R G B WH GR BL Grey Scale #13 C M Y K
DANES-PICTA.COM
A 1 2 3 4 5 6 M 8 9 10 11 12 13 14 15 B 17 18 19

AKADEMIA OBRONY NARODOWEJ

AON 8758/2006



SIECI TELEINFORMATYCZNE STANOWISK DOWODZENIA SZCZEBLA TAKTYCZNEGO WOJSK LĄDOWYCH

60543

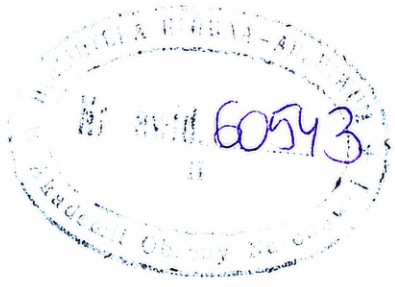


WARSZAWA 2006

Colour Chart #13
Inches Centimetres
Blue Cyan Green Yellow Red Magenta White 3/Color Black
DANES-PICTA.COM

AKADEMIA OBRONY NARODOWEJ
WYDZIAŁ WOJSK LĄDOWYCH
INSTYTUT ZARZĄDZANIA I DOWODZENIA

AON 5758/06



SIECI TELEINFORMATYCZNE STANOWISK DOWODZENIA SZCZEBLA TAKTYCZNEGO WOJSK LĄDOWYCH

**Materiały z sympozjum naukowego
Zakładu Systemów Łączności i Informatyki
19.10.2005 r.**

WARSZAWA **2006**

Redakcja:
- dr inż. Piotr DELA

Kierownictwo naukowe konferencji:
- dr hab. Janusz KRĘCIKIJ
- dr hab. inż. Józef JANCZAK
- dr hab. Jarosław WOŁEJSZO
- dr hab. Henryk SPUSTEK

Komitet organizacyjny konferencji w składzie:

Sekretarz naukowy konferencji:
- dr inż. Piotr DELA

Sekretarz organizacyjny konferencji:
- mgr inż. Sławomir BARTOSZUK

Powielenie i oprawa: Akademia Obrony Narodowej – Wydział Wydawniczy
00-910 Warszawa, al. gen. A. Chruściela 103, tel. 681-40-55, tel./faks 681-37-52
Zam. nr 70/2006

SPIS TREŚCI

Wprowadzenie 5

Informacja na SD w środowisku zautomatyzowanych systemów dowodzenia
dr inż. Piotr DELA, Akademia Obrony Narodowej 7

Sieci komputerowe wykorzystywane w ćwiczeniu „Pierścień 2005"
dr inż. Piotr DELA, Akademia Obrony Narodowej 21

Systemy sprzętowe do budowy polowych sieci teleinformatycznych na stanowiskach dowodzenia
mgr inż. Marek DRAS, Radiotechnika Marketing Sp. z o.o., Wrocław 31

Wykorzystanie oprogramowania Open Source w systemach teleinformatycznych stanowisk dowodzenia wojsk lądowych szczebla taktycznego w aspekcie koncepcji wojny sieciocentrycznej
inż. Michał GRZYBEK, Instytut Łączności 59

Rola technicznych środków dowodzenia w procesie informatyzacji stanowisk dowodzenia
dr hab. inż. Józef JANCZAK, Akademia Obrony Narodowej 87

Projektowanie i wdrożenie informatycznych systemów wspomagania procesu dowodzenia na szczeblu związku taktycznego
dr inż. Henryk ŁUKASIEWICZ, mgr inż. Artur SZLESZYŃSKI, Zakład Łączności i Informatyki, Wyższa Szkoła Oficerska Wojsk Lądowych 95

Wybrane problemy funkcjonowania sieci teleinformatycznej PKW w Iraku
mgr inż. Grzegorz PILARSKI, 16 Dywizja Zmechanizowana 101

Planowanie sieci wymiany informacji na stanowisku dowodzenia z wykorzystaniem metody symulacyjnej
dr inż. Mirosław POPIS, Wojskowa Akademia Techniczna 115

Wykorzystanie środków dowodzenia na stanowiskach dowodzenia szczebla taktycznego 127
inż. dypl. Andrzej WISZ, Akademia Obrony Narodowej

Informatyzacja procesu wsparcia logistycznego na szczeblu związku taktycznego z wykorzystaniem elementów technologii NCW
dr inż. Andrzej WOJCIECHOWSKI, Wojskowa Akademia Techniczna 137

Więzi informacyjne stanowisk dowodzenia szczebla taktycznego wojsk lądowych
dr hab. inż. Jarosław WOŁEJSZO, Akademia Obrony Narodowej 147

Łączność radiowa stanowisk dowodzenia
dr inż. Piotr DANILUK, Akademia Obrony Narodowej 173

WPROWADZENIE

Corocznie, w październiku, Zakład Systemów Łączności i Informatyki organizuje sympozjum naukowe poświęcone polowym systemom łączności i informatyki oraz wykorzystywaniu techniki telekomunikacyjnej i informatycznej w systemach dowodzenia.

Obecne, ósme już spotkanie było poświęcone problemowi sieci teleinformatycznych stanowisk dowodzenia szczebla taktycznego wojsk lądowych.

Celem sympozjum było przedstawienie dotychczasowych osiągnięć w organizacji i funkcjonowaniu sieci teleinformatycznych na stanowiskach dowodzenia, a także najnowszych rozwiązań w tym zakresie. Sympozjum miało spełnić także rolę forum wymiany myśli i dyskusji nad kierunkami dalszej pracy.

Niniejsze opracowanie zawiera wybrane referaty przedstawione podczas sympozjum. Nie były one sprawdzane ani pod względem językowym, ani merytorycznym. Za treści w nich zawarte odpowiadają autorzy.

Informacja na SD w środowisku zautomatyzowanych systemów dowodzenia

dr inż. Piotr DELA
Akademia Obrony Narodowej

Współczesne uwarunkowania powodują, iż jednym z zasadniczych elementów funkcjonowania każdej organizacji, w tym także sił zbrojnych jest posiadanie szeregu aktualnych i spójnych informacji, które stanowią o istocie oraz realizacji zasadniczych funkcji kierowania (dowodzenia) a mianowicie: planowania, organizowania i kontroli. Informacje te są zatem jednym z ważniejszych, niematerialnych zasobów każdej organizacji, w tym także sił zbrojnych. Abstrakcyjny i wieloaspektowy charakter informacji powoduje, iż może być ona przedstawiana w różnej postaci oraz za pomocą wielorakich kodów. Jednocześnie powszechność stosowania terminu informacja wyraża się tym, iż trudno wskazać dziedzinę nauk przyrodniczych lub technicznych, w której nie będziemy mieli do czynienia z pozyskiwaniem, przetwarzaniem oraz przesyłaniem informacji.

W niniejszym artykule zwrócę uwagę na kilka aspektów związanych z informacją na stanowisku dowodzenia w środowisku zautomatyzowanych systemów dowodzenia.

Istotnym kryterium informacji na stanowisku dowodzenia jest jej znaczenie w procesie decyzyjnym. Według niego wyróżniamy informacje:

- kluczowe, decydujące o najważniejszych elementach procesu podejmowania decyzji oraz determinujące poszukiwania rozwiązań optymalnych;
- istotne (obiektywne i subiektywne), wpływające na podejmowane decyzje;
- nieistotne, nie stanowiące podstawy procesów decyzyjnych oraz mające znikomy wpływ na proces podejmowania decyzji;
- rutynowe, czyli takie które zawsze pojawiają się okresowo w poszczególnych etapach działalności organizacji.

Z punktu widzenia wpływu informacji na podejmowane decyzje, wyróżniamy informacje:

- dotyczące działalności organizacji nie objętej zakresem bieżącego planowania;
- inicjujące i ustalające zadania, nie wyłączając koordynacji zadań cząstkowych;
- dostarczające danych dla przyjętej w organizacji strategii postępowania, a więc odpowiadające na pytanie: *jaki kierunek działania jest lepszy*;
- inspirujące proces podejmowania decyzji i odpowiadające na pytanie: *jakie problemy powinno się rozpatrzyć*;

- zasilające, uzupełniające poszczególne etapy procesu decyzyjnego;
- koordynacyjne, regulujące działania i procesy zachodzące pomiędzy poszczególnymi elementami organizacji;
- podające do wiadomości wyniki działania (kontrolne).

W środowisku zautomatyzowanych systemów dowodzenia informację można podzielić także ze względu na pilności i ważności przekazu. Dzieli się ją na[1]:

- błyskawiczną (ang. flash – kod Z);
- natychmiastową (ang. immediate – kod O);
- priorytetową (ang. priority – kod P)
- rutynową (ang. routine – kod R).

Informacja z kategorią „*błyskawiczna*" przeznaczona jest dla początkowego kontaktu z przeciwnikiem lub dla komunikatów bojowych o najwyższym stopniu pilności. Z tego też względu forma informacji powinna być jak najkrótsza.

Kategoria „*natychmiastowa*" zarezerwowana jest dla bardzo ważnych wiadomości odnoszących się do sytuacji, które mają istotne znaczenie dla bezpieczeństwa wojsk własnych.

Informacja z kategorią „*priorytetowa*" przekazuje wiadomości dotyczące prowadzenia toczących się operacji oraz dla innych ważnych i pilnych spraw dla których klauzula „rutynowa" jest niewystarczająca.

Ostatnia – najniższa kategoria ważności informacji – „*rutynowa*" jest wykorzystywana dla wszystkich rodzajów wiadomości, których treść nie jest wystarczająco pilna ani ważna.

Osnową funkcjonowania zautomatyzowanych systemów dowodzenia jest proces decyzyjny realizowany w trakcie podejmowania decyzji. Jak wszyscy zapewne wiemy proces ten składa się z czterech zasadniczych faz, przedstawionych na rysunku 1, a mianowicie:

- fazy ustalania położenia;
- fazy planowania;
- fazy stawiania zdań;
- fazy kontroli.

Ustalanie położenia[2] jest pierwszą z czterech faz cyklu procesu dowodzenia. Jednocześnie faza ta stanowi ciągły proces realizowany we wszystkich komórkach organizacyjno – funkcjonalnych stanowiska dowodzenia. Szczególne zintensyfikowanie czynności w ramach ustalania położenia następuje z chwilą otrzymania zadania i jest ukierunkowane na nowe zadanie. Pozwala to na jego zakwalifikowanie jako początkowej fazy cyklu dowodzenia. Faza ta

[1] Zasady organizacji łączności współdziałania w operacjach wielonarodowych, SG WP, Warszawa 1999, s. 195

charakteryzuje się przede wszystkim pozyskiwaniem, gromadzeniem, porządkowaniem, przechowywaniem, wartościowaniem, porównywaniem i przedstawianiem wszelkiego rodzaju informacji dotyczących wojsk własnych, przeciwnika oraz warunków prowadzenia działań. Prawidłowe ustalenie położenia jest niezbędne do wyciągnięcia właściwych wniosków dotyczących przyszłych działań wojsk własnych. Położenie wojsk ulega bowiem nieustannym zmianom powodując, iż obraz sytuacji staje się w wielu przypadkach niepełny lub nieaktualny.

Każdy dowódca, bez względu na szczebel dowodzenia, wraz ze swoim sztabem zobowiązany jest do systematycznego uzupełniania i uaktualniania wszelkich informacji, tak aby posiadany przez nich zbiór danych (informacji) o sytuacji był jak najbardziej kompletny i stanowił podstawę do planowania działań i dowodzenia wojskami.

W trakcie tej fazy procesu dowodzenia analizowane i przedstawiane są następujące grupy informacji:

- informacje posiadane (informacje sytuacyjne);
- informacje wpływające (informacje sytuacyjne i dyrektywne);
- informacje zdobywane (informacje sytuacyjne).

Z chwilą otrzymania zadania w pierwszej kolejności brane są pod uwagę informacje posiadane (istniejące). Informacje te zawarte są między innymi w dokumentach normatywnych, regulaminach oraz bazach danych zautomatyzowanych systemów dowodzenia.

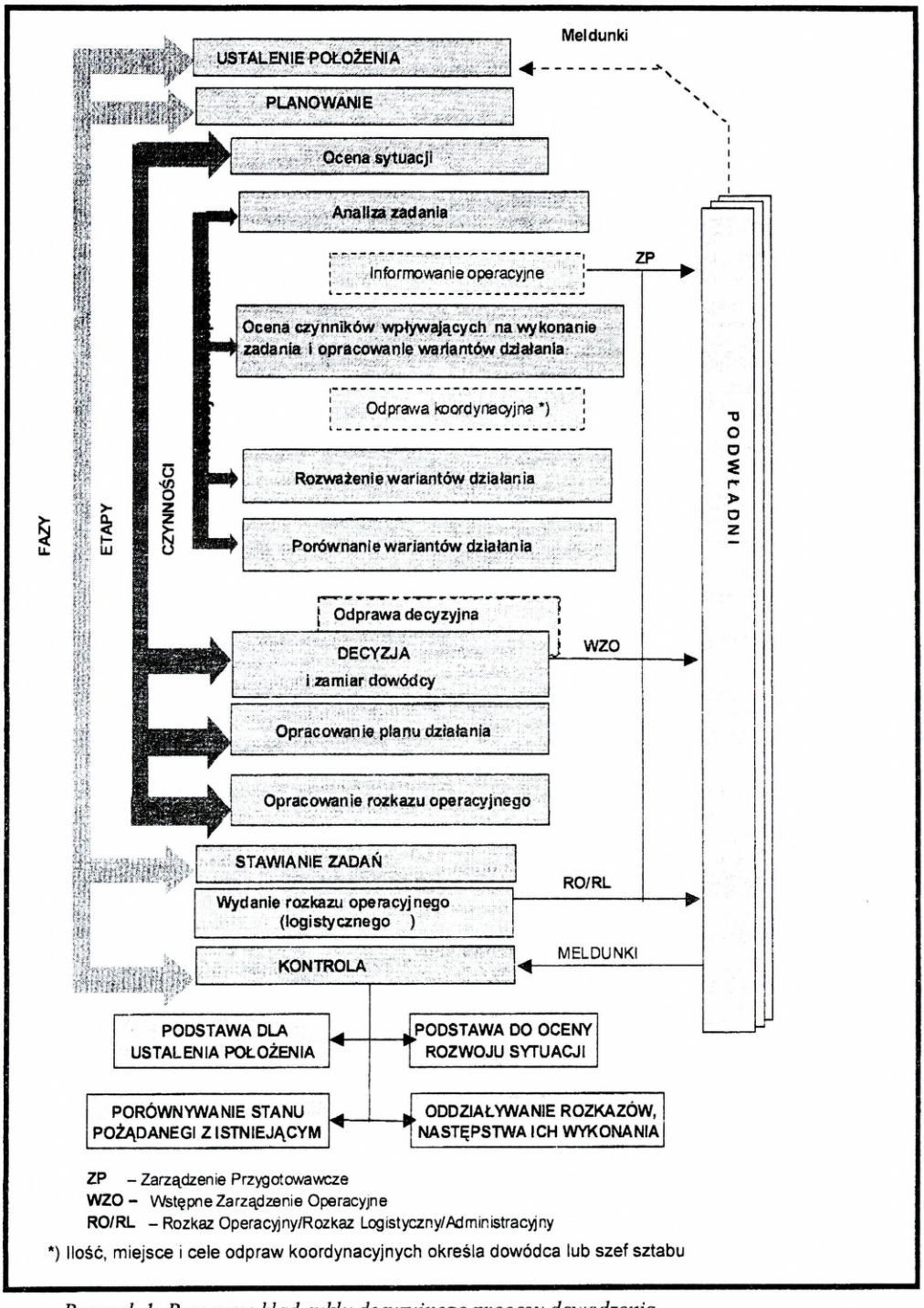
Posiadane informacje są w sposób ciągły uzupełniane poprzez informacje wpływające, do których zalicza się:

- rozkazy (zarządzenia) operacyjne;
- zarządzenia przygotowawcze;
- komunikaty;
- meldunki;
- inne uzyskane dane.

Rozkazy oraz zarządzenia przełożonego **są jednymi z zasadniczych dokumentów wykorzystywanych do ustalenia położenia. Zawierają one informacje wywierające bezpośredni wpływ na dalsze działania.**

---

[2] P. Dela, J, Kręcikij, Wspomaganie dowodzenia – Wspomaganie 1, Warszawa, AON 2003 s. 15



Rysunek.1. Ramowy układ cyklu decyzyjnego procesu dowodzenia
Źródło: J. Michniak i inni, *Metody i treść pracy zespołów funkcjonalnych na stanowisku dowodzenia wojsk lądowych*, Warszawa, AON 2000

Zarządzenia przygotowawcze umożliwiają podległym dowódcom opracowanie, we właściwym czasie, odpowiedniej ilości informacji oraz zapewniają możliwość jej wymiany zarówno z sąsiadami jak i podwładnymi. Zarządzenia przygotowawcze nie są jednorazowymi dokumentami wysyłanymi po przeprowadzeniu analizy zadania. Mogą być stosowane w całym cyklu procesu dowodzenia w celu przekazywania informacji ważnych dla podwładnych.

Do zasadniczych źródeł informacji wykorzystywanych na potrzeby ustalenia położenia należy również zaliczyć meldunki sytuacyjne. W czasie prowadzenia walki (operacji) wyodrębnia się:

- meldunki terminowe;
- meldunki doraźne.

Meldunki terminowe składane są w określonym, wyznaczanym przez przełożonego terminie, jeżeli we właściwych dokumentach normatywnych nie ma ustaleń dotyczących systemu meldunkowego. Zawierają one informacje na temat sytuacji taktycznej (operacyjnej) w rejonie odpowiedzialności meldującego dowódcy.

Meldunki doraźne składane są przez podwładnego po zaistnieniu sytuacji, o której należy niezwłocznie powiadomić przełożonego, lub na jego żądanie.

Jeżeli zaistnieje potrzeba pozyskania dodatkowych, niezbędnych informacji, dowódca danego szczebla dowodzenia powinien:

- zwrócić się z prośbą do przełożonego o dostarczenie informacji w wymaganym zakresie;
- zarządzić rozpoznanie przeciwnika i terenu własnymi środkami;
- zażądać kolejnych meldunków od podwładnych.

Dla uzyskania rzeczywistego obrazu sytuacji oprócz informacji dotyczących wojsk własnych i przeciwnika istotne są także dane dotyczące środowiska w jakim prowadzone będą działania. Podstawowym źródłem wiedzy w tym zakresie jest geografia wojskowa i narzędzia do analizy terenu oraz informacje pozyskane poprzez rozpoznanie terenu.

Posiadane, wpływające i zdobywane informacje, tworzące obraz sytuacji, przedstawia się w postaci:

- map sytuacyjnych;
- tabel;
- diagramów;
- schematów organizacyjnych;
- innych dokumentów pomocniczych.

Jak wynika z powyższych danych, wymiana informacji w fazie ustalania położenia jest bardzo istotna i stanowi podstawę do prawidłowej realizacji kolejnej fazy procesu dowodzenia – fazy planowania. Z uwagi na ilość przesyłanej informacji, a także ciągłość fazy ustalania położenia, zautomatyzowane systemy dowodzenia powinny być zdolne do wymiany sformatowanych informacji poprzez mobilne sieci radiowe. Dotyczy to w głównej mierze przesyłania rozkazów (zarządzeń) operacyjnych (przygotowawczych) i meldunków doraźnych przekazujących w swojej treści newralgiczne z punktu widzenia dowodzenia i bezpieczeństwa wojsk informacje.

Faza druga procesu podejmowania decyzji – **planowanie**[3] - odgrywa szczególną rolę. W trakcie tej fazy dokładnym analizom i ocenom podlega bowiem zadanie otrzymane od przełożonego a także wszelkie czynniki wpływające na jego realizację. W tej fazie powstają warianty działania wojsk własnych, które są następnie szczegółowo rozważane i porównywane w celu stworzenia dowódcy jak najlepszych warunków do podjęcia decyzji. W ramach planowania podejmowana jest też decyzja oraz zostaje sformułowany i wygłoszony (przez dowódcę) zamiar działania. Powstaje w tym czasie również plan działania, a także zasadniczy dokument dowodzenia o charakterze dyrektywnym – rozkaz operacyjny (bojowy).

Faza planowania podzielona jest na cztery następujące po sobie etapy. Są to:

- ocena sytuacji;
- podjęcie decyzji;
- sporządzenie planu działania;
- sporządzenie rozkazu operacyjnego.

Poszczególne etapy tej fazy procesu dowodzenia nie stanowią obszaru rozważań niniejszego opracowania. Należy zaznaczyć, że informacja wymieniana w ramach tej fazy procesu dowodzenia jest w głównej mierze informacją wewnętrzną stanowisk dowodzenia, przesyłaną pomiędzy komórkami funkcjonalnymi stanowiska dowodzenia w określony (ustalony) sposób. Zależy to w głównej mierze od struktury organizacyjno-funkcjonalnej stanowiska dowodzenia. Obieg informacji w ramach stanowiska dowodzenia i pomiędzy elementami ugrupowania bojowego przedstawiony zostanie w dalszej części opracowania.

Istotne znaczenie dla całości procesu planowania ma praca sekcji (komórki) rozpoznania jako komórki stanowiska dowodzenia realizującej główną cześć procesu Informacyjnego Przygotowania Pola Walki (IPPW) w etapie oceny sytuacji. Informacje pozyskiwane, gromadzone, opracowywane i rozprowadzane w ramach IPPW mają bardzo duży wpływ na po-

[3] Tamże, s. 22

wstawanie wariantów działania wojsk własnych, ich rozważanie, porównanie, a w konsekwencji także na decyzję dowódcy. Należy mieć świadomość, iż choć to sekcja rozpoznania ogrywa zasadniczą rolę w prowadzeniu IPPW, to proces ten nie jest sprawą tylko tego zespołu. Z tego też względu wymiana informacji pomiędzy elementami rozpoznania a stanowiskiem dowodzenia w fazie planowania ma bardzo istotne znaczenie, a informacja uzyskana z elementów rozpoznania musi być dostępna dla wszystkich komórek funkcjonalnych stanowiska dowodzenia, a nie tylko dla komórki rozpoznania. Za jej właściwą dystrybucję na stanowisku dowodzenia odpowiada **zespół bezpieczeństwa i wymiany informacji**[4].

Trzecią fazą cyklu procesu dowodzenia jest **stawianie zadań**[5]. Jej celem jest doprowadzenie do wykonawców zadań wynikających z decyzji podjętej przez dowódcę. Formalnie faza ta rozpoczyna się po zakończeniu opracowywania pełnego rozkazu operacyjnego wraz z niezbędnymi aneksami i apendyksami. Jeżeli jednak organizator pracy na stanowisku dowodzenia (szef sztabu lub dowódca) uzna za celowe zastosowanie wstępnych zarządzeń operacyjnych, wówczas faza ta rozpocznie się nieco wcześniej – po sporządzeniu planu działania i niezbędnych wstępnych zarządzeń operacyjnych. Sposób postawienia zadań może być różny i zależał będzie od następujących wielu czynników, min. od:

- szczebla dowodzenia;
- stopnia doświadczenia i wyszkolenia dowództw;
- posiadanego czasu;
- posiadania i poziomu technicznych środków łączności i wspomagania procesu dowodzenia.

Oczywistym jest fakt, że najlepszym sposobem postawienia zadań jest osobiste ich przekazanie podwładnym przez dowódcę. Kontakt osobisty przełożonego i podwładnego pozwala na dokładne przekazanie zadania oraz umożliwia szybkie i jednoznaczne wyjaśnienie niejasności lub wątpliwości. Daje też dowódcy możliwość sprawdzenia czy podwładni właściwie zrozumieli postawione im zadania i jego myśl przewodnią.

Z uwagi na charakter współczesnego pola walki, duże oddalenie walczących elementów i szybko zmieniającą się sytuację, osobiste stawianie zadań przez dowódcę jest praktycznie niemożliwe. W tym przypadku rozkazy mogą być dostarczone:

- przez oficerów łącznikowych;
- przez kurierów;

---

[4] Patrz rysunek 2 i 3
[5] P. Dela, J. Kręcikij, Wspomaganie dowodzenia, s. 52

- przy wykorzystaniu technicznych środków łączności (fon);
- przy wykorzystaniu zautomatyzowanych systemów dowodzenia.

Sposób realizacji tej fazy cyklu procesu dowodzenia każdorazowo ustala **dowódca** lub **szef sztabu**. Miejsce, czas i sposób doprowadzenia zadań do podwładnych powinno być jednoznacznie sprecyzowane podczas informowania operacyjnego i przekazane podwładnym w zarządzeniach przygotowawczych.

Postawienie zadań ustnie przez dowódcę (osobę upoważnioną) lub przy wykorzystaniu technicznych środków łączności musi być potwierdzone pisemnym (pisemno–graficznym, graficznym) dokumentem dowodzenia dostarczonym adresatowi tak szybko, jak to jest możliwe.

W tej fazie procesu dowodzenia coraz większego znaczenia nabierają możliwości zautomatyzowanych systemów dowodzenia i środki szerokopasmowej transmisji danych. Przy ich wykorzystaniu można w krótkim czasie przesłać do podwładnych rozkazy i zarządzenia uzupełnione o odpowiednia załączniki. Treść rozkazów i załączników może być w szybki sposób przetworzona, przez oprogramowania zautomatyzowanych systemów dowodzenia, do postaci rozumianej przez dowódcę (obsadę stanowiska dowodzenia), co w zdecydowany sposób przyczyni się do skrócenia tej fazy procesu dowodzenia.

Kontrola[6] pomimo tego, że jest ostatnią faza cyklu procesu dowodzenia, jednocześnie zapewnia ciągłość tego procesu. Jej rezultaty stanowią bowiem podstawę do uaktualniania posiadanych danych o sytuacji – ustalania położenia.

Celem kontroli jest sprawdzenie efektów (skutków) dotychczasowego planowania i postawienia zadań oraz efektywności ich wprowadzania w życie.

Za realizację kontroli bezpośrednio jest odpowiedzialny dowódca każdego szczebla dowodzenia. Jego obowiązkiem w tym zakresie jest zachowanie obiektywizmu oraz:

- zapewnienie właściwego zakresu kontroli, biorącej pod uwagę niezbędną dla podwładnego swobodę działania;
- zmniejszenie do niezbędnego minimum udziału kontrolowanego w kontroli, to znaczy nie odciąganie go od jego głównego zadania jakim jest osiągnięcie celu działania;
- udzielanie pomocy kontrolowanemu po stwierdzeniu, iż pomoc jest potrzebna i możliwa.

Kontrola realizowana jest poprzez:

- ustanowienie elementów dowodzenia i koordynacji działań - EDKD;
- organizację synchronizacji działań;

---

[6] Tamże, s. 53

- monitorowanie sytuacji;
- podejmowanie działań mających zmniejszyć różnice pomiędzy stanem zaplanowanym a stanem rzeczywistym.

Ułatwieniem dla skutecznego sprawowania kontroli jest jednoznaczny, wyraźny podział odpowiedzialności pomiędzy określonym szczeblem dowodzenia i podległymi mu dowódcami.

Z punktu widzenia obiegu informacji istotne znaczenie ma monitorowanie sytuacji, które obejmuje całokształt przedsięwzięć zapewniających możliwość porównania stanu zaplanowanego (*jak miało być*) ze stanem rzeczywistym (*jak jest*). Zasadnicze sposoby pozyskiwania informacji niezbędnych do sprawnego i ciągłego monitorowania sytuacji to:

- zbieranie meldunków od podwładnych,
- wizyty dowódcy w podległych mu wojskach,
- wysyłanie grup (zespołów) kontrolnych,
- prowadzenie kontroli po linii funkcjonalnej przez specjalistów rodzajów wojsk.

Informacje o aktualnej sytuacji przedstawiane są na mapach sytuacyjnych oraz dokumentach pomocniczych (zestawienia, tabele, szkice itp.) każdej organizacyjno–funkcjonalnej komórki stanowiska dowodzenia. W środowisku zautomatyzowanych systemów dowodzenia podstawą do tworzenia map sytuacyjnych i zestawień pomocniczych są meldunki zbierane od podwładnych i ich interpretacja (odzwierciedlenie) w odpowiednich bazach danych.

Informacje pochodzące od przełożonego, podwładnych i sąsiadów oraz innych źródeł są zapisywane automatycznie w dziennikach działań. Te z nich, których nie można (lub nie jest to celowe) zobrazować na mapach sytuacyjnych, a są potrzebne dla pracy zespołów funkcjonalnych powinny być umieszczone w pomocniczych dokumentach uzupełniających mapy sytuacyjne – tabelach, szkicach, zestawieniach, zgodnie z wytycznymi szefa danej komórki SD.

Monitorowane informacje stanowią podstawę do oceny czy różnice te wymagają podjęcia dodatkowych działań. Jeżeli dodatkowe czynności nie są niezbędne, dowódca i sztab kontynuują swoje standardowe działania – to znaczy realizują wcześniej ustalony plan.

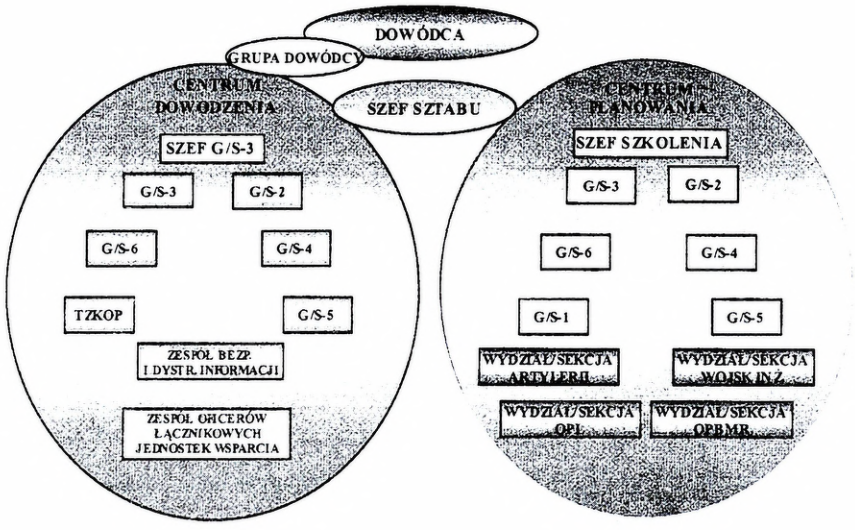
Osobnym zagadnieniem rozpatrywanym w niniejszym opracowaniu jest obieg (wymiana) informacji w środowisku zautomatyzowanych systemów dowodzenia. Realizacja i zasady wymiany informacji zależą w głównej mierze od struktury dowodzenia i struktury organizacyjno funkcjonalnej samego stanowiska dowodzenia. Na rysunkach 2 i 3 przedstawiono wariant struktury organizacyjno-funkcjonalnej głównego i tyłowego stanowiska dowodzenia.

Wariant ten został opracowany przez pracowników naukowo-dydaktycznych Instytutu Zarządzania i Dowodzenia AON i służyć może tylko jako jeden z przykładów struktury stanowiska dowodzenia. Niemniej jednak dla prawidłowej realizacji procesu dowodzenia w środowisku automatyzowanych systemów dowodzenia niezbędny jest jeden element tego stanowiska, a mianowicie **zespół bezpieczeństwa i dystrybucji informacji.**

Zespół ten jest odpowiedzialny za bezpieczeństwo i prawidłową dystrybucję danych zarówno wewnątrz stanowiska dowodzenia, jak i pomiędzy podwładnymi, przełożonym, sąsiadami, wojskami współdziałającymi. Każda informacja zarówno wewnętrzna stanowiska dowodzenia jak i wychodząca lub wychodząca musi przejść przez zespół bezpieczeństwa i dystrybucji danych. Komórka ta analizuje otrzymane dane, sprawdza ich poprawność i zagrożenie dla systemu, nadawcę i adresata a także treść informacji. Po analizie podejmowana jest decyzja co dalej z taką informację, czy jej treść można automatycznie przenieść do baz danych zautomatyzowanego systemu dowodzenia, czy przesłać ją bezpośrednio do adresata, czy odesłać ją do nadawcy jako informację niezrozumiałą. Oczywistym faktem jest także to, że komórka ta w momencie zweryfikowania i przyjęcia informacji (meldunku) generuje odpowiednie potwierdzenie dla nadawcy.

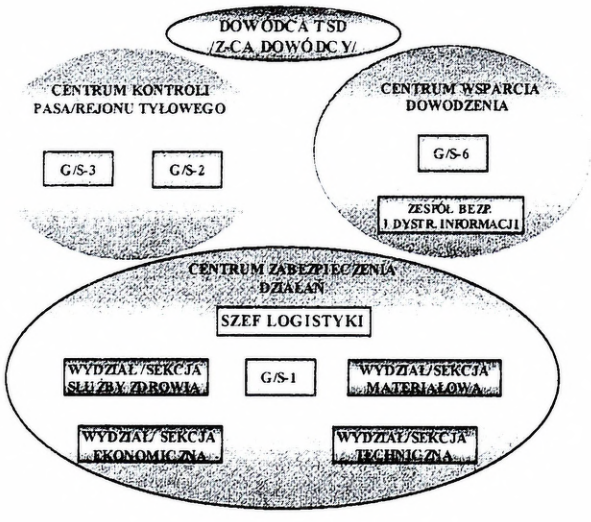
Dla przykładu sekcja artylerii centrum planowania GSD wszystkie informacje do pododdziałów artylerii przesyłać będzie poprzez komórkę bezpieczeństwa i wymiany informacji. Podobna sytuacja wystąpi w chwili przesyłania meldunków od pododdziałów artylerii do sekcji artylerii. Elementem pośredniczącym w wymianie informacji także będzie zespół bezpieczeństwa i wymiany informacji. Uogólniając, nie istnieje możliwość przesłania informacji bezpośrednio pomiędzy jakąkolwiek sekcją stanowiska dowodzenia a podległymi wojskami, a także nie istnieje możliwość przesyłania informacji bezpośrednio pomiędzy sekcjami (zespołami) stanowiska dowodzenia. Zespół bezpieczeństwa i wymiany informacji jest zespołem, przez który muszą przechodzić wszystkie informacje w ramach zautomatyzowanych systemów dowodzenia. Inne podejście spowodowałoby chaos informacyjny, co doprowadziłoby do niespójności danych (informacji) w bazach danych komórek organizacyjnych stanowiska dowodzenia.

STRUKTURA GSD DZ, BZ



Rysunek 2. Struktura GSD DZ i BZ - wariant

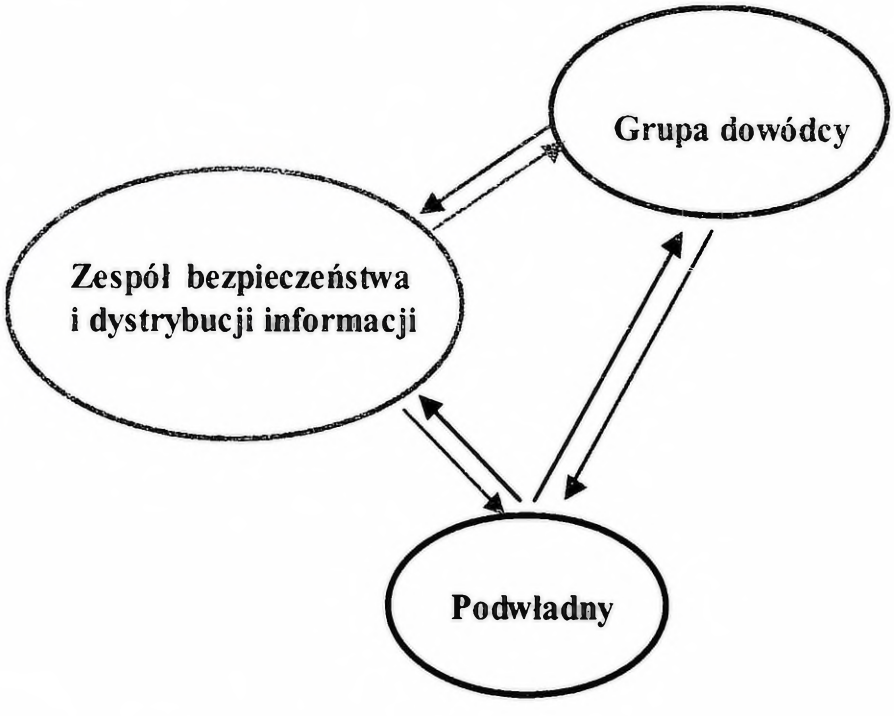
STRUKTURA TSD DZ, BZ



Rysunek 3. Struktura TSD DZ i BZ – wariant

Najważniejszym elementem decyzyjnym każdego stanowiska dowodzenia jest dowódca (grupa dowódcy). Grupa ta, ze względu na swoje funkcje kontrolne, powinna posiadać zawsze aktualne dane. Z tego też względu zespół bezpieczeństwa i informacji danych powinien wszystkie otrzymane dane kierować oprócz do adresata także do grupy dowódcy.

Taki obieg informacji jest łatwy do zrealizowania jeżeli grupa dowódcy przebywa na stanowisku dowodzenia. Zespół bezpieczeństwa i dystrybucji danych jest w stanie każdą, otrzymaną informację przesłać zarówno do grupy dowódcy jak i do adresata, oraz jeżeli zachodzi taka potrzeba uaktualnić bazy danych zautomatyzowanego stanowiska dowodzenia. Do transmisji danych w ramach stanowiska dowodzenia zespół wykorzystuje sieć komputerową stanowiska dowodzenia. Sytuacja wygląda inaczej, jeżeli grupa dowódcy uda się na rekonesans lub pracuje na PDO. W takiej sytuacji obieg informacji pomiędzy podwładnymi, głównym stanowiskiem dowodzenia a grupą dowódcy powinien odbywać się na zasadzie trójkąta informacji, przedstawionego na rysunku 4. Takie podejście do wymiany informacji zdecydowanie skraca czas obiegu informacji, zapewniając dowódcy zarówno aktualne dane z pola walki jak i możliwość bezpośredniego dowodzenia. To czy grypa dowódcy znajduje się na GSD czy też nie, musi być przekazywane do podwładnych w ustalony wcześniej sposób.



Rysunek 4. Obieg informacji podwładny -- dowódca - GSD

Na powyższym rysunku podwładny wysyła informacje (meldunek) bezpośrednio zarówno do grupy dowódcy jak i do komórki bezpieczeństwa i dystrybucji informacji na GSD. Grupa dowódcy po otrzymaniu meldunku przesyła potwierdzenie odbioru meldunku zarówno do nadawcy jak i do komórki bezpieczeństwa i dystrybucji informacji w celu poinformowania, iż takie dane już otrzymała i nie wymagają one aktualizacji. Sposób wymiany informacji pomiędzy tymi elementami w innych przypadkach (np. w przypadku gdy komórka bezpieczeństwa i dystrybucji informacji odbierze meldunek od podwładnego a nie odbierze potwierdzenia od grupy dowódcy itp.) wykracza poza ramy niniejszego artykułu.

Podsumowując, zdaję sobie sprawę, iż tak rozległy obszar dociekań jakim jest informacja, a w szczególności jej wymiana na SD w środowisku zautomatyzowanych systemów dowodzenia trudno wyczerpać na tych kilku stronach. Niemniej jednak mam nadzieję, że poruszone przeze mnie aspekty stanowić będą dla czytelników źródło refleksji i podstawę do dalszych rozważań nad kierunkami zmian w dziedzinie automatyzacji dowodzenia.

BIBLIOGRAFIA

1. Barczak A., i inni, *Planowanie systemu łączności,* Warszawa, Bellona 1999
2. Ciborowski L., *Walka informacyjna*, Toruń, Europejskie Centrum Edukacyjne 1999
3. Janczak J., Daniluk P., Wisz A., *Kierowanie mobilnymi systemami łączności wojsk lądowych, Część III*, Warszawa, AON 2002
4. Kotarbiński T., *Abecadło praktyczności*, Warszawa, Wiedza Powszechna 1974
5. Kotarbiński T., *Traktat o dobrej robocie*, Łódź, Zakład im. Ossolińskich we Wrocławiu 1955
6. Kotarbiński T., *Z zagadnień ogólnej teorii walki*, Warszawa, Wydawnictwo Sekcji Psychologicznej Towarzystwa Wiedzy Wojskowej 1938
7. Koźmiński A., Piotrowski W., *Zarządzanie. Teoria i praktyka*, Warszawa, PWN 1995
8. Kręcikij J., *Metodyka pracy sekcji dowodzenia stanowiska dowodzenia oddziału i związku taktycznego,* Warszawa, AON 2002
9. Kręcikij J., *Współczesne kierowanie wojskami. Proces dowodzenia,* Warszawa, AON 2002
10. Kręcikij J., *Wybrane problemy dowodzenia wojsk lądowych USA,* Warszawa, AON 2002
11. Kręcikij J., Wołejszo J., *Rozważenie wariantów działania metodą symulacji*, Warszawa, AON 1999
12. *Metody i treść pracy zespołów funkcjonalnych na stanowisku dowodzenia Wojsk Lądowych*, Warszawa, AON 2000
13. Michniak J., *Polowy zautomatyzowany system dowodzenia (PZSD)*, Warszawa, AON 2003
14. Michniak J. i inni, *Metody i treści pracy zespołów funkcjonalnych na stanowiskach dowodzenia wojsk lądowych*, Warszawa, AON 2000

15. Morgan G., *Obrazy organizacji*, Warszawa, PWN 1997
16. Stoner J., *Kierowanie*, Warszawa, Polskie Wydawnictwo Ekonomiczne 2001
17. Strzoda M., Prusiński N., *System dowodzenia. Terminologia część I*, Warszawa, AON 2001
18. Ścibiorek Z., *Podejmowanie decyzji*, Warszawa, Agencja Wydawnicza Ulmak 2003
19. Wołejszo J., *Metody i treść pracy zespołów funkcjonalnych na stanowisku dowodzenia wojsk lądowych Cz. IV. Rekonesans,* Warszawa, AON 2001
20. Wołejszo J., *Metody i treść pracy zespołów funkcjonalnych na stanowisku dowodzenia wojsk lądowych Cz. IV. Rozważanie wariantów działania,* Warszawa, AON 2001
21. Wołejszo J., Trembecki J. *Metody i treść pracy zespołów funkcjonalnych na stanowisku dowodzenia wojsk lądowych Cz. IV. Analiza zadania i informowanie operacyjne,* Warszawa, AON 2001
22. Zaskórski P., *Automatyzacja procesów dowodzenia*, Toruń, Wydawnictwo Adam Marszałek 2001

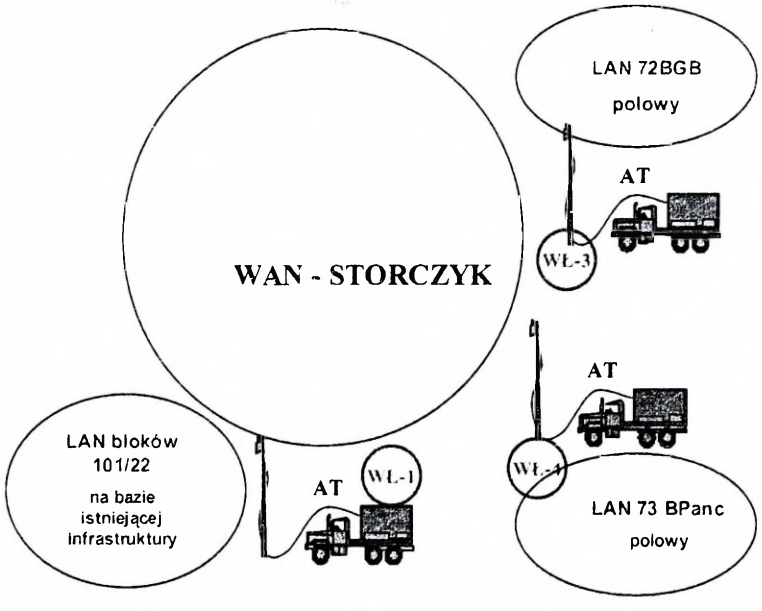
Sieci komputerowe wykorzystywane w ćwiczeniu „Pierścień 2005"

dr inż. Piotr DELA
Akademia Obrony Narodowej

Celem niniejszego referatu jest zapoznanie z budową i przeznaczeniem sieci komputerowych wykorzystywanych w trakcie ćwiczenia „Pierścień 2005", organizowanego przez Wydział Wojsk Lądowych Akademii Obrony Narodowej, w czerwcu 2005 roku. Ćwiczenie to, organizowane cyklicznie na zakończenie procesu dydaktycznego w Akademii, służy sprawdzeniu umiejętności studentów w zakresie prawidłowej realizacji procesu decyzyjnego.

Z uwagi na charakter niniejszej publikacji zarówno tło operacyjno-taktyczne jak składy ćwiczących stron zostaną pominięte

Na potrzeby ćwiczenia zostały utworzone trzy lokalne sieci komputerowe etherten z protokołem TCP/IP. Jedna z nich zbudowana była w oparciu o stacjonarny sprzęt sieciowy i komputerowy w budynkach 22 i 101. Budynki połączone były światłowodem. Pozostałe dwie sieci polowe zbudowane były w oparciu o mobilne środki informatyczne. Działały one na potrzeby 72 BGB i 73 BPanc. Połączenie między tymi trzema sieciami zapewniały aparatownie transmisyjne działające w ramach sieci radioliniowo-kablowej. Ogólny schemat połączeń sieciowych przedstawiono na rysunku 1.

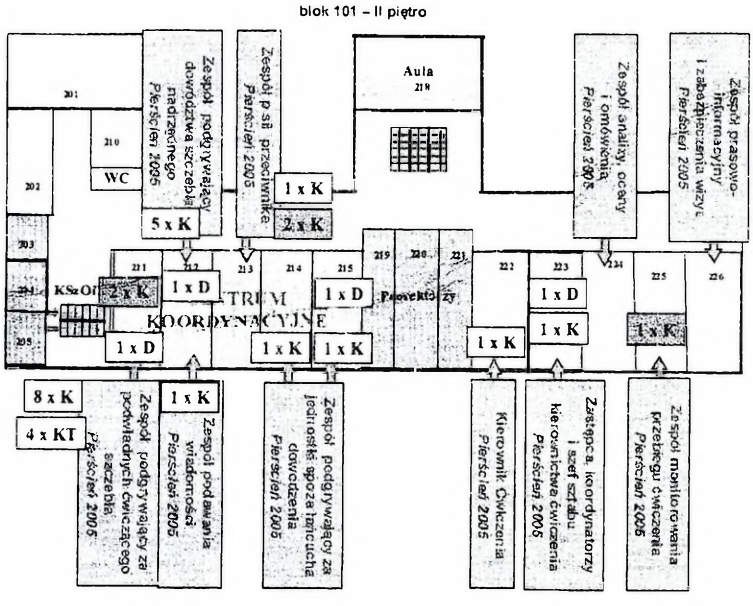


Rysunek 1. Uproszczony schemat połączeń sieci komputerowych

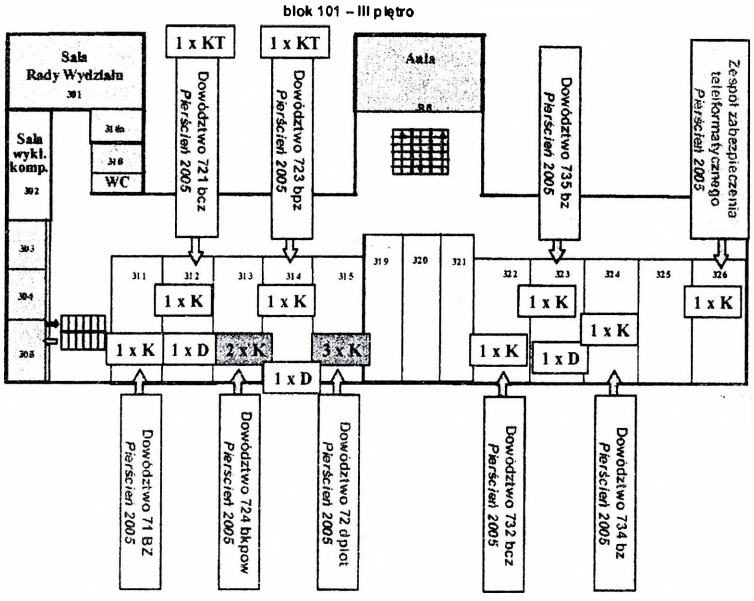
Sieć bloków 101 i 22

W blokach szkoleniowych 101 i 22 rozmieszczone były, jak wspomniano wcześniej, w głównej mierze elementy podgrywające, nadzorujące i koordynujące. Ich głównych zadaniem było podawanie i odbieranie informacji od ćwiczących brygad (72 BGB i 73 BPanc).

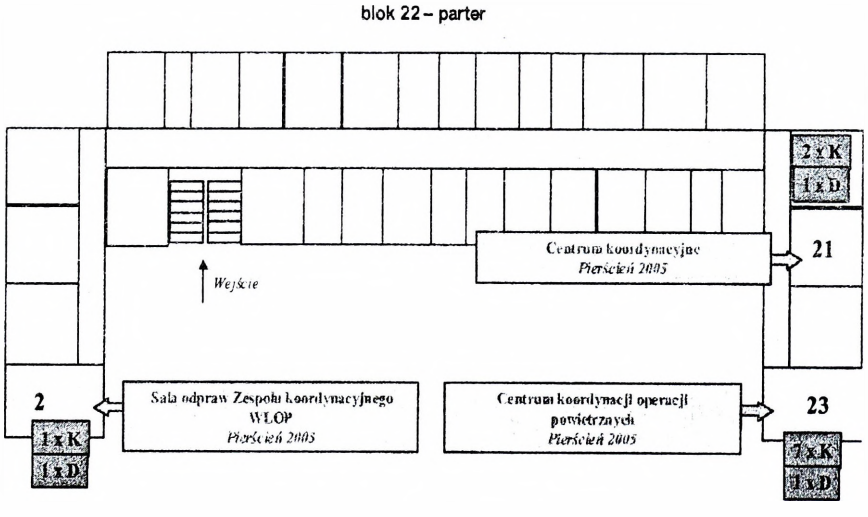
Z uwagi na to, że w blokach tych znajdowały się lokalne sieci komputerowe (na bazie okablowania strukturalnego) pracujące w sieci Internet i ich odcięcie od sieci Internet nie stanowiło żadnego problemu organizacyjnego, postanowiono do realizacji ćwiczenia wykorzystać istniejącą infrastrukturę. Pozwoliło to na znaczne zaoszczędzenie czasu rozwinięcia sieci komputerowych przy jednoczesnej redukcji kosztów. O rozmachu przeprowadzonych modyfikacji sieci świadczy fakt, że w sieci bloku 22 i 101 pracowało, w trakcie ćwiczenia, łącznie 57 komputerów. Rozmieszczenie poszczególnych zespołów ćwiczących w blokach szkoleniowych przedstawiono na rysunkach od 2 do 5.



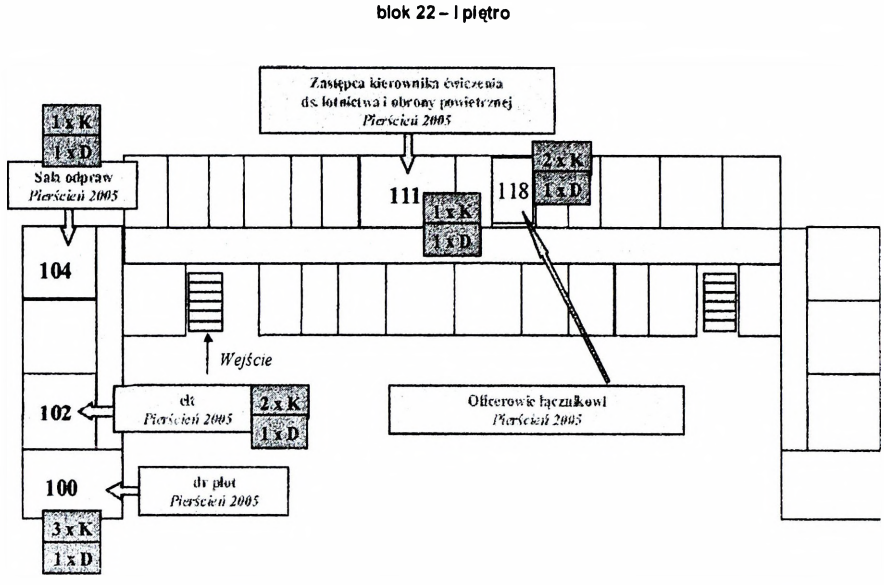
Rysunek 2. Rozmieszczenie ćwiczących zespołów w bloku 101/II piętro



Rysunek 3. Rozmieszczenie ćwiczących zespołów w bloku 101/III piętro

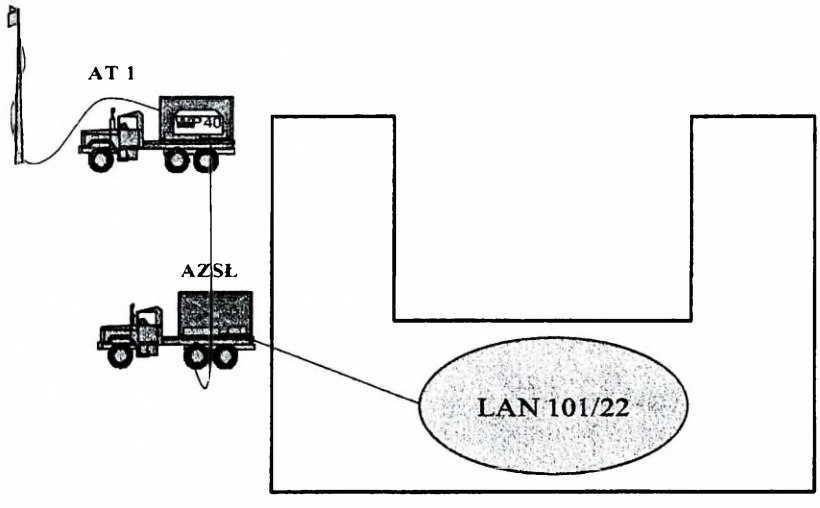


Rysunek 4. Rozmieszczenie ćwiczących zespołów w bloku 22/parter



Rysunek 5. Rozmieszczenie ćwiczących zespołów w bloku 22I piętro

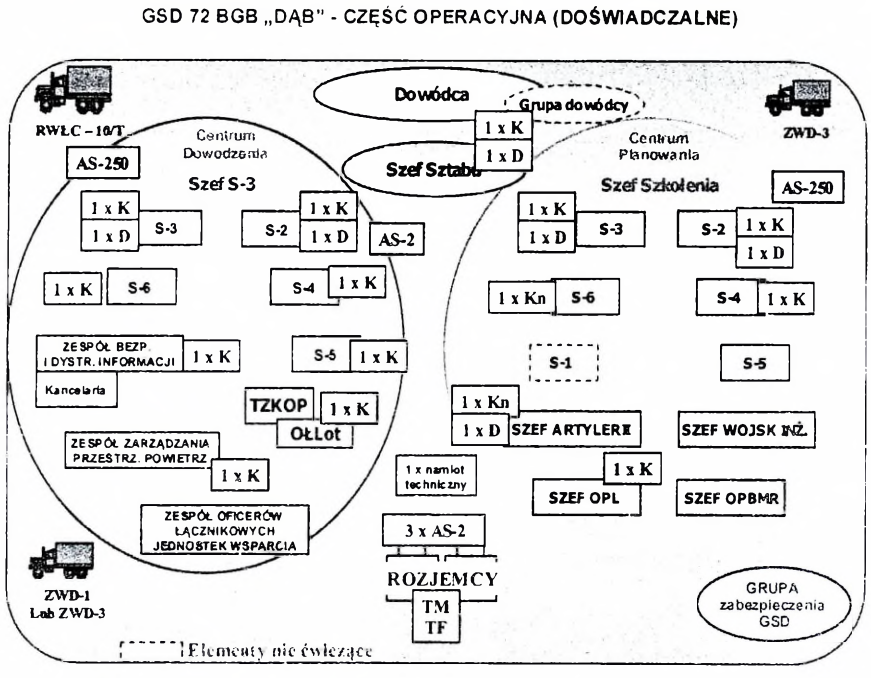
Osobnym zagadnienie było podłączenie lokalnej sieci komputerowej budynków do systemy Storczyk, w celu zapewnienia wymiany informacji z sieciami lokalnym stanowisk dowodzenia. Do tego celu wykorzystano router znajdujący się w aparatowni zarządzania systemem łączności (AZSŁ). Aparatownia ta umieszczona została przy bloku 101 i była spięta bezpośrednio światłowodem z węzłem pakietowym WP-40A aparatowni RWŁC-10T. Uproszczony schemat połączeń przedstawiony został na rysunku 6.



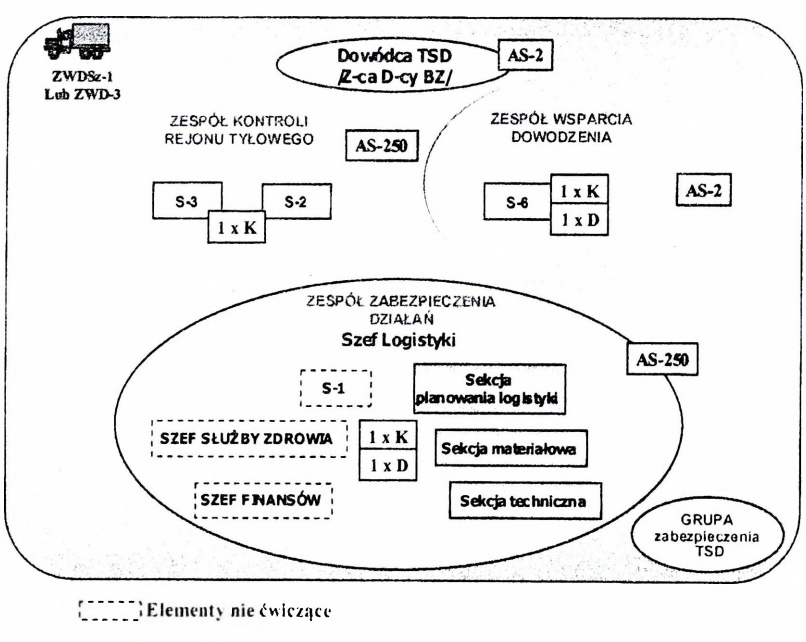
Rysunek 6. Uproszczony schemat podłączenia lokalnej sieci komputerowej budynków do systemu Storczyk

Sieć 72 BGB

Ćwiczące GSD i TSD 72 BGB rozmieszczone zostały na poligonie znajdującym się w Rembertowie. Struktury funkcjonalne stanowisk dowodzenia zostały przedstawione na rysunkach 7 i 8.



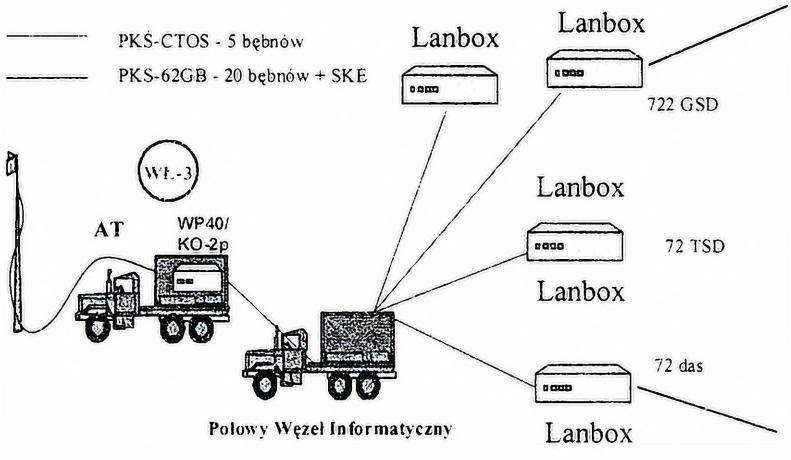
Rysunek 7. Struktura GSD 72 BGB



Rysunek 8. Struktura TSD 72 BGB

Oprócz powyższych stanowisk dowodzenia zostały rozwinięte także stanowiska dowodzenia 722 bz i 72 das. Jednak z uwagi na ograniczone środki i specyfikę ćwiczenia, stanowiska te zostały wpięte w sieć teleinformatyczną brygady. Ogólna ilość komputerów działających w sieci 72 BGB wynosiła 21 sztuk.

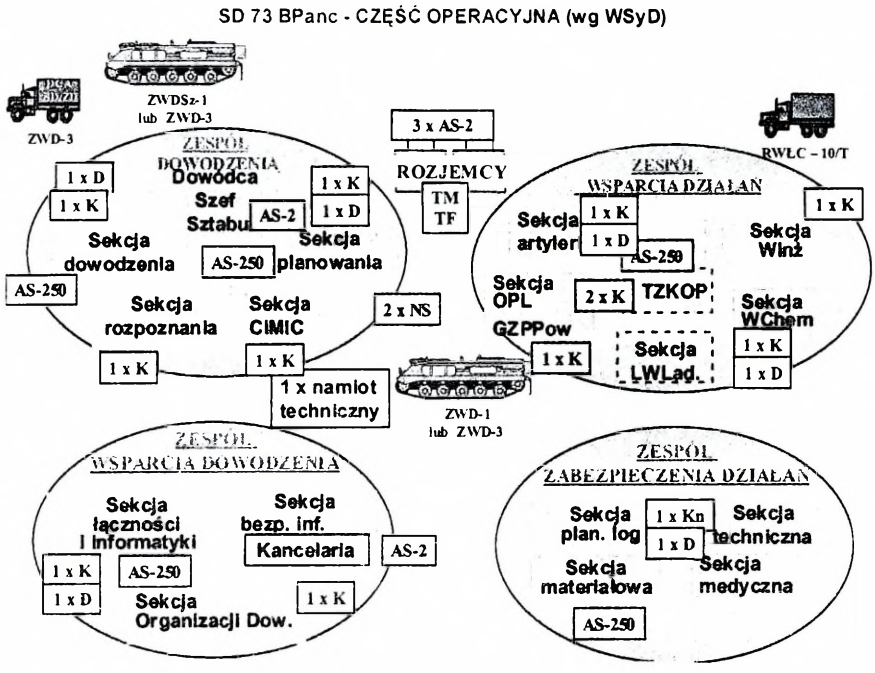
Wymianę informacji z przełożonym zapewniał polowy węzeł informatyczny (PWI), wpięty w sieć radioliniowo-kablową systemu Storczyk. Uproszczony schemat połączeń sieci komputerowej przedstawiony został na rysunku 9.



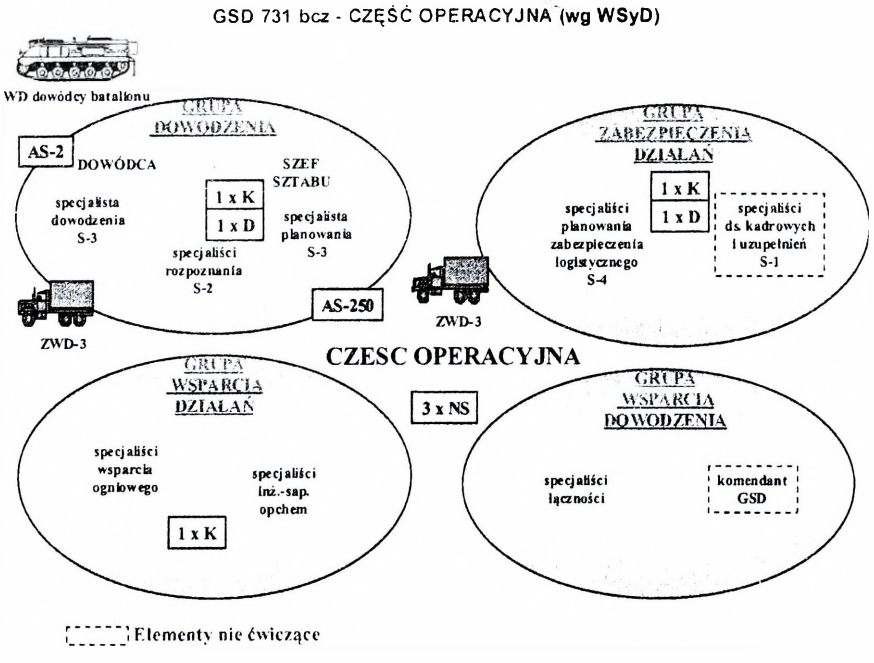
Rysunek 9. Uproszczony schemat sieci komputerowej na SD 72 BGB

Sieć 73 BPanc

Podobnie jak SD 72 BGB, także SD 73 BPanc rozmieszczone zostały na poligonie znajdującym się w Rembertowie. Struktury funkcjonalne stanowisk dowodzenia zostały przedstawione na rysunkach 10 i 11.



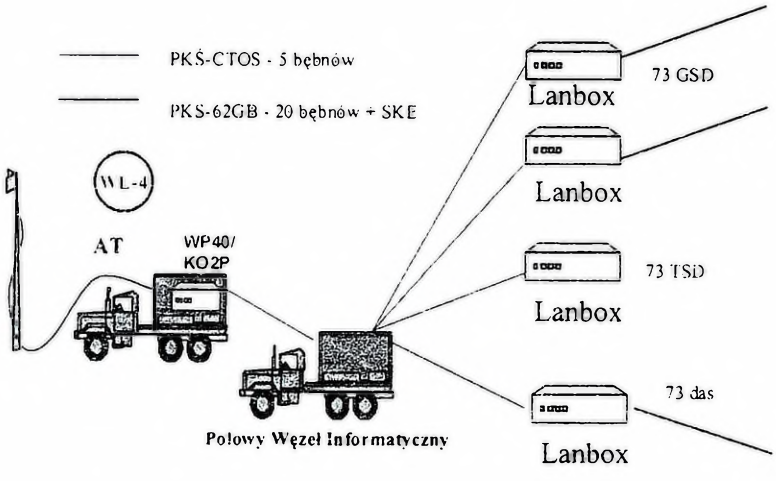
Rysunek 10. Struktura GSD 73 BPanc



Rysunek 11. Struktura TSD 72 BPanc

Oprócz powyższych stanowisk dowodzenia zostały rozwinięte także stanowiska dowodzenia 731 bcz i 73 das. Z uwagi na ograniczone środki i specyfikę ćwiczenia, stanowiska te zostały wpięte w sieć teleinformatyczną brygady.

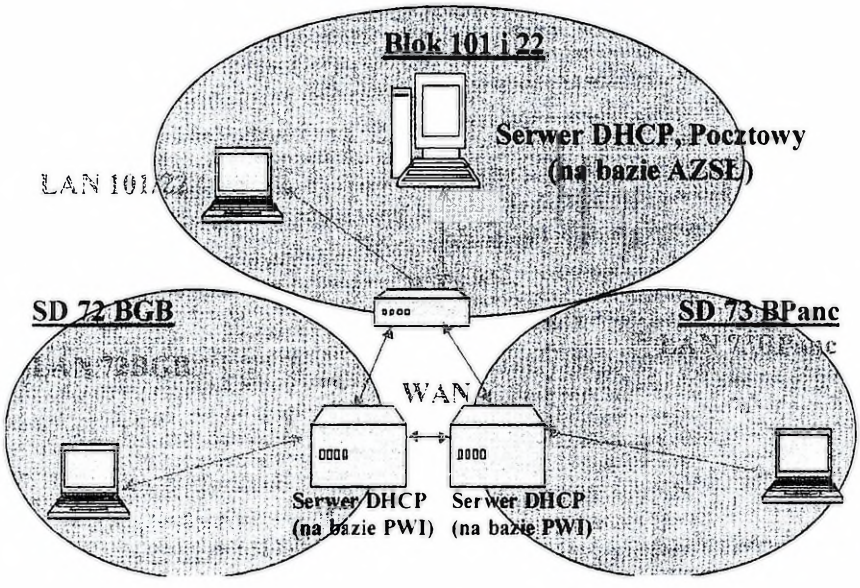
Wymianę informacji z przełożonym zapewniał polowy węzeł informatyczny (PWI), wpięty w sieć radioliniowo-kablową systemu Storczyk. Uproszczony schemat połączeń sieci komputerowej przedstawiony został na rysunku 12. W sieci 73 BPanc pracowało łącznie 17 komputerów.



Rysunek 12. Uproszczony schemat sieci komputerowej na SD 73 BPanc

Obieg informacji na ćwiczeniu

Na potrzeby ćwiczenia stworzony został specyficzny schemat obiegu informacji. Schemat ten, przedstawiony na rysunku 13, podyktowany był specyfiką ćwiczenia i brakami kadrowymi w zespole zabezpieczenia teleinformatycznego ćwiczenia. Wcześniejsze doświadczenia zdobyte w trakcie ćwiczeń „Akademicki Pierścień 2003" i „Akademicki Pierścień 2004" pozwoliły na założenie, że na potrzeby ćwiczeń realizowanych w akademii jest on wystarczający.



Rysunek 13. Schemat obiegu informacji na ćwiczeniu

Podsumowanie

Sieci teleinformatyczne wykorzystywane w trakcie ćwiczenia były kombinacją rozwiązań zarówno wojskowych jak i cywilnych. Rozwiązania czysto komercyjne zastosowane zostały w blokach szkoleniowych, natomiast rozwiązania wojskowe na polowych stanowiskach dowodzenia ćwiczących zespołów.

W czasie trwania ćwiczenia nie zaobserwowano jakichkolwiek błędów związanych z transmisją danych, a przyjęte rozwiązania spełniły swoje zadania.

Na uwagę zasługuje fakt, że sieci teleinformatyczne na polowych stanowiskach dowodzenia rozwinięte zostały w całości w oparciu o środki polowe. Do głównych środków, wykorzystywanych do tego celu, należy zaliczyć:

RWŁC-10 T/K,

AZSŁ,

PWI,

SERVERBOX,

LANBOX,

PKS ze złączem 62 BG,

PKŚ CTOS,

moduł SKE.

Jedynym zaobserwowanym mankamentem związanych z wykorzystaniem polowych środków teleinformatycznych jest czas ich rozwinięcia, a tym samym ich duży wpływ na mobilność stanowisk dowodzenia.

Systemy sprzętowe do budowy polowych sieci teleinformatycznych na stanowiskach dowodzenia

mgr inż. Marek DRAS
Radiotechnika Marketing Sp. z o.o., Wrocław

W tym artykule przedstawiona jest problematyka projektowania i budowy sprzętu teleinformatycznego wchodzącego na wyposażenie stanowisk dowodzenia. Omówiono podstawowe wymagania techniczno-eksploatacyjne oraz współczesne technologie stosowane do budowy współczesnego wojskowego sprzętu teleinformatycznego. W dalszej części przedstawiono wyroby firmy Radiotechnika Marketing produkowane w oparciu o te wymagania. Wyroby te są stosowane od kilku lat w Wojsku Polskim.

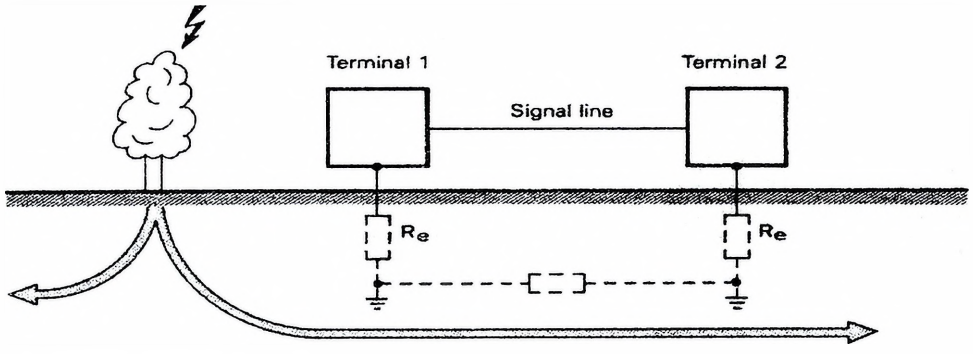
Polowe sieci teleinformatyczne rozwijane na stanowiskach dowodzenia zbudowane są z systemów przetwarzania, przechowywania i transmisji danych oraz z układu połączeń kablowych i bezprzewodowych lokalnie pomiędzy nimi (sieć LAN) oraz z systemami odległymi (sieć WAN). Systemy te zwane systemami C^4I (term. ang. Command, Control, Communication, Computers Inteligence) tworzą podstawową platformę sprzętową działania stanowisk dowodzenia (SD) zgodną z najnowszą doktryną w sieciocentrycznych operacji wojskowych (term. ang. Network-Centric Warfare). Polowe sieci teleinformatyczne (PST) i zastosowany w nich sprzęt muszą spełniać szereg wymagań ze względu na ich specyfikę zastosowań:

1. Łatwość rozwijania sieci (term. ang. deployability)w każdych warunkach pogodowych, terenowych i przy pomocy żołnierzy nie w pełni przeszkolonych we własnościach i działaniu sprzętu oraz „ nie delikatnie" obchodzących się z tym sprzętem.
2. Krótki czas rozwijania PST od 0.5 do 1 godziny ze względu na to, że czas działania SD na współczesnym polu walki jest oceniany na 3 do 4 godzin.
3. Możliwość rozwijania sprzętu w różnych warunkach lokalowych, w namiotach, w budynkach, na pojazdach.
4. Niezawodne działanie w trudnych i zmiennych warunkach otoczenia.
5. Łatwa transportowalność sprzętu różnymi środkami transportu.
6. Możliwość niezawodnego zasilania PST z różnych źródeł napięć zasilania (sieć 220V, agregaty prądotwórcze, UPS, baterie akumulatorów).
7. Konieczność eliminacji emisji elektromagnetycznej promieniowanej i przewodzonej z urządzeń i kabli.

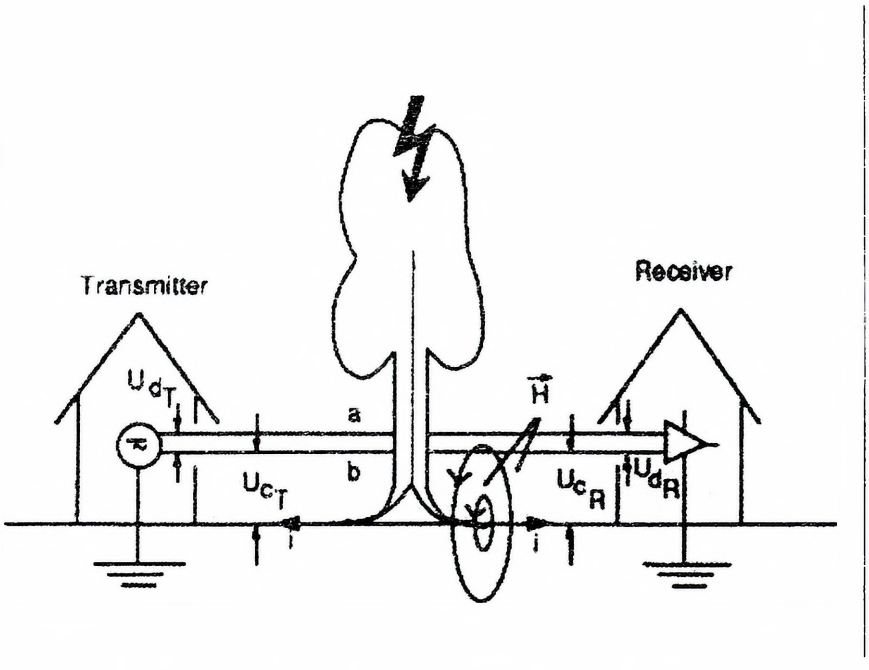
PST są zbudowane z bardzo podobnych funkcjonalnie elementów jak sieci stacjonarne, jednakże na tym kończy się ich podobieństwo. Różnice między tymi dwoma rodzajami sieci są zasadnicze zwłaszcza gdy weźmie się pod uwagę warunki ich pracy oraz sposób eksploatacji.

Główne różnice między nimi to:

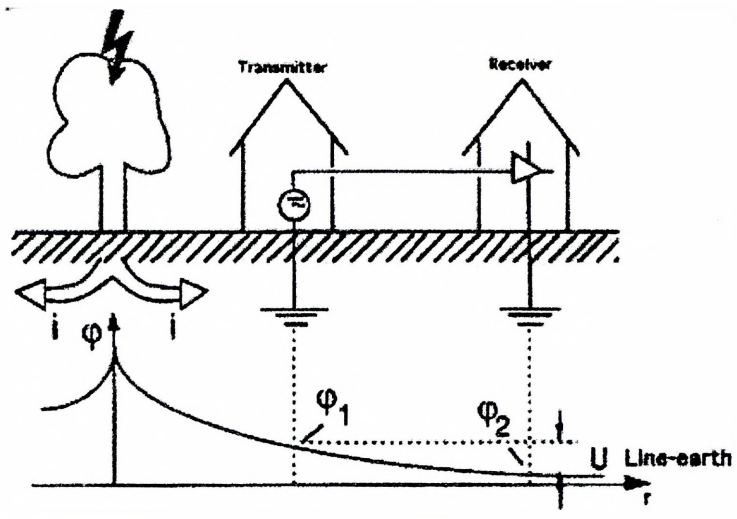
1. Trudne warunki otoczenia podczas rozwijania i pracy PST: niskie i wysokie temperatury, woda, piasek , pył, nasłonecznienie i mróz. Warunki te mogą występować jednorazowo lub oddziaływać cyklicznie w czasie na rozwiniętą PST.
2. Elementy PST muszą być szybko i łatwo rozwijalne i uruchamiane do pracy.
3. Sieci polowe są mniej rozbudowane od sieci stacjonarnych i zawierają mniej elementów.
4. Elementy PST muszą być odporne na narażenia mechaniczne i „twarde" użytkowanie podczas użytkowania.
5. Sieć PST jest zasilana z kilku źródeł napięcia. Każde może być innego rodzaju i każde może być niestabilne. Zasilanie z różnych źródeł powoduje powstawanie potencjałów i napięć rozległych i przepływy prądów wyrównawczych w samych kablach jak i w ekranach kabli. Stąd powstaje zagrożenie porażeniem prądem osób obsługujących i konieczność dobrego uziemienia instalacji w różnych warunkach glebowych.
6. Systemy polowe muszą pobierać mało mocy ze względu na ograniczone wydajności źródeł zasilania zewnętrznego a zwłaszcza UPS i baterii słonecznych spotykanych w nowych rozwiązaniach. Ponadto w systemach tych wymagane jest minimalizowanie wydzielania ciepła ze względu na konieczność pracy w wysokich temperaturach otoczenia.
7. Bezpośrednie narażenie urządzeń na oddziaływanie wyładowań elektromagnetycznych o dużych energiach (LEMP, NEMP, bomby elektromagnetyczne). Wyładowania atmosferyczne w obiekty odległe o kilkadziesiąt do kilkuset metrów od elementów PST indukują w kablach napięcia niszczące urządzenia do nich dołączone. Ekranowanie kabli zmniejsza poziom tych napięć ale ich do końca nie eliminuje. Na rysunkach 1, 2, 3 pokazano mechanizm indukowania się napięć niebezpiecznych w okablowaniu PST przy uderzeniu pioruna w pobliskie drzewo. Na rysunku 4 pokazano mechanizm indukowania się przepięć w kablach ekranowanych w skutek przepływu prądu wyładowań przez ekran kabla.
8. Wymagany krótki czas uruchamiania (podnoszenia) systemów teleinformatycznych rozwijanych w polu.



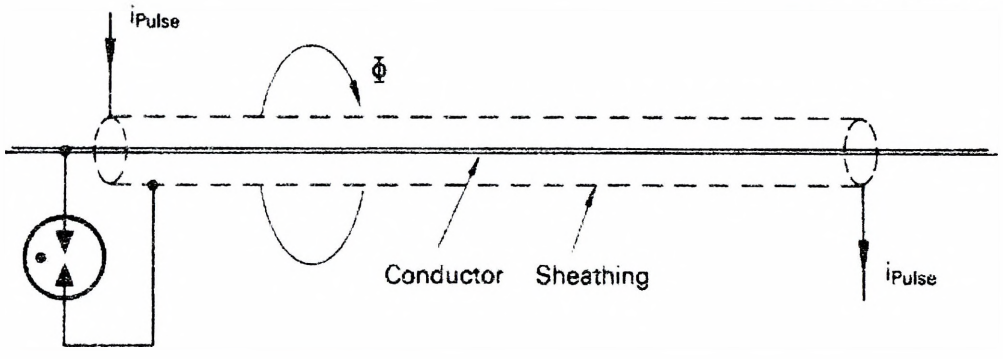
Rysunek 1. Powstawanie napięć niszczących spowodowanych przez oddalone wyładowania atmosferyczne



Rysunek 2. Indukowanie napięć niszczących w kablach rozciągniętych na ziemi



Rysunek 3. Niszczące spadki napięć powstałe w wyniku przepływu prądu wyładowania w ziemi



The magnetic coupling between cable sheathing and conductor

Rysunek 4. Mechanizm indukowania napięć niebezpiecznych w kablach ekranowanych

Bardzo ważnym wymaganiem stawianym PST jest niski poziom emisji ujawniającej promieniowanej i przewodzonej oraz jej odporność na narażenia elektromagnetyczne. Wymagania te są oparte o normy wojskowe NO-06-A200, NO-06-A500, (MIL Std 461D), MIL Std 188-125-2. Norma MIL Std 188-125-2 określa poziom odporności PST na narażenia elektromagnetyczne. Z tych norm wynika konieczność bardzo starannego ekranowania, uziemienia i wyposażania systemów w układy przeciwprzepięciowe we wszystkich obwodach i przyłączach kablowych dochodzących do nich z zewnątrz. Mogą one być antenami promieniującymi sygnały z wewnątrz lub zbierającymi sygnały niszczące przychodzące z zewnątrz.

Systemy informatyczne na stanowiskach dowodzenia pracują w sieci LAN w standardzie transmisji Ethernet IEEE802.3. Standard ten jest nadal najszybciej rozwijającym się na świecie w zakresie przewodowej transmisji danych. Stosowanie go w PST pozwala na uzyskiwanie dużych szybkości transmisji. Przez polowe kable skrętkowe kategorii piątej transmisja jest dokonywana w standardach Ethernet 10 Base T i Ethernet 100 Base Tx. Poprzez polowe kable światłowodowe transmisja dokonywana jest w standardach Ethernet 10 Base FL i Ethernet 100 Base Fx. Zgodnie z najnowszymi wymaganiami TACOMS w nowych systemach klasy C^4I jest zalecana transmisja przez kable światłowodowe w standardzie Gigabit Ethernet 1000 Base Fx. Zasięgi transmisji przez polowe kable skrętkowe wynoszą do 100m. Zasięgi przez polowe kable światłowodowe wielomodowe wynoszą od 500 do 4000m (wg STANAG 4290). Dla Gigabit Ethernet uzyskuje się zasięgi przez kable światłowodowe do 500m. Dla połączeń bezprzewodowych w standardzie IEEE802.11b,g uzyskuje się zasięgi od 600m w gęstym, mokrym lesie oraz do kilku kilometrów na otwartej przestrzeni.

W systemach polowych podstawowe media transmisyjne przewodowe tj. kable skrętkowe i światłowodowe muszą być stosowane w wykonaniach polowych. Stosowanie standardowych kabli skrętkowych i światłowodowych czyni ten element stanowiska bardzo awaryjnym. Kable te mogą być uszkadzane mechanicznie oraz przez wpływ temperatury, wodę i wilgoć. Wadliwe działanie standardowego kabla w wyniku oddziaływania tych czynników może wystąpić niekoniecznie w momencie ich oddziaływania, lecz po pewnym czasie w wyniku penetracji wnętrza kabli.

PST są zbudowane z szeregu systemów razem tworzących kompletny działający w trudnych warunkach system informatyczny, wspomagający pracę SD na różnych szczeblach. Poszczególne elementy mogą być osobno stosowane na różnych szczeblach stanowisk dowodzenia. Przy rozbudowanych SD istnieje możliwość łączenia równoległego systemów lub dołączania dodatkowych odległych systemów poprzez połączenia kablowe lub bezprzewodowe pod warunkiem posiadania przez nie jednakowych standardowych interfejsów.

Głównymi elementami PST są:

- serwery polowe pojedyncze lub klastry wieloserwerowe
- macierze dyskowe
- koncentratory linii komputerowych (zarządzane switche warstwy 2 i 3)
- routery z różnorodnymi wyjściami do sieci WAN
- terminale komputerowe
- systemy zasilania mocy podstawowe i awaryjne

- systemy łączności bezprzewodowej w sieci LAN
- okablowanie miedziane i światłowodowe

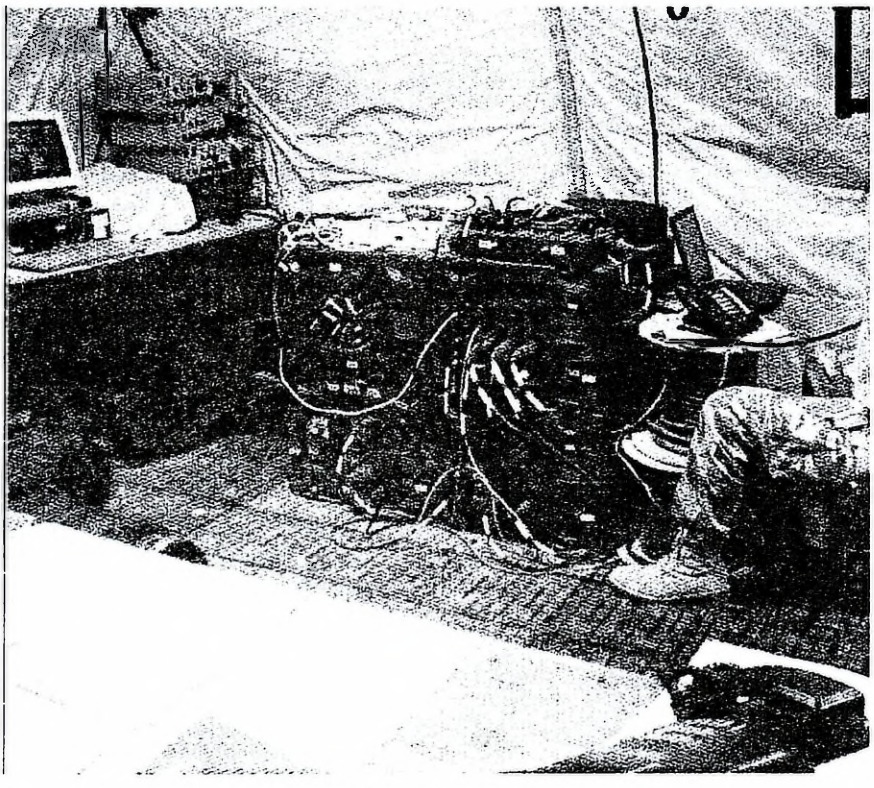
Systemy informatyczne do zastosowań w PST są wykonywane w technologiach dedykowanych do ciężkich warunków pracy. Sprzęt w wykonaniu cywilnym nie nadaje się do tego rodzaju zastosowań gdyż podstawowe warunki pracy na SD są z reguły warunkami niszczącymi ten sprzęt. Z doświadczeń i obserwacji ćwiczeń wojskowych wynika, że stosowanie tego sprzętu powoduje, że po jedno lub dwukrotnym użytkowaniu jest on bezpowrotnie uszkodzony.

Sprzęt stosowany do PST musi być w wykonaniu wojskowym, gdyż wtedy zagwarantowana jest jego niezawodna praca przez wiele lat. Jednakże jeśli weźmie się pod uwagę sprzęt pasywny to dobrze spełnia on swoje zadanie przez kilka lub kilkanaście lat eksploatacji, natomiast sprzęt aktywny podlega silnemu procesowi starzenia moralnego, co w przypadku sprzętu informatycznego czyni go niezdatnym do użytku po kilku latach. Stąd od kilku lat technologia COTS (term. ang. commercial of the shelves) jest stosowana w budowie informatycznych urządzeń wojskowych. Szczególnie powszechna jest technologia „utwardzany COTS" (term. ang. hardened COTS). Obecnie jest ona najszerzej stosowana w konstrukcjach wojskowego sprzętu informatycznego. Trendy rozwojowe obserwowane w nowych konstrukcjach i technologiach wojskowych również opierają się na technologii COTS. Rozróżnia się trzy poziomy utwardzania (rugedyzacji) V1, V2 i V3. Poziom V1 to najsłabszy poziom utwardzenia odpowiadający poziomowi urządzeń do zastosowań biurowo-przemysłowych. Poziom V2 dotyczy urządzeń do stanowisk polowych na SD i do zastosowań w pojazdach ale nie zamkniętych w szczelnych obudowach. Poziom V3 dotyczy najcięższych zastosowań z pełną odpornością systemów na wszelakie narażenia, szczelnie zabudowanych.

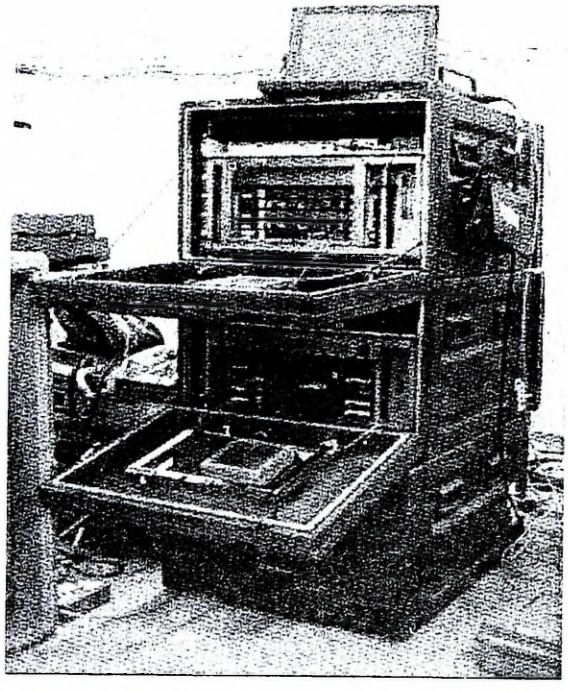
Technologia COTS, polegająca na dostosowaniu wyselekcjonowanych urządzeń informatycznych powszechnego użytku lub w wykonaniach przemysłowych do zastosowań wojskowych, pozwala na zastosowanie w urządzeniach wojskowych najnowszych technologii informatycznych. Postęp technologii informatycznych przenosi się dzięki temu łatwo i szybko do zastosowań wojskowych. Również jeżeli się weźmie pod uwagę zwykle długi czas opracowania sprzętu w wykonaniu czysto wojskowym to jest on już w momencie wdrażania do stosowania często przestarzały a technologia COTS pozwala na skrócenie tego czasu.

Dodatkową zaletą tej technologii jest możliwość uzyskania niższych kosztów wdrożenia wyrobów dla wojska. Ze względu na standaryzację technologii informatycznych istnieje możliwość modernizacji sprzętu wojskowego wykonanego w technologii COTS. Dodatkową ko-

rzyścią jest zaoszczędzenie kosztów opracowania technologii i programów informatycznych, które przejmuje się razem z systemami cywilnymi i jedynie dorabia się do nich część czysto wojskową. Na rys. 5 pokazano przykład polowego przenośnego systemu telekomunikacyjnego typu DPABX firmy EADS-Cogent z Anglii wykonanego w technologii COTS.



Rysunek 5. Rozwinięty system typu DPABX firmy EADS Cogent



Rysunek 6. Widok wnętrza systemu DPABX

Urządzenia te wchodzą do systemu Cormorant. System Cormorant jest przewoźno-przenośnym systemem do sieci rozległych (Theatre Wide Area Network), zaprojektowanym dla sił szybkiego reagowania armii brytyjskiej Joint Rapid Reaction Forces (JRRF). Są one stosowane przez armię brytyjską w operacji w Iraku. Poszczególne pojemniki zawierają wydzielone bloki funkcjonalne systemu i są między sobą połączone kablami. Na rys. 6 pokazano wnętrze tych pojemników, gdzie widać poszczególne moduły o szerokości 6U umieszczone poziomo w standardowej ramie 19". Urządzenie to jest węzłem teleinformatycznym służącym do przetwarzania danych oraz przełączania linii teleinformatycznych oraz transmisji danych. Umożliwia dołączenie terminali komputerowych, telefonów cyfrowych ISDN i analogowych oraz satelitarnych. Posiada wyjścia LAN Ethernet 10/100BaseT i interfejsy szeregowe V28, V34 oraz wyjścia typu E1 do sieci WAN. Dzięki nim łatwo łączy się z innymi systemami, w tym z systemami stacjonarnymi. System zasilany jest z sieci 220V i z napięcia stałego 28V. W opinii użytkowników (oddziały JRRF) system jest bardzo wygodny i mobilny w użyciu na różnych stopniach SD, posiada bardzo duże możliwości funkcjonalne i jest bardzo tani w eksploatacji. Uzyskano kompletną polową sieć pracującą z protokołami IP, mającą możliwość przełączania multimedia i rozwiniętą szybko w warunkach polowych. Jako cieka-

wostkę podano, że koszt zastosowania na ćwiczeniach jednego systemu jest niższy niż koszt prania mundurów po ćwiczeniach Saif Sareea w Omanie w roku 2002.

Należy od razu zaznaczyć, że technologia COTS wbrew pozorom jest trudna i nie wszędzie może być zastosowana do budowy urządzeń wojskowych.

Wady technologii COTS są następujące:

1. Trudność w wyborze urządzeń, które mogą być poddane procesowi utwardzenia.
2. Krótki czas dostępności na rynku urządzeń podlegających utwardzeniu w danej wersji, które się wybrało, wynoszący 3 do 4 lat.
3. Nieprzewidywalność zmiany bazy materiałowej na jakiej są wykonywane poszczególne serie wyrobów na rynek, które są sukcesywnie brane do produkcji dla wojska i poddawane procesowi utwardzenia.
4. Brak możliwości gruntownego sprawdzenia bazy oprogramowani urządzeń.
5. Urządzenia danego typu i pochodzące od określonego nawet renomowanego producenta naprawdę wewnątrz różnią się od siebie w zależności od partii wyrobów i są często wykonywane przez różnych wykonawców.

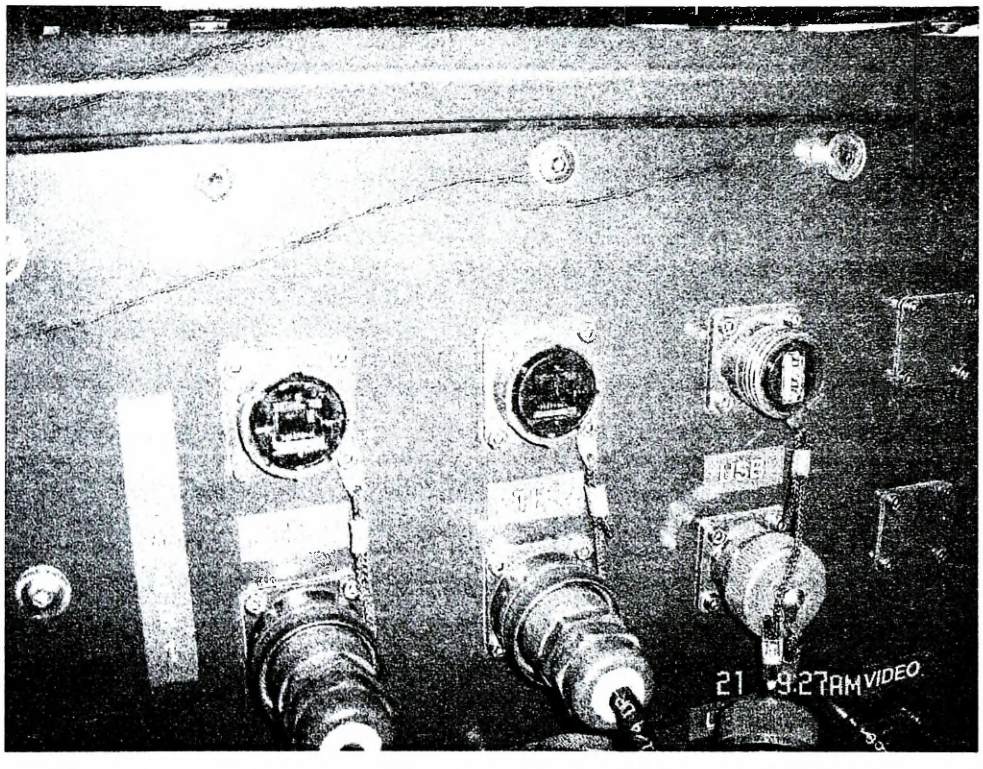
Podczas procesu utwardzania urządzeń komercyjnych dokonywane są w nich najczęściej następujące operacje i zmiany w konstrukcji:

- wymiana podzespołów na pracujące w szerokim zakresie temperatur
- wymiana zasilaczy mocy
- zmiana układu chłodzenia
- analiza termiczna urządzenia w czasie pracy i selekcja obwodów do wykonania zmian
- zmiana złącz i przełączników
- zmiana obudowy

Podczas procesu utwardzania w technologii COTS największymi trudnościami do pokonania są:

- praca procesorów z dużymi częstotliwościami taktowania w wysokich temperaturach
- start urządzeń w niskich temperaturach
- odporność twardych dysków i złącz na wibracje i udary i niskie temperatury
- efektywne odprowadzanie ciepła z obudów
- powszechne stosowanie obudów o wysokości 1U w urządzeniach wybranych do utwardzania utrudniające chłodzenie układów wewnętrznych
- ograniczanie poboru mocy przez układy
- eliminacja zakłóceń elektromagnetycznych
- źródła zasilania, zasilacze UPS

- monitory ekranowane, a zwłaszcza ich zakres temperatur pracy, odporność na narażenia mechaniczne i środowiskowe oraz eliminacja emisji elektromagnetycznej
- konieczność stosowania złączy wojskowych, stosowanie wersji wojskowych złącz typu RJ-45, USB czy Fire-Wire pozwala na dołączenie innych standardowych urządzeń również cywilnych do systemów wojskowych, rys.7.
- filtracja zakłóceń i konieczność uziemiania systemów
- konieczność unikania wprowadzania do wnętrza urządzeń powietrza chłodzącego bezpośrednio z atmosfery przez co następuje penetracja wilgoci i uszkodzenie układów w niskich temperaturach
- wbudowywanie systemów zabezpieczania układów przed niszczącymi przepięciami z zewnątrz
- szybkość i łatwość uruchamiana (podnoszenia do pracy) systemów informatycznych
- przystosowanie oprogramowania do zastosowań polowych systemów

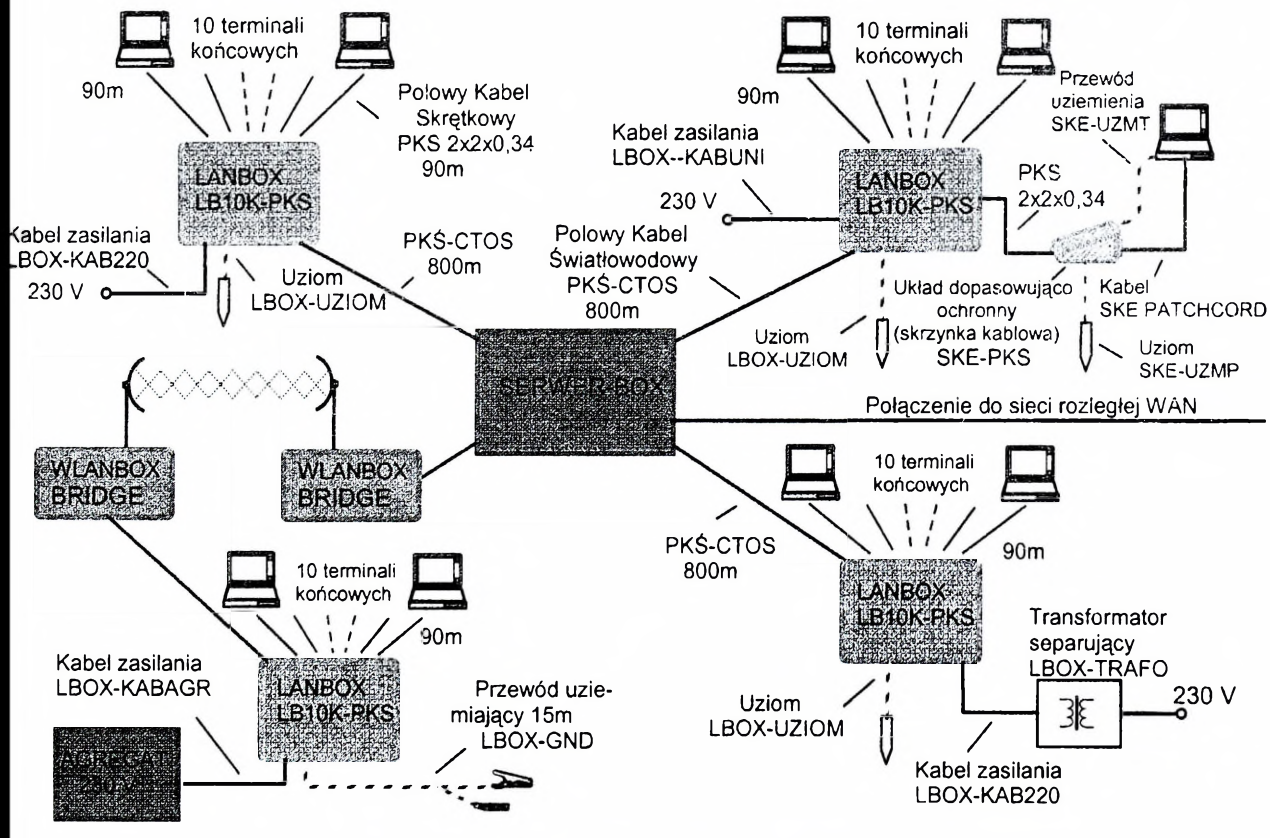


Rysunek 7. Złącza typu RJ-45 i USB w wykonaniu wojskowym umieszczone na płycie czołowej urządzenia do pracy w warunkach polowych

Wszystkie dalej przedstawione systemy spełniają powyżej opisane wymagania. Systemy te powstały przy ścisłej współpracy z Wojskiem Polskim. W ich budowie uwzględniono wymagania, które były zgłaszane wstępnie przez użytkowników lub powstały podczas ćwiczeń.

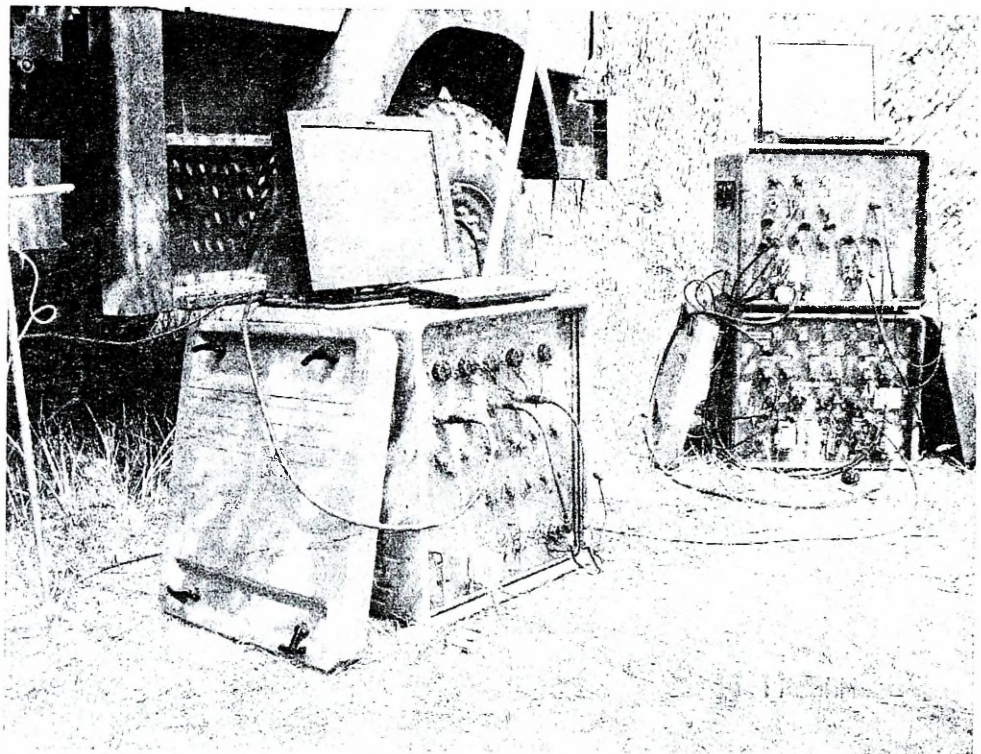
Niektóre systemy pracują w Iraku od początku tej operacji. Systemy te kwalifikują się do kategorii V2 i V3 rugedyzacji w technologii COTS.

Systemy te mogą pracować niezależnie od siebie, lub odpowiednio połączone mogą tworzyć kompletną rozbudowaną PST, rys.8. Zapewniają one kompletność rozwiązania i spełniają podstawowe funkcje systemu informatycznego na SD różnych szczebli. Wszystkie opisane systemy pracują w standardowych rodzajach pracy i są w nich wykorzystane standardowe interfejsy. Nie ma w nich żadnych rozwiązań nietypowych lub unikalnych ograniczających ich współpracę z innymi systemami lub urządzeniami pochodzącymi od innych producentów.



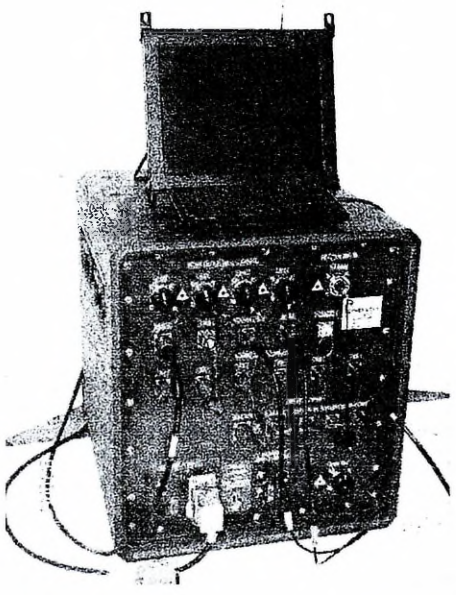
Rysunek 8. Schemat Polowej Sieci Teleinformatycznej opartej o systemy przenośno-przewoźne

System SERWER-BOX, rys.9, jest przenośnym polowym węzłem komputerowym służącym do przetwarzania danych, zarządzania Polową Siecią Komputerową (PSK) i przechowywania danych. Spełnia rolę aparatowni komputerowej, ale nie jest umieszczony w szczelnym kontenerze na pojeździe i może być instalowany w namiotach, budynkach lub na dowolnych pojazdach. Na komputerach systemu jest zainstalowane oprogramowanie Windows 2003 Serwer i Exchange 2003 Serwer jak również inne oprogramowanie. System ma budowę modułową i jego wielkość zależy od wersji i przeznaczenia. Wszelkie elementy składowe systemu SERWER-BOX są zabudowane w szczelnych środowiskowo i elektromagnetycznie pojemnikach.



Rysunek 9. Rozwinięte w polu dwa systemy SERWER BOX na SD, z lewej system wersji podstawowej i z prawej w wersji rozbudowanej

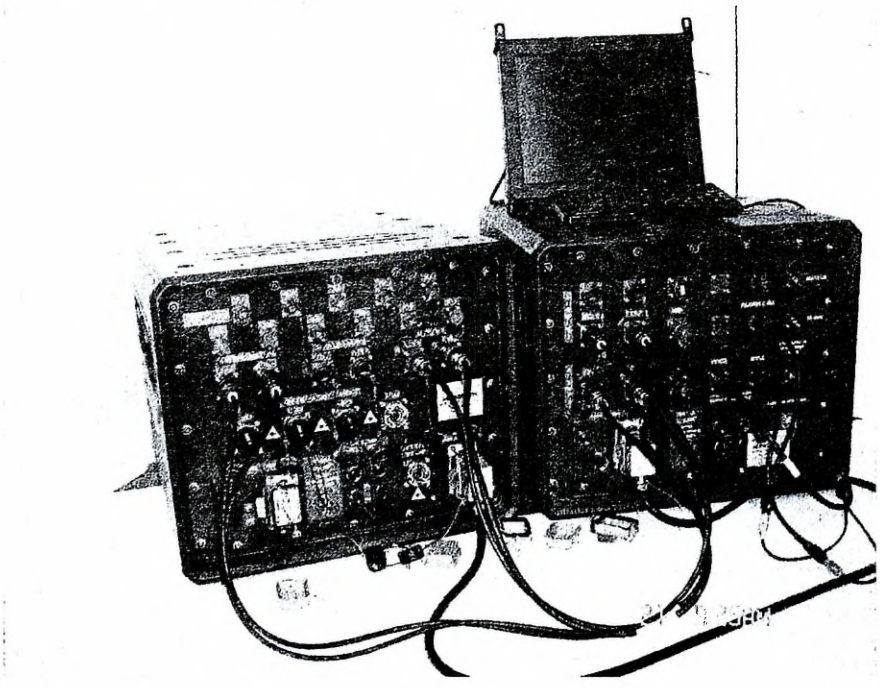
W wersji podstawowej SERWER-BOX 1 - system jest umieszczony w jednym pojemniku typu PWSK-WP (**P**olowa **W**ielostanowiskowa **S**tacja **K**omputerowa **W**ersja **P**odstawowa), rys.10.



Rysunek 10. Widok systemu SERWER BOX WP (wersja podstawowa z klawiaturą i monitorem RMK-1

System w wersji podstawowej posiada pojedynczy serwer z macierzą dyskową typu RAID-5, router z wieloma wyjściami WAN (E1, voice, V-35, ISDN) zarządzany przełącznik warstwy 2 i zasilacz UPS. Można do niego dołączyć 46 terminali końcowych poprzez koncentrator LANBOX LB10K-PKS.

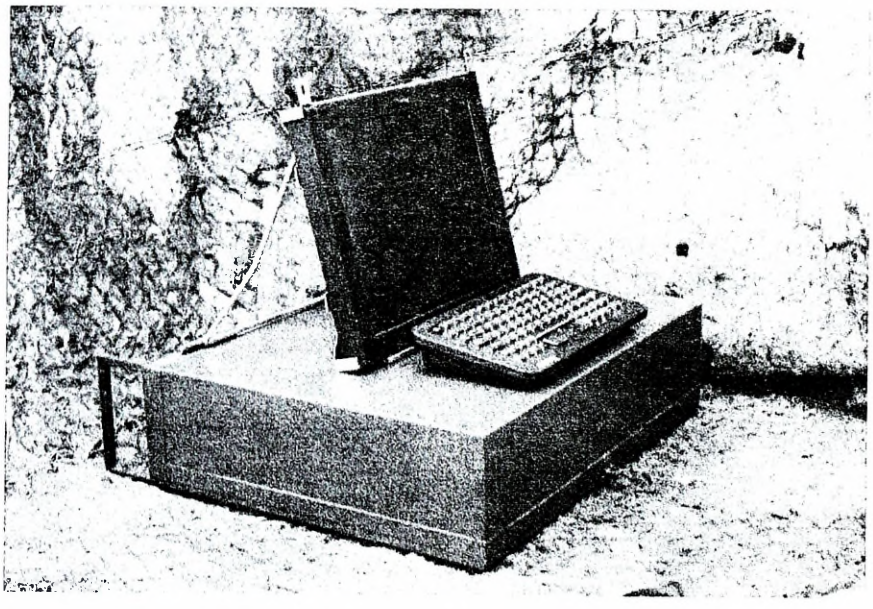
W wersji rozbudowanej SERWER-BOX 2 - system jest umieszczony w dwu pojemnikach typu PWSK-1P i PWSK-1S, rys. 11.



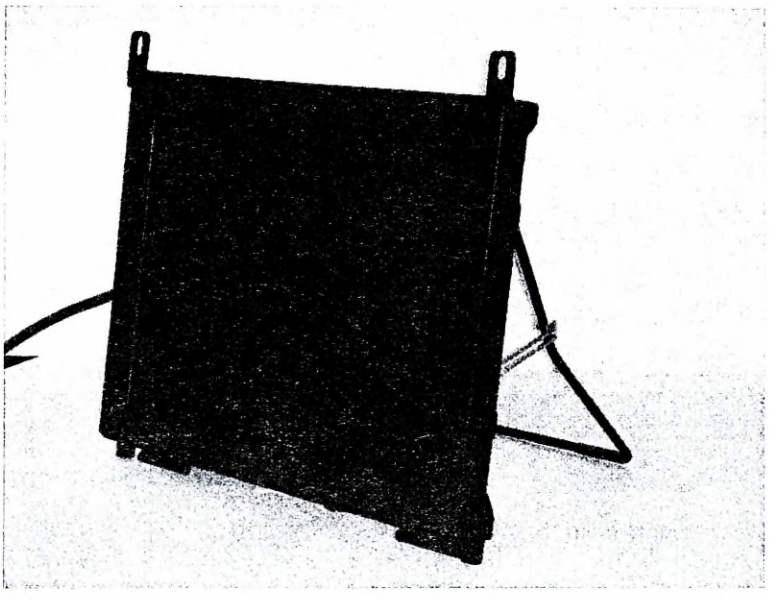
Rysunek 11. Widok systemu SERWER BOX-2 (wersja rozbudowana w dwu pojemnikach)

System SERWER-BOX w wersji rozbudowanej posiada:

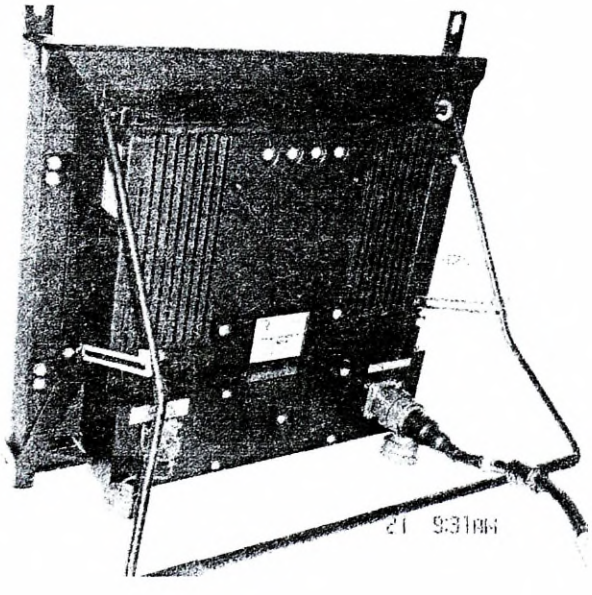
- pojemnik PWSK-1P (moduł przełączający) zawierający zasilacz UPS systemu zarządzalny przełącznik warstwy 3 z możliwością routingu i system przyłączania do serwerów stanowisk roboczych oraz odległych terminali komputerowych poprzez koncentratory LANBOX LB10K-PKS, w sumie 51 terminali.
- pojemnik PWSK-1S (moduł serwerowy) zawierający systemy wieloserwerowe, obejmujące klaster dwuserwerowy poczty elektronicznej oraz serwer bazy danych i aplikacji, a także połączone z serwerami macierze dyskowe typu RAID-5,
- obudowy RSK-1 (**R**ugedyzowane **S**tanowisko **K**omputerowe) rys.12. dające ochronę środowiskową i ekranowanie elektromagnetyczne dla umieszczonych wewnątrz standardowych komputerów notebook w obudowach plastikowych. Obudowa posiada zewnętrzny, odporny środowiskowo monitor RMK-1, rys.13 oraz szczelną, odporną na narażenia klawiaturę z myszą. Szczelna obudowa tego monitora wykonana jest z jednego bloku aluminiowego i służy również jako radiator do układów scalonych znajdujących się wewnątrz. Wszystkie złącza i ekranowane kable przyłączeniowe monitora są w wykonaniu wojskowym
- zespół ekranowanych kabli połączeniowych elementów systemu



Rysunek 12. Rugedyzowane stanowisko komputerowe RSK-1



Rysunek 13. Odporny na wpływy środowiska monitor RMK-1



Rysunek 14. Widok z tyłu szczelnej obudowy monitora RMK-1 wraz ze złączami i kablami przyłączeniowymi

Cały system SERWER BOX jest wykonany w technologii TEMPEST, zapewniającej niski poziom emisji ujawniającej, przewodzonej i promieniowanej, przez co nie musi być używany na stanowiskach dowodzenia umiejscowionych w stalowych, szczelnych kontenerach. Całość systemu jest odporna na narażenia środowiskowe, wstrząsy i wibracje wg WPN-85/N-1007 i może pracować w zakresie temperatur od -25°C do +50°C. Ciężar każdego z pojemników wynosi około 40kg. Wymiary obu pojemników systemu SERWER-BOX 2 wynoszą: W x S x D = 440 x 534 x 710mm. System zasilany jest z sieci 230V lub awaryjnie z wewnętrznego

zasilacza UPS. Dzięki temu może być używany w dowolnych miejscach na SD. W miejscach tych nie ma problemu ograniczenia ilości stanowisk pracy dla wieloosobowej obsługi, problemu znanego ze szczelnych kontenerów spawanych, rys.9.

System ma bardzo niezawodną strukturę: posiada redundantne zasilacze typu hot swap oraz redundantne serwery również typu hot swap, w tym jeden podwójny, który może być tez skonfigurowany jako klaster i dwie macierze dyskowe RAID-5 z dyskami hot swap. W przypadku awarii pojemnika PWSK-1P rolę przełącznika systemu może przejąć jeden z koncentratorów LANBOX. Zastosowana architektura serwerów zapewnia dużą wydajność w czasie pracy. Zarządzany system przełączania zapewnia dużą przepustowość danych. Możliwe jest dokonywanie usług w technologii VoIP dzięki zastosowaniu przełączników i routerów zapewniających dużą przepustowość danych. Do sytemu można też dołączyć radiostację przez styk V24.

Jako komputery stacji roboczych można stosować standardowe plastikowe komputery notebook pracujące w zamkniętych, stalowych obudowach RSK-1, chroniących je przed wpływami otoczenia i zapobiegające emisji ujawniającej. Zewnętrzne ekranowane monitory mają dużą jasność, większą niż ekrany komputerów notebook. Monitor oraz klawiatura są przenoszone w stalowym pudełku ochraniającym. Wszystkie złącza komputera notebook są wyprowadzone na tylną ściankę obudowy RSK-1 poprzez złącza wojskowe (RJ-45, USB) umożliwiając dołączenie do niego dodatkowych urządzeń zewnętrznych.

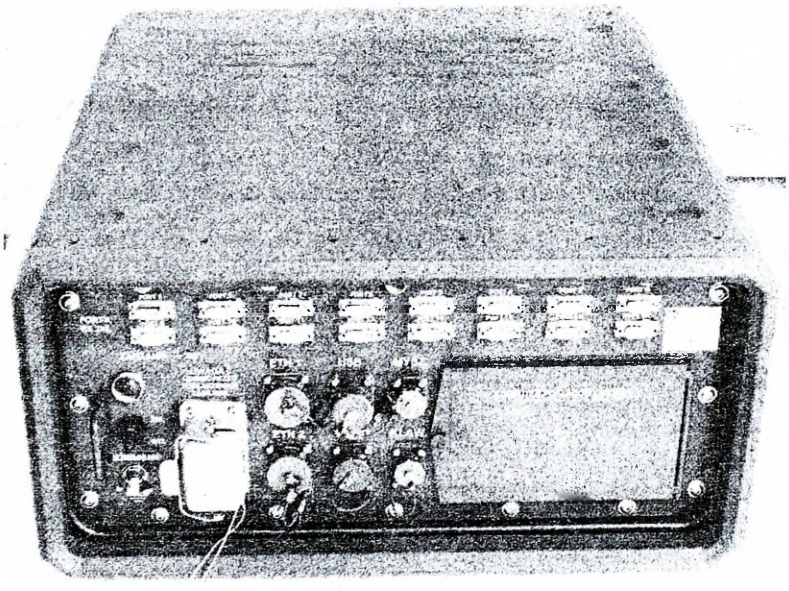
System SERWER-BOX jest typowym przykładem technologii COTS ściśle dedykowanym do pracy w trudnych warunkach pracy w polu.

Zalety systemu SERWER-BOX do zastosowań polowych są następujące:

1. Duże możliwości obliczeniowe i skalowalność systemu.
2. Szybkie rozwijanie stanowiska dowodzenia i PST w dowolnym miejscu i bez ograniczeń powierzchni.
3. Brak ograniczeń miejsca pracy obsługi występujących w kontenerowych stanowiskach dowodzenia.
4. Niska cena w stosunku do ceny aparatowni kontenerowej.
5. Możliwość szkolenia żołnierzy obsługujących stanowiska dowodzenia i całą PST na docelowym sprzęcie, który można rozwinąć w dowolnym miejscu, w krótkim czasie i niskim kosztem. Dzięki temu uzyskuje się dobre, praktyczne zapoznanie żołnierzy z tym sprzętem.

6. Możliwość używania na stanowisku dowodzenia tanich standardowych komputerów typu notebook, zawsze nowoczesnych w stosunku do drogich notebooków w wykonaniu wojskowym. Dzięki obudowom ekranującym są one dodatkowo chronione przed wpływami otoczenia.
7. Łatwość przenoszenia i transportu, możliwość przewożenia, np. na wozie kablowym, w kontenerze technicznym czy transporterze opancerzonym.

Komputer pokładowy RKP 1-1.6, rys.15, jest urządzeniem uodpornionym na wpływy otoczenia i długotrwałe narażenia transportowe a jednocześnie ma on parametry dobrego komputera do zastosowań ogólnych..

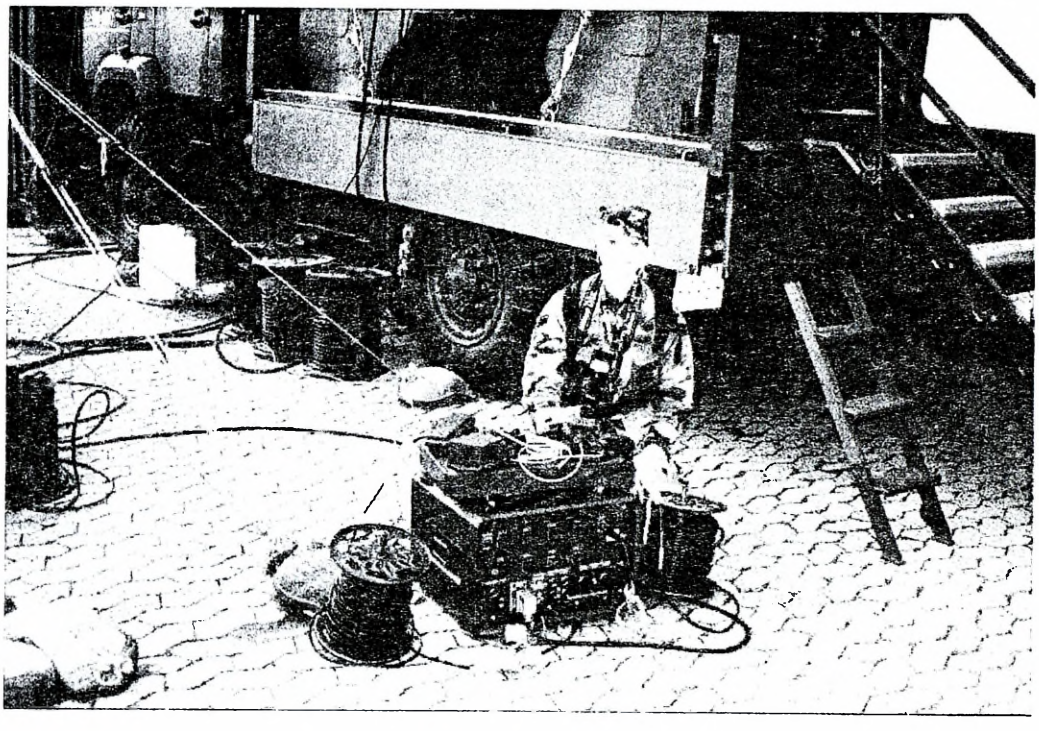


Rysunek 15. Komputer pokładowy RKP 1-1.6 do aparatowni komputerowych i pojazdów

Jest on przeznaczony do stosowania w polowych aparatowniach komputerowych oraz na pojazdach. Komputer został specjalnie zaprojektowany do systemu KROKUS produkowanego przez Wojskowy Instytut Łączności. Posiada kroploszczelną obudowę z wbudowaną ramą antywibracyjną, chroniącą układy elektroniczne. Wszystkie złącza na płycie czołowej komputera (RJ-45, USB, video, mysz, klawiatura) są w wykonaniu wojskowym. Komputer jest oparty o procesor Pentium 1,6GHz z magistralą FSB 400MHz i pamięcią L2 Cache 1MB. Pamięć operacyjna typu DDR 333 SD RAM ma pojemność 512MB. Pamięć masowa zawiera dwa dyski o pojemności po 20GB. Dodatkowo na płycie czołowej znajduje się 16 złącz interfejsu RS232 do kontroli urządzeń pokładowych w aparatowni. Posiada wbudowaną kartę sieciową Gigabit Ethernet. Zakres temperatur pracy wynosi od -5°C do +50°C. Wymiary kom-

putera 535x265x662mm a ciężar 30kg. Pobór mocy z sieci 220V wynosi 100VA. Wszystkie połączenia kablowe wychodzące z komputera są ekranowane.

Polowy koncentrator sieciowy LANBOX LB10K-PKS, rys.16, jest elementem przełączającym w lokalnych Polowych Sieciach Komputerowych PSK, rozwijanych na SD. Koncentrator jest przeznaczony do koncentracji ruchu w sieciach LAN, pracujących w systemie Ethernet. Transmisja cyfrowa po torach kablowych, miedzianych jest dokonywana poprzez Polowe Kable Skrętkowe PKS 2x2x0.34 a po torach światłowodowych poprzez Polowy Kabel Światłowodowy PKŚ CTOS.



Rysunek 16. Koncentrator LANBOX LB10K-PKS z dołączonymi polowymi kablami skrętkowymi i światłowodowymi

Koncentrator ten wraz z kablami polowymi wchodzi na wyposażenie aparatowni PWI produkowanych przez Wojskowy Instytut Łączności, systemu SZAFRAN produkowanego przez Przemysłowy Instytut Telekomunikacji oraz do aparatowni PAK 2000 opracowanej w 2 KZ w Krakowie.

Polowy przenośny koncentrator LANBOX LB10K umożliwia szybkie rozwinięcie PST w polu lub w budynkach zapewniając:

1. Dołączenie koncentratorów do odległych centralnych punktów dystrybucyjnych (CPD) na aparatowniach lub serwerach poprzez Polowy Kabel Światłowodowy PKŚ

CTOS o dług. 800m w standardzie transmisji Ethernet 10Base FL lub Ethernet 100BaseFx,

2. Dołączenie do koncentratorów od 1 do 11 stacji roboczych poprzez Polowe Kable Skrętkowe PKS 2x2x0.34 o dług. 90m, układów dopasowująco ochronnych SKE i jumperów skrętkowych o dług. 3.5m, zakończonych złączami typu RJ45, praca przy tych połączeniach jest dokonywana w standardzie transmisji Ethernet 100BaseTx.
3. Łączenie z sobą dwu koncentratorów poprzez szybkie połączenie typu uplink, kablem LBOX-UPLINK o dług. 3.5, celem zwiększenia liczby stacji roboczych dołączonych do 21 w ramach jednego SD,
4. Pracę bezobsługową oraz zarządzalność PST poprzez zastosowanie zarządzalnego przełącznika (switcha) warstwy 2 w koncentratorze, protokół SNMP, Telnet, HTTP
5. Zasilanie z sieci 220V prądu zmiennego zabezpieczone przed wyładowaniami elektromagnetycznymi lub podtrzymanie z zarządzalnego wewnętrznego zasilacza UPS,
6. Zabezpieczenie obwodów dołączonych do kabli skrętkowych przed niszczącymi skutkami wyładowań elektromagnetycznych o dużej energii,
7. Pracę na zewnątrz lub w pomieszczeniach w zakresie temperatur od –25 do +50°C,
8. Zabezpieczenie przed emisją ujawniającą promieniowaną i przewodzoną
9. Maskowanie koncentratora przy użyciu siatki rozpinanej na stelażu przykręconym do jego obudowy
10. Zabezpieczenie kabli przed przypadkowym wyrwaniem

Koncentrator zapewnia bezpośrednie połączenie i transmisję cyfrową z drugim identycznym koncentratorem, dołączonym poprzez kabel światłowodowy PKŚ CTOS w standardzie Ethernet 10Base FL lub Ethernet 100Base Fx. LANBOX LB10K-PKS zapewnia połączenie i transmisję cyfrową z CPD na aparatowniach poprzez PKŚ CTOS o dług. 800m i naburtowe złącza CTOS, zamontowane na tablicy wyprowadzeń liniowych aparatowni.

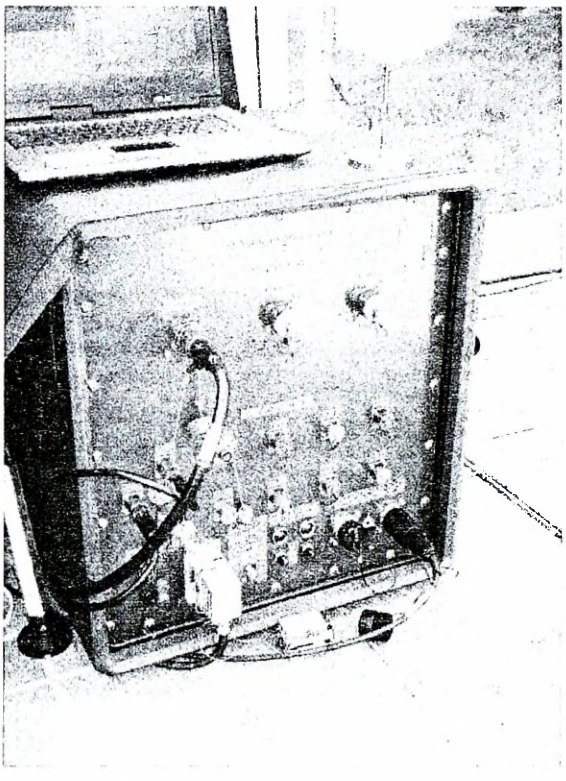
Ponadto koncentrator zapewnia połączenie z każdym wydzielonym serwerem posiadającym wejścia światłowodowe poprzez PKŚ CTOS o dług. 800m i adapter AD-CTOS mający na swym wejściu gniazdo naburtowe CTOS i cztery pojedyncze złącza światłowodowe typu ST.

Podstawowe parametry zasilania koncentratora są następujące:

1. Zasilanie 220V, 42 ÷ 65Hz
2. Pobór mocy nominalny 95VA

3. Czas pracy przy zasilaniu z zasilacza UPS co najmniej 80 minut przy temp. otoczenia wyższej niż +5°C, oraz co najmniej 35 minut przy temp. otoczenia -25°C

Koncentrator linii abonenckich LANTELBOX, rys.17 jest polowym, przenośnym urządzeniem teleinformatycznym służącym do rozwinięcia polowej sieci telefonicznej (PST) z 30 abonentami końcowymi telefonicznymi oraz do równoczesnego rozwinięcia polowej sieci komputerowej (PSK) posiadającej 10 terminali komputerowych końcowych. Koncentrator ten został opracowany przez Radiotechnikę Marketing dla systemu KROKUS i jest rozwinięciem koncepcji koncentratora LANBOX LB 10K-PKS.



Rysunek 17. Koncentrator LANTELBOX będący rozwinięciem o część telefoniczną koncentratora LANBOX LB10K-PKS

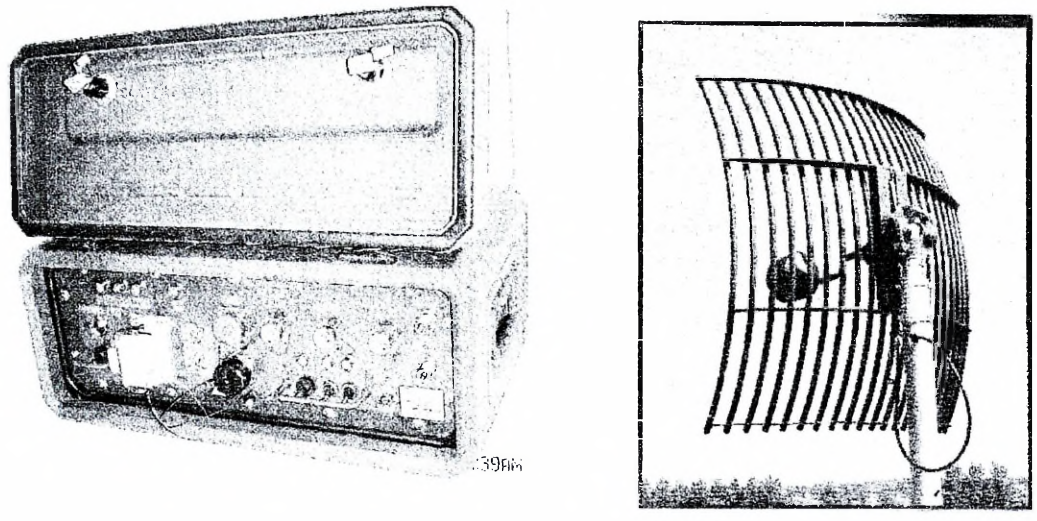
Sieć PST łączności telefonicznej, rozwinięta przy pomocy koncentratora LANTELBOX, pracuje w standardzie ISDN a sieć komputerowa PSK pracuje w standardach Ethernet 10BaseT i 100BaseTx.

Koncentrator LANTELBOX może być rozwijany w polu lub w pomieszczeniach i jest elementem składowym stanowisk dowodzenia opartych o kontenerowe aparatownie komputerowe i polowe centrale telefoniczne zainstalowane na pojazdach lub centrale stacjonarne.
Koncentrator LANTELBOX umożliwia połączenia z aparatami telefonicznymi przy pomocy kabli telefonicznych typu PKL o długości około 300m oraz skrzynek kablowych telefonicznych. Natomiast połączenia z terminalami komputerowymi dokonywane jest przy pomocy Polowych Kabli Skrętkowych typu PKS 2x2x0.34, kategorii 5 o długości 90m. Połączenie typu uplink między koncentratorem a aparatownią dokonywane jest przy pomocy polowego kabla światłowodowego PKŚ CTOS. Ponieważ w kablu PKŚ CTOS znajdują się dwie pary światłowodów, stąd dwa włókna są przeznaczone do transmisji komputerowej Ethernet 10 BaseFL lub Ethernet 100Base Fx a pozostałe dwa włókna są przeznaczone do transmisji sygnałów telefonicznych w standardzie ITU E1. Urządzenie pozwala na radykalne obniżenie czasu potrzebnego na rozwinięcie polowej sieci łączności abonenckiej przez skrócenie długości doprowadzeń abonenckich. Sygnały transmisyjne komputerowe podłączone kablem PKŚ CTOS do aparatowni są dołączone poprzez konwertery optyczne Ethernet do znajdujących się tam serwerów. Sygnały transmisyjne telefoniczne są dołączone poprzez konwertery optyczne pracujące w standardzie E1 do polowej centrali telefonicznej posiadającej wyprowadzony styk standardu E1 (styk V1 lub V5). Koncentrator LANTELBOX pracuje po włączeniu i skonfigurowaniu bezobsługowo.
System telefoniczny koncentratora jest przeznaczony do zastąpienia długiego wieloparowego połączenia centrali polowej z wyniesionymi abonentami przez połączenie kablem światłowodowym i krótkimi doprowadzeniami abonenckimi cyfrowymi ISDN. Urządzenie pozwala na wyniesienie do 30 abonentów ISDN przy pomocy łącza światłowodowego o przepustowości 2048 kbit/s (grupa1). Urządzenie udostępnia do 30 cyfrowych podstawowych dostępów ISDN (2B+D) o standardzie styku U z kodem 2BIQ
(zal. ITU G.961 app. II). Połączenie z centralą telefoniczną odpowiada stykowi V3 lub V5 (preferowane) według zalecenia ITU Q.512 (standard styku cyfrowego pomiędzy centralą telefoniczną a siecią abonencką). W obu przypadkach koncentrator pełni tylko funkcje pomocnicze zaś wszystkie funkcje usługowe są skoncentrowane w centrali. Takie rozwiązanie pozwala na uniknięcie konieczności dodatkowego konfigurowania koncentratora i prostotę konstrukcji.

Przenośny polowy system WLANBOX-BRIDGE 1-2.4, rys.18 jest przeznaczony do szybkiego nawiązywania dwukierunkowej bezprzewodowej transmisji danych w PST typu LAN, rozwijanych w ramach stanowisk dowodzenia. Zalety systemu jakimi jest łatwość i

szybkość uzyskiwania połączeń są widoczne w momencie, gdy trzeba nawiązać łączność komputerową w noworozwijanej sieci PST a długie kable światłowodowe jeszcze nie zostały rozwinięte lub w czasie ich rozwijania trzeba pokonać czasochłonne przeszkody terenowe, takie jak uczęszczane drogi, rzeki itp. W najprostszej konfiguracji mostu system może łączyć między sobą bezprzewodowo koncentrator linii komputerowych LANBOX LB10K-PKS z aparatownią komputerową lub aparatowniami systemu STORCZYK. Może również łączyć między sobą w polu dowolne urządzenia mające wyjścia w standardzie Ethernet 10/100 BaseT, np. dwa komputery, dwa koncentratory, dwie aparatownie. Każdy zespół nadawczo-odbiorczy systemu jest zasilany: z wewnętrznego akumulatora, z sieci prądu zmiennego 220V, lub z napięcia stałego 24V. Zarządzanie pracą zespołu odbywa się poprzez złącze konsoli dostępne na płycie czołowej. System ma wbudowane kryptograficzne systemy zapewniające bezpieczeństwo transmisji. System zapewnia łączność bezprzewodową w standardzie IEEE 802.11b,g w paśmie 2.4GHz z szybkością transmisji cyfrowej od 1 do 54Mb/s w zależności od warunków propagacji. System zapewnia pracę jako: most łącząc dwa punkty, jako punkt dostępowy gdzie kilka terminali jest dołączone bezprzewodowo do jednego punktu lub jako most dla grupy dostępowej. W każdym punkcie musi być rozwinięty zespół nadawczo-odbiorczy ze składaną anteną paraboliczną umieszczaną na składanym maszcie o wysokości 4m. Uzyskiwany zasięg łączności wynosi od 1000m w mokrym lesie do kilku kilometrów na otwartych przestrzeniach, a podwyższanie anten powiększa ten zasięg. Szybkość transmisji cyfrowej zależy od zasięgu i od warunków otoczenia (przeszkód). Zespół nadawczo-odbiorczy jest rozwijany i obsługiwany przez jedną osobę. System z antenami dookólnymi może być stosowany na pojazdach w ruchu. System ma wbudowane mechanizmy Quality of Service umożliwiające transmisję danych, obrazów i głosu.

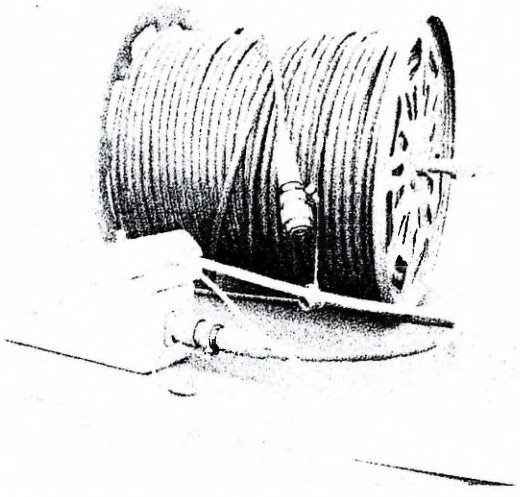
Cały system składa się z dwu zespołów nadawczo-odbiorczych. Kompletny zespół nadawczo-odbiorczy z masztem i składaną anteną paraboliczna jest umieszczony w torbie transportowej o wymiarach 500x600x1500mm. Ciężar całości wynosi około 60kg. Czas pracy z akumulatora wewnętrznego wynosi około 60 minut.



Rysunek 18. Polowy system łączności bezprzewodowej WLANBOX-BRIDGE 1-2.4. ze składaną anteną paraboliczną

Do połączeń PST między systemami są stosowane kable skrętkowe i światłowodowe wraz z osprzętem.

Polowy kabel Skrętkowy typu PKS 2 x 2 x 0.34, rys.19, jest dwuparową skrętką ekranowaną kategorii 5 przeznaczoną do transmisji sygnałów cyfrowych z szybkością do 100Mb/s. Miedziany ekran chroni kabel przed wpływem zakłóceń elektromagnetycznych i zapewnia poprawność transmisji sygnałów. Dodatkowy oplot ze strun fortepianowych zapewnia dużą odporność kabla na zrywanie dający dopuszczalną siłę naciągu kabla do 1200N. Konstrukcja kabla zapewnia możliwość jego wielokrotnego zwijania i rozwijania, podwieszanie na podporach oraz pokonywanie nim przeszkód wodnych o głębokości do 10m. Kabel na obu końcach jest zakończony kroploszczelnymi wtykami wielostykowymi (zgodnie ze standardem MIL-26482) z kapturkami zabezpieczającymi. Miejsce połączenia złącza z kablem jest dodatkowo uszczelnione kształtką termokurczliwą. Dołączanie terminali końcowych wyposażonych w gniazda niezgodne ze złączami kabla może być dokonane poprzez moduł zabezpieczająco-dopasowujący SKE.



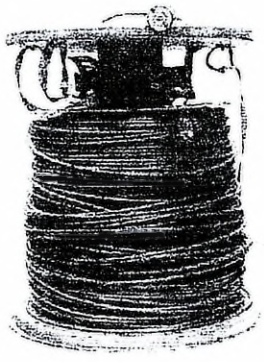
Rysunek 19. Polowy kabel skrętkowy PKS 2x2x0.34 na bębnie PKL

Podstawowe dane techniczne:

1. Kategoria kabla	5
2. Długość	90m
3. Impedancja falowa	100Ω ±15Ω
4. Dopuszczalne napięcie pracy	500V
5. Temperatura pracy	-50°C ÷ +70°C
6. Średnica zewnętrzna kabla	8.5mm ± 1mm
7. Waga kabla na bębnie PKL-2	12kg (150m), 8kg (90m)

Polowy kabel światłowodowy CTOS (PKŚ CTOS), rys.20, wykorzystywany jest w sieciach łączności wchodzących w skład stanowisk dowodzenia szczebla taktyczno-operacyjnego.

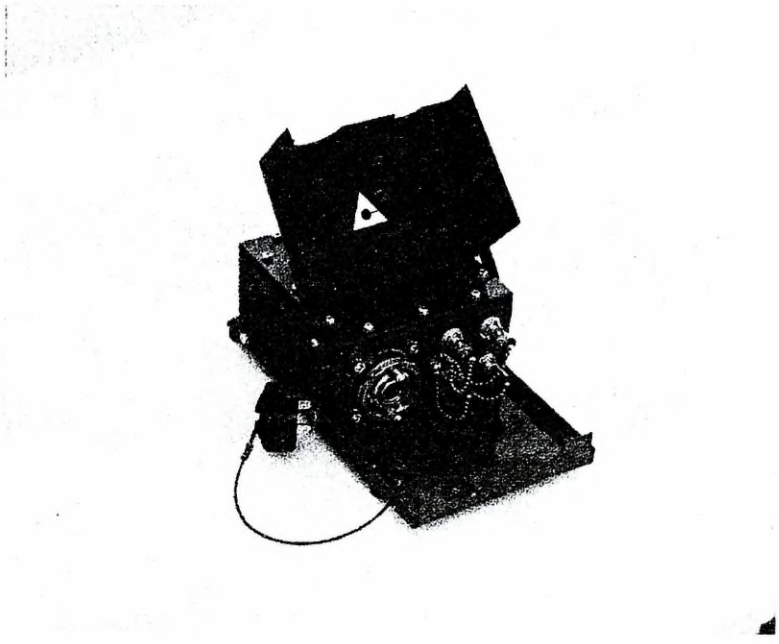
Zadaniem PKŚ CTOS jest transmisja sygnałów optycznych pomiędzy różnego rodzaju aparatowniami i koncentratorami wojskowymi zawierającymi elementy funkcjonalno-techniczne lokalnych sieci komputerowych. PKŚ CTOS jest przystosowany do częstego i wielokrotnego zwijania i rozwijania w warunkach pola walki. Posiada tłumienność 1,3dB/km dla fali 130nm a szerokość pasma przenoszenia wynosi 500MHz/km.



Rysunek .20. Polowy kabel Światłowodowy PKŚ CTOS ze złączami hemafrodycznymi CTOS

PKŚ CTOS umożliwia:

1. Transmisję sygnału optycznego przez czterowłókna światłowodowe wielomodowe w warunkach polowych pomiędzy aparatowniami na pojazdach, wynośnymi koncentratorami, aparatowniami stacjonarnymi zawierającymi elementy funkcjonalno-techniczne lokalnych sieci komputerowych na odległość 800m
2. Mechaniczne bądź ręczne wielokrotne zwijanie i rozwijanie Polowego Kabla Światłowodowego CTOS na bębnie o promieniu krzywizny co najmniej 80mm i prace w zakresie temperatur od -40°C do +70°C.
3. Hermafrodytyczność złącz CTOS - możliwe jest bezpośrednie, wielokrotne dokonywanie łączenia (bez użycia elementów pośredniczących) kilku PKŚ CTOS ze sobą w celu otrzymania toru transmisyjnego o długości większej niż długość jednego PKŚ CTOS
4. Poprzez dodatkowy adapter AD-CTOS, rys.21, możliwe jest bezpośrednie połączenie przez PKŚ CTOS odległych serwerów nie posiadających zainstalowanych złącz naburtowych typu CTOS a tylko standardowe złącza np. typu ST lub SC.

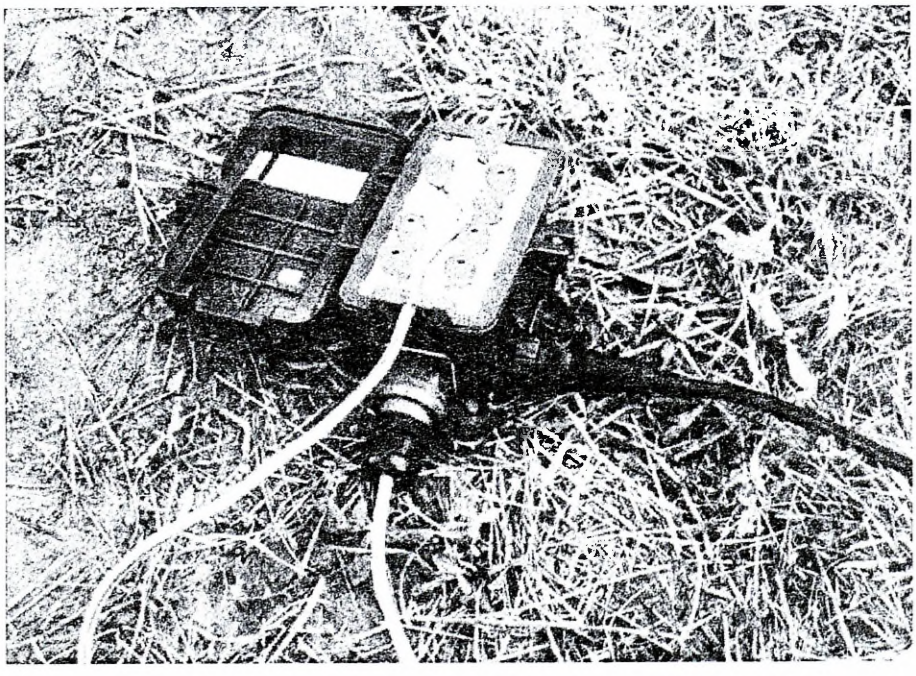


Rysunek 21. Adapter AD-CTOS służący do dołączania układów ze złączami standardowymi typu ST do kabla PKŚ CTOS

Układ zabezpieczająco-dopasowujący SKE, rys.22 służy do przyłączania różnego rodzaju urządzeń i terminali komputerowych do polowego kabla skrętkowego typu PKS 2x2x0,34.

Układ SKE jest metalowym pudełkiem z przykrywką odpornym na narażenia mechaniczne. Na ścianie bocznej znajduje się złącze do przyłączania kabla polowego oraz złącze typu RJ-45 w wersji wojskowej. Gdy współpracujące urządzenie jest wyposażone w złącze RJ-45 to można wtedy dokonać bezpośredniego połączenia z SKE. Natomiast gdy urządzenia wyposażone są w inne złącza bądź terminale, to ich połączenie z SKE dokonuje się przez dołączenie poszczególnych przewodów do indywidualnie wprowadzonych i opisanych zacisków odpowiadających przewodom poszczególnych par skrętek kabla polowego. Dostęp do tych zacisków jest możliwy po otwarciu pokrywki układu. Układ SKE może przenosić sygnały analogowe i cyfrowe (Ethernet 100BaseTx). Zastosowanie układu SKE jest szczególnie wskazane w przypadku stosowania kabli ze złączami typu RJ45, które w warunkach polowych łatwo ulegają zniszczeniu. Wtedy wymiana krótkiego odcinka kabla z uszkodzonym złączem RJ45 łączącego terminal z układem SKE jest szybka i łatwa. Wyprowadzony jest też zacisk ekranu kabla polowego do którego można dołączyć ekran kabla przyłączanego. Ponadto układ SKE ma wbudowany wewnętrzny układ zabezpieczeń przeciwprzepięciowych o dużej szybkości działania, zabezpieczający każdą parę skrętkową. Prąd pochodzący z wyładowań odprowa-

dzany jest poprzez zacisk uziemiający, przewód ochronny i wbijany uziom do ziemi. Układ jest odporny na wyładowania pierwotne i wtórne o wartości prądu do 20kA, 8/20μs. Układ ogranicza napięcia wyjściowe do wartości bezpiecznej dla obwodów wejściowych urządzeń informatycznych. Dodatkowo SKE zawiera układ wyrównywania potencjałów powstających wskutek wyładowań w obszarze, gdzie rozwinięta jest sieć rozległa. Dzięki temu zabezpiecza się urządzenia i osoby obsługujące przed porażeniami, wywołanymi wzrostem potencjału ziemi, wywołanych wyładowaniem w jednym końcu kabla i przeniesionych przez przewodzący ekran do drugiego końca kabla.



Rysunek 22. Układ zabezpieczająco-dopasowujacy SKE

Do obsługi i zarządzania polowym sprzętem informatycznym na SD Radiotechnika Marketing opracowała specjalistyczne oprogramowanie, które ułatwia i porządkuje pracę osób na SD. Oprogramowanie to zapewnia administratorowi SD pełną kontrolę i monitorowanie pracy systemów. Zautomatyzowana została instalacja i uruchamianie programów przy jednocześnie minimalnym zaangażowaniu administratora. Oprogramowanie obejmuje następujące procesy niezbędne do zapewnienia nadzoru nad działaniem PST na SD:

- monitorowanie serwera
- monitorowanie serwera pocztowego
- monitorowanie usługi Acive Directory

- monitorowanie stanu sieci:
    - pojawienie się nowych stacji
    - monitorowanie interfejsów routerów i przełączników
    - monitorowanie łączy
- procedury działań w sytuacjach awarii PST.

Przedstawiony w artykule opis technologii i przykładowych rozwiązań sprzętu informatycznego do budowy PST pozwala na dokonywanie ocen i selekcji urządzeń do zastosowań na SD. Rozwiązania te i technologie są zbieżne z tendencjami rozwoju sprzętu w NATO. Ich parametry techniczno-taktyczne pozwalają na ich zastosowanie do systemów o bardzo wysokich wymaganiach jak i do prostszych na najniższych szczeblach dowodzenia.

Wykorzystanie oprogramowania Open Source w systemach teleinformatycznych stanowisk dowodzenia wojsk lądowych szczebla taktycznego w aspekcie koncepcji wojny sieciocentrycznej

inż. Michał GRZYBEK
Instytut Łączności

1. Cyfryzacja współczesnego pola walki

Współcześnie rozwijane koncepcje walki zbrojnej opierają się na tworzeniu wielowymiarowej i wieloczynnikowej przewagi militarnej własnych sił zbrojnych w oparciu o kontrolowaną stosownie do własnych możliwości technicznych przewagę informacyjną (*ang. information superiority*), jak również technologiczną (*ang. technological superiority*). Wymienione czynniki mają decydujący wpływ na powodzenie prowadzonych działań zbrojnych, również przez formacje Wojsk Lądowych, także na szczeblu taktycznym [20].

Wykorzystanie nowoczesnych technologii informatycznych ma zapewnić uzyskanie przewagi informacyjnej i zjawiska wyprzedzenia informacyjnego względem potencjału informacyjnego i wiedzy przeciwnika, dającą możliwość przewidywania i przeciwdziałania zamierzeniom przeciwnika. Dlatego też, między innymi na potrzeby Wojsk Lądowych, dynamicznie rozwijane są systemy klasy C4I2 (*ang. Command, Control, Communication, Computer, Intelligence and Information*), systemy wspomagania dowodzenia C2IS (*ang. Command, Control and Information System*), systemy pozwalające na pozyskiwanie i przetwarzanie informacji rozpoznawczych z sieci sensorów C4ISR (*ang. Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance*) oraz inne zautomatyzowane systemy dowodzenia i kierowania środkami walki [8].

W systemie obronnym RP Wojska Lądowe stanowią istotny element polskich Sił Zbrojnych. Podstawowym zadaniem Wojsk Lądowych jest zapewnienie obrony RP w przypadku zagrożenia kraju ewentualnym atakiem lądowo-powietrznym lub innymi formami zagrożeń militarnych, jak też reakcji na zagrożenia powstające w czasie pokoju.

Wojska Lądowe składają się z jednostek organizacyjnych Wojsk Operacyjnych, Wojsk Obrony Terytorialnej oraz jednostek i instytucji porządkowych. Wszystkie te jednostki podlegają Dowództwu Wojsk Lądowych. Wojska operacyjne przygotowane są i mogą prowadzić działania bojowe na różnych teatrach działań wojennych, z czego wytypowane jednostki mogą zostać podporządkowane Dowództwu NATO. Wojska Obrony Terytorialnej pozostają

podporządkowane dowództwu narodowemu. Wojska te są przeznaczone do prowadzenia działań na obszarze własnego państwa.

Wojska Obrony Terytorialnej są przeznaczone do realizacji zadań o charakterze operacyjnym, zabezpieczającym i ratowniczym w przypadku zaistnienia katastrof i klęsk żywiołowych [5]. Struktura organizacyjna Wojsk Lądowych opiera się na dywizjach i brygadach oraz zawiera różne rodzaje wojsk w tym wojska: pancerne i zmechanizowane, aeromobilne, rakietowe i artylerii, obrony przeciwlotniczej, inżynieryjne, chemiczne, łączności i informatyki, ponadto oddziały i pododdziały rozpoznania i walki elektronicznej, działań psychologicznych i działań specjalnych a także logistyki.

W celu dowodzenia podległymi siłami Wojsk Lądowych, jak również kierowania środkami walki, na szczeblu taktycznym organizuje się określoną strukturę stanowisk dowodzenia. Struktura taka jest odpowiednio przystosowana do określonego szczebla taktycznego oraz sposobu rozmieszczenia wojsk. W zależności od szczebla taktycznego w systemie dowodzenia mogą być tworzone następujące stanowiska dowodzenia: główne stanowisko dowodzenia (GSD), tyłowe stanowisko dowodzenia (TSD), punkt dowódczo-obserwacyjny (PDO) [4].

Struktura systemu stanowisk dowodzenia pododdziałów, oddziałów, jak i związków taktycznych Wojsk Lądowych, powiązana jest wzajemnymi relacjami o dużym stopniu złożoności w przestrzeni systemu informacyjnego. W systemie dowodzenia muszą istnieć niezawodne, bezpieczne i wydajne kanały informacyjne. Kanał informacyjny według teorii informacji stanowi element łączący nadawcę z odbiorcą.

Natomiast w bardziej złożonych systemach, kanały informacyjne łączą poszczególne złożone funkcjonalnie węzły informacyjne. Istnieją w systemie informacyjnym systemu stanowisk dowodzenia relacje zewnętrzne łączące poszczególne stanowiska dowodzenia. Pionowe kanały informacyjne łączą kolejno poszczególne węzły informacyjne stanowisk dowodzenia następujących po sobie szczebli taktycznych. Poziome kanały informacyjne funkcjonują w celu wymiany danych pomiędzy węzłami informacyjnymi stanowisk dowodzenia tego samego szczebla. Kanały informacyjne tego typu zapewniają możliwości koordynacji dowodzenia i współdziałania w czasie realizacji wspólnych działań [22]. W strukturze organizacyjnej węzła informacyjnego stanowiska dowodzenia szczebla taktycznego, istnieją również wewnętrzne więzi informacyjne. Łączą one w relacjach dowodzenia, koordynowania, synchronizowania, jak też współdziałania wyspecjalizowane funkcjonalnie poszczególne komórki organizacyjne stanowiska dowodzenia [1].

Dynamika współczesnego pola walki wymaga przekazywania w czasie rzeczywistym dużych zbiorów danych. Dlatego też, istnieje konieczność wykorzystania nowoczesnych systemów łączności elektronicznej w tym teleinformatycznych, zapewniających automatyczne sterowanie strumieniami informacyjnymi w sposób wysoce niezawodny i bezpieczny [21]. Ponadto systemy takie powinny wykorzystywać kompatybilne interfejsy sieciowe oraz jednakowe formaty wymiany informacji taktycznych w celu integracji różnych platform sprzętowo-programowych. Strukturę strumieni informacyjnych systemu stanowisk dowodzenia należy rozpatrywać w aspekcie funkcjonowania systemu łączności. W systemie dowodzenia na szczeblu taktycznym kanały informacyjne zapewniane są przez techniczne środki dowodzenia a w tym poprzez łącza: kablowe, światłowodowe, radiowe, radioliniowe, w razie potrzeby również przez łącza satelitarne [3].

Faktem jest, iż postęp technologiczny, informatyzacja współczesnego pola walki oraz rozwój nauk w zakresie zarządzania w sposób zasadniczy wpływają na dynamiczny rozwój koncepcji organizacji systemów dowodzenia. Zachodzące procesy mają również wpływ na zasady funkcjonowania stanowisk dowodzenia, jak również poszczególnych komórek organizacyjnych stanowiska dowodzenia. Jedną ze współcześnie rozwijanych koncepcji jest doktryna wojny sieciocentrycznej NCW (*ang. Network Centric Warfare*).

2. Doktryna wojny sieciocentrycznej

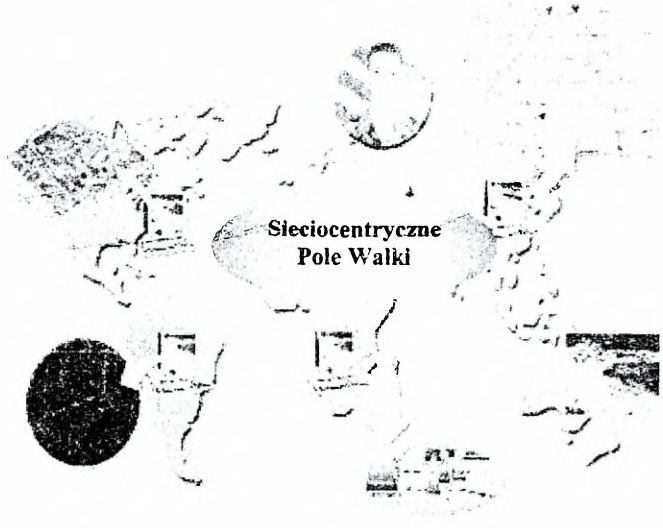
Doktryna wojny sieciocentrycznej jest jednym z elementów amerykańskiej rewolucji dotyczącej przewidywanych zmian w siłach zbrojnych w zakresie RMA (*ang. Revolution in Military Affairs*). Autorem tej doktryny jest wiceadmirał Arthur Cebrowski, kieruje on w Pentagonie Biurem Transformacji Sił Zbrojnych. Nad tą koncepcją pracuje wraz ze współpracownikami od 1995 r. Autor doktryny zakłada, że poprzez wykorzystanie założeń koncepcji NCW wojsko ma zostać lepiej przystosowane do wyzwań współczesnej wojny.

Doktryna NCW wskazuje na fakt, że współczesne konflikty zbrojne coraz bardziej swoim charakterem odbiegają od znanych w historii klasycznych form walki zbrojnej. Współczesne wojny mają często charakter asymetryczny. Walka prowadzona jest nie tylko z wojskiem wrogiego państwa, ale z ugrupowaniami terrorystycznymi i formacjami prowadzącymi działania partyzanckie, często w dużym rozproszeniu bez potrzeby centralnej koordynacji działań. Ponadto dotychczasowa hierarchiczna organizacja sił zbrojnych, złożona z

dużych oddziałów wyposażonych w ciężki sprzęt bojowy, sprawdza się zdaniem twórców koncepcji NCW coraz gorzej w aspekcie specyfiki współczesnych konfliktów zbrojnych [12].

Wdrożenie koncepcji NCW ma pozwolić na zwiększenie zdolności bojowej poprzez umiejętne wykorzystanie współdzielonej informacji, która stanowi obecnie nowy wymiar walki na współczesnym polu walki. Przewaga informacyjna zwiększa skuteczność podejmowanych działań zbrojnych. Powyższe fakty wpływają na nowe podejście do organizacji i współdziałania struktury systemu stanowisk dowodzenia oraz sposobu funkcjonowania poszczególnych komórek organizacyjnych stanowisk dowodzenia [12].

Doktryna NCW zakłada, że działania sieciocentryczne w tym prowadzone przez Wojska Lądowe możliwe są w sytuacji, kiedy istnieje rozległa, wydajna i bezpieczna infrastruktura teleinformatyczna. Cyfrowe systemy łączności oraz technologie dostępowe, mają zapewnić dołączenie do sieci wszystkich elementów współdziałających sił zbrojnych a przede wszystkim stanowisk dowodzenia. Elementy systemu walki sieciocentrycznej przedstawia rysunek nr 1.



Rysunek 1. Elementy systemu walki sieciocentycznej
Źródło: www.dharbor.com/solutions/ncw.html

W doktrynie NCW zakłada się istnienie trzech głównych domen oraz poddomen. Prowadzenie działań zbrojnych realizowane jest jednocześnie w trzech domenach. Wyróżnia się domeny: fizyczną, informacyjną oraz domenę decydowania.

Domena fizyczna jest taką domeną, w której podejmowane są działania tradycyjne oraz znajdują się w niej obiekty istniejące realnie - fizycznie. W przestrzeni tej domeny mieszczą się działania klasyczne podejmowane przez walczące siły a więc: uderzenia, obrona i manewr

realizowane we wszystkich wymiarach a mianowicie: lądowym, morskim, powietrznym oraz kosmicznym [23].

W domenie tej znajduje się cały potencjał zasobów wykorzystywanych w walce zbrojnej w tym stanowiska dowodzenia oraz nowoczesne inteligentne systemy uzbrojenia (*ang. Smart Weapons*). W domenie fizycznej funkcjonują systemy walki elektronicznej EW (*ang. Electronic Warfare*), których zadaniem jest rozpoznawanie źródeł emisji elektromagnetycznej oraz niszczenie i dezorganizacja systemów elektronicznych przeciwnika [6]. Domena fizyczna to również systemy łączności elektronicznej tworzące sieci wymiany informacji taktycznych pomiędzy węzłami informacyjnymi stanowisk dowodzenia.

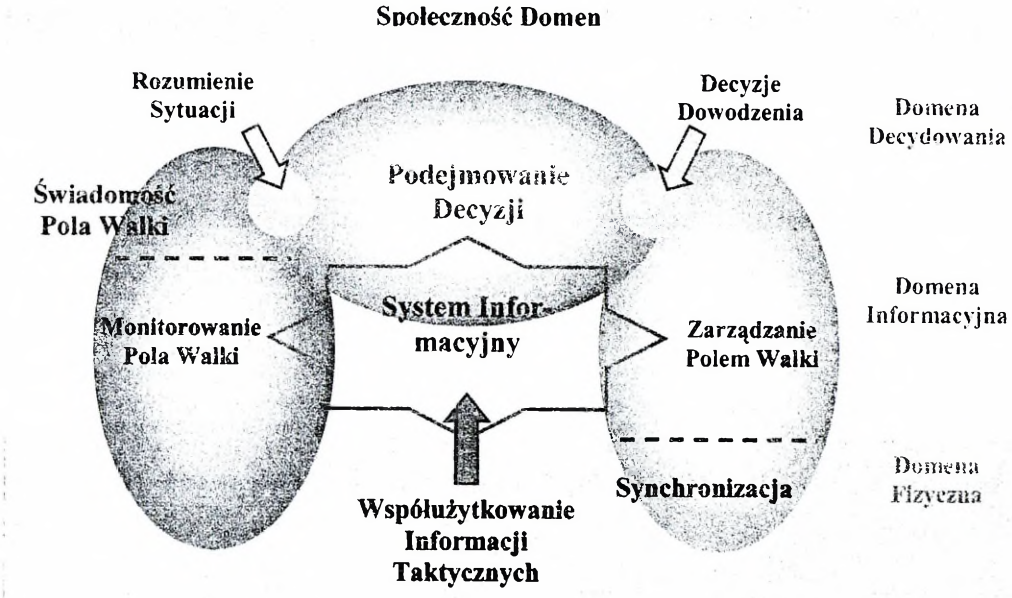
W domenie fizycznej zachodzi zjawisko synchronizacji działań, współdziałania oraz synergii wykorzystanych środków walki. Zasoby domeny fizycznej są łatwo przeliczalne. Posługując się znanymi tradycyjnymi metodami można je łatwo klasyfikować oraz oceniać ich wartość bojową [23].

Domena informacyjna zgodnie z założeniami doktryny opracowanej przez Departament Obrony USA DoD (*ang. Department of Defense*), dotyczącej prowadzenia operacji informacyjnych IO (*ang. Information Operations*), domena ta jest przestrzenią walki o przewagę informacyjną [11]. W domenie informacyjnej wszelkie informacje taktyczne są wytwarzane, przechowywane, przetwarzane i współużytkowane. W domenie tej zachodzą zjawiska analizy danych, generalizacji danych, fuzji oraz graficznego wielowarstwowego zobrazowania informacji taktycznych. W tej przestrzeni usługi swoje świadczą hurtownie danych oraz systemy wspomagania decyzji. W domenie informacyjnej zachodzi zjawisko wymiany potencjału informacyjnego pomiędzy elementami biorącymi udział w walce. W domenie tej mieści się struktura taktycznych strumieni informacyjnych łącząca stanowiska dowodzenia oraz wewnętrzne węzły informacyjne poszczególnych komórek organizacyjnych stanowisk dowodzenia.

Warto zwrócić uwagę na fakt, że w domenie informacyjnej realizowany jest proces monitorowania i zarządzania polem walki. Domena informacyjna to przestrzeń cybernetycznego pola walki (*ang. Cyber Warfare*), w której na kształtowanie przewagi informacyjnej mają wpływ wirusy komputerowe, konie trojańskie, robaki komputerowe, bomby logiczne oraz informatycy prowadzący walkę dywersyjną w zasobach informacyjnych przeciwnika. W domenie informacyjnej musi być zagwarantowany proces ochrony wszelkich zbiorów danych, jak też rożnych postaci informacji o rzeczywistym stanie sił własnych, lokalizacji, i zamiarach działań. Domena ta musi być chroniona w sposób wystarczający przed systemami rozpoznania przeciwnika. Ponieważ stanowi główny potencjał mający wpływ na wzrost zdolności bo-

jowych oraz zdobywanie przewagi informacyjnej wobec przeciwnika prowadzącego analogiczne działania [24].

Domena decydowania to domena, w której jest miejsce na indywidualizm i wspólnotę ludzkich umysłów. W domenie tej znajdują się zdolności przewodzenia poszczególnych dowódców, ich wiedza i doświadczenie oraz umiejętności. Ponadto w domenie decydowania znajdują się takie atrybuty jak: poziom wyszkolenia i doświadczenie w walce, morale żołnierzy, umiejętność współpracy, świadomość sytuacji pola walki. Ponadto indywidualne cechy osobowości uczestników walki [12]. Atrybuty, które znajdują się w tej domenie są szczególnie trudne do oceny. Każda elementarna cześć tej domeny zamknięta jest w umyśle indywidualnego człowieka, z czego każdy jest istotą niepowtarzalną [23]. Domeny oraz zachodzące w nich procesy przedstawia rysunek nr 2.



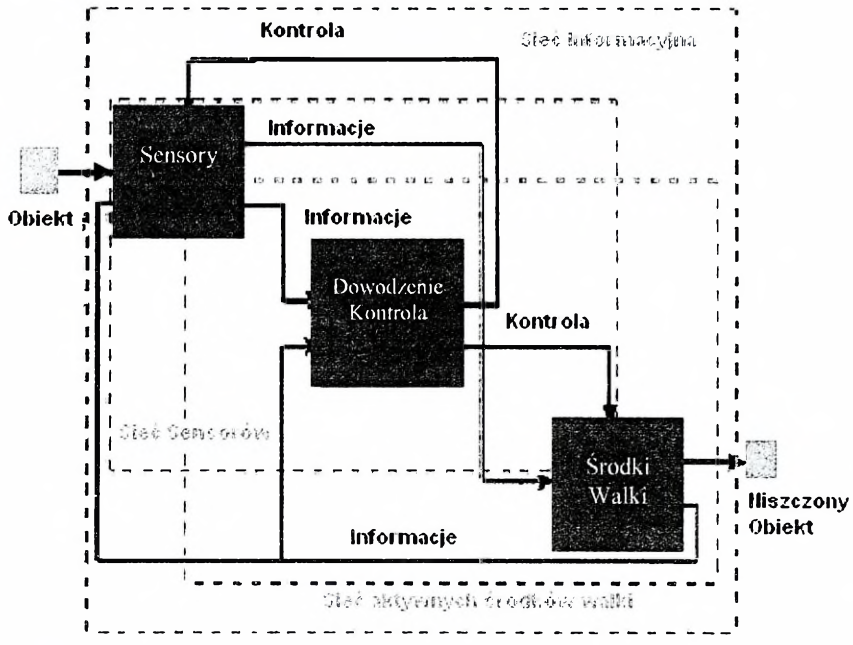
Rysunek 2.– Domeny w doktrynie wojny sieciocentrycznej
Źródło: Opracowanie własne na podstawie www.afrlhorizons.com

W domenie fizycznej, według doktryny NCW formacje Wojsk Lądowych prowadzące taktyczne działania sieciocentryczne są włączone w sieć wymiany informacji taktycznych poprzez wykorzystanie technicznych środków dowodzenia. Platformę transportową stanowi infrastruktura telekomunikacyjna. Zapewnia ona dużą mobilność, żywotność systemu, ponadto skrytość i wierność oraz terminowość przesyłanych informacji [2]. Infrastruktura telekomunikacyjna ma zapewnić w sposób bezpieczny i wydajny, pokrycie niezbędnych więzi informacyjnych pomiędzy stanowiskami dowodzenia i ich elementami, sensorami oraz podległymi siłami i aktywnymi środkami rażenia [12].

W domenie informacyjnej, walczące formacje Wojsk Lądowych posiadają zdolność do współużytkowania informacji taktycznej, dystrybucji informacji pomiędzy węzłami informacyjnymi stanowisk dowodzenia a szczególnie zapewnienia jej ochrony. Ponadto poszczególne stanowiska dowodzenia oraz jednocześnie poszczególne komórki organizacyjne stanowisk dowodzenia, osiągają stan umożliwiający uzyskanie i utrzymanie niezbędnej przewagi informacyjnej [12]. Zdolność do współdziałania stanowisk dowodzenia oraz ich elementów w domenie informacyjnej, pozwala na zwiększanie potencjału informacyjnego o siłach własnych i przeciwniku. Zdolność tą uzyskuje się poprzez zachodzące procesy: analizy, generalizacji, korelacji oraz fuzji informacji [23].

W domenie decydowania, zaangażowane w działania formacje Wojsk Lądowych są zdolne do uzyskiwania wysokiego poziomu świadomości zmieniającej się sytuacji w przestrzeni pola walki oraz jej współużytkowania. Ponadto formacje takie są zdolne do uzyskiwania i współużytkowania wiedzy o zamiarach i intencjach dowódcy, jak też wiedzy o poczynaniach przeciwnika. Jednocześnie zapewniając sobie zdolność do prognozowania przyszłych wydarzeń. Taki stan rzeczy umożliwia zaistnienie procesu samosynchronizowania prowadzonych działań taktycznych przez formacje Wojsk Lądowych, stosownie do dynamicznie zmieniającej się sytuacji na polu walki. Proces samosynchronizacji, stanowi jedną z istotniejszych cech omawianej doktryny. Ponieważ wskazuje na zwiększenie skuteczności prowadzonych działań wynikającą z zachodzących procesów informacyjnych a przede wszystkim współdzielenia informacji taktycznych. Proces kształtowania wspólnej świadomości pola walki, dzięki zaawansowanym systemom informatycznym i wydajnym kanałom informacyjnym może być realizowany w czasie zbliżonym do rzeczywistego [12].

Globalna Sieć Informacyjna GIG (*ang. Global Information Grid*), stanowić ma fizyczną platformę telekomunikacyjną zapewniającą realne funkcjonowanie koncepcji wojny sieciocentrycznej. W systemach sieciocentrycznych wyróżnić można trzy klasy wzajemnie powiązanych relacjami i współdziałających podsieci: sieci środków rozpoznania określaną mianem sieci sensorów -Sensor Grid, sieci systemu stanowisk dowodzenia -C2 Grid i sieci systemów uzbrojenia, w której funkcjonują aktywne środki walki -Shooter Grid. Istnieje konieczność połączenia tych trzech podsystemów w jeden sprawnie funkcjonujący mechanizm [12]. Zależności pomiędzy podsystemami Globalnej Sieci Informacyjnej GIG przedstawia rysunek nr 3.



Rysunek 3. Zależności pomiędzy podsystemami Globalnej Sieci Informacyjnej GIG
Źródło: opracowanie własne na podstawie:www.usni.org/Proceedings/Articles98/PROcebrowski.htm

Tak zorganizowany system jest w stanie świadczyć usługi na potrzeby stanowisk dowodzenia Wojsk Lądowych szczebla taktycznego oraz dla poszczególnych komórek organizacyjnych stanowisk dowodzenia. Do takich usług zaliczyć można dystrybucję taktycznego strumienia informacyjnego, współdzielenie informacji taktycznej pomiędzy stanowiskami dowodzenia. Ponadto dostęp do informacji rozpoznawczej. Automatyczne przekazywanie zadań do aktywnych środków walki. A co najważniejsze kształtowanie wspólnej świadomości pola walki, gdzie realizacja tego procesu powinna być gwarantowana w czasie zbliżonym do rzeczywistego. Usługi realizowane w sieci pozwolą na szybkie identyfikowanie obiektów, podejmowanie decyzji i niszczenie celów przeciwnika. Poprzez integrację tych podsystemów można osiągnąć wysoką efektywność i skuteczność podejmowanych działań przez stanowiska dowodzenia Wojsk Lądowych i ich funkcyjny personel. Dlatego też należy podkreślić fakt, że efektywność walki sieciocentrycznej jest możliwa dzięki procesowi synergii, będącej efektem współużytkowania informacji taktycznej we wspólnym środowisku operacyjnym i teleinformatycznym [23].

Istotną informacją jest fakt, że NCW nie stanowi jedynie doktryny wojskowej definiującej sposób prowadzenia działań zbrojnych.

Jest przede wszystkim koncepcją konkretnego systemu zbudowanego na określonej infrastrukturze telekomunikacyjnej oraz teleinformatycznej, wzajemnie powiązanych ze sobą podsystemów w jeden globalny mega system.

Na potrzeby sił zbrojnych USA zgodnie z założeniami doktryny NCW budowane są nowoczesne sieci telekomunikacyjne i teleinformatyczne. Jedną z podstawowych platform transportowych w zakresie wymiany informacji taktycznych na potrzeby U.S. Army stanowić ma sieć WIN-T (*ang. Warfighter Information Network – Tactical*). Program budowy tego systemu realizowany jest przez U.S. Army Communications and Electronics Command, General Dynamics C4 Systems oraz Lockheed Martin. Budowa systemu sieci WIN-T związana jest również z wykorzystaniem tego systemu na potrzeby programu organizacji przyszłościowego pola walki FCE (*ang. Future Combat System*). Ponadto stanowi platformę dostępową dla systemów JTRS (*ang. Joint Tactical Radio System*). Architektura sieci WIN-T, zapewnić ma możliwość przesyłania transmisji multimedialnych w czasie zbliżonym do rzeczywistego. W systemie tym w celu adresowania elementów sieci wykorzystywany jest protokół IP w wersji 6. Ponadto w celu transmisji głosu znajduje zastosowanie technologia VoIP (*ang. Voice over IP*). Integralną część systemu WIN-T stanowią wojskowe systemy telekomunikacyjne. Ponadto w celu budowy tego systemu mają zostać wykorzystane systemy satelitarne nowej generacji, a także systemy komórkowe trzeciej generacji. Wykorzystanie usług sieci WIN-T na stanowisku dowodzenia przedstawia rysunek nr 4.



Rysunek 4. Usługi sieci WIN-T na stanowisku dowodzenia
Źródło: www.win-t.com

Wirtualne sieciowe stanowiska dowodzenia, oraz ich implementacja stanowi integralną i jednocześnie bardzo ważną część doktryny NCW. Pozwalają one na rewolucyjne podejście do organizacji procesu dowodzenia. Ponieważ w przypadku koncepcji NCW definiowany jest sieciocentryczny proces dowodzenia. Ponadto w tego typu procesie dowodzenia przydatne są struktury dowodzenia częściowo lub całkowicie zdecentralizowane [12].

Natomiast należy zwrócić uwagę, że obecnie w organizacji systemów dowodzenia Wojsk Lądowych przeważają struktury charakteryzujące się pełną centralizacją lub częściowo zcentralizowane. Budowa wirtualnych sieciowych stanowisk dowodzenia pozwala w zależności od istniejącej sytuacji pola walki na budowę przyrostowej i zmieniającej się w czasie struktury dowodzenia. Architektura wirtualnej struktury systemu dowodzenia zależy przede wszystkim, od realizowanych zadań bojowych i celów. Wirtualna struktura dowodzenia jest tworzona z istniejących fizycznie zasobów informacyjnych w tym stanowisk dowodzenia. Jednak na czas realizacji określonych zadań jest połączona wirtualnie tworzonymi więziami informacyjnymi poprzez systemy teleinformatyczne. Po zakończeniu realizacji określonych zadań siły i środki mogą być wykorzystane do realizacji innych zadań. Takie działania mają na celu wykorzystanie jak największej ilość dostępnej informacji taktycznej, wykorzystania wspólnej świadomość pola walki, przydzielania i wykorzystywania dostępnych aktywnych środków walki. Koncepcja wirtualnych struktur dowodzenia nie jest wytworem teoretycznym, ale jest próbą przeniesienia zasad funkcjonowania wirtualnych organizacji gospodarczych w środowisko współczesnego pola walki [12].

Duże korporacje finansowe od wielu lat wykorzystują wirtualne struktury zarządzania, które w optymalny sposób skupiają niezbędne zasoby osobowe i procesy dążąc do osiągnięcia określonych celów wytwórczych, badawczych i zysków finansowych.

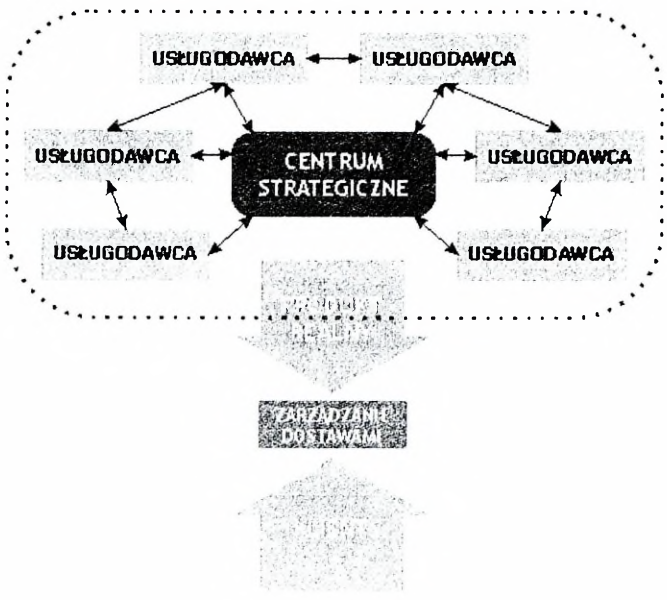
Jednocześnie wykorzystują najnowsze osiągnięcia techniki w wirtualnych strukturach zarządzania do skutecznej walki z konkurencją. Powstanie organizacji wirtualnych nie było rewolucją. Był to wynik ewolucji oraz pojawiania się coraz to nowych wymagań rynku i nowoczesnych technologii informatycznych. Organizacje takie stały się coraz bardziej elastyczne, rozproszone, skuteczne i zorientowane na zadania.

Decydujący wpływ na dynamikę zmian w przedsiębiorstwach miał rozwój Internetu oraz usług WWW. Postęp technologiczny w sposób rewolucyjny zmienił przepływ informacji i sprawił, że informacja nabrała strategicznego charakteru. Takie zjawiska jak: aktualność udostępnianej informacji, możliwość modyfikacji danych oraz rozprzestrzeniania ich na cały świat, bardzo szybka propagacja informacji, możliwość dystrybucji informacji o dowolnie zdefiniowanej szczegółowości, brak radykalnych ograniczeń wielkości informacji, przyja-

zność informacji i jej multimedialność, decydowały o powodzeniu działalności gospodarczej i osiąganiu zamierzonych celów przez organizacje wirtualne. Organizacje takie posiadają zdolność do zarządzania równoległego, które obejmuje: planowanie, zarządzanie, synchronizację procesów i informacji, łączenie informacji, motywowanie i ocenę podejmowanych działań. We wszystkich wirtualnych organizacjach gospodarczych występuje wspólny wątek wirtualności. Może on akcentować różne wymiary współpracy wirtualnej. Przestrzeń, w której elementy organizacji wirtualnych są ulokowane w dowolnych miejscach Ziemi. Czas, ponieważ organizacje wirtualne charakteryzują się tymczasowością, są to organizacje nastawione na realizację określonych zadań. Organizacje wirtualne posiadają rozproszone struktury. Wiedza organizacji wirtualnych jest głównym czynnikiem, który łączy organizacje wirtualne. Następuje proces wzajemnego uzupełniania się wiedzy i kompetencji partnerów. Ponadto proces absorbcji i przetwarzania wcześniej posiadanej wiedzy prowadzi do powstania nowej wiedzy.

Organizacje wirtualne charakteryzują ponadto różne atrybuty: Cyberprzestrzeń, to przestrzeń zlokalizowana w Internecie, w której funkcjonują organizacje wirtualne. Cyberwiedza, wynikającą z prostoty nawiązywania i utrzymywania kontaktów z obiektami posiadającymi rzadką i specjalistyczną wiedzę. Cyberczas, który biegnie szybciej niż normalny czas ze względu na bardzo szybki postęp technologiczny oraz możliwość funkcjonowania w trybie 24 godzinnym poprzez wykorzystanie różnic stref czasowych. Organizacje wirtualne posiadają swoje centra gdzie podejmuje się decyzje strategiczne, rozdziela zadania pomiędzy poszczególnych usługodawców, nadzoruje procesy powstawania produktu realnego, osiągania zamierzonych celów.

Zupełnie nowym wymogiem pojawiającym się w gospodarczych organizacjach wirtualnych, w sytuacji gdzie każdy zajmuje się tylko znikomo małym wycinkiem całości, jest konieczność zachowania spójnego obrazu całości podejmowanych działań (*ang. big picture*). Obraz ten pozwala w przypadku pojawienia się trudności na szybkie podejmowanie decyzji kierujących prace we właściwym kierunku. Big Picture w organizacjach wirtualnych ma takie same znaczenie jak wspólna świadomość pola walki w doktrynie wojny sieciocentrycznej. Doktryna NCW nie bez podstaw próbuje wdrażać sprawdzone mechanizmy funkcjonowania organizacji wirtualnych w środowisko systemu dowodzenia oraz praktyczną implementację wirtualnych stanowisk dowodzenia [12]. Zasady współpracy elementów organizacji wirtualnej przedstawia rysunek nr 5.

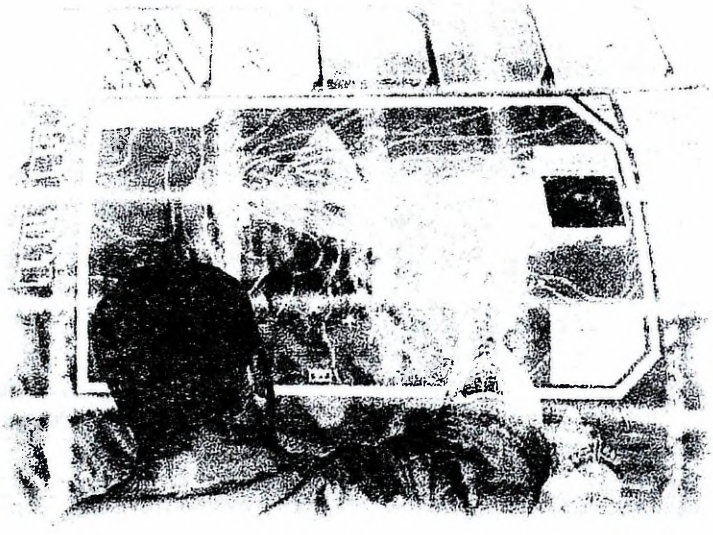


Rysunek 5. Zasady funkcjonowania organizacji wirtualnej
Źródło: www.infoflow.pl/okno.php?nid=165

Wykorzystanie nowoczesnej szerokopasmowej infrastruktury teleinformatycznej oraz budowa wirtualnej struktury systemu stanowisk dowodzenia szczebla taktycznego, pozwoli uzyskać większą zdolność bojową i efektywne wykorzystanie aktywnych środków walki oraz zapewni synchronizację działań. Zwiększenie tego potencjału zgodnie z teorią NCW jest możliwe poprzez wirtualną współprace stanowisk dowodzenia oraz ich elementów. Ponadto wirtualną integrację procesów dostępu do informacji, oraz poprzez specjalizację i świadczenie usług poszczególnych elementów środowiska sieciocentrycznego [12].

Założenia koncepcji NCW mogą okazać się bardzo pożyteczne w odniesieniu do funkcjonowania systemu dowodzenia Wojsk Obrony Terytorialnej oraz w procesie organizacji TSR (Terytorialnego Systemu Rozpoznania). W szczególności, kiedy formacje Wojsk Obrony Terytorialnej prowadziłyby działania obronne lub nieregularne funkcjonując w dużym stopniu rozproszenia, samodzielnie lub współdziałając z Wojskami Operacyjnymi. Przy założeniu zdrowej i nowoczesnej koncepcji organizacji Wojsk Obrony Terytorialnej i wyposażeniu ich w lekki, ale nowoczesny sprzęt łączności i uzbrojenia [5]. Teoretycznie wirtualna struktura systemu stanowisk dowodzenia może zapewnić dowodzenie z dowolnego punku znajdującego się na ziemi, morzu, w powietrzu a nawet w przestrzeni kosmicznej.

Wdrożenie doktryny wojny sieciocentycznej w obliczu dynamicznego postępu technologicznego jest coraz bardziej realne. Wskazuje na to rozwój technologii łączności elektronicznej umożliwiających przekraczanie dużych odległości oraz przesyłanie w łączach szerokopasmowych dużych ilości informacji w tym multimedialnych w czasie zbliżonym do rzeczywistego. Koncepcje wirtualnego stanowiska dowodzenia przedstawia rysunek nr 6.



Rysunek 6. Koncepcja wirtualnego stanowiska dowodzenia
Źródło: www.comceptinc.com/L3comcept/NET.htm

Doktryna wojny sieciocentrycznej jest często krytykowana. Zwłaszcza, jeżeli wspomina się o wymianie ciężkiego sprzętu uzbrojenia na lekki i bardziej mobilny, jednocześnie bardziej wrażliwy na zniszczenie w przypadku trafienia przez środki rażenia przeciwnika. Jednak bez względu na słuszność prezentowanej w dużym skrócie doktryny, wskazuje ona tendencje oraz możliwości wykorzystania zdobyczy techniki w zakresie systemów teleinformatycznych i nieuchronny postępujący proces wszechobecnej informatyzacji współczesnego pola walki. Ponadto wskazuje możliwości wykorzystania nowoczesnych technologii w organizacji systemów teleinformatycznych stanowisk dowodzenia Wojsk Lądowych szczebla taktycznego.

W realiach Wojsk Lądowych wirtualne struktury systemu stanowisk dowodzenia mogą być budowane przez wykorzystanie istniejących już implementacji systemów wspomagania dowodzenia C2IS (*ang. Command, Control and Information System*) takich jak SZAFRAN oraz zautomatyzowanych systemów dowodzenia i kierowania środkami walki takich jak: TOPAZ, BMS TROP, LOARA, ŁOWCZA-3 [3]. Platformę telekomunikacyjną integrującą strukturę systemu dowodzenia Wojsk Lądowych szczebla taktycznego, dostępne środki rozpoznania oraz aktywne środki walki zapewne stanowić może system STORCZYK 2000, ponadto sieci teleinformatyczne MIL-WAN i SEC-WAN. Stanowiska takie wyposażone powinny być w sprzęt komputerowy oraz oprogramowanie wspomagające proces dowodzenia oraz gwarantujące interoperacyjność z innymi systemami NATO.

3. Przyszłościowy System Walki

Opracowany przez U.S. Army Przyszłościowy System Walki FCE (*ang. Future Combat System*), stanowi praktyczne podejście do implementacji koncepcji założonych w doktrynie wojny sieciocentrycznej. Program ten stanowi bardzo duże przedsięwzięcie inżynieryjne. Platforma telekomunikacyjna FCS może obejmować 18 podsystemów. Połączone mają być one w jeden wydajny system sieciocentryczny wymiany informacji taktycznych. System połączyć ma żołnierzy oraz platformy środków walki, takie jak: załogowe i bezzałogowe pojazdy naziemne i latające. Podstawą projektu FCS jest wprowadzenie na pole walki nowoczesnych systemów uzbrojenia oraz wydajnych technologii łączności, gwarantujących współdzielenie informacji oraz zapewniających wspólną świadomość pola walki. System ma zapewnić w dowolnym momencie szybką i precyzyjną lokalizację sił własnych i przeciwnika. Ponadto dostęp do informacji rozpoznawczej z sieci sensorów oraz aktywnych środków walki, jakie można wykorzystać w celu niszczenia przeciwnika.

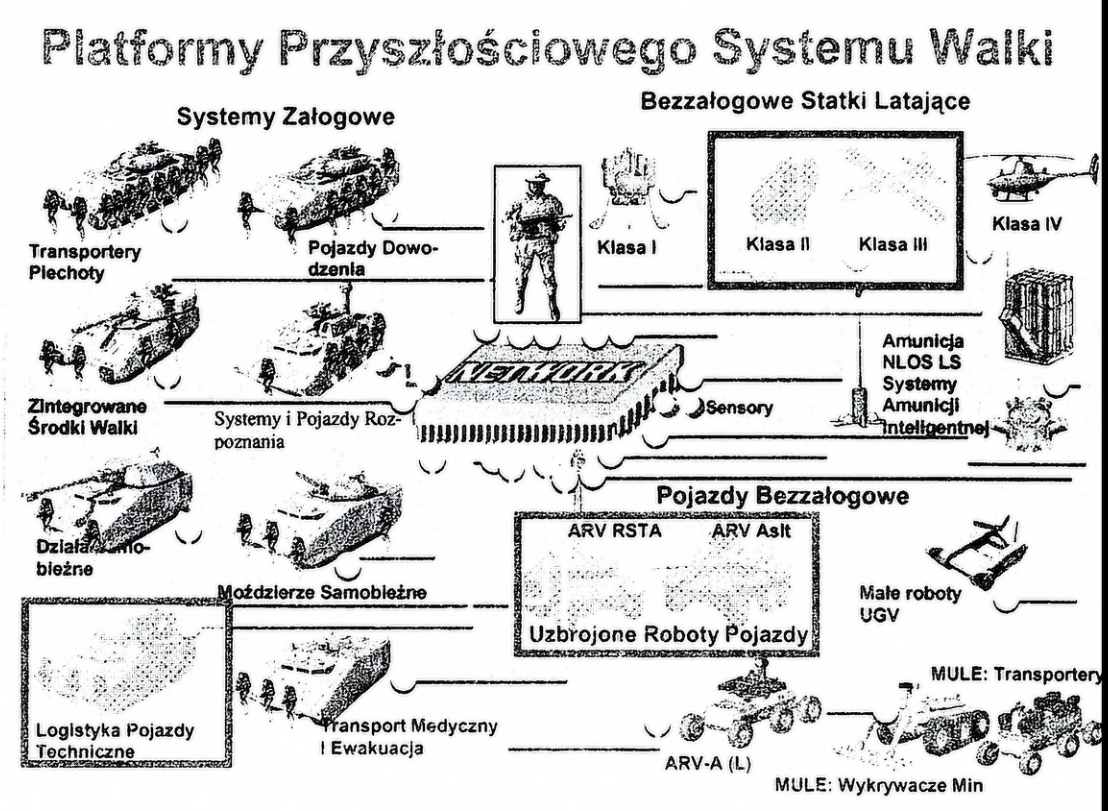
General Dynamics Advanced Information Systems, koncern, który jest odpowiedzialny za zbudowanie zintegrowanego systemu komputerowego ICS (*ang. Integrated Computer System*) na potrzeby FCS, udostępnił informacje, że do budowy tego systemu wykorzysta system operacyjny LynxOS-178. Jest to system operacyjny czasu rzeczywistego kompatybilny z systemem Linux. System operacyjny LynxOS-178 należy do klasy oprogramowania Open Source. Na potrzeby projektów wojskowych sił zbrojnych USA jest dostępny jego kod źródłowy. Jednak jest on systemem rozpowszechnianym na zasadach komercyjnych. LynxOS-178 jest „twardym" systemem czasu rzeczywistego i funkcjonuje jako system wbudowany w układy pamięci elektronicznej (*ang. embedded*). Dlatego też znajduje on szerokie zastosowanie w urządzeniach technicznych i systemach, od których wymaga się funkcjonowa-

nia z zachowaniem rygorów czasu rzeczywistego. Dlatego system operacyjny LynxOS-178 znajduje zastosowanie w systemach łączności oraz systemach sterowania uzbrojeniem. Został on opracowany przez firmę LynuxWorks Inc.

Twórcy wojskowych systemów teleinformatycznych często w swoich projektach wykorzystywali zamknięte architektury oprogramowania, często dedykowane budowane specjalnie pod konkretne zastosowania. Działania tego typu wiązały się z dużymi nakładami finansowymi i długim czasem potrzebnym na powstanie takiego systemu. Wychodzono z założenia, że bezpieczeństwo ma kluczowe znaczenie i z tego powodu unikano wykorzystania standardów otwartych.

Jednak skala współczesnych projektów militarnych oraz często potrzeba integracji wielu platform technologicznych a nawet globalnej implementacji takich systemów, wymusiły stosowanie standardów otwartych oprogramowania. System operacyjny LynxOS-178 spełnia wymagania dotyczące bezpieczeństwa systemów wojskowych o wysokim stopniu zabezpieczeń oraz w zakresie szczegółowej dokumentacji, jak też dostępności kodu źródłowego.

Bezpieczeństwo systemu zwiększa możliwość wykorzystania mechanizmu maszyn wirtualnych, które pozwalają pojedynczemu mikroprocesorowi zachowywać się tak, jak gdyby było to kilka osobnych komputerów, dla poszczególnych wystąpień zasobów oprogramowania. W branży zbrojeniowej system operacyjny LynxOS-178 wykorzystywany jest przez różne firmy w tym Rockwell Collins i Motorola. Podobnie Boeing Company, korporacja uczestnicząca w realizowanym projekcie FCE, zamierza wykorzystywać ten system operacyjny, zwłaszcza w systemach bezpilotowych statków powietrznych UCAV (*ang. Unmanned Commbat Air Vehicles*). Platformy nowoczesnych środków walki, które mogą funkcjonować w systemie FCS przedstawia rysunek nr 7.



Rysunek 7. Platformy technicznych środków walki Przyszłościowego Systemu Walki
Źródło: www.boeing.com

4. Charakterystyka stanowiska dowodzenia

Właściwe wykorzystanie informacji taktycznej przetwarzanej przez lokalne systemy teleinformatyczne stanowisk dowodzenia LAN-SD szczebla taktycznego, wpływa na zdolności manewrowe podległych wojsk, zdolność do reagowania na zmieniającą się sytuację w środowisku pola walki, siłę ognia i skuteczność rażenia środków walki, ponadto ochronę wojsk własnych a dalej zdolność przetrwania oraz sprawne dowodzenie i kierowanie.

Wdrożenie nowoczesnych technologii teleinformatycznych na stanowisku dowodzenia szczebla taktycznego, wyposażenie jego poszczególnych komórek organizacyjnych i osób funkcyjnych w wydajne i bezpieczne oprogramowanie gwarantujące współdzielenie informacji jest wymogiem czasu i standardów obowiązujących w NATO. Tego typu rozwiązania skutecznie wspomagają proces dowodzenia, poszerzają możliwości działania dowódców. System teleinformatyczny pozwala przekazywać intencje dowódców w czasie zbliżonym do rzeczywistego, wiernie i dokładnie według ściśle określonych standardów formatowania i wymiany informacji. Ponadto systemy takie zapewniają zdolność do ciągłego monitorowania sposobu wykonywania zadań. Fakt ten pozwala na zmianę decyzji stosownie do istniejącej sytuacji i zapobieganie niekorzystnemu rozwojowi zdarzeń.

Istotną zaletą współużytkowania informacji w systemach rozproszonych jest możliwość nowego podejścia do procesu dowodzenia i kierowania podległymi zasobami. A przede wszystkim możliwość wykorzystania wspólnej świadomości pola walki, także na poziomie poszczególnych komórek organizacyjnych stanowiska dowodzenia szczebla taktycznego Wojsk Lądowych. W celu osiągnięcia wysokiego stopnia synchronizacji podejmowanych działań taktycznych z innymi uczestnikami walki. Ponadto zachowania zdolności do jednoczesnego szybkiego dostosowania się do zmieniającej się sytuacji.

Współczesne stanowisko dowodzenia to zespół techniczny środków dowodzenia obejmujący również infrastrukturę teleinformatyczną oraz specjalistyczne środki łączności elektronicznej [1]. Infrastruktura teleinformatyczna stanowiska dowodzenia, to przestrzeń do funkcjonowania w środowisku rozproszonym aplikacji użytkowych wspomagających dowódcę w realizacji podstawowych zadań w procesie dowodzenia. Do takich aplikacji należy PGO (Pakiet Grafiki Operacyjnej) opracowany przez Centrum Informatyki i Łączności Obrony Narodowej.

Zasadniczo w celu budowy systemów teleinformatycznych stanowisk dowodzenia wykorzystywać można dedykowany sprzęt teleinformatyczny. Jednak ze względów wysokich kosztów takich rozwiązań, często również stosuje się komercyjny sprzęt komputerowy oraz oprogramowanie zgodnie z podejściem filozofii COTS(*ang. Commercial-Off-The-Shelf*) co znacznie zmniejsza koszty.

Lokalna sieć komputerowa stanowiska dowodzenia LAN-SD, zapewnić musi odpowiednio wysoki poziom niezawodności co oznacza gwarancję ciągłości pracy w sytuacjach awaryjnych i krytycznych wynikających ze specyfiki współczesnego pola walki. Ponadto odporność na zakłócające i niszczące oddziaływanie technicznych środków walki elektronicznej przeciwnika [7]. Szczególną ochronę należy zapewnić danym przetwarzanym, ponadto ochronę baz wiedzy przed ingerencją w nie przeciwnika.

Istnieje konieczność funkcjonowania systemu relacyjnych baz danych obsługujących model danych zgodny z założeniami standardu ATCCIS. System zapewnić musi wymianę danych z otoczeniem poprzez wykorzystanie sformalizowanych komunikatów w formacie XML, ADatP-3. Ponadto w systemie gwarantowany musi być obieg dokumentów, poczty elektronicznej, zapewnienie pracy grupowej. Istotnym elementem jest graficzny interfejs użytkownika, prosty w obsłudze i pozwalający na prezentację najistotniejszych informacji w określonym czasie a więc aktualnej sytuacji taktycznej w formie wielowarstwowego zobrazowania graficznego. Moduł prezentacji grafiki operacyjnej musi obsługiwać formaty cyfrowych map rastrowych CADRD i wektorowych DIGEST, jak również operować na globalnych i lokalnych układach współrzędnych 1942, WGS-84, UTM. Potrzebny jest również mechanizm pozwalający na obsługę numerycznego ukształtowania terenu zgodnie ze standardem DTED. System zapewnić musi mechanizmy automatyzujące przetwarzanie sformalizowanych dokumentów bojowych, czyli przenoszenie danych zawartych w dokumentach do bazy danych i graficzne obrazowanie zadań i sytuacji taktycznej na tle mapy cyfrowej[3].

System teleinformatyczny stanowiska dowodzenia szczebla taktycznego musi posiadać zdefiniowane interfejsy komunikacyjne zapewniające integrację technicznych środków łączności z siecią rozległą szczebla taktycznego, ponadto również z publicznymi systemami telekomunikacyjnymi, które wykorzystują nowoczesne technologie łączności przewodowej, światłowodowej, radiowej i satelitarnej.

5. Charakterystyka orogramowania Open Source

Otwarte oprogramowanie (*ang. Open Source*), to takie oprogramowanie, dla którego licencja jest tak zdefiniowana, że pozwala na legalne i nieodpłatne kopiowane, zarówno kodu wynikowego jak i źródłowego. Ponadto pozwala na dowolne modyfikacje udostępnionego kodu źródłowego. Podstawowa idea Open Source jest bardzo prosta. Zakłada, że jeżeli programiści mają swobodny dostęp do kodów źródłowych oprogramowania poprzez Internet, mogą taki kod źródłowy modyfikować w procesie pracy grupowej oraz go rozpowszechniać. Istnieją projekty informatyczne zrzeszające wirtualne organizacje dążące do wytworzenia określonych produktów informatycznych. Korzystając z usług sieci Internet, programiści tworzą oprogramowanie, ulepszają swoje produkty, testują i poprawiają błędy. Istotną informacją jest fakt, że w poważnych projektach informatycznych uczestniczą osoby o dużym doświadczeniu programistycznym wyniesionym również z firm komercyjnych. Ze względu na skalę organizacji wirtualnych, wszystkie procesy mogą zachodzić bardzo szybko, zwłaszcza w porównaniu z klasycznym developmentem.

Wspólnoty Open Source uzyskały w praktyce potwierdzenie, że tego rodzaju szybki proces rozwoju oprogramowania wytwarza w efekcie końcowym nieraz o wiele lepszy produkt, niż tradycyjny zamknięty model, preferowany przez firmy informatyczne. W takim przypadku tylko ograniczona liczba programistów może mieć dostęp do kodów źródłowych. Natomiast wszyscy pozostali w tym użytkownicy końcowi są zmuszeni używać jedynie zapakowanego bloku bitów w postaci kodu wykonywalnego. Często bez możliwości analizy kompletnych czynności wykonywanych przez taki program, który może posiadać zaszyte funkcje destrukcyjne dla systemu informatycznego, w którym został uruchomiony. Nie zawsze firmy komercyjne chcą udostępniać kod źródłowy swoich produktów, a w przypadku, kiedy wyrażają na to zgodę, nabycie takiego kodu źródłowego wiąże się dużymi nakładami finansowymi.

Na zasadach Open Sorce rozwijany jest system operacyjny Linux. Nie jest on jedynym produktem tworzonym w taki sposób. Do interesujących rozwiązań można zaliczyć systemy operacyjne FreeBSD, NetBSD, czy też wykorzystywany przez DoD USA (*ang. Department of Defense*) system operacyjny OpenBSD. Wsparciem dla systemu operacyjnego Linux i dużym zaangażowaniem w jego rozwój pochwalić się mogą takie firmy jak: IBM, INTEL, Sun Microsystems, Hewlett-Packard, Sybase oraz szereg innych firm z branży informatycznej.

Z pewnością należy zastanowić się czy wytwarzane w ten sposób oprogramowanie może być bezpieczne, a tym bardziej na tyle bezpieczne, aby wykorzystywać produkty Open Source w systemach teleinformatycznych stanowisk dowodzenia Wojsk Lądowych szczebla taktycznego. Podobne wątpliwości można skierować do twórców rodziny systemów operacyjnych Windows rodem z Redmond i zastanawiać się czy przypadkiem nie istnieją pozostawione „tylne drzwi" w oprogramowaniu, pozwalające na dowolną ingerencję w zgromadzone zasoby informacyjne. Inny problem to podatność produktów Microsoft Corporation na całą rzeszę coraz to doskonalszych destrukcyjnych wirusów polimorficznych.

Bezpieczeństwo i niezawodność oprogramowania systemowego Open Source, to według twórców główne zalety ich produktów wykorzystywane w konkurencji z firmą Microsoft Corporation. Kod źródłowy jest wnikliwie analizowany, przypadkowe błędy są skutecznie i szybko likwidowane, a przemyślane próby sabotażu czy działań szkodliwych szybko identyfikowane. Pomimo to nie można być bezkrytycznym wobec oprogramowania Open Source. Dlatego bardzo ważne jest, aby korzystać z wersji oprogramowania stabilnego i sprawdzonego a nie w wersjach rozwojowych, ponadto pozyskiwanego bezpośrednio od twórców takiego oprogramowania.

Otwartość kodu Open Source, stanowi istotną cechę tego typu rozwiązań w przypadku procesu certyfikacji systemów teleinformatycznych przez Wojskowe Służby Informacyjne lub Agencję Bezpieczeństwa Wewnętrznego. W takim przypadku niezbędne jest dostarczenie kodu źródłowego odpowiednio opatrzonego komentarzami, który w razie potrzeby może być wnikliwie analizowany. W produktach klasy Open Source kod źródłowy jest dostępny, można go modyfikować i dostarczyć instytucją certyfikującym w takiej formie, jaka jest wymagana. Tak jak już wspomniano w przypadku systemów zamkniętych, może istnieć poważny problem w dostępie do kodu źródłowego. Fakt ten często związany jest z poniesieniem dużych kosztów.

6. System Operacyjny Linux

Linux jest nowoczesnym, wielozadaniowym i wielodostępnym systemem operacyjnym. Z tego wynika, że jednocześnie może z niego korzystać wielu użytkowników, gdzie każdy z użytkowników może w tym samym czasie uruchamiać wiele aplikacji. System operacyjny Linux od początku swojego istnienia jest systemem przystosowanym do funkcjonowania w środowiskach sieci komputerowych [9].

System ten bez żadnych ograniczeń może być wykorzystywany w sieciach lokalnych stanowisk dowodzenia LAN-SD Wojsk Lądowych, jak również zapewniać w sposób bez-

pieczny i niezawodny wymianę informacji taktycznych w sieciach rozległych, łączących stanowiska dowodzenia na szczeblu taktycznym. Wiele pozytywnych cech tego systemu takich jak: skalowalność, bezpieczeństwo, niezawodność oraz szczególne przystosowanie tego systemu do pracy w sieci, może skłaniać do rozważań nad szerszym wykorzystaniem systemu operacyjnego Linux w procesie informatyzacji stanowisk dowodzenia Wojsk Lądowych szczebla taktycznego. Ponadto nic nie stoi na przeszkodzie, aby system ten mógł znaleźć zastosowanie w procesie budowy wirtualnych stanowisk dowodzenia szczebla taktycznego, zgodnie z założeniami doktryny wojny sieciocentrycznej. Wskazuje na to wiele sprawdzonych zastosowań tego systemu w społecznych i gospodarczych organizacjach wirtualnych [10]. Ponadto istnieje silne wsparcie dla systemu operacyjnego Linux wielu firm komercyjnych oraz organizacji takich jak: NASA (*ang. National Aeronautics and Space Administration*), DARPA (*ang. Defense Advanced Research Projects Agency*), NC3A (*ang. NATO Consultation, Command and Control Agency*), NSA (*ang. National Security Agency*).

Wsparcie sprzętowe

Linux działa na wielu platformach sprzętowych, obsługuje procesory: Intel x86, DEC Alpha (21064 i 21164), SPARC, MIPS, Motorola 680x0, PowerPC, ARM, PA-RISC, Intel 8086/80286/80386, Intel Pentium I, II, III, IV, ponadto architektury procesorów 64 bitowych. Jądro systemu w wersji 2.6.x, zostało zaprojektowane w taki sposób, aby bez problemów mogło obsługiwać architektury komputerów równoległych, wyposażone w 64 procesory i 64 GB pamięci operacyjnej RAM. W systemie stosowane są długie nazwy plików oraz wielkość obsługiwanych plików sięga do 4 TB. Ponadto wykorzystywane są zaawansowane systemy plików: EXT2, EXT3, Raiser, Reiser4, XFS, JFS. Istnieje również dostęp do systemu plików stosowanych w Windows FAT32 oraz NTFS, ale w tym ostatnim przypadku zalecany jest dostęp tylko do odczytu [9].

Usługi sieciowe

System operacyjny Linux gwarantuje możliwość pracy w sieciach komputerowych wykonanych w różnych technologiach. System ten wykorzystuje różne protokoły komunikacyjne: TCP/IP, IPX, SMB, Appletalk, X.25, także protokół następnej generacji IPv6. Ponadto może obsługiwać zaawansowane protokoły routingu: BGP, OSPF, RIP i Multicast. Komputer pracujący pod kontrolą systemu operacyjnego Linux może być zarządzany lub zarządzać innymi urządzeniami poprzez protokół SNMP (*ang. Simple Network Management Protocol*). Pozwala na budowę lokalnych sieci komputerowych z wykorzystaniem technologii NAT (*ang. Network Address Translation*), jednocześnie chroniąc sieć wewnętrzną zaporą ogniową pracującą w trybie dynamicznej kontroli strumienia pakietów (*ang. stateful–inspection*). Sys-

tem operacyjny Linux przeznaczony jest głównie do zastosowań serwerowych. Linux może funkcjonować jako serwer plików FTP (*ang. File Transfer Protocol*), serwer poczty elektronicznej wykorzystujący protokoły SMTP (*ang. Simple Mail Transfer Protocol*) oraz POP3 (*ang. Post Office Protocol*). System ten realizuje jeszcze dużo innych usług w architekturze klient-serwer. Linux w poszczególnych komórkach stanowisk dowodzenia może zapewnić współpracę z komputerami pracującymi pod kontrolą innych systemów operacyjnych klasy UNIX, jak też i Windows. Dotyczy to sieci lokalnej stanowiska dowodzenia LAN-SD, jak również komunikacji z elementami innych stanowisk dowodzenia w sieci rozległej [9].

Skalowalność systemu

Linux jest bardzo atrakcyjnym systemem operacyjnym znajdującym zastosowanie w różnych przedsięwzięciach technicznych. Jedną z istotnych cech, która o tym decyduje jest duża skalowalność tego systemu. Użytkownik ma wręcz nieograniczoną możliwość kształtowania elementów składowych systemu. W minimalnej konfiguracji system mieści się na jednej dyskietce. Znajduje również zastosowanie w rozwiązaniach prezentowanych przez firmę IBM w komputerach równoległych klasy mainframe. Linux może obsługiwać również fermy klastrów liczące tysiące komputerów. Istnieją również możliwości funkcjonowania Linuxa jako systemu czasu rzeczywistego. Do takich rozwiązań należy RTLinux.

Niezawodność Systemu

Linux posiada prawdziwą wielozadaniowość *(ang. preemptive multitasking)*, jak również ochronę pamięci. Proces uruchomiony w systemie nie może uszkodzić innego procesu, a tym bardziej procesu jądra systemu. W praktyce oznacza to, że wadliwie funkcjonująca aplikacja nie jest w stanie uszkodzić procesu innej aplikacji, a tym bardziej procesów innego użytkownika. Nie dochodzi do zawieszania się Linuxa znanego z systemu operacyjnego Windows. Pod względem wydajności, szybkości i stabilności Linux konkuruje z kosztownymi komercyjnymi systemami operacyjnymi [10].

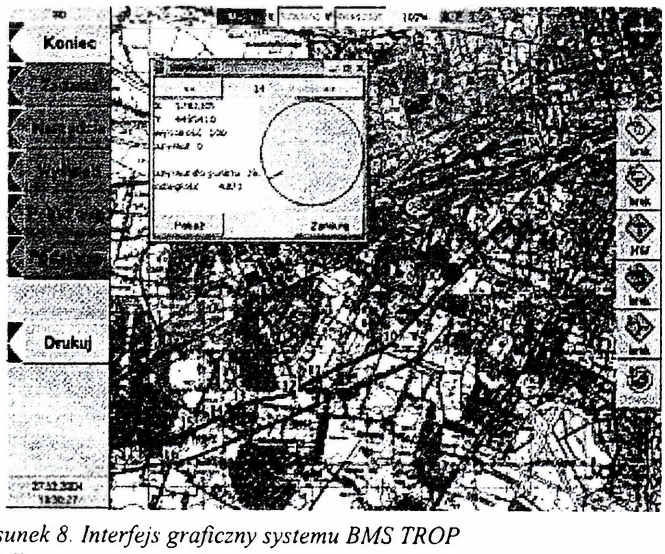
Usługi systemu w zakresie bezpieczeństwa

System operacyjny Linux wyposażony jest w silne wsparcie kryptograficzne w zakresie kryptografii symetrycznej: DES, IDEA, RC5, RC6, Twofish, Blowfish, AES i asymetrycznej DES oraz innych algorytmów kryptograficznych. W praktyce oznacza to, że istnieje możliwość szyfrowania pojedynczych plików, katalogów oraz całych partycji, także systemowych. Ciekawym rozwiązaniem jest możliwość wykorzystania plików-kontenerów, w których zapisywane i szyfrowane są struktury katalogów i plików, dostępne dla określonego użytkownika. Szyfrowanie realizowane jest na poziomie jądra systemu operacyjnego. W przypadku wyjęcia dysku twardego z komputera dane pozostają zaszyfrowane. Wykorzystanie protokołu SSH

(*ang. Secure Shell*) pozwala na zdalną komunikację pomiędzy komputerami w tym transfer plików w szyfrowanym kanale logicznym z wykorzystaniem metod szyfrowania asymetrycznego. Podobnie protokół SSL (*ang. Secure Sockets Layer*), można wykorzystać do tunelowania poczty elektronicznej. Linux może posłużyć również do budowy wirtualnych sieci prywatnych VPN (*ang. Virtual Private Network).* Istnieje również implementacja systemu identyfikacji i uwierzytelniania użytkowników Kerberos, systemu opracowanego przez MIT (*ang. Massachusetts Institute of Technology*). Ponadto wykorzystać można zaprojektowany przez NSA (*ang. National Security Agency*) zaawansowany system zarządzania bezpieczeństwem - SELinux.

Usługi systemu w zakresie prezentacji grafiki

Podstawowym interfejsem użytkownika w systemie operacyjnym Linux są konsole tekstowe. Jest to środowisko wystarczające dla administratora systemu, ale z pewnością nie dla użytkownika końcowego. Dlatego w systemie operacyjnym Linux za obsługę grafiki odpowiada X Window System. Istnieje również możliwość prezentowania grafiki o dużej rozdzielczości w trybie konsoli. Linux wyposażony jest w wiele środowisk graficznych, które również dowolnie można skalować, według wymagań użytkownika. Do takich środowisk należą: Blackbox, Fluxbox, Window Maker, Xfce, GNOME, KDE itp. System wyposażony jest w liczne biblioteki graficzne: SVGA, Gtk, Qt, SDL, OpenGL, pozwalające na prezentowanie grafiki operacyjnej na stanowiskach dowodzenia w formie 2D i 3D. Interfejs graficzny systemu BMS TROP (*ang. Battle Management Systems*) firmy WB Electronics przedstawia rysunek nr 8.

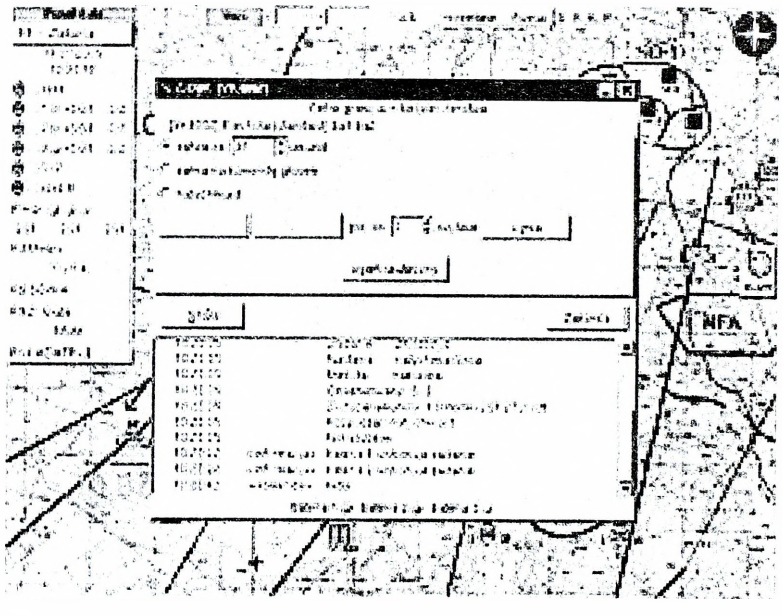


Rysunek 8. Interfejs graficzny systemu BMS TROP
Źródło: www.wb.com.pl

7. Wykorzystanie systemu Linux w Zautomatyzowanym Zestawie Kierowania Ogniem TOPAZ

Oprogramowanie Open Source obecnie znajduje zastosowanie w systemie stanowisk dowodzenia szczebla taktycznego Wojsk Lądowych. System operacyjny Linux wykorzystywany jest przez firmę WB ELECTRONICS. Do produktów tej firmy należy Zautomatyzowany Zestaw Kierowania Ogniem TOPAZ oraz system BMS TROP.

Zautomatyzowany Zestaw Kierowania Ogniem TOPAZ jest systemem, który został wykonany i jest rozwijany przez firmę WB Electronics. TOPAZ jest systemem, który zapewnia wspomaganie pracy dywizjonu artylerii. Wsparcie dotyczy zakresu dowodzenia i kierowania środkami ogniowymi. System ten przeznaczony jest dla dywizjonów artylerii wyposażonych odpowiednio w działa i wyrzutnie artylerii typu: 122 mm HS, 152 mm AHS, BM-21 oraz RM-70 przed modernizacją. System TOPAZ w warstwie oprogramowania funkcjonuje w oparciu o platformę systemu operacyjnego Linux. Oprogramowanie systemowe zostało odpowiednio zoptymalizowane i dostosowane do zakresu zadań wynikających z funkcji systemu. System wyposażony jest również w dedykowane aplikacje napisane przez programistów tej firmy, wspomagające proces dowodzenia i kierowania środkami walki. Interfejs graficzny wraz z obsługiwaną mapą cyfrową Zautomatyzowanego Zestawu Kierowania Ogniem TOPAZ przedstawia rysunek nr 9.



Rysunek 9. Interfejs graficzny systemu TOPAZ
Źródło: www.wb.com.pl

Rozproszona architektura systemu pozwala na to, aby mógł on występować w różnych konfiguracjach ilościowych i sprzętowych, przy zachowaniu określonej struktury powiązań systemowych łączności. Na topologię systemu nie ma także wpływu zróżnicowanie pojazdów występujących w dywizjonach. Wymiana informacji taktycznych realizowana jest w sposób całkowicie zautomatyzowany bez ingerencji operatora. Całość pracy systemu opiera się na wymianie informacji w postaci cyfrowej. W określonych sytuacjach zawsze możliwa jest również wymiana informacji fonicznej.

Podstawowym parametrem określającym jakość działania systemu jest pewność przekazania informacji. Ponadto jakość przekazywanych danych i czas dystrybucji informacji oraz ich interpretacji przez system. Struktura przepływu danych w systemie informatycznym TOPAZ, odpowiada hierarchicznej strukturze dowodzenia. Automatyzacja procesu dowodzenia i prowadzenia strzelań przez dywizjon artylerii obejmuje wszystkie stanowiska bojowe, zarówno dowodzenia dywizjonem, wysuniętych obserwatorów artyleryjskich oraz aktywne środki ogniowe. Rozproszona architektura sprzętowo- programowa systemu TOPAZ pozwala na wspomaganie dowódcy dywizjonu w trakcie realizacji zadania bojowego, zgodnie z wyznaczonymi zadaniami oraz obowiązującymi zasadami prowadzenia działań bojowych artylerii.

System TOPAZ zapewnia współpracę z radiostacjami, zarówno analogowymi, jak i cyfrowymi oraz gwarantuje cyfrowe przekazywanie danych w polowych sieciach przewodowych. Automatyzacja obliczeń balistycznych oraz cyfrowe przekazywanie komend i meldunków, pozwalają na skrócenie czasu otwarcia ognia przez aktywne środki walki. Prostota obsługi systemu i bieżąca prezentacja sytuacji bojowej na mapie cyfrowej, wyświetlanej na ekranie komputerów w sposób zasadniczy wspomaga pracę dowódców i osób funkcyjnych. Ponadto realizowany jest proces automatycznej i ciągłej kontroli sytuacji logistycznej, kontrola realizacji zadań oraz kontrola prawidłowości obiegu danych w systemie. Zapewniona jest również współpraca z innymi, dowolnymi systemami wyższego szczebla w tym SZAFRAN.

Zakończenie

Postęp technologiczny, informatyzacja współczesnego pola walki oraz wykorzystanie nowych generacji inteligentnych systemów uzbrojenia w sposób zasadniczy wpływa na dynamikę zmian zachodzących na współczesnym polu walki. Istniejące procesy mają również wpływ na kształt oraz zasady funkcjonowania struktury systemu stanowisk dowodzenia. Jedną ze współcześnie rozwijanych koncepcji jest doktryna wojny sieciocentrycznej NCW (ang. Network Centric Warfare). Doktryna NCW definiuje sieciocentryczny proces dowodzenia, bazujący na częściowo lub całkowicie zdecentralizowanych strukturach dowodzenia. Wirtualne stanowiska dowodzenia oraz dynamiczna struktura więzi informacyjnych, zapewnić ma efektywne i skuteczne wykorzystanie aktywnych środków walki. Podstawą osiągnięcia sukcesu w walce według doktryny NCW jest zdolność wszystkich elementów sił własnych, biorących udział w walce do współdzielenia informacji taktycznych oraz osiągania wspólnej świadomości pola walki i samosynchronizacji w zakresie realizowanych zadań bojowych.

Realizacja koncepcji NCW wymaga istnienia zintegrowanych sieci środków rozpoznania, sieci systemu stanowisk dowodzenia oraz sieci aktywnych systemów uzbrojenia. Cel ten może być osiągnięty poprzez wykorzystanie nowoczesnych technologii łączności elektronicznej w tym systemów teleinformatycznych. Natomiast systemy teleinformatyczne nie mogą poprawnie funkcjonować bez wykorzystania w nich niezawodnych i bezpiecznych systemów operacyjnych, charakteryzujących się dużym stopniem skalowalności.

Do rozwiązań takich należą systemy operacyjne implementowane na zasadach Open Source w tym Linux. System operacyjny Linux znajduje zastosowanie w systemach teleinformatycznych zarówno cywilnych, jak i militarnych. Wykorzystywany jest przez różne firmy: IBM, INTEL, Boeing Company, LynuxWorks, Sun Microsystems, Hewlett-Packard. System ten wspierany jest również przez organizacje naukowe i odpowiedzialne za bezpieczeństwo międzynarodowe a mianowicie: NASA (ang. National Aeronautics and Space Administration), DARPA (ang. Defense Advanced Research Projects Agency), NC3A (ang. NATO Consultation, Command and Control Agency), NSA (ang. National Security Agency).

Przedstawione informacje oraz fakty w aspekcie postępu technologicznego oraz rozwijanych koncepcji funkcjonowania przyszłościowego pola walki, mogą stanowić podstawy do rozważań nad szerszym wykorzystaniem systemu operacyjnego Linux w systemie stanowisk dowodzenia Wojsk Lądowych szczebla taktycznego sił zbrojnych RP.

BIBLIOGRAFIA

POZYCJE KSIĄŻKOWE

1. Józef Michniak, *Dowodzenie i Łączność*, Akademia Obrony Narodowej, Warszawa 2005.
2. Józef Janczak, praca zbiorowa, *System Łączności Brygady*, Akademia Obrony Narodowej, Warszawa 2005.
3. Józef Janczak, Piotr Daniluk, praca zbiorowa, *Środki Dowodzenia*, Akademia Obrony Narodowej, Warszawa 2003.
4. Jarosław Wołejszo, *Wybrane Aspekty Projektowania Struktury Organizacyjnej Zespołu Dowodzenia Stanowiska Dowodzenia Brygady Zmechanizowanej*, Akademia Obrony Narodowej, Warszawa 2003.
5. Grzegorz Sobolewski, *Wspólne Działania Obronne Wojsk Operacyjnych i Obrony Terytorialnej*, Akademia Obrony Narodowej, Warszawa 2005.
6. Marian Łokociejewski, Waldemar Scheffs, *Walka elektroniczna w operacji i walce*, Akademia Obrony Narodowej, Warszawa 2005.
7. płk dr inż. Józef Janczak, *Zakłócanie Informacyjne*, Akademia Obrony Narodowej, Warszawa 2002.
8. Marian Łokociejewski, praca zbiorowa, *Rozpoznanie Wojskowe-część I-Podstawy Teoretyczne*, Akademia Obrony Narodowej, Warszawa 2003.
9. Abraham Silberschatz, Peter B. Galvin, *Podstawy systemów operacyjnych,* Wydawnictwa Naukowo - Techniczne, Warszawa 2001.
10. Coulouris G., Dellimore J., Kindberg T., *Systemy rozproszone podstawy i projektowanie*, Wydawnictwa Naukowo - Techniczne, Warszawa 1998.
11. Henry H. Shelton Chairman of the Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Chiefs of Staff 1998.
12. David S. Alberts, John J. Garstka, Frederick P. Stein, *Network Centric Warfare, Developing and Leveraging Information Superiority*, DoD C4ISR Cooperative Research Program 2000.

ARTYKUŁY

20. płk prof. dr hab. inż. Piotr Sienkiewicz, *Bezpieczeństwo informacyjne w erze globalizacji*, Wydawnictwo Akademii Obrony Narodowej w Warszawie, Zeszyty Naukowe AON nr 3-4(48-49) 2002.
21. mjr dr Marek Wrzosek, *Struktura strumienia informacyjnego w taktycznym systemie rozpoznania wojsk lądowych*, część I, Wydawnictwo Akademii Obrony Narodowej w Warszawie, Zeszyty Naukowe AON nr 2(47) 2002.

22. mjr dr Marek Wrzosek, *Struktura strumienia informacyjnego w taktycznym systemie rozpoznania wojsk lądowych*, część II, Wydawnictwo Akademii Obrony Narodowej w Warszawie, Zeszyty Naukowe AON nr 3-4(48-49) 2002.

23. Płk dr inż. Ryszard Szpakowicz, Ppłk rez. dr inż. Romuald Hoffmann, *Koncepcja wojny sieciocentrycznej jako odpowiedź na zapotrzebowanie sił powietrznych XXI wieku na informacyjne wsparcie działań bojowych,* Wydawnictwo Dowództwa Sił Powietrznych, Przegląd Wojsk Lotniczych i Obrony Powietrznej Nr 8/2003.

24. płk dr inż. Józef Janczak, *Obrona informacyjna w działaniach obronnych związku operacyjnego, część I, Przedmiot, cel i zadania obrony informacyjnej*, Wydawnictwo Akademii Obrony Narodowej w Warszawie, Zeszyty Naukowe AON nr 2(47) 2002.

Rola technicznych środków dowodzenia w procesie informatyzacji stanowisk dowodzenia

dr hab. inż. Józef JANCZAK
Akademia Obrony Narodowej

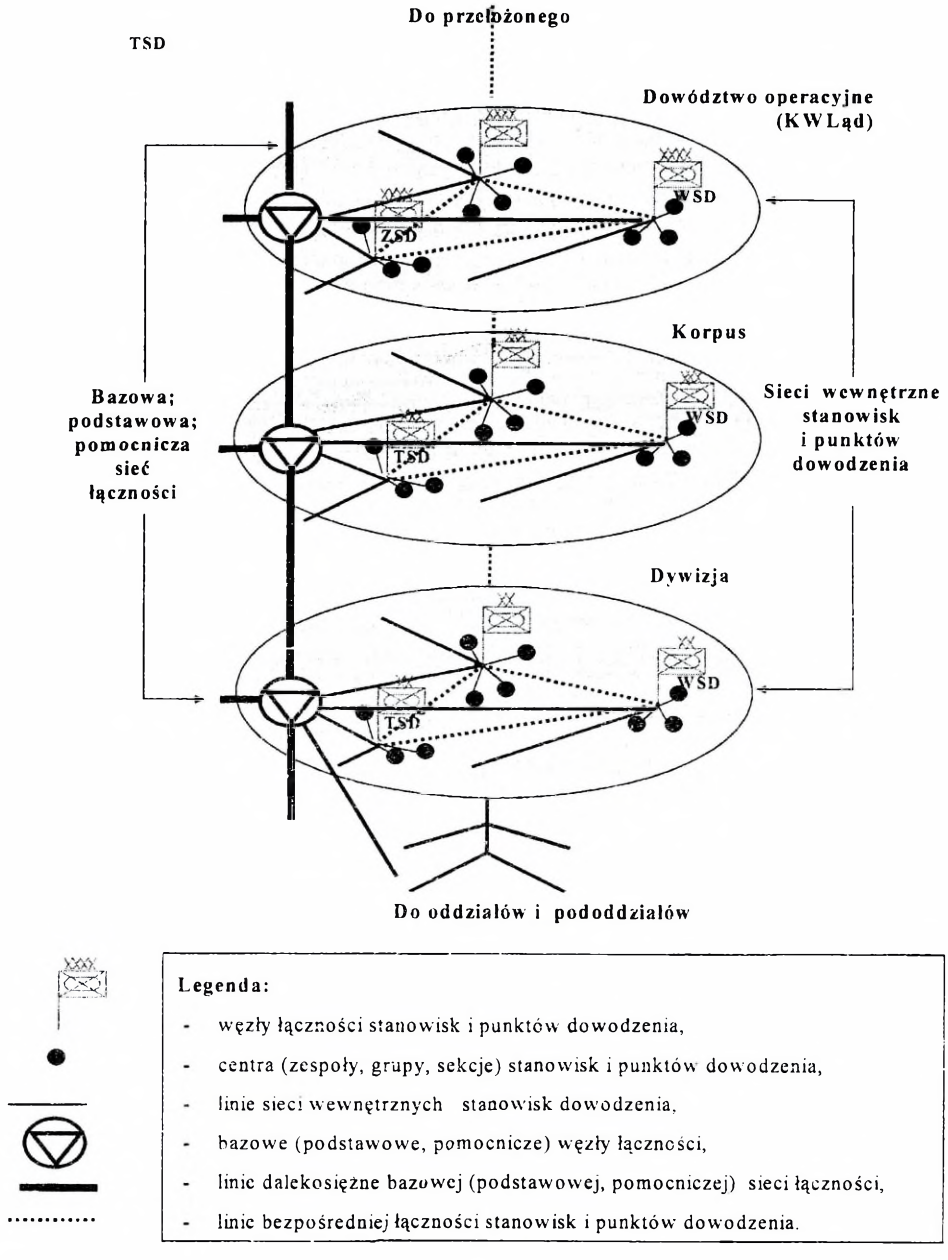
Proces informatyzacji stanowisk dowodzenia staje się ważnym czynnikiem decydującym o efektywności dowodzenia wojskami i sterowania środkami rażenia. Ma także duży wpływ na uzyskanie przewagi w tym obszarze nad potencjalnym przeciwnikiem metodami usprawniania podsystemu informacyjnego (zdobywanie, poszukiwanie, przygotowanie, przechowywanie, obieg informacji, itp.).

Techniczne środki dowodzenia, mające zasadniczy wpływ na poziom informatyzacji w obszarze dowodzenia, stają się coraz ważniejszym czynnikiem decydującym o jakości procesów dowodzenia i uzyskania przewagi metodami zwiększającymi skuteczność zarówno przygotowania jak i obiegu szeroko rozumianej informacji w systemie dowodzenia.

Techniczne środki dowodzenia, wśród których – zdaniem autora – coraz większą rolę odgrywają urządzenia łączności i informatyki, na obecnym etapie, utrudniają organizowanie na tyle spójnego systemu wymiany informacji, aby mógł on niezawodnie funkcjonować i elastycznie dostosować się do potrzeb w każdej sytuacji bojowej. Dlatego też rozwiązania dnia dzisiejszego oraz w najbliższej przyszłości utożsamiane są z dwoma wzajemnie przenikającymi się strukturalnie i funkcjonalnie podsystemami i sprzęgającymi je liniami magistralnymi. Są to dalekosiężne („obszarowe") radioliniowo-kablowe sieci telekomunikacyjne (bazowe, podstawowe, pomocnicze) rozwinięte na obszarze działań operacyjnych (taktycznych), sieci radiowe (w tym pola walki i radiodostp) oraz sieci wewnętrzne stanowisk dowodzenia[1].

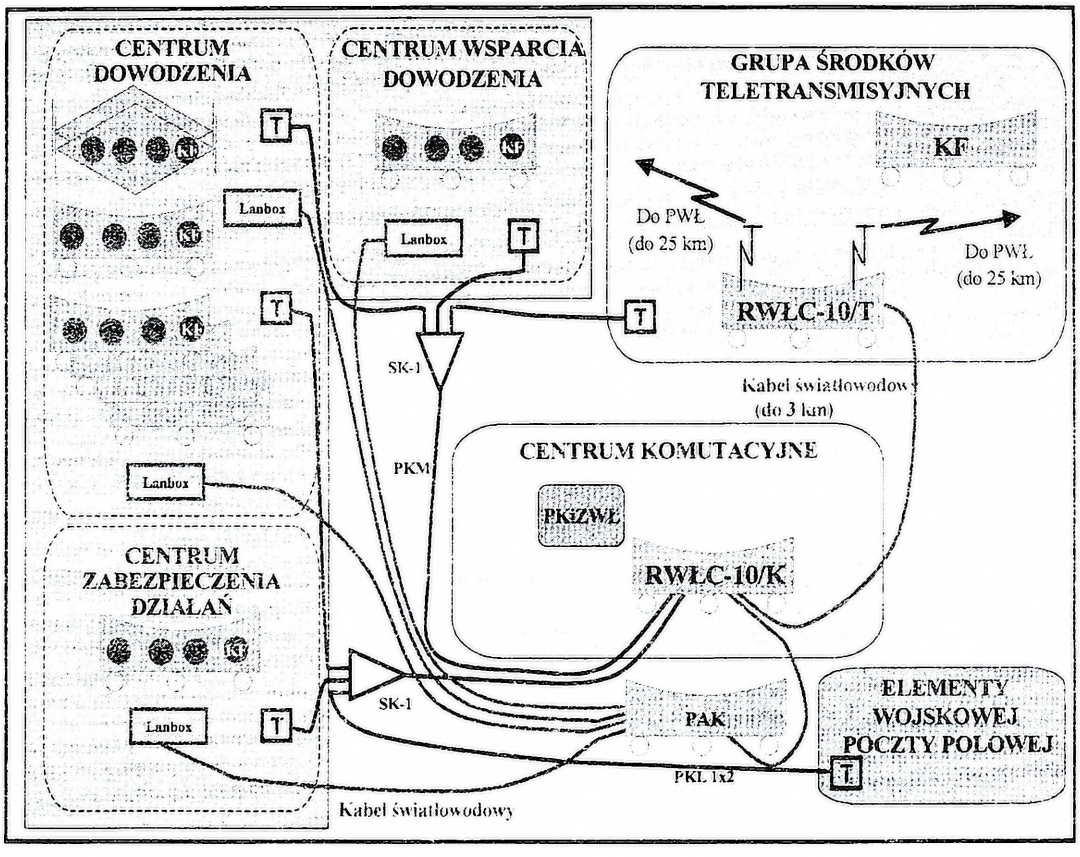
Miejsce sieci wewnętrznych stanowisk dowodzenia w wielopoziomowym systemie dowodzenia i łączności komponentu lądowego przedstawiono na rysunku 1.

[1] Stanowiska dowodzenia miedzy sobą sprzęgane są rozległymi sieciami komputerowymi, tworzonymi w oparciu o system łączności cyfrowej Storczyk-2000. W tym celu wykorzystuje się węzły pakietowe WP-40 z aparatowni RWŁC-10 T/K.



Rysunek 1. Miejsce sieci wewnętrznych stanowisk dowodzenia w wielopoziomowym systemie dowodzenia i łączności komponentu lądowego
Źródło: opracowanie własne

Sieć tę tworzą oddzielne kablowe telekomunikacyjne sieci abonenckie jawne (i niejawne) oraz komputerowe, świadczące usługi głosowe oraz transmisję danych (rysunek 2). Do rozwinięcia kablowej sieci komputerowej wykorzystywane są LANBOXy polowe kable światłowodowe PKŚ-CTOS i polowe kable skrętkowe PKS-62GB. Pomimo dużej odporności na zakłócenia i podsłuchanie podstawową wadą tych urządzeń jest długi czas rozwijania i brak wystarczającej ilości obsady osobowej stanowiska dowodzenia aby czynności te wykonywać.



Rysunek 2. Sieć komputerowa (i telefoniczna abonencka) stanowiska dowodzenia
Źródło: Janczak J., Wisz A., „System łączności brygady", wyd. AON, Warszawa, 2004.

Takie rozwiązanie zapewnia wymianę informacji na stanowiskach dowodzenia jedynie w czasie ich rozwinięcia na dłuższym postoju, czyli w obronie. Natomiast w bardziej manewrowych rodzajach działań bojowych oraz w czasie marszu (zmiany lokalizacji stanowiska dowodzenia) sieć nie jest w stanie zapewnić wymiany informacji. Niestety na dzień dzisiejszy nie została jeszcze wdrożona wymiana informacji w czasie marszu (przemieszczania stanowiska dowodzenia) drogą radiową w ramach tego systemu.

W tych bowiem sieciach należy, moim zdaniem, identyfikować problemy techniczne i stawiać wymagania operacyjno - taktyczne dotyczące zapewnienia zwiększających się potrzeb w zakresie wymiany różnych postaci informacji w systemach dowodzenia wykorzystywanych w różnych rodzajach działań wojsk lądowych. .

Nie podlega wątpliwości teza, że zakres usług teleinformatycznych świadczonych organom dowodzenia zależy od jakości użytych urządzeń łączności i techniki komputerowej.

Baza techniczna systemu dowodzenia musi tworzyć warunki do takiego podziału czasu pracy organu dowodzenia, aby jego większość przypadała na działalność koncepcyjno - organizatorską, a tylko nieznaczna ilość na przedsięwzięcia kalkulacyjne oraz redagowanie rozkazu; meldunku lub komendy i ich przesyłanie. Adresatami odpowiednio przygotowanych informacji są zarówno ludzie jak i środki rażenia (walki). Aby adresaci otrzymali wysłane informacje w czasie realnym, system musi terminowo zbierać, przetwarzać i przekazywać informacje w dwóch pionach funkcjonalnych: w pionie organów dowodzenia i w pionie kierowania środkami rażenia (walki). Adekwatnie do tego podziału należy zatem utworzyć zautomatyzowaną i automatyczną część systemu dowodzenia wyposażoną w odpowiednie sieci teleinformatyczne.

Podsystem (moduł) **zautomatyzowany** to ta część systemu, która charakteryzuje się względnie samodzielnym, zaproponowanym przez operatora systemu zbieraniem i przetwarzaniem informacji oraz wymianą informacji pomiędzy kierowniczymi organami dowodzenia.

Podsystem (moduł) automatyczny ma zapewnić kierowanie środkami ogniowymi i radioelektronicznymi i działać bez udziału człowieka. Funkcje jego organu kierującego spełniają odpowiednio wyposażone specjalizowane komputery i oprogramowane sprzężone sieciami teleinformatycznymi o dużej przepływności.

Przedstawiona idea sieci teleinformatycznej, zapewniająca wymianę różnych postaci informacji pomiędzy elementami systemów dowodzenia na różnych poziomach może być zrealizowana na bazie modelu przedstawionego na rysunku 2.

Utworzony w ten sposób zautomatyzowany system dowodzenia komponentu lądowego w świetle założeń operacji połączonej powinien spełniać następujące wymagania:

- rozwiązanie zadania bojowego nie może trwać dłużej niż czas krytyczny dla jego rozwiązania w konkretnej sytuacji,
- czas rozwiązania zadania bojowego musi być znacznie krótszy od czasu potrzebnego na ręczne wykonanie obliczeń, opracowania i przekazania decyzji do wykonawców,
- dokładność rozwiązania zadania bojowego musi być zdecydowanie wyższa niż przy ręcznym sposobie wykonania tego przedsięwzięcia.

Techniczne środki dowodzenia użyte w tym systemie dowodzenia powinny spełniać następujące wymagania:

- nie mogą angażować dodatkowej ilości osób funkcyjnych organu dowodzenia,
- muszą zapewnić jednoczesne zbieranie informacji z różnych źródeł, ich przetwarzanie, opracowanie i przekazywanie kompleksowej informacji do upoważnionych adresatów,
- muszą uprościć proces przygotowania wielowariantowych danych dla podjęcia decyzji,
- muszą zapewniać symulowanie skutków podjętych decyzji i graficzne ich zobrazowanie,
- muszą zapewniać wiarygodność przyjmowanych i przekazywanych informacji sytuacyjnych i decyzyjnych,
- powinny zapewniać wybór alternatywnych a zarazem efektywnych sposobów wykonania powziętej decyzji.

Wymagania stawiane takiemu systemowi dowodzenia mogą spełnić tylko wysokiej klasy:

- terminale,
- aparatownie transmisyjne i komutacyjne;
- zespoły (wozy dowodzenia) wyposażone w radiostacje pola walki;
- inne środki łączności cyfrowej i informatyki.

Terminalem powinien być zestaw urządzeń tworzących wielofunkcyjne stanowisko pracy, które zapewnia odbiór i nadawanie głosu, przechowywanie, przetwarzanie i zobrazowanie danych cyfrowych, przyjmowanie i kierowanie do adresatów opracowanych decyzji i komunikatów. Obserwowany rozwój technologii produkcji urządzeń elektronicznych pozwala wnioskować, że sukcesywna miniaturyzacja i niezawodność wytworów telekomuni-

kacyjnych pozwoli konstruować zautomatyzowane stanowisko pracy (ZSP) proste w obsłudze, przychylne dla użytkownika oraz podatne do zamontowania w mobilnym środku transportowym. Na dzień dzisiejszy pożądany stopień automatyzacji procesów dowodzenia zapewnia stacjonarne stanowisko pracy, którego zasadniczym elementem jest komputer z urządzeniami towarzyszącymi. Przygotowywane są terminale mobilne, np. terminal przewoźno-przenośny TPP-10, terminal pokładowy TP-10W systemu Szafran, przeznaczone do wykorzystania na mobilnym stanowisku pracy. Terminale takie powinny zapewniać między innymi:

- sprawne działanie zaimplementowanego oprogramowania (kalkulacje czasowo - przestrzenne, priorytetowanie informacji, przetwarzanie i zobrazowanie danych o wojskach własnych i przeciwniku, symulacje projektów decyzji i skutków ich wdrożenia, obsługiwanie procesów komunikacyjnych),
- ciągłe śledzenie i zobrazowanie bieżących informacji od przełożonego, podwładnych i sąsiadów,
- gromadzenie dużych zbiorów informacji i łatwy do nich dostęp osób upoważnionych,
- szybkie działanie na informacjach,
- bezpieczeństwo informacji gromadzonych w pamięciach,
- samotestowanie się przed rozpoczęciem pracy,
- niezawodność pracy w niesprzyjających warunkach otoczenia,
- szybki dostęp stanowiska pracy do bazy telekomunikacyjnej obszaru działań bojowych lub innego stanowiska pracy.

Mobilne zautomatyzowane stanowiska pracy wraz z obsługującymi je użytkownikami stają się, moim zdaniem, podstawowymi elementami organu dowodzenia każdego szczebla. Problemem nie cierpiącym zwłoki, a związanym z potrzebą szybkiej transmisji danych jest wdrożenie do wojsk nowoczesnych środków łączności i informatyki, w tym bardzo potrzebnych radiolinii dostępowych[2] czy szerokopasmowych radiostacji cyfrowych, praktycznie niezbędnych przy tworzeniu współczesnych mobilnych szerokopasmowych sieci teleinformatycznych. W kontekście tym zasadnym wydaje się rozważenie możliwości wykorzystania protokołu IP w mobilnych sieciach telekomunikacyjnych (ang. *Voice over IP*) oraz stworzenie jednolitych sieci teleinformatycznych, w których pracowałyby jednocześnie komputery, telefony i radiostacje. Stosownie do potrzeb można rozwinąć także sieci wewnętrznych

[2] Przykładem mogą być reklamowane przez firmę Transbit stacje radioliniowe R-450C.

i zewnętrznych połączeń teleinformatycznych za pomocą różnych rodzajów środków transmisyjnych. Jakość użytych środków transmisyjnych i sposób włączenia ich w jednolity system mają istotne znaczenie dla sprawowania dowodzenia w działaniach zbrojnych.

Wobec powyższego współczesne **środki transmisyjne** powinny spełniać dodatkowe wymagania w zakresie:

- niewielkich gabarytów i wagi aparatury transmisyjnej,
- dużej mobilności zestawów antenowych środków bezprzewodowych,
- elastycznych i lekkich kabli polowych oraz wydajnych urządzeń do ich rozwijania i maskowania,
- wysokiej przepływność kanałów transmisyjnych,
- bezpiecznego transportu informacji w kanałach transmisyjnych,
- zunifikowanych złącz do współpracy z systemami komutacyjnymi.

Wdrożenie urządzeń spełniających powyższe wymagania pozwoli osiągnąć wysoki stopień automatyzacji procesów w podsystemie dowodzenia działaniami bojowymi i w podsystemie kierowania środkami walki.

Z poczynionych obserwacji wynika, że bazowa (podstawowa, pomocnicza) sieć telekomunikacyjna obszaru działań będzie posiadała nadmiarowy potencjał telekomunikacyjny i wystarczającą ilość punktów dostępu do niej, a organ dowodzenia nie musi organizować, dwóch do czterech jednocześnie funkcjonujących stanowisk (punktów) dowodzenia. Zaistnieją warunki do pełnego urzeczywistnienia modelu dowodzenia poprzez cele tzn. stosownie do celu działań bojowych realizujący go organ dowodzenia rozwinie najwygodniejszy dla jego osiągnięcia system stanowisk dowodzenia[3].

Zespoły dowodzenia wyposażone w zautomatyzowane stanowiska pracy (wozy dowodzenia wraz z radiostacjami pola walki) będą mogły poruszać się wraz z elementami ugrupowania bojowego i decydować o sposobach wykonywania postawionych zadań. Umiejscowienie zespołu dowodzenia w strukturze elementu ugrupowania bojowego zapewni ochronę działania tego organu i skróci długość linii teletransmisyjnych dowodzenia bezpośrednio podległymi wojskami. Poprzez włączenie się zespołu do bazowej (podstawowej, pomocniczej) sieci łączności skorzysta on z informacji o sytuacji w całym obszarze działań bojowych, będzie składał meldunki przełożonemu, otrzymywał od niego rozkazy i decydował o sposobach ich wykonania. Czas działania, ilość i skład zespołów dowodzenia będzie na bieżąco

[3] W koncepcji wojny sieciocentrycznej NCW (ang. *Network Centric Warfare*) przewiduje się nawet tworzenie wirtualnych sieciowych stanowiska dowodzenia

regulował dowódca. Zespoły będą pełniły funkcje koordynujące działania różnych rodzajów wojsk dla osiągnięcia wspólnego celu.

Jest to idea wykorzystania organu dowodzenia rozproszonego w całym obszarze działań bojowych w świetle założeń wojny sieciocentrycznej, którą można zrealizować na poddanym rozważaniom modelu systemu dowodzenia i łączności. W modelu tym ważną rolę mają do spełnienia sieci teleinformatyczne stanowisk dowodzenia zintegrowane usługowo.

Literatura

1. Janczak J., Modelowanie symulacyjne zagrożenia elektronicznego mobilnego systemu łączności związku operacyjnego wojsk lądowych, wyd. AON, Warszawa 2000
2. Janczak J., Wisz A., „System łączności brygady", wyd. AON, Warszawa, 2004.
3. Konopka L., Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości, Myśl Wojskowa, nr 2/200
4. Michniak J. Wł., Polowy zautomatyzowany system dowodzenia, wyd. wewn. AON, Warszawa 2003
5. Zaskórski P., Automatyzacja procesów dowodzenia, Wydawnictwo Adam Marszałek, Toruń 2001
6. Założenia na oprogramowanie instalacji pilotowej PZSD ZT, Etap II, wyd. PIT, Warszawa 2000

Projektowanie i wdrożenie informatycznych systemów wspomagania procesu dowodzenia na szczeblu związku taktycznego

dr inż. Henryk ŁUKASIEWICZ, mgr inż. Artur SZLESZYŃSKI
Zakład Łączności i Informatyki, Wyższa Szkoła Oficerska Wojsk Lądowych

Powodem podjęcia prac, mających na celu przygotowanie i wdrożenie informatycznych systemów wspomagających proces dowodzenia na szczeblu związku taktycznego, jest konieczność zwiększenia efektywności działania sztabu. W trakcie prowadzenia działań bojowych do sztabu ZT docierają informacje z bardzo wielu źródeł. Metodą pozwalającą na ochronę sztabu przed chaosem informacyjnym jest stworzenie procedur przekazywania meldunków. Próba ręcznej obróbki dużej ilości informacji powoduje powstanie znacznych opóźnień w procesie podejmowania decyzji. Skutkiem tego jest porażka polegająca na nie wykonaniu postawionych zadań i nie osiągnięciu założonego celu operacji. Kolejnym skutkiem są straty w sprzęcie i straty w stanach osobowych. Dla żołnierzy wykonujących zadania najbardziej deprymujący jest fakt słabego dowodzenia i przegranej powstałej na skutek niskiej jakości procesu dowodzenia.

Należy zatem rozważyć, jakie czynniki mają wpływ na przygotowanie informatycznego systemu wspomagania procesu dowodzenia (ISWPD). Co decyduje o tym, że eksploatowane na stanowisku dowodzenia rozwiązanie, jest użytecznym narzędziem wspomagającym proces dowodzenia wojskami. Artykuł podejmuje próbę wskazania tych czynników, które – zdaniem autorów - mają istotny wpływ na jakość wdrożonego rozwiązania. Problematyka ta jest szczególnie istotna w kontekście wdrażania w Wojskach Lądowych zautomatyzowanego systemu dowodzenia „SZAFRAN-ZT".

W procesie tworzenia systemów wspomagania procesów decyzyjnych istotną rolę odgrywa przygotowanie koncepcji systemu. Koncepcja zawiera informacje o przeznaczeniu i umiejscowieniu ISWPD. Na podstawie koncepcji przygotowany zostanie dokument zawierający zbiór wymagań systemowych potrzebnych do stworzenia systemu. Z analizy literatury dotyczącej niezawodności i jakości oprogramowania wiadomo, że największa ilość błędów w programach powstaje w wyniku źle przygotowanej specyfikacji wymagań systemowych[1]. Jak

[1] Patton R., „Testowanie oprogramowania", Mikom Warszawa 2002, s.31.

zatem należy zorganizować proces tworzenia specyfikacji wymagań systemowych i jakie materiały można wykorzystać w tym procesie? Część wymagań systemowych zawarta jest w dokumentach normatywnych np. w regulaminie walki. Opracowanie specyfikacji wymagań systemowych zleca się zespołowi projektowemu. W skład zespołu projektowego powinni wejść oficerowie sztabu[2] (lub sztabów) jednostek, na potrzeby których opracowywany jest system. W doborze kadry tworzącej zespół projektowy należy się kierować doświadczeniem, jakie dana osoba posiada w pracy sztabu. Przykładowo w trakcie tworzenia ISWPD na potrzeby wojsk lądowych Królestwa Danii, w składzie zespołu projektowego znaleźli się żołnierze pracujący w sztabie brygady zmechanizowanej oraz w sztabach podległych brygadzie jednostek. Ponieważ opracowywane rozwiązanie miało być eksploatowane w innych jednostkach wojsk lądowych, do współpracy zaangażowano dowództwa innych brygad, w których planowano wdrożenie systemu. Zadaniem dowództw była konsultacja przygotowanej specyfikacji wymagań systemowych. Informacje dotyczące prac zespołu projektowego były prezentowane w formie biuletynu przesyłanego do konsultantów. Konsultanci odsyłali propozycje zmian do zespołu koordynacyjnego, w skład którego weszli przedstawiciele wojsk lądowych i pracownicy firmy wykonującej system. Do zadań zespołu koordynacyjnego należała weryfikacja opinii konsultantów i przygotowanie końcowego zbioru wymagań systemowych. Dodatkowo zespół koordynacyjny odpowiadał za opracowanie strategii rozwoju i modernizacji systemu.

Na jakie zagadnienia należy zwrócić uwagę w trakcie tworzenia specyfikacji wymagań systemowych? Oprogramowanie powinno posługiwać się terminologią zgodną dokumentami normatywnymi. System powinien umożliwiać łatwe wykonanie opisu jednostek (wyposażenie jednostki, stany ludzi i sprzętu...) wchodzących w skład związku taktycznego. Zdaniem systemu jest odwzorowanie dynamiki działań, a w szczególności zmian w stanach jednostek, zmian położenia jednostek, zmian w środowisku powstałych w rezultacie prowadzonych działań. System powinien umożliwiać przetwarzanie danych rozpoznawczych, informując sztab o wiarygodności zebranych informacji.

Zebranie, przetworzenie i prezentacja danych umożliwia dowództwu ZT podejmowanie decyzji w sposób bardziej racjonalny[3], ograniczając czynnik intuicyjny w procesie decyzyjnym. Implementacja wymienionych funkcji pozwala na sprawną pracę sztabu. Dodatkowo w składzie zespołu projektowego znaleźć się powinni informatycy. Do zadań informatyków

---

[2] Szleszyński A. „ Metodyka przygotowania i wdrożenia systemu informatycznego", Zeszyty naukowe WSOW-Ląd. nr 3 Wrocław 2004.

[3] Termin na postawie „Zarządzanie. Teoria i praktyka", red. A. Koźmiński, s.95, PWN Warszawa 2004.

należy opracowanie wymagań systemowych w zakresie bezpieczeństwa danych przetwarzanych przez system. Należy pamiętać, że po wprowadzeniu danych dotyczących zasobów jednostek cały system staje się niejawny.

Należy również rozważyć kwestie związane z eksploatacją bojową i ćwiczebną ISWPD. Jest to kwestia techniczna, szczegóły której mogą nie być znane oficerom sztabu, ale którą powinni opisać informatycy wchodzący w skład zespołu. Po opracowaniu specyfikacji wymagań systemowych, należy rozważyć kwestie związane z modyfikacją funkcjonalności opracowanego rozwiązania. Pojawić się może pytanie, w jakim celu powinno się wykonywać opisaną czynność? System informatyczny będzie ulegał zmianom tak, jak zmianom będzie podlegać środowisko w którym działa ISWPD. Modyfikację pewnych wymagań wymusi eksploatacja gotowego systemu informatycznego, użytkownicy poznawszy funkcjonalność oferowaną przez ISWPD, mogą chcieć zastąpić pewne elementy systemu innymi, lepiej dopasowanymi do rzeczywistych potrzeb użytkowników. Dodatkowo rozwiązanie powinno cechować się otwartością. Otwartość systemu informatycznego należy rozumieć jako zdolność ISWPD do wymiany danych z podobnymi systemami rodzajów wojsk i służb oraz wymianę informacji z rozwiązaniami eksploatowanymi w ramach NATO.

Podsumowując przygotowane rozwiązanie ma wspomagać pracę sztabu ZT, gromadząc dane, przetwarzając je i prezentując wyniki obróbki. System musi być łatwy w obsłudze, gwarantując jednocześnie wysoki poziom bezpieczeństwa. System musi być rozwiązaniem otwartym umożliwiającym współpracę z już istniejącymi systemami podobnej klasy lub rozwiązaniami, które zostaną wdrożone. Ponadto system rozpatrywany od strony sprzętu musi umożliwiać łatwą integrację z eksploatowanym system wojskowej łączności polowej. Z tego punktu widzenia ISWPD powinien realizować wszystkie wymagania stawiane przed wojskowym system łączności polowej[4].

Na podstawie dotychczasowych rozważań widać, iż przygotowanie ISWPD jest zadaniem złożonym, w trakcie realizacji którego projektanci będą musieli godzić cechy wzajemnie sprzeczne. Konieczność zapewnienia otwartości systemu jest jedną z przyczyn złożoności[5] wielu przedsięwzięć informatycznych. Wynika to z faktu, iż projektanci systemu muszą uwzględnić różnice w formatach danych przetwarzanych przez poszczególne systemy. Istnieje możliwość zmniejszenia rozmiaru problemu kompatybilności między systemami infor-

[4] Michniak J.,"Kierowanie mobilnymi systemami łączności wojsk lądowych. Cz. 1 Główne problemy", AON Warszawa 2002, s.83 – 121.
[5] Brooks F., „Mityczny osobomiesiąc – eseje o inżynierii oprogramowania", WNT Warszawa 2000, s. 164.

matycznymi, poprzez stosowanie standardu sformatowanych wiadomości tekstowych ADATP-3.

System informatyczny integruje w sobie trzy elementy. Element oprogramowania posiadającego określoną funkcjonalność. Element technicznym, na który składają się sprzęt komputerowy i infrastruktura teleinformatyczna. Ostatnim z elementów są użytkownicy wykorzystujący ISWPD w pracy na stanowisku dowodzenia. Realizacja połączenia pomiędzy oprogramowaniem, a niezbędną infrastrukturą teleinformatyczną jest procesem złożonym. Często występującym problemem jest brak kompatybilności pomiędzy urządzeniami teleinformatycznymi (karty sieciowe, routery), sprzętem teledacyjnym (aparatownie systemu łączności). Od obsługi technicznej odpowiedzialnej za zarządzanie ISWPD wymaga się wysokich kwalifikacji związanych z zagadnieniami takimi jak tworzenie topologii sieci lokalnej SD, zarządzania kontami użytkowników, kreowania i utrzymania odpowiedniej polityki bezpieczeństwa, zarządzania serwerem bazy danych. Wskazane jest, żeby administrator ISWPD posiadał wiedzę o urządzeniach umieszczonych w aparatowni, a wykorzystywanych do transmisji danych. Z przedstawionego opisu wynika, że administratorem ISWPD powinna być osoba, która ukończyła studia politechniczne na kierunku informatyka. Do obsługi systemu Szafran przewiduje się podoficerów. Pojawić się może pytanie czy podoficer bez wymaganego wykształcenia kierunkowego poradzi sobie z realizacją wymienionych wcześniej zadań? Zakładając, że nie znajdzie się wystarczającej liczby chętnych do pracy jako dowódcy – administratorzy ISWPD, w jaki sposób zorganizować szkolenie, które przygotuje obsługi do sprawnego posługiwania się sprzętem komputerowym i oprogramowaniem?

Kolejnym problemem, jaki należy rozważyć, jest szkolenie użytkowników ISWPD. Od poziomu wyszkolenia użytkowników zależy efektywność wykorzystania ISWPD. Ponieważ system taki jest trudny w obsłudze, należy zaplanować możliwość przygotowania stanowisk pozwalających na ćwiczenie pracy z ISWPD. Wymóg ten może wydać się irracjonalny w kontekście wcześniej umieszczonego stwierdzenia zakładającego konieczność szkolenia użytkowników systemu. Doświadczenia pokazują, że w przypadku długotrwałego nie korzystania z ISWPD, użytkownicy zapominają jak można efektywnie korzystać z systemu.

Rozwiązaniem opisanego problemu mogłoby być przygotowanie sieci lokalnej na terenie jednostki wojskowej, zarządzanej przez administratora systemu, przy wykorzystaniu której kadra mogłaby ćwiczyć pracę z systemem. Rozwiązanie to pozwala również administratorowi na ćwiczenie procedur związanych z sytuacjami awaryjnymi, jakie mogą wystąpić w czasie pracy ISWPD. Dzięki proponowanemu rozwiązaniu możliwe będzie przygotowania danych wykorzystywanych w trakcie treningów i ćwiczeń poligonowych przy zachowaniu danych

rzeczywistych do wykorzystania w przypadku pracy bojowej. Wadą proponowanego rozwiązania jest wysoki koszt, proponowane rozwiązanie należałoby wdrożyć w wielu jednostkach wojskowych.

Alternatywą dla proponowanego rozwiązania mogło być utworzenie centrów szkoleniowych na bazie Akademii Obrony Narodowej, Wyższej Szkoły Oficerskiej Wojsk Lądowych i Centrum Szkolenia Łączności i Informatyki. Centra prowadziłyby szkolenia dla użytkowników i administratorów ISWPD. Koszt utworzenia centrów byłby niższy, jednak wdrożenie rozwiązania wymagać będzie oddelegowania grupy żołnierzy celem odbycia przeszkolenia. Pojawić się musi pytanie, jak często powinno się doszkalać obsługi ISWPD? Czy wystarczy przeprowadzać szkolenie np. tydzień przed ćwiczeniami, w trakcie których zamierza się korzystać z ISWPD, czy może robić je cyklicznie np. 3 lub 4 razy w ciągu roku?
Opisane kwestie stanowią problem organizacyjny, który można rozwiązać, bazując na potrzebach zgłaszanych przez jednostki wojskowe. Należy jednak zwrócić uwagę na fakt, że użytkownicy i administratorzy nie będą mogli szkolić się w tym samym czasie. Administrator systemu pracujący w centrum szkolenia posiada inne polityki bezpieczeństwa niż administrator w jednostce. Praca w różnych zespołach może być później przyczyną powstawania konfliktów pomiędzy zespołem sztabowców, a administratorem systemu.

Jaką zatem rolę powinny pełnić wymienione wcześniej centra szkolenia? Do zadań centrów należałoby szkolenie początkowe użytkowników wymagające wprowadzenia w tło taktyczne oraz zapoznania ze strukturą i możliwościami ISWPD. Dzięki posiadanemu wyposażeniu i wiedzy przeprowadzano by szkolenie symulacyjne z wykorzystaniem ISPWD. Centra powinny się zająć wspomaganiem prac dotyczących eksploatacji i modernizacji systemu. Ponieważ modernizacje sprzętu oprogramowania będą konieczne, pojawi się potrzeba utworzenia centrum koordynacyjnego na bazie np. Dowództwa Wojsk Lądowych. Ośrodki szkolenia we współpracy z jednostkami stanowiłyby organ konsultacyjno – doradczy dla centrum koordynacyjnego.

Rolą centrów powinno być przygotowanie materiałów służących do szkolenia w jednostkach. Materiały byłyby adresowane do różnych grup użytkowników (osoby korzystające z systemu, administratorzy systemu). Materiały szkoleniowe mogłyby być dystrybuowane na płytach CD-ROM lub za pomocą sieci MIL-WAN. Wykorzystanie technik internetowych umożliwiłoby przygotowanie i uruchomienie portalu dla użytkowników i administratorów systemu służącego wymianie doświadczeń.

Proces opracowania, wdrożenia ISWPD jest złożony i trudny. Przygotowanie odpowiedniego haromonogramu prac, dobór ludzi odpowiedzialnych za przygotowanie koncepcji i specyfikacji wymagań systemowych oraz system szkolenia użytkowników i administratorów może zagwarantować, że ISWPD będzie wspomagał pracę sztabu, a nie będzie ją dezorganizował. Wysiłek włożony w odpowiednie przygotowanie i planowanie wspólnych treningów z systemem łączności doprowadzi do powstania rozwiązania, które zwiększy efektywność działania sztabu ZT, bez konieczności zwiększania obsady etatowej. Szczególną uwagę należy zwrócić na organizację procesu szkolenia użytkowników i administratorów, od poziomu posiadanej przez te osoby wiedzy zależeć będzie sprawne działanie systemu rozpatrywanego jako całość.

Bibliografia:

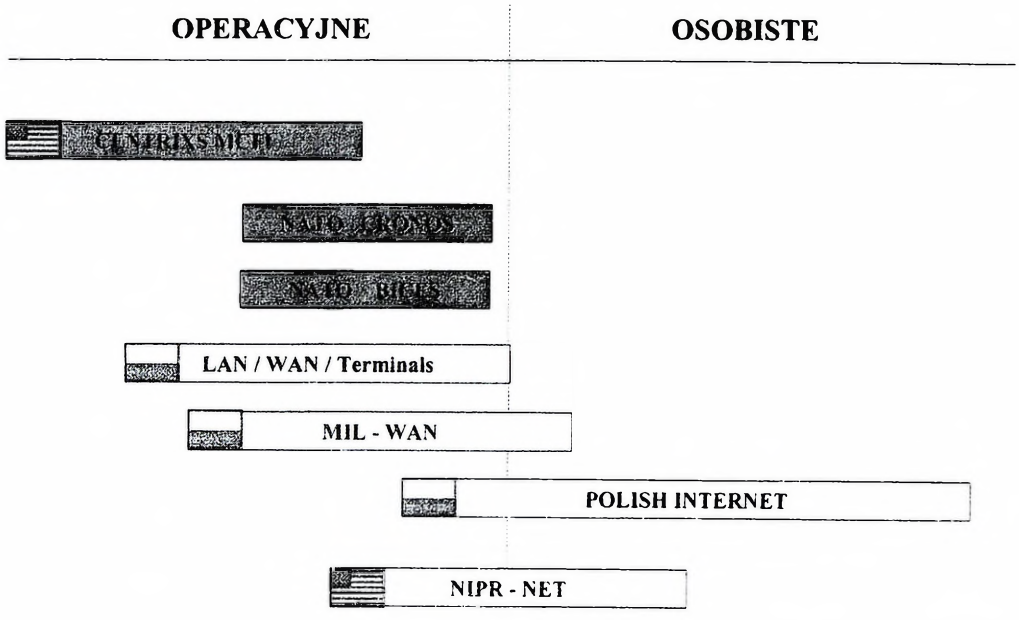
1. Adaczewski P., „Zintegrowane systemy informatyczne", Mikom Warszawa 2004.
3. Brooks F., „Mityczny osobomiesiąc – eseje o inżynierii oprogramowania", WNT Warszawa 2000.
4. Hunt A., Thomas D., „Pragmatyczny programista. Od czeladnika do mistrza", WNT Warszawa 2002.
5. Leffingwell D., Widrig D., „Zarządzanie wymaganiami", WNT Warszawa 2003.
6. Michniak J., „Kierowanie mobilnymi systemami łączności wojsk lądowych. Cz. I. Główne problemy" AON Warszawa 2002.
7. Patton R., „Testowanie oprogramowania", Mikom Warszawa 2002.
8. Phillips J., „Zarządzanie projektami IT", OnePress Gliwice 2004.
9. Szleszyński A., „Projektowanie systemów informatycznych. Dlaczego to nie zawsze się udaje?", Zeszyty Naukowe WSOWLąd. 1/2003.
10. Szleszyński A., „Metodyka przygotowania wdrożenia systemu informatycznego w Wyższej Szkole Oficerskiej Wojsk Lądowych", Zeszyty Naukowe WSOWLąd. 3/2004.

Wybrane problemy funkcjonowania sieci teleinformatycznej PKW w Iraku

mgr inż. Grzegorz PILARSKI
16 Dywizja Zmechanizowana

W dobie szerokiej koniecznej współpracy struktur militarnych NATO, a głównie Stanów Zjednoczonych, z innymi państwami podejmującymi wyzwanie walki z zagrożeniami XXI wieku takimi jak terroryzm, niekontrolowana produkcja broni masowego rażenia, jak również rozwiązywanie konfliktów lokalnych istnieje konieczność budowy integralnych globalnych systemów teleinformatycznych. Powstanie takich systemów umożliwi sprawny przepływ informacji według jednolitych standardów. Udział Polskiego Kontyngentu Wojskowego w misji stabilizacyjnej w Iraku stworzył możliwość stronie polskiej współuczestniczenia w eksploatowaniu oraz zarządzaniu przez oficerów informatyki regionalnym koalicyjnym systemem teleinformatycznym CENTRIXS MCFI (ang. *Combined Enterprise Regional Information Exchange System Multinational Coalition Forces Iraq*) we własnej strefie odpowiedzialności. Oprócz tego systemu PKW w Iraku bazuje na następującym wsparciu teleinformatycznym:

- informatyczna sieć NATO – CRONOS i BICES;
- informatyczna sieć dowodzenia LAN / WAN;
- informatyczna sieć operacyjna MIL - WAN;
- informatyczna sieć internetowa POLISH INTERNET;
- informatyczna sieć internetowa NIPR - NET.



Rysunek 1. Obszary działania sieci informatycznych w MND CS
Źródło: Opracowanie własne na podstawie analizy sieci funkcjonujących w PKW Irak.

Działanie tych sieci można umiejscowić na dwóch płaszczyznach, operacyjnej oraz osobistej, co zilustrowane jest na powyższym rysunku.

CENTRIXS MCFI – stacjonarna tajna sieć dla koalicjantów w działaniach międzynarodowych w Iraku. Podstawowym zadaniem sieci CENTRIXS jest wsparcie zabezpieczenia wymiany informacji operacyjnych i wywiadowczych poprzez niezawodną komunikację, przetwarzanie danych oraz zautomatyzowane procesy dowodzenia.

Sieć ta została stworzona w celu sprostania wymogom USA nałożonym na międzynarodowe sieci wymiany informacji. Sieci CENTRIXS są połączeniem globalnych, wielostronnych i dwustronnych, wirtualnie odrębnych sieci wspierających międzynarodowe działania np. operacja Iracka wolność OIF (ang. *Operation Iraqi Freedom*) czy globalna wojna z terroryzmem GWOT (ang. *Global War on Terrorism*). Sieci te tworzą szkielet czegoś co ma się stać globalną infrastrukturą pozwalającą Stanom Zjednoczonym na szybką wymianę informacji z wojskami koalicji na całym świecie, wspierając lokalne, regionalne oraz globalne operacje wojskowe. Dostawcą usług w tej sieci jest zarówno rząd jak również instytucje cywilne co pozwala na redukcję kosztów i zapewnienie implementacji nowoczesnych i niezawodnych rozwiązań komunikacyjnych. Sieć teleinformatyczna CENTRIXS charakteryzuje się przede wszystkim takimi cechami jak: globalizacja, interoperacyjność, ekonomiczność oraz łatwość zarządzania i obsługi.

Globalizacja i interoperacyjność odzwierciedla się w możliwości płynnej wymiany informacji pomiędzy różnymi agencjami rządowymi a koalicjantami. Ekonomiczność oznacza, iż nawet kraje z ograniczonym budżetem mają możliwość współużytkowania tej sieci. Łatwość zarządzania oraz eksploatacji sieci stanowi atut w połączonych operacjach międzynarodowych przeprowadzanych na różnych obszarach, często nieprzyjaznych pod względem klimatycznym, a także politycznym. Implementacja skutecznych oraz łatwych w obsłudze elementów kryptograficznych (KG-175 TACLANE i KIV-7) zaakceptowanych przez NSA (ang. *National Security Agency*) przy zastosowaniu łączności satelitarnej umożliwia bezpieczną wymianę informacji na duże odległości.

Usługi w CENTRIXS obejmują:

- stałą obserwację sytuacji na polu walki;
- możliwość stałej wymiany informacji wywiadowczych;
- wymianę poczty elektronicznej;
- dostępność usług sieciowych oraz serwisu informacyjnego;
- możliwość komunikacji poprzez komunikatory;
- VoIP (ang. *Voice over Secure Internet Protocol*) technologia, której głównym założeniem jest integracja ruchu telefonicznego z transmisją danych.

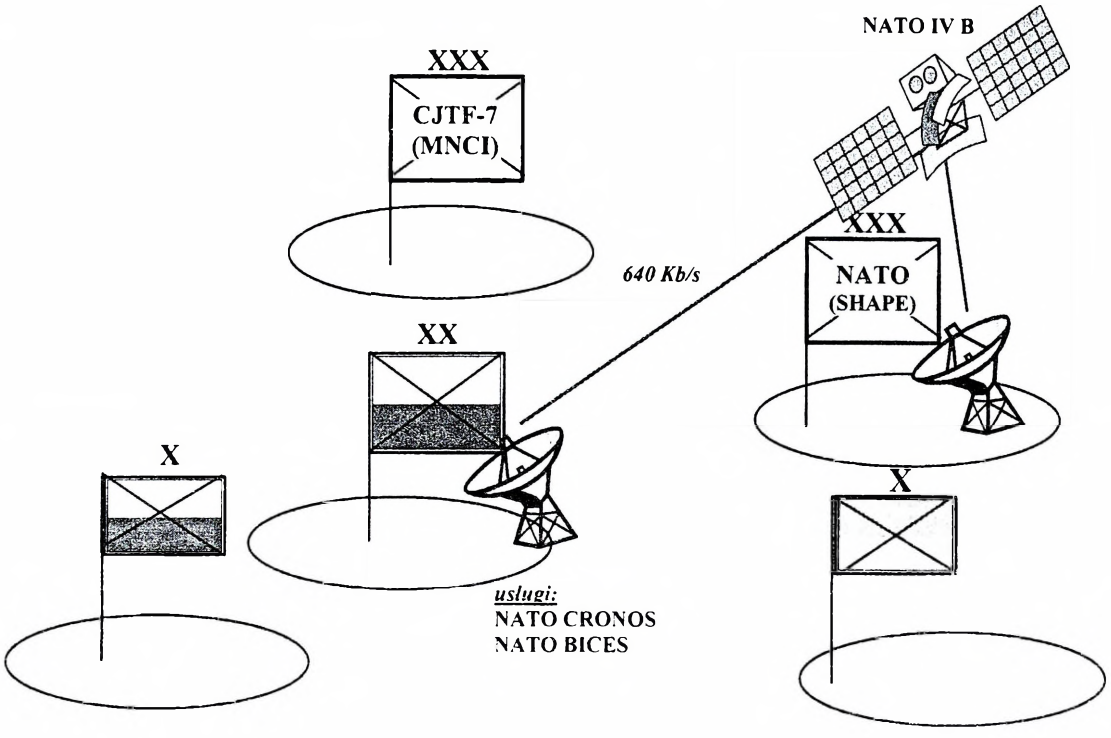
CENTRIXS MCFI jest wiodącą siecią wymiany danych w Iraku. Początkowo główne obciążenie stanowiła komunikacja w sieci LAN / WAN, ze względu na znaczne pokrycie obszaru działań. Jednakże rozbudowa tajnej sieci koalicyjnej (stymulowana przez stronę polską), umożliwiła dostęp dla podwładnych niższego szczebla (bataliony), podnosząc tym samym znacznie swoją rangę. Największy rozwój sieci CENTRIXS można było zaobserwować w czasie III zmiany PKW Irak, dlatego też sieć ta stała się głównym środkiem wymiany danych operacyjnych z podwładnymi. Łączność z przełożonym CJTF-7 (ang. *Combined Joint Task Forces 7* – Wielonarodowe Połączone Siły Operacyjne), od 1.07.2004 Wielonarodowy Korpus Irak MNCI (ang. *Multinational Corps Iraq*), od początku misji odbywała się poprzez sieć CENTRIXS oraz NIPR-NET.

Na bazie sieci teleinformatycznej CENTRIXS zostały zaimplementowane aplikacje, które wspomagały proces dowodzenia. Przykładem tego typu programu jest C2PC (ang. *Command Control Personal Computer*) system wspomagania kierowania i dowodzenia. Aplikacja ta jest dostępna tylko dla grona osób funkcyjnych posiadających dostęp do pracy w tym systemie, który umożliwia zorientowanie się w aktualnej sytuacji bojowej. Tło operacyjne stanowią mapy cyfrowe zainstalowane u użytkownika, natomiast lokalizacja

położenia obiektów odbywa się poprzez naniesienie siatki danych pochodzących z serwera na którym dane te są aktualizowane. Program ten jest bardzo pomocny przede wszystkim dla grupy oficerów pracujących w TOC-u (ang. *Tactical Operation Center*), gdzie niezbędna jest informacja na temat ruchu i położenia wojsk.

Kolejną aplikacją wspomagającą jest IWS (ang. *Info Work Space*) system komunikacji interpersonalnej. Struktura tego systemu oparta jest na wirtualnych platformach budynków z segregacją pięter (poziomów) oraz pokoi. W tych pokojach mogą się spotykać osoby posiadające dostępu do określonych pomieszczeń. Przykładem tego mogą być odprawy dowódcy z przełożonym gdzie do pokoju, w którym odbywa się rozmowa nie ma dostępu nikt poza zainteresowanymi. Przejrzystość budynków pozwala użytkownikowi na zorientowanie się w ilości osób znajdujących się w danym pokoju. Aplikacja jest swego rodzaju programem do „czatowania" oraz rozmów głosowych. Użytkownik ma wiele możliwości korzystania z tego systemu, a dostępny interfejs graficzny ułatwia i zachęca do pracy z tym programem. Dodatkowym atutem tej aplikacji jest fakt, iż odprawy i spotkania można przeprowadzać równocześnie w kilku lokalizacjach bez konieczności opuszczania stanowiska pracy.

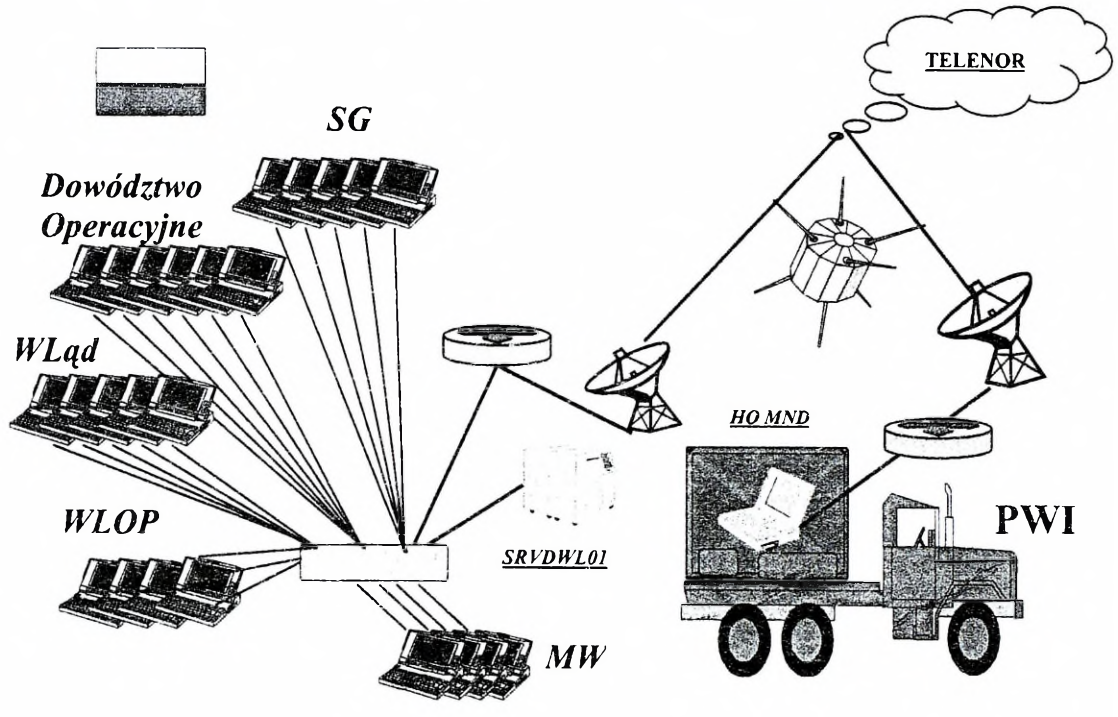
CRONOS (ang. *Crisis Reaction of NATO Open System network*) sieć systemu reagowania kryzysowego sojuszników NATO oraz **BICES** (ang. *Battlefield Information Collection and Exploitation System*) system zbierania i wykorzystywania informacji pola walki. Węzeł łączności NATO MCM (ang. *Mobile Communication Module*) zainstalowany na terenie bazy Camp Alfa w Babilonie, po relokacji w Camp Echo w Diwaniji, umożliwiał państwom należącym do sojuszu korzystanie z zasobów sieciowych NATO. Organizacja łączności, przywiązania wydzielonego węzła, odbywała się za pomocą łączności satelitarnej w kierunku bazy znajdującej się w Europie.



Rysunek 2. Poglądowy schemat organizacja łączności systemu NATO CRONOS i BICES
Źródło: Opracowanie własne na podstawie analizy wariantów funkcjonowania sieci sojuszniczych NATO

LAN / WAN (ang. *Local Area Network / Wide Area Network)* narodowy system złożony z połączonych ze sobą lokalnych sieci informatycznych tworzył sieć rozległą. Sieć WAN stanowiła podstawowe medium transmisji danych do wszystkich komponentów rozmieszczonych w strefie odpowiedzialności AOR (ang. *Area of Responsibility*). Głównym zadaniem tego systemu było umożliwienie Dowództwu Dywizji MND CS przekazywanie rozkazów oraz wymianę danych w systemie meldunkowym z podległymi komponentami. Sieć ta funkcjonowała do połowy III zmiany PKW Irak, a po relokacji funkcję wymiany informacji przejęła sieć CENTRIXS MCFI. Ze względu na skumulowanie elementów kontyngentu PKW Irak oraz ograniczenia w przepływności systemu łączności Dowództwa MND CS z pozostałymi bazami podjęto decyzję o likwidacji sieci WAN. Jednakże z uwagi na zabezpieczenie wymiany informacji pomiędzy komórkami pracującymi w systemie narodowym sieci lokalne LAN nadal funkcjonują. Budowa tego systemu oparta była na narodowej infrastrukturze telekomunikacyjnej znanej pod nazwą MPCŁU – Mobilnego Podsystemu Cyfrowej Łączności Utajnionej.

MIL – WAN (ang. *Military World Area Network*) resortowy system wymiany informacji na terenie Polski. Sieć ta umożliwia komunikację dowództwa MND CS z przełożonym w kraju. Dane operacyjne nie mogą być przesyłane siecią Internet, dlatego też sieć MIL - WAN jest wykorzystywana do tego celu. Do relokacji istniało jedno stanowisko komputerowe pracujące w tej sieci umiejscowione na PWI – Polowy Węzeł Informatyczny, natomiast w Camp Echo rola tego medium transmisji wzrosła co skutkowało przyłączeniem kilku dodatkowych stanowisk komputerowych do dyspozycji komórek operacyjnych.



Rysunek 3. Poglądowy schemat organizacja łączności systemu MIL-WAN
Źródło: Opracowanie własne na podstawie analizy wariantów funkcjonowania sieci MIL-WAN

Wymiana informacji dotyczyła nie tylko kontaktów z dowództwem Sił Zbrojnych w kraju, ale istniała możliwość komunikacji z dowolnym użytkownikiem w kraju posiadającym konto w resortowej sieci. Udogodnienie to pozwoliło na komunikację poszczególnych osób funkcyjnych z współpracownikami znajdującymi się w Polsce i przekazywanie między nimi niezbędnych informacji operacyjnych.

POLISH INTERNET jest to sieć internetowa na zamówienie Ministerstwa Obrony Narodowej, która stanowi podstawowe medium do komunikacji żołnierzy z rodzinami w kraju. Jednakże rola tej sieci na tym się nie kończy, gdyż stanowi ona nieodzowne źródło

informacji oraz możliwość współpracy cywilno – wojskowej z organami administracji rządowej oraz inwestorami. Trudno byłoby sobie wyobrazić realizację projektów infrastrukturalnych bez możliwości komunikacji, jaką zapewnia otwarta się internetowa. Sieć ta stanowi podstawowe źródło informacji oraz narzędzie pracy dla komórki CIMIC (ang. *Civil-And Military Cooperation*). Podstawowe założenie, jakim było rozwinięcie sieci w każdej lokalizacji w zależności od rozśrodkowania okazało się trafną decyzją. Możliwość kontaktu żołnierzy z rodzinami za pośrednictwem kawiarenek internetowych w każdej bazie, znacznie podnosi morale i pozwala przetrwać trudne momenty służby na misji. Największe zastosowanie w sieci ma przesyłanie poczty elektronicznej (przeważnie przesyłanie zdjęć) oraz zastosowanie różnego rodzaju aplikacji peer to peer oraz komunikatorów. W sferze operacyjnej stanowi ona nieodzowne źródło informacji kulturowej, geopolitycznej czy gospodarczej.

NIPR-NET (ang. *Non Secure Internet Protocol Router Net*) amerykańska sieć intranetowa z dostępem do globalnej sieci internetowej. Sieć ta funkcjonuje tylko w Dowództwie MND CS (ang. *Multinational Division Center South*), co stanowi ukłon ze strony władz amerykańskich, które udostępniły możliwość korzystania z tego środka wymiany informacji. Sieć ta została stworzona przez agencję DISA (ang. *Defense Information Systems Agency*) jako jawny serwis informacyjny Armii USA z dostępem do Internetu. Struktura sieci oparta jest na routerach brzegowych, stanowiących bramę między globalną siecią a wewnętrznym serwisem informacyjnym, która zabezpiecza dostęp do zasobów sieci intranetowej przed hackerami, obcymi siłami zbrojnymi, terrorystami, itp.

Routery brzegowe obsługiwane są przez pracowników armii amerykańskiej, których zadaniem jest filtracja sieci intranetowej przed upływem informacji operacyjnych (tajnych), a także obecności w sieci treści pornograficznych. Nie dozwolone jest także korzystanie z oprogramowania peer to peer co jest konsekwentnie wychwytywane przez amerykańską komórkę bezpieczeństwa. Osoba, „złapana" na złamaniu jakiejkolwiek z ustalonych zasad automatycznie pozbawiana jest możliwości pracy w tej sieci na czas określony albo bezterminowo. Za przykład może posłużyć sytuacja, w której pełnoprawny użytkownik sieci udostępnił swoje konto osobie niepowołanej, która przesłała informacje tajne informacje operacyjne do przełożonego, w konsekwencji czego konto zostało zablokowane a wobec tych dwóch osób oraz przełożonego wszczęto postępowanie wyjaśniające. W innym przypadku wychwycono w sieci przeglądanie treści pornograficznych co w konsekwencji przyczyniło się aresz-

towaniem komputera na miesiąc, oraz skasowaniem wszystkich danych znajdujących się na dysku twardym.

Problemy i wnioski

Zadanie przed jakim stanęła Polska w misji pokojowej w Iraku stanowi wielkie wyzwanie, ogrom przedsięwzięć jakie należało wykonać aby połączyć ze sobą wszystkie bazy wymagało i wymaga od kadry informatycznej dużej wiedzy o technologiach sieciowych i informatycznych oraz wielkiego zaangażowania. Należy podkreślić, że działanie na gruncie współpracy międzynarodowej, a także w niesprzyjających warunkach środowiskowych bez znaczącego wsparcia ze strony narodowego systemu jest zadaniem bardzo trudnym. Jednakże ta sfera działalności jest do tego momentu realizowana w stopniu zadawalającym.

Tak złożone zadanie nie obyło się bez problemów a niejednokrotnie pewnego rodzaju konfliktów na gruncie współpracy międzynarodowej. Dlatego też, ważnym czynnikiem charakteryzującym kadrę informatyczną jest zdolność do negocjacji, cierpliwość, a także gotowość do kompromisów.

Zabezpieczenie teleinformatyczne na współczesnym polu walki odgrywa wielkie znaczenie, niezawodność systemu a raczej jej brak może wpływać na zagrożenie życia ludzkiego. Dlatego też, kadra informatyczna dobierana do tego rodzaju misji powinna się cechować szeroką znajomością zagadnień teleinformatycznych na gruncie cywilnym, znajomością systemów narodowych oraz posiadać doświadczenie w pracy z systemami koalicjantów.

Ważnym zagadnieniem jest naliczanie osobowe do stawianych zadań. Trudno sobie wyobrazić aby raptem trzy osoby (w tym pracownik amerykański) zajmowały się administrowaniem sieci lokalnej i rozległej, oraz tzw. „help deskiem" (bezpośrednia pomoc użytkownikowi), głównej sieci wymiany danych złożonej z ok. 150 stacji roboczych rozmieszczonych na znacznym obszarze. Zrozumiałym jest fakt, iż w przypadku zmniejszania liczby sił w misji należy ograniczyć stan osobowy, ale z drugiej strony nie można dopuścić do sytuacji gdzie system od którego niejednokrotnie zależy ludzkie życie może być narażony na awarię z powodu braków kadrowych.

Doświadczenia z tej misji do tej pory dowodzą, że w dzisiejszej dobie system teleinformatyczny jest bardzo istotny i należy zwrócić szczególną uwagę na jego bezpieczeństwo.

Przy planowaniu redukcji etatów należy wziąć pod uwagę prognozy przełożonych (MNCI), co miało miejsce w III zmianie PKW w Iraku, gdzie podczas jej trwania zapadła decyzja o relokacji baz Alfa, Lima, Kilo, Juliet do bazy Echo. W wydziale systemów informatycznych MND CS przy przejściu z II na III zmianę zapadła decyzja redukcji etatu specja-

listy informatyka, co znacznie utrudniło wykonanie zadania związanego z relokacją. Należy także brać pod uwagę przypadki losowe – choroba, śmierć – odnośnie kadry informatycznej. Nie odpowiednie planowanie osobowe może w takim przypadku spowodować wielkie zagrożenie dla uczestników misji.

Głównym zadaniem wydziału systemów informatycznych jest zabezpieczenie sprawnego funkcjonowania sieci teleinformatycznych na obszarze działania misji oraz współpraca międzynarodowa w zakresie administrowania oraz wsparcia logistycznego.

Nie trzeba chyba podkreślać, że znajomość jeżyka angielskiego na jak najwyższym poziomie jest niezbędnym elementem funkcjonowania podczas misji a w szczególności wykonywania zadań związanych z zabezpieczeniem informatycznym. „Help desk" jak również wspólne administrowanie systemem wymaga precyzji w wypowiadaniu się oraz rozumienia potrzeb i problemów.

Podczas realizacji zagadnienia dotyczącego funkcjonowania sieci pojawiły się różne problemy. Jednym z nich jest destrukcyjny wpływ warunków klimatycznych w postaci wysokiej temperatury, piasku przedostającego się do układów chłodzących na poprawne działanie sprzętu informatycznego, czego obrazem są częste awarie komputerów i urządzeń aktywnych sieci. Brak profesjonalnego warsztatu naprawczego oraz personelu zabezpieczającego uniemożliwia skuteczną naprawę uszkodzonego sprzętu, co wiąże się z malejącą liczbą funkcjonującego sprzętu informatycznego. Wniosek nasuwa się jeden, przy braku zaplecza naprawy sprzętu należy zapewnić sprawnie działający logistyczny system zaopatrywania. Jeśli takiego nie ma to poprawne funkcjonowanie systemu informatycznego może być zagrożone. Przykładem tego może być sytuacja switcha spinającego 23 stanowiska komputerowe, który ulega uszkodzeniu i w przypadku braku zapasu konsekwencją jest brak możliwości pracy tych stacji w sieci, a co za tym idzie brak możliwości wymiany danych z przełożonym i podwładnymi.

Kolejnym problemem jest awaryjność sieci i jej naprawa. Aby sprawnie i szybko zadziałać na uszkodzenie systemu niezbędna jest wiedza o budowie strukturalnej funkcjonującej sieci. Bardzo ważna jest szczegółowa i kompletna dokumentacja, która umożliwi w szybki i łatwy sposób zlokalizowanie awarii wykrytej przez system zarządzania i monitoringu sieci. Plany budowy sieci powinny być na tyle czytelne i zrozumiałe, aby osoba która po raz pierwszy się z nimi zapoznaje miała czytelny obraz stanu rzeczy.

W sieciach stacjonarnych przewodowych ważnym elementem jest umiejętne rozmieszczenie infrastruktury sieciowej – zabezpieczenie przed warunkami atmosferycznymi (ulewami), uszkodzeniami mechanicznymi – oraz szczegółowy opis okablowania. Pośpiech, brak planu rozwinięcia sieci teleinformatycznej skutkuje w dłuższym czasie jej eksploatowa-

nia częstymi awariami i trudnością w lokalizacji uszkodzenia. Przy rozwijaniu sieci jawnej i niejawnej celowym jest wykorzystywanie różnych kolorów kabla do rożnych systemów. Pozwala to na uniknięcie bezpośredniej pomyłki połączenia obu sieci ze sobą.

Istotnym problemem jest również zabezpieczenie energetyczne sieci komputerowych. Ważnym elementem jest budowa wydzielonej sieci energetycznej, która gwarantuje stabilną pracę urządzeń elektronicznych bez skoków napięcia i przepięć co może doprowadzić do uszkodzenia poszczególnych stacji roboczych. Niezbędne z punktu widzenia niezawodności systemu jest zasilanie awaryjne aktywnych elementów sieci.

W planowaniu budowy sieci ważnym elementem jest poprawna organizacja funkcjonowania sieci rozległej. Należy zwrócić uwagę na zabezpieczenie pracy w sieci lokalnej w przypadku awarii łączności radioliniowej na łączach rozległych (wanowskich). Struktura domenowa powinna być tak zaplanowana, aby wymiana informacji w sieciach lokalnych była możliwa do momentu naprawy sieci WAN. Dlatego też, dla sieci LAN / WAN korzystne jest zastosowanie wariantu zaufania domen. Zaletą tego rozwiązania jest brak wymiany informacji *Active Directory* w systemie operacyjnym MS Windows Serwer, co przy wariancie niestabilnej łączności rozległej pozwala na bezawaryjną pracę sieci lokalnych oraz zbieranie informacji wychodzących na serwerze do czasu poprawnego działania systemu łączności radioliniowej. Wadą natomiast są trudności w implementacji skrzynki adresowej.

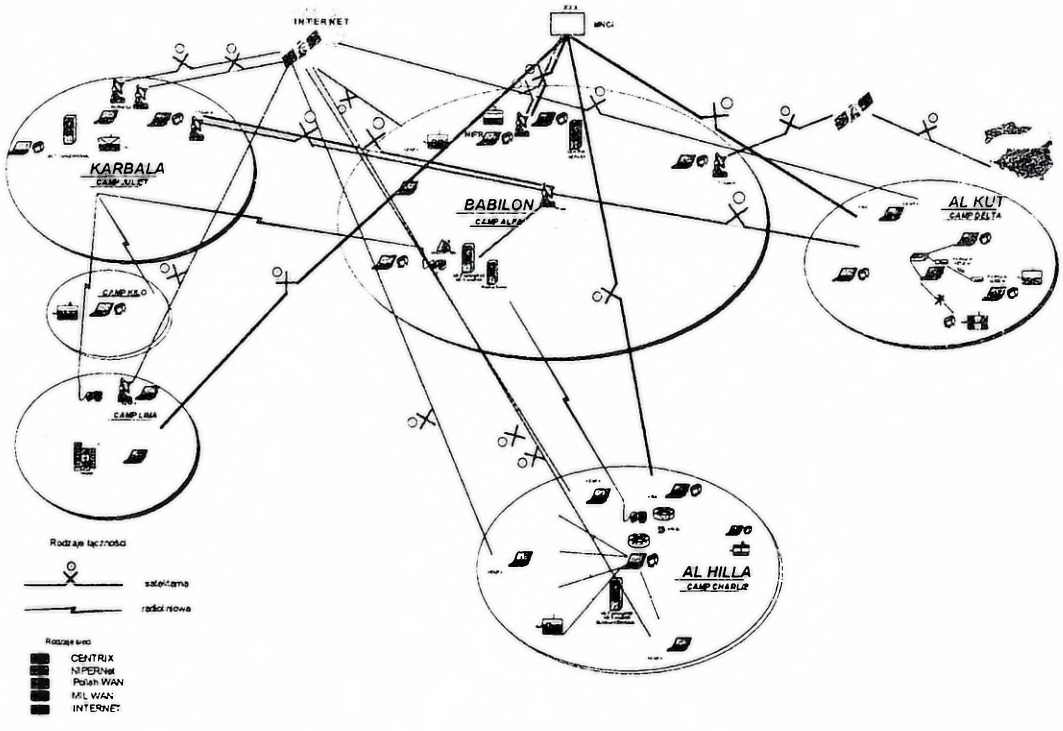
Kolejnym problemem na który należy zwrócić uwagę, jest odpowiedni dobór firm dostarczających usługi internetowe. Na przełomie I ÷ III zmiany nagminnie zdarzały się problemy w poprawnym funkcjonowaniu usług internetowych, co skutkowało niezadowoleniem ze strony żołnierzy w kontaktach z rodzinami w kraju. Zamówienie na dostawę usług internetowych powinno być jasno określone z zaznaczeniem specyfikacji QoS (ang. *Quality of Service*) oraz minimalnej przepływności CIR (ang. *Committed Information Rate*). Należy również określić i egzekwować restrykcje w przypadku niedotrzymania warunków umowy pod groźbą wysokich kar finansowych, a także rozwiązania umowy w trybie natychmiastowym.

Istotnym problemem są zagadnienia związane z bezpieczeństwem teleinformatycznym. Kadra udająca się na misję powinna mieć pojęcie o zagrożeniach jakie niesie ze sobą nie przestrzeganie przepisów o ochronie informacji niejawnych. Trudnym zagadnieniem nękającym personel bezpieczeństwa jest stosowanie przez użytkowników pamięci zewnętrznej tzw. *memory flash* (pot. stick). Problem związany z wyłapaniem łamania przepisów, poprzez stosowanie tej pamięci w sieci jawnej i niejawnej stwarza wielkie zagrożenie, jest trudny do realizacji. Zachowanie to stwarza możliwość upływu informacji niejawnych, a także infekcji

zamkniętej sieci niejawnej. Taki przypadek miał miejsce na III zmianie, co skutkowało awarią sieci CENTRIXS oraz kilkugodzinną przerwą w funkcjonowaniu. Takie zachowanie jest niedopuszczalne i powinno być surowo karane. Filtracja sieci amerykańskich jest na tyle skuteczna, iż wykrywane były przypadki posiadania nielegalnego oprogramowania (np. *virus maker*, *Trojan*, itd.), a także treści pornograficznych (NIPR - NET).

Przestrzeganie przepisów dotyczących informacji niejawnych w warunkach bojowych jest niejednokrotnie trudne do zrealizowania. Dlatego też, pewne procedury na wypadek misji zagranicznych powinny być uproszczone. Przykładem może być dokument dopuszczający do wytwarzania, przechowywania i przetwarzania informacji niejawnych w systemie informatycznym – Szczególne Wymagania Bezpieczeństwa na System (SWBS) i Procedury Bezpiecznej Eksploatacji (PBE), które to dokumenty zostały opracowane i przesłane do akceptacji w czasie I zmiany, a podczas III zmiany wróciły do poprawki (kiedy praktycznie system już nie funkcjonował).

Ważnym zagadnieniem jakie miało miejsce w III zmianie PKW w Iraku była relokacja. Poniższy schemat przedstawia poglądową strukturę systemów teleinformatycznych wykorzystywanych w czasie misji.



Rysunek 4. Poglądowy schemat sieci teleinformatycznych przed relokacją
Źródło: Opracowanie własne na podstawie analizy wariantów wymiany danych w Iraku

W fazie przygotowania do relokacji należało odpowiedzieć sobie na kilka nurtujących pytań takich jak:

W jaki sposób zabezpieczyć transmisję danych w bazie funkcjonującej i rozwijanej?

W jakiej kolejności przenosić poszczególne sieci i elementy aktywne?

W jaki sposób naliczać środki informatyczne na funkcjonujące zespoły z uwzględnieniem zabezpieczenia informatycznego dla stanu osobowego obecnej zmiany oraz zmniejszonej IV?

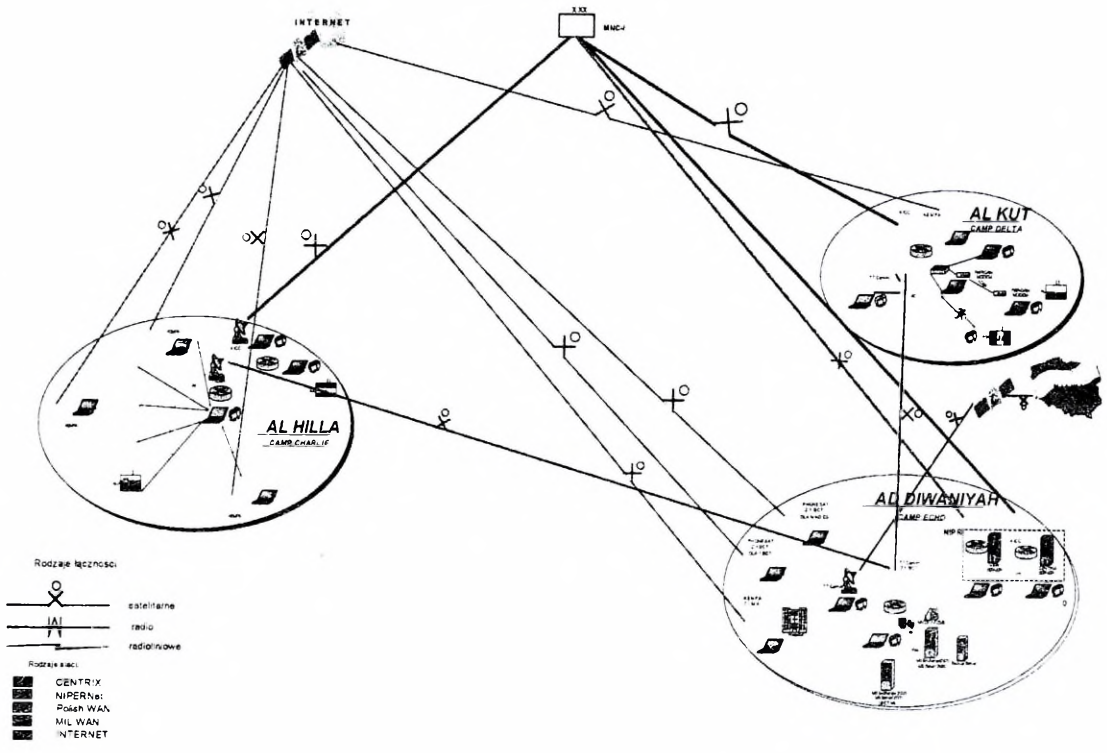
W jaki sposób zabezpieczyć dane, konta pocztowe na czas przemieszczenia poszczególnych osób funkcyjnych?

To tylko nieliczne pytania, jakie pojawiły się w czasie przemieszczenia.

W wyniku długotrwałej eksploatacji w ekstremalnych warunkach klimatycznych i w niesprzyjających warunkach lokalowych, sprzęt informatyczny ulegał częstym awariom. Zdarzały się sytuacje, że sprzęt funkcjonował dobrze a kiedy nastąpiło jego przeniesienie i powtórne uruchomienie okazywało się że już jest niesprawny. Takie sytuacje często miały miejsce. Niestety problem jaki się pojawił odnośnie rozliczenia sprzętu za I i II zmianę skutkował embargiem dostaw ze strony amerykańskiej. Dlatego też, istotnym zagadnieniem jest szczegółowe rozliczanie osób kończących misję oraz czytelna ewidencja środków informatycznych. Problemy z dostawą nowego sprzętu z kraju związane z procedurami przetargowymi na zakup sprzętu informatycznego pogłębiały i tak już trudną sytuację w czasie relokacji. Wskazane jest, aby procedury zaopatrywania w sprzęt na potrzeby misji prowadzonych poza granicami kraju były zmodyfikowane tak aby, możliwy był zakup niezbędnego wyposażenia z uwagi na wykonywane działania. Trudno jest planować w działaniach bojowych z wyprzedzeniem rocznym jeśli sytuacja w czasie misji zmienia się dynamicznie.

Kolejnym problemem jaki napotkano był brak danych związanych z naliczeniem sprzętu informatycznego na poszczególne komórki organizacyjne adekwatnie do naliczeń osobowych i rodzaju przeprowadzonych działań. Dodatkową trudność sprawił brak informacji o strukturze etatowej IV zmiany, wiadomo było tylko że będzie mniejsza.

Stan informatyki po relokacji został ograniczony z uwagi na przyszłe działania kolejnej zmiany, a także z przyczyn niezależnych związanych z uszkodzeniami sprzętu w wyniku długotrwałej pracy i oddziaływania warunków klimatycznych. Poniższy schemat przedstawia jeden z wariantów rozpatrywanych w czasie planowania funkcjonowania systemów teleinformatycznych.



Rysunek 5. Poglądowy schemat sieci teleinformatycznych po relokacji
Źródło: Opracowanie własne na podstawie analizy wariantów wymiany danych w Iraku

Posumowanie

Strategiczną platformą na bazie której opiera się łączność i transmisja danych podczas pełnienia misji pokojowej w Iraku jest system satelitarny, który umożliwia połączenie baz stacjonujących w rejonie odpowiedzialności Dywizji MND CS oraz kontakt z krajem.

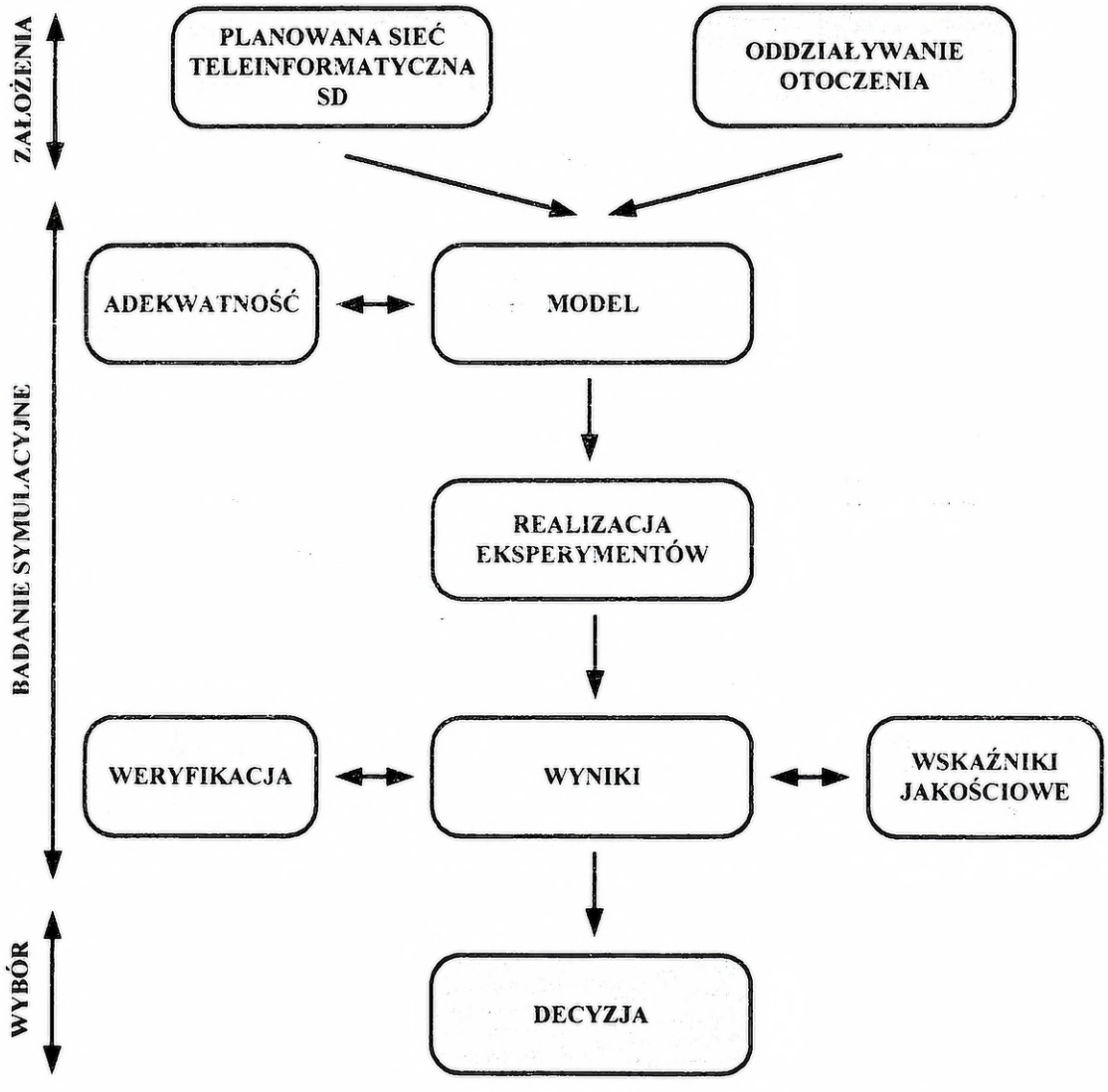
Bazując na powyższym stwierdzeniu wskazane wydaje się wprowadzenie w wydzielonych pododdziałach dowodzenia komponentu (plutonu) odpowiedzialnego za rozwinięcie systemu satelitarnego umożliwiającego łączenie stanowisk dowodzenia (baz) na duże odległości o transferze adekwatnym do realizowanych zadań i funkcjonujących usług sieciowych.

Z punktu widzenia ekonomicznego celowym jest budowa jednej sieci teleinformatycznej o jednym scentralizowanym systemie zarządzania, umożliwiającej transmisję danych oraz prowadzenie rozmów telefonicznych. Wprowadzenie telefonii IP umożliwi znaczne obniżenie kosztów eksploatacyjnych systemu oraz zredukuje do minimum budowę sieci telefonicznych na stanowisku dowodzenia.

Planowanie sieci wymiany informacji na stanowisku dowodzenia z wykorzystaniem metody symulacyjnej

dr inż. Mirosław POPIS
Wojskowa Akademia Techniczna

Referat zawiera propozycję postępowania konstruktora systemów łączności na etapie planowania nowej lub modyfikowania istniejącej sieci telekomunikacyjnej.



Rysunek1. Algorytm postępowania przy planowaniu sieci LAN SD z wykorzystaniem pakietu symulacyjnego

Opracowanie dotyczy etapu weryfikacji sieci łączności i informatyki rozwijanych na SD przy czym sposób postępowania nie jest zależny od postaci sieci teleinformatycznej ani od szczebla dowodzenia na rzecz którego ma być rozwinięta.

Realizacja, zaprezentowanego na rys.1, algorytmu postępowania pozwala ocenić czy planowana sieć SD jest w stanie zagwarantować świadczenie usług teleinformatycznych na żądanym poziomie.

1. Identyfikacja niezbędnych danych

Proponowany sposób realizacji procesu planowania na etapie weryfikacji sieci wymiany informacji wymaga ustalenia możliwej struktury, stopnia złożoności, zastosowanych technik i technologii a także ilości użytkowników, rodzaju, poziomu i ukierunkowania generowanego ruchu w rozpatrywanym systemie.

Poniżej zidentyfikowano niezbędne informacje, które będą wykorzystane w trakcie realizacji scenariusza badania przedmiotowej sieci teleinformatycznej WŁ SD w czasie budowania jej modelu.

1.1. Obiekt badawczy

W celu identyfikacji rozpatrywanego obiektu należy pozyskać informacje opisujące:

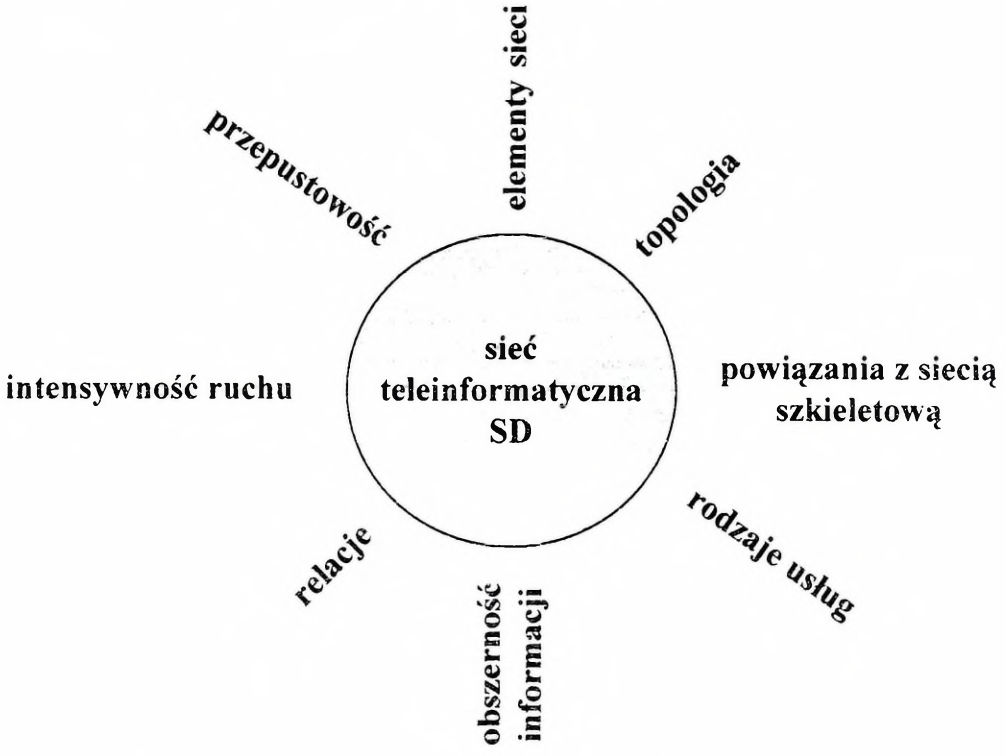
- budowę sieci lokalnych (elementy sieci, typy urządzeń łączności i informatyki oraz zastosowane tory transmisyjne łączące te urządzenia,
- topologię (rozmieszczenie elementów (urządzeń) łączności i informatyki w terenie oraz usytuowanie ich względem siebie wraz z powiązaniem torami transmisyjnymi,
- powiązanie z siecią szkieletową,
- wymagane usługi teleinformatyczne,
- planowana intensywność i natężenie ruchu generowanego na rozpatrywanym SD,
- obszerność informacji wymienianych w systemie,
- ukierunkowanie ruchu,
- wielkość ruchu teleinformatycznego innych WŁ obciążających sieć szkieletową,

Najistotniejsze informacje opisujące sieć teleinformatyczną SD prezentuje rys.2.

W pierwszym kroku należy zaproponować infrastrukturę sieci teleinformatycznej SD. Najczęściej są to dwie wyodrębnione lub przenikające się sieci:

- LAN,
- z komutacją kanałów.

Obecnie pierwsze z nich opierają się na rozwiązaniach LAN z technologią Ethernet (10, 100, 1000 Mb/s), Token Ring (4 i 16 Mb/s) lub FDDI (100 Mb/s). LAN WŁ SD w chwili obecnej będą rozwijane w oparciu o Polowe Aparatownie Informatyczne (PWI) pozwalające na rozwinięcie i eksploatację sieci Ethernetowej.



Rysunek 2. Najistotniejsze informacje opisujące sieć teleinformatyczną SD

Ponieważ poszczególne fragmenty sieci łączy się ze sobą za pomocą urządzeń i mediów transmisyjnych należy określić jakie konkretne mosty, haby, przełączniki, rutery, multipleksery czy tory kablowe przewidziano do zastosowania w przewidywanej sieci. Należy również zidentyfikować osobiste terminale komputerowe i urządzenia wykonujące zadania serwerów.

Analogicznie należy określić parametry urządzeń łączności i torów kablowych jakie planuje się użyć do zbudowania sieci abonenckiej. Obecnie możliwe jest rozwinięcie komutowanej sieci abonenckiej w oparciu o KX-30, ŁC-240 (480, 960) i/lub ŁK-24 zainstalowanych na RWŁC-10 (RWŁC-10K, RWŁC-10T, AK, AT, AT-K) i WD. Trzeba też ustalić parametry mediów transmisyjnych, a także określić typy i rodzaje urządzeń końcowych osób funkcyjnych jakie zastosowano w projekcie.

Należy zaznaczyć, że pakiety (programy) symulacyjne zawierają w swoich bibliotekach modele różnych węzłów sieciowych co znacznie może zwiększyć efektywność budowania modeli sieci teleinformatycznych. W przeciwnym przypadku należy przenieść z katalogów firmowych odpowiednie parametry urządzeń do okien dialogowych. Najczęściej ze względu na znikomy wpływ lokalnych przewodowych torów transmisyjnych (poprawnie rozwiniętych) na jakość rozpatrywanych sieci zostają one najczęściej pomijane w opisie modeli.

Podczas projektowania sieci komputerowej i abonenckiej SD należy zastanowić się nad ich topologiami. Zazwyczaj koszty instalacji kablowej, kart sterujących i osprzętu sieciowego są w warunkach działań wojennych pomijalnie nieistotne, natomiast należy wziąć pod uwagę elastyczność architektury sieci dającą możliwość jej rekonfiguracji lub wprowadzenie dodatkowych węzłów (komputerów, urządzeń peryferyjnych). Istotna jest też niezawodność realizacyjna zadań teleinformatycznych uzyskiwana na drodze redundancji komunikacyjnej między węzłami sieci i poprzez zastosowanie dodatkowych węzłów sieci stosownie do wagi zadań.

Oczywistym jest, że zasięg wymiany informacji obejmuje nie tylko obręb rozpatrywanych sieci łączności SD ale również odbywać się będzie w relacjach zewnętrznych. Zazwyczaj WŁ SD od szczebla oddziału dowiązywane są bezpośrednio do węzłów łączności sieci szkieletowych nazwanych w zależności od obsługiwanego szczebla dowodzenia BSŁ (bazową siecią łączności), PSŁ (podstawową siecią łączności) lub psł (pomocniczą siecią łączności). Występuje oczywista potrzeba sprzęgnięcia wymienionych sieci ze sobą co pozwala na wymianę informacji między uprawnionymi do tego osobami funkcyjnymi różnych szczebli dowodzenia. Projektant planowanej sieci łączności SD w celu uzyskania zysku na efektywności badania może uwzględnić wymienione sieci przestrzenne w sposób zagregowany w postaci węzła reprezentującego źródła i ujścia różnych strumieni danych.

W kolejnym kroku powinno się ustalić jakie usługi telekomunikacyjne będą udostępnione przez LAN i sieć abonencką oficerom SD. Obecnie do najbardziej przydatnych usług w systemie dowodzenia i sterownia środkami rażenia można zaliczyć:

- przesyłanie (zbieranie, rozpowszechnianie) danych (przesył depesz, komunikatów, e-mail, sygnałów sterujących, informacji do/z baz danych,);
- usługę tekstową (faks);
- telefonię;
- wideotelefonię.

Dostęp końcowych urządzeń abonenckich do sieci jest zapewniany poprzez tory kablowe miedziane, światłowodowe lub bezprzewodowe.

Trzeba jednak zauważyć, że grupa czynników związana ze środkami dowodzenia jest jedynie pochodną potrzeb informacyjnych organów dowodzenia. Do określenia wpływu systemu dowodzenia na obciążenie sieci łączności SD należy wziąć pod uwagę potrzeby informacyjne organów dowodzenia (w tym relacje wymiany informacji) oraz ilość, rodzaj i postać generowanych, przechowywanych w bazach danych i przesyłanych informacji.

W przypadku usług z komutacją kanałów należy uzyskać informacje o przewidywanym natężeniu ruchu generowanym przez pojedynczych użytkowników lub co najmniej grupy użytkowników, po czym uwzględniając spodziewany czas pojedynczych połączeń i korzystając z definicji Erlanga obliczyć częstość uruchamiania każdej z usług.

$$I = \frac{n \times t_p}{60} [Erl]$$

gdzie:

I – natężenie ruchu w erlangach;

n –ilość inicjacji połączeń przez jedno urządzenie w czasie 1 godziny;

t_p – czas trwania połączenia w minutach.

Mając obliczoną ilość połączeń dla jednego urządzenia łatwo obliczyć ją dla źródła reprezentującego rzeczywistą ilość telefonów (faksów, i innych urządzeń korzystających z kanałów komutowanych) na SD, po czym określić co ile sekund zagregowane źródło podejmować będzie próby wywołań.

$$n_z = \frac{n}{z} [1/godz.]$$

gdzie:

n_z - ilość inicjacji połączeń przez zagregowaną grupę urządzeń końcowych w czasie 1 godziny;

n - ilość inicjacji połączeń przez jedno urządzenie w czasie 1 godziny;

z – ilość urządzeń w grupie.

$$t_c = \frac{3600}{n_z} [s]$$

gdzie:

t_c – czas między wywołaniami realizowanymi przez urządzenia końcowe grupy urządzeń (intensywność generowanego ruchu);

n_z - ilość inicjacji połączeń przez zagregowaną grupę urządzeń końcowych w czasie 1 godziny.

Również dla usług informatycznych, należy posiąść wiedzę o przewidywanej intensywności korzystania z nich przez każdą uprawnioną osobę funkcyjną. Podobnie jak to wcześniej przedstawiono, planista musi ustalić tę częstość dla grupy każdego rodzaju usługi. Agregowanie urządzeń tego samego typu i spełniających takie same zadania oraz posiadających identyczne uprawnienia powodują znaczne zwiększenie efektywności badania bez uszczerbku na informatywności.

Kolejny krok dotyczy identyfikacji objętości wysyłanych informacji. W przypadku usług korzystających z komutacji kanałów należy ustalić wymaganą szybkość pracy liniowej dla urządzeń końcowych (w kb/s) oraz czas zajmowania kanału przez te urządzenia. Oceniając wielkość wiadomości należy określić ją w kb. Jest oczywiste, że oszacowane wielkości czasu zajętości kanałów oraz objętości wiadomości wyrażone liczbowo będą obarczone błędami. W celu zminimalizowania błędów zdarzenia te są opisywane odpowiednimi rozkładami prawdopodobieństwa podobnie jak intensywność korzystania z usług telekomunikacyjnych.

W następnym etapie należy uwzględnić potrzeby użytkowników sieci telekomunikacyjnej SD i ukierunkować ruch wewnętrzny i zewnętrzny. Pakiety symulacyjne zazwyczaj umożliwiają losowy wybór adresatów będących w zasięgu tylko sąsiednich węzłów lub obsługiwanych przez wszystkie węzły znajdujące się w sieci telekomunikacyjnej. Jednak takie adresowanie węzłów docelowych jest obarczone dużym błędem w przypadku gdy faktycznie ruch jest wzmożony tylko w niektórych relacjach. Dlatego zazwyczaj stosuje się nadawanie odpowiednich wag dla każdej możliwej relacji wymiany informacji.

Kolejnym problemem, który należy rozwiązać to identyfikacja poziomu ruchu telekomunikacyjnego przenoszonego przez sieć szkieletową do rozpatrywanego stanowiska dowodzenia. Poziom zajętości traktów będzie miał istotny wpływ na czas dostarczania wiadomości z rozpatrywanej sieci LAN SD do serwerów pracujących na WŁ innych SD.

Podobnie stan zajętości łączy sieci szkieletowych będzie w decydującym stopniu wpływać na jakość realizacji usług korzystających z kanałów komutowanych (blokady

zgłoszeń i wywołań, rozłączenia wywołaniami z aparatów końcowych o wyższych priorytetach).

1.2 Wpływ wojsk przeciwnika

Przeciwnik będzie dążył do dokonania fizycznych zniszczeń jak największej ilości elementów sieci telekomunikacyjnej i prób obezwładnienia systemu środkami walki elektronicznej[1]. Skuteczność tego oddziaływania zależeć będzie między innymi od możliwości rozpoznania jej elementów. Stąd można sformułować pewnik, że przeciwnik będzie starał się za wszelką cenę określić topologię, strukturę i urządzenia jakie zastosowano do budowy sieci telekomunikacyjnej. Ponadto należy liczyć się z działaniami zmierzającymi przechwytu wiadomości przesyłanych w sieci telekomunikacyjnej by następnie wykorzystać je do osiągnięcia swoich celów. Zdobyte przez przeciwnika informacje mogłyby być mu wysoce pomocne do skutecznego rażenia elementów rozpatrywanej sieci środkami ogniowymi i obezwładnienia nadajnikami zakłócającymi.

Ponadto należy przeprowadzić badanie sieci abonenckiej i komputerowej SD w warunkach uszkodzeń (obezwładnienia) elementów sieci telekomunikacyjnej i poddać ocenie czy są one w stanie zapewnić zakładany poziom jakościowy. W tym celu mając wiedzę o dotychczasowym działaniu przeciwnika, planiści powinni dążyć do zidentyfikowania poziomu uszkodzeń sieci przy którym będzie ona jeszcze w stanie zadowolić użytkowników.

1.3. Wskaźniki określające jakość sieci abonenckiej i LAN

Jakość[2] sieci abonenckiej i LAN najczęściej określana jest przy pomocy różnych wskaźników opisujących cechy badanych sieci. Dostęp do usług oraz niezawodność, żywotność, mobilność sieci oraz bezpieczeństwo informacji są podstawowymi atrybutami sieci telekomunikacyjnych. Z punktu widzenia użytkownika oferowane usługi[3] powinny być kompletne, dostępne i realizowalne w krótkim czasie.

Z tego punktu widzenia planujący sieci typu telefonicznego i komputerowego powinni otrzymać w zadaniu:

- wykaz usług jakie mają być udostępnione wskazanym osobom funkcyjnym,
- wykaz urządzeń (osób) z przydzielonymi wyższymi priorytetami,

---

1 M. Popis, A. Bajda, Czynniki wpływające na strukturę i funkcjonowanie sieci telekomunikacyjnej korpusu wojsk lądowych w operacji obronnej, Myśl Wojskowa, Warszawa 2004, vol. III (wyd. niejawne)

[2] Jakość usługi - zespół właściwości usługi, określający stopień zaspokojenia określonych potrzeb użytkownika [PN-93/N-50191]

- wartości wskaźników jakościowych:
  - dopuszczalne średnie i maksymalne poziomy blokad (rozłączeń) dla usług z komutacją kanałów w ruchu wewnętrznym i zewnętrznym,
  - dopuszczalne średnie i maksymalne czasy przesyłania wiadomości dla poszczególnych usług informatycznych w obrębie własnego SD i w relacjach zewnętrznych.

Kolejny etap w postępowaniu planistycznym polega na opracowaniu i realizacji scenariusza przebiegu badania.

2. Scenariusz badań symulacyjnych

Zgodnie z celem badania realizacja szeregu zadań cząstkowych powinna dać odpowiedź na następujące pytania:

1. Jaka jest jakość poszczególnych wariantów badanych sieci SD?
2. Które z badanych sieci spełniają założone wskaźniki jakościowe?
3. Jak zmienią się atrybuty sieci w skutek oddziaływania przeciwnika?
4. Jakie warianty sieci abonenckiej i komputerowej zaproponować do realizacji?

W scenariuszu należy określić:

- *Adekwatność modelu*

Adekwatność modelu rozumiana tu jako dokładność odwzorowania badanego obiektu przy pomocy narzędzia symulacyjnego ma zasadniczy wpływ na poziom informatywności i efektywności badania. Jest oczywiste, że wzrost efektywności będzie powodował zmniejszenie informatywności. Projektant znając czas jaki został mu przydzielony do przeprowadzenia badania powinien dążyć stworzenia modelu o jak najwyższej możliwej do osiągnięcia informatywności. Dokładne określenie adekwatności zbudowanego modelu jest możliwe tylko w przypadku porównania uzyskanych wyników z danymi empirycznymi lub wyliczonymi matematycznie.

- *Zmienne czynniki wejściowe*

Przygotowując badania planiści powinni zidentyfikować zmienne parametry wejściowe oraz wartości poziomów z jakimi będą implementowane do modeli sieci. Ilość tych czynników i poziomów będzie determinować ilość eksperymentów jakie zostaną przeprowadzone. Czynnikami mogą być sprawność lub uszkodzenia poszczególnych elementów sieci

---

[3] Usługa - zbiór funkcji oferowanych użytkownikowi przez organizację, [PN-93/N-50191-01-04] [CCITT Rec.E.800,M.6]

telekomunikacyjnej, topologia, parametry zastosowanych urządzeń, technologie i techniki zaimplementowane w badanym obiekcie, charakterystyki ruchowe, wielkości wiadomości, czas trwania połączeń i inne.

- *Obserwowane czynniki opisujące zdarzenia w sieci*

W trakcie przebiegów symulacyjnych, jeśli używany pakiet na to pozwala, warto obserwować procesy jakie zachodzą w badanym systemie. Pozwala to na zidentyfikowanie zdarzeń, które mogą niekorzystnie wpływać na funkcjonowanie systemu telekomunikacyjnego co z kolei pozwala wprowadzać zawczasu korekty do planowanej sieci. Niestety wizualizacja zjawisk zachodzących w badanym obiekcie znacznie wydłuża czas zbierania danych.

- *Ilość ocenowych czynników wyjściowych*

Przed uruchomieniem symulacji należy zdecydować jakie raporty z danymi mają być zbierane aby ich analiza umożliwiła realizację celu badania. Zbieranie zbyt dużej liczby raportów wpływa negatywnie na efektywność symulacji. Zazwyczaj raporty dotyczą zdarzeń w węzłach, liniach transmisyjnych oraz w sieci rozległej a także różne wskaźniki dotyczące źródeł aplikacji, wiadomości i połączeń sesji.

- *Wiarygodność wyników*

Wiarygodność uzyskanych wyników zależy w dużym stopniu od ilości powtórzeń przebiegów w każdym z eksperymentów. Liczność próbek można obliczyć, zakładając wcześniej dokładność wyników (0,x σ) przy określonym poziomie ufności (1-α), posługując się zależnością:

$$N \geq \frac{\sigma^2 u^2_{\alpha/2}}{d^2}$$

gdzie:

N – liczba powtórzeń,

σ – odchylenie standardowe,

d – dokładność oszacowania wartości średniej,

$u_{\alpha/2}$ - wartość standaryzowanej zmiennej losowej $u = \mu / \sigma / \sqrt{N}$ o rozkładzie normalnym N(0,1), μ – wartość średnia populacji generalnej.

Zakładając błąd wyników na poziomie 30% odchylenia standardowego dla poziomu ufności (1-α) = 0,95 ilość powtórzeń wynosi 43.

- *Czas rozbiegu*

W celu wyeliminowania niekorzystnych zjawisk, związanych z niestabilnością badanego obiektu, mogących się pojawić w początkowym okresie funkcjonowania modelu należy określić moment początku zbierania wyników w raportach. Poniżej przytoczono najczęściej używane metody wyznaczania czasu zimnego startu:

Metoda CONWAY'a – należy odrzucać ostatnie wyniki symulacji do czasu, aż następny wynik nie będzie maksymalny lub minimalny.

Metoda EMSHOFF'a i SIMSSON'a - początkowy okres symulacji kończy się, gdy liczba obserwacji o wartościach mniejszych od wartości średniej będzie równa liczbie obserwacji o wartościach większych od wartości średniej lub gdy zmiany wartości średniej są mało istotne, to model znajduje się w stanie równowagi.

Metoda FISHMAN'a – gdy wyniki podlegają autokorelacji, należy wyznaczyć maksymalny przedział czasu t, na końcach którego w sposób znaczny występuje autokorelacja i nie uwzględniać go w oszacowaniu charakterystyk wyjściowych.

Metoda TOCHER'a – najdłuższy cykl funkcjonowania modelu powinien być powtórzony trzy - cztery razy.

Metoda GORDON'a – należy skonstruować wykres odchylenia standardowego wielkości wyjściowej w funkcji liczności próby w skali logarytmiczno-liniowej. Gdy wykres ten można aproksymować prostą o nachyleniu –1/2 to można przyjąć jest stan równowagi modelu.

- *Czas zbierania informacji*

Przedział czasu przeznaczony na zbieranie danych powinien odpowiadać celowi badania. Najczęściej kryterium krytycznym są najbardziej niekorzystne warunki funkcjonowania systemu w dającym się przewidzieć okresie czasu. Zazwyczaj czas ten to GNR (godzina największego ruchu) z zastrzeżeniem by w tym czasie zostały zrealizowane przynajmniej jednokrotnie wszystkie usługi i zaistniały niekorzystne zdarzenia np. uszkodzenia urządzeń.

Należy przy tym mieć świadomość, że faktyczny czas trwania przebiegu symulacyjnego w przypadku złożonych i wysokoobciążonych sieci trwa zazwyczaj wielokrotnie dłużej.

- *Zebranie i opracowanie wyników*

Wyniki symulacji dla każdego powtórzenia wszystkich eksperymentów najczęściej zbierane i prezentowane są w formie tabelarycznej. Od poprawnej interpretacji danych liczbowych zależeć będzie czy otrzymane rezultaty można przyjąć za wiarygodne.

W celu analizy zjawisk zachodzących w badanych sieciach i z potrzeby ustalenia ich słabych stron planiści dążyć będą do zbierania stosunkowo dużej ilości różnych czynników wyjściowych.

Charakteryzować będą one:

- *węzły* – np. centrale, rutery, haby, przełączniki itp. (wykorzystanie pamięci, procesora, buforów itp.);
- *linie transmisyjne* – punkt-punkt, wielodostępowe (wykorzystanie kanału, liczbę kolizji, liczba i poziom przywołań itp.);
- *sieć rozległą* – WAN - (opóźnienie i liczba ramek wirtualnych, statystyka połączeń itp.);
- *źródła aplikacji* – oprogramowanie użytkowe (czas uruchomienia);
- *źródła wiadomości i odpowiedzi* – np. e-mail (opóźnienia wiadomości i pakietów);
- *źródła połączeń* – np. aparat telefoniczny, faks (liczba zrealizowanych, zablokowanych i rozłączonych połączeń itp.);
- *źródła sesji* – np. ftp, www itp. (opóźnienie wiadomości, pakietów, ustawień, długość sesji, liczba pobieranych danych);
- *polecenia transportu, odpowiedzi, ustawień* – (opóźnienia wiadomości, pakietów, długość sesji, liczba ustawień itp.)

Każdy z czynników wyjściowych w postaci wyżej wymienionych wskaźników powinien być poddany obróbce matematycznej. Najczęściej planista będzie wyznaczał wartości średnie i odchylenie standardowe ale równie ważne są zaistniałe wartości ekstremalne.

Ponadto w celu zbadania adekwatności modelu a tym samym poprawności uzyskanych wyników należy sprawdzić rozkład uzyskanych danych w poszczególnych powtórzeniach dla każdego eksperymentu. W tym celu często korzysta się z rozkładu t Studenta wyznaczając z niego, dla przyjętego poziomu ufności, błąd graniczny lub/i błąd średnich arytmetycznych co z kolei umożliwia stwierdzić czy odpowiednia ilość otrzymanych wartości wskaźników mieści się w wyliczonym przedziale międzygranicznym. Jeśli warunek ten jest spełniony mamy pewność, że uzyskane wyniki są poprawne i planista na ich podstawie ma możliwość podjęcia trafnej decyzji.

- Podjęcie decyzji o najlepszej konfiguracji sieci stanowiska dowodzenia jest ostatnim etapem pracy planistycznym. W tym przypadku polega na dokonaniu wyboru jednego z kilku przebadanych modeli sieci teleinformatycznej SD. Kryteria wyboru powinny być przekazane planiście przez przełożonego. W przypadku gdyby żądane wymagania speł-

niało więcej niż jedno rozwiązanie należy wybrać to, które będzie wymagało zaangażowania najmniejszych sił i środków.

3. Wnioski

Przedstawiona metodologia badania sieci teleinformatycznej SD, na etapie planowania, może być zastosowana do badania również innych sieci telekomunikacyjnych. W wyniku poprawnej realizacji metody można mieć założoną pewność, że przedmiotowa sieć będzie w stanie spełnić wymagania użytkownika. Należy jednak zwrócić uwagę na złożoność i czasochłonność tego sposobu badania systemów. Nieodzownym jest by, osoby funkcyjne dysponowały gotowymi typowymi zbiorami modułów reprezentującymi podsystemy i urządzenia łączności, oraz oprogramowanie pomocnicze do obróbki statystycznej uzyskanych wyników.

Wykorzystanie środków dowodzenia na stanowiskach dowodzenia szczebla taktycznego

inż. dypl. Andrzej WISZ
Akademia Obrony Narodowej

Współczesne i perspektywiczne pole walki wymaga i wymagać będzie umiejętnego koordynowania i synchronizacji działań wielu szczebli dowodzenia, rodzajów sił zbrojnych i wojsk. Posiadanie takich możliwości, powiązane ze zdolnością do szybkiego przekazywania zadań i zbierania meldunków o sytuacji, stanowić będzie zasadnicze uwarunkowanie osiągnięcia powodzenia. Jest to jednak możliwe tylko w przypadku dysponowania nowoczesnym, wysoce sprawnym systemem wspierającym dowodzenie, którego osnową powinien być nowoczesny środki dowodzenia.

Współczesne środki dowodzenia muszą mieć zdolność przyjęcia i obsłużenia dużej ilości użytkowników w zakresie:

- zobrazowania aktualnej sytuacji wojsk własnych i przeciwnika;
- szybkiego wykonywania dużej ilości obliczeń;
- redagowania meldunków;
- tworzenia tematycznych (profesjonalnych) bibliotek zbiorów informacji;
- transmisji, odbioru i zobrazowania wielu danych.

Procesy te powinny być realizowane w czasie rzeczywistym.

Specyfika działań bojowych wymaga, aby środki dowodzenia na stanowiskach dowodzenia zapewniały:

- realizację automatycznych połączeń pomiędzy zautomatyzowanymi miejscami pracy osób funkcyjnych wewnątrz stanowisk dowodzenia oraz z innymi stanowiskami dowodzenia na obszarze działań,
- priorytetowe zestawianie połączeń dalekosiężnych dla upoważnionych dowódców i oficerów sztabów,
- zestawianie połączeń konferencyjnych zarówno dla osób funkcyjnych danego stanowiska dowodzenia, jak i dowolnych stanowisk dowodzenia na obszarze działań,
- automatyczny odbiór i przekazywanie komend i sygnałów dowodzenia bojowego, sygnałów ostrzegania i alarmowania w postaci dźwiękowej (głosowej) lub różnorodnych form zobrazowania (monitor, drukarka, planszet, tablica sygnalizacyjna itp.),

– tworzenie banków i baz danych oraz kontrolowaną dystrybucję wszelkich informacji w tym także decyzyjnych - w formie obligatoryjnej lub na żądanie w sposób zautomatyzowany, bez względu na aktualne rozmieszczenie w terenie miejsc pracy dowódców i osób funkcyjnych systemu dowodzenia,

– wysoką podatność na rekonfigurację zbioru abonentów (przemieszczanie do innych stanowisk dowodzenia z zachowaniem numeru abonenta, priorytetów, itp.),

– wysoką odporność na celowe i przypadkowe zakłócenia radioelektroniczne,

– przekazywanie informacji z gwarantowaną mocą kryptograficzną,

– możliwość automatycznej kontroli i rejestracji stanu łączności.

Spełnienie tych wymagań zależy od jakości mediów transmisyjnych, środków komutacyjnych oraz urządzeń końcowych (w tym również urządzeń przetwarzania danych).

Wyniki badań prowadzonych, przez oficerów zakładu łączności i informatyki, w zakresie możliwości wykorzystania obecnych środków dowodzenia na stanowiskach dowodzenia szczebla taktycznego przedstawiono poniżej.

Prowadzone badania w czasie ćwiczeń dowódczo-sztabowych „Akademicki Pierścień 2005" i „Pierścień 2005" dotyczyły określenie ilości i rodzaju urządzeń końcowych-abonenckich niezbędnych dla prawidłowego funkcjonowania poszczególnych komórek stanowisk dowodzenia dywizji i brygady oraz obejmowały następujące obszary:

1. Określenia liczby i rodzaju urządzeń końcowych-abonenckich niezbędnych dla prawidłowego funkcjonowania poszczególnych komórek stanowiska dowodzenia dywizji i brygady dokonano poprzez zbadanie:

– stopnia wykorzystania aparatów telefonicznych typu CB.

– stopnia wykorzystania telefaksów do przesyłania dokumentów tekstowych i graficznych.

– stopnia wykorzystania wynosów radiowych przez osoby funkcyjne stanowiska dowodzenia brygady i dywizji.

– zakresu wykorzystania zautomatyzowanych stacji pracy przez osoby funkcyjne stanowiska dowodzenia dywizji i brygady.

– zakres wykorzystania terminali komputerowych.

2. Określenie możliwości organizowania dalekosiężnych linii telekomunikacyjnych dokonano poprzez zbadanie zakres wykorzystania jednokanałowych terminali satelitarnych.

3. Określenie zakresu wykorzystania aparatowni zarządzania systemem łączności do sterowania sieci łączności i sieci komputerowych.

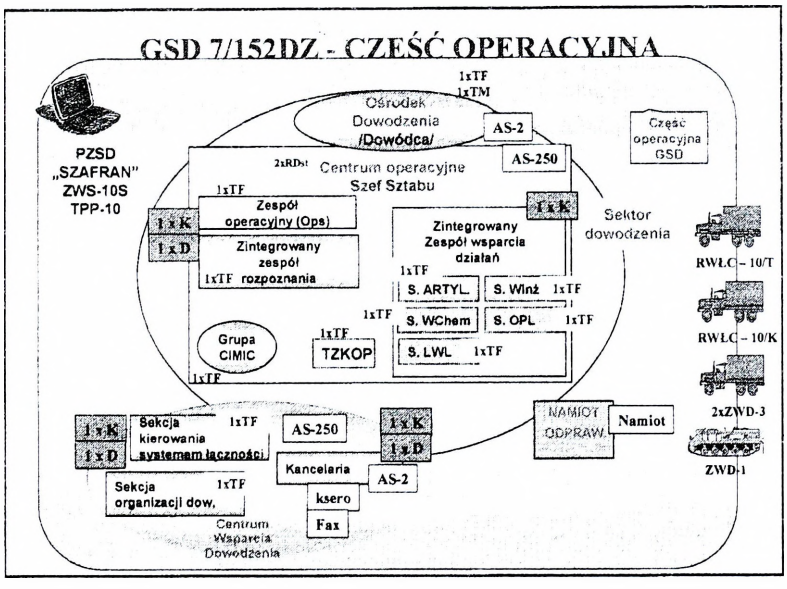
Badania oparto o założone ilości urządzeń końcowych (terminalowych), a przedstawionych w dokumentacji ćwiczeń dowódczo-sztabowego oraz dokonaną obserwację w trakcie trwania ćwiczeń.

Celem obserwacji było określenie, na ile wystarczająca była zaplanowana (przewidziana) liczba wykorzystywanych urządzeń końcowych dla właściwego funkcjonowania stanowisk dowodzenia brygad i dywizji. Obserwacja była dokonana na obszarze polowych stanowisk dowodzenia dywizji i dwóch brygad oraz na podstawie uzyskiwanych informacji o stanie łączności w zespole zabezpieczenia teleinformatycznego ćwiczenia[1] przy wykorzystaniu aparatowni zarządzania systemem łączności.

Urządzeniami końcowymi poddanymi badaniom były:

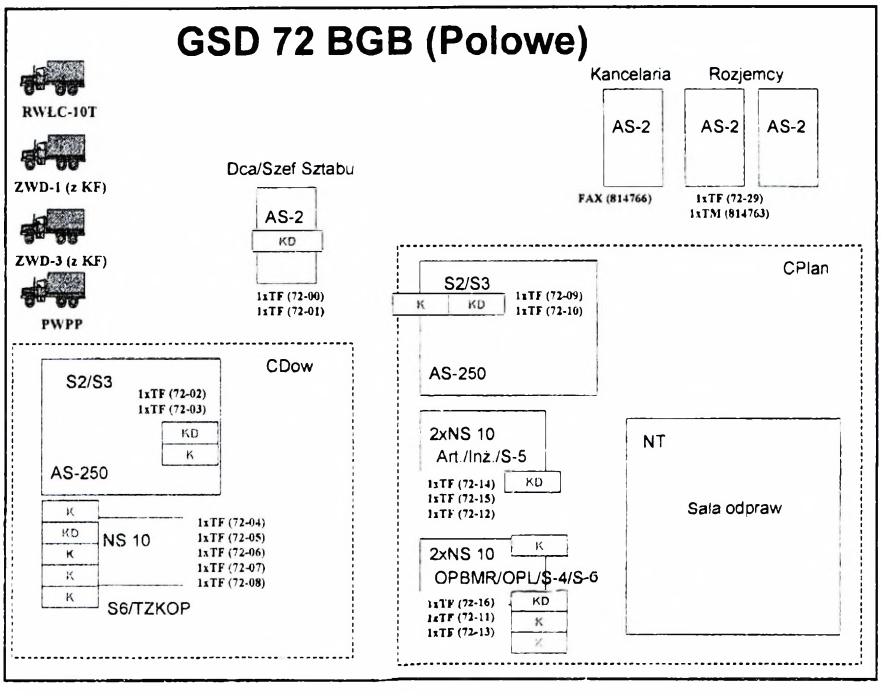
- aparaty telefoniczne ATS-1;
- wynosy radiowe – manipulatory radiowe;
- terminale komputerowe.

Aparaty telefoniczne i terminale komputerowe przydzielono zgodnie z dokumentacją ćwiczenia rys. 1, 2 i 3.

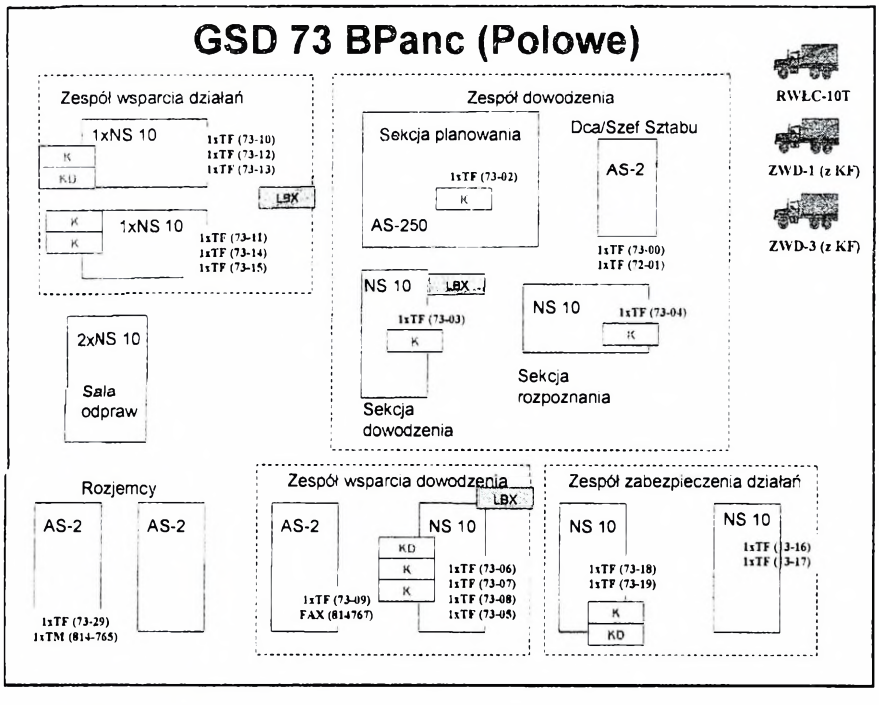


Rys. 1. Schemat rozmieszczenia urządzeń końcowych-abonenckich oraz elementów stanowiska dowodzenia dywizji w ćwiczeniu dowódczo-sztabowym „Akademicki Pierścień 2004"
Źródło: Opracowanie własne

[1] Autor w czasie ćwiczenia "Pierścień 2005" pełnił funkcję kierownika zespołu zabezpieczenia teleinformatycznego



Rys. 2. Schemat rozmieszczenia urządzeń końcowych (abonenckich) oraz elementów stanowiska dowodzenia 72 BGB w ćwiczeniu dowódczo-sztabowym „Pierścień 2005"
Źródło: Opracowanie własne



Rys. 3. Schemat rozmieszczenia urządzeń końcowych (abonenckich) oraz elementów stanowiska dowodzenia 73 BPanc w ćwiczeniu dowódczo-sztabowym „Pierścień 2005"
Źródło: Opracowanie własne

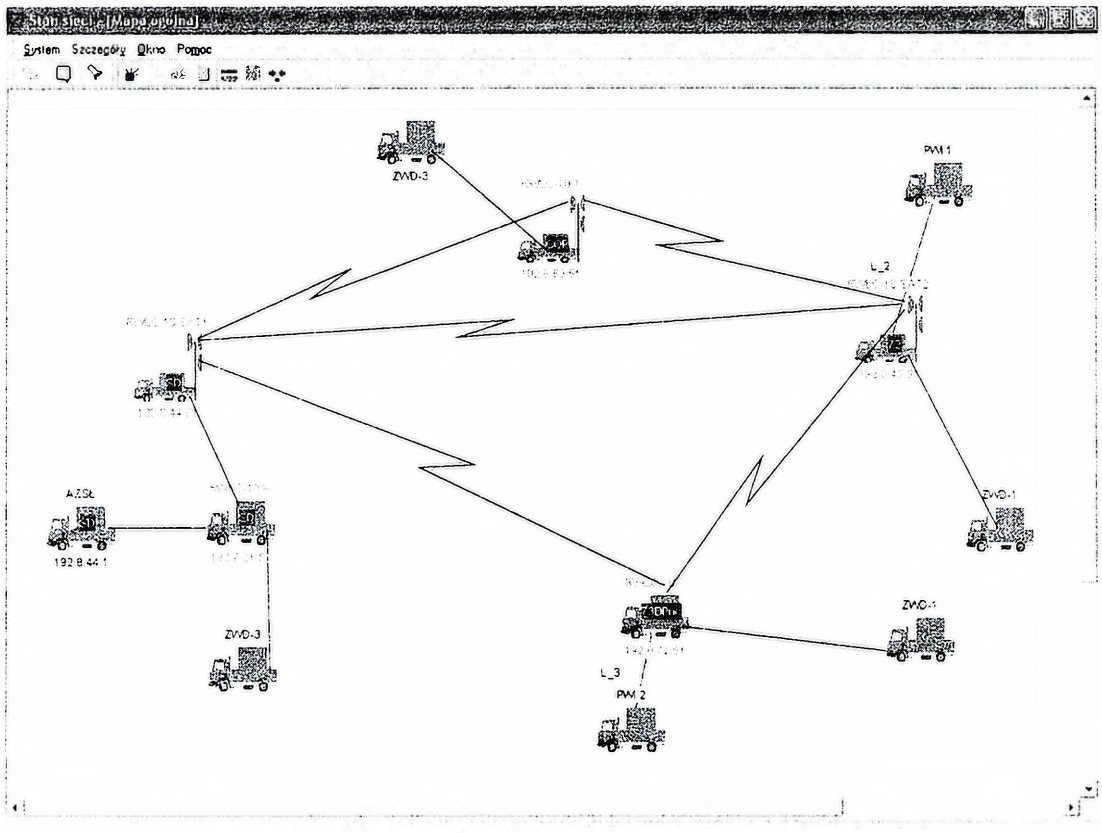
W czasie obserwacji przeprowadzono badania dotyczące zastosowania jednokanałowych terminali satelitarnych.

Jednokanałowy terminal satelitarny (rys. 4) przydzielono dowódcy 72 BGB. Przeznaczony był do zestawiania dalekosiężnej satelitarnej linii telekomunikacyjnej między aparatownią transmisyjną (RWŁC-10/T) rozwiniętą na węźle łączności głównego stanowiska dowodzenia 72 BGB a wozem dowodzenia dowódcy brygady pracującym poza stanowiskiem dowodzenia.

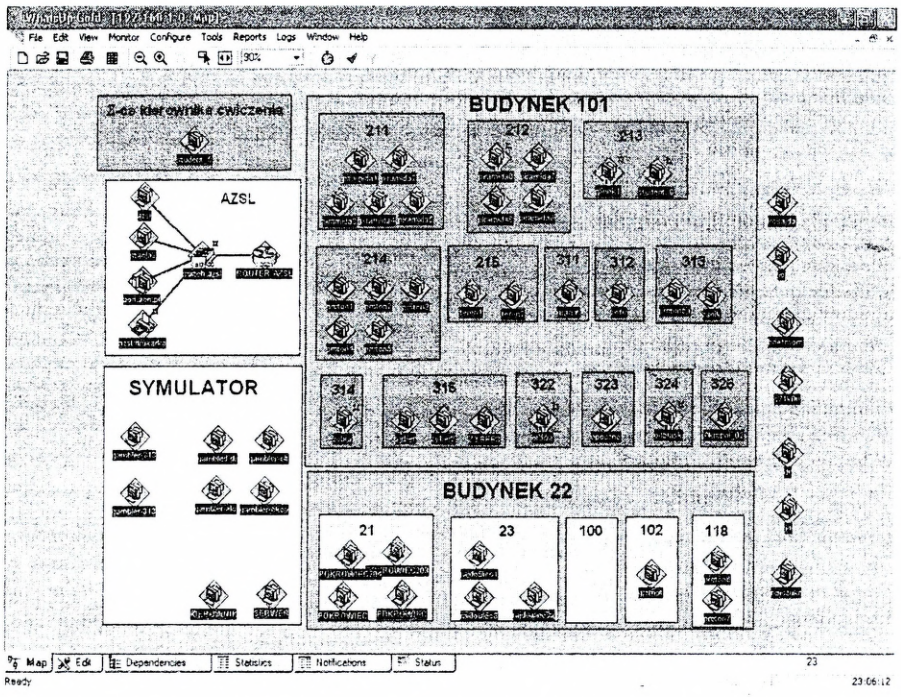


Rys. 4. Widok jednokanałowego terminala satelitarnego systemu INMARSAT
Źródło: Opracowanie własne

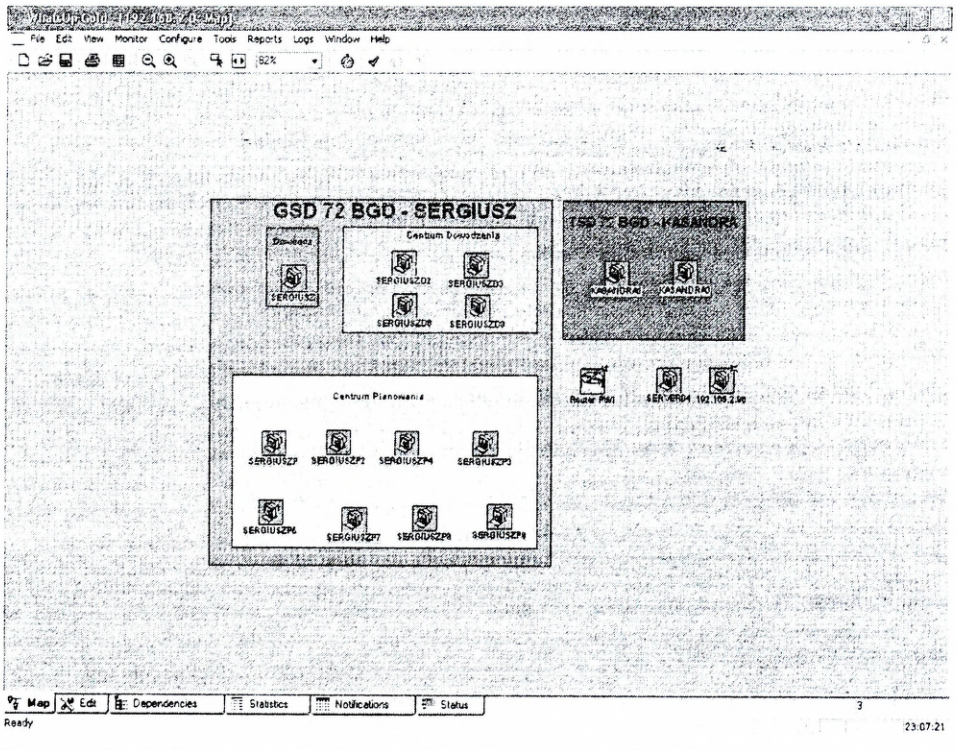
W czasie ćwiczenia przeprowadzono badania w zakresie możliwości wykorzystania aparatowni zarządzania systemem łączności (AZSŁ) w strukturze sieci łączności dywizji. Badana aparatownia została przydzielona do zespołu zabezpieczenia teleinformatycznego ćwiczenia. W czasie realizacji określonych zadań członkowie zespołu, dzięki możliwościom technicznym AZSŁ mogli na bieżąco sterować pracą sieci teleinformatycznej ćwiczenia, co zobrazowano na rys. 5, 6, 7 i 8.



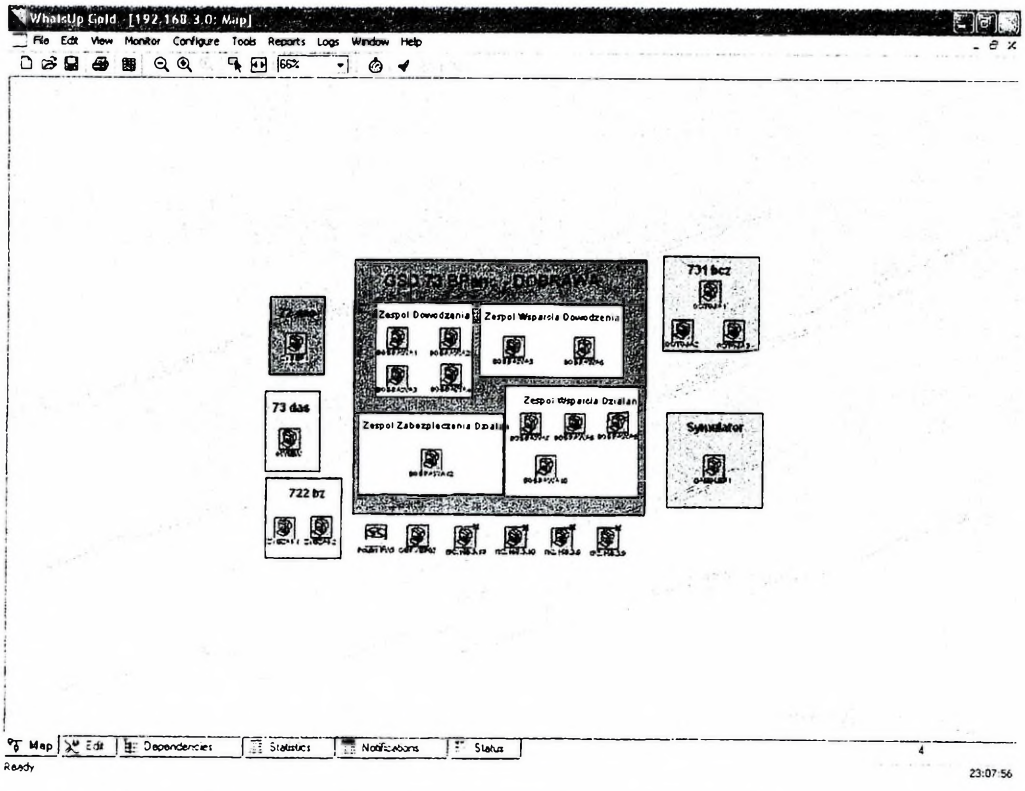
Rys. 5. Struktura sieci teletransmisyjnej ćwiczenia „Pierścień 2005" zobrazowana przy wykorzystaniu AZSŁ
Źródło: Opracowanie własne



Rys. 6. Struktura sieci informatycznej ćwiczenia „Pierścień 2005" w bloku 101 i 22 zobrazowana przy wykorzystaniu AZSŁ
Źródło: Opracowanie własne



Rys. 7. Struktura sieci informatycznej ćwiczenia „Pierścień 2005" na GSD i TSD 72 BGB zobrazowana przy wykorzystaniu AZSŁ
Źródło: Opracowanie własne



Rys. 8. Struktura sieci informatycznej ćwiczenia „Pierścień 2005" na GSD 73 BPanc zobrazowana przy wykorzystaniu AZSŁ
Źródło: Opracowanie własne

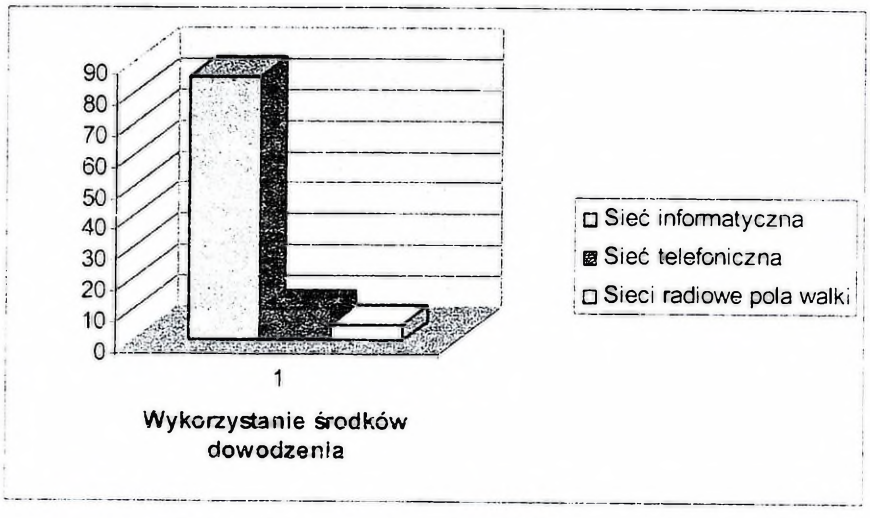
Wnioski i spostrzeżenia w zakresie przeprowadzonych badań:

1. **Urządzenia końcowe (abonenckie)** -- zaobserwowano w czasie ćwiczenia, że większość osób funkcyjnych pracujących na stanowiskach dowodzenia przesyła informacje przede wszystkim korzystając z terminali komputerowych. Dokonana analiza ilości informacji przekazywanych w określonych sieciach telekomunikacyjnych pozwoliła określić, jakie środki dowodzenia są w czasie ćwiczenia najbardziej wykorzystywane, co przedstawiono na rys. 9.

2. **Wynosy radiowe – manipulatory radiowe** – liczba tego typu urządzeń nie powinna być zbyt duża ze względu na niewielkie zapotrzebowanie na tego rodzaju łączność. Powinny funkcjonować dla tych zespołów, które posiadają „własne sieci radiowe" lub wymagają uzyskiwania informacji droga radiową. Za główne niedomaganie pracujących urządzeń uznano brak możliwości automatycznego wybierania poprzez wynosy z wozów dowodzenia i wozów dowódczo-sztabowych poszczególnych radiostacji w wyposażeniu tych wozów. W czasie prowadzonej obserwacji autor stwierdził, że sterowanie radiostacją KF z urządzenia wynośnego jest niemożliwe.

3. **Terminale satelitarne** – badane terminale powinny być wykorzystywane w strukturze sieci łączności dywizji do budowy linii telekomunikacyjnych o dużym zasięgu.

4. **Aparatownia zarządzania systemem łączności** – zaobserwowane możliwości techniczne aparatowni zapewniają możliwość sterowania sieciami łączności od szczebla brygady do dywizji. Wykorzystanie tego typu aparatowni w strukturze sieci łączności dywizji umożliwi realizację zadań w zakresie zarządzania i sterowania siecią telekomunikacyjną.



Rys. 9. Zakres wykorzystania środków dowodzenia na ćwiczeniu „Pierścień 2005"
Źródło: Opracowanie własne

Informatyzacja procesu wsparcia logistycznego na szczeblu związku taktycznego z wykorzystaniem elementów technologii NCW

dr inż. Andrzej WOJCIECHOWSKI
Wojskowa Akademia Techniczna

Wprowadzanie

Wojna w Iraku dowodzi, że powszechnie akceptowalne teorie wojny spychane są lamusa. Tym samym zamknięta została era wieku, w którym główna uwaga skupiała się przede wszystkim na platformie lądowego, powietrznego czy wodnego środka uderzenia lub rozpoznania. Wraz z nadejściem nowoczesnych zintegrowanych systemów informatycznych, które są ciągłym wyzwaniem dla współczesnych armii świata, pojawiała się nowa teoria walki określana mianem „sieciocentrycznych działań bojowych" (ang.: Network Centric Warfare – NCW).[1] Technologie NCW w najbliższych latach zdominują współczesne techniki informatyczne i znajdą szerokie zastosowanie w systemie dowodzenia wojskami, w tym przede wszystkim w logistyce wojskowej. Są one współczesną odpowiedzią na nowe wyznania przed jakimi stanęły przodujące armie świata u progu XXI w. Tym samym znajdują szerokie zastosowanie w procesach dowodzenia w zarządzaniu procesami logistycznymi w NATO. Dzięki połączeniom sieciowym NCW umożliwia stworzenie wirtualnych Centrów Dowodzenia i Wsparcia Logistycznego, które bezpośrednio będą mogły tworzyć obraz pola walki i śledzić łańcuch dostaw logistycznych. Rozwiązanie takie pozwala to znacznie zwiększyć potencjał bojowy wojsk.

Praktycznym przykładem wykorzystania NCW była ostatnia operacja w Iraku, gdzie system znalazł zastosowanie w dowodzeniu wojskami i sterowaniu procesami logistycznymi w łańcuchu dostaw. Dzięki stworzeniu wirtualnego obrazu pola walki, logistyka mogła reagować zgodnie ze swoją nadrzędną zasadą Just Times.

Koncepcja automatyzacji systemu wparcia logistycznego

Wraz z nadejściem nowej ery informatycznej Dowództwo Sił Zbrojnych zdąża obecnie w kierunku pełnego nasycenia podległych mu wojsk techniką komputerową. O ile w większości Wojska Lotnicze i Obrony Powietrznej oraz Marynarka Wojenna jest już pra-

[1] Termin „Sieciocentryczne działania wojenne", będący tłumaczeniem anglojęzycznego terminu „Network Centric Warfare" (NCW) w języku polskim nie posiada odpowiednika. Stosowany często jako zamiennik pojęciowy dla ogółu przedsięwzięć związanych z poszukiwaniem alternatyw dla tradycyjnych procesów dowodzenia i sterowania łańcuchem logistycznym.. Po raz pierwszy termin pojawił się w Joint Vision 2010 (SV2010) – The Vision for Future Joint Fighting. Dokument nie określa definitywnych rozwiązań, ale sugeruje zasadnicze kierunki rozwoju i działań reengineeringowych w zakresie NCW.

wie w pełni skomputeryzowana, to w wojskach lądowych, szczególnie na szczeblu taktycznym, głównie w logistyce, wprowadzanie komputerów oraz nowoczesnych systemów wspomagających kierowanie postępuje znacznie wolniej.

Stosowany obecnie na zachodzie C^4 *Computerized Command, Control Communication and Intelligence* można tłumaczyć jako „jedność" dowodzenia, kontroli komunikacji komputerowej. Pełne opanowanie tych czterech dziedzin telekomunikacyjnych ma decydujący wpływ na osiągnięcie powodzenia w warunkach szybkich zmian sytuacji na współczesnym polu walki.

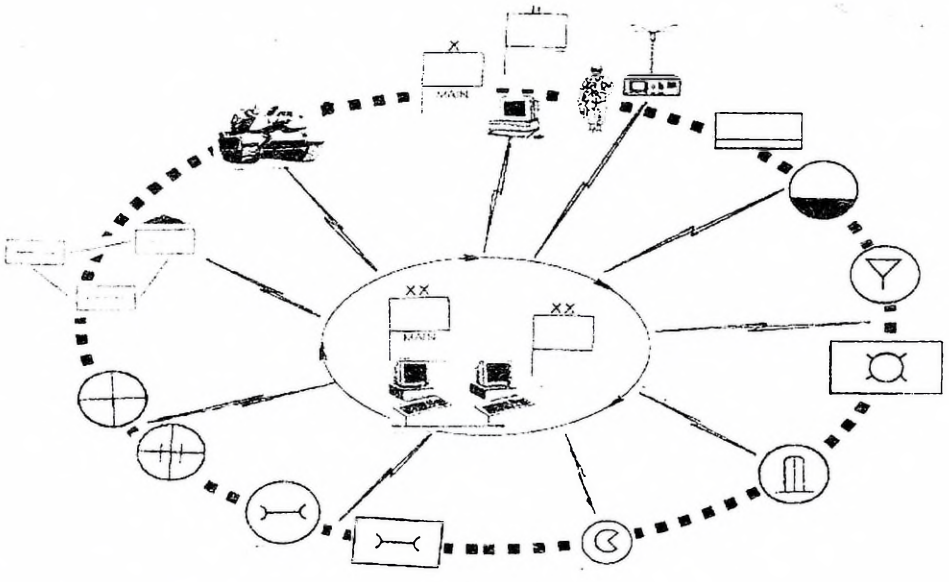
Decyzje dowódcy zależą zarówno od posiadanych informacji o przeciwniku jak też o wojskach własnych. Wszelkie opóźnienia, pomyłki i błędne kalkulacje wynikają z faktu otrzymywania informacji o sytuacji bojowej w czasie nierzeczywistym tzn. na podstawie meldunków uzyskiwanych z pewnym opóźnieniem bezpośrednio od walczących wojsk.

Dowódca *(odpowiedzialny za zabezpieczenie logistyczne)* nie może tracić czasu w oczekiwaniu na informacje o walczących wojskach. Muszą one być relewantne i napływać na bieżąco w miarę rozwoju sytuacji bojowej, gdyż w przeciwnym wypadku straty mogą prowadzić do niepowodzenia. Zniszczenie systemu łączności i przerwanie dopływu informacji może mieć katastrofalne następstwa. Znaczący wpływ na ogólną sytuację bojową mają także złe, wzajemnie niedopasowane systemy wspomagania dowodzenia poszczególnych rodzajów sił zbrojnych. Jak długo pozostaną w wyposażeniu wojsk urządzenia starego typu i nie zostanie wprowadzony jednolity system teleinformatyczny zapewniający natychmiastowe, pewne i wszechstronne połączenia z podległymi wojskami tak długo będą istniały warunki zagrożenia systemu łączności.

W armiach zachodnich spycha się do lamusa technologię dowodzenia polegającą na przesyłaniu rozkazu o wsparciu logistycznym przy wykorzystaniu „gońca". Siła działań skoncentrowana jest na przesłaniu rozkazu, informacji logistycznej w czasie rzeczywistym. Posiadanie takich danych stwarza nieograniczone możliwości, a przede wszystkim zwiększa potencjał elastyczności reagowania pododdziałów logistycznych na polu walki. Działania takie możliwe są przy zastosowaniu najnowszych technologii informatycznych wykorzystujących zautomatyzowane systemy dowodzenia i wsparcia logistycznego.

Z technicznego punktu widzenia system taki na szczeblu taktycznym powinien posiadać odpowiednią architekturę oraz zapewniać:

- przystosowanie systemów łączności i systemów komputerowych do nowoczesnego sposobu komutacji połączeń na szczeblu taktycznym przy rezygnacji z węzłowego systemu sieci łączności z wykorzystaniem central;
- objęcie systemem łączności wszystkich walczących wojsk za pomocą torów integrujących system pod względem użytkowników i usług;
- integracja użytkowników na polu walki ze wszystkimi źródłami informacji;
- możliwość przekazywania danych o kierowaniu wojskami na niższe szczeble dowodzenia;
- możliwość składania meldunków przez podwładnych;
- bieżącą aktualizację danych logistycznych;
- połączenie sieci z ogólnym systemem nawigacyjnym.



Rysunek 1. Przykład taktycznej sieci wymiany informacji

Architekturę systemu przedstawioną na rys. 1. tworzy sieć wzajemnie powiązanych, w sposób elektroniczny, pododdziałów, środków (elementów systemów dowodzenia, optoelektronicznego rozpoznania, analizy, transmisji, oraz danych o przeciwniku) przeznaczonych do przesyłania i analizowania danych przez dowódców i pion G4.

W celu stworzenia systemu o takich właściwościach należy wykorzystać (opracować) na szczeblu taktycznym zintegrowany system dystrybucji informacji, który ma usprawnić wymianę informacji między pododdziałami i rodzajami wojsk oraz zapewnić dowódcom szczebla taktycznego łączność odporną na zakłócanie i podsłuch pozwalającą na precyzyjną nawigację i automatyczną identyfikację korespondenta.

Powinien to być cyfrowy system komputerowy pracujący w bardzo krótkich przedziałach czasowych lecz przesyłający bardzo dużą ilość informacji. Nadawany do wspólnej sieci meldunek powinien być kierowany do ogólnego banku danych dostępnego dla wszystkich użytkowników włączonych do sieci pętlicowej. Sieć powinna składać się z:

- wielozadaniowego komputera cyfrowego sterującego pracą urządzeń końcowych, w czasie rzeczywistym, formułującym meldunki wejściowe i wyjściowe oraz sterujący systemowym podziałem czasowym;
- procesora sygnałowego, czyli urządzenia przystosowanego do współpracy z przewodowymi urządzeniami łączności wykorzystujący logikę stałą, zawierające układ modulatora i demodulatora *(modem)*, układy szyfrowania;
- urządzenia diagnozującego system;
- urządzeń nadawczo-odbiorczych *(abonenckich)* posiadających interfejsy przyłączeniowe do sieci w ruchomych stanowiskach dowodzenia;
- taktycznych cyfrowych urządzeń fotokopiujących pozwalających na szybkie przesyłania kopii dokumentów *(drukowanych, pisanych odręcznie, map i szkiców sytuacyjnych, fotografii)* standardowymi kanałami cyfrowymi;
- telefonów cyfrowych;
- urządzeń zabezpieczających odbiorniki przed zakłóceniami celowymi i przypadkowymi.

W tak rozumianej sieci potrzebujący informacji uzyskuje ją bezpośrednio bez wnikania w źródło jej pochodzenia i bez wyczekiwania na połączenie. Informacja lub meldunek dotyczący wykonywanego zadania mogą być przyjęte bezpośrednio lub wyszukane w banku danych. O konieczności wyszukania informacji decyduje zapotrzebowujący. Informację dostarcza wówczas automatyczny bank danych, który aktualizowany jest na bieżąco. Odbierane przez sieć meldunki mogą być przekazywane bezpośrednio do innych systemów informatycznych w relacji *„komputer – komputer"* bądź też na zasadzie ciągłego nasłuchu lub wydruku.

Meldunek *„wczytany"* do banku danych może być przeznaczony do wykorzystania ogólnego lub skierowany do jednego względnie wielu odbiorców.

Pętlicowa struktura sieci eliminuje punkty węzłowe a tym samym ogniwa pośrednie służące do przełączania pozostałych użytkowników systemu. Z tego też względu system jest odporny na zniszczenia strukturalne. W systemie proponuję zastosować dwa rodzaje urządzeń końcowych: małe – dla pojedynczych egzemplarzy UiSW np. czołgi, bwp, PRPT, GER oraz duże – dla stanowisk dowodzenia, tyłowych stanowisk dowodzenia. Różnica pomiędzy wielkością tych urządzeń polega tylko na pojemności zastosowanych komputerów.

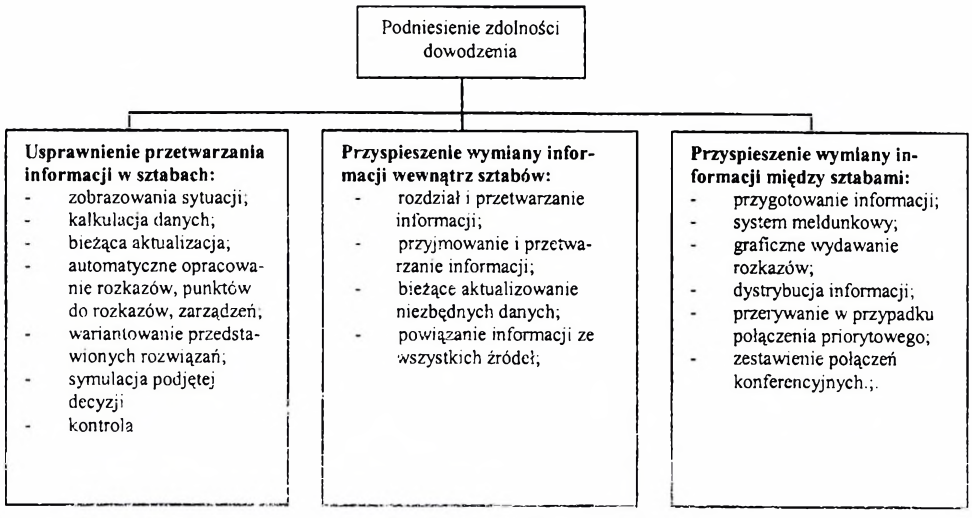
Proponowane rozwiązanie zautomatyzowanego systemu dowodzenia w równym stopniu wykorzystywane byłoby do wspomagania procesów decyzyjnych dowódcy w zakresie zabezpieczenia logistycznego *(przetwarzanie danych logistycznych, kierowania przemieszczaniem pododdziałów logistycznych, zbierania i opracowywania danych z zakresu zabezpieczenia materiałowego, technicznego i medycznego)*

Z dotychczasowych rozważań wynika, że w proponowanym zautomatyzowanym systemie dowodzenia i wsparcia logistycznego główną rolę odgrywać będą komputery, terminale i niezbędne oprogramowanie. Aktualnie większość programów informatycznych funkcjonujących w wojsku można zaliczyć do programów ewidencyjno-kontrolnych, najczęściej wycinkowego przetwarzania danych księgowych, rzadziej – kompleksowego przetwarzania danych. W pierwszym z nich realizowane jest w zasadzie tylko tradycyjne przetwarzanie danych, czyli sortowanie, sumowanie, porównywanie itp.

Dążeniem dowódców, sztabów logistyki jest eksploatacja systemów informacyjno-decyzyjnych, a więc takich w których oprócz funkcji ewidencyjnych można realizować szeroko pojęte wspomaganie decyzji dowódców i szefów logistyki. Systemy takie należy zaliczyć do najbardziej złożonych technicznie, gdyż powinny łączyć ze sobą:

- systemy ewidencyjno-kontrolne;
- systemy konwersacyjne wykorzystujące system zarządzania bazą danych *(rozproszoną lub scentralizowaną)*, umożliwiają dialogowe korzystanie z niej przez wielu użytkowników;
- systemy optymalizacyjno-symulacyjne oparte na bazach danych wykorzystującą dodatkowo bazę procedur, umożliwiając zastosowanie w szerokiej skali modeli sformalizowanych, za pomocą których dowódca może zarówno optymalizować decyzję, jak również zbadać skutki różnych wariantów decyzyjnych.

Połączenie wymienionych systemów jest jednym z najtrudniejszych zadań w zakresie stworzenia systemu zintegrowanego, który powinien zapewnić dowódcy i szefowi logistyki podniesienie skuteczności dowodzenia *(Rys. 2.)*.



Rysunek 2. Cele zautomatyzowanego systemu dowodzenia i wsparcia logistyką

Większość współczesnych komputerów pracuje w warunkach stacjonarnych np.: biurach, sztabach. Jednak dowództwa i sztaby wojskowe muszą zawsze brać pod uwagę, że urządzenia te muszą być zabierane w teren, daleko od czystych cichych i klimatyzowanych pomieszczeń. Z tego powodu komputery zastosowane w zautomatyzowanym systemie dowodzenie i wsparcia logistycznego muszą być przystosowane do działania w trudnych warunkach atmosferycznych, klimatycznych i terenowych. Muszą być konstruowane według określonych wymogów narzuconych przez wojsko *(hermetycznie zamknięte, lekkie, przenośne, odporne na impuls elektromagnetyczny, wstrząsoodporne, odporne na przeciwdziałanie radioelektroniczne przeciwnika i przechwytywanie przez z informacje, niego odporne na wysokie temperatury, charakteryzujące się dużą efektywnością wykorzystania mocy, kompatybilnością komputer - telefon, komputer - radiostacja.)*.

Tak opracowany uniwersalny sprzęt komputerowy oraz oprogramowanie powinno stanowić przyszłościową bazę systemów dowodzenia i wsparcia logistycznego na wszystkich szczeblach dowodzenia. Nim jednak zostanie on wprowadzony do wojsk musi być do końca dopracowany, przetestowany i sprawdzony w najtrudniejszych warunkach klimatyczno terenowych bezpośrednio przez użytkowników, tzn. dowódców i żołnierzy.

Dotychczas eksploatowane i użytkowane systemy informatyczne wymagają dynamicznej modyfikacji i doskonalenia. Zachodzi zatem pilna potrzeba budowy nowych standaryzowanych zintegrowanych systemów dowodzenia i wsparcia logistycznego zgodnych z zaleceniami studium C4, pakietami przystosowanymi do procedur obowiązujących w NATO, oraz wdrażanie nowoczesnych licencjonowanych technologii informatycznych kompatybilnych z ich odpowiednikami stosowanych w państwach sojuszu szczególnie w warstwach:

sprzętowej, oprogramowania podstawowego, aplikacji użytkowych, sieci komputerowych i zarządzania systemami.

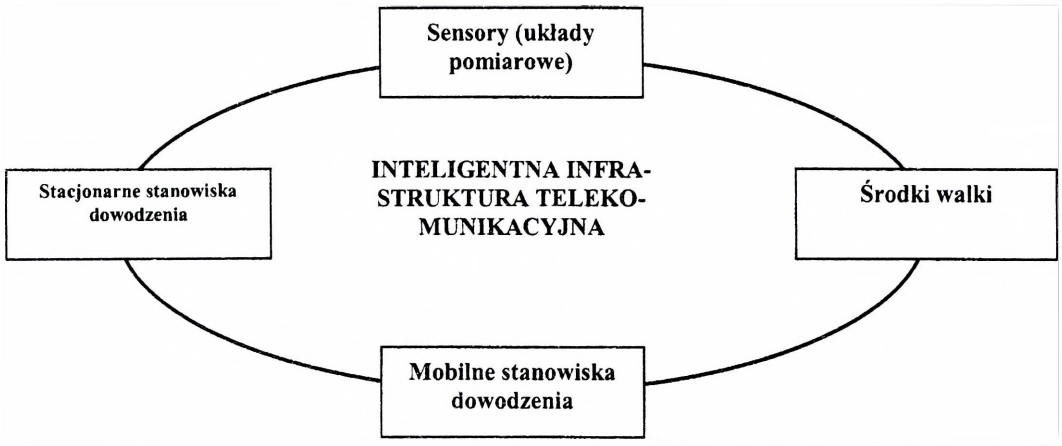
Elementy NCW w systemie dowodzenia i wsparcia logistycznego

Zastosowanie technologii NCW w działaniach wojennych, w tym również w logistyce jest punktem zwrotnym w sferze doktrynalnych koncepcji sztuki operacyjnej i taktyki. Istotą działania technologii NCW jest przede wszystkim kształtowanie przewagi militarnej w czasoprzestrzennej sieci procesów walki. Możliwe jest to poprzez budowę odpowiedniej infrastruktury sieciowej.

Architekturę sieci NCW przedstawiono na rysunku 3.

Właściwe przygotowanie architektury NCW polega na stworzeniu odpowiedniego systemu przypominającego swoją budową uporządkowaną siatkę. Architektura siatki tworzona jest przez trzy składowe: siatkę informacyjną, siatkę sensorów oraz siatkę środków walki. Zadaniem siatki informacyjnej (ang. information grid) jest obsługiwanie, przyjmowanie, przetwarzanie, przesyłanie, zapamiętywanie i zabezpieczanie selektywnej informacji niezbędnej dowódcom do walki. Stanowi ona „serce" obliczeniowe sieci NCW umożliwiające dokonywanie analiz najświeższych dostępnych danych niezbędnych do planowania. Siatki sensorów czyli elementów zdobywających informację (ang. sensor grids) są podstawowym wyposażeniem platform centrycznych pracujących na lądzie, w powietrzu, na morzu, w przestrzeni kosmicznej. Pod tym pojęciem rozumieć należy element rozpoznawczy (np. elektroniczny, optyczny itd.), mogący rozpoznać przetworzyć i wprowadzić dane o polu walki do sieci. Mogą one być umieszczone na okrętach, samolotach, kontenerach oraz samochodach specjalnych.[2] Siatka zapewnia posiadanie wysokiej jakości danych o sytuacji sił własnych, sił przeciwnika oraz środowiska w jakim prowadzone są działania bojowe. Siatka środków walki (ang. engagement grids) jest ogniwem umożliwiającym wykorzystanie własnych środków walki do osiągnięcia określonego efektu w czasie i przestrzeni.

[2] Sensory w armii amerykańskiej są na wyposażeniu indywidualnym żołnierzy i służb logistycznych są nimi np. kamery montowane w hełmach. Stworzenie gęstej siatki sensorów zwiększa prawdopodobieństwo dokładności przesyłanej informacji.



Rysunek 3. Architektura systemu NCW
Źródło: Opracowanie własne

Istotną rolę przy tworzeniu sieci NCW jest stosowanie odpowiednich modeli referencyjnych. Stanowi ona istotne wyzwanie intelektualne dla dyscypliny, która w literaturze jest określana jako Command and Control Systems Science. Do głównych problemów przedstawionej dyscypliny należy system referencyjnych, analitycznie konstruowanych pojęć, zapewniający nie tylko sprawność i jednoznaczność definiowania koncepcji doktrynalnych, lecz także jednolitość ich rozumienia w różnych, z reguły interdyscyplinarnych, obszarach implementacyjnych.

W szczególności dotyczy to specjalistów zaangażowanych w problematykę planowania badań i rozwoju infrastruktury informacyjnej – również związanej z bazą algorytmów taktyczno – operacyjnych i modelowaniem działań wojennych.

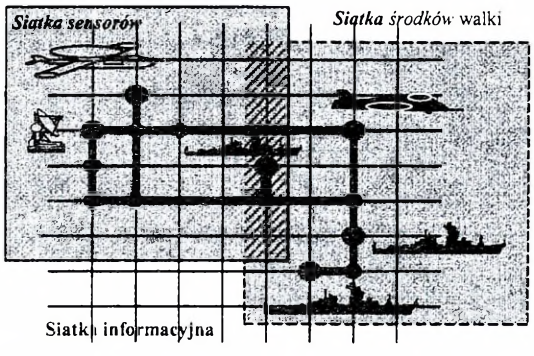
Zasadniczą role przy konstruowaniu aparatu pojęciowego odgrywają modele referencyjne.[1] W swojej istocie powinny one charakteryzować się:

- dynamicznością, a więc zdolnością do reprezentowania zjawisk opisywanych w sposób analitycznych;
- strukturalnością, to zdolność reprezentowania elementów będących przedmiotem modelowania, jak również zdolność do opisania relacji między tymi elementami;
- otwartością, polegającą na rozbudowie modelu pod względem liczby elementów i relacji między nimi poprzez rozbudowę obiektu opisywanego w postaci zapisu analitycznego;
- analitycznością, polegającą na algorytmizacji opisywanych zjawisk;
- możliwością symulacyjną, czyli zastosowaniu technik symulacyjnych, za pomocą standardowych, jednolitych narzędzi informatycznych, bez potrzeby tworzenia nowych, specyficznych programów komputerowych umożliwiających symulowanie zjawisk;

- komplementarnością, możliwość jednolitego ujęcia modelu w triadzie pojęć <Command- - Communication – Intelligence>.

Sieć NCW jest teoretycznym zbiorem pojęć składającym się z układów sensorów i środków walki rozpiętych na siatce informacyjnej wykorzystującą infrastrukturę telekomunikacyjną. Zadaniem tak powstałej sieci jest przesłanie informacji w dowolnym kierunku sieci dowodzenia oraz łańcucha dostaw logistycznych. Ponadto umożliwia ona stworzenie koherentnego obrazu pola walki, wypracowanie hipotez o potencjalnych zagrożeniach jakie może stworzyć przeciwnik co w efekcie wykorzystuje się do przeprowadzenie odpowiedniego przeciwdziałania. [1].

Przykład siatki sensorów i środków walki rozpiętych na siatce informacyjnej przedstawia rysunek 2.



Rysunek 4. Siatka sensorów i środków walki rozpięta na siatce informacyjnej
Źródło: Keus Hans E., Network Centric Operations: Implications for Allied and Coalition Operations, SMI Conferences on Network Centric Warfare, London, October 2000r., s. 4

Przedstawiona na rysunku siatka NCW umożliwia zbieranie informacji źródłowej i przesyłanie jej do centralnych stanowisk dowodzenia. Przetworzona informacja jako źródło wiedzy dowódców wykorzystywana jest do podejmowania właściwej decyzji. Decyzja dowódców przekazywana jest w czasie rzeczywistym do wszystkich podległych jednostek. Informacja taka szczególnie jest istotna dla służb logistycznych, w tym oficerów zajmujących się prognozowaniem zużyciem amunicji.

Siatka umożliwia wirtualizację informacji. Oznacza to w praktyce zastąpienie dialogowej wymiany dokumentów poprzez udostępnienie informacji źródłowej „pożądanemu" odbiorcy poprzez aktywny portal teleinformatyczny. W ten sposób użytkownicy sieci, jakimi są między innymi dowódcy i służby logistyczne odpowiedzialne za realizację procesów logistycznych, w tym zaopatrywania w amunicje, posiadają aktualną, rzeczywistą informację o sytuacji na polu walki. Informacje docierają do użytkowników w czasie rzeczywistym. Takie rozwiązanie jest szczególnie ważne dla służb logistycznych realizujących zadania wsparcia

wojsk walczących. Umożliwia ono bieżące planowanie oraz prognozowanie zużycia środków bojowych. Tym samym pozwala to na zarządzanie łańcuchem dostaw logistycznych rzeczywistym. Dodatkowym atutem technologii NCW jest możliwość włączenia do sieci systemu śledzenia zasobów logistycznych i wykorzystanie platformy LOGFASS. [2]

Zakończenie

Wizja - połączenia koncepcji NCW z tradycyjnym systemem kierowania zabezpieczeniem logistycznym - stworzenia tym samym nowoczesnego SDiWL w postaci maszyny matematycznej jest bardzo zachęcająca. Podchodząc jednak do sprawy racjonalnie, trzeba stwierdzić, że wprawdzie komputery mogą eliminować trudne i żmudne obliczenia, umieją ukierunkować strumienie napływających meldunków i informacji, tych danych do odbiorców, to czy umieszczenie komputera w *„zielonej skrzynce"* i nazwania go sprzętem wojskowym jest już wystarczające.

Koncepcja wojny sieciocentrycznej w najbliższych latach stanie się zapewne odpowiedzią na nowe zapotrzebowanie sił zbrojnych w XXI w. jakim będzie informacyjne wsparcie działań bojowych. Dowodzenie sieciocentrycznym łańcuchem działań bojowych, w tym logistycznych w najbliższych latach stanie się rzeczywistością. Sieciocentryczne podejście do procesów powoduje, że wkraczamy w nową dobę walki zbrojnej. Zapewne przedstawiona wizja przemian technologicznych wykorzystywanych do celów wojskowych, jeszcze szokuje. Należy jednak zdawać sobie sprawę, że nie da się jej zmienić i zapewne uniknąć. Nowoczesne armie świata, w tym również siły zbrojne RP poprzez swoje ośrodki naukowe prowadzą badania w tym zakresie.

Konstatując można wysnuć tezę, że koncepcja działań NCW przekłada przewagę informacyjną na siłę uderzenia poprzez efektywne połączenie (fizyczne i logiczne) elementów pola walki wyposażonego w wiedzę. Armie, które zdecydują się na pozostanie przy starych technikach działania nie tylko szybko znajdą się na marginesie nowoczesności, ale także niewiele będą miały do powiedzenia na ewentualnym współczesnym polu walki.

Literatura

1. Wojciechowski A., Zautomatyzowany system dowodzenia logistyką na szczeblu taktycznym. Biuletyn Instytutu Automatyzacji Systemów Dowodzenia i Logistyki, WAT 2003 r.
2. Wojciechowski A., Koncepcja zautomatyzowanego systemu dowodzenia i wsparcia logistycznego, Myśl Wojskowa nr 2/2003

Więzi informacyjne stanowisk dowodzenia szczebla taktycznego wojsk lądowych

dr hab. inż. Jarosław WOŁEJSZO
Akademia Obrony Narodowej

O jakości i sposobie przepływu informacji w dowództwach szczebla taktycznego wojsk lądowych decyduje struktura informacyjno-decyzyjna, przez którą należy rozumieć określony jakościowo i organizacyjnie stały porządek przestrzenno-czasowych relacji, związanych z wymianą różnych informacji, zwłaszcza rozkazów, zarządzeń i decyzji oraz meldunków, sprawozdań, danych o przeciwniku, jego możliwościach bojowych oraz parametrach taktyczno-technicznych wykorzystywanych środków walki. Obieg tego rodzaju informacji pomiędzy zhierarchizowanymi organami dowodzenia i elementami tworzącymi zgrupowania zadaniowe, funkcjonującymi na określonych poziomach dowodzenia, odbywa się za pomocą środków łączności i informatyki. Każdy element tej struktury stanowi mniej lub bardziej rozbudowany węzeł sieci informacyjnej, w którym zbiegają się zbiory informacyjne (informacja sytuacyjna i informacja decyzyjna) pochodzące z różnych źródeł, w postaci ustalonych sygnałów, najczęściej depesz (telegramów) oraz maszynowych nośników informacji. Środki i relacje łączności oraz dokonywane w nich procesy informacyjne jednoczą poszczególne elementy składowe systemu w jednolitą, zintegrowaną informacyjno-decyzyjną całość, z nałożonymi obwodami informacyjno-decyzyjnymi podsystemów: *organów i stanowisk dowodzenia, łączności, rozpoznania i kontroli sytuacji.*

Struktura organizacyjna dowództw szczebla taktycznego dotyczy zbioru stosunków organizacyjnych, czyli takich, które mają znaczenie w realizacji określonego celu działania i których wyrazem są określone więzi organizacyjne.

Mianem *więzi informacyjnych dowództw szczebla taktycznego wojsk lądowych* można określić utrwalone drogi przepływu informacji między elementami danego dowództwa bądź między danym dowództwem a systemem wyższego przełożonego i otoczeniem, niezbędne do integrowania i koordynowania prowadzonej działalności.

W literaturze przedmiotu podkreślane jest wielokrotnie, że pod względem organizacyjnym *system dowodzenia*, tak jak każdy system kierowania, stanowi zbiór określonych relacji sprzężonych ze sobą informacyjnie lub technicznie, niezależnie od hierarchicznego poziomu (szczebla) dowodzenia. Jest, więc on zbiorem ludzi wyposażonych w określone środki dowodzenia, powiązanych ze sobą, odpowiednio do struktury organizacyjnej poszczególnych do-

wództw oraz decyzji dowódcy podejmowanych w ramach wykonywania funkcji dowodzenia. Infrastrukturę systemu dowodzenia na szczeblach taktycznych wojsk lądowych stanowią:

– *mobilno-stacjonarne i mobilne* (*aeromobilne*) stanowiska dowodzenia organizowane na szczeblach taktycznych;

– *sieci telekomunikacyjne* organizowane przy użyciu środków łączności: radiowej, radioliniowej, przewodowej, satelitarnej;

– *sieci informatyczne* organizowane przy użyciu urządzeń i środków informatycznych dostarczających informacji o sytuacji: powietrznej, lądowej, elektromagnetycznej (w eterze), chemicznej (punkty obserwacji wzrokowej lub technicznej i elementy zintegrowanego rozpoznania) itp.

Reasumując stwierdzić można, że *system dowodzenia szczebla taktycznego wojsk lądowych jest to hierarchicznie uporządkowany zbiór stanowisk dowodzenia funkcjonujący w środowisku sieci łączności i informatyki oraz kierujący działaniami w obszarze powietrzno-lądowym*. Ważnym elementem w tym systemie dowodzenia są stanowiska dowodzenia, które stanowią centra kierowania działaniami. Umożliwiają one dowódcy dowodzenie w każdym rodzaju działań. Stanowiska dowodzenia, powiązane ze sobą funkcjonalnie i informacyjnie w określonym układzie poziomym i pionowym, są ważnymi elementami całego systemu dowodzenia. W wojskach lądowych na szczeblach taktycznych powinno się organizować następujące rodzaje stanowisk dowodzenia:

– *stale funkcjonujące*: główne stanowiska dowodzenia (GSD), zapasowe stanowiska dowodzenia (ZSD), tyłowe stanowiska dowodzenia (TSD),

– *doraźnie funkcjonujące*: wysunięte stanowiska dowodzenia (WSD), punkty dowódczo-obserwacyjnych (PDO) i powietrznych punktów dowodzenia (PPD) – wydzielane z GSD.

Przeprowadzone analizy literatury pozwalają sądzić, że w wojskach lądowych na szczeblach taktycznych przyjmuje się tworzenie i funkcjonowanie następujących *typów* stanowisk dowodzenia:

– *mobilno-stacjonarne,*

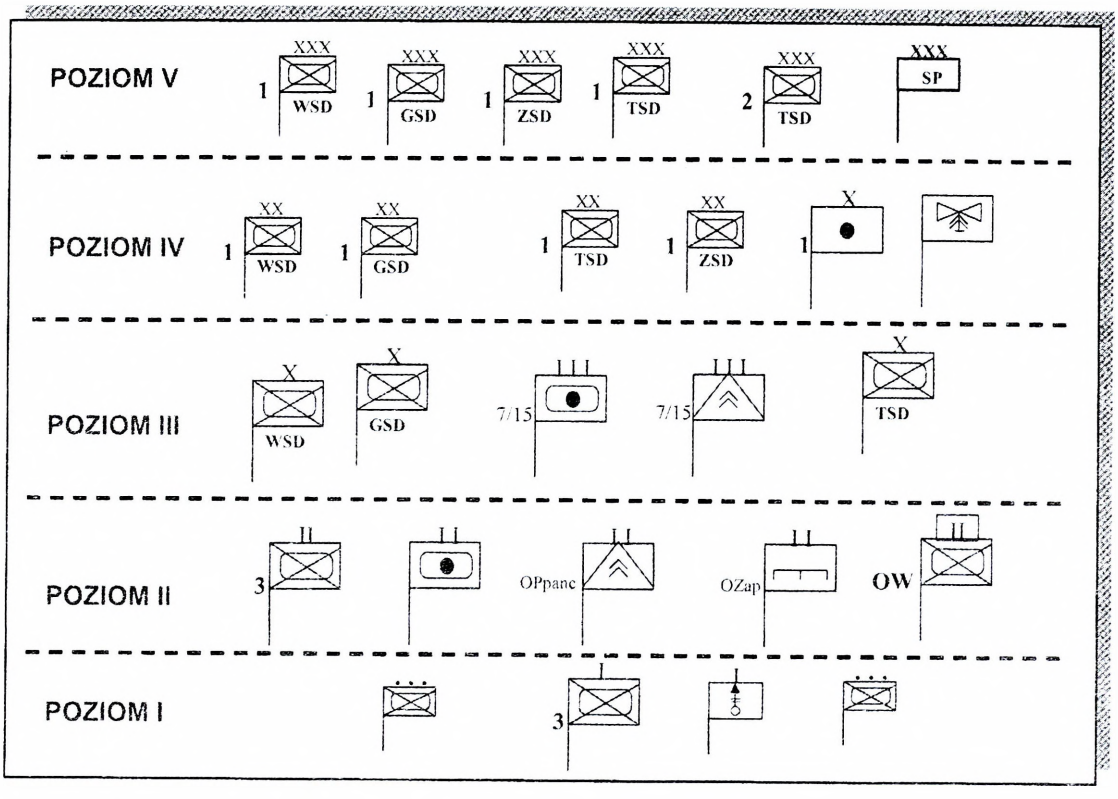
– *mobilne (aeromobilne).*

Mobilno-stacjonarne stanowisko dowodzenia może być rozmieszczane w obiektach, które nie pokrywają potrzeb w zakresie łączności, a mobilne środki łączności stanowią główną bazę w zakresie zaspokojenia potrzeb dowodzenia na usługi łączności i informatyki.

Mobilne (aeromobilne) stanowisko dowodzenia jest przygotowane do rozmieszczenia w każdych warunkach i rejonach, z wykorzystaniem i bez obiektów stacjonarnych, a praca

sztabowa prowadzona byłaby na środkach mobilnych lub aeromobilnych, autonomicznych pod względem usług łączności i informatyki.

Wieloaspektowe ujęcie tej problematyki zostało przedstawione w książce *Stanowiska dowodzenia w wojskach lądowych* autorstwa J. Michniaka, który proponuje wyróżniać (rys. 1.) następujące poziomy dowodzenia.



Rysunek 1. Poziomy dowodzenia wojskami lądowymi na szczeblach taktycznych
Źródło: opracowanie własne na podst. J. Michniak, Stanowiska dowodzenia w wojskach lądowych, AON, Warszawa 2003, s. 15–16

Pierwszy poziom stanowią główne stanowiska dowodzenia pojedynczych pododdziałów (elementów ugrupowania).

Drugi poziom to stanowiska dowodzenia wydzielonych oddziałów, desantów taktycznych oraz batalionów (równorzędnych), a także jednostek brygadowych.

Trzeci poziom stanowią stanowiska dowodzenia (GSD, TSD i WSD), brygad i jednostek dywizyjnych.

Czwarty poziom tworzą stanowiska dowodzenia organizowane na szczeblu dywizji, tj. główne stanowisko dowodzenia (GSD), zapasowe stanowisko dowodzenia (ZSD), tyłowe

stanowisko dowodzenia (TSD), wysunięte stanowisko dowodzenia (WSD) i stanowiska dowodzenia jednostek korpusu, w tym pododdziałów lotnictwa wojsk lądowych.

Piąty poziom stanowią stanowiska dowodzenia organizowane na szczeblu korpusu zmechanizowanego, tj. główne stanowisko dowodzenia (GSD), zapasowe stanowisko dowodzenia (ZSD), tyłowe stanowisko dowodzenia (TSD), wysunięte stanowisko dowodzenia (WSD) oraz stanowiska dowodzenia pozostałych związków operacyjnych (ZO), związków operacyjno-taktycznych (ZO-T) i dowództw (sztabów) współdziałających (POW, SOW, KOP, Kl, itp.).

Stosując ten podział dowodzenia ze względu na poziomy ich organizacyjnego rozmieszczenia zrozumieć można lepiej, architekturę systemu dowodzenia szczebla taktycznego w wojskach lądowych. Zrozumienie jej jest potrzebne do zaprojektowania więzi informacyjnych występujących pomiędzy poszczególnymi stanowiskami dowodzenia.

Analiza literatury przedmiotu wykazuje, że w organizowanych stanowiskach dowodzenia zawsze występują określone komponenty (dla przykładu rys. 2.).

Mogą nimi być:

1) *organa dowodzenia* – zorganizowane w zespoły funkcjonalne odpowiadające obszarom problemowym dowodzenia; są one głównym elementem części operacyjnej stanowisk dowodzenia przeznaczonym do sprawowania dowodzenia;

2) *węzeł telekomunikacyjny i siły poczty polowej* – zapewniają przepływ informacji poprzez techniczne i pocztowe środki łączności oraz obiegu informacji wewnątrz stanowiska dowodzenia i między stanowiskami dowodzenia zgodnie z zasadami organizacji łączności dowodzenia, współdziałania i powiadamiania (ostrzegania, alarmowania);

3) *grupę zabezpieczenia* – organizującą wszechstronne zabezpieczenie bojowe i logistyczne stanowiska dowodzenia.

Ponadto w pobliżu rejonu stanowiska dowodzenia, w zależności od szczebla, organizuje się lądowisko dla śmigłowców łącznikowych i PPD oraz punkt wymiany poczty polowej (PWPP) ze składu wojskowej stacji pocztowej (WSP) stanowiska dowodzenia.

Liczba poszczególnych komórek organizacyjnych stanowisk dowodzenia oraz wielkość obsady personalnej uzależnione są od wielu czynników. Można do nich zaliczyć:

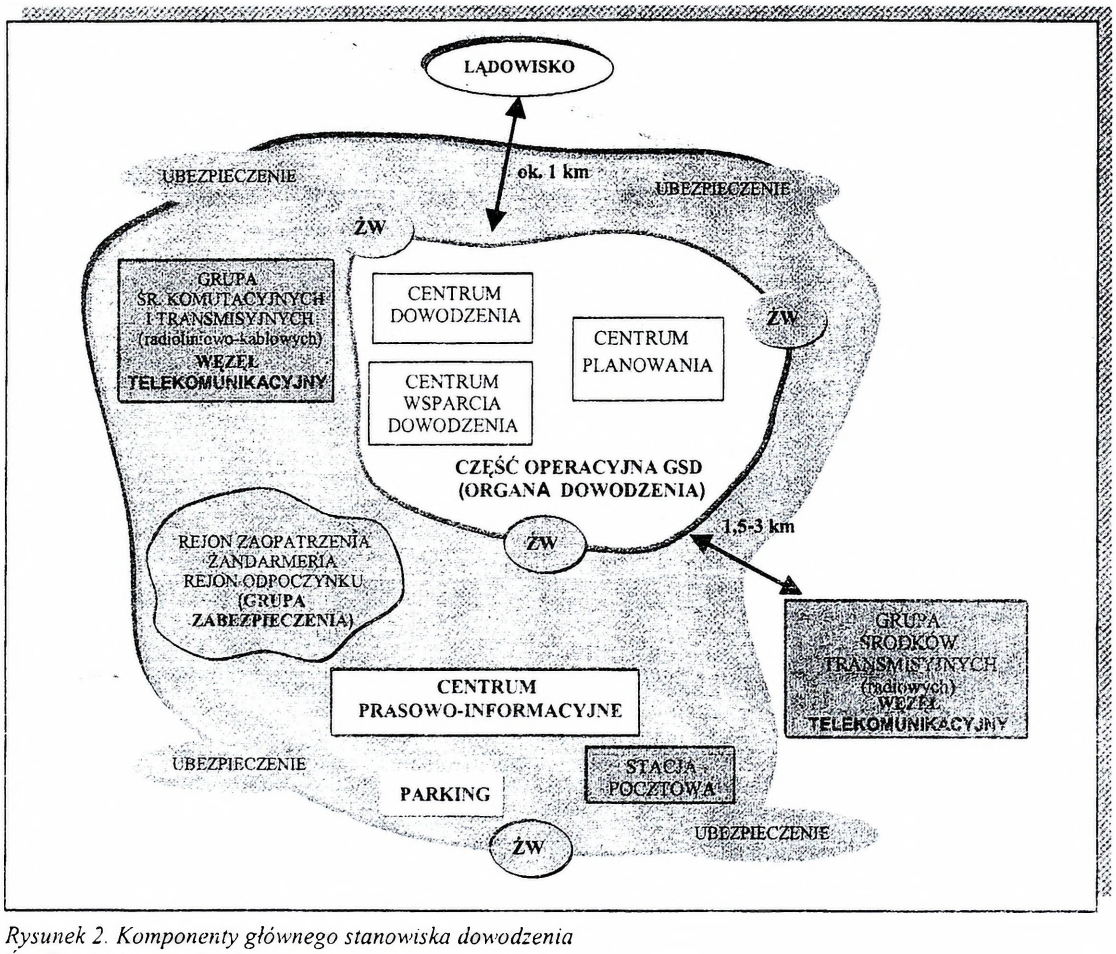
– zadania, jakie ma realizować dany zespół stanowiska dowodzenia,

– stopień przygotowania personelu i wyposażenia w techniczne środki dowodzenia,

– wymogi określane przez zasady organizacji rozmieszczenia i pracy stanowisk dowodzenia,

– potrzebę zapewnienia ciągłości pracy podczas 24 godzin z uwzględnieniem systemu dwuzmianowego,

– wytyczne dowódcy i szefa sztabu.



Rysunek 2. Komponenty głównego stanowiska dowodzenia
Źródło: opracowanie własne

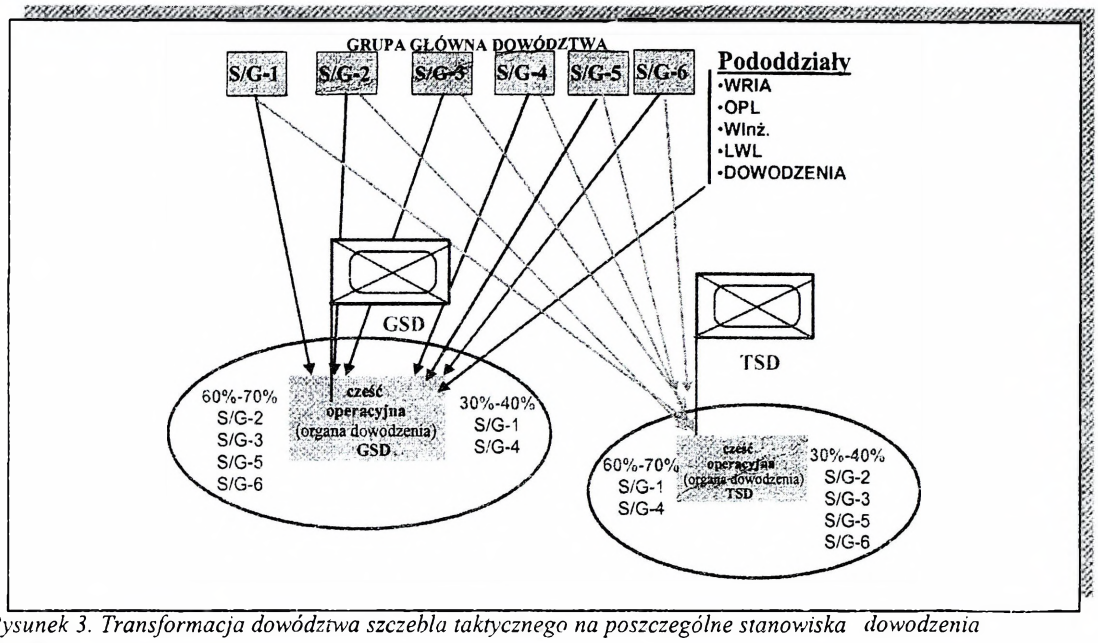
Aby uzyskać pełną strukturę stanowiska dowodzenia, należy dokonać podziału dowództwa na stanowiska dowodzenia. Podczas konwersji dowództwa szczebla taktycznego (rys. 3 i 4), należy przestrzegać reguły zachowania specyfiki poszczególnych komórek organizacyjnych dowództwa z poszczególnymi zespołami centrów stanowisk dowodzenia.

Centrum Planowania (CP) – w skład tego zespołu wchodzą specjaliści z poszczególnych grup od S/G-1 do S/G-6 dowództwa oraz specjaliści rodzajów wojsk z S/G-3.

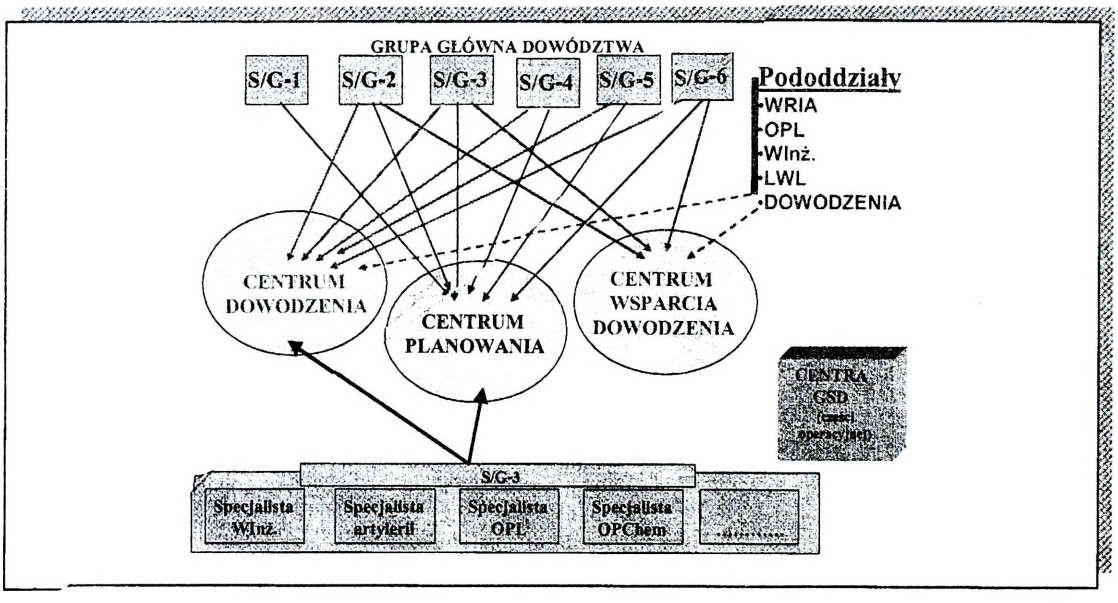
Centrum Dowodzenia (CD) – w skład tego zespołu wchodzą specjaliści z poszczególnych grup od S/G-2 do S/G-6 dowództwa oraz specjaliści rodzajów wojsk z S/G-3. Dodatko-

wo w skład tego centrum mogą wchodzić grupy operacyjne dowódców jednostek wsparcia po przybyciu na główne stanowisko dowodzenia danego szczebla.

Centrum Wsparcia Dowodzenia (CWDow*)* – w skład tego centrum wchodzą poszczególni specjaliści z S/G-6, S/G-3 i S/G-2 oraz dodatkowo po przybyciu na główne stanowisko dowodzenia grupa operacyjna z pododdziału (oddziału) dowodzenia.

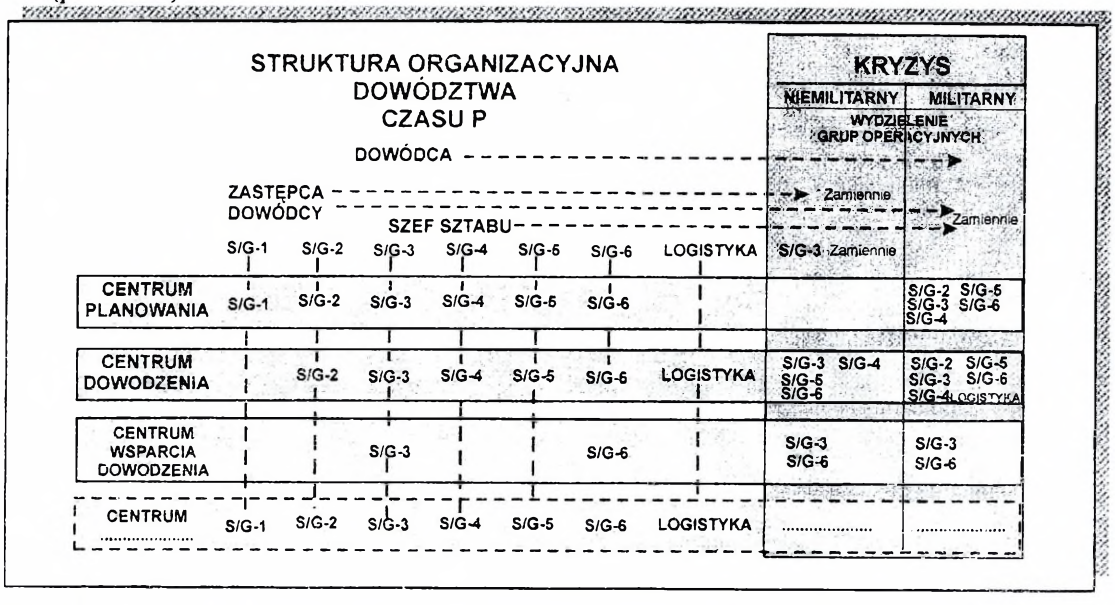


Rysunek 3. Transformacja dowództwa szczebla taktycznego na poszczególne stanowiska dowodzenia
Źródło: opracowanie własne

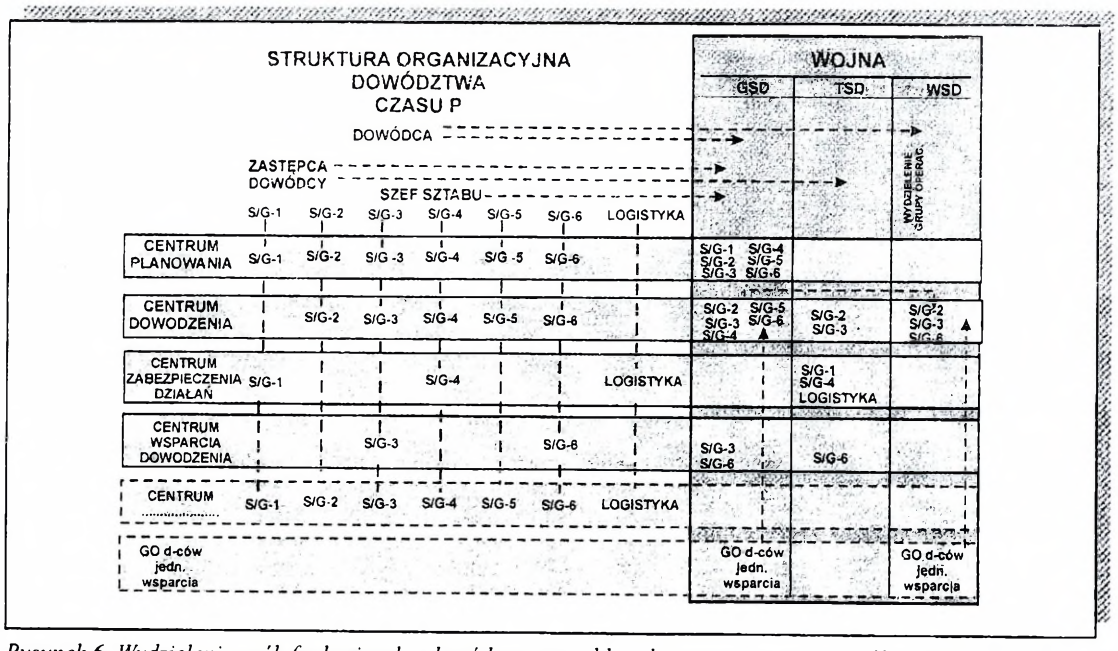


Rysunek 4. Transformacja dowództwa na poszczególne centra części operacyjnej głównego stanowiska dowodzenia
Źródło: opracowanie własne

Przeprowadzone analizy przez autora pozwalają stwierdzić, że zastosowanie struktury sieciowej (rys. 5 i 6) do transformacji dowództwa szczebla taktycznego wojsk lądowych na poszczególne stanowiska dowodzenia jest bardziej praktyczne. Unika się zmiany nazwy danego specjalisty dowództwa, gdyż i w jednym, i drugim wypadku występuje on np. jako oficer (podoficer) S/G-3.



Rysunek 5. Wydzielenie grup operacyjnych z dowództwa szczebla taktycznego w trakcie realizacji zadań w okresie kryzysu
Źródło: opracowanie własne



Rysunek 6. Wydzielenie osób funkcyjnych z dowództwa szczebla taktycznego na poszczególne stanowiska dowodzenia
Źródło: opracowanie własne

Zastosowanie tej metody wydaje się bardziej zasadne z punktu widzenia realizacji zadań przez poszczególne osoby funkcyjne dowództwa szczebla taktycznego w zależności od rodzaju kryzysu. Skład osobowy poszczególnych grup operacyjnych stanowisk dowodzenia będzie zależało od konkretnej sytuacji i decyzji dowódcy.

Na wypadek działań wojennych z dowództwa szczebla taktycznego będzie dokonana również transformacja osób funkcyjnych na poszczególne stanowiska dowodzenia, przy czym obsada personalna poszczególnych stanowisk dowodzenia zależeć będzie od decyzji dowódcy danego szczebla dowodzenia. Na szczeblach taktycznych – w związku taktycznym[1] lub oddziale – dla potrzeb dowodzenia zorganizowane zostaje główne stanowisko dowodzenia (GSD) i tyłowe stanowisko dowodzenia (TSD) oraz doraźne WSD lub PPD[2]. Rozmieszczone są one w ugrupowaniu bojowym w tyłowym pasie (rejonie). Tak skonstruowana sieć stanowisk dowodzenia zapewnia żywotność i ciągłość dowodzenia dywizją. Skład poszczególnych zespołów będzie zależał od charakteru działań prowadzonych przez związek taktyczny lub oddział.

Dowodzenie wojskami to ciągły proces wymiany informacji realizowany w poziomie (wewnątrz autonomicznego systemu informacyjnego i wewnątrz systemów peryferyjnych współpracujących) oraz w pionie (są to zadania stawiane przez przełożonych podwładnym, a także informacje zwrotne – meldunki terminowe i doraźne, jakie z kolei składają podwładni swoim przełożonym).

Proces podejmowania decyzji jest swego rodzaju procesem przetwarzania informacji już dojrzałej sytuacji decyzyjnej. Informacja[3] stanowi punkt wyjścia tego procesu, a jego rezultat – podjęta decyzja jest także informacją o tym, co, jak, kto, w jakim celu lub jak powinien działać. System generowania, przesyłania i przetwarzania danych w poszczególnych dowództwach szczebla taktycznego wojsk lądowych ma istotny wpływ na przebieg procesów decyzyjnych i trafność podejmowanych decyzji, a także na ich realizację. Sprawność działania tych dowództw zależy w dużym stopniu od tego, czy system informacyjny dobrze czy źle służy procesowi dowodzenia.

Decyzje podejmowane przez dowódców szczebla taktycznego wojsk lądowych powinny być „wystarczająco zadawalające" (najkorzystniejsze). Można je podejmować tylko w warunkach pewności, mając pełne informacje o rozwiązywanym problemie. Rzadko w warun-

---

[1] Po 2006 r. planuje się utworzyć zapasowe stanowisko dowodzenia.

[2] Doraźnie tylko w związku taktycznym lub brygadzie kawalerii powietrznej.

[3] Por. J. Kurnal, *Organizacyjne problemy kierowania zespołami pracowniczymi, Podejmowanie decyzji kierowniczych w trudnych sytuacjach decyzyjnych*, Wyższa Szkoła Menadżerska SIG, Warszawa 2001, s.47.

kach wojennych będzie dochodziło do takiej sytuacji, aby informacja dostępna dowódcy była równocześnie informacją pełną. Między pełnym czy pożądanym zasobem informacji a zasobem dostępnym z reguły występuje mniejsza lub większa luka, zwana luką informacyjną. Głównym zadaniem systemu informacyjnego w dowództwach szczebla taktycznego wojsk lądowych jest ograniczenie tej luki i dostarczenie wystarczającego zasobu informacji dowódcy o rozwiązywanym problemie, jak również o jego otoczeniu. Jednak nie chodzi w tym przypadku tylko o liczbę danych, ale także o ich jakość. Nadmiar informacji, zwłaszcza nieprzetworzonych, może być bardziej szkodliwy dla jakości podejmowanej decyzji niż ich niedobór. Szkodliwe są tzw. szumy informacyjne, czyli zakłócenia w procesie przekazywania informacji, mogące utrudnić odbiór lub zniekształcić wiadomość. System informacyjny powinien[4]:

– minimalizować (zmniejszać niedobór) lukę informacyjną,

– zapobiegać nadmiarowi informacji nieprzetworzonych i niemożliwych do opanowania,

– eliminować szumy informacyjne.

W takim kontekście zgodzić się można z tezą, że każda informacja jest szczególną formą sygnału, która oprócz wspólnych cech wyróżnialności, właściwych dla sygnału i informacji, posiada jeszcze tę właściwość, że inspiruje umysł ludzki do tworzenia pewnej wyobraźni – w sensie prakseologicznym wizji działań (czynu jako takiego).

Przyjmując ***kryterium struktury organizacyjnej***, w systemie informacyjnym w dowództwach szczebla taktycznego wojsk lądowych wyróżnia się następujące rodzaje więzi informacyjnych:

– *służbowe* (hierarchiczne, rozkazodawcze, synchronizacji) – związane z podległością służbową (można je podzielić na „w dół" – *rozkazy* i „w górę" – *meldunki*),

– *koordynacji* – związane z wymianą informacji pomiędzy osobami wewnątrz dowództw (wewnętrzne więzi informacyjne) lub wymianą informacji w ramach specjalności, uzupełnianiem potrzebnych informacji pomiędzy specjalnościami na tym samym poziomie lub pomiędzy różnymi szczeblami z pominięciem przełożonych (zewnętrzne więzi informacyjne współdziałania),

[4] Por. M. Bielski, *Organizacje (istota, struktury, procesy)*, Uniwersytet Łódzki, Łódź 1997, s. 260.

– *współdziałania* – związane z wymianą informacji pomiędzy poszczególnymi stanowiskami dowodzenia nie mającymi zależności służbowych, a wynikające bezpośrednio z wykonywanego zadania.

Stosując ***kryterium kierunku przepływu informacji***, na stanowisku dowodzenia szczebla taktycznego wojsk lądowych można wyróżnić następujące rodzaje więzi informacyjnych:

– *zewnętrzne wchodzące* – związane ze zbieraniem (gromadzeniem) informacji z szeroko pojętego otoczenia (służbowe i współdziałania, a więc np. rozkazów, meldunków czy też komunikatów),

– *wewnętrzne* – związane z wytwarzaniem i przekazywaniem informacji wewnątrz stanowiska dowodzenia (np. informacji planistycznych),

– *zewnętrzne wychodzące* – związane z przekazywaniem informacji (wytworzonych lub zebranych) poza stanowisko dowodzenia.

Porównując przedstawiane kryteria podziału więzi informacyjnych, do dalszych rozważań autor przyjął więzi organizacyjne wyrażające stosunki między poszczególnymi osobami funkcyjnymi (stanowiskami pracy) a oddziałami, wydziałami (komórkami organizacyjnymi), w których te zasoby zostały zlokalizowane. Klasyfikowane są one najczęściej ze ***względu na kierunek powiązań***. Z tego punktu widzenia więzi organizacyjne dowództwa szczebla taktycznego wojsk lądowych można podzielić na:

– służbowe (hierarchiczne) – zachodzące na tle rozmieszczenie uprawnień decyzyjnych, które posiadają w organizacjach wojskowych tylko dowódcy,

– funkcjonalne – zachodzące na tle zróżnicowania kompetencji zawodowych,

– informowania – zachodzące na tle wymiany informacji.

Warto zauważyć, że więzi *informowania* i *funkcjonalne* są wtórne w stosunku do *więzi służbowej*, która łączy dowódcę z wszystkim elementami dowództwa szczebla taktycznego. Służy ona do przekazywania poleceń i informacji z góry. Charakteryzuje się uprawnieniami danego dowódcy do decydowania o zakresie, rodzaju, czasie oraz strukturze pracy podwładnego. Przełożony jest uprawniony do przydzielania zadań, które podwładni mają wykonać, a w razie konieczności może decydować także o sposobach i kolejności ich realizacji. Tak szerokie uprawnienia mogą być również ograniczone przez szczególne rozwiązania organizacyjne.

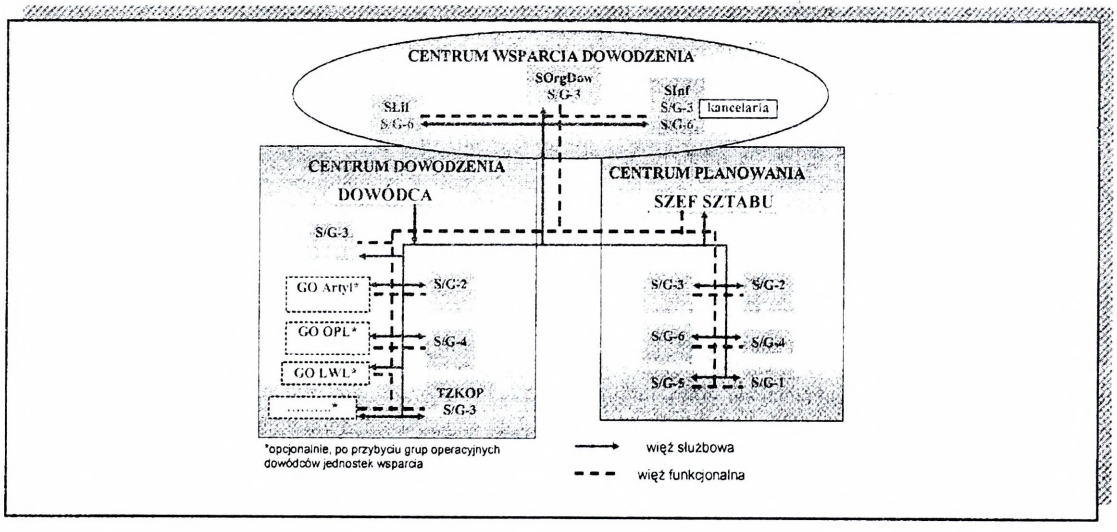
Więź funkcjonalna, która powstaje w wyniku wyodrębnienia się najpierw stanowisk pracy, później komórek organizacyjnych wspomagających merytorycznie kierowników zespołów

(sekcji) poszczególnych centrów głównego stanowiska dowodzenia. Więź ta występuje między komórkami niezależnymi od siebie służbowo.

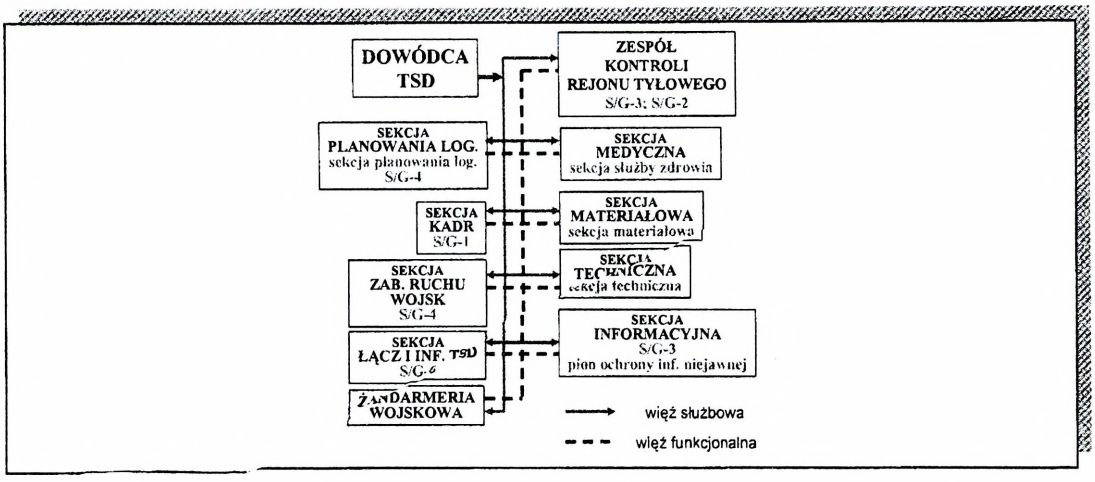
Więź informowania – na ogół pokrywa się z innymi więziami: podporządkowania, funkcjonalną, bezpośredniego zasilania i koordynacyjną. Może jednak przebiegać także niezależnie od nich.

Do określenia pełnego zbioru powiązań informacyjnych pomiędzy poszczególnymi zespołami funkcjonalnymi i osobami funkcyjnymi stanowiska dowodzenia zastosowane zostały jednocześnie: *kryterium struktury organizacyjnej, kryterium kierunku przepływu informacji oraz kierunku powiązań.*

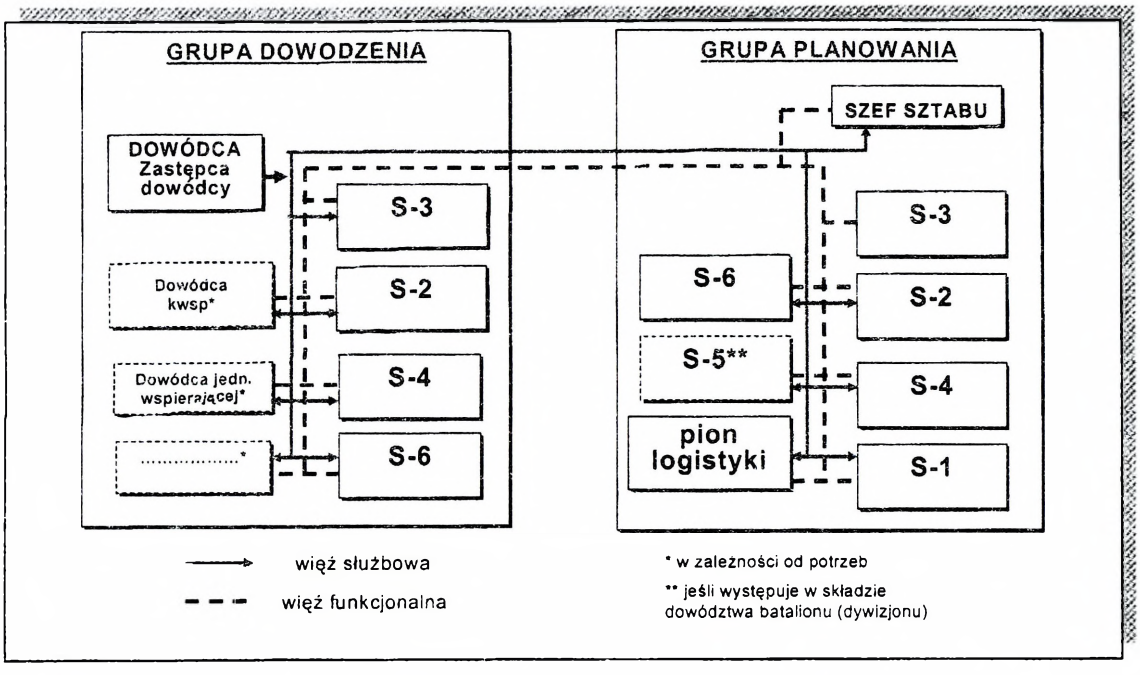
Za organizację ***wewnętrznych więzi informacyjnych*** na stanowisku dowodzenia odpowiada szef sztabu (danego szczebla organizacyjnego). Więzi te są związane z przekazywaniem informacji potrzebnych w trakcie realizacji poszczególnych faz cyklu decyzyjnego procesu dowodzenia. Poszczególne osoby (jak również sekcje) części operacyjnej poszczególnych stanowisk dowodzenia szczebla taktycznego mają możliwość wymiany informacji (koordynacji działań) bez ingerencji osób trzecich czy też przełożonych. Szczegółowe wewnętrzne więzi informacyjne poszczególnych dowództw szczebla taktycznego zostały przedstawione poniżej na rysunkach od 7 do 9.



Rysunek 7. Wewnętrzne więzi informacyjne części operacyjnej głównego stanowiska dowodzenia związku taktycznego lub oddziału
Źródło: opracowanie własne



Rysunek 8. Wewnętrzne więzi informacyjne części operacyjnej tyłowego stanowiska dowodzenia związku taktycznego lub oddziału
Źródło: opracowanie własne

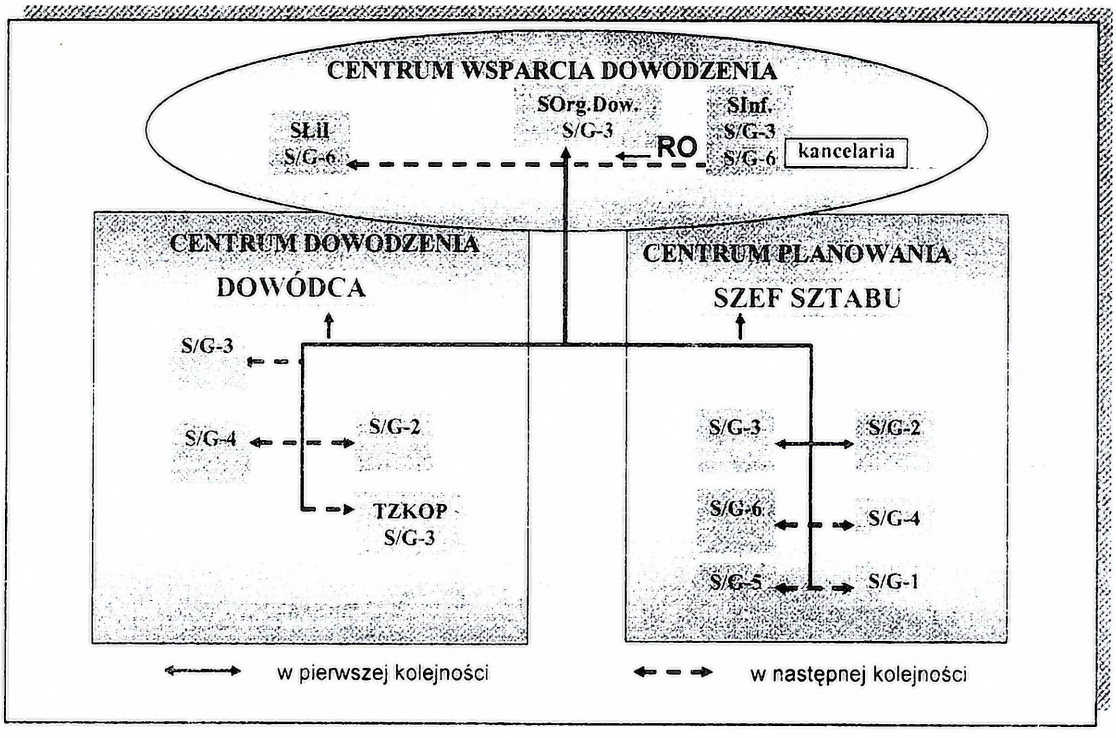


Rysunek 9. Wewnętrzne więzi informacyjne części operacyjnej głównego stanowiska dowodzenia pododdziału
Źródło: opracowanie własne

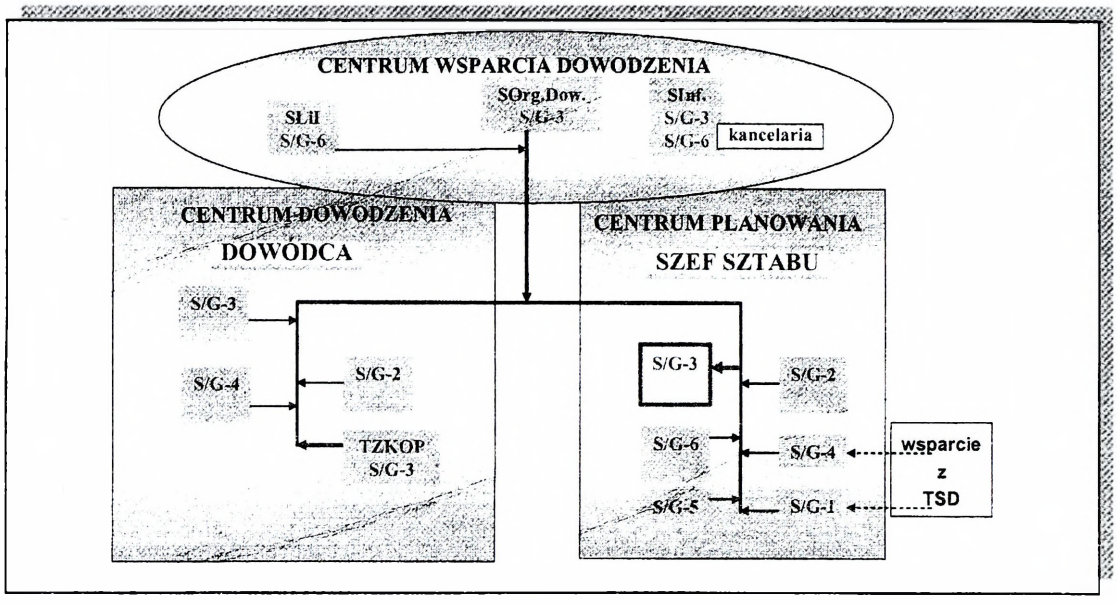
Prześledźmy teraz przykładowo wewnętrzne więzi informacyjne w zakresie przesyłania dokumentów dowodzenia:

A. Po wpłynięciu rozkazu operacyjnego do kancelarii sekcji informacyjnej centrum wsparcia dowodzenia w brygadzie, dokument ten – zgodnie z rozdzielnikiem oraz nakazanym priorytetem – przekazywany jest w pierwszej kolejności do dowódcy, szefa sztabu oraz centrum planowania. Następnie jest przekazywany do pozostałych osób funkcyjnych głównego stanowiska dowodzenia (rys. 10).

B. Rozkaz operacyjny opracowywany jest w centrum planowania przez jednego z oficerów (podoficera) S/G-3 przy współudziale pozostałych (rys. 11) osób funkcyjnych centrum wsparcia dowodzenia, centrum planowania oraz niektórych osób funkcyjnych tyłowego stanowiska dowodzenia (przede wszystkim przy współudziale S/G-1, S/G-4 oraz pionu logistyki).

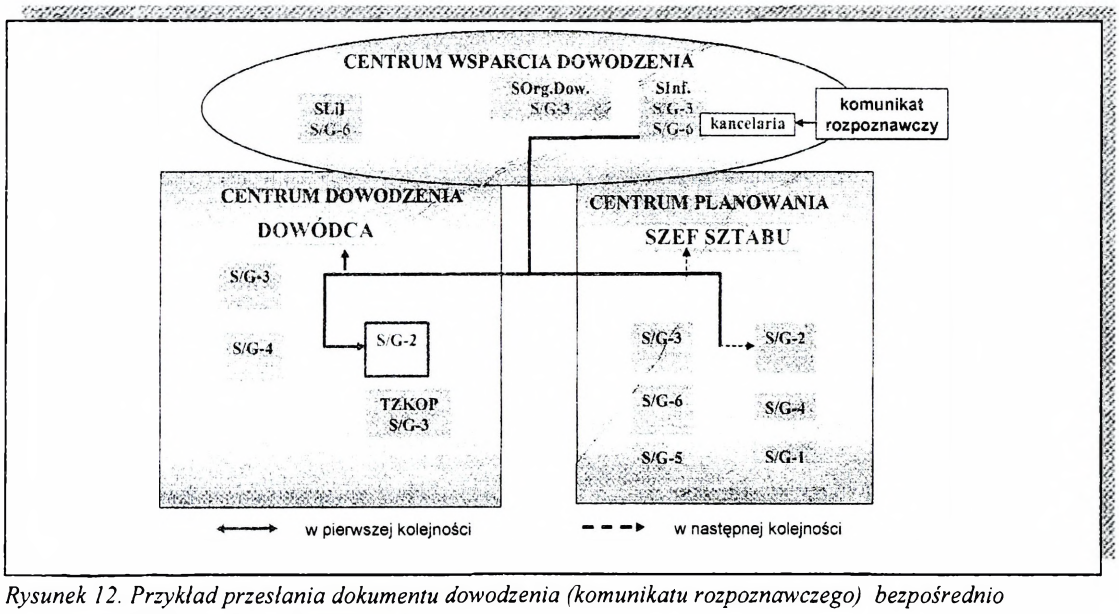


Rysunek 10. Więzi informacyjne wewnętrzne – kierunek przesłania rozkazu operacyjnego do poszczególnych osób funkcyjnych
Źródło: opracowanie własne



Rysunek 11. Więzi informacyjne wewnętrzne występujące przy opracowaniu rozkazu operacyjnego
Źródło: opracowanie własne

Pozostałe dokumenty dowodzenia przesyłane przez kancelarię sekcji informacyjnej centrum wsparcia dowodzenia bezpośrednio do adresatów (rys. 12).



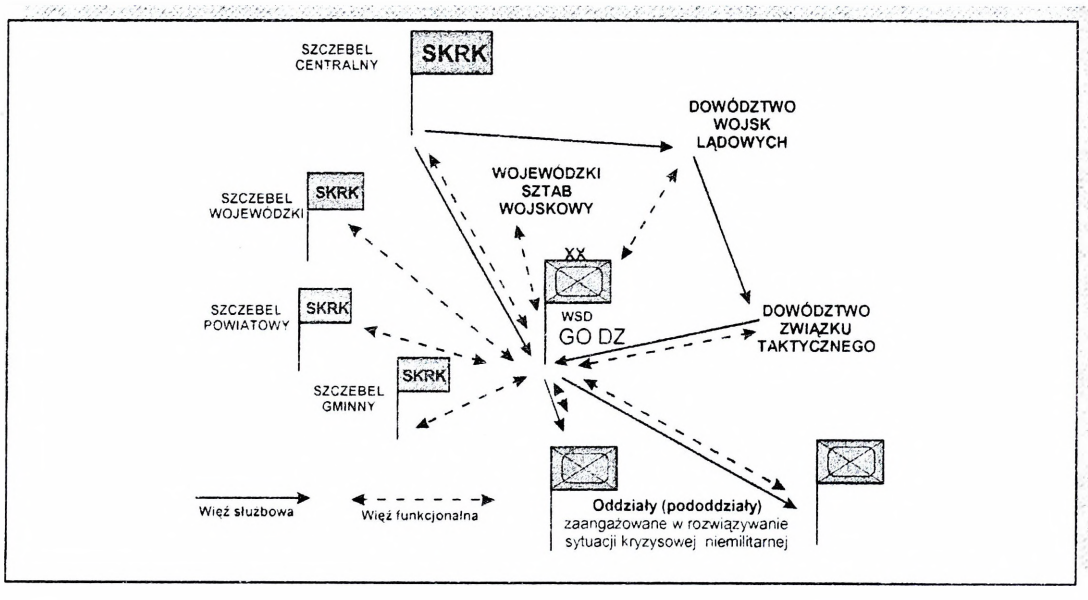
Rysunek 12. Przykład przesłania dokumentu dowodzenia (komunikatu rozpoznawczego) bezpośrednio do adresata (S/G-2 centrum dowodzenia)
Źródło: opracowanie własne

W przypadku wpłynięcia kilku dokumentów jednocześnie do kierownika sekcji informacyjnej, dokumenty te rozsyłane są w nakazanej kolejności zgodnie z nadanym priorytetem (np. dokumenty rozkazodawcze – 1, sprawozdawczo-informacyjne – 2, planistyczne – 3,

gdzie 1 jest najwyższą wartością). Określenie priorytetów poszczególnym dokumentom zapewni natychmiastowe dostarczenie ich do adresatów.

Zewnętrzne więzi informacyjne związane są ze zbieraniem (gromadzeniem) informacji (służbowe – dowodzenia, synchronizacji, i współdziałania, a więc np. do rozkazów, meldunków czy też komunikatów) z szeroko pojętego otoczenia. Na szczeblu taktycznym możemy do nich zaliczyć: przełożonego, podwładnego, a także ich najbliższe otoczenie.

W *sytuacji kryzysu niemilitarnego* więzi organizacyjne dowództwa szczebla taktycznego mogą się przedstawiać następująco (rys. 13.) Z danego dowództwa szczebla taktycznego tworzona jest grupa operacyjna (GO) z poszczególnych specjalistów dowództwa (w zależności od rozwiązywanej sytuacji kryzysowej). Grupa operacyjna pod dowództwem (najlepiej zastępcy dowódcy – lub innego oficera ze składu dowództwa), rozwinie wysunięte stanowisko dowodzenia (WSD).



Rysunek 13. Zewnętrzne więzi organizacyjne dowództwa szczebla taktycznego – związku taktycznego – w przypadku rozwiązywania sytuacji kryzysowej niemilitarnej
Źródło: opracowanie własne

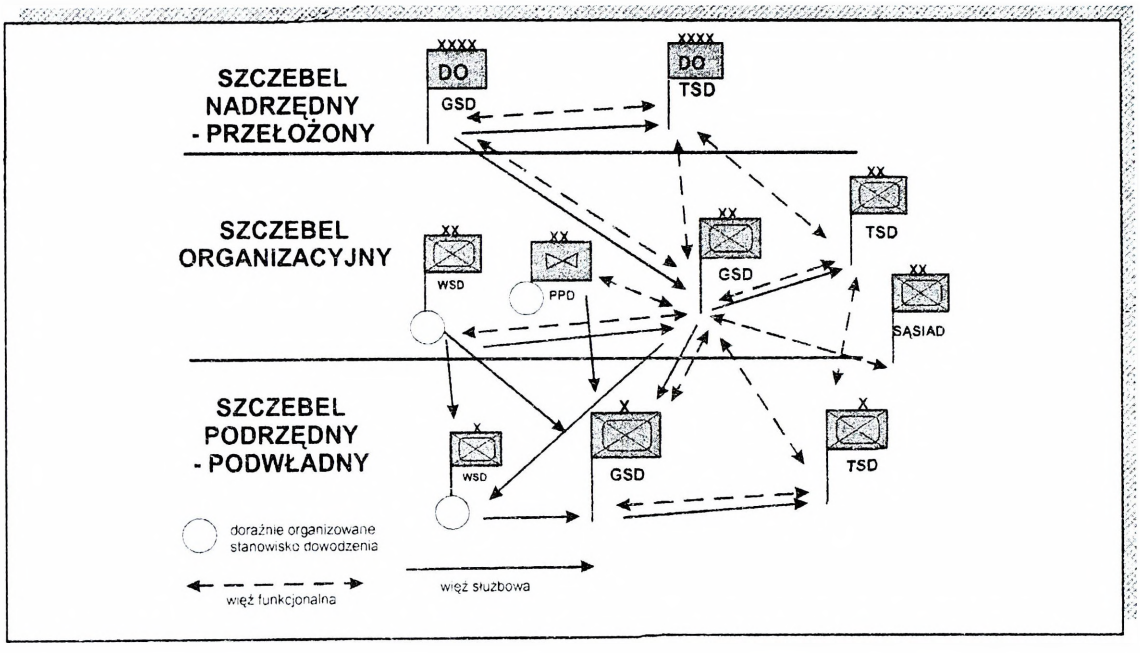
Wysunięte stanowisko dowodzenia więź organizacyjną będzie utrzymywać z:

- dowództwem szczebla taktycznego – *więź służbowa i funkcjonalna*,
- Dowództwem Wojsk Lądowych – *więź funkcjonalna*,
- Wojewódzkim Sztabem Wojskowym – *więź funkcjonalna*,
- Stanowiskiem Kierowania Reagowaniem Kryzysowym (SKRK) – *więź służbowa* (zakres uprawnień tylko do stawiania zadań dotyczących sytuacji kryzysowej), *więź funkcjonalna*,

– wojewódzkim, powiatowym, gminnym Zespołem Zarządzania Kryzysowego – *więź funkcjonalna*,

– podległymi siłami przeznaczonymi do rozwiązywania sytuacji kryzysowej – *więź służbowa i funkcjonalna*.

W sytuacji *kryzysu militarnego* dowództwa szczebla taktycznego będą rozwijać swoje poszczególne stanowiska dowodzenia (rys. 14) zgodnie z *Instrukcją Wojennego Systemu Dowodzenia*. W poszczególnym stanach gotowości bojowej będą uzupełniane składy osobowe poszczególnych SD.



Rysunek 14. Zewnętrzne więzi organizacyjne dowództwa szczebla taktycznego – związku taktycznego – w sytuacji kryzysu militarnego
Źródło: opracowanie własne

Zewnętrzne więzi organizacyjne głównego stanowiska dowodzenia będą się przedstawiały następująco:

– z przełożonym – dowództwem operacyjnym (DO) – *więź służbowa i funkcjonalna*,

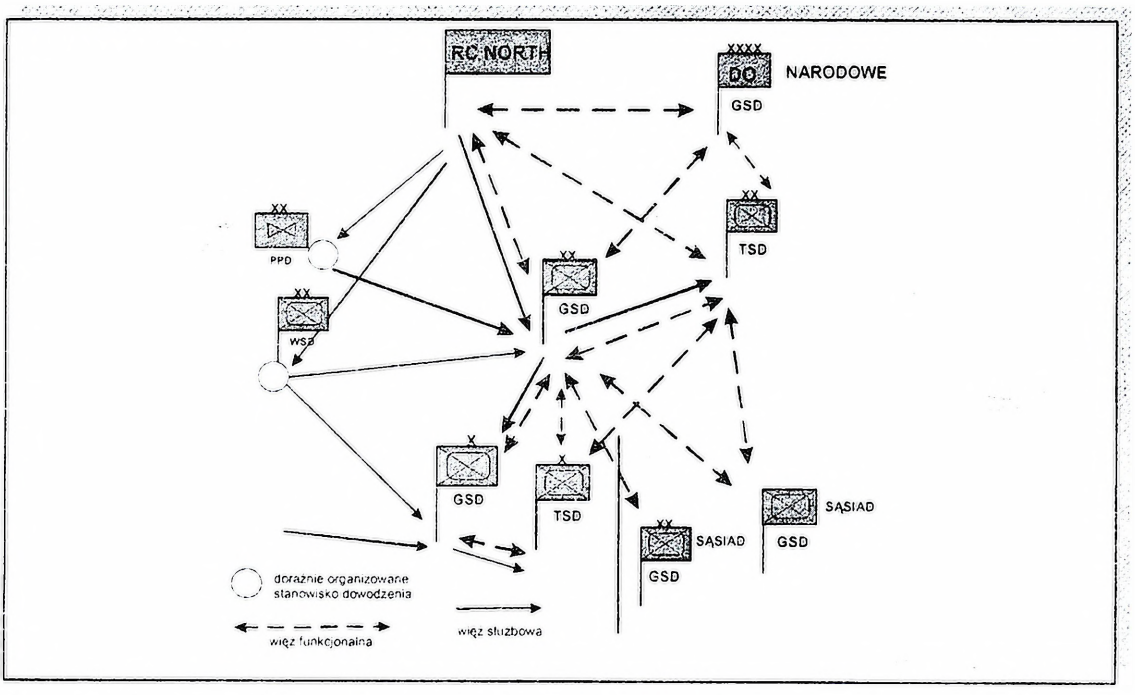
– pomiędzy własnymi stanowiskami dowodzenia (głównym stanowiskiem dowodzenia – GSD, tyłowym stanowiskiem dowodzenia – TSD oraz doraźnie organizowanymi wysuniętym stanowiskiem dowodzenia – WSD i powietrznym punktem dowodzenia – PPD) – *więź służbowa i funkcjonalna*,

– z podwładnymi – *więź służbowa i funkcjonalna*,

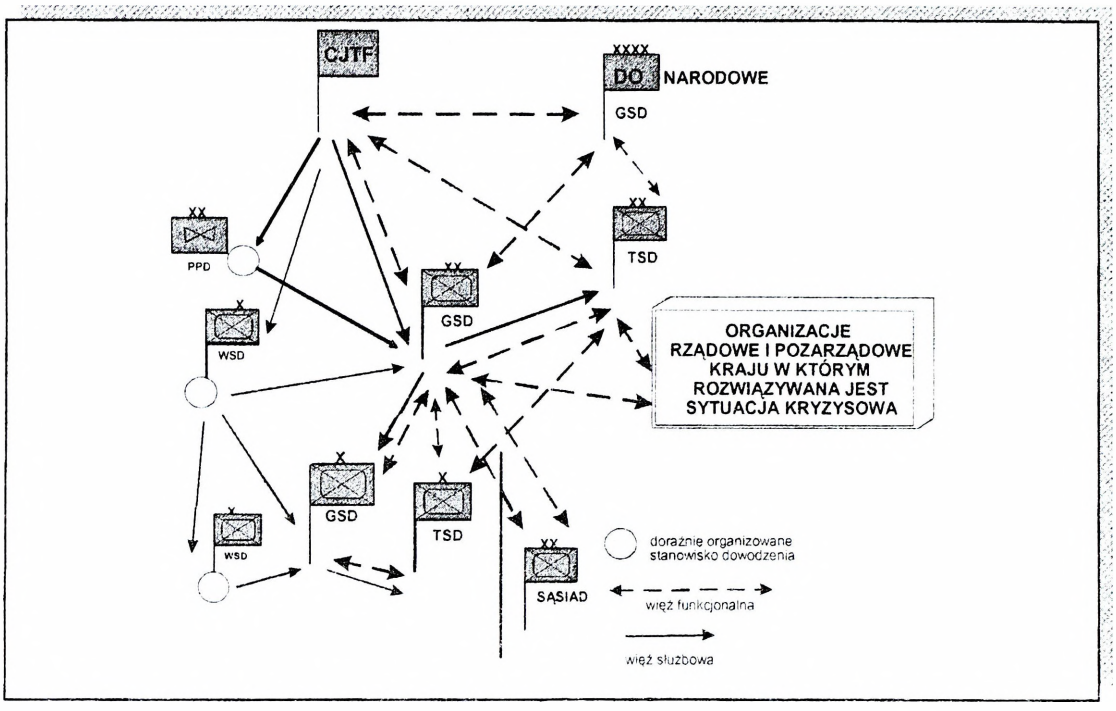
– z sąsiadami (otoczeniem) – *więź funkcjonalna*.

Dowództwa szczebla taktycznego wojsk lądowych mogą brać udział również w rozwiązywaniu sytuacji kryzysowej militarnej w ramach NATO (rys. 15) lub działań międzynarodowych (rys. 16), wtedy więzi organizacyjne mogą przedstawiać się następująco:

- przełożony – *więź służbowa i funkcjonalna*,
- podwładny – *więź służbowa i funkcjonalna*,
- dowództwo narodowe – *więź funkcjonalna*,
- sąsiad (otoczenie)– *więź funkcjonalna*.



Rysunek 15. Zewnętrzne więzi organizacyjne dowództwa szczebla taktycznego – związku taktycznego – w przypadku rozwiązywania sytuacji kryzysowej militarnej w ramach Sojuszu
Źródło: opracowanie własne



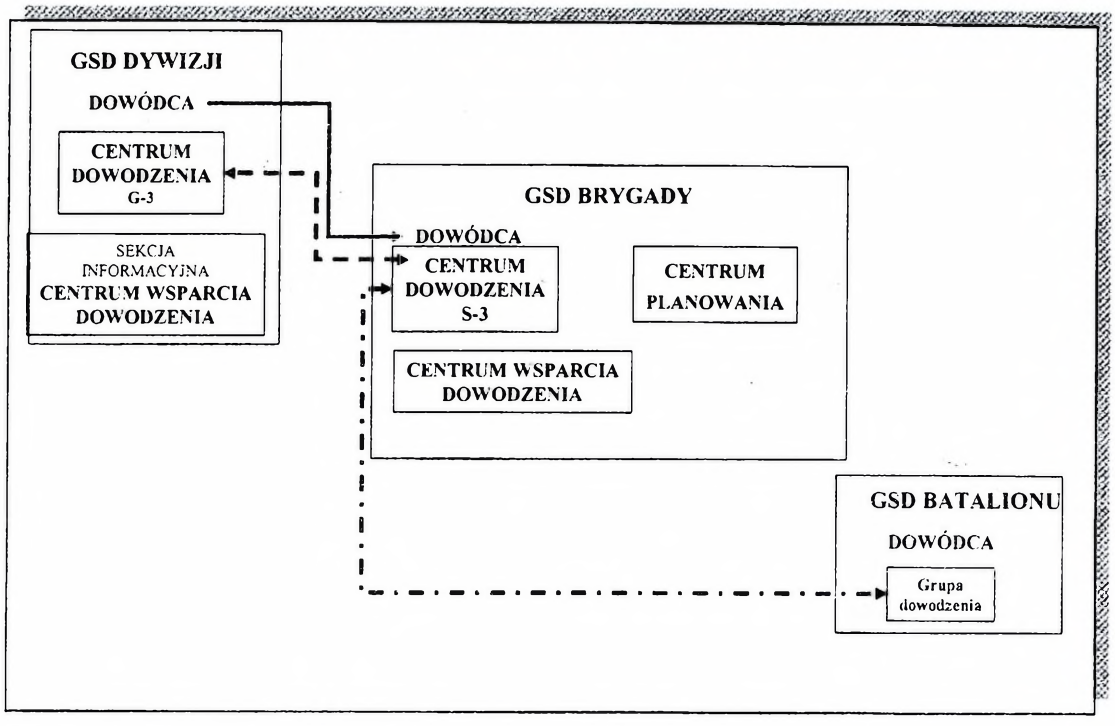
Rysunek 16. Zewnętrzne więzi organizacyjne dowództwa szczebla taktycznego – związku taktycznego – w przypadku rozwiązywania międzynarodowej sytuacji kryzysowej
Źródło: opracowanie własne

W celu przedstawienia pozostałych więzi zewnętrznych dowództwa szczebla taktycznego wojsk lądowych założyć można następujące sytuacje:

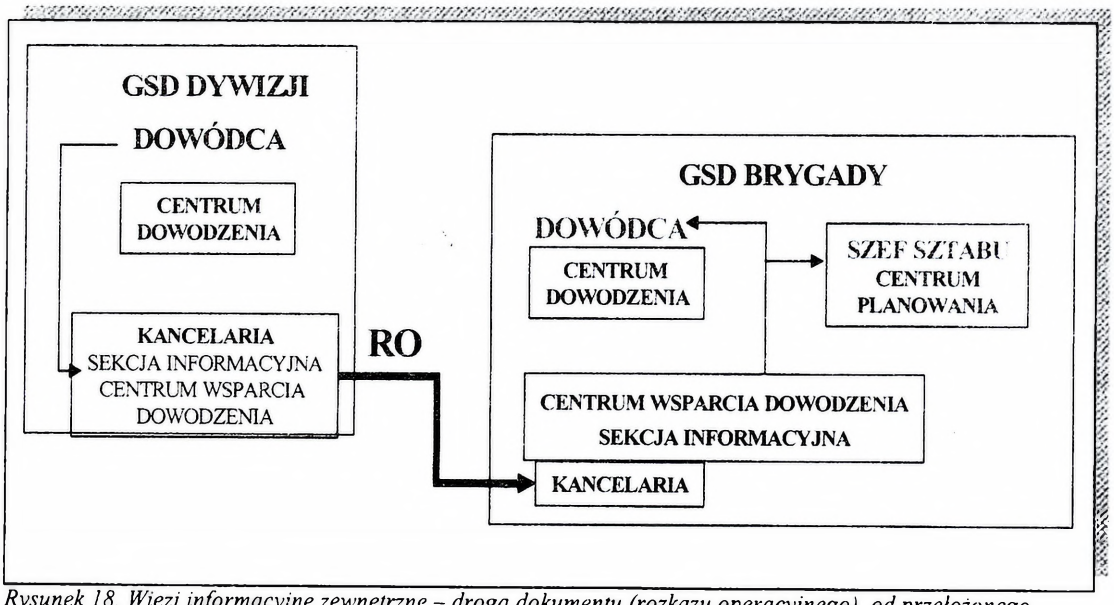
A. Dowódca dywizji otrzymuje zadanie do dalszego działania od dowódcy korpusu na odprawie poświęconej stawianiu zadań. W tym czasie na stanowisku dowodzenia dywizji sekcja dowodzenia zespołu dowodzenia kieruje działaniami podległych wojsk (rys. 17).

B. Rozkaz operacyjny po opracowaniu przez sekcję planowania zespołu dowodzenia i podpisaniu przez dowódcę, przekazany zostaje do sekcji informacyjnej zespołu wsparcia dowodzenia, a następnie przez kancelarię przesłany do kancelarii sekcji informacyjnej zespołu wsparcia dowodzenia podwładnego (rys. 18).

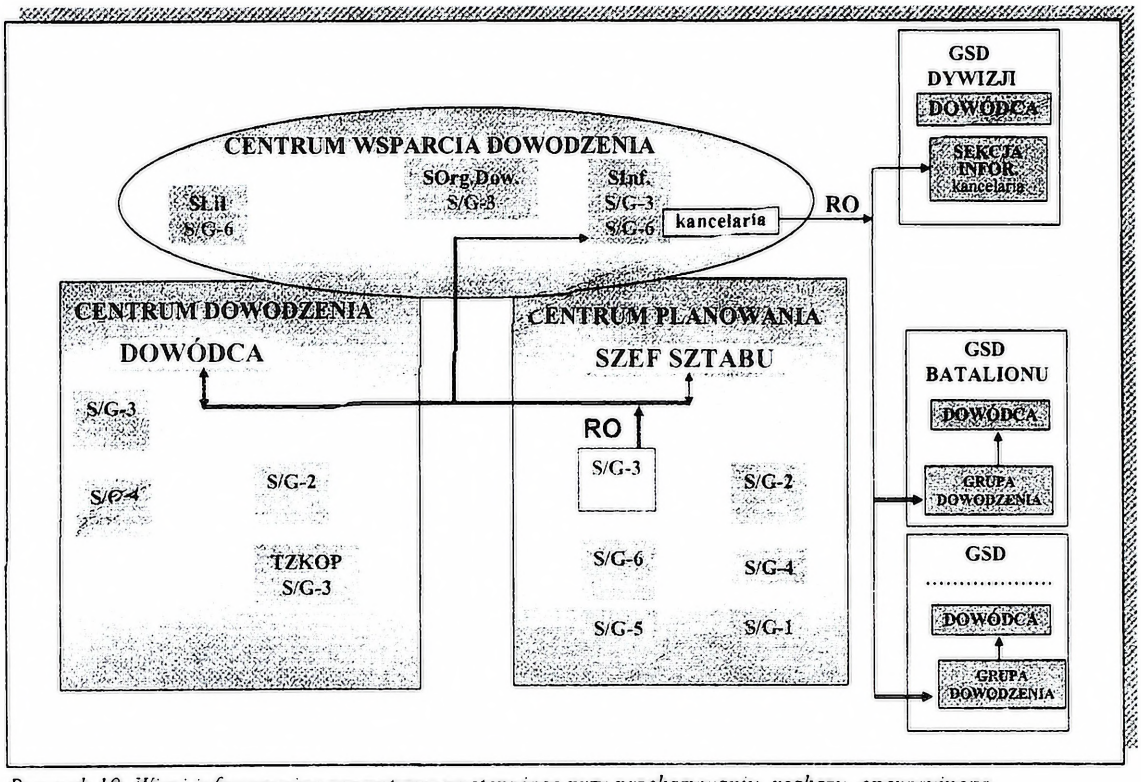
C. Po opracowaniu i zatwierdzeniu przez dowódcę rozkaz operacyjny jest przesyłany z centrum planowania do centrum wsparcia dowodzenia sekcji informacyjnej i przez kancelarię przesyłany do podwładnych (rys. 19) oraz do przełożonego, następnie jest rozprowadzany po wszystkich centrach, zespołach i sekcjach części operacyjnej głównego i tyłowego stanowiska dowodzenia.



Rysunek 17. Więzi informacyjne zewnętrzne – otrzymanie zadania od przełożonego oraz kierowanie działaniami podwładnego poprzez centrum (grupę) dowodzenia głównego stanowiska dowodzenia
Źródło: opracowanie własne

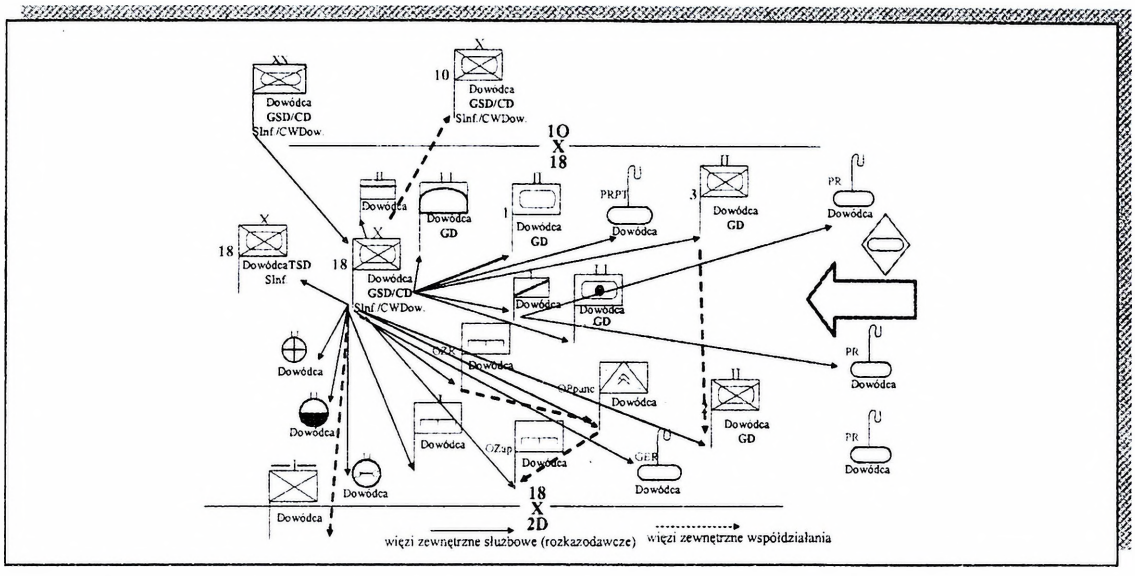


Rysunek 18. Więzi informacyjne zewnętrzne – droga dokumentu (rozkazu operacyjnego) od przełożonego do podwładnego
Źródło: opracowanie własne

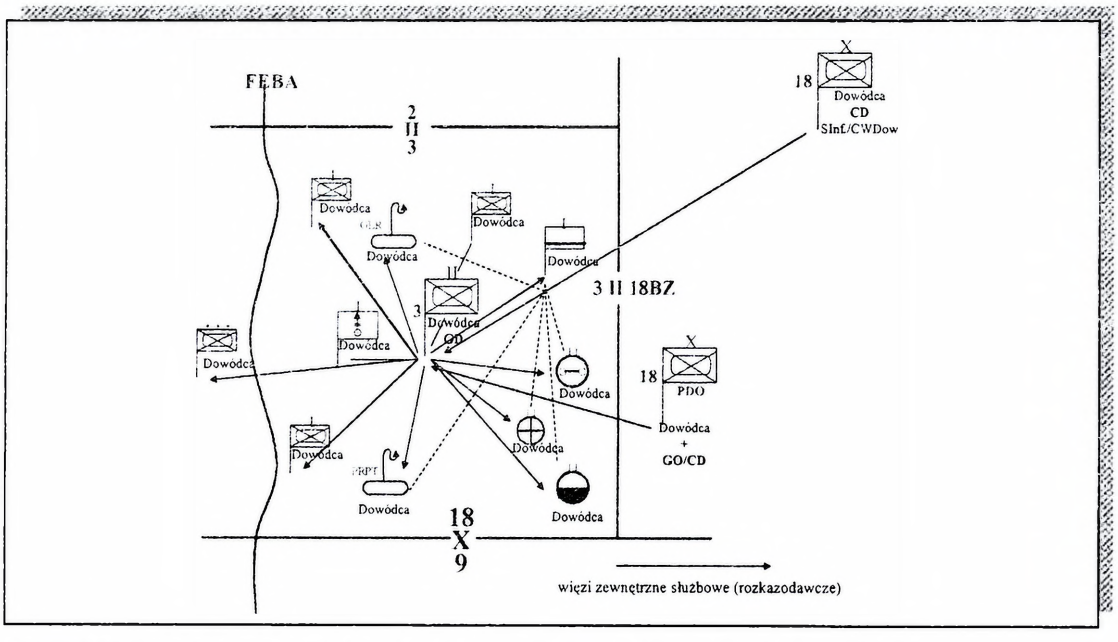


Rysunek 19. Więzi informacyjne zewnętrzne występujące przy przekazywaniu rozkazu operacyjnego
Źródło: opracowanie własne

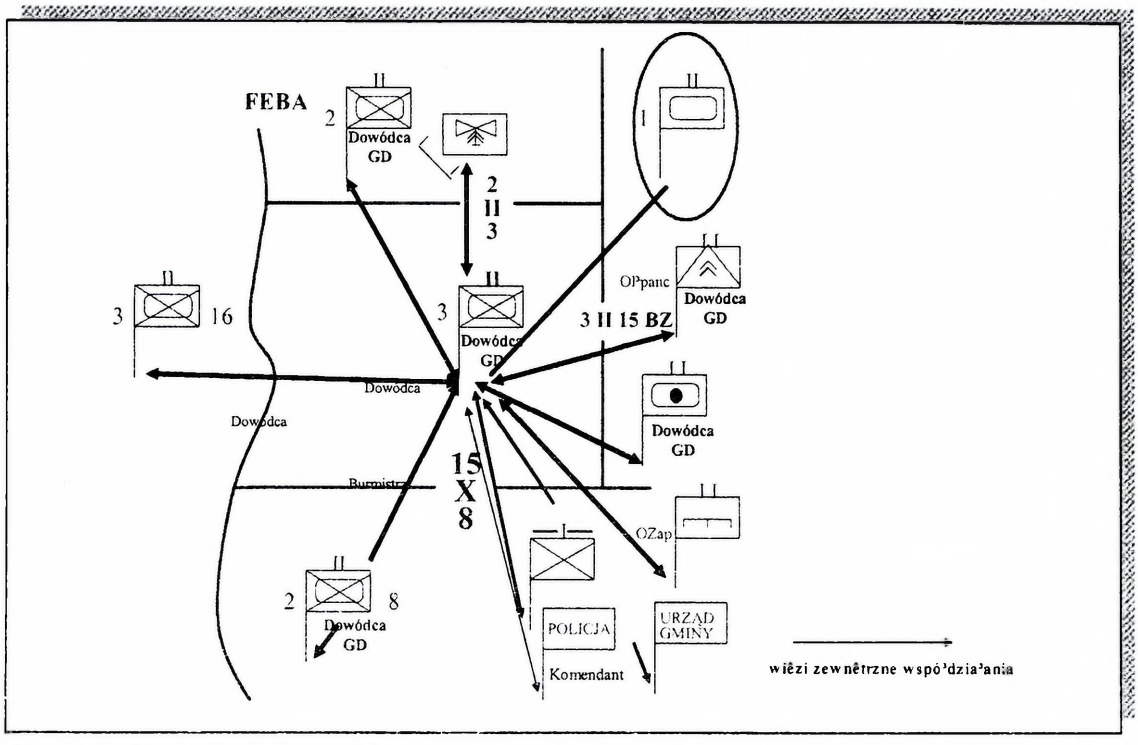
Więzi informacyjne zewnętrzne służbowe (rozkazodawcze) oraz współdziałania pomiędzy poszczególnymi stanowiskami dowodzenia na szczeblach taktycznych przedstawiają się następująco: dowódca poprzez centrum (grupę) dowodzenia bezpośrednio kieruje walką podległych elementów swojego ugrupowania bojowego, natomiast przepływ dokumentów następuje przez sekcję informacyjną centrum wsparcia dowodzenia (jak opisano to wcześniej – rys. 20, 21 i 22).



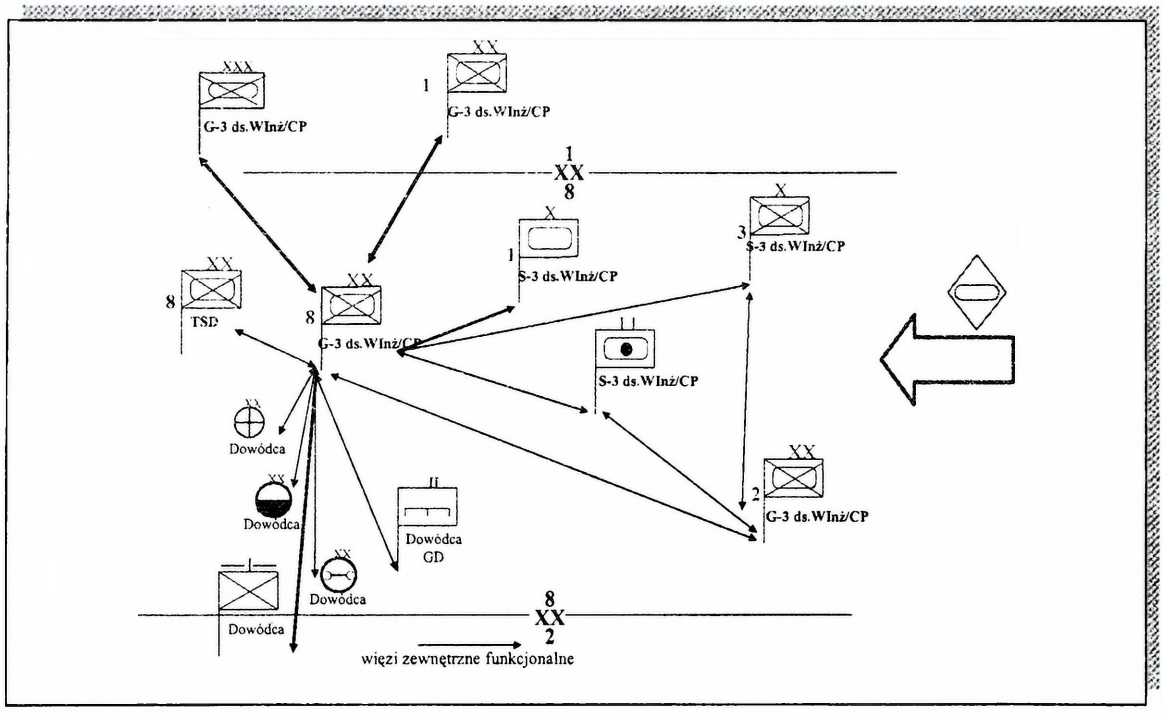
Rysunek 20. Więzi zewnętrzne służbowe (rozkazodawcze) i współdziałania na szczeblu oddziału
Źródło: opracowanie własne



Rysunek 21. Więzi zewnętrzne służbowe (rozkazodawcze) występujące na szczeblu pododdziału
Źródło: opracowanie własne



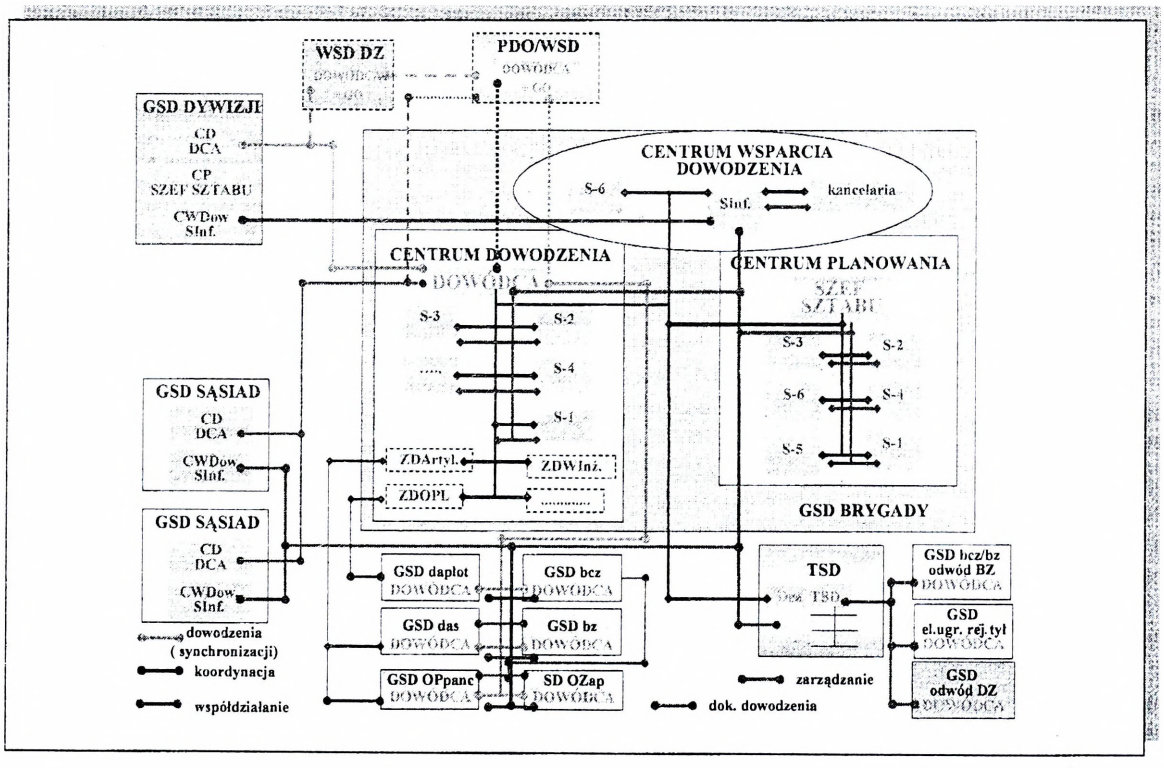
Rysunek 22. Więzi zewnętrzne współdziałania występujące na szczeblu pododdziału
Źródło: opracowanie własne



Rysunek 23. Więzi informacyjne zewnętrzne – funkcjonalne – pomiędzy G-3 ds. WInż centrum planowania a elementami ugrupowania bojowego dywizji, przełożonego oraz sąsiadów (otoczenia)
Źródło: opracowanie własne

Rozpatrując zewnętrzne więzi informacyjne, należy uwzględnić zewnętrzne więzi funkcjonalne, które występują pomiędzy poszczególnymi osobami stanowiska dowodzenia w relacji, np. G-3 ds. WInż dywizji – S-3 ds. WInż. brygady. Na tym kierunku przekazywane są przede wszystkim informacje specjalistyczne. Nie zawierają żadnych relacji rozkazodawczych, są bardziej sprawozdawczo-informacyjne (rys. 24). Przesłanie dokumentu odbywa się przez poszczególne sekcje informacyjne i ich kancelarie. Zapewni to wymianę informacji pomiędzy poszczególnymi specjalistami bez oczekiwania na dokument główny, który „spłynie" od przełożonego po jakimś terminie.

Analizując zewnętrzne więzi informacyjne poszczególnych stanowisk dowodzenia szczebla taktycznego, nie należy zapominać o więziach synchronizacji oraz współdziałania. Więzi synchronizacji organizuje dowódca danego szczebla w stosunku do podwładnych. Natomiast więzi współdziałania występują w trakcie realizacji wspólnych zadań, bez udziału przełożonego.



Rysunek 24. Przebieg więzi informacyjnych w dowództwie szczebla taktycznego (na przykładzie głównego stanowiska dowodzenia brygady zmechanizowanej)
Źródło: opracowanie własne

W przypadku gdy dowódca wykorzystuje czasowo WSD, dysponuje on więzią służbową ze wszystkimi podwładnymi i przełożonym. Oficerowie pracujący wraz z nim posiadają więzi funkcjonalne z właściwymi stanowiskami dowodzenia podwładnych oraz swoimi zespołami, na GSD. Powietrzny punkt dowodzenia zapewnia dowódcy dywizji więź służbową ze stanowiskami dowodzenia podległych oddziałów oraz z przełożonym.

Duże znaczenie mają również powiązania informacyjne między GSD i TSD. Powiązania te muszą umożliwić przesyłanie na TSD dokumentów dowodzenia, sporządzanych na GSD w ramach cyklu procesu decyzyjnego, aby zapewnić ciągłość dowodzenia i możliwość przejęcia funkcji GSD przez TSD.

W konkluzji przeprowadzonych powyżej wyjaśnień można sformułować następujące **wnioski**:

1. Struktura organizacyjna dowództwa szczebla taktycznego wojsk lądowych powinna się składać z zespołów organizacyjnych odpowiadających funkcjonalnym obszarom pola walki.

2. Liczba komórek organizacyjnych stanowisk dowodzenia poszczególnych dowództw szczebla taktycznego oraz wielkość obsady personalnej uzależnione są od wielu czynników. Można do nich zaliczyć:

– *zadania, jakie ma realizować dany zespół stanowiska dowodzenia,*

– *stopień przygotowania personelu i wyposażenia w techniczne środki dowodzenia,*

– *wymogi określane przez zasady organizacji rozmieszczenia i pracy stanowisk dowodzenia,*

– *potrzebę zapewnienia ciągłości pracy podczas 24 godzin z uwzględnieniem systemu dwuzmianowego (w przypadku działań podczas kryzysu powinno się nawet stosować trzyzmianowość pracy na stanowisku dowodzenia),*

– *wytyczne dowódcy i szefa sztabu.*

3. Z punktu widzenia kryteriów informatycznych (skrócenie czasu i dróg obiegu informacji, integralności baz danych itp.) powinno się zmierzać w kierunku rozwarstwienia systemu dowodzenia na centra, zespoły i piony zadaniowe, tworzone na zasadzie jednorodności zadań taktyczno-operacyjnych i związanych z tym obszarów dowodzenia, a nie rodzajów wojsk i służb, które zadania te wykonują.

4. Przechodzenie struktury organizacyjnej dowództw z okresu „P" na okres „W", uwarunkowane jest w znacznej mierze potrzebami dowodzenia wojskami w zmieniających się

warunkach współczesnego pola walki i sterowania środkami walki. Organizowany wojenny system dowodzenia obejmuje określony podsystem stanowisk dowodzenia, które powiązane są określonymi relacjami informacyjnymi wewnętrznymi i zewnętrznymi. Stawiane obecnie przed dowodzeniem wymagania oraz czynniki warunkujące jego sprawność są podstawą do przedstawienia w procesie badawczym zadań systemu dowodzenia w czterech obszarach:

- *dowodzenia,*
- *planowania,*
- *wsparcia dowodzenia,*
- *zabezpieczenia działań.*

5. Każda z komórek organizacyjnych części operacyjnej stanowisk dowodzenia powinna tworzyć względnie niezależny organizacyjnie zespół funkcjonalny dowodzenia (planowania, zarządzania, sterowania), wyposażony informatycznie i komunikacyjnie w siły i środki umożliwiające przejęcie funkcji dowódczo-sztabowych innego zespołu funkcjonalnego (komórki organizacyjnej) stanowiska dowodzenia lub przynajmniej funkcji planowania dowodzenia (operacyjnego lub taktycznego).

Łączność radiowa stanowisk dowodzenia

dr inż. Piotr DANILUK
Akademia Obrony Narodowej

W niniejszym artykule została dokonana syntetyczna ocena dotychczasowych oraz perspektywicznych rozwiązań dotyczących łączności radiowej na potrzeby stanowisk dowodzenia.

Szerokie spektrum koncepcji dotyczących przyszłości systemów łączności radiowej determinowało ograniczenie uwagi autora do sieci radiowych pola walki, sieci radiotelefonicznych, radiostępowych oraz tylko wybranych radiokomunikacji ruchomej i bezprzewodowej transmisji danych.

1. Dotychczasowe uwarunkowania

Problematyka związana z organizacją łączności radiowej na potrzeby stanowisk dowodzenia zawsze była postrzegana jako istotna. Do niedawna w znakomitej większości przypadków łączność pomiędzy osobami znajdującymi się na stanowiskach dowodzenia realizowano za pomocą wewnętrznej sieci kablowej. Wynikało to z kilku zasadniczych powodów:

a) ograniczania do minimum promieniowania środków radiowych, co posiadało swoje przyczyny, w dwóch obszarach:
   - przewidywania znacznego zagrożenia pracy radiostacji nadajnikami zakłócającymi małej mocy zrzuconymi w pobliżu;
   - zbyt złożonemu procesowi zapewnienia na wystarczającym poziomie kompatybilności elektromagnetycznej na tak małym obszarze;

b) zbyt dużych wymiarów i małej niezawodności urządzeń radiowych.

Stosowane niespełna kilkanaście lat temu urządzenia radiowe, szczególnie te małej mocy i przenośne, pracowały w stosunkowo wąskich zakresach, z dużym odstępstwem częstotliwościowym (falowym) oraz szerokopasmowym widmem sygnału. To sprawiało, że zapewniały bardzo mały zasięg i małą odporność na zakłócenia.

W przypadku konstrukcji lampowych i tylko tranzystorowych występowały istotne niedogodności eksploatacyjne związane z wymiarami, a co najważniejsze – z krótkim czasem pracy nadawczej. Przykładami takich radiostacji mogą być urządzenia typu R-126, R-105, R-108 czy TUBEROZA.

Takie uwarunkowania techniczne łączności radiowej spowodowały dominująca rolę łączności kablowej w ramach stanowisk dowodzenia.

2. Nowe uwarunkowania

Od kilkunastu lat następuje nasilenie dynamicznych zjawisk technologicznych i społecznych, które również posiadają swoje odniesienie w obszarze wojskowej łączności. Wyodrębniono trzy zasadnicze obszary tych zmian:

- niebywały rozwój technologii mikroprocesorowych, co spowodowało miniaturyzację i wielofunkcyjność (w tym zwiększenie bezpieczeństwa pracy) urządzeń radiowych (telefony GSM, telefony DECT/UMTS, telefony satelitarne, skanery i radiostacje wielozakresowe 2 – 2000 MHz);
- dynamicznie postępujący poziom wiedzy i umiejętności technicznych szerokich mas społeczeństwa szczególnie w zakresie obsługi multimediów;
- silna presja do przesyłania potężnej ilości informacji przy dużej mobilności abonentów systemu.

Tak zdefiniowane uwarunkowania posiadają znaczny wpływ na obecne i perspektywiczne funkcjonowanie stanowisk dowodzenia. W związku z tym pojawiły się nowe i znacznie szersze zastosowania łączności radiowej na stanowisku dowodzenia. Zawarte je w kilku obszarach:

- wykorzystania radiostacji wojskowych do pracy w sieciach tylko do tego przeznaczonych. Sieci takie nazywane są sieciami radiowymi stanowisk dowodzenia i zapewniają niewielki zasięg. W rozwiązaniach armii brytyjskiej są to sieci przede wszystkim do zapewnienia łączności podczas przemieszczenia stanowisk dowodzenia;
- wykorzystania środków radiotelefonicznych do pracy lokalnej. Występują dwie odmiany takich sieci – o rzeczywiście lokalnym zasięgu bez stacji pozwalającej wejść w sieć radioliniowo-kablową oraz sieci o cechach trankingu;
- wykorzystania szerokopasmowych sieci radiowych. Występują dwie zasadnicze odmiany takich sieci – o cechach czysto wojskowych pracujących w sieciach typu EPLRS lub JTIDS oraz o cechach czysto komercyjnych zgodnych ze standardami związanymi z dostępem typu Wi-Fi oraz Wi-Max.

Poniżej scharakteryzowano tak wyodrębnione systemy łączności radiowej.

Na początku poddano ocenie pierwotne sieci wykorzystywane już od dawna, choć w ograniczonym zakresie, na stanowiskach dowodzenia różnego szczebla.

3. Sieci radiowe stanowisk dowodzenia

W dokonanej analizie oparto się na koncepcji propagowanej przez pracowników Zakładu Systemów Łączności i Informatyki, określającej mobilną sieć łączności występująca na po-

ziomach taktycznych – dywizji, brygad, pułków i pododdziałów jako zbiór następujących podsieci[1]:

- radioliniowo-kablowej,
- radiowych pola walki,
- radiodostępu,
- komputerowej;
- pocztowej

Przedstawione założenia i kalkulacje w pracach naukowo-badawczych prowadzonych w Instytucie Zarządzania i Dowodzenia, stanęły u podstaw zaprezentowanej szczegółowo struktury sieci radiowych pola walki, jako:

- sieci dowodzenia dywizji, brygad, pułków i pododdziałów;
- sieci sztabu dywizji i brygad;
- sieci współdziałania dywizji, brygad i pułków;
- sieci rozpoznania dywizji i brygad;
- sieci wewnętrznych stanowisk dowodzenia dywizji i brygad;
- sieci zabezpieczenia logistycznego dywizji, brygad, pułków i batalionów / dywizjonów.

Tak określone miejsce sieci stanowisk dowodzenia pozwalają następnie określić ich wewnętrzną strukturę, którą zaprezentowano w tabeli 1. oraz na rysunku 1.

Tabela 1. Skład sieci radiowej stanowisk dowodzenia dywizji

Nazwa sieci radiowej	Abonenci	Miejsce znajdowania się abonenta	Rodzaj / typ radiostacji
Stanowisk dowodzenia DZ (UKF)	D-ca DZ	SD DZ/WSD/PPD	RR-9500
	Dowódca TSD DZ	TSD DZ	RR-9500
	Centrum zabezpieczenia działań	SD DZ	RR-9500
	Zespół dowodzenia	SD DZ/WSD/PPD	RR-9500
	Zespół łączności i informatyki	SD DZ	RR-9500
	Zespół rozpoznania	SD DZ	RR-9500
	Zespół opchem (OAS)	SD DZ	RR-9500
	Zespół artylerii	SD DZ	RR-9500
	Zespół Winż.	SD DZ	RR-9500
	Zespół OPL	SD DZ	RR-9500

Źródło: Mobilne sieci łączności – album schematów, pod kierownictwem J. Janczaka, AON, Warszawa 2003, s. 55

[1] Mobilne sieci łączności – album schematów, pod kierownictwem J. Janczaka, AON, Warszawa 2003, s. 26

Sieci wewnętrzne stanowisk dowodzenia dywizji i brygad organizowane są w celu wymiany informacji niezbędnych w procesie dowodzenia w ramach komórek funkcjonalnych stanowisk dowodzenia. Oznacza to, że są to sieci przede wszystkim foniczne, choć niewielkie odległości abonentów pozwalają na transmisję danych i to ze znacznymi wartościami przepustowości. Ze względu na niewielki zasięg oraz potrzebę włączenia innych lokalnych środków łączności radiowej, są to sieci zakresu ultrakrótkofalowego (tj. 30 – 87 MHz).

Rola sieci stanowisk dowodzenia jest szczególna w okresie przemieszczeń. Cały wysiłek planistyczny oraz organizacyjny powinien być skierowany również na funkcjonowanie łączności elementów stanowiska dowodzenia podczas marszu, na postojach oraz w miejscu odpoczynku.

W obszarze zapewnienia łączności w okresie marszu powinno uwzględnić się szerokie stosowanie retransmisji oraz wykorzystanie radiodostępu, choćby w ograniczonym stopniu.

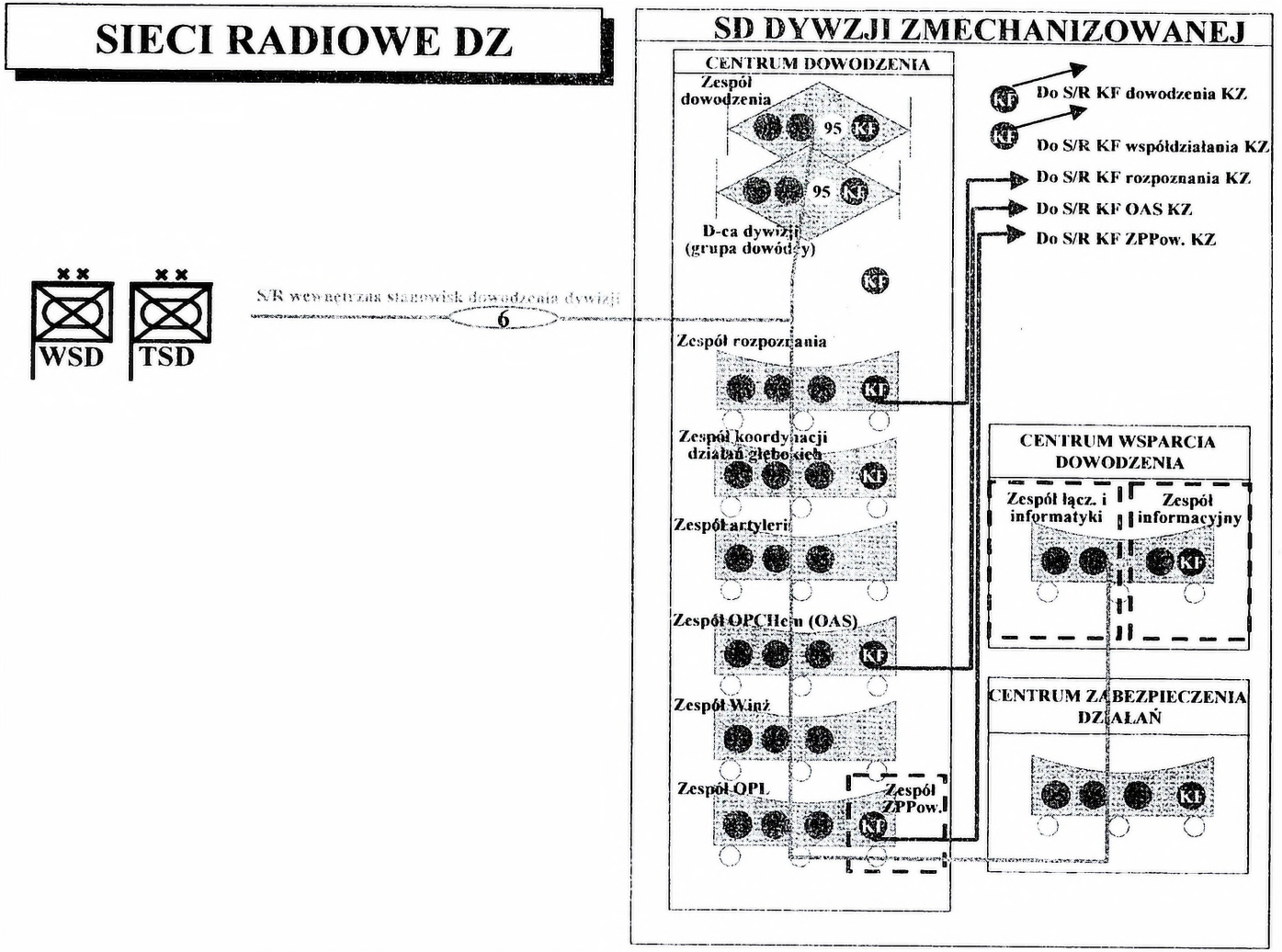
Według autorów prezentowanej koncepcji w sieci radiowej stanowisk dowodzenia dywizji i brygad powinny funkcjonować radiostacje: komórek zespołu dowodzenia SD, rozpoznania, artylerii, łączności i informatyki, OPChem, WInż, OPL, zabezpieczenia działań, dowódcy TSD, centrum dowodzenia TSD, centrum wsparcia dowodzenia TSD.

Możliwości organizacyjne oraz techniczne determinują wykorzystanie radiostacji pokładowych typu RRC-9500 (TRC-9500). .

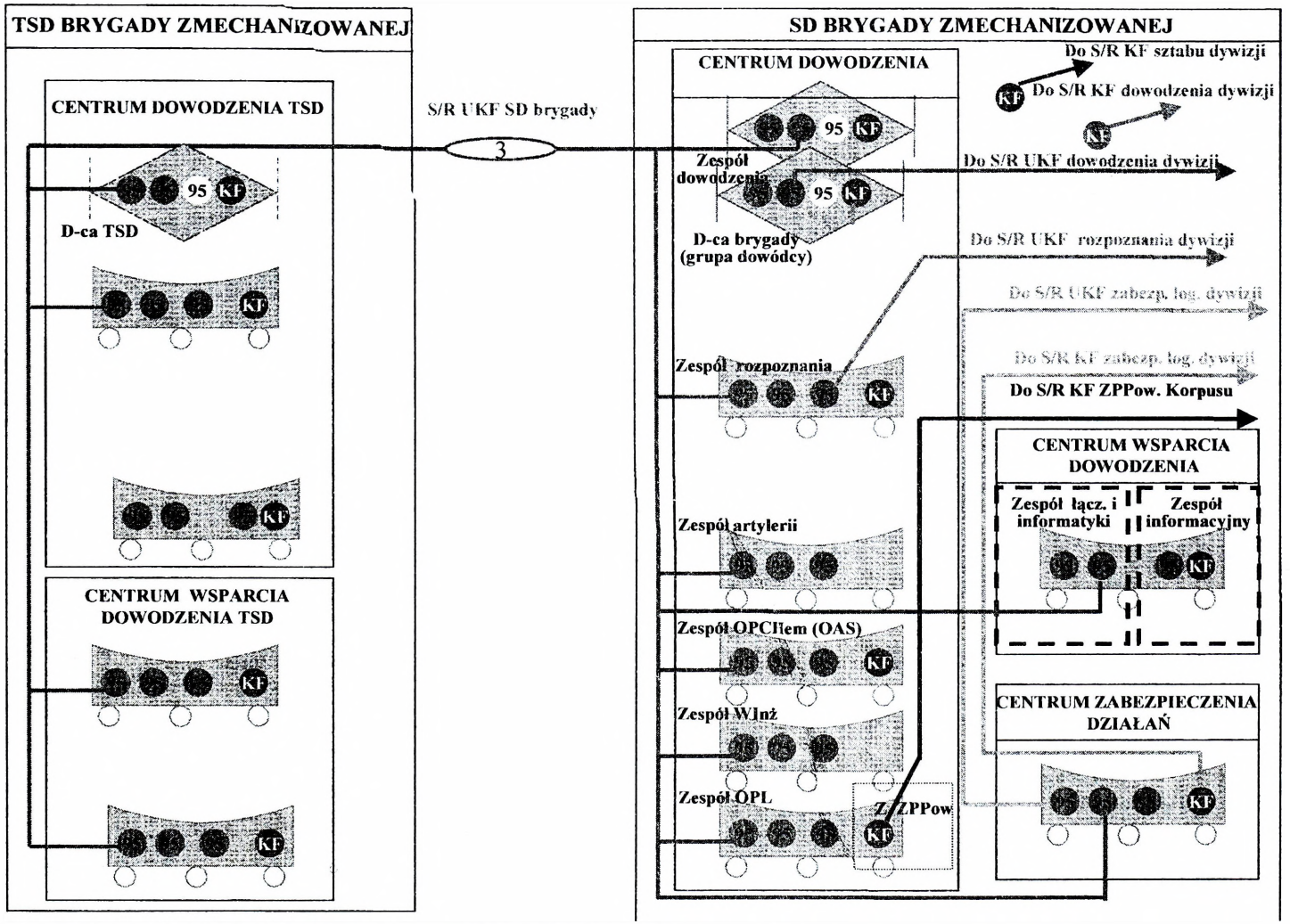
Wykorzystanie radiostacji pokładowych pozwala na utrzymanie łączności z jakością na wystarczającym poziomie, szczególnie w czasie przemieszczeń - tak krytycznych dla funkcjonowanie stanowisk dowodzenia szczebla taktycznego.

Włączanie radiostacji przenośnych typu RRC-9200 (TRC-9200) i ręcznych R-3601 oraz R-3505 jest wskazane szczególnie podczas rozwijania, funkcjonowania i zwijania stanowisk dowodzenia. W okresie prowadzenia marszu środki takie zapewniają bardzo ograniczoną łączność.

Skład sieci radiowej stanowisk dowodzenia brygady oparty na prezentowanej koncepcji przedstawia tabela 2., natomiast strukturę rysunek 2.



Rys. 1. Schemat sieci radiowej wewnętrznej stanowisk dowodzenia dywizji
Źródło: Mobilne sieci łączności – album schematów, pod kierownictwem J. Janczaka, AON, Warszawa 2003, s. 52



Rys. 2. Schemat sieci radiowej wewnętrznej stanowisk dowodzenia brygady
Źródło: Mobilne sieci łączności – album schematów, pod kierownictwem J. Janczaka, AON, Warszawa 2003, s. 81

Tabela 2. Skład sieci radiowej wewnętrznej stanowisk dowodzenia brygady

Nazwa sieci radiowej	Abonenci	Miejsce znajdowania się abonenta	Rodzaj / typ radiostacji
Wewnętrzna stanowisk dowodzenia brygady (UKF)	Zespół dowodzenia	SD	RRC 9500
	Zespół rozpoznania	SD	RRC 9500
	Zespół artylerii	SD	RRC 9500
	Zespół łączności i informatyki	SD	RRC 9500
	Zespół OPChem	SD	RRC 9500
	Zespół Winż	SD	RRC 9500
	Zespół OPL	SD	RRC 9500
	Zespół zabezpieczenia działań	SD	RRC 9500
	Centrum dowodzenia TSD	TSD	RRC 9500
	Centrum wsparcia dowodzenia TSD	TSD	RRC 9500

Źródło: Mobilne sieci łączności – album schematów, pod kierownictwem J. Janczaka, AON, Warszawa 2003, s. 80

4. Sieci radiotelefoniczne

Wykorzystanie sieci radiotelefonicznych wydaje się być szczególnym wskazane jako świetnie uzupełnienie pracujących sieci radiowych wewnętrznych stanowisk dowodzenia dywizji i brygad.

Ja wspomniano na wstępie, łączność radiotelefoniczną można rozpatrywać jako dwa obszary jej wykorzystania.

Pierwszy, najprostszy w zastosowaniu, polega na wykorzystaniu radiotelefonów do łączności lokalnych (ręcznych, przenośnych i pokładowego jako stacji bazowej). Standardowym wykorzystaniem sieci opartej o pracę takich urządzeń jest:

a) łączność służb dyżurnych i wart w obrębie stanowiska dowodzenia;

b) łączność osób funkcyjnych stanowiska dowodzenia dla zasięgów w jego obrębie

Takie sieci radiotelefoniczne mogą funkcjonować w oparciu o urządzenia pracujące w izolowanych (niezależnych) podzakresach ogólnodostępnych, np. 147 – 174 MHz, 420 – 470 MHz.

Jednak wskazanym jest tworzyć sieci radiotelefoniczne w oparciu środki radiowe pracujące w zakresach obejmujących wojskowe zastosowania, tj. 30 – 87 MHz, gdyż wtedy istnieje możliwość współpracy w ramach sieci radiowej stanowiska dowodzenia, chociażby z wykorzystaniem emisji analogowych.

Drugim ważnym obszarem wykorzystania łączności na potrzeby stanowiska dowodzenia jest radiotelefonia trankingowa. Staje się to szczególnie aktualne w sytuacji znacznej presji politycznej i społecznej do większego współdziałania wojsk lądowych z elementami administracji państwowej, organizacji społecznych – paramilitarnych. Jest to rezultatem coraz

większej współpracy różnych sił i organizacji w sytuacji kryzysowej wywołanej klęskami żywiołowymi oraz zamachami terrorystycznymi.

Takie uwarunkowania wskazują na dynamiczny rozwój łączności trankingowej również w obszarze wojsk lądowych. Pewne doświadczenia wojska lądowe posiadają z kilku już funkcjonujących sieci o takim charakterze.

Z dużym prawdopodobieństwem można więc przewidywać zastosowanie takiej łączności w ramach stanowisk dowodzenia. Dotyczyć będzie to współpracy wojsk lądowych z elementami reagowania kryzysowego na obszarze kraju. Współpraca osób funkcyjnych na stanowisku dowodzenia oraz z obszaru MSWiA będzie możliwa, poza siecią kablową wewnętrzną, właśnie z wykorzystaniem środków sieci trankingowych.

Przeprowadzone badanie literatury oraz dokumentacji technicznej pozwalają wybrać dwa zasadnicze systemy – TETRA (ang. TransEuropean Trunked Radio) oraz EDACS. (ang. Enhanced Digital Communication System)

Trudno w tej chwili wskazać na jeden z nich, gdyż nie dokonano tego w służbach, które taki rodzaj łączności traktują jako podstawowy do zapewnienia mobilnej komunikacji. Dopiero wskazanie przez abonentów resortów MSWiA na konkretny system może zainicjować rozwój takich sieci w obszarze wojskowym – w tym stanowisk dowodzenia.

5. Możliwości wykorzystania innych sieci

Przeprowadzone badania pozwoliły cały obszar innych systemów radiowych poza powyżej scharakteryzowanymi podzielić na dwa rodzaje:

- systemy wojskowej łączności radiowej służące do szybkiej transmisji danych;
- systemy publicznej radiokomunikacji ruchomej.

W toku przeprowadzonych badań za wojskowe perspektywiczne systemy, w które można włączyć sieci stanowisk dowodzenia uznano radiowe sieci dystrybucji danych występujące, jako:

- sieci pozycjonowania, nawigacji (ang. POS/NAV) oraz kontrolowania ugrupowania bojowego (meldowania). Trudno obecnie jednoznacznie stwierdzić, w którym kierunku będą prowadzone prace badawcze i wdrożeniowe jeśli chodzi o polskie siły zbrojne. Można z dużym prawdopodobieństwem stwierdzić, że będą to rozwiązania bardzo zbliżone lub identyczne z amerykańskimi systemami EPLRS (ang. Enhanced Posicion Location Reporting System);
- Taktycznych Systemów Dystrybucji Informacji JTIDS (ang. - Joint Tactical Information Distribution System) związanych z transmisją danych i posiadających swój

ekwiwalent w takich systemach jak TADIL-J (ang. - Tactical Digital Information Links), a w koncepcjach NATO jest on znany w postaci standardu Link-16.

W przypadku współdziałania cywilno-wojskowego wspólne stanowiska dowodzenia lub punkty kierowania mogą być wyposażone w środki łączności komórkowej oraz telefonii bezprzewodowej DECT (ang. Digital European Cordless Telephony). tylko uzupełniające funkcjonujące sieci zasadnicze.

Sieci takie mogą być przeznaczone do wymiany informacji nie objętych klauzulą bezpieczeństwa albo przy wykorzystaniu specjalnych aparatów dwusystemowych DECT/GSM umożliwiających wymianę różnych kategorii informacji.

BIBLIOTEKA GŁÓWNA – ARCHIWUM
Nr ewid. 60543
II
Akademii Obrony

Akademia
Obrony
Narodowej