



# PRZEGLĄD WOJSK LĄDOWYCH



Nr 10 (556) PAŹDZIERNIK 2005



18 X  
ŚWIĘTO  
WOJSK  
ŁĄCZNOŚCI  
I INFORMATYKI

Płk dypl. MIROSŁAW SIEDLECKI

SZEF ZARZĄDU ŁĄCZNOŚCI I INFORMATYKI (G-6) DWŁAD

## PERSPEKTYWICZNY SYSTEM TELEINFORMATYCZNY WOJSK LĄDOWYCH



Obserwowane w ostatnich latach diametralne zmiany charakteru zagrożeń determinują restrukturyzację sił Sojuszu, a tym samym decydują o istocie i charakterze naszych zobowiązań. Opracowane plany rozwoju i modernizacji wojsk lądowych zakładają stopniową ewolucję w kierunku jednostek lekkich, w pełni mobilnych i zdolnych do przerzutu, działających często w ekstremalnych warunkach terenowych i klimatycznych. To z kolei wymusza zmiany w systemie dowodzenia i kierowania wojskami, w którym decydującą rolę odgrywają nowoczesne systemy łączności i automatyzacji.

**P**roces wyposażania jednostek wojsk lądowych w nowoczesny sprzęt łączności i informatyki jest realizowany od kilku lat. Stopień jego zaawansowania jest szczególnie widoczny w jednostkach wydzielanych do sił odpowiedzi NATO zgodnie z celami Sił Zbrojnych. Czynnikiem decydującym o powodzeniu jego realizacji jest konieczność nadążania za postępem technologicznym oraz kompleksowa wymiana przestarzałego sprzętu na sprzęt nowej generacji.

Podstawą wprowadzania systemów przyszłości są własne doświadczenia zdobywane w trakcie misji pokojowych, zwłaszcza tej w Iraku, przede wszystkim jednak uważne śledzenie dynamicznych zmian w dziedzinie techniki łączności i informatyki w armiach stanowiących światową awangardę technologiczną. A zakres i tempo zachodzących zmian są imponujące – to, co kilka lat temu wydawało się odległą, a nawet mglistą perspektywą, okazuje się być sprzętem lub systemami wprowadzanymi obecnie do wyposażenia jednostek.

Biorąc pod uwagę przedstawione trendy, uważam, że nasze wysiłki w najbliższej przyszłości powinny koncentrować się na trzech głównych kierunkach:

- ✓ automatyzacji procesów dowodzenia i kierowania środkami walki na wszystkich szczeblach, by docelowo dotrzeć do każdego żołnierza;
- ✓ mobilnych systemach dowodzenia i łączności;
- ✓ sukcesywnej odnowie technicznej, technologicznej i programowej eksploatowanych systemów teleinformatycznych WŁad.

Określając strategię działania wykraczającą poza rok 2010, trzeba przyjąć podstawowy kierunek działań, zresztą powszechnie eksponowany, czyli **osiągnięcie zdolności sieciocentrycznych**.

Koncepcja NCW<sup>1</sup> jest pomyślana jako implementacja **wieloczynnikowej przewagi militarnej** (*multifactor military superiority*) bazującej w obszarze operacyjnych czynników potencjału bojowego na **dominacji informacyjnej** (*information superiority*), a w odniesieniu do wszystkich pozostałych czynników – na dominacji technologicznej (*technological superiority*). U podstaw NCW leży doktrynalne założenie, że operacyjne czynniki potencjału bojowego, wykorzystujące dominację technologiczną, w praktyce mogą być podstawą odniesienia sukcesu na polu walki **jedynie w warunkach bezwzględnej dominacji informacyjnej**.

Systematycznie zwiększające się uzależnienie wszystkich obszarów funkcjonowania współczesnych społeczeństw, w tym zarządzania potencjałem obronnym i systemów dowodzenia, a także środków walki od infrastruktury informacyjnej stworzyło nie tylko nowe szanse, ale i nowe zagrożenia. Potencjał informacyjny stał się bowiem faktycznie czynnikiem warunkującym powodzenie wszelkich doktryn opartych na dynamicznym tworzeniu lokalnych ognisk rozstrzygającej przewagi potencjału bojowego w wybranym miejscu i czasie.

Szczególną rolę przypisuje się potencjałowi informacyjnemu. Może być on istotnym czynnikiem decydującym o przewadze potencjału dowodzenia i rażenia (*key superiority enabler*).

**Na operacyjny potencjał informacyjny składają się przede wszystkim:**

- ✘ wiedza sytuacyjna, na przykład o: bieżącym położeniu i działaniu wojsk przeciwnika, jego zamiarach operacyjnych i taktycznych, charakterystykach technicznych uzbrojenia itp.;
- ✘ ludzie uczestniczący w procesach informacyjnych wraz z ich indywidualną wiedzą i wyszkoleniem, stanem emocjonalnym i motywacjami;
- ✘ infrastruktura informacyjna funkcjonująca na rzecz systemów rozpoznania i dowodzenia wojskami oraz kierowania środkami walki (obejmująca m.in. infrastrukturę sensorową, telekomunikacyjną i informatyczną).

Szczególna rola potencjału informacyjnego wynika z tego, że zaawansowane technologie informacyjne tworzą dziś nie tyle element, ile infrastrukturę informacyjną systemów zarządzania siłami zbrojnymi, dowodzenia wojskami i kierowania środkami walki, a także systemów uzbrojenia i sprzętu wojskowego.

Nowa rola potencjału informacyjnego znalazła swój wyraz w dokumentach doktrynalnych USA, znanych jako *Joint Doctrine for Information Operations, Joint Pub 3-13*. Wynika z nich, że doktrynalnym celem **operacji informacyjnych** jest zamierzone oddziaływanie na systemy i zasoby informacyjne przeciwnika przy jednoczesnej obronie własnych. Dlatego też odpowiednie zabezpieczenie wywiadowcze i telekomunikacyjne tych wartości jest traktowane jako krytyczny czynnik sukcesu.

W systemach epoki NCW **bezpieczeństwo informacyjne powinno być integralnym kryterium ich projektowania oraz procedur eksploatacji**.

Informacje o położeniu wojsk własnych otrzymywane w wyniku stosowania tradycyjnych procedur meldunkowych nie zawsze są wiarogodne, zwykle uzyskiwane są bowiem w zbyt długim cyklu, dając jedynie lokalny obraz sytuacji. Z tych samych przy-

<sup>1</sup> *Network Centric Warfare – sieciocentryczne działania wojenne*

czyn informacje o wojskach przeciwnika są niekompletne i nie nadążają za dynamicznym rozwojem działań (tzw. fragmentacja informacji – według kanałów jej pozyskiwania). Wynika to z faktu, że potencjał intelektualny i informacyjny (stanowiący komponenty systemu dowodzenia) jest w zasadzie ograniczony do zasobów każdego stanowiska dowodzenia. Natomiast system szkolenia jest ukierunkowany na ogół na rutynowe rozstrzygnięcie problemów decyzyjnych zgodnie z normami operacyjno-taktycznymi, co prowadzi zwykle do bezradności w zaskakujących sytuacjach.

Jednolity obraz pola walki na tolerowanym poziomie entropii może zapewnić jedynie system monitorowania, syntezy i oceny sytuacji z wielu komplementarnych źródeł, zapewniający efekt synergii i funkcjonujący jako usługa na rzecz „wszystkich, którzy potrzebują informacji, w zakresie ich potrzeb i uprawnień”.

Szybki rozwój społeczeństwa informacyjnego, w tym powstanie nowych dziedzin i usług, przede wszystkim Internetu i sieci komórkowych, wpłynął zasadniczo na kierunki ewolucji systemów telekomunikacyjnych. Także wojskowe polowe i stacjonarne systemy telekomunikacyjne przechodzą szybką ewolucję, wymuszoną nowymi wymaganiami i potrzebami.

Zmienia się również taktyka wojsk łączności, obejmując obszary obsługujące użytkowników o dużym stopniu mobilności i znacznych potrzebach telekomunikacyjnych. Użytkownicy wymagają nie tylko transmisji utajnionych sygnałów mowy, lecz przede wszystkim szybkich systemów transmisji danych o dużych przepustowościach, zdolnych do obsługi współczesnych czujników systemów rozpoznania (sensorów), w tym utajnionych sygnałów wideo. **Dlatego też powstały nowe koncepcje działań sieciocentrycznych wymagające innego spojrzenia na polowe systemy łączności.**

Jeszcze niedawno przeważał pogląd, że uniwersalną infrastrukturą telekomunikacyjną, zarówno w systemach polowych, jak i stacjonarnych, będzie szerokopasmowa sieć zintegrowana (B-ISDN) wykorzystująca technikę ATM, wspomagana przez kolejne generacje sieci inteligentnej (IN).

Koncepcja ta była podstawą rozpoczęcia pracy powołanego w ramach porozumienia dwunastu państw członkowskich NATO<sup>2</sup> zespołu, znanego jako TACOMS POST 2000, którego celem było opracowanie propozycji nowych norm działania (STANAG-ów).

W 2003 r. TACOMS POST 2000 przeprowadził prace nad zmianą koncepcji i zrezygnował z preferowania technologii ATM (opracowanie WP13202 „*Reorientation study*”) na rzecz rozwoju polowych systemów łączności w świetle nowych uwarunkowań. Nie uwzględnił przy tym podsystemów radiowych KF i UKF działających autonomicznie, których umiejscowienie w systemie łączności będzie wymagać oddzielne potraktowania.

## Perspektywiczna technologia – IP

Obecnie coraz częściej stosowaną technologią komunikacyjną dla transferu głosu jest Voice over IP (VoIP), w której wyeliminowano takie ułomności, jak duże opóźnienie przejścia i niska jakość głosu, spowodowane zbyt dużą jego kompresją oraz

<sup>2</sup> Do zespołu tego Polska dołączyła w 2002 r.

małą elastycznością systemu wynikającą z braku interfejsów do pracy w sieci publicznej PSTN.

Zdaniem ekspertów, ten rodzaj transmisji głosu stanowi najlepsze obecnie rozwiązanie na najbliższą przyszłość. Dzisiejsza technologia transmisyjna oraz komutacyjna w tym zakresie pozwala na budowę niezawodnych sieci pakietowych o dużych przepływnościach. Rozwój procesorów sygnałowych DSP pozwala bowiem na łatwą implementację systemów cyfryzacji fonii i efektywnych systemów kompresji sygnałów fonicznych. W sieciach rozległych wdrożono nowe protokoły routingowe, które zapewniają optymalny transfer pakietów głosu i danych. Możliwy stał się zatem transfer różnych rodzajów informacji w jednej sieci i na jednej platformie, co znacznie usprawnia i unowocześnia działanie jednolitego systemu, a przy tym zmniejsza koszty jego budowy i utrzymania. Racjonalne zatem staje się wykorzystanie technologii IP do budowy sieci łączności (zarówno fonii, wideo, jak i danych) do komunikacji między węzłami łączności. Z funkcjonalnego punktu widzenia sieć ta będzie stanowić infrastrukturę korporacyjną wykorzystującą dzierżawione trakty transmisyjne oraz własne systemy komutacyjne. Wykorzystywanie wspólnej platformy IP do transferu wszystkich rodzajów sygnałów pozwoli zbudować wspólną sieć zarządzaną w jednakowy sposób. Nie bez znaczenia jest fakt, że koszt jej eksploatacji już teraz jest znacznie mniejszy niż sieci z komutacją kanałów. Ponadto technologia ta umożliwi nam wprowadzenie na dużą skalę bezpiecznej komunikacji między węzłami (dzięki zastosowaniu np. mechanizmów IPSec), z jednoczesnym szyfrowaniem przesyłanej informacji. Natomiast wprowadzenie kolejnej wersji protokołu IPv 6 spowoduje, że ta sama technika stanie się znacznie stabilniejsza i dojrzała.

## Charakterystyka perspektywicznych mobilnych systemów teleinformatycznych

Współczesne polowe systemy łączności można rozpatrywać z dwóch podstawowych punktów widzenia, czyli wymagań taktyczno-operacyjnych i technicznych.<sup>3</sup>

Dokonując zatem analizy systemu z punktu widzenia wymagań taktyczno-operacyjnych, należy odnotować następujące zmiany:

- ❖ jednostki wojskowe, zwłaszcza korpusty i kontyngenty wojskowe wysyłane w ramach misji pokojowych, stały się podmiotami wielonarodowymi (np. Wielonarodowy Korpus Północny Wschód w Szczecinie);
- ❖ jednostki te nie biorą udziału w typowych działaniach bojowych z zachowaniem linii frontu i jasno określonym pasem działania. Regułą stały się bowiem konflikty asymetryczne oraz działania przeciwpartyzanckie i antyterrorystyczne. Obszar, na którym się toczą, jest coraz większy, a wskazane jednostki nie pokrywają swoją działalnością całego terytorium, lecz działają metodą zwartych zgrupowań rozmieszczonych w znacznej odległości od siebie. Dlatego też dotychczasowy obszarowy (oparty głównie na radioliniach horyzontalnych) system łączności powinien być bardziej rozległy i nie musi pokrywać ściśle całego obszaru odpowiedzialności;
- ❖ zwiększające się wymagania związane z mobilnością wojsk, wymuszające również zapewnienie im sprawnej obsługi przez system łączności.

<sup>3</sup> Należy zauważyć, że w ostatnich latach nastąpiły istotne zmiany zarówno w zakresie wymagań, jak i poziomu techniki warunkujące ponowne spojrzenie na problem budowy systemów łączności poziomu taktycznego.

System musi zapewniać utajniony, odporny na zakłócanie transfer dużych ilości informacji w rzeczywistym czasie między wieloma rozproszonymi mobilnymi jednostkami różnych rodzajów wojsk. Muszą zatem powstać nowe podsystemy łączności ruchomej, przewyższające wiele ograniczeń charakterystycznych dla istniejących systemów, a związanych z pojemnością, stopniem pokrycia obszaru, interoperacyjnością, żywotnością i wrażliwością na przeciwdziałanie, redukując przy tym niebezpieczeństwo utraty lub przeterminowania danych. Podsystemy te nie zastępują klasycznej sieci łączności radioliniowej, lecz stanowią jej bardzo ważne uzupełnienie w zakresie współpracy różnych rodzajów wojsk i obsługi mobilnych jednostek poziomu taktycznego;

❖ powstają nowe problemy w utrzymywaniu łączności dalekosiężnej z jednostkami wydzielonymi do PKW.

Ze względu na duże potrzeby telekomunikacyjne niewystarczające są w tych sytuacjach klasyczne systemy łączności radiowej KF i abonenckie systemy satelitarne (takie jak Inmarsat B). Wymagane są systemy zapewniające duże pojemności transmisyjne;

❖ wzrastają potrzeby związane z przepustowością relacji zwłaszcza systemów teleinformatycznych.

Dotychczasowe zastosowania systemów ograniczane do transmisji sformalizowanych wiadomości i informacji tekstowych przestały być wystarczające. Pojawiło się wiele nowych aplikacji zapewniających użytkownikom nowe możliwości, lecz wymagających znacznej przepustowości. Coraz częściej są stosowane wideokonferencje (oraz cała sfera transmisji obrazów ruchomych i nieruchomych) wymagająca zaangażowania wielu elementów systemu pracujących w czasie rzeczywistym.

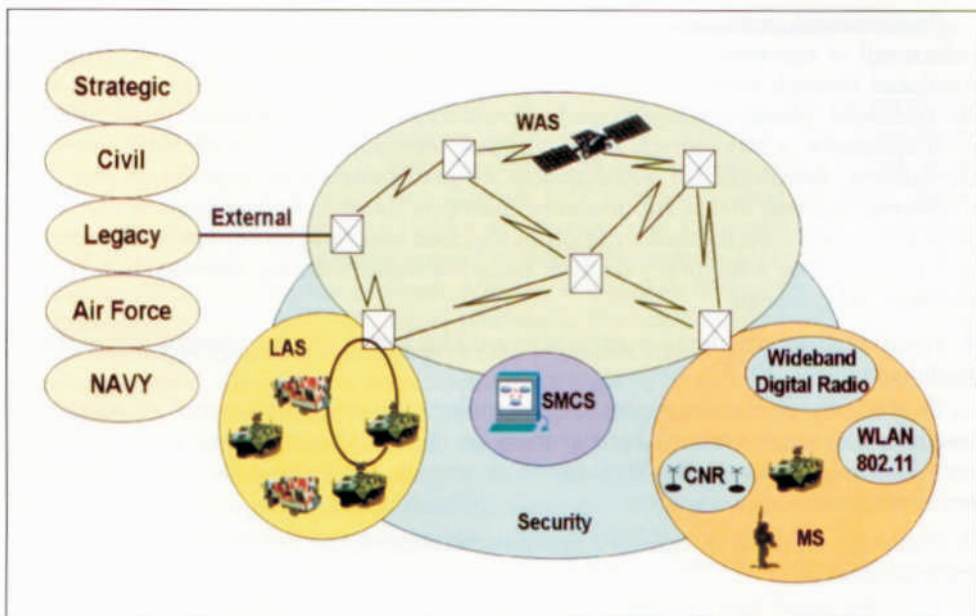
Niezależnie od zaprezentowanych kierunków zmian, pozostaje nadal aktualny kanon budowy systemu łączności związku taktycznego i operacyjnego zdolny połączyć stanowiska dowodzenia jednostek podległych i wspierających.

Najprostszym i najtańszym rozwiązaniem jest budowa sieci bazowej wykorzystującej radiolinie horyzontalne dużej przepustowości, zawierające cztery węzły bazowe dla dywizji i osiemnaście węzłów bazowych dla korpusu. Jednak w świetle nowych wymagań konieczne jest uzupełnienie systemu o środki pozahoryzontalne, satelitarne i troposferyczne, mogące zapewnić łączność bezpośrednią z jednostkami działającymi w znacznym oddaleniu od sił głównych.

## Architektura współczesnych systemów teleinformatycznych

W perspektywnym wojskowym systemie teleinformatycznym z technicznego punktu widzenia można wyróżnić następujące elementy składowe (rys. 1):

- ✓ rozległy system transmisyjny (*Wide Area Subsystem – WAS*) tworzący bazową sieć transmisyjną;
- ✓ lokalny system abonencki (*Local Area Subsystem – LAS*) tworzący sieć abonencką na stanowiskach dowodzenia;
- ✓ system dostępu bezprzewodowego (*Mobile Subsystem – MS*) obsługujący obiekty ruchome, w tym systemy związane z LAS i WAS (szeroko- i wąskopasmowe systemy dostępowe, standard 802.11) oraz systemy w znacznym stopniu autonomiczne (np. typu LINK-16);



Rys. 1. Architektura perspektywnego systemu teleinformatycznego wojsk lądowych zgodnie z propozycją zawartą w STANAG-u 4636

- ✓ system szyfrowania wiadomości (*Security*);
- ✓ system zarządzania i utrzymania systemu (*System Management and Control Subsystem – SCMS*).

Podstawowymi elementami systemu transmisyjnego będą:

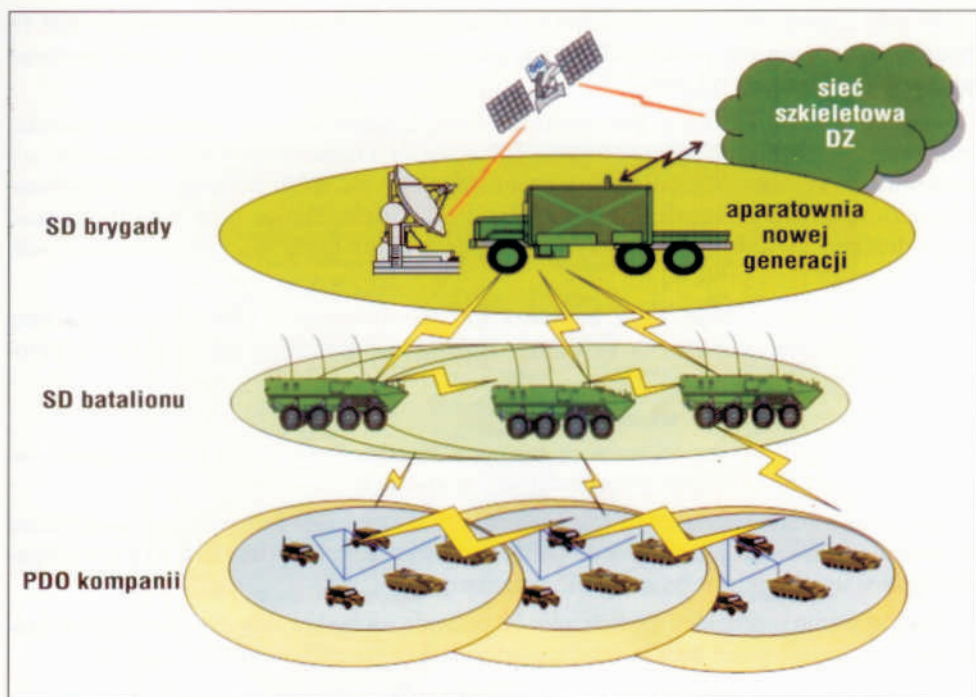
#### ✗ Mobilne terminale satelitarne szczebla strategicznego i taktycznego

Są one przewidywane do zapewnienia realizacji połączeń dalekosiężnych, jak również połączeń końcowych typu punkt-punkt i międzywęzłowych w układzie narodowym i koalicyjnym; parametry techniczne terminala powinny być zgodne ze STANAG-iem 4484 ed. 2 i 4486 ed. 2.

#### ✗ Radiowe systemy dostępu szerokopasmowego

Jednym z czynników, który w znaczny sposób ograniczał możliwość budowy lokalnych i rozległych sieci komputerowych na szczeblu pododdziału, był brak urządzeń zapewniających transmisję szerokopasmową. Rozwiązaniem są radiostacje szerokopasmowe, znane pod techniczną nazwą HCDR (*High Capacity Data Radio*). Zapewnią one docelowo niezbędne przepływności transmisyjne – do 512 kbit/s do budowy sieci komputerowych (rys. 2).

Radiostacje szerokopasmowe pracują dzięki wykorzystaniu protokołów IP. Odpowiedni stopień nasycenia tymi radiostacjami obszaru działań zapewni odporne i elastyczne środowisko teleinformatyczne, w którym informacje będą przesyłane w relacjach pionowych i poziomych, od sensorów przez decydenta do wykonawcy. Użytkownicy systemu wyposażeni w radiostacje HCDR z systemami GPS oraz systemem IFF uzyskają dostęp do informacji o sytuacji wojsk własnych i przeciwnika w czasie rzeczywistym lub bliskim rzeczywistemu.



Rys. 2. Wykorzystanie systemów szerokopasmowych

### × Lokalny system abonencki

Stanowią go elementy spełniające wymagania standardów TACOMS POST 2000. W skład LAS wchodzi:

- urządzenia warstwy dostępu do sieci rozległej WAS (*access layer*), wśród których powinny być takie elementy, jak WAN Box'y<sup>4</sup> i ROUTER Box'y;
- urządzenia warstwy szkieletowej LAS (*backbone layer*), takie jak LAN Backbone Box' i Serwer Box'y;
- urządzenia warstwy dostępu użytkowników (*user access layer*) w miejscach ich pracy, zlokalizowanych w kontenerach sztabowych, w tymczasowych pomieszczeniach stacjonarnych i w namiotach wyposażonych w LAN Access Box'y.

### × System dostępu bezprzewodowego

Zapewnia bardzo szybkie rozwijanie sieci komputerowej, zwłaszcza na szczeblach taktycznych. Możliwość taką stwarza technologia sieci bezprzewodowych LAN wykorzystująca protokoły IEEE 802.11. Użytkownicy sieci bezprzewodowej mogą się swobodnie przemieszczać wewnątrz ugrupowania bojowego lub między jego elementami, mając jednocześnie dostęp do bazy danych przechowywanych w serwerach centralnych.

<sup>4</sup> Nazewnictwo robocze.



W celu zapewnienia bezpieczeństwa tym sieciom wprowadzono standard 802.1x będący rozwiązaniem problemu braku uwierzytelniania i odpowiedniego poziomu poufności w sieciach WLAN.

Implementacja systemu zarządzania siecią bezprzewodową umożliwia monitoring wszystkich urządzeń aktywnych, jak również klientów sieci z określeniem ich położenia w systemie (współrzędne geograficzne).<sup>5</sup> Ponadto pozwala na określenie elementów wojsk własnych i przeciwnika. Próby nielegalnego oraz nieautoryzowanego dostępu są natomiast wykrywane wraz z ustaleniem miejsca położenia osób dokonujących tych prób.

Praca mobilnych sieci LAN powinna być chroniona przez bezpieczne systemy wirtualnych sieci prywatnych VPN, protokoły IPSec oraz silne mechanizmy kryptograficzne.

#### **✕ System szyfrowania wiadomości**

Może być realizowany za pomocą zarówno standardowych, jak i wyspecjalizowanych środków (np. IPCrypto) stosowanych w sieciach IP.

Modułowa budowa systemu LAS pozwala w łatwy i przejrzysty dla organizatora systemu sposób zaimplementować politykę bezpieczeństwa umożliwiającą wyseparowanie w systemie strefy „czarnej” i „czerwonej”.

Zastosowanie technologii szyfrowania IP pozwala na budowanie sieci rozległej, w której pracują użytkownicy wykorzystujący informacje o różnych klauzulach tajności.

#### **✕ System zarządzania, utrzymania i kontroli**

System ten (*System Management and Control Subsystem – SMCS*) powinien zapewniać zarządzanie technicznymi zasobami łączności oraz przetwarzaniem informacji. Powinien składać się z elementów sprzętowych i programowych, których celem będzie koordynowanie i wspomaganie kierowania oraz zapewnienie efektywnej pracy systemu łączności.

Koncepcja zarządzania i monitoringu powinna wykorzystywać system transmisji informacji TCP/IP, w skład którego wchodzi takie protokoły, jak: TCP, UDP, SNMP, ICMP itp.

Podstawowym protokołem zarządzania powinien być SNMP (*Single Network Management Protocol*) w wersji v.3.

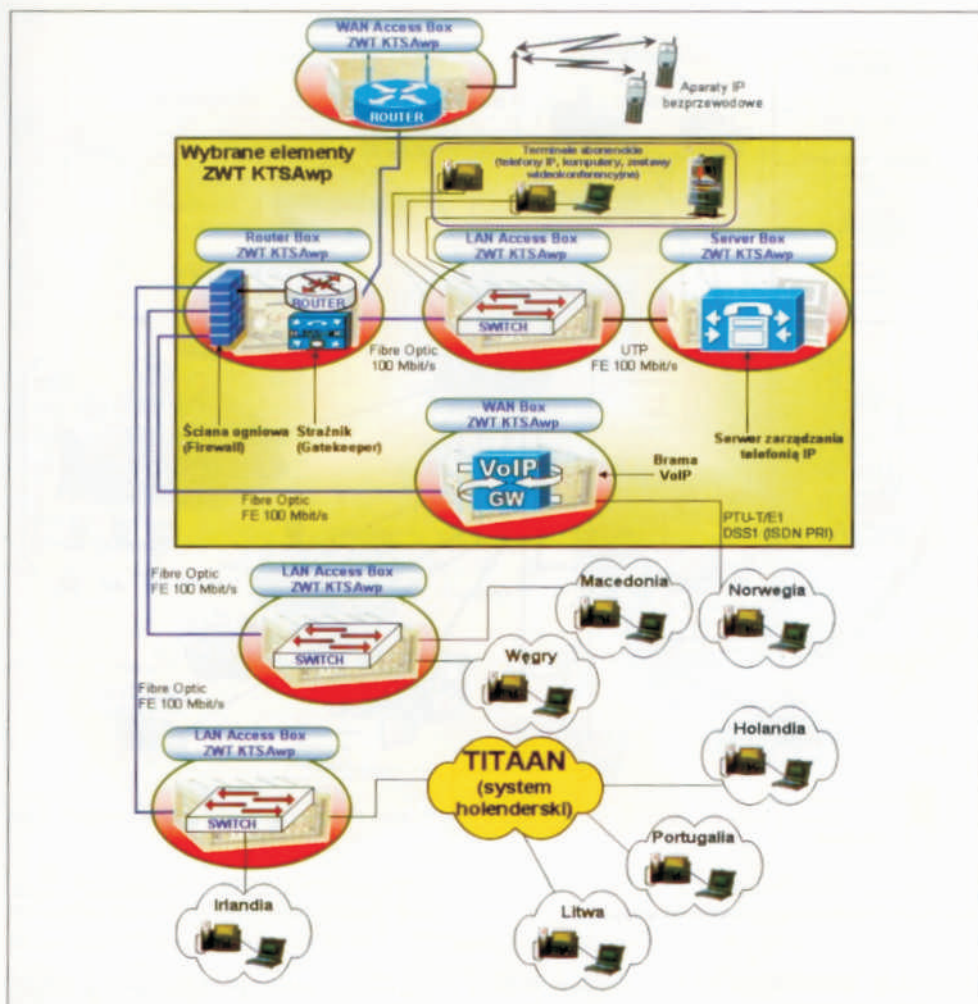
Wśród elementów sprzętowych systemu zarządzania i kontroli powinny znajdować się:

- ✓ aparatownie zarządzania rozłokowane na szczeblu WAS;
- ✓ stacje zarządzania przeznaczone do realizacji zarządzania i kontroli na poziomie lokanych centrów zarządzania w ramach LAS;
- ✓ zintegrowane elementy sprzętowe zamontowane w poszczególnych urządzeniach i przeznaczone do zarządzania nimi.

## **Dzień dzisiejszy systemu teleinformatycznego wojsk lądowych**

Wojska lądowe dysponują mobilnym sprzętem teleinformatycznym spełniającym zalecenia NATO – środkami transmisyjnymi tworzącymi WAS i LAS. Są to aparatu-

<sup>5</sup> Umożliwia między innymi takie oprogramowanie, jak: *Wireless Solution Engine*, *Cisco Distributed WLAN* i *Cisco Wireless Control System*.



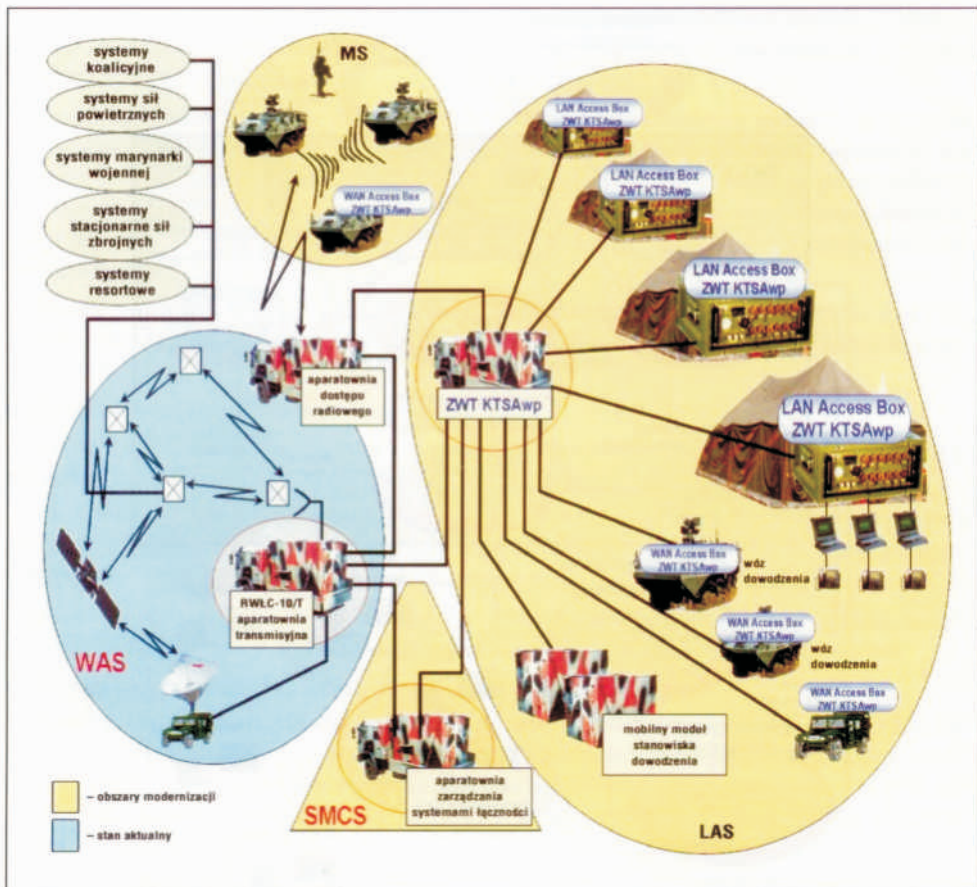
Rys. 3. Schemat połączeń realizowanych w trakcie testów VoIP podczas międzynarodowych warsztatów łączności „Combined Endeavor 2005”

townie systemu STORCZYK typu RWLC-10/T i RWLC-10/K oraz obecnie wdrażane zintegrowane węzły teleinformatyczne KTSAwp.

Rozwój technologii telekomunikacji oraz prace międzynarodowego zespołu opracowującego architekturę taktycznego systemu telekomunikacyjnego pk. TACOMS wiążą się z koniecznością szybszego modernizowania posiadanego potencjału teleinformatycznego.

Międzynarodowe warsztaty łączności „Combined Endeavor 2005” (zorganizowane w Niemczech w dniach 13-26 maja 2005 r.) były kolejnymi, na których testowano m.in. technologię Voice over IP (rys. 3). Bez wątpienia wykazały one potrzebę implementowania tych rozwiązań na większą skalę, w tym w SZ RP.

Na 43 państwa biorące udział w tych warsztatach tylko 8 krajów (w tym Polska) posiadało systemy wykorzystujące technikę VoIP. Jednak co roku przybywa armii, które wdrażają technologię VoIP do swoich systemów teleinformatycznych i wyra-



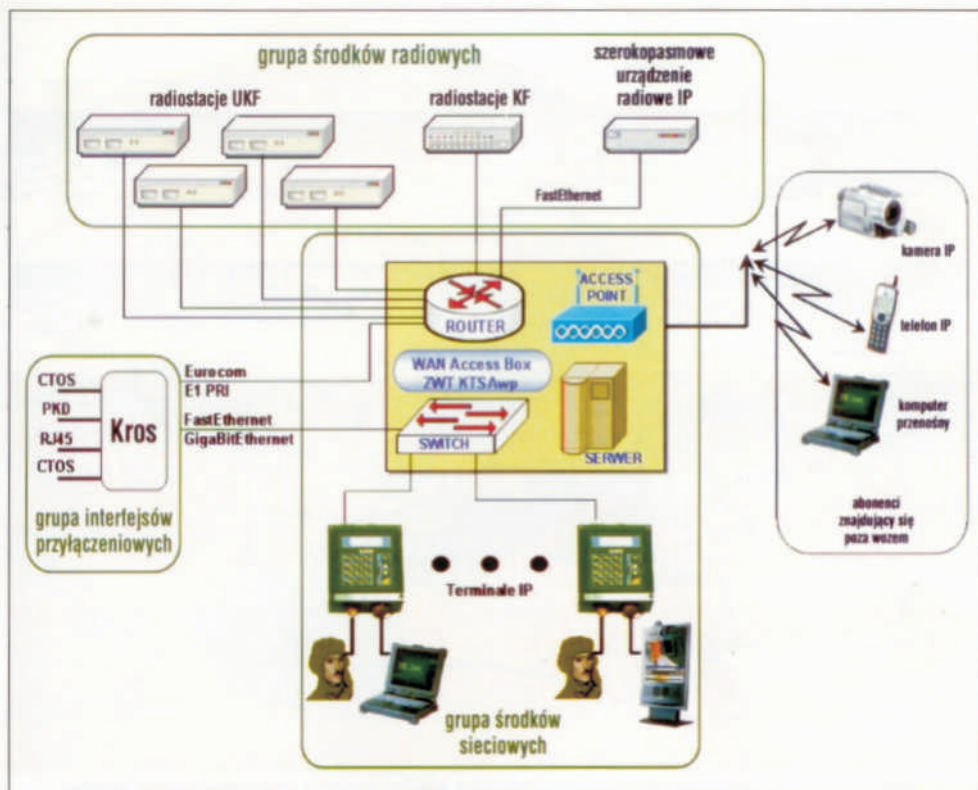
Rys. 4. Zmodernizowany system teleinformatyczny SD

zają chęć testowania tych urządzeń w celu osiągnięcia interoperacyjności z systemami innych państw.

W bieżącym roku Polska przedstawiła do testowania rozwiązanie telefonii IP przy zastosowaniu systemu ZWT KTSAwP. Testy tych urządzeń również dotyczyły sprzęgnięcia systemu informatycznego SZAFRAN z systemami innych krajów. Testy telefonii IP i VoIP przebiegły pozytywnie.

Uwzględniając przedstawione rozważania, należy stwierdzić, że **perspektywny wojskowy system teleinformatyczny wojsk lądowych** musi w większym stopniu wykorzystywać transmisję danych, głosu i obrazu (ruchomego i statycznego) na potrzeby systemów dowodzenia i kierowania środkami walki.

**Modernizacja istniejącego systemu teleinformatycznego** wynika przede wszystkim z konieczności zastosowania informatyki na stanowiskach dowodzenia, w tym informatycznych systemów dowodzenia typu SZAFRAN-ZT oraz systemów kierowania środkami walki typu TOPAZ, ŁOWCZA i REGA, a także na potrzeby logistyki, kadr itp.



Rys. 5. Propozycja wykorzystania elementów WAN Access Box ZWT KTSAwP w wozach dowodzenia nowej generacji

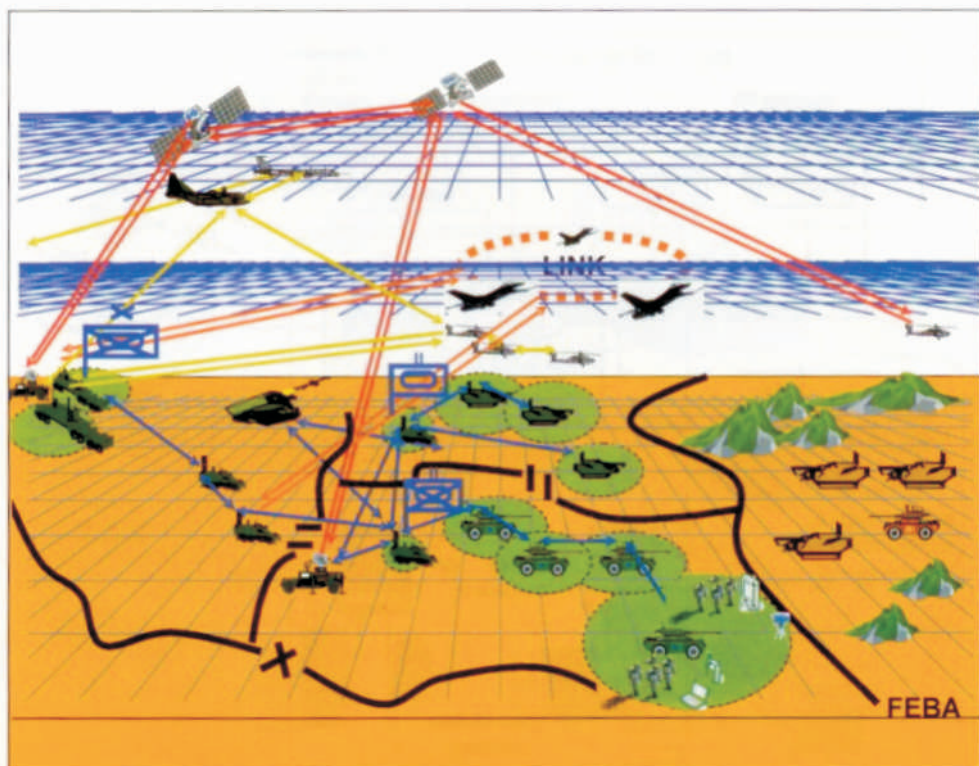
W następstwie pozytywnych rezultatów rozbudowy stacjonarnej infrastruktury rozległej sieci teleinformatycznej MIL WAN wojska lądowe poszukiwały rozwiązań, które umożliwią eksploatację informatycznych systemów dowodzenia w warunkach polowych. Takie możliwości daje zintegrowany węzeł teleinformatyczny KTSAwP w wersji polowej.

Wprowadzenie nowej generacji sprzętu na stanowisko dowodzenia pozwoli na kompleksowe wykorzystanie głosu, danych oraz transmisji obrazów stałych i ruchomych, a także na wyeliminowanie nadmiernego rozwijania kabli przez drużyny kablowe. Przyniesie to wymierne oszczędności zarówno ilościowe, jak i finansowe (rys. 4).

Nowego spojrzenia wymaga także potrzeba zapewnienia aktualnej informacji na stanowiskach dowodzenia organizowanych doraźnie na polu walki z wykorzystaniem wozów dowodzenia i wozów bojowych.

Wóz bojowy powinien zostać wyposażony w niezbędne środki radiowe (szerokopasmowe, szerokopasmowe spełniające standard 802.11) w celu zapewnienia jemu komunikacji z elementami ugrupowania bojowego zarówno wówczas, gdy jest w ruchu lub został zatrzymany.

Ogólnym założeniem jest to, by osoba funkcyjna, wykorzystując wyposażenie znajdujące się w wozie dowodzenia lub bojowym (telefon IP, kamera, wiedotelefon



Rys. 6. Osiągnięcie zdolności sieciocentrycznych w zakresie infrastruktury teleinformatycznej w ugrupowaniu bojowym (przykład)

i komputer), była w stanie wysyłać i odbierać dane oraz prowadzić rozmowy telefoniczne bez względu na to, jakie medium jest dostępne w danej chwili.

Nowoczesny wóz bojowy (rys. 5) powinien być wyposażony w grupy urządzeń:

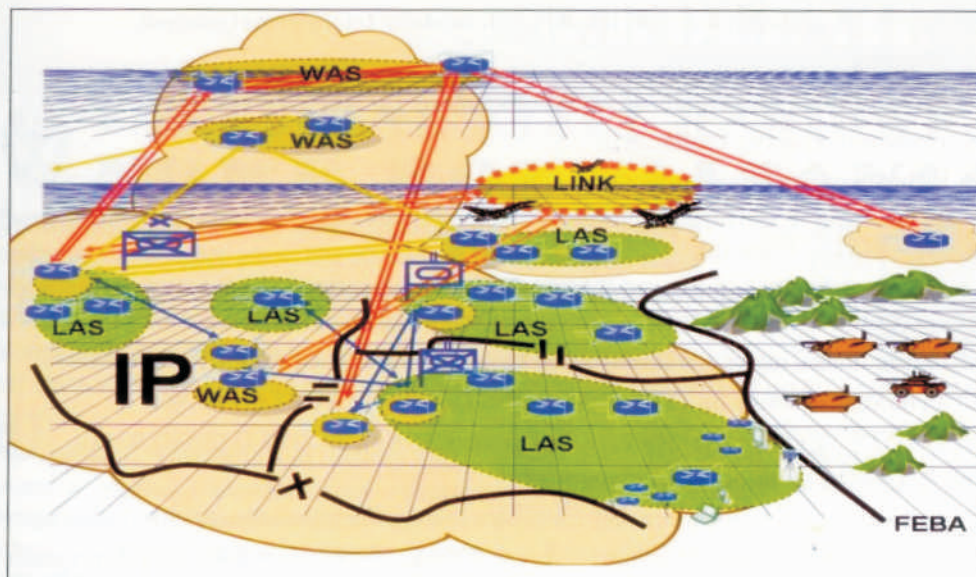
- ✓ sieciowych,
- ✓ radiowych,
- ✓ interfejsów przyłączeniowych.

Każda z tych grup ma możliwości, które w zależności od układu pracy można wykorzystać, by zapewnić odpowiednie warunki pracy osobom funkcyjnym.

Niezbędne jest także wyposażanie wozu bojowego w sprzęt informatyczny zbudowany zgodnie z technologią IP, tj. wprowadzenie mobilnego routera i switcha do budowy lokalnej sieci komputerowej LAN uzupełnionej zestawem interfejsów światłowodowych i serwerem pokładowym.

Omawiane rozwiązania umożliwiają osiągnięcie już w niedługim czasie zdolności sieciocentrycznych na najniższych szczeblach dowodzenia (rys. 6, 7).

Dlatego też mobilność na polu walki to również ciągły przepływ pakietów IP niosących dane, głos i obraz w trzech obszarach, a mianowicie radiowym, satelitarnym i standardem 802.11 (rys. 8).

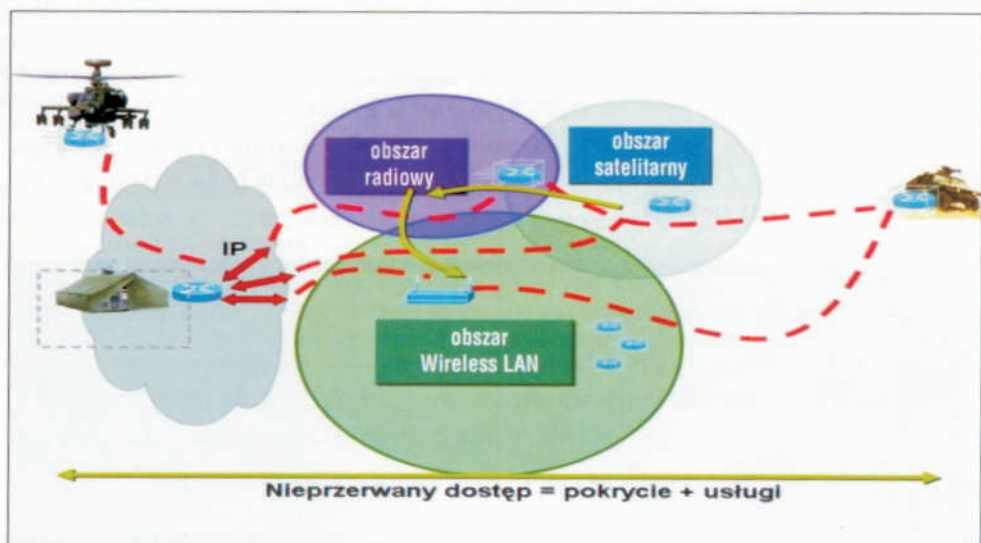


Rys. 7. Sieć IP wraz z bramą do sieci LINK

Obszary te zapewnią nieprzerwany dostęp do usług realizowanych w sieci z każdego miejsca ugrupowania bojowego.

Proponowany system teleinformatyczny będzie w pełni interoperacyjny dzięki:

- ✗ zapewnieniu realizacji obowiązujących światowych standardów teleinformatycznych;
- ✗ zgodności z aktualnymi standardami NATO (STANAG);
- ✗ wykorzystaniu elementów technologii komercyjnej (*Commercial Off The Shelf – COTS*) w mniej mobilnych elementach ugrupowania bojowego;



Rys. 8. Obszary teletransmisyjne mobilnej sieci IP

✘ zapewnieniu dostępności do istniejących mediów teleinformatycznych.

Ponadto:

- ❖ zapewni dużą niezawodność eksploatacyjną,
- ❖ zmniejszy koszty eksploatacji,
- ❖ będzie rozwiązaniem najnowocześniejszym.

W procesie modernizacji należy uwzględnić podstawowe dokumenty i nowe propozycje NATO, takie jak:

- ☆ CR149 Consultancy Report: TACOMS Operational C2 and information architectures prepared by NC3A;
- ☆ Interconnection of Communications and Informaton System (AC/322-D/0030);
- ☆ Primary Directive on INFOSEC (AC/35-D/2004) 7 (AC/322-D/0030);
- ☆ NATO C3 System Architecture Framework (NAF), AC/322-D (2004) 0041;
- ☆ STANAG-i od numeru 4637 do 4647.

W związku z tym, modernizując narodowy system teleinformatyczny, niezbędne są:

- a) wnikliwa analiza przesłanych przez NC3A STANAG-ów dotyczących projektu TACOMS POST 2000;
- b) wdrożenie w mobilnych aparatuwniach styku ETHERNET 1000 SX jako podstawowego w połączeniach międzysystemowych;
- c) pełne wykorzystanie zintegrowanego węzła teleinformatycznego KTSAwP;
- d) rozwiązanie problemu funkcjonowania urządzeń utajniających, bazujących na protokole IP;
- e) wdrożenie nowej rodziny radiostacji UKF mających styk ETHERNET;
- f) wyposażenie wozów dowodzenia w nową rodzinę urządzeń informatycznych bazujących również na protokole IP;
- g) wprowadzenie radiostacji szerokozakresowych, szerokopasmowych i standardu 802.11.

Realizacja tych przedsięwzięć będzie wymagać ogromnego wysiłku wszystkich tych, którzy zajmują się problematyką dowodzenia i łączności.

Uważam, że kadra, żołnierze i pracownicy wojska sprostają tym wymaganiom i tak jak dotychczas z dużym zaangażowaniem i poświęceniem będą wykonywać postawione przed nimi zadania.

*Z okazji Święta Wojsk Łączności i Informatyki składam wszystkim żołnierzom i pracownikom wojska serdeczne życzenia zdrowia, pomysłowości i sukcesów w życiu osobistym i rodzinnym oraz satysfakcji z wykonywanych, niewątpliwie trudnych, obowiązków służbowych.*