskiej.

---

[25] A. Cebrowski, J. Garstka, *Network Centric Warfare – Its Origins and Future*, Proceedings of the Naval Institute 1998, s. 4.

Następną siecią (podrzędną w stosunku do sieci resorowych, komercyjnych i użytku publicznego) powinna być sieć szkieletowa przestrzeni walki, która byłaby z punktu widzenia modelu siedmiowarstwowego ISO-OSI siecią rozległą (WAN – *Wide Area Network*). Ponieważ jednym z wyznaczników sieciocentryczności jest rezygnacja z klasycznego (hierarchicznego) systemu dowodzenia, sieć ta nie powinna być przypisana do konkretnego szczebla dowodzenia. Stąd też nie powinno się jej kojarzyć np. z siecią radioliniowo-kablową dywizji bądź korpusu. Na dzień dzisiejszy głównymi elementami sieci powinny być sieciowe węzły łączności wyposażone w radiolinie z rodziny R-450 systemu „Storczyk", terminale satelitarne i radiostacje szerokopasmowe. Zasięg sieci szkieletowej przestrzeni walki powinien uwzględniać aktualnie realizowane zadania i kształtować się od kilkunastu do kilkuset kilometrów. Każdy węzeł sieci szkieletowej powinien być punktem dostępowym (*access point*) dla innych sieci rozwijanych w przestrzeni walki, zarówno poprzez radiolinie, terminale satelitarne, jak i radiostacje szerokopasmowe. Strukturę węzła sieciowego i sieci szkieletowej przedstawiono na rysunkach 1 i 2.

Przeprowadzone analizy pozwalają na stwierdzenie, że rozpatrywany system walki elektronicznej wykorzystywałby sieć szkieletową jako główne medium transmisyjne. Takie podejście umożliwia zwiększenie zasięgu systemu, zwiększa bowiem jego niezawodność i jest zgodne z koncepcją swobodnego dostępu do informacji wytwarzanej przez sensory – w tym przypadku namierniki.

Koncepcja wykorzystania sieci informatycznych

Zgodnie z „Programem rozwoju SZ na lata 2005–2010" ogłoszonym w MON 1 października 2004 roku jednostki, m.in. WE, mają składać się z kompatybilnych ze sobą modułów (segmentów) określonych sił i środków. Grupowanie jednostek w kilka modułów pozwoliłoby delegować poszczególne segmenty na potrzeby określonych działań. Program ten ma decydujący wpływ na perspektywiczny system WE, bowiem każdy moduł musi posiadać zarówno podsystem rozpoznania i przeciwdziałania elektronicznego z jednoczesną obroną elektroniczną.

Z przeprowadzonych analiz wynika, że perspektywiczny system walki elektronicznej składałby się z trzech zasadniczych elementów, a mianowicie:

– modułu dowodzenia,

– modułu stacji rozpoznania i namierzania (w tym SIGINT[26], ELINT[27] i COMINT[28]),

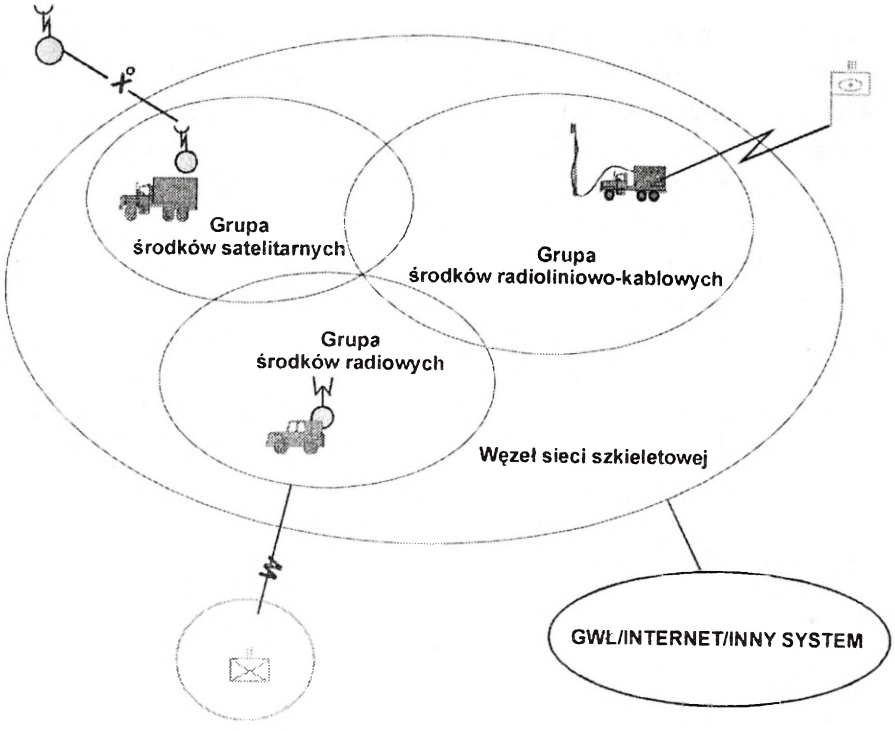
– modułu stacji zakłóceń (przeciwdziałania elektronicznego HF, VHF, UHF i SHF).

---

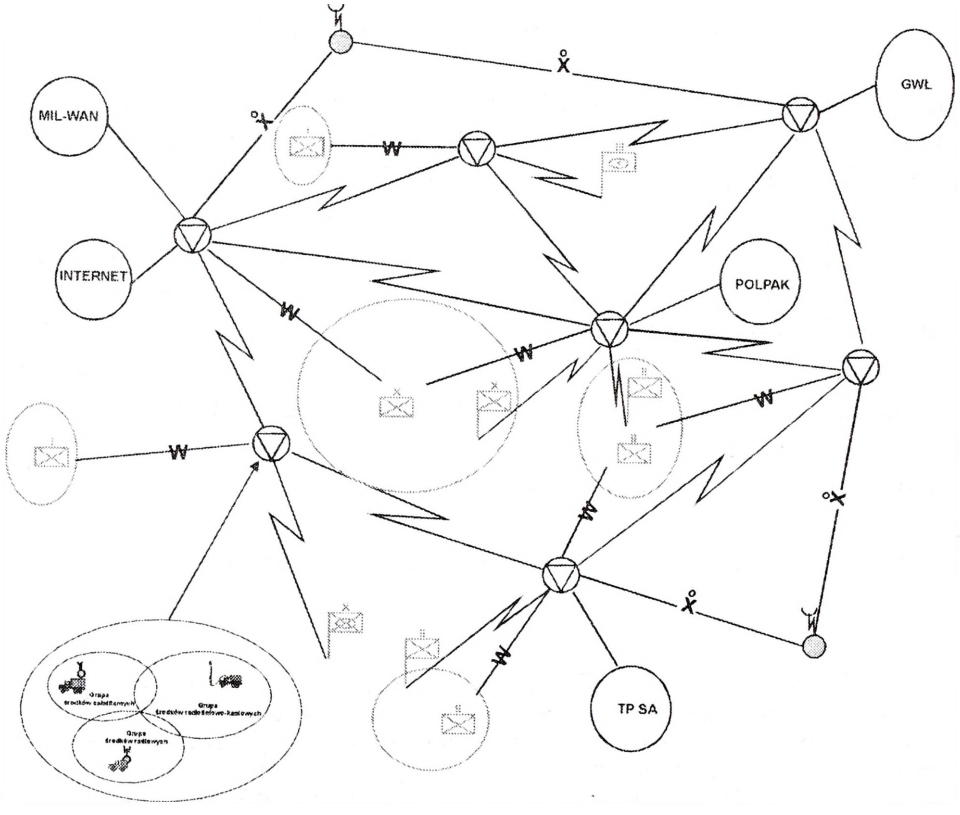
[26] W polskiej teorii walki elektronicznej terminy SIGINT, ELINT i COMINT mieszczą się w ogólnym pojęciu „rozpoznanie elektroniczne". Rozpoznanie elektroniczne traktowane jest jako wsparcie wszystkich jednostek biorących udział w każdej operacji (połączonej, kryzysowej, morskiej itp.). Zakres działania powinien być nieograniczony ze względu na obszar.

[27] Rozpoznanie sygnałów nieradiowych, do których zaliczać będziemy sygnały radiolokacyjne i inne postacie sygnałów nieniosących informacji np. nawigacyjne.

[28] Rozpoznanie radiowe (UKF, radioliniowe, radiosatelitarne, teletransmisja). Będą to wszystkie sygnały, które mogą przenosić różne postacie danych.



Rys. 1. Struktura węzła sieciowego



Rys. 2. Struktura sieci szkieletowej

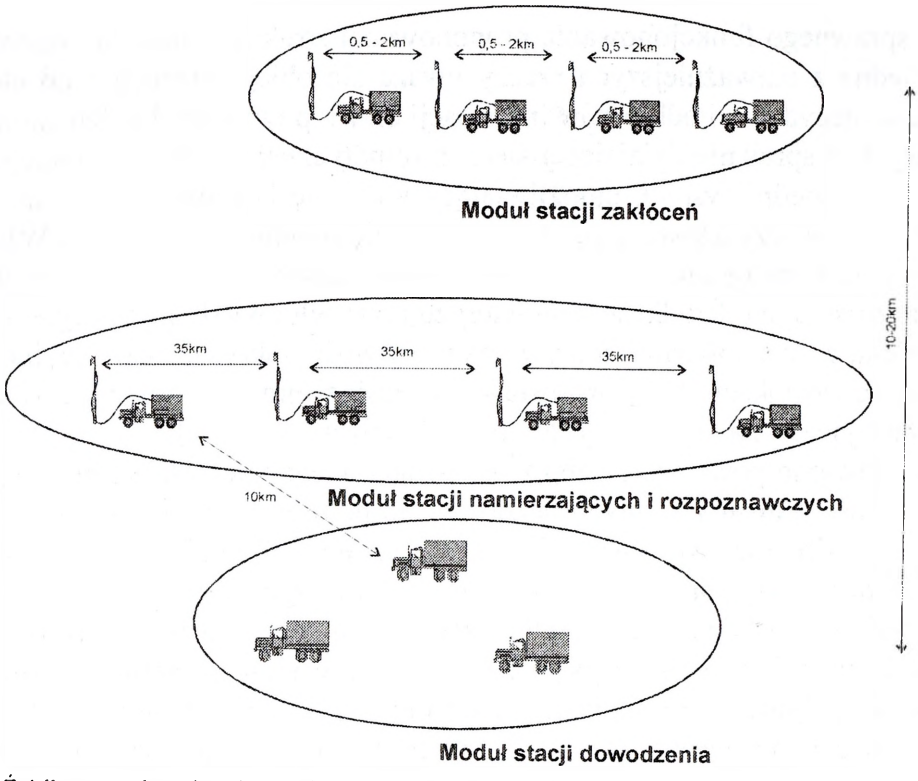
Dla sprawnego funkcjonowania proponowanej struktury modułu systemowego WE za jedną z najważniejszych rzeczy uważa się obieg informacji od elementu systemu do decydenta i odbiorców informacji oraz z powrotem do elementu. Obieg informacji bez sprawnie działającej sieci informatycznej nie będzie funkcjonował. Dlatego odpowiedni system, umożliwiający wymianę informacji, jest kluczowym zagadnieniem w przyszłościowych rozwiązaniach modelowych systemu WE.

W klasycznym ujęciu system walki elektronicznej bazuje na własnych środkach transmisyjnych. Środki te charakteryzują się odpowiednim zasięgiem i przepustowością, co bezpośrednio wpływa na możliwości taktyczno-operacyjne całego systemu. Na rysunkach 3 i 4 przedstawiono zasięgi pracy systemu walki elektronicznej bazującego na organicznych środkach transmisji danych.

Przedstawione powyżej rozwiązanie posiada wiele zalet. Najważniejszą z nich jest możliwość transmisji danych bezpośrednio pomiędzy modułami systemu, bez elementów pośrednich wprowadzających opóźnienia. Krótki czas transmisji danych z modułu stacji namierzających i rozpoznawczych do modułu dowodzenia oraz z modułu dowodzenia do modułu stacji zakłóceń umożliwia szybką reakcję systemu na zaistniałą sytuację. Wysoka skuteczność systemu walki elektronicznej jest możliwa jedynie wtedy, gdy wszystkie moduły systemu będą posiadały środki transmisyjne zapewniające odpowiednią przepustowość. Z tego względu najlepszym rozwiązaniem byłoby wyposażenie modułów systemu w radiolinie horyzontalne. Wykorzystywanie do transmisji danych sieci radiowych (w tym sieci szerokopasmowych) nie zapewnia odpowiedniej przepustowości i zwiększa ryzyko wykrycia przez przeciwnika.

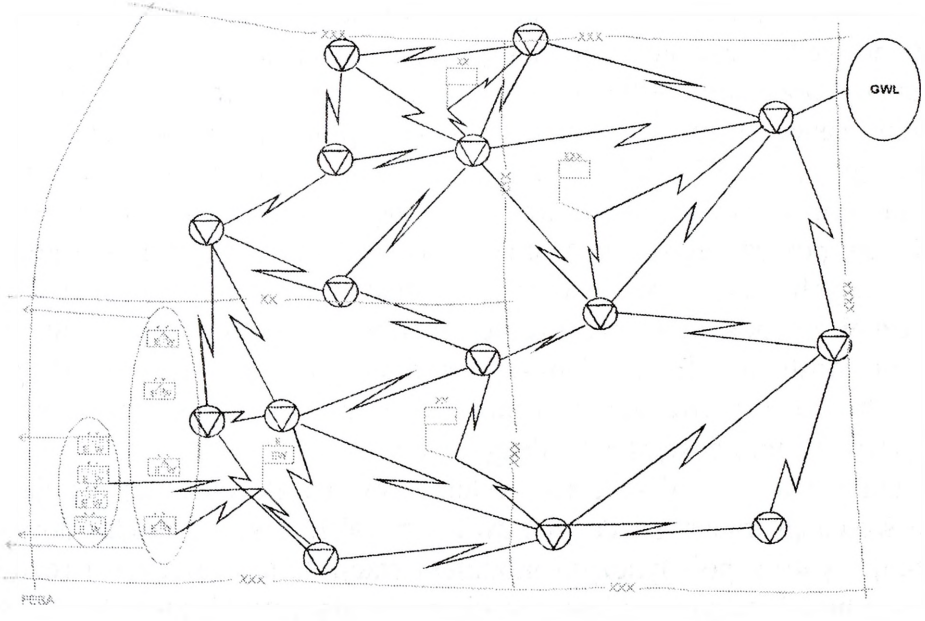
Pomimo niepodważalnej zalety, jaką jest szybkość transmisji pomiędzy modułami systemu walki elektronicznej, istnieje jedna poważna wada rozwiązania bazującego na wykorzystaniu tylko organicznych środków łączności. Wadą tą jest ograniczony zasięg systemu, co w znacznym stopniu ogranicza jego możliwości operacyjno-taktyczne. Wynika to bezpośrednio z faktu zastosowania do transmisji danych radiolinii horyzontowych, których zasięg ogranicza się do 40 km. Innym mankamentem powyższego rozwiązania jest hermetyczność systemu i ograniczony dostęp do danych rozpoznawczych w nim przetwarzanych. Koncepcja walki sieciocentrycznej zakłada m.in. stworzenie sieci sensorów, z których dane byłyby bezpośrednio dostępne dla decydentów. Dane uzyskiwane przez moduł stacji namierzających i rozpoznawczych powinny być, w myśl koncepcji walki sieciocentrycznej, bezpośrednio dostępne dla decydentów.

O ograniczonych możliwościach systemu walki elektronicznej bazującego na własnych środkach transmisji danych świadczy także fakt, że moduł dowodzenia współpracuje tylko z pojedynczym modułem stacji namierzających i rozpoznawczych oraz z pojedynczym modułem stacji zakłócających. Możliwości całego systemu są ograniczone do rozpoznawania i zakłócania tylko jednego, wybranego kierunku.



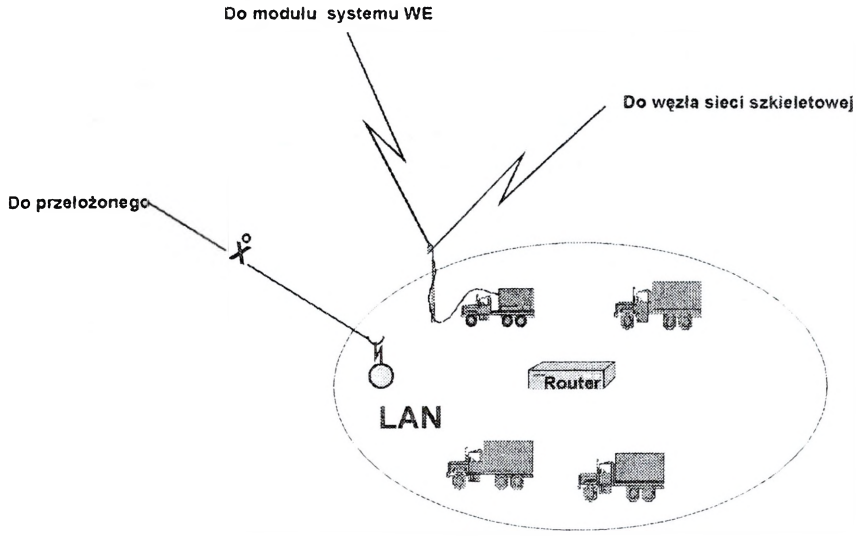
Źródło: na podstawie założeń dla systemu WE „Kaktus".

Rys. 3. Zasięgi pracy systemu walki elektronicznej bazującego na organicznych środkach transmisji danych – wariant



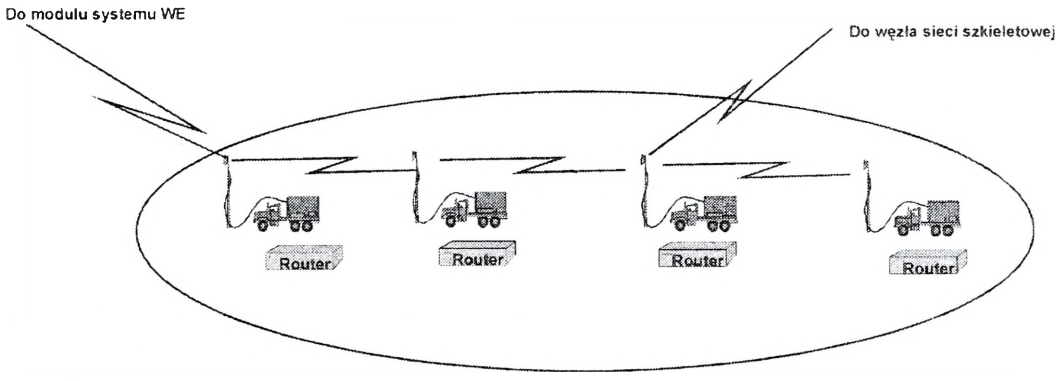
Źródło: na podstawie założeń dla systemu WE „Kaktus".

Rys. 4. Wykorzystanie systemu walki elektronicznej bazującego na organicznych środkach łączności – wariant



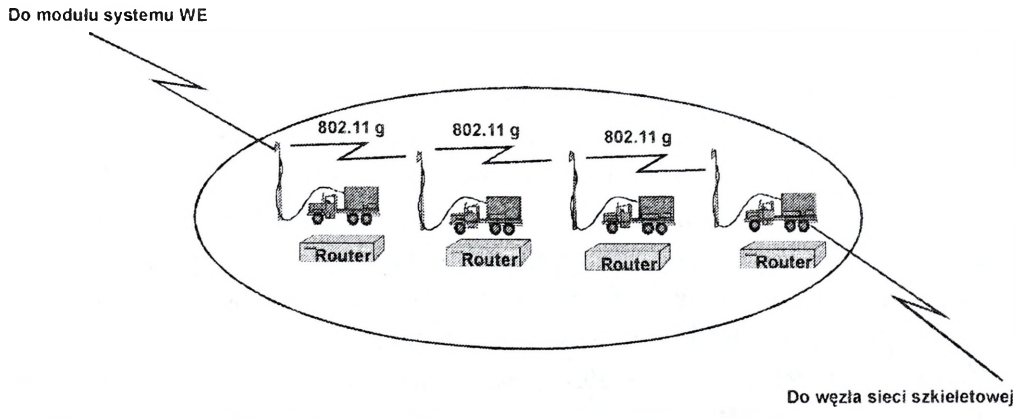
Źródło: na podstawie założeń dla systemu WE „Kaktus".

Rys. 5. Wyposażenie modułu dowodzenia – przykład



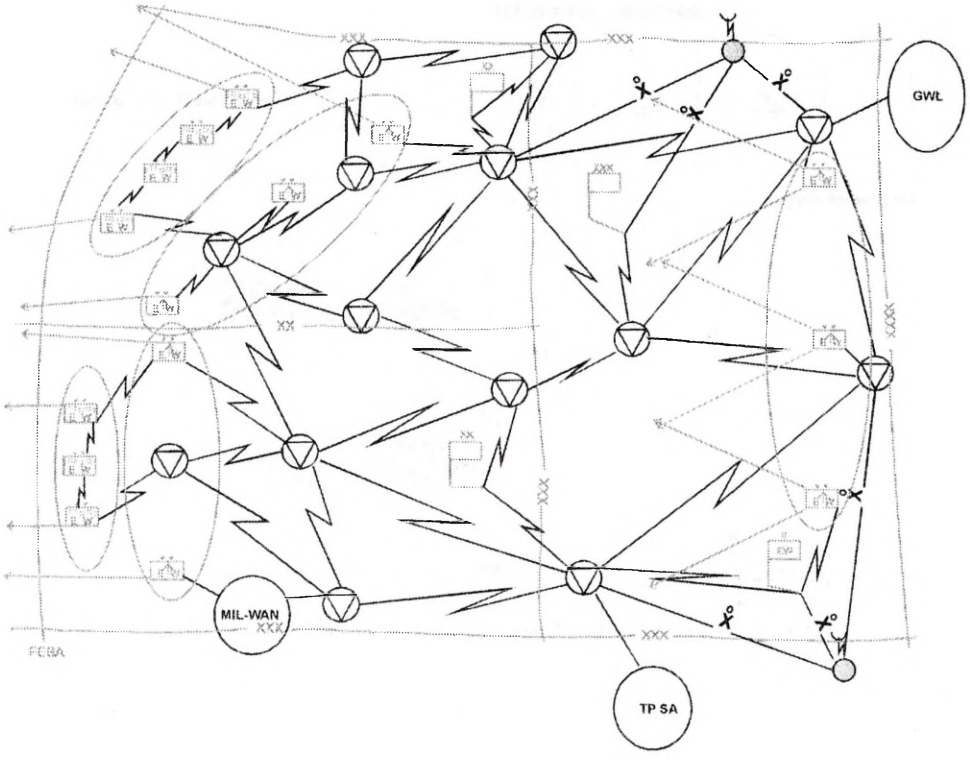
Źródło: na podstawie założeń dla systemu WE „Kaktus".

Rys. 6. Wyposażenie modułu stacji namierzających i rozpoznawczych – przykład



Źródło: na podstawie założeń dla systemu WE „Kaktus".

Rys. 7. Wyposażenie modułu stacji zakłóceń – przykład



Źródło: na podstawie założeń dla systemu WE „Kaktus".

Rys. 8. Wykorzystanie systemu walki elektronicznej bazującego na sieci szkieletowej – wariant

Wyeliminowanie powyższych bolączek możliwe jest poprzez wykorzystanie, do transmisji danych, sieci szkieletowej. Sieć ta, jak wspomniano wcześniej, zapewnia transmisję danych pomiędzy wszystkimi elementami biorącymi udział w działaniach. Przepustowość sieci i wykorzystywane protokoły transmisyjne (oparte na technologii IP) powodują, że opóźnienia w sieci są minimalne, a transmisja danych odbywa się w czasie prawie rzeczywistym. Wpływ opóźnień transmisji danych, wytwarzanych przez sieć, na skuteczność systemu walki elektronicznej byłby nieistotny i niezauważalny.

W celu wykorzystania sieci szkieletowej na potrzeby transmisji danych w systemie walki elektronicznej niezbędna jest modyfikacja wyposażenia modułów systemu. Ponieważ sieć szkieletowa wykorzystywać będzie protokoły routowalne (w tym protokół IP), wszystkie stacje (wozy) systemu należy wyposażyć m.in. w routery. Umożliwiałyby one współpracę lokalnych sieci komputerowych stacji (wozów) z siecią szkieletową i innymi elementami systemu walki elektronicznej. Do połączeń pomiędzy modułami systemu a węzłami sieci szkieletowej powinny być wykorzystane radiolinie i systemy satelitarne. Z uwagi na charakterystykę pracy modułu stacji zakłóceń istnieje także możliwość wykorzystania, do transmisji danych pomiędzy stacjami modułu, sieci bezprzewodowej w standardzie 802.11g. (z wykorzystaniem anten kierunkowych).

Wykorzystanie sieci szkieletowej jako podstawowego medium transmisyjnego dla modułów systemu walki elektronicznej zwiększa możliwości operacyjno-taktyczne samego systemu. Moduł dowodzenia może znajdować się w znacznej odległości do pozostałych modułów systemu. Ograniczeniem w tym przypadku jest zasięg sieci szkieletowej. Dodatkowo jeden moduł dowodzenia jest w stanie współpracować z wieloma modułami stacji namierzania i rozpoznania oraz z wieloma modułami stacji zakłócania, co umożliwia prowadzenie zakłócania i rozpoznania na wielu kierunkach.

Na poniższych rysunkach przedstawiono uproszczone przykłady wyposażenia modułów systemu oraz wariant pracy systemu walki elektronicznej.

Podsumowanie

W klasycznym ujęciu systemu, bazującym na organicznych środkach transmisji danych, jego możliwości taktyczno-operacyjne są ograniczone zasięgiem wykorzystywanych środków. Oprócz tego jeden moduł dowodzenia zarządza tylko jednym modułem stacji namierzających i rozpoznawczych oraz jednym modułem stacji zakłóceń. System taki może jednorazowo prowadzić działania namierzania i zakłócania tylko w jednym kierunku.

Wykorzystanie sieci szkieletowej jako podstawowego medium transmisyjnego dla systemu zwiększa jego możliwości operacyjno-taktyczne poprzez zwiększenie obszaru działania systemu oraz umożliwia prowadzenie namierzania i zakłócania na wielu kierunkach. Jeden moduł dowodzenia jest zdolny do zarządzania wieloma modułami stacji namierzania i rozpoznania oraz wieloma modułami stacji zakłóceń. Jedynym ograniczeniem zaproponowanego rozwiązania jest zasięg i przepustowość sieci szkieletowej.

Konkludując, można stwierdzić, że wykorzystanie sieci szkieletowej na potrzeby funkcjonowania systemu walki elektronicznej zwiększy jego możliwości operacyjno-taktyczne i stworzy nowe możliwości prowadzenia namierzania i zakłócania na wielu kierunkach

Bibliografia

Cebrowski A., Garstka J., *Network Centric Warfare – Its Origins and Future*, Proceedings of the Naval Institute 1998.

Coulouris G., Dollimore J., Kindberg T., *Systemy rozproszone – podstawy i projektowanie*, Wydawnictwa Naukowo-Techniczne, Warszawa 1998.

Dalecki R., Nowosielski L., Tomaszewski B., *Taktyczna sieć wymiany informacji z zastosowaniem szerokopasmowych radiostacji sieci IP-HCDR*, materiały z międzynarodowej konferencji naukowej nt. „Sieci teleinformatyczne w działaniach sieciocentrycznych", AON, Warszawa 2007.

Daniluk P., *Radiowa służba stała i ruchoma*, AON, Warszawa 2004.

Dras M., *Systemy sprzętowe do budowy polowych sieci teleinformatycznych na stanowiskach dowodzenia*, materiały z sympozjum nt. „Sieci teleinformatyczne stanowisk dowodzenia wojsk lądowych szczebla taktycznego", AON, Warszawa 2005.
Liberty J., *C++ – Księga eksperta*, Wydawnictwo Helion, Gliwice 1999.
Michniak J., *Dowodzenie i łączność*, AON, Warszawa 2005.
Łokociejewski M., *Walka elektroniczna w działaniach połączonych*, AON, Warszawa 2004.
System łączności brygady, praca zbiorowa pod kierunkiem J. Janczaka, AON, Warszawa 2004.
Scheffs W., *Walka elektroniczna w operacjach wsparcia pokoju*, AON, Warszawa 2005.
Scheffs W., *System walki elektronicznej w operacjach kryzysowych*, AON, Warszawa 2006.
Silberschatz A., Galvin P.B., *Podstawy systemów operacyjnych*, Wydawnictwa Naukowo-Techniczne, Warszawa 2001.
Stallings W., *Ochrona danych w sieci i intersieci w teorii i praktyce*, Wydawnictwa Naukowo-Techniczne, Warszawa 1997.

Marek DRAS
Prezes Radiotechnika Marketing Sp. z o.o.
ul. Fabryczna 20, Pietrzykowice 55-080 Kąty Wrocławskie

SENSORY I SIECI BEZPRZEWODOWYCH SENSORÓW DO ZASTOSOWAŃ WOJSKOWYCH

Sensory bezprzewodowe oraz sieci sensorów bezprzewodowych należą do najszybciej rozwijających się technologii telekomunikacyjnych w ciągu ostatnich 10 lat. Zostały zakwalifikowane jako jedne z najbardziej obiecujących technologii początku XXI wieku. Technologia sensorów bezprzewodowych do zastosowań wojskowych jest technologią typu COTS. Została przeniesiona z zastosowań cywilnych i przemysłowych do wojskowych. Dokonujący się w ostatnich latach gwałtowny postęp w komunikacyjnych technologiach bezprzewodowych znalazł też swoje odbicie w technice sensorowej. Znacznie wzrosły techniczne możliwości komunikacji i przesyłania danych z i do sensorów oraz między nimi. Sensory bezprzewodowe mogą pracować pojedynczo lub być rozmieszczone w większej liczbie na danym obszarze, tworząc sieć sensorów bezprzewodowych komunikujących się automatycznie między sobą oraz z węzłami zbierania informacji z sieci. Postęp technologiczny w budowie przetworników wielkości fizycznych, takich jak dźwięk, ruch, wibracje czy obraz, pozwolił na miniaturyzację oraz odporność sensorów na wpływ warunków otoczenia. Technologie mechatroniczne MEMS czy kamery wizyjne typu CMOS pozwoliły na miniaturyzację sensorów i zmniejszenie ich zapotrzebowania na moc zasilania. Przetworniki wibracji i drgań oparte o technologie MEMS pozwalają na równoczesne wytwarzanie całych sensorów wraz z przetwornikami w jednym krysztale krzemowym, który wraz z dołączoną baterią stanowi gotowy do zainstalowania i pracy sensor. Sensory do zastosowań wojskowych opierają się na rozwiązaniach przemysłowych, jednakże technologie ich budowy, konieczność uzyskania wysokich parametrów w zakresie wykrywania obserwowanych zjawisk, uzyskiwanie dużych zasięgów transmisji bezprzewodowej, aspekty bezpieczeństwa elektromagnetycznego i informatycznego, konieczność długotrwałej pracy z baterii zasilającej oraz wytrzymałość mechaniczna odróżniają je od ich prekursorów. Aspekty bezpieczeństwa transmisji, komunikowanie się sensorów przez sieć globalną GPS stanowią znaczący wyróżnik między sensorami wojskowymi i cywilnymi. W USA najnowsze osiągnięcia techniczne w dziedzinie sensorów są pozyskiwane do zastosowań wojskowych poprzez organizowane i sponsorowane przez wojskową rządową agencję DARPA uniwersyteckie programy badawcze. Z tych programów wybierane są najlepsze rozwiązania, które następnie są kierowane do dalszych prac wdrożeniowych o ściśle wojskowym przeznaczeniu w wybranych firmach sektora wojskowego. Dzięki temu zaawansowane technologie cywilne są optymalnie adaptowane do celów wojskowych, ale ten pro-

ces jest wieloetapowy i pozwala na pełniejsze spełnianie wymagań wojskowych. Patrząc historycznie, po raz pierwszy sensory bezprzewodowe zaczęły stosować Stany Zjednoczone w czasie wojny wietnamskiej. Zadaniem tamtych sensorów było wykrycie ruchu pojazdów zaopatrujących Vietcong, w dżungli, na tzw. szlaku Ho Chi Minha. Tego ruchu nie można było wykryć z samolotów, stąd powstał pomysł zastosowania sensorów komunikujących się z patrolującymi obszar samolotami. Działanie tych pierwszych sensorów nie było doskonałe – wpływ roślinności i innych elementów otoczenia powodował często fałszywe alarmy, dlatego podchodzono do danych z sensorów z dużą rezerwą. W następnych latach zaczęto udoskonalać budowę sensorów, czyniąc z nich coraz lepszy element rozpoznania przeciwnika na polu walki. Obecnie sensory są stosowane we wszystkich rodzajach wojsk. Każdy rodzaj wojsk używa innego rodzaju specjalistycznych sensorów. Łączenie sensorów działających na różnych platformach na rozległych obszarach i zbiorcze wykorzystywanie uzyskanych z nich informacji to jeden z celów działań sieciocentrycznych.

Obecnie stosowane lub wprowadzane do działań wojsk lądowych nienadzorowane sensory naziemne (UGS – *Unattended Ground Sensors*) zapewniają wykrywanie, obserwowanie, nadzór, identyfikację i klasyfikację celów naziemnych, dokonywaną w czasie realnym, z dokładną lokalizacją za pomocą systemu GPS. Dla sprostania tym zadaniom w sensorach zastosowane są czujniki: akustyczne, sejsmiczne, magnetyczne, podczerwieni, elektrooptyczne – każde w swoim zakresie funkcyjnym z komplementarnością tych działań. Do obróbki danych pochodzących z przetworników w wewnętrznych komputerach sensorów stosowane są złożone algorytmy matematyczne. Dzięki temu w samym sensorze są wbudowane mechanizmy pozwalające ocenić, czy np. czujniki sejsmiczne i akustyczne wykryły cel, który jest pojazdem na gąsienicach, czy na oponach, albo też samochodem osobowym, lub czy wykryty strzał pochodzi z broni krótkiej, czy z moździerza. Czujniki magnetyczne wykrywają zmiany pola wywołane przez przedmioty metalowe, a czujniki podczerwieni mierzą temperaturę przemieszczającego się obiektu, co pozwala określić ilość i kierunek ruchu tych obiektów. Detektory sejsmiczne i akustyczne mogą wykrywać wielkie obiekty na odległość kilkuset metrów, podczas gdy czujniki magnetyczne i podczerwieni mają zasięg kilkudziesięciu metrów. Czujniki elektrooptyczne przesyłają obraz obiektu, pozwalając obserwatorom na jego identyfikację. Głównym zadaniem nienadzorowanych sensorów naziemnych jest nie tylko wykrywanie celów, ale również ocena i klasyfikacja uzyskanych informacji i dopiero po tym wysłanie ich drogą radiową do punktów zbierania informacji czy stanowisk dowodzenia. Dzięki temu uzyskuje się lepsze wykorzystanie pasma częstotliwości pracy i oszczędność energii ze źródeł zasilania sensorów. Źródła zasilania sensorów są najważniejszym czynnikiem wyznaczającym czas działania sensorów w polu. Stąd mechanizm działania sensorów musi być ściśle zoptymalizowany pod kątem maksymalnej oszczędności energii. Największa ilość energii zasilającej jest zużywana do komunikacji radiowej między sensorami oraz na przetwarzanie sygnałów we wbudowanych układach mikroprocesorowych

i cyfrowego przetwarzania danych. Sieci sensorów bezprzewodowych po rozłożeniu lub zrzuceniu z samolotów na danym terenie samoczynnie nawiązują ze sobą łączność i przesyłają między sobą oraz dalej do punktów węzłowych informacje o wykrytych obiektach. System informatyczny sieci sensorów musi przetwarzać informacje, a następnie są one przesyłane i odbierane przez następne sensory. To działanie powoduje pobieranie energii ze źródła zasilania, dlatego oprócz optymalizacji pod kątem energooszczędności układów elektronicznych system informatyczny przechodzi w stan uśpienia z minimalnym poborem mocy, gdy nie występują żadne zjawiska na kontrolowanym obszarze. Układ przechodzi do stanu działania automatycznie po wystąpieniu obserwowanych zjawisk fizycznych.

W stosunku do sieci sensorów przewodowych działających w opisany powyżej sposób są stawiane bardzo wysokie wymagania, których spełnienie nie zawsze jest możliwe przy obecnym poziomie technologii. Poniżej zamieszczono listę najistotniejszych wymagań wobec sieci sensorów:

- możliwie najwyższa niezawodność działania,
- niska cena,
- małe wymiary i ciężar,
- uproszczona logistyka instalowania i współpracy z siecią,
- niskie koszty eksploatacji,
- wysoka jakość uzyskiwanych informacji,
- dostarczanie możliwie dokładnych obrazów z obserwowanych obszarów,
- minimalny pobór mocy,
- praca w każdym terenie,
- odporność na wpływy otoczenia,
- zabezpieczenie przed wrogim namierzeniem i przechwyceniem sensorów oraz podsłuchem radiowym,
- odporność na obecność wrogich sensorów w obszarze działania sieci,
- odporność na podszywanie się wrogich sensorów do pracującej sieci,
- odporność na zakłócenia elektromagnetyczne,
- odporność na uszkodzenia pojedynczego sensora w pracującej sieci,
- łatwość instalacji przez niewykwalifikowanych żołnierzy,
- działanie w systemach zarządzanych i niezarządzanych,
- samokonfigurowalność sieci,
- automatyczna lokalizacja sensorów w sieci.

Jak widać z powyższych rozważań, sensory i sieci sensorów bezprzewodowych są bardzo pożytecznym i wydajnym środkiem rozpoznania na współczesnym polu walki. Ich działanie zastępuje pracę oddziałów zwiadowczych i daje możliwość działania w trudnych warunkach otoczenia. Szybki postęp techniczny w budowie sensorów i ich sieci powoduje, że obecnie stosowane urządzenia szybko podlegają procesowi „starzenia moralnego".

Mjr mgr Karol DYMANOWSKI
Zarząd Rozpoznania i Walki Elektronicznej
Dowództwa Sił Powietrznych

SAMOOBRONA STATKÓW POWIETRZNYCH W ASPEKCIE SIECIOCENTRYCZNOŚCI

Członkostwo Polski w Sojuszu Północnoatlantyckim oraz zacieśnianie więzi militarnych w ramach Unii Europejskiej niosą ze sobą zobowiązania związane z udziałem Sił Zbrojnych RP, w tym wydzielonych sił i środków sił powietrznych, w operacjach sojuszniczych i koalicyjnych poza terytorium kraju. Aktualnie, choć należy założyć, że również w najbliższej przyszłości, operacje te będą miały głównie charakter reagowania na kryzysy i sytuacje kryzysowe o podłożu militarnym i niemilitarnym (społecznym i naturalnym), zdefiniowanym w NATO jako operacje reagowania kryzysowego (*Crisis-Response Operations*)[29]. Z dotychczas przeprowadzonych operacji tego typu wynika, że siły powietrzne ze względu na swoje właściwości (szybkość, mobilność oraz zasięg i precyzję oddziaływania) były najczęściej stosowanym komponentem, zapewniającym uzyskanie przewagi informacyjnej, ciągłe monitorowanie obszaru operacji, transport powietrzny oraz realizującym misje stricte bojowe. Niezależnie jednak od rodzaju operacji i charakteru działań sił powietrznych jednym z zasadniczych zadań jest zapewnienie bezpieczeństwa dla własnych sił i środków oraz ograniczenie, a najlepiej całkowite wyeliminowanie strat. W ramach tego do głównych zadań WE należą neutralizacja improwizowanych ładunków wybuchowych aktywowanych drogą radiową oraz wykrywanie i przeciwdziałanie przenośnym i mobilnym zestawom rakietowym. Drugie z tych zadań realizowane jest m.in. przez pokładowe systemy WE i w literaturze określane jest terminem „samoobrona statków powietrznych". W związku z tym samoobrona statków powietrznych jest obecnie jednym z najważniejszych przedsięwzięć WE realizowanych przez komponent powietrzny we współczesnych operacjach militarnych.

Jednocześnie, mając na uwadze aktualne trendy w myśli wojskowej oraz rozwój technologii, należy rozpatrywać zagadnienia związane z samoobroną statków powietrznych w aspekcie sieciocentryczności. Koncepcja działań sieciocentrycznych NCO (*Network Centric Operations*) to przyszłość, a być może już teraźniejszość prowadzenia operacji militarnych. Jest ona związana ze zmianami we współczesnych społeczeństwach i organizacjach, w tym również wojskowych, oraz ze zmianami charakteru współczesnych zagrożeń. Choć zmiany te podyktowane są

[29] W ramach operacji reagowania kryzysowego wyróżnia się: operacje wsparcia pokoju (wymuszanie, budowanie, utrzymanie i tworzenie pokoju, operacje humanitarne i zapobieganie konfliktom), operacje poszukiwawczo-ratownicze, wsparcie w usuwaniu klęsk żywiołowych, wsparcie operacji humanitarnych, wsparcie operacji ewakuacyjnych, wymuszanie sankcji i embarga, wojskowe wsparcie władz cywilnych oraz wycofanie sił. Zob. *AJP 3.4 – Non-Article 5 Crisis Response Operations*, MAS NATO, Bruksela 2004.

głównie rozwojem technologii i wejściem ludzkości w erę informacji, to teoria wojny sieciocentrycznej nie może być kojarzona tylko i wyłącznie z aspektem technologicznym, ale również, a może przede wszystkim, z aspektami strukturalnym, organizacyjnym i doktrynalnym. Dlatego również podczas rozważań nad samoobroną statków powietrznych należy wziąć pod uwagę każdy z wymienionych obszarów. Warto zauważyć, że w samej definicji działań sieciocentrycznych, zaproponowanej przez prekursorów tej koncepcji[30], zwraca się uwagę na fakt, że NCO pozwala m.in. zapewnić większą żywotność własnych sił i środków. W odniesieniu do statków powietrznych jednym z zasadniczych elementów zapewniających tę żywotność jest system samoobrony. Dlatego w świetle potencjalnego zwiększenia zaangażowania sił powietrznych RP w operacje reagowania kryzysowego poza terytorium kraju warto zastanowić się nad aspektami przygotowania i prowadzenia samoobrony przez statki powietrzne w działaniach sieciocentrycznych.

Zagrożenia dla statków powietrznych

Pożądane zdolności systemów samoobrony statków powietrznych powinny być ściśle związane z zagrożeniami, jakie można napotkać w rejonach aktualnych oraz potencjalnych konfliktów. Na szczycie NATO w Stambule (28–29 czerwca 2004 roku) zatwierdzono „Sojuszniczy program prac na rzecz obrony przed terroryzmem", zgodnie z którym jednym z zasadniczych zadań jest obrona przed przenośnymi zestawami rakietowymi MANPADS (*Man Portable Air Defense System*). Tym samym zestawy MANPADS uznano za jedno z największych zagrożeń dla cywilnych i wojskowych platform powietrznych realizujących misje poza terytorium Sojuszu, zagrożenie wymagające opracowania wspólnych i kompleksowych procedur przeciwdziałania. Jednocześnie podczas szczytu zwrócono uwagę na konieczność zabezpieczenia wywiadowczego pozwalającego oszacować poziom zagrożenia ze strony przenośnych zestawów rakietowych w danym obszarze operacji. Wskutek tego w NATO funkcjonuje m.in. procedura wymiany pomiędzy narodowymi i sojuszniczymi komórkami rozpoznania raportów o zagrożeniach, np. w postaci tzw. *Air Threat Assessment.*

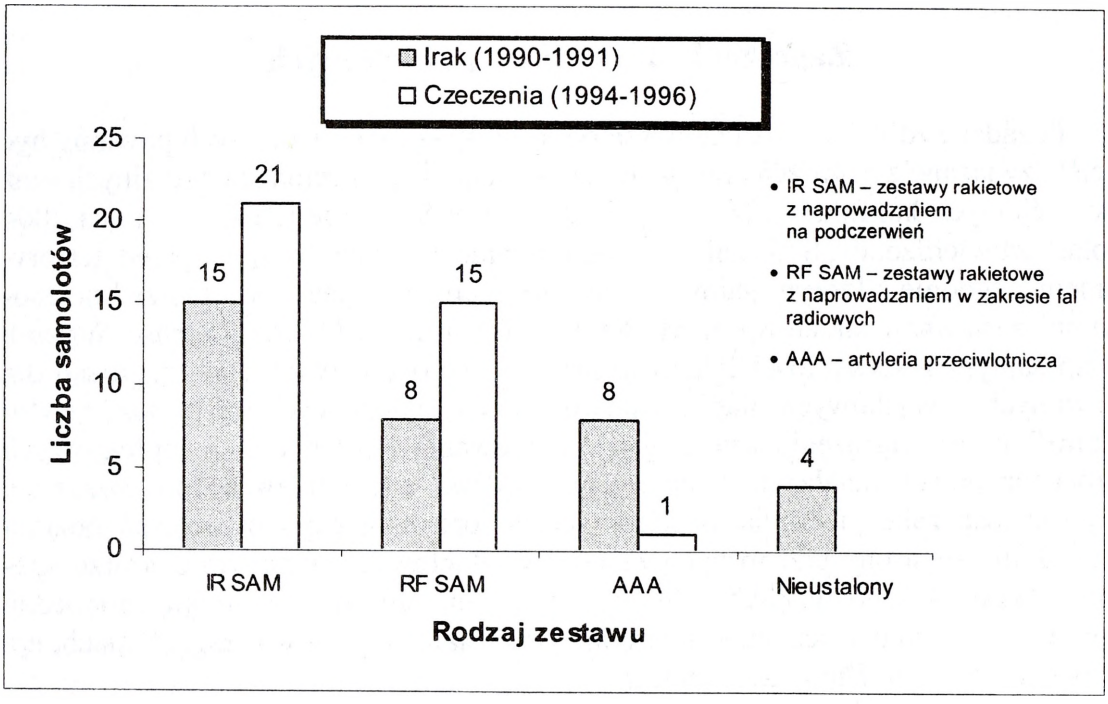
O tym, jak wielkim zagrożeniem są zestawy MANPADS, świadczy już sama ich ilość. Ocenia się, że od lat 50. wyprodukowano około 1 mln tego rodzaju zestawów. Aktualnie ich liczbę szacuje się na 500–750 tys., z czego około 5000–7000 na czarnym rynku, poza kontrolą rządową, w posiadaniu organizacji niepaństwowych[31]. Naprowadzane laserowo i na podczerwień zestawy przenośne są trudne do wykrycia, a odpalane z reguły do celów nisko lecących dają załodze statku powietrznego mało czasu na właściwą reakcję. Poza tym w dalszym ciągu pojawiają się coraz nowsze, bardziej zaawansowane technologicznie, a tym samym

[30] Zob. D.S. Alberts, J.J. Garstka, F.P. Stein, *Network Centric Warfare – Developing and Leveraging Information Superiority*, CCRP, Waszyngton 2000, s. 2.

[31] Zob. M. Schroeder, *Rogue Missiles – Tracking MANPADS Proliferation Trends*, „Jane's Intelligence Review", November 2007.

trudniejsze do przeciwdziałania techniki naprowadzania, np. z wykorzystaniem tzw. głowicy odwzorowującej (*imaging infra-red*).

Kolejne miejsce w hierarchii zagrożeń dla statków powietrznych zajmują mobilne zestawy rakietowe oraz artylerii przeciwlotniczej. Są one stosunkowo tanie, łatwo dostępne i skuteczne, a co za tym idzie – znajdują się na wyposażaniu wielu państw w zapalnych punktach świata. Zestawy te, naprowadzane radiolokacyjnie, w ostatnich konfliktach były powodem mniejszej ilości strat platform powietrznych niż MANPADS (patrz rys. 1). Niższa skuteczność może wynikać z faktu, iż są one łatwiejsze do wykrycia (optycznego i/lub elektronicznego), oraz stosowania bardziej zaawansowanych technik zakłóceń w paśmie radiolokacyjnym. Niemniej jednak proliferacja mobilnych zestawów rakietowych z naprowadzaniem radiolokacyjnym, szczególnie zestawów produkcji radzieckiej, powoduje, że nadal należy się liczyć z dużym zagrożeniem z ich strony.



Źródło: opracowanie na podstawie „F-16 Avionics Technician Training Package – Penetration Aids and ECM Systems", Air Force Training Center Kjevik.

Rys. 1. Straty poniesione od zestawów przeciwlotniczych przez siły koalicji antyirackiej podczas operacji „Pustynna Burza" oraz przez Rosję podczas pierwszej wojny w Czeczenii

Z powyższego wynika, że głównym zagrożeniem dla platform powietrznych biorących udział w operacjach poza terytorium kraju są aktualnie przenośne i mobilne zestawy przeciwlotnicze krótkiego zasięgu. Oczywiście, w wypadku operacji „Desert Storm" czy misji pokojowych na Bałkanach zagrożenie stwarzały również

zestawy rakietowe średniego i dużego zasięgu oraz lotnictwo[32]. Jednak straty sił koalicyjnych/sojuszniczych poniesione w wyniku oddziaływania tych zagrożeń były niemal zerowe[33]. Należy również zwrócić uwagę na nowe zagrożenia dla platform powietrznych w domenie elektromagnetycznej (EM), takie jak zakłócanie satelitarnych systemów nawigacyjnych GPS. Co prawda, doświadczenia z ostatnich operacji, szczególnie „Iraqi Freedom", wskazują, że choć stosowanie przez przeciwnika zakłóceń tego typu nie spowodowało strat ani negatywnych skutków użycia broni precyzyjnej[34], to jednak, ze względu na coraz szersze wykorzystanie systemów GPS, należy przypuszczać, że w przyszłości znaczenie tego rodzaju zakłóceń, a tym samym zagrożeń z tym związanych, będzie rosło.

Rozpatrując udział sił powietrznych (platform powietrznych) w operacjach reagowania kryzysowego poza terytorium kraju, oprócz zagrożeń, należy rozważyć czynniki specyficzne dla tego typu operacji. Uwarunkowania owe będą bowiem rzutować również na prowadzenie WE, w tym samoobrony statków powietrznych. Niewątpliwie jednymi z zasadniczych czynników będą rodzaj operacji oraz założony cel, którego osiągnięcie będzie wyznacznikiem powodzenia operacji. Z tego wynikać będą uwarunkowania polityczno-prawne, m.in. zasady użycia sił ROE (*Rules of Engagement*). W świetle wymagań i ograniczeń związanych z użyciem sił powietrznych w operacjach poza terytorium kraju bardzo ciekawym kryterium podziału tych operacji oraz implikacji wpływających na użycie sił powietrznych jest kryterium ryzyka. Zgodnie z tym kryterium operacje reagowania kryzysowego można podzielić na trzy zasadnicze grupy, stosownie do ryzyka poniesienia strat przez siły powietrzne[35].

Niezależnie jednak od przyjętego kryterium oraz rodzaju operacji reagowania kryzysowego, siły i środki zaangażowane w działania mają prawo do samoobrony. W domenie EM załogi statków powietrznych będą wykorzystywać do tego celu zintegrowane systemy pokładowych urządzeń WE, które w literaturze przedmiotu określa się jako systemy samoobrony statków powietrznych lub systemy obrony indywidualnej samolotu (*aircraft self-protection*).

---

[32] W Kosowie wpływ na niskie straty spowodowane przez artylerię plot oraz MANPADS miał zakaz wykonywania lotów poniżej 15 000 stóp. Zob. A. Price, *The History of US Electronic Warfare, Vol. III*, AOC, 2007.

[33] Aczkolwiek podczas konfliktu w Kosowie doszło do spektakularnego zestrzelenia przez Serbów amerykańskiego samolotu F-117 wykonanego w technologii stealth. Jednak wpływ na to miała nie tyle sama skuteczność zestawu, prawdopodobnie SA-3 (S-125 NEWA), lecz błędy popełnione przez planistów: ta sama trasa samolotu czwarty dzień z rzędu oraz zbytnie oddalenie samolotów zakłóceń wspierających typu EA-6B Prowler. Zob. A. Price, *The History of US Electronic Warfare, Vol. III*, AOC, 2000; B.S. Lambeth, *Kosovo and the Continuing SEAD Challenge*, „Aerospace Power Journal", Summer 2002.

[34] Według źródeł amerykańskich wojska irackie posiadały sześć urządzeń zakłócających GPS, które jednak szybko zostały zneutralizowane przez koalicjantów. Zob. E. Schechter, *Mixed Signals*, „C4ISR – The Journal of Net-Centric Warfare", Vol. 6, No. 8, September 2007.

[35] Zob. M. Marszałek, *Siły powietrzne w operacjach reagowania kryzysowego*, rozprawa habilitacyjna, „Zeszyty naukowe AON", Warszawa 2007.

Przeciwdziałanie zagrożeniom

Ogólnie w ramach przeciwdziałania zagrożeniom dla statków powietrznych w domenie EM można wykorzystać:

– urządzenia rozpoznawczo-ostrzegawcze (np. RWR – *Radar Warning Receiver*, MAWS – *Missile Approach Warning System*),

– pasywne i aktywne urządzenia zakłócające (nadajniki zakłóceń, wyrzutnie flar i dipoli, wabiki itd. do zakłócania systemów radiowych i radiolokacyjnych, w podczerwieni oraz urządzeń optoelektronicznych),

– pociski przeciwradiolokacyjne,

– energię wiązkową,

– rozwiązania konstrukcyjne (odpowiedni kształt, pokrycie kadłuba, czyli tzw. technologia *stealth*),

– osłonę elektroniczną zapewnioną przez inne platformy powietrzne (zakłócenia wpierające),

– odpowiednią taktykę działania (profil lotu, odpowiednie manewry i ugrupowanie samolotów),

– oddziaływanie ogniowe w ramach przełamania obrony powietrznej przeciwnika w działaniach połączonych (np. neutralizacja zagrożenia przez pododdział wojsk specjalnych lub artylerię konwencjonalną)[36].

Z przedstawionych wcześniej uwarunkowań operacji reagowania kryzysowego wynikają implikacje dotyczące przygotowania i prowadzenia WE. Ograniczenia odnośnie do stosowania środków destrukcyjnych (energia wiązkowa, pociski przeciwradiolokacyjne, oddziaływanie ogniowe) powodują, że największe zastosowanie w tego typu operacjach będą miały działania pasywne z wykorzystaniem systemów samoobrony statków powietrznych. Tego typu system integruje w sobie urządzenia rozpoznawczo-odbiorcze oraz zakłócające i powinien umożliwiać kompleksowe przeciwdziałanie w jak najszerszym paśmie częstotliwości, z uwzględnieniem zagrożeń charakterystycznych dla danego obszaru operacji. Ponadto warto dodać, że samoloty najnowszej generacji mogą wykorzystywać do celów samoobrony takie cechy, jak konstrukcję *stealth* oraz supermanewrowość.

W związku z powyższym zadaniem zintegrowanego systemu samoobrony jest zapewnienie skutecznej osłony elektronicznej statku powietrznego na danym obszarze operacji poprzez rozpoznanie zagrożeń w domenie EM (ich wykrycie, identyfikację, klasyfikację i hierarchizację) oraz zastosowanie odpowiedniej techniki przeciwdziałania, a najlepiej kilku naraz, w celu uniknięcia zagrożenia lub zminimalizowania skutków jego oddziaływania. Do właściwej realizacji tego zadania potrzebny jest odpowiednio zorganizowany system (elementy funkcjonalne i powiązania informacyjne) zapewniający prawidłowe przygotowanie oraz funkcjonowanie samoobrony statków powietrznych w trakcie realizacji misji poza terytorium

[36] Zob. K. Dymanowski, *Przełamanie obrony powietrznej przeciwnika*, „Przegląd Sił Powietrznych" 2007, nr 1.

kraju. System ten powinien być elementem (podsystemem) narodowego systemu rozpoznania i WE oraz ściśle współdziałać z systemem sojuszniczym/koalicyjnym (patrz rys. 3). Jego głównym zadaniem powinna być ciągła ocena zagrożenia na obszarze operacji i uzupełnianie baz danych o zagrożeniach w domenie EM, jak również ocena skuteczności, aktualizacja i przeprogramowywanie systemów samoobrony statków powietrznych. Całość przedsięwzięć mających na celu przygotowanie systemu samoobrony do pracy, a następnie zabezpieczenie jego funkcjonowania w czasie trwania operacji może być ujęta w przedstawioną poniżej procedurę.

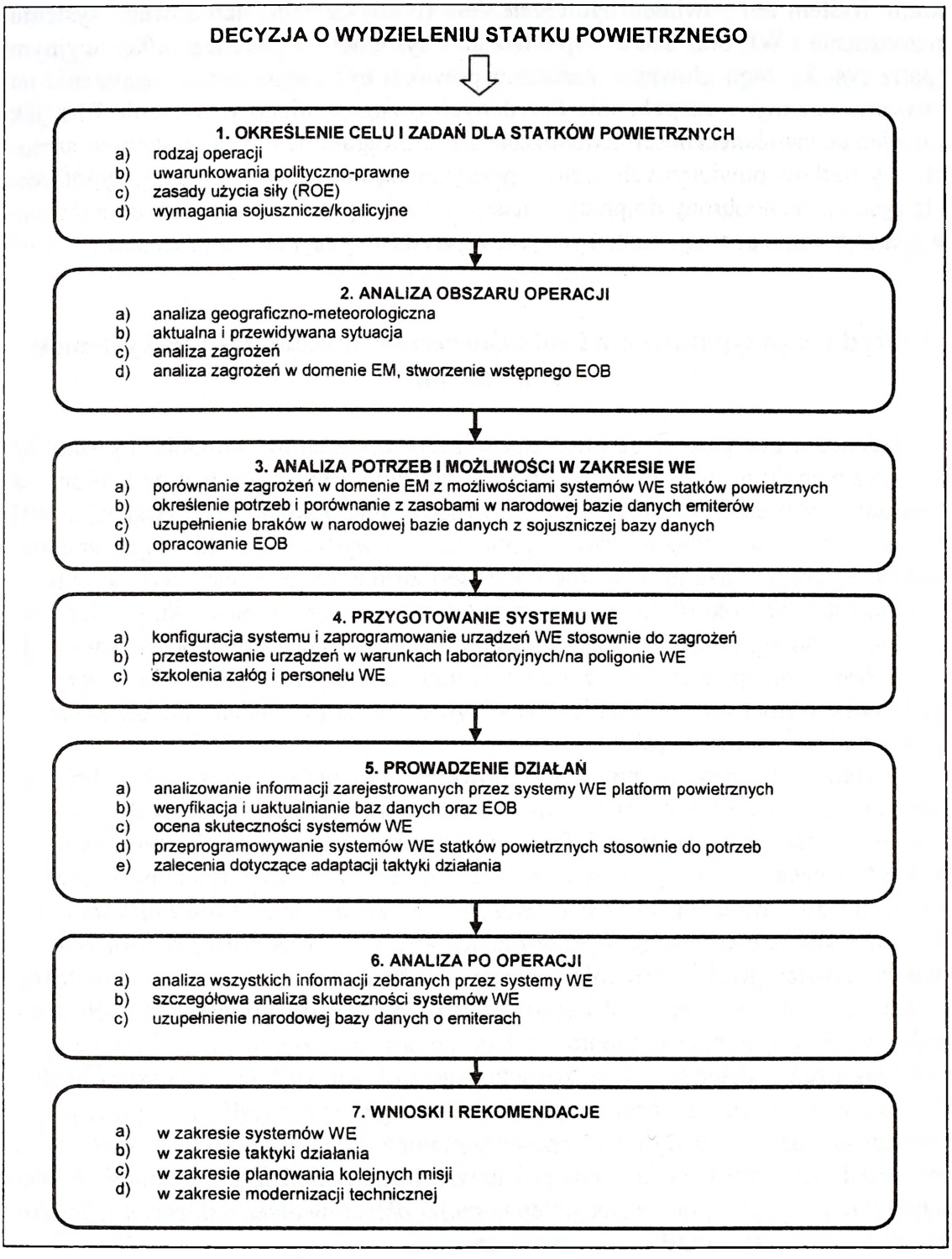
Procedura przygotowania i zabezpieczenia funkcjonowania systemów samoobrony

Procedura przygotowania oraz zabezpieczenia systemów samoobrony statków powietrznych do prowadzenia misji poza terytorium kraju może być podzielona na 7 zasadniczych etapów (patrz rys. 2). Przygotowanie pokładowych systemów WE rozpoczyna się po podjęciu decyzji politycznej o wydzieleniu sił, w tym statków powietrznych, do udziału w operacji poza terytorium kraju. Punkt wyjścia (etap 1) powinno stanowić określenie celu oraz zadań stosownie do typu statku powietrznego (transportowy, bojowy, rozpoznawczy itd.). Dodatkowo powinno się uwzględnić rodzaj operacji, związane z nim uwarunkowania cywilno-prawne i przyjęte ROE oraz wymagania sojusznicze/koalicyjne dotyczące zadań dla określonych typów statków powietrznych.

W etapie 2 komórki rozpoznawcze powinny dokonać szczegółowej analizy obszaru operacji. Zgodnie ze stosowaną obecnie metodyką ocenę należy przeprowadzić w postaci *połączonego informacyjnego przygotowania obszaru operacji*, w ramach czego komórki analityczne sił powietrznych będą realizować analizę wymiaru powietrznego (*Aerospace Intelligence Preparation of the Battlespace*)[37]. W kontekście przygotowania i prowadzenia WE, w tym na potrzeby samoobrony statków powietrznych, szczególną uwagę należy zwrócić na analizę aktualnych i potencjalnych zagrożeń na obszarze operacji oraz na trasach ewentualnych przelotów w rejon operacji. Następnie z całego zbioru zagrożeń należy wydzielić podzbiór zagrożeń w dziedzinie EM, który będzie punktem wyjścia do dalszych analiz. Do oceny zagrożeń komórki rozpoznawcze mogą wykorzystywać opracowania sojusznicze lub innych krajów (np. wspomniane *Air Threat Assessment*), które prowadziły lub prowadzą działania powietrzne na danym obszarze operacji. W tym etapie powinna być opracowana wstępna *mapa obiektów elektronicznych* (*Electronic Order of Battle* – EOB) na obszarze operacji.

---

[37] Zob. *AFPAM 14-118 – Aerospace Intelligence Preparation of the Battlespace*, Departament of the Air Force, 2001; Z. Chojnacki, K. Dymanowski, P. Ponczyński, *Połączone informacyjne przygotowanie przestrzeni operacji*, „Myśl Wojskowa" 2007, nr 1. Warto jednak zaznaczyć, że termin *Intelligence Preparation of the Battlespace* w siłach zbrojnych USA został już zastąpiony terminem *Intelligence Preparation of the Operational Environment*. Zob. *JP 2-0 – Joint Intelligence*, Joint Staff 2007.



Opracowanie własne.

Rys. 2. Procedura przygotowania i zabezpieczenia systemów samoobrony statków powietrznych na potrzeby prowadzenia operacji poza terytorium kraju

W następnym etapie dokonujemy porównania zidentyfikowanych zagrożeń z możliwościami systemów samoobrony statków powietrznych. Oceniamy, czy system samoobrony jest zdolny do przeciwdziałania danemu zagrożeniu, tzn. czy posiada możliwość jego wykrycia oraz czy zaimplementowane są odpowiednie, skuteczne techniki przeciwdziałania. Zdolność do wykrycia i przeciwdziałania zależy od jakości parametrów sygnałowych zagrożenia (np. określonego typu radaru zestawu rakietowego) zgromadzonych w bazie danych systemu samoobrony, tzw. bibliotece zagrożeń i ustanowionych na tej podstawie algorytmów działania dla poszczególnych zagrożeń. Biblioteki zagrożeń powinny być uzupełnianie przed każdą misją danymi pochodzącymi z narodowej bazy danych emiterów promieniowania EM (BDE) tworzonej i uaktualnianej w wyznaczonej do tego komórce analitycznej sił powietrznych[38]. Ponadto, w ramach umów sojuszniczych, można skorzystać z zasobów sojuszniczej bazy danych emiterów NEDB (*NATO Emitter Data Base*) zarządzanej przez Połączony Zespół NATO ds. Walki Elektronicznej JEWCS (*Joint Electronic Warfare Core Staff*) z pomocą Grupy Doradczej ds. NEDB – NEBDAG (*NEDB Advisory Group*). W przypadku braków danych lub braku pewności co do ich aktualności komórki analityczne określają potrzeby rozpoznawcze, na podstawie których rozesłane zostaną zapotrzebowania na informację RFI (*Request for Information*) do instytucji sojuszniczych lub innych krajów. Dodatkowo podjęte powinny zostać działania wywiadowcze mające na celu uzupełnienie luk w bibliotekach zagrożeń. Etap 3 powinien zostać zakończony opracowaniem kompleksowego EOB, w którym oprócz parametrów i położenia wrogich emiterów powinny znaleźć się również przewidywane emitery własne (sojusznicze).

W etapie 4 przystępujemy do konfiguracji i oceny skuteczności systemu samoobrony. Konfigurację systemu można przeprowadzić na dwa sposoby: poprzez zmiany i uaktualnienie oprogramowania (tzw. *software configuration and update*) lub poprzez zmiany i uaktualnienie sprzętu (tzw. *hardware configuration and update*). Zmiany w oprogramowaniu będą polegały na uaktualnieniu bibliotek zagrożeń oraz algorytmów (sekwencji) działania systemów samoobrony. Z kolei rekonfiguracja sprzętu konieczna jest w sytuacji, gdy stwierdzimy, że system samoobrony nie jest zdolny do przeciwdziałania określonym zagrożeniom (np. niezgodność zakresów częstotliwości zagrożenia i urządzenia RWR). Jeśli nie istnieje możliwość takiej rekonfiguracji, to podczas planowania działań platformy nad obszarem operacji należy to uwzględnić, np. planując specjalne trasy i profile lotów lub zapewniając wsparcie elektroniczne ze strony innych platform. Po dokonaniu koniecznych zmian i uzupełnieniu wszystkich danych należy przeszkolić załogi samolotów w zakresie wiedzy teoretycznej dotyczącej zagrożeń na obszarze operacji oraz sposobów przeciwdziałania. Kolejnym krokiem powinno być przetestowanie systemów w warunkach laboratoryjnych lub w miarę możliwości na poligonie WE w środowisku EM maksymalnie zbliżonym do tego na obszarze operacji. Testom poddaje się zarówno urządzenia techniczne, jak i reakcję załóg. W ten sposób oceniany jest stopień wyszkolenia załóg oraz wpływ tzw. czynnika ludzkiego

[38] Aktualnie w SZ RP trwają prace nad utworzeniem bazy danych emiterów promieniowania radiolokacyjnego.

(*man-in-the-loop*) na całkowitą skuteczność samoobrony statku powietrznego. Wyniki testów stanowią podstawę do ewentualnych zmian w oprogramowaniu oraz wytycznych odnośnie do zachowań pilotów, np. określonych manewrów, czasów na podjęcie decyzji itp.

W trakcie prowadzenia działań (etap 5) konieczna jest ciągła weryfikacja i aktualizacja oprogramowania systemów samoobrony. Po wykonaniu każdej misji należy dokładnie przeanalizować dane z urządzeń rozpoznawczo-ostrzegawczych w celu wyszukiwania nowych zagrożeń oraz nowych modów pracy i parametrów. Dane dotyczące nowych zagrożeń należy pozyskiwać również z innych źródeł (sojuszniczych systemów rozpoznania elektronicznego oraz innych źródeł rozpoznania, np. rozpoznania osobowego). W przypadku, gdy doszło do użycia systemu samoobrony, należy dokładnie ocenić reakcję systemu oraz przyczyny ewentualnej nieskuteczności. Bardzo ważne są analizy ukierunkowane na ocenę czynników, które przyczyniły się do uniknięcia zagrożenia. Należy ocenić, czy było to wynikiem prawidłowej pracy urządzeń WE, właściwej reakcji pilota, czy też jednego i drugiego. Należy również uwzględnić hipotezy związane z nieprawidłową pracą urządzeń naprowadzających zestawu rakietowego lub błędami operatora. Analiza zagrożeń oraz funkcjonowania systemów samoobrony pozwoli na odpowiednie rekonfigurowanie urządzeń ostrzegawczych i zakłócających oraz adaptację taktyki działania poszczególnych typów statków powietrznych.

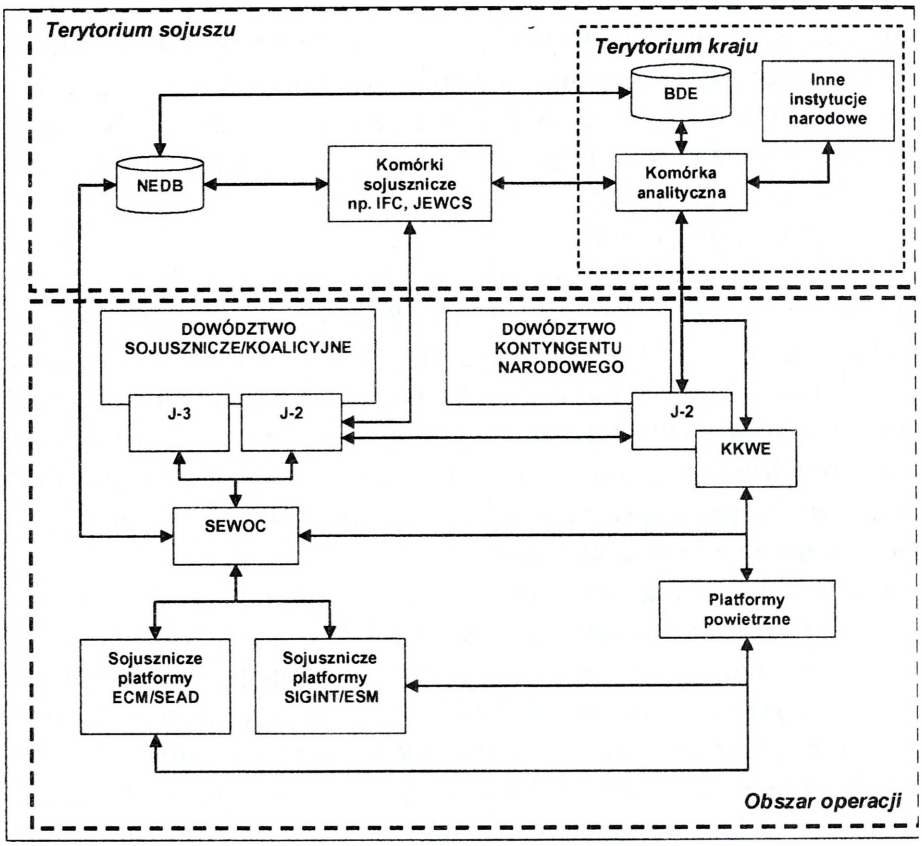
Po zakończeniu operacji w pierwszej kolejności należy dokonać powtórnej, szczegółowej analizy wszystkich danych zebranych podczas trwania operacji oraz przeprowadzić kompleksową ocenę skuteczności systemów samoobrony. Dane (parametry zagrożeń) powinny zostać ponownie zweryfikowane, a następnie wykorzystane w narodowej bazie danych emiterów BDE poprzez wprowadzenie nowych zagrożeń lub aktualizację i uzupełnienie zagrożeń już ujętych.

Ostatnim etapem przedstawionej procedury powinno być opracowanie raportu zawierającego wnioski i rekomendacje dotyczące przygotowania i użycia systemów samoobrony oraz taktyki działania poszczególnych typów statków powietrznych w odniesieniu do określonych zagrożeń. Raport powinien stanowić podstawę do planowania i organizacji kolejnych operacji poza terytorium kraju. Wskazane powinny być również kierunki modernizacji technicznej systemów samoobrony, jak również wytyczne odnośnie do szkolenia pilotów oraz naziemnego personelu rozpoznania i WE.

Struktura systemu walki elektronicznej oraz zabezpieczenie rozpoznawcze

Zadania mające na celu zabezpieczenie funkcjonowania systemów samoobrony statków powietrznych w trakcie operacji reagowania kryzysowego poza terytorium kraju realizowane będą przez wydzielone elementy systemu WE rozwinięte zarówno na obszarze operacji, jak i na terytorium kraju. Struktura systemu WE będzie bezpośrednio związana ze strukturą dowodzenia kontyngentu narodowego wydzielonego do udziału w operacji.

Wariant organizacji takiego systemu oraz powiązania informacyjne w ramach kontyngentu narodowego i sił sojuszniczych/koalicyjnych przedstawiono na rysunku 3. Kluczowym elementem tak zbudowanego systemu WE jest komórka koordynacji walki elektronicznej (KKWE), utworzona na szczeblu dowództwa kontyngentu narodowego i podległa komórce rozpoznawczej J2 tego dowództwa[39]. Głównym zadaniem KKWE jest koordynacja całości przedsięwzięć z zakresu WE (rozpoznania, przeciwdziałania i obrony elektronicznej) prowadzonych przez siły i środki kontyngentu[40]. Do zabezpieczenia funkcjonowania systemów samoobrony (etap 5 przedstawionej wcześniej procedury) powinna być wyznaczona grupa oficerów ze składu sił powietrznych.



Opracowanie własne.

Rys. 3. Organizacja systemu WE w operacji poza terytorium kraju z uwzględnieniem realizacji zadań na potrzeby systemów samoobrony platform powietrznych

[39] W przypadku utworzenia narodowego komponentu powietrznego możliwe jest również zorganizowanie KKWE w ramach komórki rozpoznawczej A2, która powinna być odpowiedzialna za realizację zadań na rzecz samoobrony statków powietrznych. Powiązania informacyjne przedstawione na rys. 3 nie ulegną jednak zmianie, ponieważ wszelkie działania powinny być koordynowane i realizowane poprzez KKWE na szczeblu J2, dlatego na schemacie pominięto ewentualny szczebel komponentu powietrznego.

[40] W celu bardziej szczegółowego zapoznania się z zadaniami KKWE zob. *Walka elektroniczna*, Szt. Gen., 1549/2003, *AJP-3.6 – Allied Joint Electronic Warfare Doctrine*, NSA 2003.

W zakresie oceny i prognozy zagrożeń KKWE powinna współpracować z instytucjami narodowym i sojuszniczymi poprzez J2, które powinno być w stałym kontakcie z J2 dowództwa międzynarodowego oraz instytucjami sojuszniczymi, np. Centrum Analiz Wywiadowczych IFC (*Intelligence Fusion Centre*), i narodowymi (komórki rozpoznania SZ RP, Służba Wywiadu Wojskowego, Służba Kontrwywiadu Wojskowego, Agencja Wywiadu itd.). Z kolei na potrzeby oceny sytuacji elektronicznej oraz zabezpieczenia funkcjonowania systemów samoobrony zasadniczym źródłem informacji będzie Centrum Operacji Wywiadu i Walki Elektronicznej SEWOC (*Signals Intelligence/Electronic Warfare Operations Centre*). Głównym produktem otrzymywanym z SEWOC powinno być uaktualniane w czasie zbliżonym do rzeczywistego EOB. Do SEWOC przesyłane powinny być dane zebrane przez narodowe systemy WE, w tym systemy samoobrony statków powietrznych oraz RFI dotyczące zabezpieczenia systemów samoobrony w przypadku, gdy konieczne informacje nie zostały uzyskane w układzie narodowym. Na tej podstawie w KKWE dokonywana powinna być bieżąca aktualizacja własnego EOB oraz bibliotek zagrożeń na obszarze operacji.

Na terytorium kraju powinna zostać wydzielona dedykowana komórka analityczna mająca możliwość przesyłania i otrzymywania danych z KKWE poprzez niejawne systemy łączności (np. satelitarnej). Komórka analityczna na terenie kraju korzystałaby z zasobów BDE, NEDB oraz z pomocy fachowej ze strony instytucji sojuszniczych i narodowych. Pozwoliłoby to na prowadzenie wielu szczegółowych analiz na terenie kraju i natychmiastowe przesyłanie ich wyników do KKWE (tzw. *reachback capabilities*) bez konieczności transportu dużej ilości wykwalifikowanej kadry i specjalistycznego sprzętu w rejon operacji. Takie rozwiązanie jest bardzo efektywne i jednocześnie stosunkowo tanie.

Załogi narodowych platform powietrznych realizujących zadania na obszarze operacji na bieżąco informowane są przez KKWE o sytuacji elektronicznej i potencjalnych zagrożeniach. W trakcie wykonywania misji, w sytuacjach nagłego zagrożenia (tzw. *pop-up threats*), możliwe jest przekazywanie informacji bezpośrednio z sojuszniczych platform wywiadu i rozpoznania elektronicznego SIGINT/ESM (*Electronic Support Measures*) oraz wsparcie ze strony samolotów przeciwdziałania elektronicznego ECM (*Electronic Countermeasures*) lub przełamania obrony powietrznej SEAD (*Suppression of Enemy Air Defense*).

Dla zapewnienia sprawnej realizacji wszystkich powyższych zadań KKWE powinna być wyposażona w niezbędny sprzęt łączności oraz teleinformatyczny. Na potrzeby wymiany danych z sojuszniczymi i narodowymi komórkami rozpoznania i WE komórka J2, w tym również KKWE, powinna mieć zapewniony m.in. dostęp do następujących sieci teleinformatycznych: CRONOS (*Crisis Response Operations NATO Open System*), BICES (*Battlefield Intelligence Collection and Exploitation System*) oraz COINS (*Communications and Information System*).

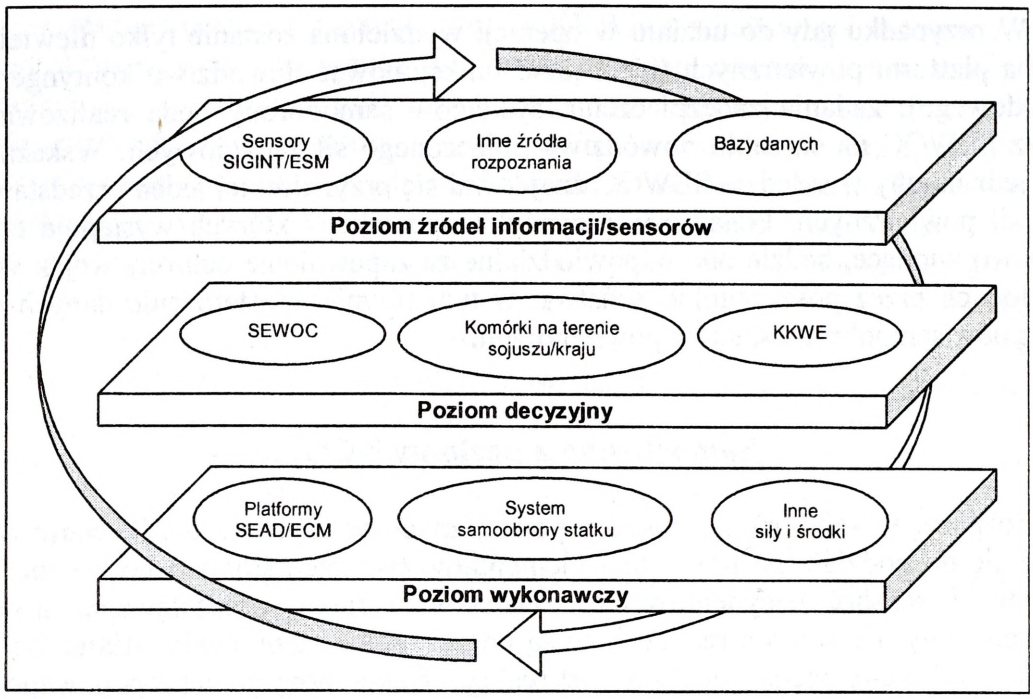
W przypadku gdy do udziału w operacji wydzielona zostanie tylko niewielka liczba platform powietrznych (nie będzie funkcjonować dowództwo kontyngentu narodowego), zadania zabezpieczenia systemów samoobrony będą realizowane przez SEWOC na szczeblu dowództwa połączonego sił zadaniowych. Wskazane jest jednak, aby w składzie SEWOC znajdował się przynajmniej jeden przedstawiciel sił powietrznych. Ponadto w przypadku operacji, w których występuje tzw. państwo wiodące, będzie ono odpowiedzialne za zapewnienie ochrony wojsk wydzielonych przez poszczególne państwa, w tym również dostarczenie danych do systemów samoobrony statków powietrznych.

Samoobrona a poziomy NCO

Rozpatrując samoobronę statków powietrznych w aspekcie NCO, warto odnieść się do podziału na trzy grupy elementarne tworzące środowisko sieciocentryczne, tj. sensory, decydentów i wykonawców. Z reguły przedstawiane są one jako poziomy, na których realizowane są poszczególne etapy cyklu działań bojowych – wykrycie, ocena i decyzja oraz reakcja. Dekompozycja zaproponowanego powyżej systemu WE, zabezpieczającego przygotowanie i prowadzenie samoobrony przez statki powietrzne zgodnie z poziomami NCO, przedstawiona jest na rysunku 4. Poziom sensorów tworzą powietrzne platformy SIGINT/ESM oraz inne źródła rozpoznania naziemnego, morskiego i powietrznego. Na tym poziomie umiejscowiono również bazy danych (BDE, NEDB, EOB i inne), które nie są sensu stricto sensorami do gromadzenia danych, ale są źródłem informacji oraz wspomagają ocenę sytuacji i wypracowywanie wniosków na kolejnym poziomie – decyzyjnym, składającym się z KKWE, SEWOC oraz wpierających komórek analitycznych na terytorium sojuszu/kraju w ramach *reachback capabilities*. Koncepcja *reachback capabilities* jest jednocześnie implementacją jednej z głównych zasad NCO – tzw. wirtualnej współpracy (*virtual collaboration*)[41]. Poziom wykonawczy to głównie system samoobrony statku powietrznego, ale również wszelkie siły i środki SEAD/WE oraz innego rodzaju oddziaływania zdolne do neutralizacji zagrożenia dla statku powietrznego, np. siły specjalne.

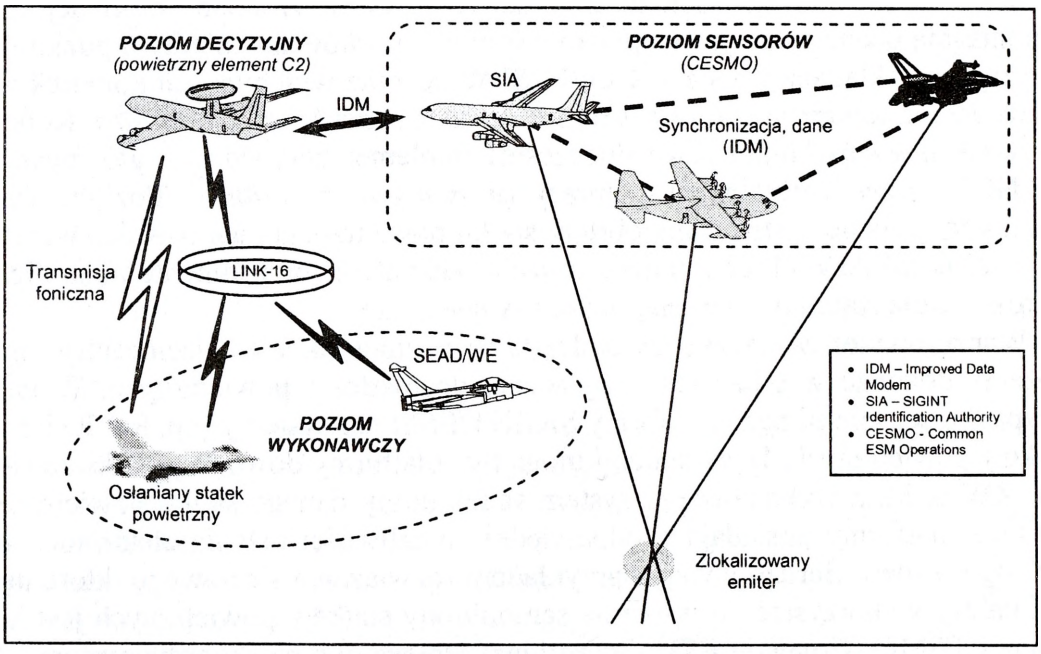
Warto również zaznaczyć, że podziału na poziomy działań sieciocentrycznych możemy dokonać w odniesieniu wyłącznie do platform powietrznych. W takim przypadku sensorami będą platformy SIGINT/ESM lub systemy (np. RWR) innych statków powietrznych. Decydentami mogą być platformy dowodzenia i kierowania (np. AWACS), a wykonawcami system samoobrony danego statku powietrznego lub inne platformy posiadające odpowiednie możliwości rażenia elektronicznego i/lub ogniowego. Bardzo dobrym przykładem rozwiązania sieciowego, które można i należy wykorzystać do wsparcia samoobrony statków powietrznych jest koncepcja CESMO (*Common ESM Operations*). Polega ona na skoordynowanym dyżurowaniu kilku platform powietrznych nad danym obszarem operacji i prowadzeniu przez nie zsynchronizowanego rozpoznania i namierzania wykrytych emiterów.

[41] Zob. D.S. Alberts, J.J. Garstka, F.P. Stein, *Network*..., wyd. cyt., s. 108–111.



Opracowanie własne.

Rys. 4. Organizacja systemu WE na potrzeby samoobrony statków powietrznych w ujęciu poziomów działań sieciocentrycznych



Opracowanie własne.

Rys. 5. Idea wykorzystania CESMO na potrzeby wsparcia samoobrony statku powietrznego

Dane z poszczególnych platform prowadzących CESMO przesyłane są do platformy głównej, tzw. SIA (*SIGINT Identification Authority*)[42], która dokonuje kojarzenia danych oraz ustala rodzaj i lokalizację emitera. Następnie SIA przekazuje informacje do odpowiedniego powietrznego lub naziemnego elementu dowodzenia C2 (*Command and Control*), który może rozesłać ostrzeżenie o wykrytym zagrożeniu i jego rodzaju (parametrach) do pozostałych użytkowników przestrzeni powietrznej. W ten sposób dane z CESMO, a więc z poziomu sensorów, przekazywane są poprzez poziom decyzyjny C2 do poziomu wykonawczego (platform prowadzących w danej chwili misje lub platform wspierających – SEAD/WE) w czasie zbliżonym do rzeczywistego. Do dystrybucji danych można wykorzystać standard Link-16 lub dedykowany kanał fonicznej łączności radiowej. Tak utworzona struktura sieciowa platform powietrznych (przedstawiona na rys. 5) jest zgodna z koncepcją NCO i pozwala na wsparcie systemów samoobrony statków powietrznych na danym obszarze operacji.

Podsumowanie

Mając na uwadze koncepcje rozwoju sił powietrznych, modernizację techniczną oraz pozyskiwane nowe zdolności operacyjne, a wreszcie zobowiązania sojusznicze, należy przypuszczać, że w najbliższej przyszłości zaangażowanie sił powietrznych w przeciwdziałanie sytuacjom kryzysowym poza terytorium RP będzie wzrastać. Dlatego też wychodząc naprzeciw nowym wymaganiom, należy kontynuować proces transformacji WE w SP RP w celu uzyskania zdolności sieciocentrycznych, w tym również na potrzeby prowadzenia operacji reagowania kryzysowego poza terytorium kraju. W ramach tego jednym z priorytetowych przedsięwzięć powinno być zabezpieczenie systemów samoobrony statków powietrznych. Samoobrona pozostaje bowiem zgodna z restrykcyjnymi zasadami użycia siły ROE obowiązującymi w operacjach reagowania kryzysowego, stanowiąc jednocześnie jeden z zasadniczych środków zapewniających zminimalizowanie strat, tak niepożądanych w tego rodzaju operacjach.

Sieciocentryczność to koncepcja, która stwarza nowe możliwości i w pewnym sensie rozszerza pojęcie systemu samoobrony statku powietrznego. Właściwe wykorzystywanie trzech głównych filarów NCO (ciągłego rozpoznania, szybkich połączeń sieciowych oraz zdolności do natychmiastowych działań bojowych[43]) umożliwia współdziałanie wszystkich komórek i platform zabezpieczających funkcjonowanie systemów samoobrony na teatrze działań. Pozwala to na ciągłe monitorowanie sytuacji elektronicznej, porównywanie jej z zasobami w posiadanych bazach danych, uzupełnianie bibliotek zagrożeń systemów samoobrony, jak również

[42] Aktualnie do przesyłania danych pomiędzy platformami realizującymi CESMO oraz do naziemnych i powietrznych elementów C2 testowana jest technologia IDM (*Improved Data Modem*).

[43] Zob. C. Kopp, *NCW 101 Networked Operations*, Part 1 – *Network Centric Fundamentals*, „Defense Today", May 2005.

ostrzeganie o zagrożeniu oraz ewentualne wsparcie statków powietrznych w jego neutralizacji. W obecnych czasach bowiem statek powietrzny nie może być pozostawiony na obszarze operacji sam sobie. Jego system samoobrony powinien korzystać z własnej biblioteki zagrożeń zdefiniowanej przed misją oraz w równym stopniu z informacji przekazywanych, w czasie rzeczywistym, z innych statków powietrznych oraz elementów naziemnych. Taka kooperacja (współpraca wirtualna) pozwala postrzegać samoobronę w szerszym sensie, jako zespół kompleksowych przedsięwzięć zwiększających żywotność statków powietrznych, w które zaangażowanych jest wiele komponentów systemu rozpoznania i WE działających w środowisku sieciocentrycznym.

Bibliografia

AFPAM 14-118 – *Aerospace Intelligence Preparation of the Battlespace*, Departament of the Air Force 2001.

AJP-3.4 – *Non-Article 5 Crisis Response Operations*, MAS NATO 2004.

AJP-3.6 – *Allied Joint Electronic Warfare Doctrine*, NSA 2003.

Alberts D.S., Garstka J.J., Stein F.P., *Network Centric Warfare – Developing and Levering Information Superiority*, CCRP, Waszyngton 2000.

Chojnacki Z., Dymanowski K., Ponczyński P., *Połączone informacyjne przygotowanie przestrzeni operacji*, „Myśl Wojskowa" 2007, nr 1.

Dymanowski K., *Przełamanie obrony powietrznej przeciwnika*, „Przegląd Sił Powietrznych" 2007, nr 1.

F-16 Avionics Technician Training Package – Penetration Aids and ECM Systems, Air Force Training Center Kjevik.

JP 2-0 – *Joint Intelligence*, Joint Staff 2007.

Kopp C., *NCW 101 Networked Operations*, Part 1 – *Network Centric Fundamentals*, „Defense Today", May 2005.

Lambeth B.S., *Kosovo and the Continuing SEAD Challenge*, „Aerospace Power Journal", Summer 2002.

Marszałek M., *Siły powietrzne w operacjach reagowania kryzysowego*, rozprawa habilitacyjna, „Zeszyty Naukowe AON", Warszawa 2007.

Price A., *The History of US Electronic Warfare*, Vol. III, AOC 2000.

Schechter E., *Mixed Signals*, „C4ISR – The Journal of Net-Centric Warfare", Vol. 6, No. 8, September 2007.

Schroeder M., *Rogue Missiles – Tracking MANPADS Proliferation Trends*, „Jane's Intelligence Review", November 2007.

Walka elektroniczna, Szt. Gen. 1549/2003.

Kpt. mgr Szymon MARKIEWICZ
Student Podyplomowych Studiów Operacyjno-Taktycznych

ZASADY WALKI ELEKTRONICZNEJ W DZIAŁANIACH SIECIOCENTRYCZNYCH

Każde sprawne działanie oparte jest na sprawdzonych wcześniej, wypracowanych naukowo prawach, rządzących badaną dziedziną wiedzy lub praktycznej działalności człowieka. Podobnie jest również w dziedzinie wojskowości, gdzie na podstawie doświadczeń (konfliktów zbrojnych dotychczas prowadzonych), badania przyczyn porażki lub zwycięstwa, stosowanych metod walki i środków rażenia wypracowywane są prawa walki zbrojnej. Są efektem poszukiwania uogólnień odnoszących się do wszelkich form świadomego i celowego działania, rozpatrywanego ze względu na sprawność, czyli konstruowanie i uzasadnianie dyrektyw praktycznych do dalszego stosowania.

Wynik wojen i bitew nie jest dziełem przypadku, lecz zazwyczaj efektem przemyślanych działań, na które wpływa wiele zmiennych czynników, których oddziaływania do końca nie da się przewidzieć[44]. Należy brać pod uwagę czynniki decydujące i warunkujące bezpośrednio przebieg walki zbrojnej, w której występują pewne prawidłowości, rozumiane jako: „***obiektywne, stale powtarzające się relacje cech i zdarzeń w niej zachodzących***"[45]. Gdy zostaną poznane i wszechstronnie zbadane, przyjmują postać **praw walki** rozumianych jako: „***stałe, występujące zawsze w określonych warunkach zależności rzeczy lub zdarzeń, uświadomiona prawidłowość walki***"[46].

Ogólnie, zasada rozumiana jest jako: „*teza, w której treści zawarte jest prawo rządzące jakimiś procesami; podstawa, na której coś się opiera, reguła*"[47]. Natomiast zasady sztuki wojennej przedstawiane są jako: „*ogólne normy racjonalnego i skutecznego postępowania dowódców i oficerów sztabu oraz działania wojsk w okresie przygotowania i prowadzenia operacji (walki, bitwy); podstawowe idee i reguły, według których prowadzi się działania wojenne; stanowią one jednocześnie kryterium oceny prawidłowego przebiegu działań wojennych*"[48].

Według S. Kozieja zasady sztuki wojennej: „*są to historycznie ukształtowane reguły przygotowania i prowadzenia zbrojnych działań wojennych, będące podstawą racjonalnej działalności dowództw i wojsk w skali taktycznej, operacyjnej i strategicznej. Stosowanie ich jest niezbędnym warunkiem uzyskania, utrzymania i wykorzystania przewagi ilościowej i jakościowej (w tym sytuacyjnej) nad prze-*

---

[44] J. Zieliński, *Zasady sztuki wojennej. Operacyjne aspekty*, AON, Warszawa 1994, s. 14.
[45] Tamże.
[46] A. Polak, *Praktyczny wymiar zasad sztuki wojennej*, AON, Warszawa 2003, s. 10.
[47] *Słownik języka polskiego*, PWN, Warszawa 2003, płyta CD.
[48] *Leksykon wiedzy wojskowej*, Warszawa 1979, s. 517.

ciwnikiem, by przy jak najmniejszych stratach własnych osiągnąć cel walki, operacji i kampanii (wojny) w możliwie najkrótszym czasie"[49].

Można zauważyć, że w kolejnych konfliktach zbrojnych tworzono nowe lub inaczej stosowano istniejące zasady. Stosowanie tego samego układu działania lub naśladowanie innych skazywało na klęskę. Z. Galewski w „Czynnikach powodzenia we współczesnej walce" stwierdził, że „(...) *zasady starzeją się. Tak było zawsze, dlatego każda kolejna wojna weryfikowała reguły przydatne w czasie trwania swojej poprzedniczki*"[50]. Wynika to ze zmian sposobów walki i rozwoju wykorzystywanych środków. Z tego też powodu zasady sztuki wojennej, a zarazem zasady walki elektronicznej można uważać za kategorię podlegającą ewolucji w zależności od rozwoju środków i form walki zbrojnej.

Z. Galewski twierdzi, że „*zasady wyrażają prawdy niezwykle ogólne, co podnosi ich uniwersalność, czyniąc przydatnymi niezależnie od rodzaju działań i sytuacji, ale płacą za to wysoką cenę: zachowując wiarygodność, zyskują opinię niewiele mówiących ogólników*". Ponadto zauważa, że są „*bezdyskusyjnymi przesłankami sukcesu*", ale pod warunkiem, że „(...) *w lakoniczną wymowę ich nazw wkłada się odpowiednią treść*"[51], czyli odpowiednie ich zastosowanie – nie same zasady – może prowadzić do osiągnięcia sukcesu.

Można zauważyć, że dobór treści odpowiadających określonej zasadzie będą warunkowały takie czynniki, jak: obszar, przeciwnik, sytuacja, czas i informacja. Dlatego też należy określić, które zasady mają w obecnej chwili największe znaczenie, w zależności od sytuacji i sposobu działania, oraz jakie treści one kryją w sobie.

Obowiązujące zasady sztuki wojennej i walki elektronicznej

Współcześni nam teoretycy związani z polskim nurtem akademickim prezentują również różne podejścia do zasad sztuki wojennej. I tak B. Chocha, rozpatrując kwestie walki taktycznej, wyróżnił zasady taktyki, do których zaliczył: inicjatywę, zaskoczenie – ryzyko i fortel wojenny, przewagę, masowanie wysiłku, rozśrodkowanie, ruchliwość i aktywność, zdecydowanie i ciągłość działań, ogień i manewr, żywotność i odporność wojsk[52]. F. Skibiński wyróżnia następujące: cel, koncentracja wysiłku, ekonomia sił, manewr, prostota, natarcie, zaskoczenie, swoboda działania, jedność dowodzenia[53]. Z kolei S. Koziej – oprócz przewagi, którą traktuje jako „zasadę zasad" lub „superzasadę" – wyróżnia następujące zasady sztuki wojennej: celowość działania, ekonomia sił, zaskoczenie, inicjatywa (aktywność),

[49] S. Koziej, *Teoria sztuki wojennej*, Warszawa 1993, s. 68.
[50] Z. Galewski, *Czynniki powodzenia we współczesnej walce*, Warszawa 1986, s. 152.
[51] Tamże, s. 152–154.
[52] B. Chocha, *Rozważania o taktyce*, WMON, Warszawa 1982, s. 40–64.
[53] F. Skibiński, *Rozważania o sztuce wojennej*, WIH, Warszawa 1990, s. 441–463.

manewr, synergiczność – osiągana w rezultacie współdziałania, utrzymanie zdolności bojowej wojsk[54].

Walka elektroniczna jako składowa walki zbrojnej zawiera pewne właściwości i cechy charakterystyczne tylko dla niej, co nie oznacza, że nie powstały na ogólnie przyjętych zasadach walki. W jej realizacji obowiązują reguły wynikające z ogólnych zasad sztuki wojennej, które z kolei wynikają bezpośrednio z praw walki zbrojnej. Można zatem stwierdzić, że zasady sztuki wojennej są nadrzędne w stosunku do zasad walki elektronicznej.

Zasady walki elektronicznej *„to grupa czynników (tj. twierdzenia, reguły, prawidłowości, wytyczne, wskazówki) wywodzących się z tradycji prowadzenia WE, opracowanych teoretycznie i stosowanych w praktyce, które określają racjonalne sposoby działania i współdziałania podsystemów WE podczas przygotowania i prowadzenia działań"*[55].

Do ogólnych zasad prowadzenia walki elektronicznej[56] zaliczano: celowość, terminowość, zaskoczenie, kompleksowość, ciągłość i skrytość jej prowadzenia oraz żywotność. Zasady te rozumiane są następująco:

– celowość – zgodność przedsięwzięć WE z zamiarem działań bojowych oraz wykorzystanie sił i środków zgodnie z ich możliwościami operacyjno-technicznymi;

– terminowość – realizowanie zadań WE zgodnie z terminami zawartymi w planie operacji podlegającym korektom w zależności od rozwoju sytuacji operacyjnej (bojowej) i elektronicznej;

– zaskoczenie – wykonanie zadań WE w sposób uniemożliwiający przeciwnikowi natychmiastowe zastosowanie skutecznych przedsięwzięć obrony elektronicznej (nieoczekiwanie dla przeciwnika pod względem terminu, sposobu, sił i środków, kierunku, obszaru itd.);

– kompleksowość – polega na skumulowanym, celowym użyciu, w określonym przedziale czasowym i obszarze, wszystkich składowych WE, z zastosowaniem najbardziej efektywnych metod i sposobów, z użyciem optymalnej ilości różnorodnych sił i środków;

– ciągłość oddziaływania elektronicznego – realizowanie zadań w sposób nieprzerwany, z intensywnością dostosowaną do potrzeb operacyjnych i bojowych;

– skrytość – przygotowanie i wykorzystanie sił i środków WE eliminujące do minimum ich przedwczesne wykrycie i lokalizację;

– żywotność systemu WE – jego odporność i zdolność do sprawnego odtworzenia gotowości w warunkach prowadzenia działań na współczesnym polu walki.

---

[54] S. Koziej, wyd. cyt., s. 72.

[55] M. Łokociejewski, W. Scheffs, *Walka elektroniczna w operacji i walce*, AON, Warszawa 2005, s. 28.

[56] W instrukcji *Walka elektroniczna*, SGWP, Warszawa 2003, s. 21, 22 określane są jako czynniki warunkujące skuteczność WE.

W literaturze przedmiotu można również odnaleźć inne zasady walki elektronicznej[57], choć podobne w brzmieniu, to jednak znaczeniowo różniące się. Do nich zaliczyć można:

– ciągłość oddziaływania elektronicznego i ogniowego,

– zmasowane i kompleksowe użycie środków WE, zsynchronizowane z działalnością ogniową,

– skrytość rozpoznania elektronicznego,

– kompleksowość przedsięwzięć obrony elektronicznej.

Analizując literaturę dotyczącą działań sieciocentrycznych, można wyróżnić następujące ich zasady[58]:

1) walka w pierwszej kolejności o przewagę informacyjną (*fight first for information superiority*);

2) dostęp do informacji: udział świadomości (*access to information: shared awareness*);

3) szybki cykl dowodzenia i decydowania (*speed of coomand and decision making*);

4) samosynchronizacja (*Self-synchronization*);

5) rozproszenie sił: nielinearne działanie (*dispersed forces: non-contiguous operations*);

6) dekoncentracja sił w przestrzeni (*demassification*);

7) masowe użycie sensorów (*deep sensor reach*);

8) zmiana warunków początkowych: wykorzystywanie tempa zmian (*alter initial conditions at higher rates of change*);

9) kompresja poziomów działań zbrojnych (*compressed operations and levels of war*).

Ad. 1) Walka w pierwszej kolejności o przewagę informacyjną

Pod pojęciem przewagi informacyjnej rozumiana jest zazwyczaj „(...) *zdolność do zbierania, gromadzenia, przetwarzania, analizowania i dystrybucji informacji, utrzymania nieprzerwanego strumienia ich przepływu oraz pełnego ich wykorzystania, przy jednoczesnym posiadaniu możliwości wzbraniania przeciwnikowi prowadzenia podobnej działalności informacyjnej* (...)"[59]. Przy takim definiowaniu przewagi informacyjnej można stwierdzić, że istotą tej zasady jest zdobywanie przewagi poprzez zapewnienie terminowej, dokładnej oraz rzeczowej informacji.

---

[57] J. Janczak, *Walka elektroniczna w działaniach taktycznych wojsk lądowych*, AON, Warszawa 1999, s. 22–30.

[58] *The Implementation of Network – Centric Warfare*, Office of Force Transformation Office of the Secretary of Defense, Washington 2004, s. 8–10.

[59] *JP 3-13 – Joint Doctrine for Information Operations*, Department of Defense, Washington 1998; za L. Konopka, *Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości*, „Myśl Wojskowa" 2004, nr 2, s. 67.

Ad. 2) Dostęp do informacji

Istotą tej zasady jest zapewnienie szybkiego, prostego i bezpiecznego dostępu użytkowników do informacji bez względu na poziom działań, celem zapewnienia odpowiedniego poziomu wspólnego postrzegania sytuacji operacyjno-taktycznej.

Ad. 3) Szybki cykl dowodzenia i decydowania

Istotą tej zasady jest minimalizowanie czasu od otrzymania zadania do podjęcia decyzji. Polega na wykorzystaniu przewagi informacyjnej przez siły własne. Szybkie wykrycie (poprzez stosowanie szeroko pojętego rozpoznania) i pełny obraz przestrzeni walki zapewnią szybką realizację procedur dowodzenia. To, co nie jest możliwe przy realizacji dotychczasowych rozwiązań, oraz ryzyko związane z podejmowaniem decyzji powinno być zminimalizowane poprzez większą świadomość faktów zaistniałych w przestrzeni walki.

Ad. 4) Samosynchronizacja

Istotą tej zasady jest zdolność sił niższych szczebli dowodzenia do prowadzenia działań samodzielnie, samodzielnego dostosowywania swych zadań w zależności od zaistniałej sytuacji, na podstawie ciągłej świadomości rozwoju sytuacji kształtowanej poprzez dostęp do terminowej i pewnej informacji. Należy jednak nadmienić, że działania te muszą być zgodne z myślą przewodnią dowódcy.

Ad. 5) Rozproszenie sił: nielinearne działanie

Założeniem tej zasady jest kontrola nad terenem w taki sposób, aby uniemożliwić przeciwnikowi jego wykorzystanie. Jest to zdolność do generowania na żądanie określonego potencjału bojowego i użycie go w odpowiednim miejscu i czasie.

Ad. 6) Dekoncentracja sił w przestrzeni

Istotą tej zasady jest skupienie wysiłku na efektach (zamierzonych skutkach) działań. Jest to nic innego jak dążenie do osiągania maksymalnego efektu przy wykorzystaniu minimalnego potencjału. Wykorzystanie informacji (posiadanie świadomości wydarzeń w przestrzeni walki) pozwala na zmniejszenie fizycznej koncentracji sił i środków w określonym rejonie oraz zwiększa szybkość reakcji na zaistniałą sytuację.

Ad. 7) Masowe użycie sensorów

Istotą tej zasady jest szerokie stosowanie sensorów (zarówno przestrzennie, jak i specjalistycznie) działających w przestrzeni informacyjnej (mających możliwość natychmiastowego przekazywania informacji o zmianach w przestrzeni walki), jak też rozmieszczanie ich w taki sposób, aby z całej przestrzeni walki zapewnić dopływ informacji niezbędnej dla osiągania celów. Wykorzystanie sensorów (czujników) na szeroką skalę czyni działalność rozpoznawczą skuteczniejszą.

Ad. 8) Zmiana warunków początkowych (wykorzystywanie tempa zmian)

Istotą tej zasady jest szybka identyfikacja zagrożeń oraz możliwość przekształcania ich w taki sposób, aby stały się silną stroną własnych sił. Jest to adaptowanie na własne potrzeby każdej zmiany zaistniałej w przestrzeni walki. Odnosi się to do zmian niezależnych od czynnika ludzkiego (teren w powiązaniu z pogodą), jak również do konkretnych wydarzeń zaplanowanych i realizowanych przez przeciwnika.

Ad. 9) Kompresja poziomów działań zbrojnych

Istotą tej zasady jest zacieranie różnic pomiędzy poziomami działań, jak również rodzajami sił zbrojnych. Odnosi się do prowadzenia działań połączonych na najniższych szczeblach dowodzenia. Efektem takich działań będzie osiąganie większych skutków w porównaniu do skutków uzyskanych przez poszczególne rodzaje sił zbrojnych czy rodzaje wojsk. Będzie to również większa możliwość przemieszczania i działania poszczególnych rodzajów sił zbrojnych oraz kompatybilne procedury dotyczące prowadzenia działań.

Tabela 1

Tabela porównawcza zasad

Zasady sztuki wojennej			Zasady walki elektronicznej	Zasady działań sieciocentrycznych
wg B. Chocha	wg F. Skibińskiego	wg S. Kozieja		
przewaga	cel	przewaga – superzasada	celowość	walka w pierwszej kolejności o przewagę informacyjną
zaskoczenie – ryzyko i fortel wojenny	koncentracja wysiłku	celowość działania	terminowość	dostęp do informacji: udział świadomości
inicjatywa	ekonomia sił	ekonomia sił	zaskoczenie	szybki cykl dowodzenia i decydowania
masowanie wysiłku	manewr	zaskoczenie	żywotność	samosynchronizacja
rozśrodkowanie	prostota	inicjatywa (aktywność)	ciągłość oddziaływania elektronicznego	rozproszenie sił: nielinearne działanie
ruchliwość i aktywność	natarcie	manewr	skrytość	dekoncentracja sił w przestrzeni
zdecydowanie i ciągłość działań	zaskoczenie	synergiczność	kompleksowość	masowe użycie sensorów
ogień i manewr	swoboda działania	utrzymanie zdolności bojowej wojsk		zmiana warunków początkowych (wykorzystywanie tempa zmian)
żywotność i odporność wojsk	jedność dowodzenia			kompresja poziomów działań zbrojnych

Opracowanie własne.

Podsumowanie

Występujące w literaturze zasady działań sieciocentrycznych należy traktować jako wyróżniki tych działań od działań dotychczasowych. Sieciocentryczność, jako nowa idea prowadzenia działań, jest na etapie koncepcyjnym. Nie ma możliwości wygenerowania szczegółowych zasad, które w sposób uniwersalny odnosiłyby się do całości prowadzonych działań, ponieważ nie zostały jeszcze zastosowane w wymiarze praktycznym, kompleksowo. Pomimo to zauważyć należy, że niektóre zasady walki elektronicznej, mimo ich uniwersalności, muszą zostać poddane redefiniowaniu. Ich zastosowanie w działaniach sieciocentrycznych w dotychczasowym interpretowaniu wydaje się niepełne.

Zasada terminowości powinna, moim zdaniem, obejmować czas nie tylko operacji, ale także czas poprzedzający, niezbędny na dostarczenie informacji potrzebnej do planowania operacji. Rozpoznanie elektroniczne, jako składowa WE, zdobyte informacje powinno dostarczać decydentom w czasie rzeczywistym lub zbliżonym do rzeczywistego, a jego prowadzenie powinno być realizowane z wyprzedzeniem czasowym względem innych działań.

W znaczeniu zasady kompleksowości powinno ująć się również: łączenie szczebli (strategiczny, operacyjny i taktyczny) wykorzystujących urządzenia WE, dostępność informacji na poszczególnych szczeblach dowodzenia, bez względu na szczebel organizacyjny urządzeń prowadzących WE, większą decentralizację dowodzenia, mającą na celu samoistne przekierowanie zadań w zależności od rozwoju sytuacji, wykorzystywanie nadarzających się okazji do skutecznego oddziaływania na urządzenia przeciwnika bez decyzji wyższego szczebla (jednak zgodnie z myślą przewodnią przełożonego).

W ciągłości prowadzenia oddziaływania elektronicznego znaczenia nabiera ciągłość prowadzenia rozpoznania elektronicznego, ciągłe monitorowanie sytuacji elektronicznej przeciwnika przy wykorzystaniu posiadanych sił i środków WE, celem tworzenia u decydentów świadomości przestrzeni walki.

Bibliografia

Chocha B., *Rozważania o taktyce*, WMON, Warszawa 1982.

Galewski Z., *Czynniki powodzenia we współczesnej walce*, Warszawa 1986.

Janczak J., *Walka elektroniczna w działaniach taktycznych wojsk lądowych*, AON, Warszawa 1999.

Konopka L., *Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości*, „Myśl Wojskowa" 2004, nr 2.

Koziej S., *Teoria sztuki wojennej*, Warszawa 1993.

Leksykon wiedzy wojskowej, Warszawa 1979.

Łokociejewski M., W. Scheffs, *Walka elektroniczna w operacji i walce*, AON, Warszawa 2005.

Polak A., *Praktyczny wymiar zasad sztuki wojennej*, AON, Warszawa 2003.

Skibiński F., *Rozważania o sztuce wojennej*, WIH, Warszawa 1990.

Słownik języka polskiego, PWN, Warszawa 2003, płyta CD.
The Implementation of Network – Centric Warfare, Office of Force Transformation Office of the Secretary of Defense, Washington 2004.
Zieliński J., *Zasady sztuki wojennej. Operacyjne aspekty*, AON, Warszawa 1994.

Płk dr inż. Jan POSOBIEC
Dyrektor Instytutu Wojsk Lądowych
Wydziału Zarządzania i Dowodzenia AON

WYZNACZNIKI DZIAŁAŃ SIECIOCENTRYCZNYCH

Nowoczesne rozwiązania techniczne i powiększające się możliwości wykorzystania **informacji** jako głównego czynnika sukcesu w wielu obszarach działalności ludzkiej ujawniły nowe możliwości komunikowania się ludzi oraz przyczyniły się do znaczących zmian we współczesnym świecie. W **erze informacyjnej** społeczeństw przełomu XX i XXI wieku informacja nabrała szczególnego znaczenia w teorii i praktyce sztuki wojennej, a przede wszystkim w dowodzeniu.

Wielowymiarowość, dynamizm i stale rosnące potrzeby informacyjne w operacjach militarnych prowadzonych w zróżnicowanych warunkach przez wielonarodowe siły są obecnie zjawiskiem powszechnym. Poszukiwanie sposobów pozwalających zapewnić wysoką efektywność działań zaowocowało powstaniem nowych koncepcji prowadzenia walki (wojny), w których przewiduje się **wykorzystanie walorów technologii informatycznych i telekomunikacji do zmiany oblicza i charakteru działań prowadzonych przez wysoko utechnicznione siły zbrojne**.

W efekcie takiego rozwoju sytuacji w Stanach Zjednoczonych opracowano podstawy koncepcji prowadzenia działań, w których dzięki zastosowaniu sieciowego powiązania wszystkich uczestników operacji można uzyskać większą efektywność działań. Koncepcja ta, ze względu na centralną rolę informacji, jako następstwo połączenia wielu sieci w jedną megasieć szybko uzyskała miano sieciocentrycznej, a prognozowane prowadzenie działań według jej założeń i reguł nazwano działaniami sieciocentrycznymi.

Przeprowadzone analizy literatury przedmiotu wskazują, że pierwsze udokumentowane ślady koncepcji sieciocentrycznych pojawiły się w połowie lat dziewięćdziesiątych XX wieku, kiedy to rewolucyjny wręcz rozwój elektroniki, techniki i technologii informatycznych ujawnił zupełnie nowe możliwości[60]. Zastosowanie ich w działaniach zbrojnych do zasilania informacyjnego i sterowania środkami walki zwiększyło precyzję i skuteczność rażenia. Postępująca miniaturyzacja środków rozpoznawczych i ich duża dokładność umożliwiły „podglądanie" przeciwnika, terenu z ziemi, powietrza i przestrzeni kosmicznej, a także przekazywanie informacji w czasie zbliżonym do rzeczywistego do odbiorców. Uzyskane w ten sposób dane są niezwykle istotne w działaniach, a dodatkowo pozyskiwanie ich

[60] Za twórców koncepcji sieciocentrycznych powszechnie uznaje się wiceadmirała Arthura K. Cebrowskiego oraz Johna Garstka, którzy w 1998 roku opublikowali artykuł pt. *Network Centric Warfare: Its Origins and Future* (Sieciocentryczna wojna: jej początki i przyszłość). W artykule zawarte zostały podstawowe założenia przyszłych koncepcji sieciocentrycznych.

niejako „na życzenie" użytkownika stworzyło zupełnie nowe możliwości, które przyczyniły się do wykrystalizowania się teorii działań sieciocentrycznych.

Specjaliści wojskowi, dostrzegając znaczenie **przewagi informacyjnej** funkcjonującej w wydaniu komercyjnym w środowisku cywilnym i rozumianej bardziej jako środek do ekonomicznego rozwoju i dynamicznego dostosowywania się do potrzeb rynku przez przedsiębiorstwa i firmy, dokonali adaptacji stosowanych rozwiązań do potrzeb wojskowych. Nowe sposoby i metody osiągania przewagi informacyjnej pozwalały bowiem radykalnie ją zwiększyć, również w obszarze militarnym. Przekładało się to również na efektywność działania sił zbrojnych poprzez poprawienie relacji *„zaangażowane siły – uzyskany efekt taktyczny (operacyjny, strategiczny)"*[61]. Takie podejście preferowane jest przede wszystkim w armiach wysoko rozwiniętych państw, w których rozpoczęto transformację systemów obronnych oraz sił zbrojnych, dostosowując je do wymogów koncepcji **wojny sieciocentrycznej** (*Network Centric Warfare* – NCW).

Działania sieciocentryczne szczególnie mocno akcentowane są w USA, Kanadzie, Wielkiej Brytanii, RFN, Szwecji, Australii. Ponadto, dostrzegając duże możliwości tkwiące w koncepcji działań sieciocentrycznych, podjęte zostały przez Sojusz Północnoatlantycki szeroko zakrojone programy badacze, zmierzające do zaadaptowania oraz wdrożenia ich zasadniczych założeń do praktyki NATO.

Współużytkowanie informacji źródłem siły

Dostrzegając znaczące korzyści płynące z nowej koncepcji, w siłach zbrojnych USA rozpoczęto proces jej wdrażania, a odzwierciedlenie NCW znalazło się w koncepcji transformacji zawartej w nowej doktrynie militarnej *Joint Vision 2020*, wydanej w 2000 roku. Projekty badawcze, wprowadzane w życie rozwiązania oraz kierunki transformacji sił zbrojnych USA zostały zaprezentowane w wydanej przez szefa Biura Transformacji Sił Zbrojnych A.K. Cebrowskiego książce pt. „The Implementation of Network Centric Warfare"[62].

Amerykańskie poglądy szybko zostały podchwycone przez większość wysoko rozwiniętych państw[63], które zaczęły aktywnie angażować się w rozwój rodzimych rozwiązań, zgodnych z podstawowymi założeniami NCW. Wysoka dynamika zmian oraz spodziewane korzyści w wydatny sposób przyczyniły się do tego typu podejścia. Zainicjowane badania i postępujące wdrożenia dotyczą zarówno kwestii operacyjnych, jak również typowo technicznych rozwiązań problematyki działań sieciocentrycznych. Przybrały one różnorodną formę i postać, od artykułów, publi-

---

[61] J. Wołejszo, M. Siedlecki, *Walka sieciocentryczna – wyzwaniem XXI wieku*, [w:] *System dowodzenia w środowisku sieciocentrycznym*, ZN AON 2007, nr 3(68)A.

[62] A.K. Cebrowski, *The Implementation of Network Centric Warfare*, Force Transformation, Office of the Secretary of Defense, Washington, January 2005.

[63] J. Posobiec, *Organizacja dowodzenia w środowisku sieciocentrycznym*, AON, Warszawa 2008, s. 26.

kacji książkowych dotyczących walki sieciocentrycznej do licznych odwołań i zapisów w doktrynach oraz planach transformacji sił zbrojnych. Amerykańska teoria NCW została zaadaptowana i funkcjonuje pod różnymi, często narodowymi nazwami w wielu państwach świata oraz w NATO. W społeczeństwach informacyjnych rozprzestrzenianie się nowych koncepcji nie napotyka na większe bariery. Zjawiska globalizacji, sieciowych powiązań i zależności wyraźnie ułatwiły przyswojenie i zaakceptowanie nowego kierunku rozwoju sił zbrojnych, zwłaszcza w państwach, w których świadomość wagi i znaczenia informacji jest doceniana. Poniżej przedstawiono różnorodne określenia i terminy funkcjonujące na świecie:

- w Sojuszu Północnoatlantyckim – NNEC (*NATO Network Enabled Capabilities*)[64],
- w USA – NCW (ang. *Network Centric Warfare*)[65],
- w Wielkiej Brytanii – NEC (ang. *Network Enabled Capabilities*)[66],
- w Kanadzie – NEO (ang. *Network Enabled Operations*, fr. *Les Opérations Réseaucentriques*)[67],
- we Francji – NEB (fr. *La numérisation de l'espace de bataille* lub *La Guerre Infocentre*)[68],
- w Australii – NEW (ang. *Network Enabled Warfare*)[69],
- w Republice Federalnej Niemiec – NetOpFü (niem. *Vernetzten Operationsführung*)[70],
- w Szwecji – NBD (ang. *Network Based Defence*)[71],
- w Singapurze – K-BC2 (ang. *Knowledge-Based Command and Control*)[72].

W zaprezentowanych nazwach koncepcji sieciocentrycznych, implementowanych w poszczególnych krajach, wyraźnie zauważalne jest dostosowywanie ich założeń i kierunków rozwoju do narodowych lub sojuszniczych potrzeb, możliwo-

---

[64] *Network Enabled Capability, Feasibility Study, Executive Summary: ver. 2.0*, NC3A, October 2005.

[65] A. Cebrowski, J. Garstka, *Network Centric Warfare...*, wyd. cyt. Po 2003 roku pojawiło się również pojęcie *Network Centric Operations*.

[66] *Network Enabled Capability Handbook...*, wyd. cyt.

[67] M.H. Thomson, B.D. Adams, *Network Enabled Operations: A Canadian Perspective*, Defense Research and Development Canada, Toronto 2005.

[68] *French Army and MoD Experiment Network-Enabled Operations*, www.reports.edas (wejście 18.12.2007); *Exercice de numérisation de l'espace de bataille*, Armée de Terre, www.defense.gouv.fr/terre (wejście 20.12.2007).

[69] W Australii proponowany jest również inny termin, mający zastąpić NEW: *Fourth Generation Warfare (4GW) doctrine.*

[70] S. Collmer, *Information as a Key Resource: The Influence of RMA and Network-Centric Operations on the Transformation of the German Armed Forces*, European Center For Security Studies George C. Marshall, Occasional Paper Series No. 8, February 2007, s. 13; *NetOpFü – Das Wir der Truppe*, www.luftwaffe.de. (wejście 21.12.2007).

[71] P. Nilsson, *Opportunities and risks in a Network-Based Defence*, „Swedish Journal of Military Technology" 2003, No. 3.

[72] C. Wilson, *Network Centric Warfare, Background and oversight Issues for Congress*, CRS, Washington 2004, s. 24; J. Janczak, *Uwarunkowania działań sieciocentrycznych determinujące organizację sieci teleinformatycznych*, [w:] *Sieci teleinformatyczne w działaniach sieciocentrycznych*, AON, Warszawa 2006, s. 22.

ści ekonomicznych, poziomu rozwoju technologicznego poszczególnych państw. Niemniej jednak zauważalne jest znaczne zainteresowanie tą niezwykle złożoną problematyką przyszłych działań militarnych w uwarunkowaniach XXI wieku, uznanym za wiek dominacji informacyjnej, która jest źródłem siły wysoko rozwiniętych, nowoczesnych państw i organizacji na świecie.

Podstawy koncepcji sieciocentrycznych

Dążenie do zwiększenia potencjału wyrażanego siłą bojową wojsk, w sposób pozwalający dominować nad przeciwnikiem w „informacyjnym" XXI wieku, materializowane jest w koncepcji **działań sieciocentrycznych**, którą w zgodnej opinii wielu teoretyków i praktyków wojskowych trudno jest jednoznacznie zdefiniować. W literaturze przedmiotu dotyczącej problematyki sieciocentryzmu funkcjonuje terminologia zaczerpnięta z języka angielskiego. Jest to konsekwencja formowania się podstaw koncepcji sieciocentrycznych w USA i krajach anglosaskich oraz przyjęcia języka angielskiego (obok francuskiego) jako obowiązującego w NATO. Dodatkowo tłumaczenia z języka angielskiego przyczyniają się często do powstania rozbieżności lub wręcz odmiennej interpretacji specyficznego języka i terminologii wojskowej, która opisuje działania sieciocentryczne. Koncepcje sieciocentryczne są bowiem w większości oparte na nowo tworzonych terminach i definicjach, które w dalszym ciągu podlegają nieustannym przeobrażeniom, są uzupełniane i rozwijane w wyniku prowadzonych badań oraz uzyskanych doświadczeń.

Stosownie do dokonanych ustaleń w wymiarze operacyjnym sieciocentryczności przyjmuje się następujące terminy związane z koncepcjami działań sieciocentrycznych:

Walka sieciocentryczna – WSC (*Network Centric Warfare* – NCW) – to rozwijająca się teoria działań wojennych, wyrażona poprzez zbiór reguł i zasad, które mogą być użyte do opracowania nowych sposobów prowadzenia walki. Dotyczy ona ludzkiego i organizacyjnego zachowania się w informacyjnym środowisku XXI wieku. Teoria WSC opiera się na następujących zasadach[73]:

- połączenie niezawodną siecią pozwalającą współdzielić wszelkie dane i informacje;
- współdzielenie danych i informacji poprawia ich jakość, tworzy wspólną świadomość sytuacyjną;
- wspólna świadomość sytuacyjna umożliwia współpracę i osiągnięcie samosynchronizacji, co usprawnia dowodzenie i jego szybkość.

Zakłada się, że powyższe możliwości znacząco zwiększają sprawność prowadzenia misji (operacji) przez **przygotowane pod względem technicznym, organizacyjnym i przede wszystkim „mentalnym"** zgrupowania wojsk. Często walka

[73] Por. D.S. Alberts, J.J. Garstka, F.P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, wyd. 2, CCRP Publication Series, Washington 2000, s. 87.

sieciocentryczna interpretowana jest również jako wojna sieciocentryczna, co w ocenie specjalistów uznawane jest za poprawne i uzależnione jedynie od kontekstu[74].

Zdolność sieciocentryczna (*Network Enabled Capability* – NEC)[75] – to zdolność do szybkiego i precyzyjnego osiągnięcia zamierzonego efektu operacyjnego poprzez wykorzystanie infrastruktury informacyjnej (sieci) wiążącej sensory, decydentów i środki walki. Uzależniona jest ona od możliwości pozyskania, integracji i analizy informacji w czasie zbliżonym do rzeczywistego, pozwalającej na szybkie podejmowanie decyzji oraz osiągnięcie pożądanego efektu. Dotyczy tych zdolności, które powinny posiadać siły zbrojne, jako niezbędne do wykorzystania ich pełnego potencjału bojowego poprzez powiązanie w sieć lub sieci. W opiniach specjalistów jest to europejska odmiana koncepcji działań sieciocentrycznych[76].

W Sojuszu Północnoatlantyckim powstała odmiana koncepcji sieciocentrycznej adaptująca amerykańskie i brytyjskie rozwiązania, funkcjonująca pod pojęciem **NATO Network Enabled Capability – NNEC**[77], które rozumiane jest jako osiągnięcie szczególnej zdolności do prowadzenia efektywnych działań, wynikających z kompleksowej integracji – za pośrednictwem sieci teleinformatycznych – wszystkich sił z poszczególnych państw członkowskich Sojuszu, zaangażowanych w prowadzone operacje, począwszy od poziomu strategicznego, a na poziomie taktycznym skończywszy. Zakłada się, że integracja ta zapewni osiągnięcie znacznej przewagi informacyjnej, a w konsekwencji przewagi decyzyjnej, umożliwiającej uzyskanie zamierzonego efektu operacyjnego w krótkim czasie przy efektywnym wykorzystaniu potencjału militarnego.

W Polsce funkcjonuje pojęcie **zdolność sieciocentryczna Sił Zbrojnych Rzeczypospolitej Polskiej** (ZSC SZ RP) – rozumiana jako zdolność sił zbrojnych do integracji różnych elementów środowiska operacyjnego, od poziomu strategicznego (włączając w to Dowództwo Połączonych Sił WP) do poziomu taktycznego poprzez sieć (lub sieć sieci) umożliwiającą szybkie i precyzyjne osiągnięcie zamierzonego efektu operacyjnego[78]. Osiągniecie zdolności sieciocentrycznych w obszarze operacyjnym ukierunkowane jest na następujące cele:

- samodzielność w działaniu – rób to, co w tej sytuacji należy, nie czekaj biernie na rozkazy (głębokie współdziałanie);
- dogłębne zrozumienie myśli przewodniej;

---

[74] R. Szpakowicz, *Wojna czy walka sieciocentryczna, dane czy informacja*, [w:] *Wsparcie informacyjne obrony powietrznej*, materiały z sympozjum naukowego, AON, Warszawa 2003, s. 68.

[75] Por. *Network Enabled Capability*, Joint Services Publication 777, UK Ministry of Defence, London, January 2005, s. 9.

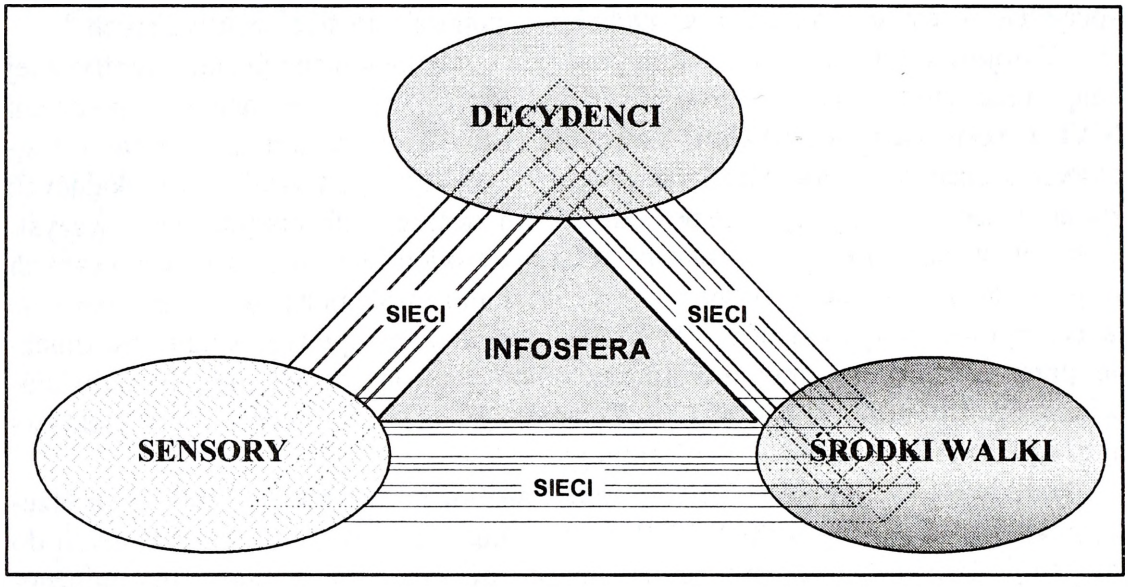
[76] A. Kącki, R. Szpakowicz, *System DUNAJ jako przykład rozwiązań wpisujących się w koncepcję działań sieciocentrycznych*, [w:] *Sieci teleinformatyczne w działaniach sieciocentrycznych*, AON, Warszawa 2007, s. 80.

[77] *Network Enabled Capability, Feasibility Study, Executive Summary*, NC3A, October 2005.

[78] Ekspertyza pt. *Wykonanie studium wykonalności projektu Network Enabled Capabilities*, Zegrze 2006, s. 72.

- zrozumienie sytuacji w przestrzeni walki na wszystkich poziomach;
- zwiększony dostęp do wspólnej wiedzy o sytuacji[79].

Podstawę działań sieciocentrycznych tworzą rozwiązania techniczne i operacyjne, które pozwalają osiągnąć nową jakość dzięki wykorzystaniu wiedzy powstałej w wyniku dostępu do danych (generujące wspólną świadomość sytuacyjną) w czasie zbliżonym prawie do rzeczywistego. Interpretację elementów koncepcji sieciocentrycznej przedstawia rysunek 1. Ideę działań sieciocentrycznych można bowiem wyrazić jako **integrację decydentów, sensorów i platform uzbrojenia w niematerialnej *przestrzeni informacyjnej* (cyberprzestrzeni), która zapewnia pełne wykorzystanie wiedzy**.



Opracowanie własne.

Rys. 1. Główne elementy współtworzące koncepcję działań sieciocentrycznych

Koncepcja zakłada, że głównym zadaniem **sieci** w działaniach sieciocentrycznych będzie dystrybucja informacji. Poprzez jej pozyskiwanie, zdobywanie, przetwarzanie i przesyłanie będą się odbywać procesy dystrybucji i odpowiedniego jej wykorzystania w środowisku operacyjnym, jak również poza nim. Ocenia się, że z jednej strony – uzyskany rezultat funkcjonowania sieci będzie miał duży wpływ na działania w przestrzeni operacyjnej, z drugiej zaś – zapewni możliwość właściwego i terminowego wsparcia oraz zabezpieczenia logistycznego działań.

Sieci przyczynią się do przepływu informacji i zapewnią możliwości efektywnego zbierania i zarządzania informacjami, co powinno doprowadzić do wyższości informacyjnej nad przeciwnikiem. Jednocześnie sieci muszą spełniać wysokie

[79] J. Kręcikij, *Istota działań sieciocentrycznych*, „Zeszyty Naukowe AON" 2004, nr 4(65), s. 128.

wymagania związane z bezpieczeństwem oraz ochroną przed atakami strony przeciwnej zarówno fizycznymi, jak i cyberatakami.

Decydenci są newralgicznym składnikiem koncepcji działań sieciocentrycznych. Odpowiednie kompetencje i predyspozycje personelu determinują w znaczącym stopniu osiąganie zdolności sieciocentrycznych. Dlatego też w wielu prognozach uwaga skupiona jest na kształceniu (szkoleniu) personelu wojskowego, tak aby mógł w pełni wykorzystać posiadaną wiedzę, umiejętności i doświadczenie. Użytkownicy powinni nie tylko znać możliwości NCW, ale i aktywnie uczestniczyć w generowaniu oraz współdzieleniu się informacją, która powinna być wykorzystana w jak największym stopniu w planowaniu oraz podejmowaniu decyzji. Wyraźnie akcentowany jest przy tym wymóg wzajemnego zaufania i konieczność polegania na współużytkownikach sieci.

Zbierane poprzez powszechne zastosowanie zróżnicowanych **sensorów** dane stają się „wirtualną bazą danych" istniejącą w infosferze. Dostępna, wiarygodna, nieustannie weryfikowana, uzupełniana i uaktualniana w czasie rzeczywistym informacja o stanie sytuacji bieżącej stworzy tzw. wspólny obraz sytuacji (*Common Operational Picture* – COP). W systemie dowodzenia wszystkich szczebli i poziomów dowodzenia będzie dostępny w każdej chwili dla funkcjonujących w systemie decydentów, z zachowaniem wymaganego stopnia dostępności i szczegółowości dla każdego z nich.

Taka zdolność do współużytkowania, współdzielenia informacji tworzących wspólną sytuację operacyjną dzięki efektywnym systemom dowodzenia i kontroli (C2) daje możliwość działania z niezwykłą efektywnością oraz pozwala wykorzystać efekt synergii, w wyniku transformacji tradycyjnych systemów walki i dowodzenia, zgodnie z założeniami i zasadami koncepcji walki sieciocentrycznej (*Network Centric Warfare*). Sprzężenie sensorów, decydentów i środków walki (wojska i środki walki) pozwala generować wzrost siły bojowej, co prowadzi do osiągnięcia możliwości[80]:

- współdzielenia świadomości sytuacyjnej,
- wzrostu szybkości dowodzenia,
- zwiększenia tempa (operacyjnego) prowadzenia działań,
- większej śmiercionośności wobec przeciwnika,
- podniesienia zdolności przetrwania sił własnych na polu walki,
- adaptacyjności do dynamicznie zmieniających się sytuacji wskutek sprzężenia szybkich cykli decyzyjnych.

Powstanie i rozwój koncepcji określanych mianem sieciocentrycznych związane są z przemianami następującymi zarówno w technologicznym rozwoju, jak i świadomości cywilizacji informatycznych. Wzrost znaczenia informacji, jej niezwykła waga – nie tylko w wypadku konfliktu zbrojnego – stały się przedmio-

[80] M.H. Thomson, B.D. Adams, *Network Enabled Operations*..., s. 6.

tem intensywnych badań i naukowych dociekań możliwości wykorzystania dorobku wielu dziedzin w procesie pozyskiwania, zarządzania, a przede wszystkim wykorzystywania informacji[81].

Struktura działań sieciocentrycznych

Sieciocentryczne środowisko tworzy nową jakość w dowodzeniu, a wielowymiarowość i złożoność zjawisk oraz specyficzne właściwości przyczyniają się do niejednoznacznego podziału przestrzeni egzemplifikujących działania sieciocentryczne. Podkreślić również należy, że nie ma w tym względzie jednolitej zgodności wśród ekspertów i znawców zagadnień sieciocentrycznych. Przeprowadzone analizy i oceny wskazują, że działania te są obecne we wszystkich wymiarach: szerokości, wysokości i głębokości pola walki. Ponadto rozciągają się również na przestrzeń elektromagnetyczną oraz tzw. przestrzeń informacyjną. W literaturze przedmiotu najczęściej spotykany jest podział na[82] domeny, sieci i warstwy.

Domena traktowana jest jako obszar, w którym występują zjawiska charakteryzujące środowisko sieciocentryczne. W ocenie autora wyjaśnia ona najbardziej istotne kwestie działań sieciocentrycznych, dlatego też zaprezentowany zostanie tylko ten podział.

Domeny obejmują materialną i niematerialną sferę wszystkich zjawisk i powiązań występujących w działaniach sieciocentrycznych. W ocenie ekspertów całokształt zjawisk urzeczywistniających działania i środowisko sieciocentryczne wyraża się w następujących trzech domenach[83] (rys. 2): fizycznej, informacyjnej oraz poznawczej.

W niektórych źródłach, zwłaszcza powstałych po 2002 roku, pojawia się jeszcze jedna domena – **socjalna**[84], która została wydzielona z domeny poznawczej. W większości koncepcji przypisywane jej zjawiska i wartości sytuowane są jednak w domenie poznawczej. Według poglądów wielu specjalistów współczesne działania militarne o charakterze sieciocentrycznym muszą być prowadzone jednocześnie we wszystkich wymienionych domenach[85]. Zachowana bowiem powinna być komplementarność i spójność działań wynikająca z wzajemnych powiązań i sprzężeń między poszczególnymi domenami.

---

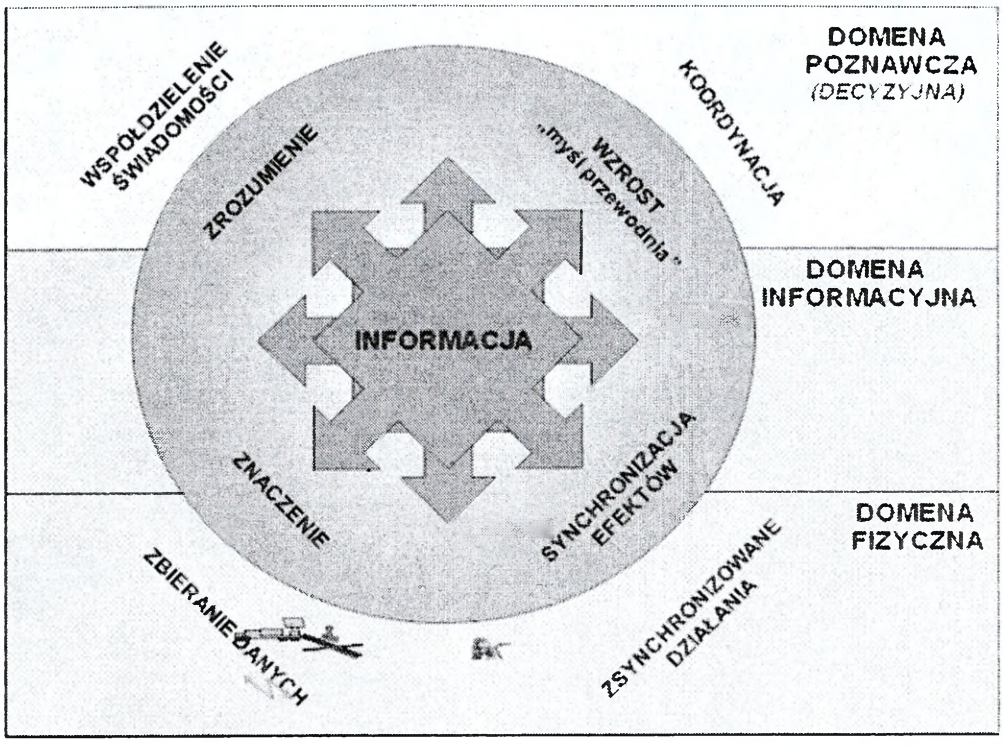
[81] L. Ciborowski, *Walka informacyjna*, Wyd. Europejskie Centrum Edukacyjne, Toruń 1999; R. Szpyra, *Militarne operacje informacyjne*, AON, Warszawa 2003; A. i H. Toffler, *Wojna i antywojna. Jak przetrwać na progu XXI wieku*, Wyd. Muza SA, Warszawa 1997; Z. Ścibiorek, *Podejmowanie decyzji*, Ulmak, Warszawa 2003; R. Kwećka, *Informacja w walce zbrojnej*, AON, Warszawa 2001; D. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, WNT, Warszawa 2002.

[82] A.L. Money, *Raport on Network Centric Warfare*..., s. 3–8; J. Wołejszo, M. Siedlecki, *Walka sieciocentryczna*..., s. 31.

[83] Por. *Network Centric Warfare, Raport to Congress, DoD*, Washington, July 2001, p. 3–8; R. Szpakowicz, *Uwarunkowania wdrażania zdolności sieciocentrycznej w Wojsku Polskim*, [w:] *Problemy automatyzacji*..., s. 31.

[84] D.S. Alberts, R.E. Hayes, *Power to the*..., s. 15; *The Implementation*..., s. 20.

[85] Por. M. Huzarski, *Istota wojny (walki)*..., s. 23.



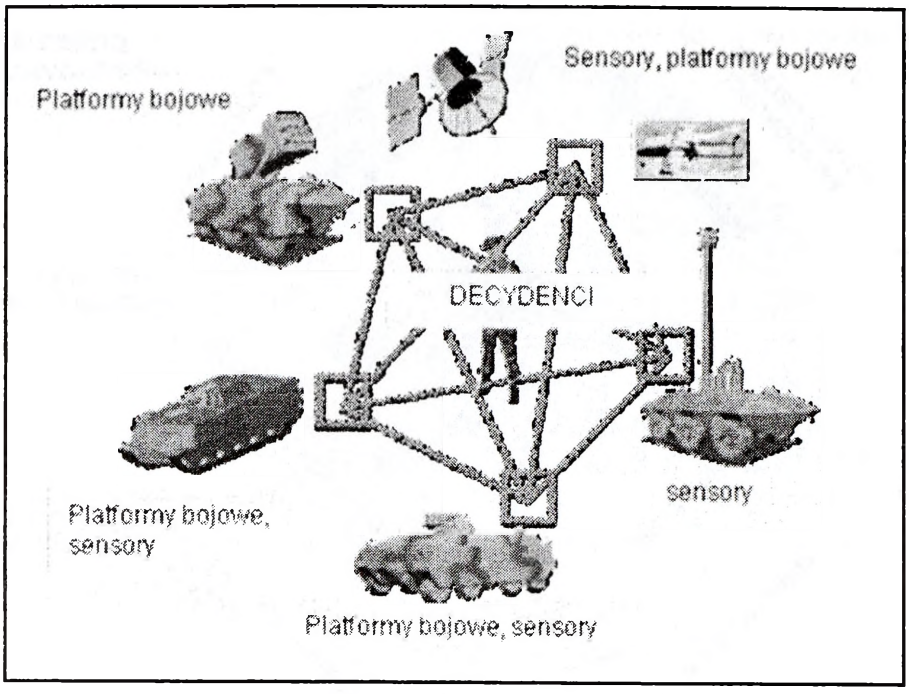
Opracowanie własne.

Rys. 2. Domeny współtworzące strukturę środowiska działań sieciocentrycznych

Domena informacyjna jest najważniejszym składnikiem egzemplifikującym dowodzenie. W niej tworzony jest wspólny obraz sytuacji oraz wytwarzana jest przewaga informacyjna nad przeciwnikiem. W domenie informacyjnej dokonywane są procesy zbierania danych, ich obróbki, przetwarzania, tworzenia i przechowywania informacji. W niej funkcjonują bazy danych (w elektronicznej formie), systemy wspomagania decyzji, następuje przepływ informacji (rozkazy, meldunki, sygnały dowodzenia, zamiary itd.) między elementami działającymi w środowisku działań sieciocentrycznych. Realizowany jest proces monitorowania i zarządzania cyberprzestrzenią działań.

Domena poznawcza (często określana też jako decyzyjna) jest trudna do zidentyfikowania i oceny[86], tworzą ją bowiem niematerialne elementy, zawierające się w tzw. czynniku ludzkim. Obejmują takie aspekty, jak: przywództwo, morale, poziom wiedzy, doświadczenie, jakość wyszkolenia, motywacja, świadomość sytuacyjna, umiejętności współpracy i działania zespołowego. W tej domenie umiejscowione są również: doktryny, teoria działania, procedury postępowania i podejmowania decyzji oraz zamiar dowódcy.

[86] R. Szpakowicz, R. Hoffmann, *Koncepcja wojny sieciocentrycznej jako odpowiedź na zapotrzebowanie sił powietrznych XXI wieku na informacyjne wsparcie działań bojowych*, PWLiOP 2003, nr 8, s. 10–11.



Opracowanie własne.

Rys. 3. Powiązania elementów koncepcji sieciocentrycznej w domenie fizycznej

Domena socjalna[87] (często traktowana jako część domeny poznawczej) – zachodzą w niej określone interakcje międzyludzkie pomiędzy wszystkimi uczestnikami działań (dowództw, podległych wojsk itp.). Ujawniają się predyspozycje do dowodzenia, pracy sztabowej personelu[88].

Atrybuty domeny poznawczej (oraz socjalnej) są niemierzalne, ale w sieciocentrycznych uwarunkowaniach najtrudniejsze do pokonania. Wymagają bowiem dokonania znaczących przeobrażeń w systemie kształcenia oficerów i użytkowników sieciocentrycznych systemów przyszłości. Sprostać bowiem muszą wysokim wymaganiom i potrzebom wynikającym z nowoczesnych technologii, procedur działania i przewartościowań założeń teoretycznych, doktryn, metod i sposobów działania dowództw w procesie dowodzenia.

W działaniach sieciocentrycznych przewaga informacyjna transponowana jest na siłę bojową poprzez połączenie dysponujących wiedzą zróżnicowanych jakościowo jednostek organizacyjnych na polu walki (często obecnie określanym również jako przestrzeń walki)[89]. To połączenie zapewnia jednak bardziej wydajne i efektywne wykorzystanie możliwości i potencjału bojowego wszystkich uczestni-

[87] *The Implementation of...*, s. 20.

[88] D. Alberts, R. Hayes, *Command Control in the Information Age*, CCRP, Washington 2003, s. 44.

[89] Z. Maślak, *Informacje w obronie powietrznej. Potrzeby, wymagania, zagrożenia*, PWLiOP 2002, nr 7, s. 24.

ków działań niż w działaniach platformocentrycznych. Ściśle związane jest to również z potrzebą dostosowania się do wysokich wymogów sieciocentrycznego pola walki.

Zasady działania w środowisku sieciocentrycznym

Wysoka wartość nowych sposobów działania wojsk warunkowana jest przestrzeganiem wielu zasad, które w literaturze przedmiotu są różnie identyfikowane[90]. W kontekście problematyki walki elektronicznej implikują one perspektywiczne przeobrażenia w działaniach wojsk. Na podstawie „The Implementation of Network – Centric Warfare" J. Kręcikij do zasad działań sieciocentrycznych zaliczył[91]:

- dążenie do zdobycia przewagi informacyjnej (wyższość informacyjna);
- dostęp do zasobów informacji spełniającej określone wymagania i pochodzącej z różnorodnych źródeł, zgodnie z potrzebami i specyfiką określonego poziomu (szczebla) dowodzenia (każdego rodzaju sił zbrojnych i wojsk);
- szybkość dowodzenia wyrażającą się w szybkich cyklach dowodzenia;
- samosynchronizację;
- nielinearne pole walki (przestrzeń działań);
- rozproszenie sił (bardziej rozumiane jako przeciwstawienie się fizycznemu i geograficznemu zmasowaniu sił i środków);
- masowe użycie sensorów;
- wykorzystywanie okazji;
- zmniejszenie różnic między poszczególnymi poziomami działań zbrojnych oraz zacieranie granic między uczestniczącymi w działaniach rodzajami sił zbrojnych i wojsk.

Przeprowadzone analizy i oceny wskazują, że sformułowane powyżej zasady powinno się postrzegać jako istotne, ogólne wskazówki[92] przy prowadzeniu działań, które wówczas uzyskają sieciocentryczny charakter w pełnym wymiarze. Należy jednak mieć na uwadze fakt, że zmieniająca się rzeczywistość i przeobrażenia wynikające z ewolucji założeń i koncepcyjnego charakteru działań sieciocentrycznych przyczyniają się do otwartości na zmiany. Ponadto powinny one być traktowane w sposób kompleksowy, bowiem są one wobec siebie komplementarne. Razem tworzą określoną całość.

Z punktu widzenia właściwości walki elektronicznej **dążenie do zdobycia przewagi informacyjnej (wyższość informacyjna)** odgrywa szczególną rolę. Oznacza ono bowiem prowadzenie operacji na danych, informacjach, wyrażające się w osiągnięciu zdolności do pozyskiwania (zbierania, zdobywania), akumulo-

---

[90] *The Implementation of Network – Centric Warfare*, Department of Defense, Washington, 2005, s. 8; M. Huzarski, *Istota wojny (walki)*..., s. 24.

[91] J. Kręcikij, *Istota działań sieciocentrycznych*..., s. 130.

[92] M. Huzarski, *Zagadnienia taktyki wojsk lądowych*, Wyd. Adam Marszałek, Toruń 1999, s. 34.

wania, przetwarzania (analizowania i oceny), dystrybucji informacji przy użyciu wszelkich dostępnych narzędzi, z wszystkich możliwych źródeł. Jednocześnie uniemożliwiane jest prowadzenie takiej samej działalności przeciwnikowi[93], w czym walka elektroniczna powinna partycypować w szczególnie istotnym zakresie. Związane z tą zasadą działania w pełni egzemplifikują: *operacje informacyjne*[94] i *walka informacyjna*[95]. Według ich prawideł prowadzone są szeroko zakrojone i niezwykle istotne przedsięwzięcia w konsekwentnym dążeniu do zdobycia przewagi informacyjnej.

Wymiernym efektem powyższej zasady jest zorganizowanie ***przestrzeni informacyjnej***, w której własnym siłom:

- zapewniany jest ciągły dostęp do informacji terminowych, wiarygodnych, dokładnych i co najważniejsze – w czasie rzeczywistym z wielu źródeł;
- zmniejszane są potrzeby informacyjne w zakresie ich objętości, przez wzrost zdolności wykorzystania wszystkich podmiotów zbierających[96] (sensorów) informacje;
- zapewniona jest skuteczna ochrona systemów informacyjnych, w tym również sensorów.

Z kolei wobec potencjalnego przeciwnika generowane są warunki uniemożliwiające mu uzyskanie pełnej wiedzy o sytuacji i prowadzące wręcz do jego dezinformacji, co w sytuacji niezwykle intensywnego wykorzystania widma elektromagnetycznego do zapewnienia łączności radiowej jest niezwykle istotne. Wyraża się to w zwiększaniu potrzeb informacyjnych przeciwnika poprzez:

- utrudnianie, zakłócanie dostępu do informacji,
- pozbawianie go informacji,
- manipulowanie informacją,
- generowanie informacji bezwartościowych, absorbujących systemy informacyjne przeciwnika.

Dostęp do zasobów informacji – rozumianej bardziej jako podział, rozdzielanie świadomości sytuacyjnej. W uwarunkowaniach mnogości źródeł informacji oraz ogromnych ich ilości niezbędne staje się **zarządzanie informacją**. Funkcjonujące w systemach dowodzenia zbiory informacyjne są nieustannie aktualizowane, pojawiają się nowe ich ilości, usuwane są nieaktualne informacje, ponadto **systemy informacyjne narażone są na oddziaływanie przeciwnika (w tym elektroniczne), który prowadzić będzie walkę w przestrzeni informacyjnej**. Nieodzowne w tej sytuacji staje się zapewnienie pewnego, bezpiecznego dostępu do niej dla wszystkich użytkowników, z zachowaniem szybkości, ciągłości i prostoty dostępu, łatwości korzystania ze zgromadzonych w bazach danych informacji, które w zamierzeniu wytwarzać powinny wysokiej jakości **wspólną świadomość sytuacyjną**. Stworzona w tym celu sieć i współpracujące w niej podmioty powinny

---

[93] Por. M. Huzarski, *Istota*..., wyd. cyt., s. 24; J. Kręcikij, *Istota działań*..., wyd. cyt., s. 130.
[94] R. Szpyra, *Militarne operacje informacyjne*, AON, Warszawa 2003.
[95] L. Ciborowski, *Walka informacyjna*, wyd. cyt.
[96] *The Implementation*..., wyd. cyt., s. 8.

dostarczać informacje ze wszystkich możliwych źródeł, z jednoczesnym, terminowym wprowadzaniem nowych danych, niezależnie od fizycznego rozmieszczenia w przestrzeni działań (walki, operacji). Wysoka jakość dostępu i rozdziału świadomości powinna pozostawać w zgodności z bezwzględnym zachowaniem **wysokiego poziomu ochrony i bezpieczeństwa sieci i informacji**. Dostępowi towarzyszyć powinna odpowiedzialność i świadomość usługowego charakteru sieci informacyjnej oraz korzystania z informacji adekwatnych do potrzeb, bez niepotrzebnego blokowania sieci.

Masowe użycie sensorów – zasada ta jest w ocenie K. Ficonia[97] podstawą funkcjonowania systemów NCW. Polega ona na stworzeniu warstwy sensorów (receptorów, czujników), usytuowanych bezpośrednio w przestrzeni operacyjnej obszarów, rejonów działań, w każdym środowisku fizycznym (powietrze, ląd, woda, kosmos). Najważniejsze są jednak: masowość ich występowania, wzajemne uzupełnianie się, nieustanne zbieranie danych i zasilanie nimi systemów informacyjnych w czasie rzeczywistym, potwierdzanie informacji oraz danych przez inne źródła, stałe monitorowanie parametrów obiektów i środowiska działania[98]. W praktyce takie podejście do wykorzystywania sensorów powinno zapewnić skuteczne działanie rozpoznania, pełnię wiedzy o wszystkich elementach i obiektach występujących na danym obszarze, stwarzając tym samym przewagę informacyjną nad potencjalnym przeciwnikiem. W działaniach sieciocentrycznych każdy środek, platforma bojowa powinna być wykorzystywana jako receptor i przekaźnik informacji, od pojedynczego żołnierza do satelity włącznie[99].

Wykorzystywanie okazji – zasada ta odnosi się głównie do spożytkowania pozytywnych efektów wszystkich wymienionych powyżej zasad poprzez osiągnięcie zdolności sił własnych, w szczególności dowództw, do: „(...) *szybkiej identyfikacji i adaptacji na własne potrzeby każdej zmiany w sytuacji, nawet jeżeli sterował nią przeciwnik*"[100]. Zasada ta wskazuje na decydentów jako głównych animatorów i moderatorów działań sieciocentrycznych sił. Przedkłada inicjatywę i szybkość procedur decyzyjnych oraz zakłada prowadzenie działań w warunkach zwiększonego poziomu ryzyka. Niemniej jednak idea wykorzystywania okazji ma prowadzić do większej efektywności działań.

Z kolei takie zasady, jak: **dostęp do zasobów informacji** spełniającej określone wymagania i pochodzącej z różnorodnych źródeł, zgodnie z potrzebami i specyfiką określonego poziomu (szczebla) dowodzenia (każdego rodzaju sił zbrojnych i wojsk); **samosynchronizacja**; **rozproszenie sił** (bardziej rozumiane jako przeciwstawienie się fizycznemu i geograficznemu zmasowaniu sił i środków); **masowe użycie sensorów**; **zmniejszenie różnic** pomiędzy poszczególnymi poziomami działań zbrojnych oraz zacieranie granic pomiędzy uczestniczącymi w działaniach

---

[97] K. Ficoń, *Inteligentny pył podstawą funkcjonowania systemów Network Centric Warfare*, „Myśl Wojskowa" 2006, nr 6, s. 57.

[98] Tamże, s. 60.

[99] *The Implementation*..., wyd. cyt., s. 10.

[100] M. Huzarski, *Istota*..., wyd. cyt., s. 25.

rodzajami sił zbrojnych i wojsk należy uznać za specyficzne, występujące w działaniach sieciocentrycznych[101]. Dopiero one podkreślają w znaczący sposób charakter działań i pozwalają nadać im nowy wymiar, odróżniający je od działań uznawanych za klasyczne. Mają one również swój udział we wszystkich procedurach i procesach zachodzących w dowodzeniu. Porównawcze zestawienie przedstawia tabela 1.

Tabela 1

Wyróżniki działań sieciocentrycznych w zderzeniu z działaniami klasycznymi

Działania typu NCW	Działania typu „klasycznego"
Powszechny dostęp do informacji wiarygodnej, pozyskiwanej w czasie zbliżonym do rzeczywistego, terminowej i dokładnej, doskonałe zorientowanie w sytuacji bojowej	Informacje zdobywane w sposób tradycyjny, czasochłonny, nieterminowy i niedokładny, niepełna wiedza o sytuacji bojowej
Samosynchronizacja (współdziałanie)	Synchronizacja organizowana przez szczebel nadrzędny
Rozproszenie sił, skupianie efektów, a nie sił i środków, sekwencyjność, jednoczesność, precyzja działań	Koncentracja sił i środków, masa wojsk, oddziaływanie na szerokich frontach, wyniszczające bitwy, starcia
Masowe użycie sensorów (każdy element NCW ma być sensorem, od żołnierza do satelity)	Tradycyjne użycie sensorów, zwykle ściśle związanych z platformami uzbrojenia i obsługą
Zacieranie granic pomiędzy poziomami działań, rodzajami SZ i wojsk	Formalny i doktrynalny podział na rodzaje wojsk i SZ, sztywna systematyka poziomów działań

Źródło: opracowano na podstawie J. Kręcikij, *Istota działań sieciocentrycznych*, „Zeszyty Naukowe AON" 2004, nr 4(65).

Zauważalne jest zatem, że koncepcja działań sieciocentrycznych wykorzystuje dotychczasowe osiągnięcia teorii i praktyki, adaptując sprawdzone rozwiązania i łącząc je z nowymi. Dostrzega również potrzebę zastosowania zmodernizowanego podejścia do znanych prawideł, co wynika z nowych uwarunkowań. Jednak wyraźnie podkreśla potrzebę zespolenia wszystkich reguł działań, zarówno znanych, jak i nowych z podstawowym uwarunkowaniem: **integracja i jedność**, a nie **zestawienie i rozłączne** traktowanie każdej z nich.

Brytyjski matematyk James. Moffat[102] na podstawie analizy i oceny założeń działań sieciocentrycznych wyróżnił również szereg czynników, których cechy opisują i precyzują szczegółowo ich specyficzne właściwości. Zostały one przedstawione w tabeli 2.

---

[101] J. Kręcikij, *Istota działań...*, wyd. cyt., s. 135.

[102] Szerzej J. Moffat, *Command and Control in the Information Age: Representing its Impact*, The Stationery Office, London 2002; J. Moffat, *Complexity Theory and Network Centric Warfare*, CCR Publication Series, September 2003, s. 49.

Tabela 2

Cechy czynników działań sieciocentrycznych

Nazwa czynnika	Cechy czynnika
Nielinearne powiązania	Siły walczące składają się z dużej liczby rozproszonych elementów, które spięte poprzez system informatyczny nie są uzależnione od sztywnych struktur dowodzenia.
Decentralizacja dowodzenia	W systemie dowodzenia nie występuje wyraźny szczebel nadrzędny, dystrybucja danych i informacji nie jest zależna od przełożonego, każdy rozproszony element ugrupowania ma dostęp do baz danych, ma wgląd w tzw. wspólny obraz sytuacji, którego jest w części twórcą, funkcjonuje w wirtualnej przestrzeni informacyjnej, posiada większą decyzyjność.
Samoorganizacja	Występuje wiele działań lokalnych, których zadania cząstkowe składają się na zadanie główne (cel) długookresowe (nadrzędne) z maksymalnym wykorzystaniem efektu synergii.
Niepewność	Konflikty zbrojne z natury stają się bardzo zmienne i złożone. W związku z tym kluczowe jest korelowanie działań lokalnych, tj. niewielkich, a jednocześnie licznych elementów ugrupowania. Wymuszane są na przeciwniku większe potrzeby informacyjne ze względu na skoordynowane działania rozproszonych sił. Tworzona jest „mgła informacyjna" wobec systemów informacyjnych i rozpoznawczych przeciwnika.
Adaptacyjność	Działające siły muszą aktywnie i dynamicznie dostosowywać się do zmieniającej się sytuacji.
Dynamizm	Istnieje zależność (sprzężenie zwrotne) pomiędzy wysiłkiem walczących a strukturą systemu dowodzenia.

Źródło: J. Moffat, *Complexity Theory and Network Centric Warfare*, CCR Publication Series, September 2003, s. 49.

Tak postrzegane czynniki i wyróżniki działań sieciocentrycznych charakteryzują w istocie nowe środowisko, które w aspekcie dowodzenia stwarza określone warunki oraz wpływa na zachodzące zjawiska, zależności i zachowania zespołów ludzkich oraz organizacji.

Funkcjonowanie i rozwój koncepcji NEC jest bowiem *pochodną połączenia specyficznych, twórczych możliwości człowieka oraz nowoczesnych technologii informatycznych i środków walki*. Dlatego też zakłada się, że nieodzowne jest stworzenie odpowiednich warunków, które zapewnią: **właściwe zrozumienie**, **kształcenie** oraz **szkolenie** wszystkich osób zaangażowanych i współtworzących nowe sieciocentryczne właściwości – od żołnierza poprzez dowódców najniższych szczebli, personel sztabu (operatorów i administratorów sytemu) do dowódców najwyższych operacyjnych i strategicznych poziomów dowodzenia. Sieci pozwalają lepiej, szybciej współpracować dowódcom i sztabom na wszystkich oraz ze wszystkimi szczeblami dowodzenia.

Podsumowując, należy stwierdzić, że **działania sieciocentryczne** warunkowane są następującymi właściwościami:

- osiągnięciem możliwości współdzielenia świadomości sytuacyjnej na wszystkich szczeblach i poziomach dowodzenia (działania);

- zapewnieniem pełnego dostępu do informacji wszystkim użytkownikom systemu, w tym pobierania, wprowadzania i wymiany informacji oraz danych;
- synchronizacją działań, która prowadzić ma do maksymalizacji efektów działań połączonych;
- osiągnięciem zdolności do szybkiego generowania sił zadaniowych, stosownie do potrzeb i prognozowanych zadań;
- osiągnięciem zdolności dowodzenia w dynamicznych, ciągłych i zsynchronizowanych działaniach;
- stworzeniem infrastruktury informacyjnej, umożliwiającej dostęp do informacji oraz zapewniającej jej wysoką jakość i bezpieczeństwo;
- kompleksowymi i skoordynowanymi badaniami oraz wdrażaniem nowych technologii egzemplifikujących zdolności sieciocentryczne.

Problematyka związana z działaniami sieciocentrycznymi ma interdyscyplinarny charakter. Obejmuje ona wiele dziedzin, dyscyplin i specjalności naukowych. Powinna być rozpatrywana kompleksowo, przez pryzmat: techniki i technologii, informatyki i łączności (telekomunikacji), organizacji i zarządzania, dowodzenia, sztuki wojennej i jeszcze wielu innych czynników. Tak znaczące spektrum i potrzeby interdyscyplinarnego podejścia są wyrazem powiązania osiągnięć i walorów wielu dziedzin nauki, które wzajemnie się uzupełniają w kreowaniu nowych jakościowo zjawisk i zachowań w działaniach o charakterze sieciocentrycznym w uwarunkowaniach początku XXI wieku. Niewątpliwie walka elektroniczna ma znaczące możliwości do wypełniania swoich zadań w sytuacji coraz wyraźniej zarysowujących się kształtów koncepcji działań sieciocentrycznych. Natomiast jakie będzie jej miejsce, rola i wpływ na skuteczność działań o charakterze sieciocentrycznym w przyszłości, pozostaje kwestią otwartą, która – sądzę, że będzie przyświecać tej konferencji.

Płk mgr Krzysztof PROSTACKI
Zarząd Analiz Wywiadowczych i Rozpoznawczych – P2

MOŻLIWOŚCI WYKORZYSTANIA SYSTEMU WALKI ELEKTRONICZNEJ W DZIAŁANIACH SIECIOCENTRYCZNYCH

Idea działań sieciocentrycznych

Od kilku lat modnym słowem związanym z działaniami bojowymi stała się sieciocentryczność. Jest to nowa teoria walki, która pojawiła się we wiodących armiach świata wraz z nadejściem ery informatycznej. Jest to teoria coraz powszechniej akceptowana i adoptowana. Spycha ona do lamusa wojnę, w której zasadnicza uwaga skupiała się przede wszystkim na platformie lądowego, powietrznego oraz wodnego środka rozpoznania i uderzenia. Koncepcja ta była wynikiem sprostania nowym uwarunkowaniom prowadzenia działań związanym z koniecznością pozyskiwania i przetwarzania coraz większej ilości danych pochodzących z wielu źródeł. Za tym poszła konieczność zwiększenia efektywności procesu prowadzenia działań. Jak pokazują doświadczenia z ostatnich kilku lat, koncepcja sieciocentryczności to nie wizja czy fantazja jej twórców, to nie wirtualna zabawka, lecz konieczność chwili.

Analizując dostępną literaturę, można dostrzec wiele wątków koncepcji sieciocentryczności wynikających z różnego podejścia do działań sieciocentrycznych w różnych krajach. Różne były terminy z nią związane, różna też była strona techniczna koncepcji, uwarunkowana aktualnym poziomem myśli technicznej i zdolnościami do przełożenia myśli w czyny. Według tej nowej teorii walki sieć to zespół wzajemnie powiązanych w sposób elektroniczny środków, takich jak elementy systemu dowodzenia, rozpoznania, analizy, transmisji i zobrazowania danych oraz aktywne środki rażenia przeznaczone do prowadzenia działań bojowych na współczesnym polu walki.

Centralną rolę w działaniach sieciocentrycznych odgrywa informacja jako potencjalne źródło siły wojsk. Nawet wojska rozproszone na znacznym obszarze, ale doskonale zorientowane w sytuacji bojowej, są w stanie sprostać nieproporcjonalnym dla nich zadaniom, które w tradycyjnym podejściu do działań bojowych byłyby nie do osiągnięcia. W działaniach sieciocentrycznych, w porównaniu z dotychczasowymi klasycznymi działaniami, szybkość zdobywania i wykorzystania informacji oraz dokonywanie precyzyjnych uderzeń wygrywa z dotychczasową liczebnością wojsk, a wysoki stopień jednoczesnych, synergicznych uderzeń z działaniami sekwencyjnymi. Działania sieciocentryczne umożliwiają odejście od angażowania liczbowo wielkich wojsk w następujących po sobie bitwach na rzecz precyzyjnych, niemal jednoczesnych ataków, dokonywanych przez znacznie mniejsze,

lecz jakościowo inne siły. Sieciocentryczne działania bojowe oparte są na zasadzie synergizmu, gdzie współdziałanie różnych składowych jest skuteczniejsze niż suma ich oddzielnych działań. Jednak aby działania sieciocentryczne były skuteczne, niezbędna jest bogata informacja o potencjalnym przeciwniku, zdobywana z różnych źródeł, kojarzona ze sobą i dystrybuowana do wszystkich jej użytkowników w czasie prawie rzeczywistym. Ideą sieciocentryczności jest więc zwiększenie potencjału własnych możliwości, lecz nie przez rozbudowę ilościową sił i środków, ale przez bardziej racjonalne i efektywne ich wykorzystanie przez dowódców. A to wszystko dzięki posiadaniu aktualnej, terminowej i wiarygodnej informacji oraz nieograniczonej jej dystrybucji.

Fundamentalną prawdę o przewadze informacyjnej w wojnie dostrzegł już około 500 roku p.n.e. chiński strateg Sun Tzu, który w swoim dziele „Sztuka wojny" napisał: „Jeśli znasz siebie i swego wroga, przetrwasz pomyślnie sto bitew". Było to jedno z pierwszych oświadczeń potwierdzających znaczenie informacji w walce. Istotą obecnej rewolucji w obszarze informacji jest szybkość jej zdobywania, możliwość komputerowej analizy, dystrybucji do wszystkich elementów sieci oraz właściwego zarządzania nią, jak również wykorzystywania jej w działaniach bojowych.

Dziś technologia informatyczna uwalnia wojska od ograniczeń geograficzno-położeniowych i umożliwia odejście od zasady grupowania wojsk na rzecz grupowania efektów. Sensory mogą wykrywać i rozpoznawać, a środki bojowe atakować różne cele, często bez konieczności zmiany swego położenia. Pomimo rozproszenia, wojska będą mogły działać jako system zdolny do koncentracji uderzeń precyzyjnych, czyli zdolny do generowania synergicznych efektów. Jednak sama technika nic nie da, jeśli systemy rozpoznania elektronicznego nie zostaną wyposażone w różnorodne sensory wykrywające i śledzące działania potencjalnego przeciwnika w szerokim spektrum częstotliwości. Możliwości właściwej oceny zagrożeń i zdolności potencjalnego przeciwnika zależeć będą w znacznej mierze od możliwości rozpoznawczych sensorów dostarczających informacje.

Siła działań sieciocentrycznych wynika także z zabezpieczenia w informacje wszystkich decydentów pola walki, a nie tylko niektórych. Nowe pole walki wymaga odmiennego podejścia w zakresie dowodzenia i kierowania niż praktykowane do tej pory. W działaniach sieciocentrycznych dotychczasowy hierarchiczny system planowania i wydawania rozkazów może skutkować tylko opóźnieniem i zamieszaniem, a tym samym obniżeniem skuteczności wykonania zadań.

Działania sieciocentryczne mają swoją specyfikę. Z jednej strony zbierane są wszelkie dostępne informacje o przeciwniku, jednak z drugiej strony samo zbieranie informacji nie wystarcza. Każdy element własnych sił, do którego informacja została przesłana, musi ją sam zinterpretować i wyciągnąć wnioski do działań na swoim szczeblu. Ale efektem takich działań jest to, że każdy taki element ma wystarczającą wiedzę o położeniu swoim, wojsk własnych i przeciwnika. Może samodzielnie synchronizować dalsze działania bez dodatkowych, dokładnych rozkazów wyższych szczebli. Tym samym rola wyższych szczebli dowodzenia będzie, w coraz większym

stopniu, ograniczała się do wydawania ogólnego zamiaru działań. Zejście z informacją na wszystkie szczeble dowodzenia, nawet te najniższe, spowoduje uzyskanie przewagi nad przeciwnikiem w każdym momencie i obszarze. Aby ten moment wykorzystać, siły i środki na najniższych szczeblach walki muszą mieć adekwatną strukturę oraz posiadać szeroką gamę efektywnych środków walki.

Architektura działań sieciocentrycznych

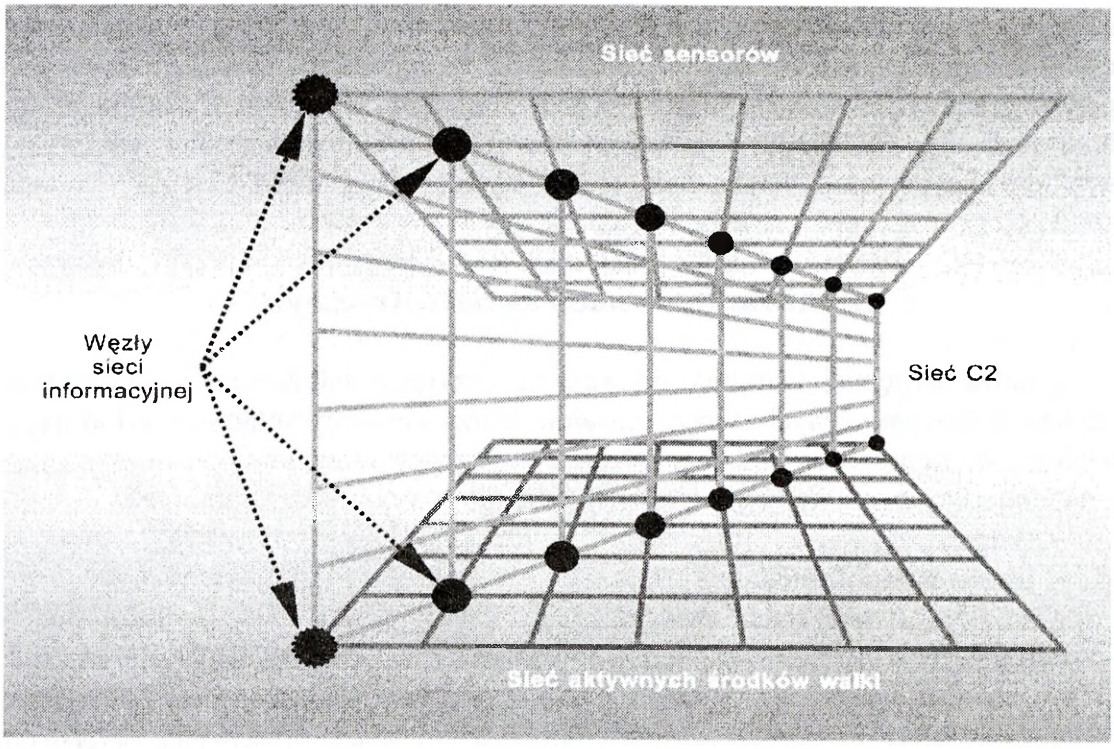
Analiza dostępnej literatury pozwala na przyjęcie założenia, że architekturę działań sieciocentrycznych tworzą zasadnicze trzy elementy składowe, od których uzależnione są możliwości działań sieciocentrycznych, w tym i systemu rozpoznania elektronicznego i walki elektronicznej. Są to:

- sensory,
- przekaźniki informacji,
- środki uderzenia (oddziaływania).

Pod pojęciem **sensora** rozumie się dowolny element rozpoznawczy (np. elektroniczny, optyczny), mogący rozpoznać, przetworzyć i wprowadzić do sieci dane o polu walki. Sieć takich sensorów dostarcza informacji o siłach przeciwnika, własnych i całym środowisku walki w przestrzeni działań bojowych i obejmuje sensory rozmieszczone w przestrzeni cybernetycznej, powietrzu, na lądzie, wodzie i pod wodą.

Przekaźnikami informacji jest cała sieć transmisji, czyli sieć informacyjna, za pomocą której przekazywany jest głos, obraz oraz dane liczbowe. Umożliwia ona stworzenie wspólnego zobrazowania sytuacji o przestrzeni walki, wpływa na uzyskanie wysokiego tempa działań, zwiększoną efektywność bojową, jak również lepszą ochronę własnych wojsk. Jej struktura powinna mieć zdolność przyłączania innych sensorów i środków walki, a także zapewniać bezpieczne przesyłanie przekazywanej informacji. Sieć transmisji informacji umożliwia wymianę, przetwarzanie, przechowywanie i ochronę informacji. Składać się ona będzie z kanałów łączności, węzłów informatycznych, systemów operacyjnych oraz aplikacji zarządzania informacjami. Możliwości techniczne sieci informacyjnej warunkują stopień przesyłania sygnałów i wiadomości sytuacyjnych wygenerowanych przez sieć sensorów. Sieć transmisyjna stanowi więc o możliwości uzyskania przewagi informacyjnej.

Sieć **środków uderzenia** obejmuje środki, których zadaniem jest stworzenie wymaganych efektów w danym miejscu i czasie. Ich architektura operacyjna umożliwia dowódcy planowanie i wykonywanie zadań bojowych w sposób efektywny, w precyzyjnym czasie i miejscu. Sieć środków walki opierać się będzie na sieci dowodzenia, która ma zapewnić dowodzenie platformami bojowymi w przestrzeni walki. Sieć ta umożliwia wykorzystanie informacji o przestrzeni działań bojowych, a przez to zapewnia działającym siłom możliwości wykonania manewrów, precyzyjnych uderzeń w wymaganym czasie i miejscu.



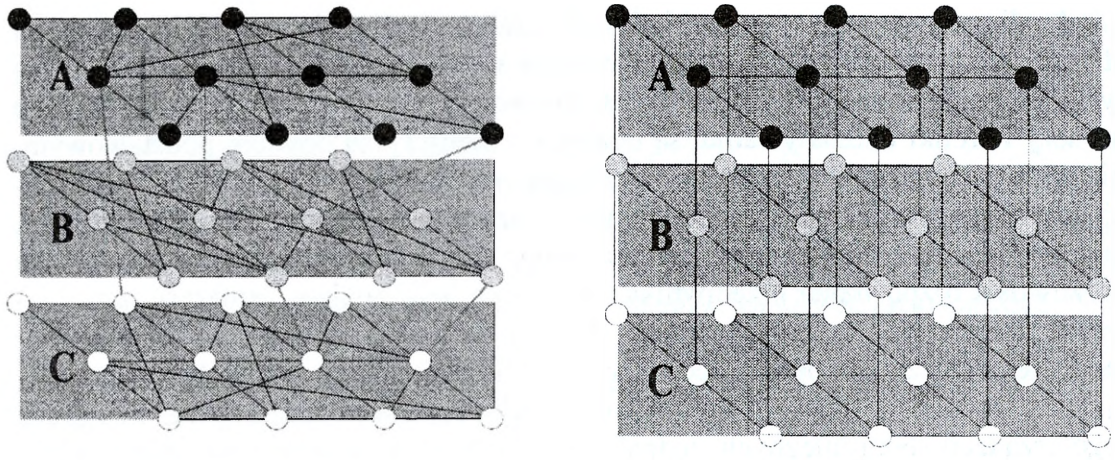
Źródło: R. Szpakowicz, R. Hoffmann, *Koncepcja wojny sieciocentrycznej jako odpowiedź na zapotrzebowanie sił powietrznych XXI wieku na informacyjne wsparcie działań bojowych*, „Przegląd WLOP", sierpień 2003.

Rys. 1. Idea sieciocentryczności – powiązanie sieci sensorów oraz środków walki poprzez sieć informacyjną

Zarówno definicja walki sieciocentrycznej, jak i architektura przestrzeni walki sieciocentrycznej wskazują, że za podstawę dla prowadzenia działań sieciocentrycznych należy uznać elementy umożliwiające spięcie całości sił i środków w sieć informacyjną oraz wymianę, przetwarzanie, udostępnianie i przechowywanie informacji.

Przedstawiona na rysunku 2 uproszczona idea sieciocentryczności pokazuje, że koncepcja ta obejmuje wszystkie elementy, które uczestniczą w poszczególnych przedsięwzięciach, niezależnie od swojej roli i przeznaczenia. W dotychczasowych działaniach (rys. a) różne obszary autonomiczne (płaszczyzny A, B, C), np. rozpoznanie, dowodzenie czy logistyka, wykorzystywały sieć wewnętrznych połączeń, natomiast między sobą powiązane były jednym lub tylko kilkoma kanałami przesyłania informacji. W działaniach sieciocentrycznych (rys. b) płaszczyzny połączone są licznymi kanałami, w dowolnej konfiguracji połączeń.

Wszystkie elementy składowe koncepcji sieciocentryczności, mimo potencjalnie dużego rozśrodkowania, mają zapewnić uzyskanie zsynchronizowanej czasowo i przestrzennie przez wszystkich użytkowników sieci oceny sytuacji, określanej w wielu publikacjach jako „świadomość sytuacyjna". Oznacza to, że teoretycznie tę samą informację powinien mieć każdy użytkownik w systemie.



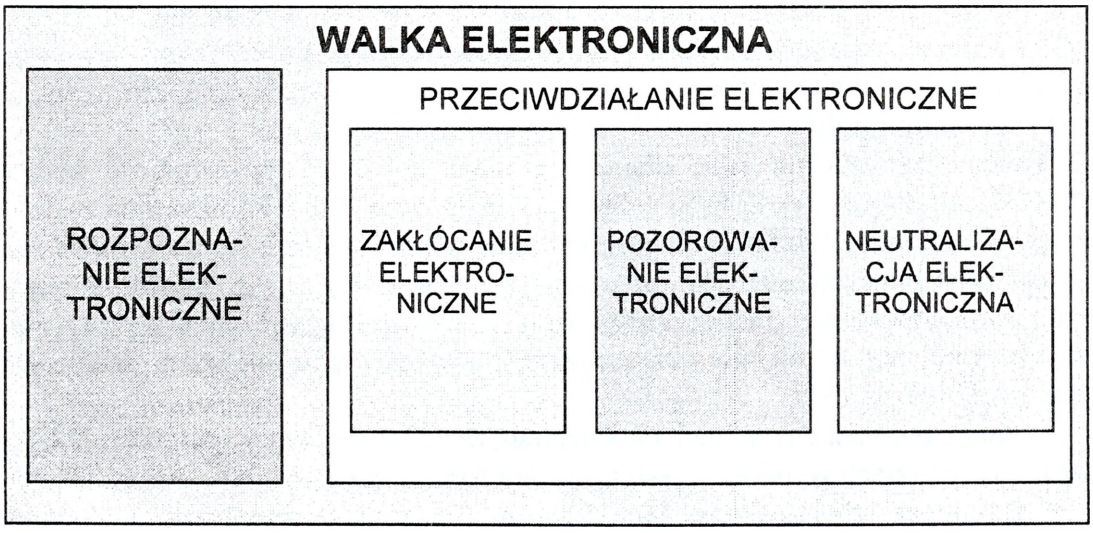
a b

Źródło: (a) opracowanie własne oraz (b) K. Rokiciński, *Możliwości zastosowania koncepcji sieciocentryczności na obszarach morskich Rzeczypospolitej Polskiej*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2007, rok XLVIII, nr 3(170).

Rys. 2. Porównanie dotychczasowego systemu powiązań systemów funkcjonalnych (rys. a) i w układzie sieciocentrycznym (rys. b)

Koncepcja sieciocentryczności a walka elektroniczna

Jak do koncepcji sieciocentryczności ma się walka elektroniczna? Walka elektroniczna obejmuje rozpoznanie elektroniczne oraz przeciwdziałanie elektroniczne, w skład którego z kolei wchodzą zakłócanie elektroniczne, pozorowanie elektroniczne oraz neutralizacja elektroniczna.



Opracowanie własne.

Rys. 3. Obszary walki elektronicznej

Analiza koncepcji oraz architektury działań sieciocentrycznych pozwala na stwierdzenie, że walka elektroniczna wpisuje się we wszystkie zasadnicze elementy składowe koncepcji, czy też walki sieciocentrycznej. Dwa z nich, a mianowicie sensory i środki oddziaływania, są oczywiste. Sensory są bowiem podstawowym, pierwotnym elementem systemu, warunkującym zdobywanie i posiadanie informacji o przeciwniku. Stanowią one elementy rozpoznania elektronicznego. Od tego, jakimi sensorami dysponować będzie system walki elektronicznej, zależeć będą możliwości rozpoznania przeciwnika, określenia jego miejsca, struktury organizacyjnej, dyslokacji i zamiaru działania. Z kolei drugi element – środki przeciwdziałania elektronicznego, będzie decydował o zakłócaniu, pozorowaniu lub neutralizacji środków elektronicznych przeciwnika, czyli aktywnym oddziaływaniu na pracę jego urządzeń elektronicznych. Jednak aby powiązać ze sobą elementy zdobywania danych o przeciwniku z elementami oddziaływania na jego środki elektroniczne, niezbędny jest skuteczny system przepływu informacji, który byłby zdolny do przekazania danych w czasie prawie rzeczywistym, niezbędnych do podejmowania decyzji na szybko zmieniającym się współczesnym polu walki.

Jak więc widać, w walce elektronicznej możemy mówić niejako o trzech autonomicznych „podsieciach": sensorów, środków oddziaływania oraz środków przesyłania informacji. Podsieci te muszą ze sobą współpracować, aby można było mówić o skutecznym prowadzeniu walki elektronicznej. Wydaje się, że obecnie zapewnić nam to może tylko sieciocentryczność. Możemy więc mówić o „małej sieciocentryczności", obejmującej walkę elektroniczną, która jednak będzie elementem składowym ogólnej zdolności sieciocentrycznej wojsk.

Funkcjonująca obecnie w siłach zbrojnych wielopoziomowa struktura wielu systemów i sieci teleinformatycznych, tworzonych na potrzeby różnych użytkowników, w najbliższej przyszłości nie sprosta wymaganiom rozpoznania, dowodzenia i kierowania środkami walki. Jaka powinna więc być struktura nowej „supersieci", która temu sprosta? Z analizy dostępnej literatury wynika, że zasadniczą część koncepcji działań sieciocentrycznych stanowi sfera informacyjna oparta na rozległej, globalnej sieci informatycznej. To ona warunkować będzie, kto, w jakim czasie i w jakim miejscu będzie miał dostęp do informacji.

Walka elektroniczna jako element działań bojowych uczestniczyć będzie w ogólnej supersieci. Nie sposób sobie wyobrazić, że w dobie korelowania ze sobą różnych systemów teleinformatycznych w jedną globalną sieć informatyczną walka elektroniczna pozostanie z boku. Sieciocentryczność polegać więc będzie na stworzeniu jednej globalnej sieci sensorów oraz środków oddziaływania, wykorzystywanych dotąd autonomicznie przez różnych użytkowników, poprzez spięcie ich siecią teleinformatyczną.

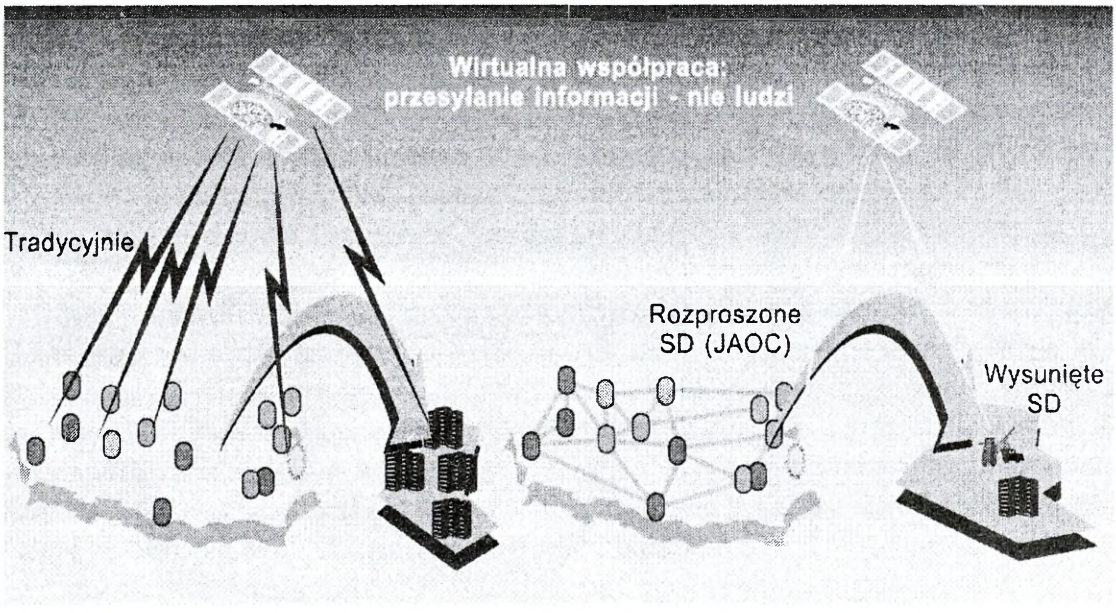
Z badań prowadzonych nad określeniem zasad sieciocentryczności w NATO oraz różnych krajach wynika, że taka sieć teleinformatyczna powinna cechować się:

– globalnym charakterem, tzn. powinna obejmować możliwie wszystkich użytkowników zaangażowanych w realizację danego zadania,

– zasięgiem i pasmem wystarczającym do spełnienia wymagań w całej przestrzeni działań sieciocentrycznych,

– zapewnieniem dostępu wszystkich użytkowników do informacji w czasie prawie rzeczywistym,
– mobilnością,
– zdolnością do szybkiej rekonfiguracji,
– bezpieczeństwem i niezawodnością.

Ważnym elementem w koncepcji działań sieciocentrycznych jest organizacja stanowisk dowodzenia. Obejmować ona będzie również stanowiska dowodzenia lub elementy stanowisk dowodzenia odpowiedzialne za walkę elektroniczną. Sieciocentryczność zakłada tworzenie „wirtualnych" stanowisk dowodzenia o rozproszonej strukturze, które umożliwią dowodzenie z miejsc niezagrożonych bezpośrednim oddziaływaniem przeciwnika.



Źródło: R. Szpakowicz, R. Hoffmann, *Koncepcja wojny sieciocentrycznej*..., wyd. cyt.

Rys. 4. Sieciocentryczne – wirtualne stanowiska dowodzenia

Wykorzystując sieć, nie będzie konieczności umiejscawiania stanowisk dowodzenia w rejonie działań bojowych. Wystarczy zagwarantować skuteczny i terminowy przepływ informacji między nimi oraz sensorami. Należy się spodziewać, że informacja z sensorów rozpoznania elektronicznego będzie mogła również być odbierana bezpośrednio przez elementy walki elektronicznej, inicjując tym samym możliwość przygotowania środków walki elektronicznej do użycia. Jednak o użyciu środków walki elektronicznej decyduje obecnie i decydować będzie nadal dowódca prowadzący operację. On określa, kto, kiedy i jakie środki powinny być użyte, aby osiągnąć zamierzony efekt w walce elektronicznej, nie pozbawiając własnych sił systemu łączności dowodzenia.

Możliwości wdrażania koncepcji sieciocentryczności w systemie walki elektronicznej sił zbrojnych RP

Zgodnie ze strategią NATO sojusz będzie budował systemy sieciocentryczne na bazie narodowych systemów państw członkowskich. W Siłach Zbrojnych RP rozpoczęto już prace nad strategią osiągania przez nie zdolności sieciocentrycznych. Jako tymczasową podstawę przyjęto zreorganizowanie stacjonarnego systemu łączności, który będzie stanowić bazę dla rozwijanych sieci teleinformatycznych. W dalszym etapie przewiduje się objęcie sieciocentrycznością polowego systemu łączności. Na bazie systemów łączności zwiększane będą zakresy współpracy istniejących zautomatyzowanych systemów, w tym systemów rozpoznawczo-zakłócających, aż do osiągnięcia zakładanych zdolności modelu sieciocentryczności działań sił zbrojnych. W pierwszej kolejności przewiduje się osiągnięcie takich zdolności przez jednostki i stanowiska dowodzenia wyższych szczebli, a następnie zejście na szczeble niższe, aż do pojedynczego żołnierza. Pozwoli to na budowę taktycznego systemu kierowania, aż do osiągnięcia zintegrowanego obrazu pola walki na potrzeby wszystkich żołnierzy zaangażowanych w działania bojowe.

W zakresie systemu dowodzenia walką elektroniczną istnieje wiele obszarów, w których należałoby dokonać transformacji. Wydaje sie, że punktem wyjściowym powinno być stworzenie autonomicznej zintegrowanej sieci dowodzenia i kierowania walką elektroniczną, która weszłaby w skład nadrzędnej globalnej supersieci. Struktura takiej sieci obejmowałaby zagwarantowanie odpowiedniej jakości usług w ramach platformy działań sieciocentrycznych obejmującej sensory, decydentów oraz środki walki. Istotnym elementem jest stworzenie wspólnego zintegrowanego obrazu sytuacji (*Common Operational Picture* – COP), bowiem powodzenie w każdej operacji, w tym i w walce elektronicznej, uwarunkowane jest od stałej i wiarygodnej informacji o sytuacji bieżącej na polu walki. Ideą COP jest właśnie stworzenie takiego rzeczywistego, pełnego i jednakowo rozumianego obrazu pola walki, pochodzącego ze wszystkich sensorów wykorzystywanych na różnych szczeblach dowodzenia. Obraz taki powinien być tworzony na bieżąco i dostępny w dowolnej chwili z wymaganym zakresem informacyjnym. Stworzenie takiego narzędzia pozwoli m.in. na zwiększenie skuteczności dowodzenia i efektywności pracy dowództw, w tym walki elektronicznej, zmniejszenie stanów osobowych, a także lepszą synchronizację działań.

Przygotowanie jednostek walki elektronicznej do działań sieciocentrycznych

Analiza aktualnego stanu wyposażenia jednostek walki elektronicznej przemawia za posiadaniem zautomatyzowanego systemu dowodzenia i kierowania walką elektroniczną. System ten mógłby docelowo stanowić element ogólnej sieci informatycznej. System taki powinien mieć otwartą architekturę informatyczną podatną

na zmiany, w szczególności w systemie łączności i wyposażenia technicznego (urządzeń rozpoznania i zakłóceń elektronicznych). Powinien zapewniać dowodzenie i kierowanie rozpoznaniem oraz przeciwdziałaniem elektronicznym na wszystkich szczeblach dowodzenia, aż do pojedynczych posterunków rozpoznania i zakłóceń podległych, a także dystrybucję informacji.

W celu przygotowania jednostek walki elektronicznej do działań w strukturach sieciocentrycznych niezbędne jest dokonanie zmian strukturalnych i organizacyjnych, jak również w obszarze wyposażenia sprzętowego. W koncepcji modernizacji systemu walki elektronicznej należy odnieść się do rozwiązań umożliwiających:

– automatyzację procesów przetwarzania danych o źródłach emisji sygnałów radioelektronicznych odbieranych przez urządzenia rozpoznania,

– automatyzację dowodzenia pododdziałami walki elektronicznej,

– zapewnienie możliwości kierowania walką elektroniczną z systemu nadrzędnego (np. stanowiska dowodzenia centrum operacji),

– dostarczanie w czasie prawie rzeczywistym danych z rozpoznania elektronicznego do systemu dowodzenia celem wykorzystania ich przy tworzeniu zintegrowanego obrazu sytuacji bojowej,

– cyfrową transmisję danych, komend, rozkazów i meldunków za pomocą środków łączności.

System dowodzenia i kierowania walką elektroniczną powinien realizować funkcje dowodzenia i kierowania pracą bojową całego potencjału rozpoznawczego. Kierowanie procesem pozyskiwania danych oraz przeciwdziałania elektronicznego polega głównie na generowaniu i transmisji komend do wykonawców i przyjmowaniu od nich meldunków realizacyjnych. Wynikiem realizowanych przedsięwzięć na poszczególnych szczeblach systemu powinna być wygenerowana sytuacja elektroniczna w rejonie odpowiedzialności danego stanowiska dowodzenia, która skojarzona z danymi z innych źródeł rozpoznania dałaby ogólny zintegrowany obraz zagrożenia danego obszaru.

Dane rozpoznawcze pozyskane w trakcie rozpoznania elektronicznego stanowią obecnie główną część meldunków rozpoznawczych generowanych przez operatorów urządzeń wykrywania. W systemie sieciocentrycznym meldunki takie nie będą przesyłane bezpośrednio do szczebla nadrzędnego (jak dotychczas w tradycyjnym autonomicznym systemie przekazywania danych), a do globalnej sieci rozpoznania. Z jednej strony będą dostępne dla bezpośredniego przełożonego w celu wypracowania decyzji, a z drugiej strony będą dostępne dla innych dowódców. Pozwolą one im na orientację w sytuacji elektronicznej sąsiadów i właściwe terminowe ukierunkowanie swoich działań rozpoznawczych. Ponadto będą one stanowiły wzbogacenie informacji rozpoznawczej, dając pełniejszy obraz sytuacji elektronicznej i bojowej, na podstawie którego możliwe będzie trafniejsze przewidzenie zamiarów potencjalnego przeciwnika i dokonanie manewru własnymi siłami, środkami i zadaniami.

Kierowanie procesem przeciwdziałania elektronicznego obejmuje realizację procedur związanych z określeniem parametrów technicznych emisji zakłócających. Automatyzacja tych procedur, realizowana w ramach zautomatyzowanych systemów dowodzenia i kierowania środkami walki elektronicznej, pozwoli na optymalne wykorzystanie właściwości elementów zakłócających. Należy mieć na uwadze, że w kontekście działań sieciocentrycznych sposób użycia środków przeciwdziałania elektronicznego nie ulegnie istotnej zmianie. Decyzje o użyciu środków zakłóceń elektronicznych podejmuje szczebel dowodzenia odpowiedzialny za osłonę danych obiektów. Do jego zadań należeć więc będzie opracowanie konfiguracji systemu osłony, która byłaby w danej sytuacji geoprzestrzennej najbardziej skuteczna. Na podstawie danych wynikających z bieżącej sytuacji bojowej i elektronicznej formułowane będą zadania dla elementów walki elektronicznej. Będą one stanowiły podstawę do wyboru parametrów technicznych sygnałów zakłócających, których użycie będzie najbardziej skuteczne dla obezwładnienia danego środka elektronicznego przeciwnika.

Wyposażenie techniczne jednostek rozpoznania i przeciwdziałania elektronicznego pokazuje, że posiadają one sensory oraz środki oddziaływania elektronicznego. Sensory rozpoznania elektronicznego stanowią względnie nowoczesną grupę urządzeń, natomiast grupa środków oddziaływania wymaga pozyskania nowoczesnego sprzętu, podatnego na włączenie w zautomatyzowane systemy dowodzenia.

Według ocen specjalistów niezbędne jest więc wykonanie szeregu przedsięwzięć wymagających znacznych nakładów finansowych i czasu. Czy stać nas na podjęcie takiego wyzwania? Jest to konieczność chwili i należy to zrobić, aby nie zostać w tyle za innymi siłami zbrojnymi. Jest to również niezwykle istotne w kontekście udziału polskich kontyngentów wojskowych w misjach i operacjach poza granicami kraju.

Podsumowanie

Przedstawione w materiale problemy związane z możliwościami systemu walki elektronicznej w działaniach sieciocentrycznych są zagadnieniami relatywnie nowymi. Dostępna literatura dotyczy ogólnie pojętej sieciocentryczności i zasad prowadzenia działań w środowisku sieciocentrycznym. Brak jest do tej pory opracowań odnoszących się do udziału w działaniach sieciocentrycznych specyficznego obszaru jakim jest walka elektroniczna. Wzrost znaczenia informacji na współczesnym polu walki w powiązaniu z postępem dokonującym się w dziedzinie technologii informatycznych skłania do podniesienia ważności zagadnienia działań sieciocentrycznych, które wydają się właściwym kierunkiem rozwoju i modernizacji sił zbrojnych w najbliższych latach.

Bibliografia

Konopka L., *Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości*, „Myśl Wojskowa" 2004, nr 2.

Kręcikij J., *Istota działań sieciocentrycznych*, „Zeszyty Naukowe AON" 2006, kwartalnik nr 4(65).

Krysiński S., Koziełło M., *Rozwój zdolności sieciocentrycznych NATO*, „Kwartalnik Bellona" 2007, nr 3.

Polcikiewicz Z., Świętochowski N., *Artyleria na sieciocentrycznym polu walki*, „Myśl Wojskowa" 2006, nr 5.

Posobiec J., *Proces dowodzenia w środowisku sieciocentrycznym*, „Zeszyty Naukowe AON", kwartalnik nr 3(68)A – *System dowodzenia w środowisku sieciocentrycznym* – materiały z konferencji naukowej z 2007 r.

Rokiciński K., *Możliwości zastosowania koncepcji sieciocentryczności na obszarach morskich Rzeczypospolitej Polskiej*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2007, rok XLVIII, nr 3(170).

Szpakowicz R., Hoffmann R., *Koncepcja wojny sieciocentrycznej jako odpowiedź na zapotrzebowanie sił powietrznych XXI wieku na informacyjne wsparcie działań bojowych*, „Przegląd WLOP", sierpień 2003.

Szpakowicz R., *Wojna w Iraku a koncepcja wojny sieciocentrycznej*, „Przegląd WLOP", listopad 2003.

Wołejszo J., Siedlecki M., *Walka sieciocentryczna wyzwaniem XXI wieku*, „Zeszyty Naukowe AON", kwartalnik nr 3(68)A – *System dowodzenia w środowisku sieciocentrycznym* – materiały z konferencji naukowej z 2007 r.

Ppłk dr inż. Waldemar SCHEFFS
Zarząd Rozpoznania i Walki Elektronicznej
Instytutu Wojsk Lądowych Wydziału Zarządzania i Dowodzenia AON

ZAŁOŻENIA WALKI ELEKTRONICZNEJ W ŚRODOWISKU SIECIOCENTRYCZNYM

Wprowadzenie

Doświadczenia płynące z analiz i ocen teorii oraz praktyki działań prowadzonych przez różne SZ w drugiej połowie XX wieku, a także uwarunkowania polityczno-militarne i społeczno-ekonomiczne, jakie pojawiły się na przełomie wieków, stały się podstawą do wypracowania i praktycznego zastosowania skuteczniejszych metod prowadzenia działań zbrojnych. Zwłaszcza że zauważono, iż źródła siły nie tkwią tylko w destrukcyjnych systemach broni, lecz również w zakresie możliwości wykorzystywania do celów militarnych nowoczesnych, zaawansowanych technologii informatycznych. Stały się one motorem napędowym dla tworzenia globalnej sieci informatycznej. Świat został opleciony siecią informatyczną, zautomatyzowano niektóre czynności procesu dowodzenia. Informacja stała się motorem postępu i nieodzownym warunkiem sukcesu w erze informacyjnej, za jaką uznaje się współczesne czasy[103].

Dążenie do dominacji jednych sił zbrojnych nad drugimi wynikał nie tylko z ilości posiadanego sprzętu, ale głównie z postępu technologicznego i redukcji sił zbrojnych w większości państw. Występowanie dodatkowo nowych zagrożeń, związanych ze światowym terroryzmem, jeszcze bardziej wymusiło potrzebę szukania nowych rozwiązań w wykorzystaniu wojsk. Postęp w wielu dziedzinach związanych z rozpoznaniem i WE, przekazywaniem oraz przechowywaniem informacji traktowanej jako źródło siły w nowoczesnych działaniach zgrupowań wojsk doprowadził do powstania koncepcji wojny (walki) sieciocentrycznej NCW (*Network Centric Warfare*)[104], którą szybko podchwycono i rozpropagowano w wielu państwach na świecie. Koncepcja ta ewoluowała, doprowadzając do powstania nowego jakościowo zjawiska, tworzącego sieciocentryczne środowisko działań wojsk. Na kanwie tych koncepcji wpisują się w przeszłe działania poszczególne rodzaje wojsk i służby. Walka elektroniczna nie jest wyjątkiem. Informatyzacja dostrzeżona została także przez specjalistów WE, a możliwości, jakie można osiągnąć we współczesnej walce elektronicznej, jeszcze nie zostały do końca odkryte.

---

[103] Por. A. i H. Tofler, *Wojna i antywojna*, wyd. cyt.
[104] M. Siedlecki, *Dużymi krokami w kierunku NEC*, „Przegląd Wojsk Lądowych" 2006, nr 10, s. 5.

Zarys rozwoju walki elektronicznej

Początków prowadzenia walki elektronicznej należy upatrywać z chwilą masowego wprowadzenia do wojsk środków radiowych i radiolokacyjnych. Ten ostatni środek w pierwszym okresie zdominował prowadzenie walki elektronicznej. Wprowadzenie radaru do wyposażenia wojsk datuje się już od momentu rozpoczęcia I wojny światowej. Jednocześnie z wprowadzeniem radaru jako nowego środka rozpoznawczego pracowano nad możliwościami jego „unieruchomienia", przewidywano bowiem, że radar może mieć decydujący wpływ na przebieg działań bojowych. Prace nad nim prowadzone były równolegle w kilku krajach. Do przodujących należy zaliczyć: Wielką Brytanię, Niemcy, USA, Związek Radziecki. Później dołączały inne państwa, tj. Japonia, Włochy, Francja.

Walka elektroniczna w początkowym okresie jej rozwoju skoncentrowana była na przeciwdziałaniu urządzeniom radarowym montowanym na lądzie, które prowadziły rozpoznanie nadlatujących samolotów, oraz przeciwko radarom kierowania ogniem artylerii. W miarę potrzep i postępu technologicznego przeniosła się ona na samoloty i okręty. Z uwagi na dużą autonomiczność tych ostatnich środków walki i ich możliwości rażenia radiolokatory służyły głównie do wykrywania sygnałów radiolokacyjnych systemów kierowania ogniem, lokalizacji miejsc rozmieszczenia. W podobny sposób wykorzystywano radary na okrętach.

Walka elektroniczna w początkowym okresie organizacji dzieliła się na rozpoznanie i przeciwdziałanie oraz maskowanie (głównie pasywne).

Prowadzenie rozpoznania radarowego polegało głównie na rozpoznaniu częstotliwości nośnej i kierunku nadejścia sygnału (z reguły na podstawie kierunku ustawienia anteny). Metody te były niedoskonałe. Dopiero w chwili wynalezienia radionamiernika sytuacja uległa znacznej poprawie.

Pierwsze radarowe systemy rozpoznawcze rozmieszczane były wzdłuż wybrzeży morskich. Posterunki radiolokacyjne ustawiano na kierunkach spodziewanych nalotów. Pierwsze systemy radarowe zorganizowano w Anglii. Kolejne w czasie II wojny światowej we Francji na terenach okupowanych przez Niemców. Zasięg prowadzonego rozpoznania wynosił średnio około 150 km.

Równolegle z prowadzonym rozpoznaniem rozwijano sposoby przeciwdziałania. W tym okresie stosowano dwa sposoby zakłóceń: aktywny i pasywny.

Zakłócenia aktywne polegały na uruchomieniu nadajnika zakłócającego znajdującego się na samolocie. Wykrycie radaru przez zbliżający się do sieci radarów samolot było łatwiejszym zadaniem niż wykrycie tego samolotu przez radar. Jeżeli zasięg radaru wynosił 100 km, to zasięg wykrycia radaru przez samolot był większy i wynosił około 150–200 km. Spowodowane to było zastosowaniem odbiornika radiolokacyjnego na samolocie o podobnej czułości jak w radarze. Ze względu na małą moc, jaką ma sygnał odbity od samolotu, samolotowy nadajnik zakłócający nie musi mieć takiej dużej mocy jak nadajnik radarowy. Jest on wobec tego mały i bez problemu mieści się w samolocie. Zakłócanie aktywne radaru jest wobec powyższego łatwe.

Zakłócenia pasywne polegały głównie na zrzucaniu z samolotu pasków metalizowanego papieru o odpowiednio dobranej długości, zależnej od długości fal pracy radaru. Każda rozsypana paczka pasków (kilkaset sztuk) dawała echo odpowiadające temu odbijanemu przez samolot bombowy[105].

Postęp w dziedzinie przeciwdziałania radioelektronicznego zależy w dużym stopniu od opracowania poszczególnych elementów, a zwłaszcza odnosi się do lamp elektronowych. Skonstruowanie magnetronów, klistronów, karcinotronów czy lamp z falą bieżącą spowodowało bardzo znaczny postęp w budowie radarów i ulepszaniu ich poszczególnych parametrów, tj. częstotliwości pracy, rozróżnialności celów, zasięgu, mocy. Największy rozwój radarów związany był ze zwiększeniem częstotliwości pracy. Nie wszystkie państwa potrafiły opanować najnowsze technologie, w związku z powyższym trwał ciągły wyścig technologiczny.

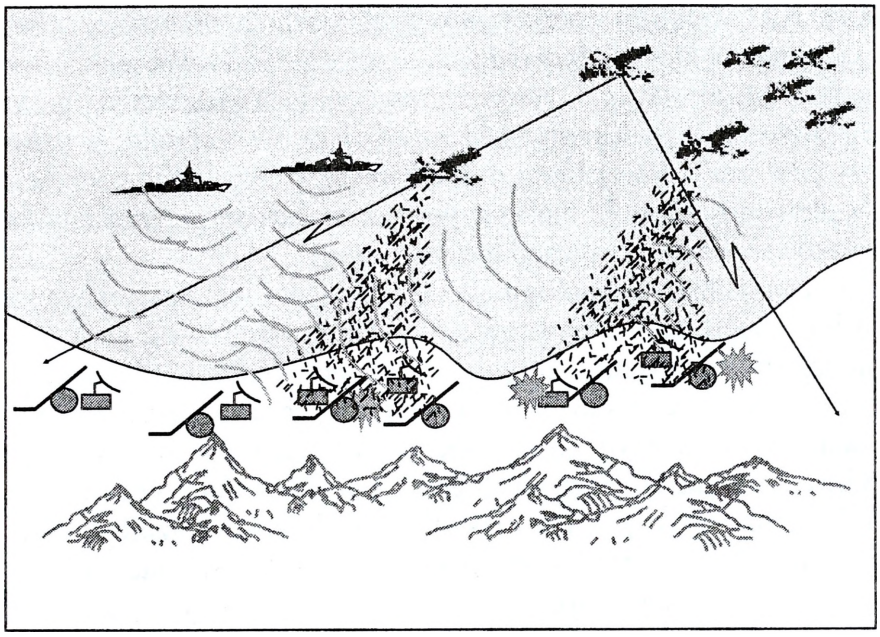
Rozpoznanie i zakłócanie radioelektroniczne w pierwszej połowie XX wieku było uważane za wyścig z czasem. Ich powodzenie zależało od właściwego zorganizowania współpracy placówek naukowych, zakładów produkcyjnych i jednostek walczących. Dużą rolę w tym wyścigu odegrał wywiad wojskowy, dostarczający informacji o przygotowaniach przeciwnika w zakresie produkcji radarów i kierunków rozwojowych w tej dziedzinie.

Walka elektroniczna to nie tylko wyścig z czasem, lecz również wyścig pod względem produkcji urządzeń, które mogą pracować na nowych częstotliwościach i wysyłać jak największą energię. Był to więc wyścig zakresów częstotliwości i wyścig mocy nadajników.

Scenariusz działania środków WE ukształtował się w latach 40., głównie podczas II wojny światowej. Ponieważ radary obserwacji przestrzeni powietrznej miały niskie czułości, działania środków zakłócających i rozpoznawczych przeniesiono w powietrze. Drugim czynnikiem, który ukształtował działania środków WE z powietrza, było położenie walczących stron – przedzielone morzem. Zarówno SZ Niemiec jak i Wielkiej Brytanii oraz USA zmuszone były do działań poprzez naloty lotnictwa (do chwili lądowania w Normandii). Po obu stronach wybrzeża dla osłony własnego terytorium organizowano sieć posterunków radarowych. Posterunki radarowe ściśle współdziałały z obroną przeciwlotniczą. Aby pokonać OPL na wybrzeżu, należało najpierw ją rozpoznać, a następnie zakłócić radioelektronicznie. Planując nalot lotniczy, alianci prowadzili regularne loty rozpoznawcze wzdłuż wybrzeża. Przechwycone informacje służyły do ustalenia częstotliwości roboczych SRL. Na bazie tych częstotliwości można było odpowiednio przygotować paski odbijające i aktywne stacje zakłócające. W następnej kolejności w rejon przekraczania wybrzeża morskiego wysyłane były niewielkie grupy bombowców celem zniszczenia urządzeń radiolokacyjnych. Po wykonaniu nalotu bombowego następował właściwy nalot, poprzedzany samolotami zakłócającymi rozrzucającymi paski metalizowanej folii w połączeniu z aktywnymi zakłóceniami. Całość tych

[105] W czasie II wojny światowej elementy odbijające nosiły nazwę „Window", a w późniejszym czasie wprowadzono nowe elementy o nazwie „Rope". *Zagadnienia wojny elektronicznej w Stanach Zjednoczonych*, WPZ 1961, s. 11.

działań była zabezpieczana i nadzorowana przez samolot rozpoznawczy dyżurujący na dużej wysokości. Po rozrzuceniu pasków folii następował nalot właściwy, w którym także stosowano zakłócenia aktywne przeciwko radiolokatorom przeciwlotniczym kierującym środkami artyleryjskimi (rys. 1).



Opracowanie własne.

Rys. 1. Scenariusz działania środków WE w czasie II wojny światowej

Dodatkowo w działaniach połączonych okręty marynarki wojennej prowadziły rozpoznanie i zakłócanie radarów nabrzeżnych, wspomagając wykonanie zadania przez lotnictwo.

Przedstawiony scenariusz działania środków WE przetrwał prawie w niezmienionej formie do lat 60. i 70., a nawet do czasów współczesnych. Dodano środki bezpilotowe jako elementy pozorujące i podnoszące gotowość bojową w systemach obrony przeciwlotniczej przeciwnika. Drugim istotnym elementem są samoloty WE dyżurujące w strefach i prowadzące ciągłe oddziaływanie na systemy elektroniczne przeciwnika.

Jak wynika z uwarunkowań historycznych, WE rozwinęła się głównie w powietrzu i na morzu w państwach zachodnich, natomiast w państwach wschodnich głownie na lądzie. Powodów takiego podziału jest kilka. Jedne z głównych to: niski stopień wiedzy i dostępnych technologii mikrofalowych, niskie nakłady finansowe, brak naukowców i ośrodków naukowych oraz konieczność odbudowy kraju po zniszczeniach wojennych, a dopiero w drugiej kolejności nakłady finansowe na rozbudowę urządzeń wojskowych.

Gwałtowny postęp w takich dziedzinach nauki, jak elektronika, informatyka, wymusił rozwój innych technologii i gałęzi przemysłu związanych z elektroniką i prowadzeniem działań WE. Kolejne dekady XX wieku to burzliwy rozwój urządzeń rozpoznania i zakłócania radiowego, radionawigacyjnego, radioliniowego, środków maskowania elektronicznego, pozoracji elektronicznej. Ostatnia dekada XX i początek XXI wieku to dominacja w systemach satelitarnych, informatycznych, czujnikowych, w których prowadzi się rozpoznanie i zakłócanie już nie tylko w spektrum fal EM, ale także w innych przestrzeniach pola walki (pola magnetyczne, fale akustyczne). Systematycznie rozwijające się technologie mikrofalowe spowodowały powstanie nowej broni mikrofalowej działającej w oparciu o impulsy elektromagnetyczne. Została ona przyporządkowana do przeciwdziałania elektronicznego jako element neutralizacji elektronicznej.

Najnowsze osiągnięcia technologii elektronicznych i informatycznych w zakresie przekazu informacji legły u podstaw tworzenia nowych teorii walk, wśród których dominującą rolę zaczynają odgrywać działania w środowisku sieciocentrycznym. Połączenie sensorów nadawczych i odbiorczych siecią przekazu informacji w czasie nieomal rzeczywistym są stymulatorem kreującym nowe koncepcje prowadzenia WE. Konieczność profesjonalnego prowadzania przyszłych wojen stwarza wymogi dla automatyzacji wielu urządzeń WE. Szybkość działania i reakcji na zachodzące zmiany stawia przed systemami WE wysokie wymagania sprawności pracy, kierowania, które muszą być spełnione, aby możliwe było działanie systemu WE w środowisku sieciocentrycznym.

Wymagania stawiane systemom WE

Charakter działań sieciocentrycznych i zmieniająca się w ślad za tym taktyka prowadzenia działań wojennych są źródłem generowania wymagań względem systemu WE. Ponieważ proces ten trwa nieustannie, zbiór wymagań nie może mieć charakteru zamkniętego. Zatem tworząc zbiór otwarty wymagań pod adresem organizowania systemu WE dla potrzeb działań sieciocentrycznych[106] realizowanych przez system WE, należy rozważyć wstępnie następujące grupy problemów:

– wielkość obszaru odpowiedzialności prowadzenia WE,

– ukształtowanie terenu i warunki meteorologiczne w obszarze odpowiedzialności prowadzonej WE,

– warunki rozprzestrzeniania się fal elektromagnetycznych i innych fal, np. akustycznych w obszarze prowadzonej WE,

– charakter działań sieciocentrycznych, w tym szczególnie realizacja nadzorowania pracy źródeł elektronicznych przeciwnych oraz źródeł elektronicznych innych sił destabilizujących sytuację w danym obszarze,

[106] Zakładamy, że działania sieciocentryczne będą miały ograniczony zasięg do konkretnego zdefiniowanego obszaru, w którym prowadzone będą działania bojowe.

– stan infrastruktury telekomunikacyjnej, radiowej, radiolokacyjnej, radionawigacyjnej, satelitarnej i innych urządzeń elektronicznych w obszarze odpowiedzialności prowadzonych działań WE,

– charakter zadań zespołów funkcjonalnych organów WE.

Na podstawie podanego zbioru problemów można sądzić, że wymagania w stosunku do organizowania systemu WE powinny obejmować:

– warunki dostępu fizycznego i energetycznego do źródeł elektronicznych przeciwnika, które muszą być wystarczające, aby możliwe było ich rozpoznanie, umiejscowienie oraz przeciwdziałanie w całym obszarze działań sieciocentrycznych bez względu na ich charakter i dynamikę działań,

– przygotowanie do pracy systemów WE w warunkach dużej intensywności oddziaływania elektromagnetycznego przeciwnika,

– wysoką trwałość (żywotność), mobilność, przepustowość i bezpieczeństwo działania systemu WE we wszystkich fazach działań sieciocentrycznych,

– szybką dystrybucję danych (wewnętrzną i zewnętrzną) dla wszystkich pododdziałów i dowództw zainteresowanych tymi informacjami,

– współpracę z innymi systemami rozpoznawczymi i WE, uczestników walki,

– gromadzenie danych w bazach danych i wykorzystanie treści tam zawartych do identyfikacji źródeł lub obiektów.

Jednym z ważniejszych wymagań podczas organizowania systemu WE w działaniach sieciocentrycznych jest wiarygodność i dostępność do uzyskanych danych. Zdobycie przez systemy walki elektronicznej danych na potrzeby oceny sytuacji i środków ogniowych jest wymaganiem wynikającym bezpośrednio z zakresu zadań systemu WE. Jest jednocześnie warunkiem koniecznym podczas działań sieciocentrycznych na każdym poziomie dowodzenia. Organa WE muszą bowiem w krótkim czasie zebrać, przetworzyć i przekazać dane o źródłach lub obiektach elektronicznych i jednocześnie kontrolować stan realizowanych przez podwładnych zadań. Proces ten przebiega równocześnie w pionowych i poziomych strukturach systemu WE, a organa WE pełnią funkcję dowódczo-koordynującą z miejsc pracy określonych regulaminowo jako stanowiska dowodzenia, dlatego wymagają również, aby miały:

– zapewnioną bezpośrednią łączność odzwierciedlającą nadzór nad prowadzoną walką elektroniczną przez desygnowane systemy WE,

– zapewnioną łączność na zasadzie „każdy z każdym w dowolnym czasie i miejscu pobytu" w obszarze odpowiedzialności prowadzonej WE w środowisku sieciocentrycznym.

Spełnienie wymagań wynikających ze współdziałania z innymi systemami WE lub systemami rozpoznawczymi i jednoczesna szybka dystrybucja danych mogą nastąpić poprzez wyposażenie miejsc pracy (wozów dowodzenia WE) w środki dystrybucji danych, do których można zaliczyć: szerokozakresowe radiostacje sprzężone z terminalami abonenckimi zaprogramowane do pracy w odpowiednich sieciach i kierunkach radiowych, wykorzystywanie relacji radioliniowych i systemów komputerowego nadzoru przekazów danych lub pracę w sieciach informatycznych (LAN

i WAN). Na obecnym etapie technicznego wyposażenia pododdziałów WE to wymaganie nie w pełni jest jeszcze spełnione. Możliwości funkcjonalne analizowanego systemu WE są niewystarczające. W ekstremalnie niekorzystnych warunkach istniejąca sieć łączności nie zapewnia przepływu danych i dowodzenia elementami WE, dlatego istnieje pilna potrzeba wyposażenia pododdziałów WE w sprzęt łączności zdolny spełnić wymagania środowiska sieciocentrycznego.

System WE wszechstronnie spełniający wymagania środowiska sieciocentrycznego powinien powstać w efekcie kompleksowego rozwiązania problemów organizacyjnych i technicznych zawartych w zasadzie „każdy z każdym w dowolnym czasie i miejscu". Rysuje się tu nowa trudność, bowiem wymagania organów dowodzenia będą rosły niemalże z każdą chwilą, a system WE jako struktura dość statyczna nie jest przygotowany na spełnienie takich warunków w krótkim czasie.

Czynnikami powodującymi generację dalszych wymagań będą:

– nowoczesne środki walki wywierające wpływ na prowadzenie działań w środowisku sieciocentrycznym,

– sposoby rozpoznania oraz przeciwdziałania środkom elektronicznym wykorzystywanym przez nowoczesne środki walki,

– wzrastające trudności w możliwościach rozpoznawania, zakłócania i lokalizacji źródeł EM i innych źródeł promieniowania, np. fal akustycznych czy pól magnetycznych będących w zasięgu dostępności fizycznej i energetycznej systemu WE,

– wzrastające potrzeby działania systemu WE w sposób nieregularny, rozproszony („plaster miodu"),

– wzrastające potrzeby działania w sposób nieregularny zespołów funkcjonalnych organów systemu WE poza stanowiskami dowodzenia,

– trudne do przewidzenia zmiany struktur organizacyjnych systemów WE, organów kierowania WE w dynamicznie zmieniającym się środowisku sieciocentrycznym.

Wymienione czynniki mogą w istotnym stopniu zmniejszyć lub zwiększyć możliwości eksploatacyjne systemu WE. Sprawność działania każdego systemu determinowana jest przez jego najsłabsze ogniowo. W systemach WE najsłabszym ogniwem są systemy łączności. Środowisko sieciocentryczne wymusza jakościowo inne podejście do problematyki utrzymywania łączności w systemie i z innymi systemami. Dotychczasowa łączność radiowa jest zawodna i mimo coraz doskonalszych radiostacji (np. szerokopasmowych) ma określone obostrzenia, np. dotyczące przepustowości. Należy szukać nowych rozwiązań. Kierunkiem, który przy obecnym rozwoju techniki i technologii najbardziej jest predysponowany do natychmiastowego i niezawodnego utrzymywania łączności (przekazu informacji), są sieci i systemy informatyczne. Traktowanie ich jako medium transmisyjnego z jednoczesnym zarządzaniem i kierowaniem systemami rozpoznania i przeciwdziałania jest rozwiązaniem, które wpisuje się w technologie środowiska sieciocentrycznego. Systemy informatyczne mogą pełnić rolę integracyjną wszystkich sensorów WE używanych na polu walki. Patrząc jednak realnie, nie należy utożsamiać systemów łączności WE tylko z sieciami informatycznymi. Łączność radiową należy nadal utrzymywać, doskonalić ją i traktować jako równoległy element łączno-

ści. Sieci informatyczne mogą tworzyć bazę i stanowić podstawę do dystrybucji informacji, gromadzenia wyników rozpoznania i przeciwdziałania, kierowania sensorami WE, ale nie mogą być jedynym elementem łączności.

W procesie zarządzania i kierowania walką elektroniczną w środowisku sieciocentrycznym wykorzystywane systemy informatyczne muszą zapewnić sprawne funkcjonowanie zorganizowanego systemu WE. Zaproponowane przez P. Delę sieci szkieletowe są jednym z rozwiązań tego problemu. Sieci szkieletowe pozwalają zachować istotne właściwości całego systemu. Do takich właściwości zalicza się: jedność kierowania (*Unity of Command*), ciągłość kierowania (*Continuity of Command*), przejrzystą strukturę systemu kierowania (*Clear Chain of Command*), integrację kierowania (*Integration of Command*) oraz decentralizację kierowania (*Decentralization of Command*)[107].

Teoria prowadzenia WE w działaniach sieciocentrycznych wyróżnia szereg wymagań, które powinny być spełnione przez organizatorów systemu WE. Można je podzielić na dwie podstawowe podgrupy: wymagania operacyjne i wymagania techniczne.

Wymagania operacyjne

Wymagania operacyjne wynikają w głównej mierze z faktu, że wykorzystywane systemy WE są systemami złożonymi i działają w ramach funkcjonowania innych systemów WE, zarówno podrzędnych, równorzędnych, jak i nadrzędnych. Wykorzystywane systemy powinny być ze sobą w pełni kompatybilne (mieć możliwość wymiany pomiędzy sobą informacji). Z tego względu można wyróżnić pięć podstawowych wymagań operacyjnych, a mianowicie: gotowość traktowaną jako dostępność systemu WE do pracy w każdym środowisku, szybkość rozpoznania i dystrybucji informacji, terminowość, precyzję lokalizacji źródeł elektronicznych (ŹE), pewność przeciwdziałania elektronicznego. Wynikają one przede wszystkim z zadań stawianych przed organizowanym systemem walki elektronicznej i decydują o ich skuteczności operacyjnej.

Gotowość (dostępność) jest to zdolność systemu WE do terminowego przejścia z jednego stanu do innego, niezbędnego do zapewnienia kierowania systemem WE. Dostępność osiąga się poprzez stworzenie odpowiedniej struktury organizacyjno-funkcjonalnej systemu WE, w skład której wchodzą także właściwe procedury oraz wyposażenie techniczne pozwalające na realizację wyznaczonych zadań w każdym środowisku. Do podstawowych wskaźników określających gotowość (dostępność) należy zaliczyć czas przejścia systemu WE do stanu pełnej wydajności i prawdopodobieństwo terminowego wykonania zaplanowanych przedsięwzięć w określonym czasie. Należy zauważyć, że do osiągnięcia gotowości systemu WE niezbędny jest wysoki poziom wyszkolenia personelu technicznego utrzymującego ten system.

---

[107] P. Dela, *Sieci informatyczne rozwijane na potrzeby systemu walki elektronicznej*, seminarium w ZRiWE nt. „Walka elektroniczna w działaniach sieciocentrycznych", AON, Warszawa 2008.

Szybkość rozpoznania to zdolność systemów (urządzeń) rozpoznawczych do natychmiastowego rozpoznania ŹE i identyfikacji, wykorzystując do tego dane zawarte w bazach danych. Określana jest ona jako czas wykrycia, identyfikacji i przekazu informacji od efektora do decydenta przy ustaleniu określonych priorytetów dla rozpoznawanych ŹE.

Terminowość dystrybucji informacji stanowi zdolność systemów łączności (informatycznych) do przekazywania informacji w określonym czasie. Jest ona określana jako prawdopodobieństwo przesyłania informacji w czasie, który nie przekracza dopuszczalnych wartości dla ustalonych priorytetów przesyłanych informacji przy uwzględnieniu obciążenia systemów łączności (informatycznych). Z badań wynika, że systemy informatyczne powinny zapewnić dostęp do niezbędnych usług i informacji w czasie rzeczywistym lub zbliżonym do rzeczywistego.

Precyzja lokalizacji ŹE to zdolność systemu namierzania do określenia miejsca znajdowania się ŹE na podstawie określenia kierunków, z których do systemu antenowego dociera energia od emitującego ŹE z zadaną dokładnością przy uwzględnieniu istniejących zakłóceń i zniekształceń. Warunkiem koniecznym do uzyskania lokalizacji jest praca aktywna ŹE i posiadanie systemu namierników składających się minimum z dwóch urządzeń namierzających. W nowoczesnych systemach namierzających miarą jakości lokalizacji jest prawdopodobieństwo wystąpienia minimalnej stopy błędów w trójkącie błędu. Precyzja lokalizacji uzależniona jest w dużej mierze od jakości urządzeń (ich automatyczności, jakości wykonania, czułości elementów), pola antenowego (usytuowania, rozstawienia anten, wypionowania), warunków meteorologicznych. Przy automatycznych systemach lokalizacji czynnik ludzki traktowany jako jeden z elementów wprowadzania błędów jest zbyteczny i może służyć tylko jako nadzór nad pracującymi urządzeniami.

Pewność (skuteczność) przeciwdziałania elektronicznego to zdolność do pozbawienia odbioru informacji przesyłanej przez środki elektroniczne przeciwnika. Polega na dostarczeniu do zakłócanego urządzenia odbiorczego takiej porcji energii zakłócającej, która przy jego parametrach technicznych, rodzaju pracy oraz warunkach taktycznych uniemożliwi poprawne odebranie sygnału użytecznego.

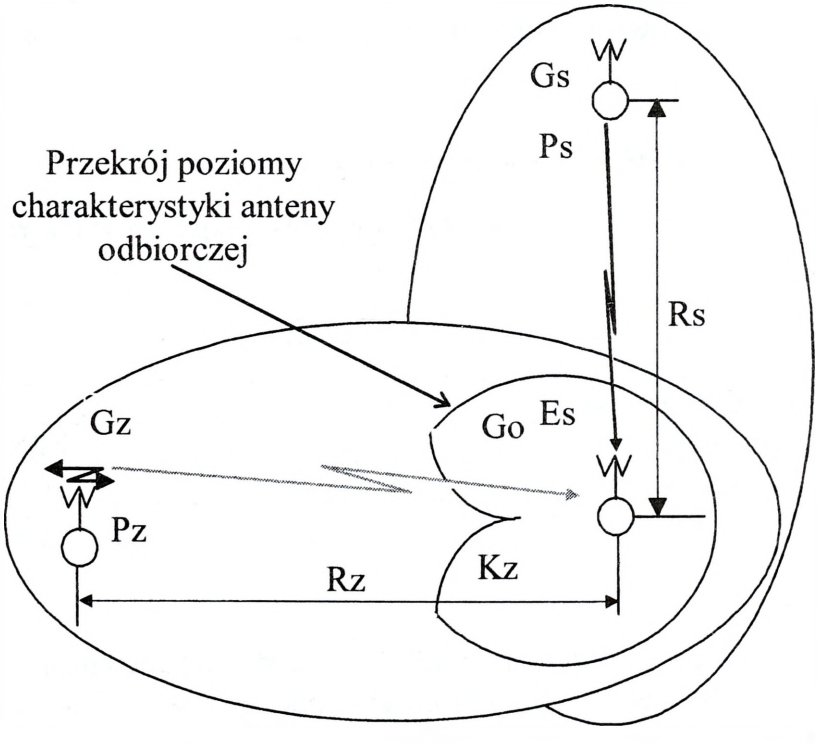
W wyniku stosowania przeciwdziałania elektronicznego dopływ informacji do dowództw i sztabów oraz do wojsk i środków walki na pewien czas może być całkowicie przerwany. Brak informacji lub mały stopień ich wiarygodności uniemożliwia lub utrudnia realizację terminowego, skoordynowanego i operatywnego dowodzenia wojskami i kierowania środkami walki. Niedostatek informacji w poważnym stopniu obniża efektywność bojową wojsk, ich siłę uderzeniową i skuteczność działań, uniemożliwia terminowe wykonanie zadań bojowych i bardzo często prowadzi do znacznych strat w sile żywej i sprzęcie bojowym.

Przeciwdziałanie elektroniczne może być prowadzone selektywnie w stosunku do wybranych obiektów i ŹE lub zaporowo (szerokopasmowo) w wybranych sektorach. Taki podział nie jest nowy, ale w środowisku sieciocentrycznym nabiera szczególnego znaczenia. Musimy mieć pewność, że stosowane zakłócenia oddziaływają na konkretne ŹE, wcześniej przewidziane do zakłócania. Nie powinno się

zakłócać wszystkiego (to jest niemożliwe). Wybór odpowiednich obiektów lub częstotliwości przeznaczonych do zakłócania stanowi podstawę do zaplanowania miejsca i czasu działania dla wojsk operacyjnych.

Stosowanie selektywnych zakłóceń łączności radiowej, w zakresie ultrakrótkofalowym i krótkofalowym na fali przyziemnej, zależy od następujących zasadniczych (rys. 2) czynników:

- mocy nadajnika stacji zakłócającej wykorzystywanej do zakłócania łączności radiowej przeciwnika (Pz),
- mocy radiostacji przeciwnika przekazującej informacje w zorganizowanych relacjach łączności (Ps),
- odległości między nadajnikiem a odbiornikiem w zakłócanych relacjach łączności przeciwnika (Rs),
- odległości między urządzeniem odbiorczym (zakłócanym) a stacją (nadajnikiem) zakłócającą (Rz),
- współczynnika zysku kierunkowości anteny radiostacji przeciwnika (Gs) i stacji zakłócającej (Gz),
- współczynnika zakłóceń określonego dla danego rodzaju pracy i typu środka łączności (Kz),
- współczynnika tłumienności anteny odbiornika z kierunku na stację zakłócającą (Go).



Opracowanie własne.

Rys. 2. Czynniki wpływające na skuteczność zakłóceń radiowych

Wszystkie wymienione czynniki decydujące o skuteczności zakłócania są ze sobą ściśle współzależne. Podczas oceny skuteczności zakłóceń należy wziąć pod uwagę fakt, że urządzenia odbiorcze mogą być zakłócone przy odpowiednim poziomie sygnału zakłócającego w stosunku do sygnału użytecznego w miejscu jego rozwinięcia. Stosunek ten przyjęto nazywać współczynnikiem zakłóceń. Współczynnik zakłóceń (Kz) jest wyrażany stosunkiem natężenia pola elektrycznego pochodzącego ze stacji zakłócającej (Ez) do natężenia pola elektrycznego pochodzącego z nadajnika pracującej radiostacji (Es), mierzonego na wejściu antenowym zakłócanego odbiornika. W teorii zakłóceń wyróżnia się dwa rodzaje współczynników zakłóceń: według napięcia (natężenia pola elektrycznego) i według mocy sygnału zakłócającego oraz użytecznego, które można przedstawić w postaci zależności:

$$Kz^{E} = \frac{Ez}{Es} \text{ lub } Kz^{P} = \frac{Pz}{Ps} \qquad [1]$$

Aby skutecznie zakłócać dany środek elektroniczny, powinien być zapewniony odpowiednio wysoki, tzw. wymagany współczynnik zakłóceń, którego wartość jest wyznaczana doświadczalnie i zależy od rodzaju sprzętu, jego parametrów technicznych, a przede wszystkim rodzaju sygnału (emisji) bezpośrednio związanego z rodzajem pracy. Wartości wymaganych współczynników zakłóceń (Kz_w) dla konwencjonalnego odbiornika superheterodynowego przedstawiono w tabeli 1.

Tabela 1

Wartość wymaganego współczynnika zakłóceń (Kz_w)

Rodzaj emisji	Wymagana wartość współczynnika zakłóceń	
	wg natężenia pola (Kz_w^E)	wg mocy (Kz_w^P)
Manipulacja amplitudy	0,8	0,64
Manipulacja częstotliwości	1–1,1	1–1,21
Modulacja amplitudy	1,5–2	2,25–4
Modulacja jednowstęgowa	4–5	16–25
Modulacja częstotliwości	1,5	2,25

Opracowanie własne.

Na wyznaczenie współczynników zakłóceń oczekują takie emisje, jak: rozproszone emisje szerokopasmowe, FH szumopodobne, cyfrowe, modulowane fazowo oraz inne, pojawiające się w spektrum elektromagnetycznym.

Zależności [1], po odpowiednim rozwinięciu, można przedstawić jako ocenę skuteczności zakłóceń (Kz_{RZ}^E):

$$K^{E}_{z_{rz}} = \left(\frac{R_s}{R_z}\right)^2 * \sqrt{\frac{P_z * G_z * G_o}{P_s * G_s}} \qquad [2]$$

Jeżeli $K^{E}_{z_{rz}} \rangle K_{z_w}$ (uwzględnianego dla danego rodzaju pracy radiostacji), to oceniana linia łączności będzie skutecznie zakłócona, w przeciwnym wypadku ww. linia jest odporna na zakłócenia.

Natomiast ocenę głębokości skutecznych zakłóceń (Rz_{sk}) można przedstawić za pomocą:

$$R_{zsk} = R_s * \sqrt[4]{\frac{P_z * G_z * G_o}{Ps * K^2_{z_w} * G_s}} \ \textbf{[km]} \qquad [3]$$

Ocenę skutecznej mocy zakłóceń (Pz_{sk}) natomiast za pomocą:

$$P_{zsk} = \frac{Ps * R_z^4 * G_s * K^2_{z_w}}{R_s^4 * G_z * G_o} \ \textbf{[W]} \qquad [4]$$

Dla oceny skuteczności zakłóceń łączności KF i UKF w relacjach samolot--samolot i ziemia-samolot, gdzie nie występuje zjawisko tłumienia fal elektromagnetycznych przez pokrycie terenu, celowe jest wykorzystanie przedstawionych niżej zależności:

1. Ocena skuteczności zakłóceń $\left(K^{E}_{z_{rz}}\right)$:

$$K^{E}_{z_{rz}} = \frac{R_s}{R_z} * \sqrt{\frac{P_z * G_z * G_o}{P_s * G_s}} \qquad [5]$$

Jeżeli $K^{E}_{z_{rz}} \rangle K_{z_w}$ (uwzględnianego dla danego rodzaju pracy radiostacji), to oceniana linia będzie skutecznie zakłócona, w przeciwnym wypadku ww. linia jest odporna na zakłócenia.

2. Ocena głębokości skutecznych zakłóceń (Rz_{sk}):

$$R_{zsk} = R_s * \sqrt{\frac{P_z * G_z * G_o}{Ps * K^2_{z_w} * G_s}} \ \textbf{[km]} \qquad [6]$$

3. Ocena skutecznej mocy zakłóceń (Pz_{sk}):

$$P_{zsk} = \frac{Ps * R_z^2 * G_s * K^2_{z_w}}{R_s^2 * G_z * G_o} \ \textbf{[W]} \qquad [7]$$

Dla emisji FH (*frequency hopping*) istotnym czynnikiem zapewniającym skuteczność zakłóceń jest czas zakłócania sygnału na jednej częstotliwości. Wynosi on nie mniej niż 50%. W niektórych przypadkach przez zakłócanie końcowych sekwencji sygnału (synchronizujących) można doprowadzić do zerwania współpracy w pracujących sieciach, co prowadzi do braku możliwości przekazywania informacji.

Wymagania techniczno-eksploatacyjne

Wymagania techniczno-eksploatacyjne dla systemów WE działających w środowisku sieciocentrycznym związane są z efektywnością i właściwym funkcjonowaniem organizowanego systemu WE. Wymagania techniczne definiują istotne właściwości wykorzystywanych środków rozpoznawczych zakłócających oraz zasady ich funkcjonowania. Z przeprowadzonych badań wynika, że do głównych wymagań technicznych systemów WE związanych z funkcjonowaniem i przekazywaniem informacji można zaliczyć:

- przepustowość systemu,
- odporność systemu na oddziaływanie elektroniczne i ogniowe,
- bezpieczeństwo systemu,
- mobilność,
- niezawodność,
- uniwersalność koordynacyjną działań.

Przepustowość systemu WE dotyczy w głównej mierze systemów łączności wykorzystywanych w systemach WE. W odniesieniu do działań sieciocentrycznych przepustowość systemu odnosi się do sieci informatycznych lub zaproponowanych wcześniej sieci szkieletowych. Przepustowość systemu łączności określana jest przez potencjalne możliwości tych systemów w zakresie transmisji odpowiednich strumieni danych w jednostce czasu. Jest ona ustalana dla poszczególnych relacji wymiany informacji (pary węzłów, kanału łączności, linii telekomunikacyjnych). Ważne jest także zapewnienie niezbędnego pasma transmisji danych dla najniższych szczebli kierowania, co umożliwi pozyskiwanie informacji o zaistniałej sytuacji od ŹE. Do podstawowych wskaźników określających przepustowość systemu łączności (informatycznego) można zaliczyć: maksymalną szybkość transmisji, ilość podstawowych kanałów w relacji łączności, wartość oczekiwaną ilości kanałów w relacji łączności.

Odporność (trwałość) systemu WE to jego zdolność do pracy podczas oddziaływania energią EM ze strony przeciwnika, jego środków rażenia (ogniowego i impulsem EM), a także różnorodnych czynników zewnętrznych związanych w głównej mierze z niekorzystnym oddziaływaniem warunków meteorologicznych, terenowych itp. Odporność na zakłócenia systemu WE definiuje się jako zdolność tego systemu do realizacji zamierzonych (zaplanowanych) zadań w warunkach oddziaływania wszystkich rodzajów zakłóceń elektronicznych i rażenia ogniowego (w tym impulsem EM). Niezawodność pracy systemu WE to nic innego jak zdolność do wykonania postawionych zadań przy zachowaniu odpowiednich wartości parametrów eksploatacyjnych sprzętu rozpoznawczego i zakłócającego.

Do podstawowych wskaźników określających odporność systemu WE należy m.in. zaliczyć: współczynnik sprawności, średni czas poprawnej pracy systemu WE, prawdopodobieństwo, że czas przerwy w pracy systemu nie przekroczy dopuszczalnej wartości.

Mobilność systemu WE determinowana jest poprzez rodzaj przeznaczonych do przemieszczania całości systemu platform. Mobilność jest właściwością systemu, która przejawia się zdolnością do sprawnego i terminowego odtworzenia struktury ugrupowania poszczególnych podsystemów WE po dokonanej zmianie miejsca położenia. Mobilność można określić wskaźnikami: prawdopodobieństwem terminowego wykonania zadania w zakresie zmiany struktury i funkcjonalności systemu WE, granicznym czasem zmiany miejsca położenia i czasem wykonania zadań walki elektronicznej z określoną niezawodnością.

Bezpieczeństwo systemu WE rozumiane jest jako zdolność tego systemu do przeciwstawienia się wszystkim rodzajom zagrożeń, w tym: zagrożeniom bezpośrednim (napaść, zniszczenie, kradzież lub zniszczenie sprzętu), zagrożeniom pośrednim (podsłuch, modyfikacja danych, odmowa usługi, dezinformacja). Zapewnienie bezpieczeństwa systemu WE należy do zadań najtrudniejszych i najbardziej skomplikowanych. Chronić system WE to zapewnić odpowiednią skrytość działań zarówno w przestrzeni elektromagnetycznej, jak i przed rozpoznaniem bezpośrednim. Maskowanie działalności bojowej związane jest ściśle z obroną elektroniczną systemów WE, której jednym z elementów jest ochrona własnych systemów przed rozpoznaniem elektronicznym przeciwka oraz maskowanie własnych działań. Przedsięwzięcia te wymagają zarówno działań organizacyjnych, jak i rozwiązań technicznych.

Niezawodność systemu WE to zdolność do natychmiastowej pracy bojowo-rozpoznawczej całości systemu lub poszczególnych jego elementów w każdych warunkach meteorologicznych i środowisku (przestrzeniach) elektromagnetycznym albo innym środowisku, z którego pozyskiwane są dane. Niezawodność uzyskuje się poprzez utrzymywanie w ciągłej sprawności sprzętu elektronicznego i przystosowanie go do odbioru wszystkich możliwych sygnałów (EM, magnetycznych, akustycznych itd.).

Uniwersalność koordynacyjna działań to zdolność do kierowania WE przez zespoły do tego powołane we wszystkich rodzajach działań (pokojowych, operacyjnych, stabilizacyjnych) ze stanowisk dowodzenia przygotowanych do tych działań. Uniwersalność koordynacji działań obejmuje funkcjonowanie własnych systemów WE wszystkich RSZ i systemów WE innych krajów (sojuszu) działających wspólnie, np. w operacjach stabilizacyjnych. Uniwersalność koordynacyjna to także możliwość wspólnego działania w ramach zwalczania przeciwnika w powietrzu, np. w ramach SEAD, przeciwdziałania terroryzmowi lub innych działań o podobnym charakterze.

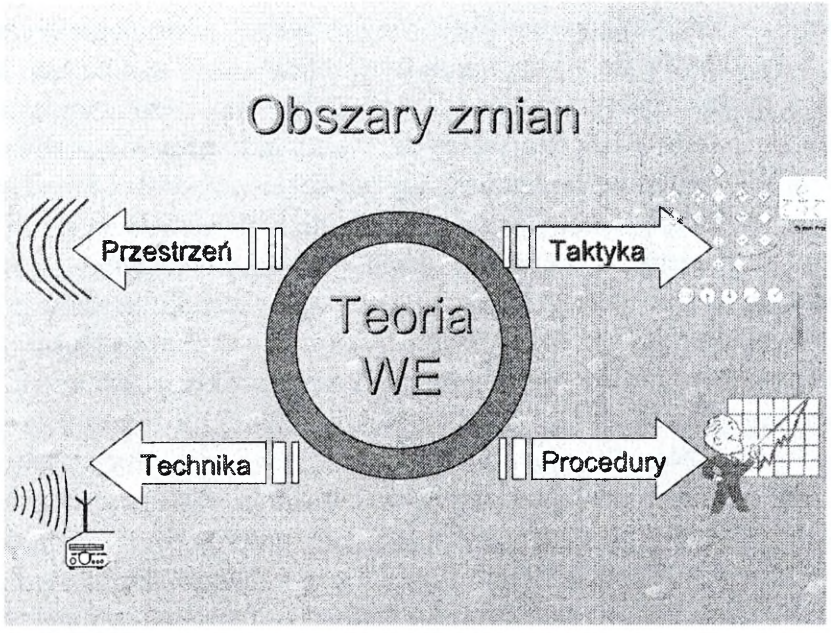
Obszary zmian działalności systemu WE w środowisku sieciocentrycznym

Szybki postęp naukowo-techniczny, albo wręcz kolejny etap rewolucji technologicznej, to zasadniczy element decydujący o kierunkach transformacji systemów WE. Przewaga techniczna i technologiczna pozostanie jednym z podstawowych kryteriów skutecznego prowadzenia rozpoznania i przeciwdziałania elektronicznego. Nasze myślenie o nowoczesnych systemach WE będzie wiarygodne i skuteczne wówczas, gdy będziemy zdolni zaadoptować przełomowe rozwiązania technologiczne. Twierdzenie, że „siła ognia jest potęgą" należy odrzucić, oddając pierwszeństwo informacji – „jeden gram krzemu zawartego w procesorze znaczy więcej niż tony klasycznych bomb i pocisków".

Dzisiaj nowoczesność czołowych armii świata kształtuje informatyzacja (rozpoznanie elektroniczne, przeciwdziałanie), broń satelitarna, impulsowa, nawigacja kosmiczna i broń precyzyjna, działania w sieciach internetowych. Nowa technika to potrzeba nowych ludzi – zawodowców. Dlatego też dalsza profesjonalizacja sił zbrojnych stanowi ważny warunek ich skutecznej transformacji. Jako docelowe rozwiązanie przyjmujemy całkowitą profesjonalizację, którą będziemy gotowi rozpocząć z dniem 1 stycznia 2010 roku. Proces ten powinien mieć charakter sekwencyjny, ponieważ taki wydaje się bardziej realny.

Nieustanny wyścig technologiczny pomiędzy systemami łączności, dowodzenia, kierowania, przekazu informacji a systemami przeciwdziałającymi i utrudniającymi pracę wspomnianych systemów doprowadza do nieustannego rozwoju środków i systemów elektronicznych. Środki łączności doskonalą sposoby przekazu informacji, a środki WE doskonalą się w ich zakłócaniu. Aktualnie można powiedzieć, że każdemu nowemu urządzeniu przeznaczonemu do przekazu danych towarzyszy powstanie nowego urządzenia zakłócającego jego pracę. Wyścig tych działań znajduje swoje odzwierciedlenie w działaniach, których podstawą są techniki radiowe, informatyczne, satelitarne, radioliniowe, czujnikowe. W przyszłych działaniach opartych na środowisku sieciocentrycznym nie ma już miejsca na urządzenia obsługiwane ręcznie. Dążenie do automatyzacji nieomal wszystkich możliwych procesów nadających się do zautomatyzowania jest już wymogiem koniecznym.

Zmiany technologiczne wymuszają na systemach walki elektronicznej budowanie takich systemów, które w sposób automatyczny będą pracowały w przestrzeni walki, bez ingerencji człowieka. Już dzisiaj należy budować i zmieniać teorię WE, dostosowując ją do środowiska sieciocentrycznego. Zmiany te dotyczą głównie przestrzeni prowadzenia WE, zastosowanych technik walki, związanych z tym taktyki wykorzystania sprzętu oraz sprawnego zarządzania systemami (rys. 3).



Opracowanie własne.

Rys. 3. Obszar zmian w prowadzeniu walki elektronicznej

Oczywiste jest, iż w przestrzeni elektromagnetycznej walka elektroniczna będzie nadal dominowała. Spektrum fal elektromagnetycznych jest i należy się spodziewać, że jeszcze długo pozostanie dominujące. Zbyt dużo jest urządzeń i systemów działających w oparciu o fale elektromagnetyczne, aby można było powiedzieć, że nadchodzi jej kres. Tym bardziej że nie odkryto jeszcze innego środowiska, mogącego zastąpić tak szeroko stosowane fale EM.

Można natomiast wyróżnić inne środowiska prowadzenia WE, które zaczęły odgrywać coraz większą rolę na polu walki. Można do nich zaliczyć: przestrzeń działania systemów informatycznych, przestrzeń akustyczną, pola magnetyczne. W wymienionych przestrzeniach na uwagę zasługuje przestrzeń informatyczna jako jedna z najbardziej prężnie rozwijających się gałęzi elektroniki, a ściślej informatyki. O ile w przestrzeni EM obserwuje się tendencję do wykorzystywania coraz to wyższych pasm częstotliwości, o tyle w informatycznej spotykamy już pojęcie globalizacji sieci, tzn. że jesteśmy w stanie łączyć się z każdego punku na Ziemi z kimkolwiek chcemy (jeżeli druga strona posiada komputer).

Przestrzeń akustyczna jako obszar rozpoznania jest dość powszechnie znana, bowiem wiele państw wykorzystuje urządzenia elektroniczne do rozpoznania dźwięków, np. system Rembas do rozpoznania strzelającej artylerii. Brakuje natomiast systemów i urządzeń do zakłócania pracy takich urządzeń. Należy więc się spodziewać również w tej dziedzinie postępu.

Urządzenia wykorzystujące indukcję magnetyczną (pole magnetyczne) wykorzystywane były głównie do wykrywania min i niewybuchów. Okazało się jednak, iż to zjawisko można wykorzystać do innych celów, np. rozpoznania linii telefonicznych lub do ochrony baz wojskowych, wkopując specjalne przewody detekcyjne. Istnieją też naukowe podstawy, aby pójść jeszcze dalej i wykorzystywać pole magnetyczne Ziemi do zakłócania przestrzeni. Dzisiaj wydaje się to fikcją, jak wiele rzeczy, które jeszcze niedawno wydawały się nieosiągalne, ale człowiek w dążeniu do zdobycia coraz większej wiedzy ciągle poszukuje nowych rozwiązań i dokonuje owych odkryć, nie należy więc wykluczyć, iż w przyszłości może także zdominować przestrzeń pola magnetycznego Ziemi do własnych potrzeb.

Kolejnym kierunkiem zmian w walce elektronicznej możliwej do wykorzystania w środowisku sieciocentrycznym jest nowoczesna technika. Kierunki zmian w technice WE uzależnione są od przewartościowania obszaru prowadzenia WE. Aktualnie WE w SZ RP prowadzona jest głównie w przestrzeni lądowej i częściowo morskiej. Przestrzeń powietrzna, mimo iż jest w państwach zachodnich dominująca, w SZ RP jest niedowartościowana. Należy zmienić ten stan rzeczy i zwiększyć oddziaływanie urządzeń WE w przestrzeni powietrznej, w przyszłości także rozpocząć działania w przestrzeni kosmicznej. Technika kosmiczna w niedalekiej przyszłości będzie wiodła prym w rozpoznaniu i lokalizowaniu obiektów i ŹE. W związku z powyższym rozpoznanie satelitarne stanie się jednym z głównych narzędzi prowadzenia WE. Dzisiejsze satelity wykorzystujące promienie laserowe są fikcją, ale w niedalekiej przyszłości należy spodziewać się, iż mogą wykorzystywać techniki skupionych energii do niszczenia ŹE, zakłócania urządzeń lub ich rozpoznania. Już dzisiaj satelity wykorzystywane są jako retlanslatory komunikacyjne (np. informacji z rozpoznania), urządzenia optoelektroniczne monitorujące duże obszary powierzchni kamerami o bardzo dużej rozdzielczości i szybkości robionych zdjęć lub filmów, jako urządzenia radiolokacyjne do rozpoznania obiektów stałych i ruchomych, rozpoznania pogody (radiolokatory meteorologiczne), a nawet do rozpoznania tego, co znajduje się pod powierzchnią ziemi.

Przewiduje się, że zmiany w technice dotyczyć będą integracji sensorów rozpoznawczych w jednym urządzeniu czujnikowym. Rozpoznanie i zakłócanie czujnikowe z uwagi na swój zasięg i małe konstrukcje może dominować szczególnie tam, gdzie człowiek i inne urządzenia nie będą miały dostępu. Modułowość urządzeń (zestawów) rozpoznawczo-zakłócających i związana z tym wymienność układów to już dzisiaj osiągalne technologie. Należy więc dążyć do gromadzenia jak największej ilości informacji o systemach elektronicznych przeciwnika, aby możliwe było wcześniejsze przygotowanie odpowiednich modułów rozpoznawczo-zakłócających.

Wszystkie urządzania WE powinny być odpowiednio spięte systemem łączności zdolnym do przekazywania danych w czasie nieomal rzeczywistym. Można to osiągnąć, automatyzując procesy rozpoznania, namierzania i zakłócania elektronicznego. Automatyzacja procesu WE jest jednym z najtrudniejszych przedsięwzięć dla instytutów i firm zajmujących się systemami walki.

Należy także przewidzieć, że automatyzacja działań WE wymusi korzystanie z urządzeń, które będą posiadały ograniczone możliwości podejmowania decyzji, czyli robotów. Będą to niezawodne i odporne na zakłócenia urządzenia, tanie w produkcji i skuteczne w działaniu.

Kierunek zmian w taktyce prowadzenia WE w środowisku sieciocentrycznym wiązać się będzie głównie z możliwościami oddziaływania w przestrzeni powietrznej na znacznie większe głębokości niż dotychczas. Ograniczony zasięg działania narzucał niejako taktykę do obszarów przyporządkowanych szczeblom organizacyjnym wojsk lądowych (brygada, dywizja, korpus, armia). Przeniesienie wysiłku w obszar powietrzny pozwala zwiększyć zasięg i zmienić taktykę szczególnie dla wojsk lądowych. Zmianie ulegną także poszczególne sposoby wykorzystania urządzeń do prowadzenia tych rodzajów rozpoznania, które do tej pory nie były rozpoznawane i zakłócane, np. systemy telekomunikacyjne GPS, GSM, optoelektroniki, informatyki. Odrębną dziedziną będzie posiadanie i wykorzystanie broni wiązkowej. W tej dziedzinie jeszcze wielu teoretyków prowadzi dyskusje, gdzie tę broń przyporządkować.

Zmian należy także upatrywać w wykorzystaniu nadajników zakłóceń jednorazowego użytku (NZJU). Taktyka użycia NZJU pociąga za sobą zmianę w technice ich budowy i przeznaczenia. Dzisiaj są to tylko urządzenia do zakłócania lub czasami traktowane są jako miny. W przyszłości mają to być sensory jako czujniki aktywne do rozpoznania i zakłócania. Przewiduje się nieco większe ich gabaryty. Zmiany w sposobach użycia NZJU to głównie:

- inny, lepszy rodzaj środka przenoszenia (MLRS, samolot, śmigłowiec, rakieta),
- zwiększenie zasięgu oddziaływania energią EM,
- możliwości rozpoznania i zakłócania większego spektrum fal EM w jednym urządzeniu z możliwością strojenia podczas zostawiania lub dolotu,
- zwiększenie czasu działania urządzenia,
- integracja różnych urządzeń rozpoznawczych i zakłócających w jednym urządzeniu,
- wykorzystanie po zużyciu źródła zasilania jako miny.

Zmiany w procedurach przygotowania i prowadzenia WE związane są głównie z trzema przedsięwzięciami, mianowicie z: wykorzystaniem wspomagających programów komputerowych do oceny i prognozowania zagrożeń, wykorzystaniem baz danych, zarządzaniem systemami WE poprzez automatyzowanie procesów dowodzenia WE. Optymalne ugrupowanie systemu WE będzie podpowiadane przez „inteligentne programy wspomagające" zarządzane z komórki koordynacji WE na SD. W związku z takim przepływem informacji automatyzacja procesów decyzyjnych będzie szybsza i będzie miała więcej możliwości przeanalizowania potencjalnych zdarzeń (warunek, że dostarczymy odpowiednie dane). Decydent odnosi się tylko do wyniku działań. Decyzja dotyczy nie tego, co zakłócać i rozpoznać, ale tego, czy zakłócić i rozpoznawać?

Podsumowanie

Dominacja spektrum elektromagnetycznego w WE jest niekwestionowana. Upłynie jeszcze wiele lat, nim inne obszary prowadzenia WE zrównają się ze spektrum EM albo gdy odkryjemy jeszcze inne obszary dotychczas niedostrzegalne dla naszych zmysłów.

Wymienione kierunki zmian w WE charakteryzują się jedną wspólną płaszczyzną – muszą być spięte systemem przekazu i przepływu informacji wewnątrz systemu i na zewnątrz, w poziomie i w pionie – słowem, należy zautomatyzować dowodzenie i kierowanie WE oraz wszystkimi rodzajami rozpoznania. Bez automatyzacji dowodzenia żaden system nie będzie w pełni skuteczny. Automatyzacja to nie tylko proces zarządzania, ale głównie środki przekazu informacji, czyli łączność radiowa, radioliniowa i sieci informatyczne. Jeżeli połączymy te środki przekazu w efektywną sieć, osiągniemy zakładany sukces.

Dynamiczne pole walki wskazało jeszcze inną płaszczyznę rozwoju systemów WE. Płaszczyzną tą jest mobilność. Mobilność traktowana jako środek szybkiej zmiany położenia (pojazd kołowy, lotniczy). Jednocześnie mobilność związana jest z automatyzacją dowodzenia. Tam, gdzie wyniknie potrzeba lub luka w rozpoznaniu albo przeciwdziałaniu, natychmiast powinien być skierowany odpowiedni moduł WE. Tylko szybka reakcja pozwala na skuteczne przeciwstawienie się powstałym zagrożeniom.

Przedstawione w referacie kierunki zmian w środowisku sieciocentrycznym powinny być inspiracją dla decydentów w zakresie unowocześniania systemów WE, jednocześnie powinny być asumptem do planowania rozwoju sprzętu i systemów WE wytwarzanych przez instytuty i zakłady produkujące urządzenia elektroniczne na potrzeby polskiej armii.

Bibliografia

ATP-51 (Stanag 6010) – *Electronic Warfare Land Battle*.

Ciborowski L., Nowak A., *Planowanie, organizowanie i prowadzenie walki informacyjnej na szczeblach taktycznych wojsk lądowych*, Warszawa 2000.

Ciborowski L., *Planowanie i organizowanie walki zbrojnej według poglądów NATO*, cz. I, AON, Warszawa 1996.

Ciborowski L., *Rozpoznanie i walka elektroniczna*, AON, Warszawa 1993.

Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji*, WNT, Warszawa 2002.

Dras M., *Sensory i sieci bezprzewodowych sensorów do zastosowań wojskowych*, seminarium naukowe w ZRWiWE, AON, Warszawa 2008.

FM-34-1 – *Intelligence and electronic warfare operations*, Headquorters Departments of the Army, Washington DC 1994.

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

Janczak J. (red), *Walka elektroniczna w działaniach związku taktycznego*, AON, Warszawa 2000.

Janczak J., Scheffs W., *Rola, struktury i zadania komórki koordynacji walki elektronicznej (EWCC) na poszczególnych szczeblach dowodzenia sił zbrojnych RP w świetle dyrektywy (BI-S.C. Directive Number 80–19)*, AON, Warszawa 2004.

Kręcikij J., *Istota działań sieciocentrycznych*, ZN AON nr 4(65), Warszawa 2006.

Markiewicz S., *Zarządzanie zasobami informacyjnymi w rozpoznaniu elektronicznym na szczeblu operacyjnym*, AON, Warszawa 2004.

Nowacki G., Scheffs W., *Elektroniczne przygotowanie pola walki*, AON, Warszawa 1998.

Posobiec J. (red), Żakowski A., Frącik K., *Właściwości działań sieciocentrycznych*, AON, Warszawa 2007.

Posobiec J., *Organizacja dowodzenia w działaniach sieciocentrycznych*, AON, Warszawa 2008.

Posobiec J., *System dowodzenia w działaniach sieciocentrycznych*, AON, Warszawa 2007.

Walka elektroniczna, Szt. Gen., Warszawa 2003.

Płk dr hab. Marek WRZOSEK

ZAKOŃCZENIE

Celem seminarium było uzyskanie odpowiedzi na pytanie: jak dalece aktualny stan teorii walki elektronicznej powinien ulec modyfikacji, aby możliwe było skuteczne prowadzenie działań w środowisku sieciocentrycznym?

Analiza założeń prowadzenia walki w środowisku sieciocentrycznym legła u podstaw wypracowania założeń realizacji zadań dla sensorów rozpoznawczych i WE. Jedna z trzech definiowanych płaszczyzn w środowisku sieciocentrycznym – płaszczyzna sensoryczna, stanowi główne źródło dostarczania wiedzy o przeciwniku. Połączenie płaszczyzny sensorów rozpoznawczych, WE i innych ze środkami przekazu danych w relacjach poziomych i pionowych stanowi o istocie ich działania w środowisku sieciocentrycznym.

Dostrzegając zmienność zaprezentowanych uwarunkowań sytuacji w płaszczyźnie sensorycznej, należy zatem rozważyć argumenty wskazujące na przydatność lub nie różnych rozwiązań z zakresu wykorzystania, zarządzania zasobami informacyjnymi oraz w odniesieniu do modyfikacji systemowej i sprzętowej możliwej do użycia w tym środowisku.

W powszechnej opinii specjalistów wojskowych panuje przekonanie, że zakończenie etapu przygotowawczego pod przyszłe działania w środowisku sieciocentrycznym weszło w decydującą fazę realizacji. W wielu krajach ociągnięto już poziom konstrukcji poszczególnych elementów każdego z poziomów. W niektórych trwa nadal opracowywanie koncepcji działania wojsk w środowisku sieciocentrycznym. W polskich siłach zbrojnych proces ten także nie osiągnął jeszcze wystarczającego poziomu rozwoju. Wiele zostało jeszcze do zrobienia.

Specjaliści szacują, że przyszłe konflikty mogą przerodzić się z małych terytorialnie konfliktów w konflikty globalne, w których żołnierz niekoniecznie będzie uzbrojony w karabin, tylko w minikomputer. Może się okazać, że będzie to cyberwojownik.

W publikacjach wielu placówek naukowych zajmujących się problematyką sieciocentryczności podkreśla się, że płaszczyzny sensoryczne i przekazu informacji to podstawa działań. Środki rażenia i dowodzenia będą ogrywały nie mniej ważną rolę, lecz muszą być wspomagane informacjami napływającymi od sensorów rozpoznawczych.

Na tle tych wymagań istotnego znaczenia nabierają zagrożenia dla stabilizacji w Europie, a na świecie nierozwiązane do dziś konflikty narodowościowe lub etniczne, a także działalność terrorystyczna. Waśnie i spory pomiędzy nowo powstałymi państwami mogą – w ocenie ekspertów – eksplodować wybuchem działań militarnych nawet w młodych demokracjach. Nawet ubogie gospodarczo kraje mogą dysponować najnowszą techniką elektroniczną i uzbrojeniem. Wystarczy, że będą

prowadziły działania tylko przez niedługi czas, a mogą osiągnąć sukces. Co prawda, nie dostrzeżono jeszcze takich konfliktów, ale specjaliści przewidują, że jest to kwestią czasu. Wiele państw naśladuje bądź czerpie gotowe wzorce z bogatych państw, oczywiście w mniejszej skali. Integracja sprzętu starszej generacji i najnowszej wspólnymi platformami łączności i teleinformatyki (np. w armii amerykańskiej) jest naśladowana przez wiele innych armii. Zaproponowany kierunek stał się wyznacznikiem działań w środowisku teleinformatycznym i szerzej – w sieciocentrycznym.

Wskazane powyżej argumenty stanowiły przesłankę do zorganizowania konferencji na temat: „Walka elektroniczna w działaniach sieciocentrycznych".

W toku dyskusji podkreślano, że zarówno czas przeznaczony na konferencję, jak i międzynarodowe grono dyskutantów nie umożliwiły pełnego przeglądu problematyki zawartej w temacie konferencji. Prodziekan Wydziału Zarządzania i Dowodzenia w podsumowaniu konferencji zwrócił uwagę na fakt, że zaprezentowane treści powinny być przedmiotem dalszych rozważań, a opracowane wnioski muszą znaleźć swoje odzwierciedlenie w treściach kształcenia nowych programów dla studentów.

Zamówienia
na publikacje Akademii Obrony Narodowej
można składać telefonicznie lub pisemnie na adres:

Wydział Wydawniczy AON
al. gen. A. Chruściela 103, bl. 2
00-910 Warszawa
tel. 022 681 40 55, tel./fax 022 681 37 52
e-mail: i.podemska@aon.edu.pl

Wykaz publikacji znajduje się na stronie internetowej
księgarni akademickiej

www.biblioteka.aon.edu.pl