17

AKADEMIA
OBRONY
NARODOWEJ

Płk mgr inż. Dariusz STOŃ

STACJONARNA SIEĆ TELEINFORMATYCZNA SIŁ ZBROJNYCH RZECZYPOSPOLITEJ POLSKIEJ

Rozprawa doktorska

WARSZAWA

AKADEMIA OBRONY NARODOWEJ
WYDZIAŁ WOJSK LĄDOWYCH

płk mgr inż. Dariusz STOŃ

STACJONARNA SIEĆ TELEINFORMATYCZNA SIŁ ZBROJNYCH RZECZYPOSPOLITEJ POLSKIEJ

ROZPRAWA DOKTORSKA

Promotor
Prof. dr hab. inż. Józef MICHNIAK

WARSZAWA 2008 r.

Wyrazy serdecznego podziękowania

składam

Panu Profesorowi dr. hab. inż. Józefowi Michniakowi za cenne wskazówki, uwagi merytoryczne oraz życzliwą opiekę naukową.

Dariusz Stoń

SPIS TREŚCI

WSTĘP

Wydarzenia polityczno-militarne przełomu XX i XXI wieku sprawiły, że nastąpiły zmiany filozofii myślenia o zagrożeniach bezpieczeństwa narodowego. Do niedawna największe zagrożenia definiowane były w obszarze militarnym. Tempo zmian cywilizacyjnych oraz nowoczesne technologie, wykreowały nowe obszary bezpieczeństwa narodowego.

Współcześnie obejmują one w coraz większym stopniu zagrożenia niemilitarne czyli zdolność ochrony i ratownictwa ludności, gdyż zagrożenia takie jak katastrofy i awarie techniczne, klęski żywiołowe i skażenie środowiska są często równe **skutkom wojny**. Tak więc współczesna definicja zagrożenia bezpieczeństwa państwa, jest to taki splot zdarzeń wewnętrznych lub w stosunkach międzynarodowych, w którym z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu i rozwoju wewnętrznego, bądź naruszenie lub utrata suwerenności państwa oraz jego partnerskiego traktowania w stosunkach międzynarodowych. Bezpieczeństwo ma charakter podmiotowy, a będąc naczelną potrzebą człowieka i grup społecznych, jest zarazem podstawową potrzebą państwa i systemów międzynarodowych. Jego brak powoduje niepokój i stan zagrożenia.

Reasumując powyższe można stwierdzić, że identyfikacja zmian otoczenia czyli analiza strategiczna, jest niezbędna aby organizacja mogła na nie reagować i zapewnić sukces. By żyć i osiągać swoje cele bez poczucia lęku, obawy czy strachu, musimy ciągle zdobywać wiedzę umożliwiającą zrozumienie otaczającego nas świata, zachodzących w nim zdarzeń i procesów, mogących zakłócić nasz spokój i komfort.

W związku z rosnącym zagrożeniem dla sprawnego funkcjonowania państwa ze strony grup (krajowych i międzynarodowych) zorganizowanej przestępczości, siły zbrojne powinny utrzymywać zdolność realizacji swoich funkcji w warunkach zakłóceń spowodowanych przestępczością, a jednocześnie przyczyniać się do kreowania nowych środków i form obrony państwa przed tymi zagrożeniami. Dlatego też, siły zbrojne powinny być gotowe do wydzielenia odpowiednio przygotowanych, **wyposażonych i wyspecjalizowanych** jednostek sił specjalnych do wspierania działań protekcyjnych.

Różnorodność problemów wymagać będzie od Sił Zbrojnych RP, angażowania się wyspecjalizowanymi siłami i środkami w państwowym (międzynarodowym) systemie monitorowania sytuacji, prognozowania, rozpoznania i alarmowania, ratownictwa, przeciwdziałania i likwidacji szkód.

Systemy teleinformatyczne są niezbędne do zarządzania bezpieczeństwem państwa i dlatego na bieżąco, w sposób ciągły powinniśmy obserwować ewolucję rodzaju zagrożeń, ich skalę oraz miejsca występowania w systemach teleinformatycznych. Z drugiej strony, te systemy teleinformatyczne narażone są na różnego rodzaju uszkodzenia i dlatego na bieżąco, w sposób ciągły powinniśmy wprowadzać istotne zmiany spowodowane głównie dynamiczną ewolucją technologii teleinformatycznych.

Obowiązująca strategia bezpieczeństwa naszego kraju ma charakter typowo obronny i zakłada działania wojsk głównie na obszarze kraju, choć nie wyklucza działań zbrojnych poza granicami kraju np. w ramach operacji sojuszniczych NATO.

W związku z powyższym, można założyć, że na potrzeby systemu dowodzenia sił zbrojnych na szczeblu strategicznym, udział stacjonarnych sieci teleinformatycznej będzie znacznie większy niż, polowych systemów teleinformatycznych. Przy czym jest oczywiste, że w warunkach prowadzenia działań zbrojnych na obszarze kraju, zakres oraz sposoby wykorzystania stacjonarnej sieci teleinformatycznej będą różne w zależności od rejonu obrony.

Rozszerzający się obszar odpowiedzialności oraz dynamiczny rozwój środków walki, skłania mnie do stwierdzenia, że dla zapewnienia pełnego obiegu informacji w procesie dowodzenia wojskami, stacjonarna sieć teleinformatyczna musi osiągnąć zdolność dynamicznej organizacji systemów dowodzenia, w dowolnym miejscu kraju i realnym czasie wynikającym z potrzeb procesu dowodzenia.

Dlatego prawidłowy rozwój coraz bardziej złożonej struktury sieci, jest procesem kompleksowym, wymagającym wprowadzenia całej gamy stale udoskonalonych komputerowych narzędzi wspomagających, systemów modelowania optymalizacyjnego tj. topologii, kierowania rozpływem ruchu, jakości usług niezawodności.

Telekomunikacja ruchoma i bezprzewodowa odgrywa coraz większą rolę, zajmując znaczącą pozycję w obszarze organizacji sieci teleinformatycznych. Techniczne systemy teleinformatyczne jako składnik systemu dowodzenia powinny

składać się z komponentów ***środków stacjonarnych*** jak i ***środków wysoce mobilnych***.

Z tego względu w rozprawie doktorskiej zajmę się zgłębieniem aspektów związanych ze stacjonarną siecią teleinformatyczną Sił Zbrojnych Rzeczypospolitej Polskiej. Istotą opracowania jest ocena istniejącej stacjonarnej sieci teleinformatycznej Sił Zbrojnych jako elementu niezbędnego do dowodzenia w czasie pokoju, kryzysu oraz zagrożenia militarnego państwa oraz określenie podstawowych wymagań organizacyjno - technicznych na organizację sieci teleinformatycznej. Organizacja powyższej sieci jest ściśle związana z zapotrzebowaniem na niezbędne **usługi telekomunikacyjne**[1], występujące w procesie dowodzenia w czasie pokoju, kryzysu oraz zagrożenia militarnego państwa. Systemy teleinformatyczne umożliwiają przesyłanie szerokiej gamy usług głosowych, transmisji danych oraz obrazu. W literaturze przedmiotu można spotkać wiele klasyfikacji usług telekomunikacyjnych, które autor zamieścił w **zał. 1.**

Stąd, też celem niniejszej pracy jest opracowanie ***koncepcji struktury organizacyjno – technicznej stacjonarnej sieci teleinformatycznej aby mogła zapewnić świadczenie podstawowych usług teleinformatycznych w procesie dowodzenia Siłami Zbrojnymi.***

Wspomniany zamiar opracowania ***koncepcji struktury organizacyjno – technicznej stacjonarnej sieci teleinformatycznej*** stawiany przed niniejszą pracą doktorską osiągnięto w następujący sposób:

Pierwsza część rozprawy doktorskiej przybliża czytelnikowi istotę podjętej analizy stacjonarnej sieci teleinformatycznej oraz założenia metodologiczne.

W rozdziale 2. rozprawy doktorskiej autor scharakteryzował rolę stacjonarnej sieci teleinformatycznej oraz wymagania i potrzeby w zakresie usług teleinformatycznych jakie generuje system dowodzenia.

System teleinformatyczny Sił Zbrojnych Rzeczypospolitej Polskiej w przeważającej części zbudowany jest na bazie zasobów operatorów publicznych, mówiąc krótko Siły Zbrojne dzierżawią zasoby teletransmisyjne. W związku z tym

---

[1] **Usługa telekomunikacyjna** to termin prawniczy, którego definicja zawarta jest w ustawie z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne*. Wg tej definicji usługa telekomunikacyjna to usługa polegająca głównie na przekazywaniu ***sygnałów*** w ***sieci telekomunikacyjnej***. ***Sygnał*** w tym przypadku traktowany jest jako nośnik informacji na dowolne odległości. Natomiast ***sieć telekomunikacyjna*** to zgodnie z w/w ustawą termin oznaczający systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju.

większość przedsięwzięć powinny być realizowane przez operatorów w celu przygotowania własnej infrastruktury w taki sposób, ażeby w zależności od zaistniałej sytuacji w najpewniejszy i elastyczny sposób mogła dostosować się do potrzeb dowodzenia w czasie pokoju, kryzysu oraz zagrożenia militarnego. Problematyką regulacji ustawowych z operatorami komercyjnymi oraz opisem zmian organizacyjno – technicznych w obszarze stacjonarnej sieci teleinformatycznej Sił Zbrojnych, podjętych w latach 1995 – 2005 autor opisał w rozdziale 3.

W miarę rozwoju systemów teleinformatycznych znacznie wzrasta zagrożenie atakami fizycznymi oraz atakami w tzw. cyberprzestrzeni i dlatego musimy podejmować szereg przedsięwzięć, które powinniśmy zrealizować aby zabezpieczać się przed groźnymi skutkami uszkodzenia systemu teleinformatycznego. Problematykę bezpieczeństwa systemu teleinformatycznego autor opisał się w rozdziale 4.

W kolejnym bloku zagadnieniowym zidentyfikowano dostępne urządzenia i technologie teleinformatyczne oraz określono możliwości zastosowania ich w stacjonarnej sieci teleinformatycznej, aby mogły sprawniej spełniać stawiane przed nią zadania łączności.

Techniki zarządzania i sterowania siecią przynoszą operatorom korzyści handlowe w czasie pokoju, ale podczas wojny i w sytuacjach kryzysowych będą miały zasadnicze znaczenie dla zachowania ciągłości świadczenia usług telekomunikacyjnych. Z tego powodu należy wymagać od operatorów sieci publicznych, aby ich Centra Zarządzania Siecią (NMC – Network Management Centre) były czynne bez przerwy i pożądane jest umiejscowienie ich w chronionych obiektach oddalonych od potencjalnych obszarów ataków. Łącza pomiędzy NMC i węzłami sieci powinny być bardzo niezawodne.

Rozprawę kończy rozdział 6., w którym na bazie przedstawionych powyżej wniosków wypracowano koncepcję struktury organizacyjno – technicznej stacjonarnej sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej.

1. ZAŁOŻENIA METODOLOGICZNE

1.1 Uzasadnienie wyboru tematu

Wstąpienie Polski do Organizacji Traktu Północnoatlantyckiego spowodowało zmiany charakteru działań Sił Zbrojnych Rzeczypospolitej Polskiej na zadania wewnątrz „narodowe" i zewnętrzne. Z drugiej strony, w ujęciu globalnym rewolucyjne zmiany w technologii łączności i informatyki wymuszają ewolucję podejścia do sposobu planowania i organizacji stacjonarnych systemów teleinformatycznych dla potrzeb Sił Zbrojnych Rzeczypospolitej Polskiej. Proces planowania tak złożonej struktury jaką jest sieć teleinformatyczna w warunkach stałego, dynamicznego rozwoju i zastosowań zaawansowanych technologii telekomunikacyjnych oraz nowoczesnych usług zintegrowanych, jest przedsięwzięciem o wysokim stopniu komplikacji, którego prawidłowy, optymalizowany rozwój wymaga spełnienia szeregu uwarunkowań o charakterze interdyscyplinarnym oraz stosowania nowoczesnej metodologii jako narzędzia wspomagającego. Prace badawczo-rozwojowe w dziedzinie metodologii opartej na bazie wspomagających systemów komputerowych, do planowania rozwoju sieci telekomunikacyjnych, powinny mieć charakter ciągły. Wynika to przede wszystkim z ciągłości procesu rozwoju struktury sieci, związanych z tym wprowadzanych nowych technologii i usług, w warunkach stale rosnącej konkurencji na scenie krajowego i globalnego rynku telekomunikacyjnego. W rozwijającej się gamie różnorodnych sieci i nowych usług postępuje proces integracji, w jedną cyfrową sieć teleinformatyczną, a następnie wraz ze wzrostem wymagań na świadczenie szerokopasmowych usług multimedialnych. Postępuje coraz wyraźniej proces zbieżności telekomunikacji, informatyki oraz telewizji. Światowa sieć telekomunikacyjna przechodzi ewolucję w kierunku sieci zintegrowanych, przed którą stoją coraz wyższe wymagania transportowania ogromnej ilości danych ze wzrastającą prędkością. Na rynku krajowym zanika uprzywilejowana pozycja operatora monopolistycznego, przechodząc do roli operatora dominującego w otoczeniu nowych operatorów. Pojawia się nowy scenariusz w którym uczestniczy wzrastająca liczba rywalizujących operatorów, dostawców usług, użytkowników oraz firm dostarczających nowoczesne urządzenia i technologie. W takich nowych uwarunkowaniach liberalizacji i rosnącej konkurencji, operatorzy sieci teleinformatycznych coraz bardziej zainteresowani są

rozwojem i wprowadzaniem nowoczesnych metodologii planowania działających w oparciu o nowoczesne techniki systemowego wspomagania decyzji.

Rozszerzający się obszar odpowiedzialności oraz dynamiczny rozwój środków i sposobów walki, skłania mnie do stwierdzenia, że dla zapewnienia pełnego obiegu informacji w procesie dowodzenia wojskami, stacjonarna sieć teleinformatyczna musi osiągnąć zdolność dynamicznej organizacji systemów dowodzenia, w dowolnym miejscu kraju i realnym czasie wynikającym z potrzeb procesu dowodzenia. Prawidłowy rozwój coraz bardziej złożonej struktury sieci jest procesem kompleksowym, wymagającym wprowadzenia całej gamy stale udoskonalonych komputerowych narzędzi wspomagających modelowanie systemów teleinformatycznych tj. topologii, kierowania rozpływem ruchu, jakości usług i niezawodności. Rozwój sieci w warunkach działania operatora monopolistycznego jest rozwojem ilościowym, przy zaniedbaniu właściwego rozwoju jakościowego uwzględniającego możliwości optymalizacji. Brak możliwości porównawczych eliminuje skuteczne oddziaływanie użytkowników na operatorów.

Dynamiczny rozwój łączności w latach 90. w Siłach Zbrojnych Rzeczypospolitej Polskiej, przebiegał pod nadzorem i przy współpracy jedynego operatora na polskim rynku TP S.A. i dlatego zabrakło elementu opisywanego wcześniej jakim jest jakość. Wszelkiego rodzaju łącza analogowe były zastępowane łączami cyfrowymi o maksymalnej szybkości 2 Mbit/s. Tak budowana sieć teletransmisyjna nie spełnia podstawowych wymagań. Tradycyjne metody projektowania i planowania sieci wymagają rewizji i uaktualnienia, ponieważ stają się nieadekwatne w stale zmieniających się uwarunkowaniach. Nowoczesne sieci teleinformatyczne, różnią się zasadniczo od sieci analogowych, gdyż charakteryzują się między innymi: cyfrowymi urządzeniami transmisyjnymi o dużej szybkości transmisji i modularności przepustowości, rekonfiguracją strumieni cyfrowych, cyfrowym polem komutacyjnym czyli pełną automatykę pozwalającą na zabezpieczenie wymagań pod dedykowane nowoczesne usługi takie jak ISDN, IP oraz multimedialne. Pojawiający się inni operatorzy telekomunikacyjni w Siłach Zbrojnych, powodują zmianę uwarunkowań pod kątem rozwoju metodologii i związanych z nią narządzi do wspomagania planowania sieci. Jest to proces ciągły, podobnie jak ciągły proces rozwoju samej sieci teleinformatycznej. Coraz większą rolę odgrywa telekomunikacja ruchoma i bezprzewodowa, zajmując znaczącą pozycję w obszarze organizacji sieci teleinformatycznych. Techniczne systemy teleinformatyczne jako składnik systemu

dowodzenia powinny składać się z komponentów środków stacjonarnych jak i środków wysoce mobilnych.

Doktryna wojny sieciocentrycznej stawia olbrzymie wymagania dla sieci teletransmisyjnej na potrzeby dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej kładąc nacisk na umożliwienie dostępu stanowisk dowodzenia do pozyskiwania danych, szybkiego ich przetwarzania i wykorzystania w procesach decyzyjnych.

Do realizacji zmian związanych z budową sieciocentrycznego systemu Sił Zbrojnych niezbędne są zmiany w strukturach: planistycznych, organizacyjnych i wykonawczych, mających na celu efektywne wykonywanie zamierzeń, określenie kompetencyjności a także metod działania. Wydaje się nieodzowne przeprowadzenie w najbliższym czasie kilku zmian na płaszczyźnie organizacyjno - technicznej:

- uruchomienie szkieletowej sieci teleinformatycznej pomiędzy węzłami regionalnymi;
- uruchomienie wojskowego systemu satelitarnego obejmującego elementy stacjonarne i mobilne;
- modernizacja dowiązań operatorów publicznych do sieci resortowej Obrony Narodowej na terenie całego kraju;
- wprowadzenie szerokopasmowych urządzeń radioliniowych jako rozwiązań typu back-up dla sieci ;
- wprowadzenie do szerokiej eksploatacji urządzeń szyfrowych na bazie protokołu IP (ochrona kryptograficzna sieci informatycznych: MILWAN, SEC-WAN).

W tej sytuacji, uwzględniając moje dotychczasowe doświadczenia zawodowe i pojawiającą się potrzebę zmian w organizacji stacjonarnych systemów i sieci teleinformatycznych podjąłem się opracowania niniejszej dysertacji w której zamierzam w sposób naukowo uzasadniony określić strukturę organizacyjno – techniczną stacjonarnej sieci teleinformatycznej tak aby mogła zapewnić świadczenie podstawowych usług teleinformatycznych w procesie dowodzenia Siłami Zbrojnymi.

1.2 Przedmiot badań, cel badań, problemy badawcze

Przedmiotem badań jest stacjonarna sieć teleinformatyczna Sił Zbrojnych Rzeczypospolitej Polskie. Zasadniczym celem jest: ***wypracowanie, naukowo uzasadnionej, struktury organizacyjno – technicznej stacjonarnej sieci teleinformatycznej niezbędnej do zabezpieczenia procesu dowodzenia siłami zbrojnymi w okresie pokoju, kryzysu i zagrożenia militarnego państwa. Następnie na podstawie uzyskanych wyników badań określić, jakie należy podjąć niezbędne działania techniczno - organizacyjne, w celu osiągnięcia pełnej zdolności części stacjonarnej sieci teleinformatycznej do organizacji i eksploatacji wszystkich klas sieci na potrzeby dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej.***

Założony cel dysertacji planuje się osiągnąć poprzez realizację następujących celów cząstkowych:

1. Określenie podstawowych potrzeb organów dowodzenia wojskami na usługi teleinformatyczne.
2. Identyfikacja elementów struktury organizacyjno-technicznej sieci teleinformatycznej, użytkowanej przez Siły Zbrojne Rzeczypospolitej Polskiej na terenie kraju, i ich ocenę pod kątem spełnienia przez nią wymagań wynikających z potrzeb procesu dowodzenia wojskami Rzeczypospolitej Polskiej podczas pokoju, kryzysu i zagrożenia militarnego państwa;
3. Identyfikacja potrzeb przeprowadzenia niezbędnych zmian w obszarze organizacyjno-technicznym sieci teleinformatycznej w celu zabezpieczenia procesu dowodzenia w czasie pokoju, kryzysu i zagrożenia militarnego państwa;
4. Wypracowanie, na bazie uzyskanych wyników badań, autorskiej koncepcji struktury organizacyjno – technicznej stacjonarnej sieci teleinformatycznej, zapewniającej realizację zadań łączności dla potrzeb dowodzenia wojskami w czasie pokoju, kryzysu i zagrożenia militarnego państwa.

Przyjęty cel rozprawy wymaga rozwiązania zasadniczego problemu badawczego, zawierającego się w pytaniu:

Czy obecna struktura organizacyjno – techniczna stacjonarnej sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej, zabezpiecza świadczenie usług teleinformatycznych na potrzeby wynikające z procesu

dowodzenia wojskami w czasie pokoju, kryzysu i zagrożenia militarnego państwa, a jeżeli nie, to jaka powinna ona być?

W celu uszczegółowienia założenia zawartego w głównym problemie badawczym wygenerowano problemy cząstkowe w postaci następujących pytań :

1. Jakie wymagania i potrzeby w zakresie usług teleinformatycznych generuje system dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej w czasie pokoju, kryzysu i zagrożenia militarnego państwa ?
2. Jaka jest rola stacjonarnej sieci teleinformatycznej w realizacji zadań łączności w toku dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej ?
3. W jakim stopniu aktualne regulacje ustawowe określają zasady współpracy operatorów telekomunikacyjnych z Siłami Zbrojnymi Rzeczypospolitej Polskiej w czasie pokoju, kryzysu i zagrożenia militarnego państwa ?
4. W jakim stopniu zmiany organizacyjno – techniczne w obszarze stacjonarnej sieci teleinformatycznej Sił Zbrojnych, podjęte w latach 1995 – 2005, wpłynęły na realizację potrzeb w zakresie usług teleinformatycznych generowanych w procesie dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej w czasie pokoju, kryzysu i zagrożenia militarnego państwa ?
5. Jakie zagrożenia i czynniki wpływają lub mogą wpływać na sprawne funkcjonowanie stacjonarnej sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej ?
6. Jakie współczesne urządzenia i technologie teleinformatyczne są możliwe do zastosowania w stacjonarnej sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej aby mogła sprawniej spełniać stawiane przed nią zadania łączności?
7. Jaka powinna być struktura organizacyjno – techniczna stacjonarnej sieci teleinformatycznej aby mogła zapewnić świadczenie podstawowych usług teleinformatycznych w procesie dowodzenia Siłami Zbrojnymi ?

1.3 Hipoteza robocza

Na podstawie posiadanej wiedzy uzyskanej na podstawie wyników z wstępnego etapu badań i dotychczasowego doświadczenia zawodowego mogłem stwierdzić, ***że aktualny stan sieci teleinformatycznej użytkowanej przez Siły Zbrojne Rzeczypospolitej Polskiej nie w pełni zabezpiecza potrzebę świadczenia***

określonych usług teleinformatycznych niezbędnych do dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej w warunkach pokoju, kryzysu i zagrożenia militarnego państwa. Uważam, że zasadniczą przyczynę takiego stanu rzeczy powodują uwarunkowania związane z szybkimi zmianami technologicznymi systemu, które w wielu wypadkach odbiegają od potrzeb uzyskania zdolności sieciocentrycznych i komercyjnych uwarunkowań krajowego rynku telekomunikacyjnego, co automatycznie przekłada się na wystąpienie licznych niedostatków – tak organizacyjnych, jak i technicznych.

Dotychczasowe treści poznawcze – zebrane z przedmiotowego obszaru badań – wskazują, że pozytywnego rozwiązania należy upatrywać w szkieletowej infrastrukturze dostosowanej funkcjonalnie i przestrzennie do uruchomienia sieci synchronicznych typu SDH (ang. Synchronous Digital Hierarchy), zapewniających skalowalność w każdej warstwie zwielokrotnienia, jak również fakt, że aktualne regulacje ustawowe o obowiązkach operatorów łączności i przedsiębiorców telekomunikacyjnych w zakresie działań na rzecz obronności i bezpieczeństwa państwa, pozwalają na zastosowanie takiego rozwiązania[2]. Tym samym stwarza to szanse na pozytywny przebieg negocjacji resortowo – komercyjnych, pomiędzy przedstawicielami wojska i istniejącymi prawnie krajowymi usługodawcami dostaw teleinformatycznych.

1.4 Metody i techniki badawcze

W trakcie rozwiązywania problemów badawczych i weryfikacji przyjętej hipotezy roboczej zastosowałem szereg metod badawczych, zarówno empirycznych, jak i teoretycznych.

Podczas realizacji procesu badań naukowych zastosowałem poniższe metody empiryczne:

- ***obserwacji biernej;***
- ***obserwacji uczestniczącej;***
- ***badań opinii ekspertów.***

Metoda ***obserwacji*** zarówno biernej jak i uczestniczącej umożliwiła mi uzyskanie niezbędnych informacji charakteryzujących stan techniczno – organizacyjny stacjonarnej sieci teleinformatycznej, użytkowanej przez Siły Zbrojne

[2] Rozporządzenie Rady Ministrów z dnia 20 sierpnia 2004 r. w sprawie wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo – obronnym (Dz. U. z 2004 r., nr 192, poz. 1965).

Rzeczypospolitej Polskiej oraz identyfikację kierunków rozwoju sieci teleinformatycznych, głównych, kluczowych operatorów telekomunikacyjnych mających strategiczne znaczenie dla obronności i bezpieczeństwa państwa takich jak TPSA, EXATEL.

Reasumując, zastosowanie metod empirycznych zapewniło pozyskanie niezbędnej informacji i wiedzy oraz przyczyniło się do:

- określenia struktury organizacyjno – techniczne sieci teleinformatycznej użytkowanej przez Siły Zbrojne Rzeczypospolitej Polskiej na terenie kraju;
- precyzyjnego określenia wymagań oraz jakości sieci teleinformatycznej użytkowanej przez Siły Zbrojne Rzeczypospolitej Polskiej na terenie kraju;
- ustalenia przedsięwzięć organizacyjno – technicznych eliminujących zdefiniowane czynniki wpływające na jakość sieci teleinformatycznej użytkowanej przez Siły Zbrojne Rzeczypospolitej Polskiej w zależności od realizowanych zadań łączności;
- określenia potencjalnych kierunków rozwoju sieci teleinformatycznych wynikających z potrzeb dowodzenia oraz związanych z tym przedsięwzięć organizacyjno – technicznych w zakresie zapewnienia wysokiej jakości.

W procesie badawczym zastosowałem również metody teoretyczne, jak: ***analizę***, ***syntezę***, ***abstrahowanie***, ***porównanie***, ***uogólnienie*** oraz ***wnioskowanie***.

Zastosowałem również **analizę i ocenę literatury** przedmiotu, ze szczególnym uwzględnieniem opracowań dotyczących aspektów prawnych, regulujących sprawy związane z przygotowaniem i wykorzystaniem sieci teleinformatycznych, oraz identyfikację możliwości sieci głównych przedsiębiorstw telekomunikacyjnych, mających strategiczne znaczenie dla obronności państwa, na bazie których, można zaprojektować sieć teleinformatyczną na potrzeby dowodzenia wojskami Sił Zbrojnych Rzeczypospolitej Polskiej.

Pierwszy i drugi szczegółowy problem badawczy, opisany w drugim rozdziale, rozwiązuję metodą obserwacji biernej (pośredniej) i uczestniczącej (bezpośredniej) oraz techniką analizy dokumentów, co umożliwiło zebranie niezbędnego materiału badawczego. Następnie stosując metody teoretyczne: uogólnienie, analizę i syntezę, dokonałem identyfikacji struktury organizacyjnej systemu dowodzenia Sił Zbrojnych Rzeczypospolitej Polskiej. Powyższe techniki pozwoliły na pełną analizę i ocenę aktualnego stanu sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej.

W rozdziale trzecim zajmuję się rozwiązywaniem trzeciego i czwartego szczegółowego problemu badawczego, gdzie zastosowałem oprócz metod teoretycznych: uogólnienia, analizy, syntezy, porównania również sondaż diagnostyczny techniką obserwacji pośredniej. Powyższe podejście metodologiczne pozwoliło na identyfikację elementów struktury organizacyjno – technicznej użytkowanej przez Siły Zbrojne Rzeczypospolitej Polskiej, na terenie kraju pod kątem spełniania przez nią potrzeb w procesie dowodzenia wojskami podczas pokoju, kryzysu i zagrożenia militarnego państwa. Analizie poddano także organizację struktur instytucji resortu obrony narodowej, które w swoich zakresach działań mają zapisane zadania związane z pełnieniem obowiązków organizatora wojskowego systemu teleinformatycznego.

Dla rozwiązania piątego problemu szczegółowego, w czwartym rozdziale zastosowałem badania metodą opinii ekspertów, która posłużyła do zgromadzenia nieodzownego materiału badawczego. Analiza i synteza pozwoliły na konsolidacje wyników badań. Natomiast wnioskowanie, abstrahowanie oraz uogólnienie, umożliwiło określenie najistotniejszych czynników mających bezpośredni lub pośredni wpływ na bezpieczeństwo sieci teleinformatycznej sił zbrojnych.

Szósty szczegółowy problem badawczy rozwiązuję metodami: analizy, syntezy, abstrahowania, porównania, uogólnienia oraz wnioskowania, które poprzedzone techniką analizy dokumentów, umożliwiły określenie współczesnych urządzeń i technologii teleinformatycznych możliwych do zastosowania w stacjonarnej sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej organów dowodzenia wojskami, w celu sprawniejszego spełniania stawianych przed nią zadań łączności.

Kolejny szczegółowy problemy badawcze: jaka powinna być struktura organizacyjno - techniczna sieci teleinformatycznej aby mogła zapewnić potrzeby w zakresie łączności, wynikające z procesu dowodzenia Siłami Zbrojnymi rozpatrywane w rozdziale szóstym, rozwiązuję stosując badania metodą analizy, syntezy, uogólnienia, analizy dokumentów oraz badania metodą opinii ekspertów. Dokonując porównania wyników przeprowadzonych badań teoretycznych oraz empirycznych przedstawiam autorską koncepcję założeń na struktury organizacyjno – technicznej stacjonarnej sieci teleinformatycznej taką aby mogła zapewnić świadczenie podstawowych usług teleinformatycznych w procesie dowodzenia Siłami Zbrojnymi.

1.5 Przebieg badań

W celu wypracowania naukowo uzasadnionej koncepcji, struktury organizacyjno-technicznej sieci teleinformatycznej, zapewniającej realizację zadań łączności dla potrzeb dowodzenia wojskami w poszczególnych fazach konfliktu, koniecznym było zebranie wielu faktów, których poznanie było możliwe dzięki metodzie ***badań opinii ekspertów***. Jako typową metodę badania sądów, zastosowałem wywiad ekspertów. Metodą tą, objąłem wybranych przedstawicieli Generalnego Zarządu Dowodzenia i Łączności P-6 , Departamentu Informatyki i Telekomunikacji, Centrum Zarządzania Systemami Teleinformatycznych, Dowództwa Garnizonu Warszawa oraz Centralnego Węzła Łączności Ministerstwa Obrony Narodowej, którzy zajmują się planowaniem i organizacją sieci teleinformatycznych na potrzeby dowodzenia wojskami, jak również wytypowanych Szefów Węzłów Łączności, którzy posiadają doświadczenia, we współpracy sprzętu mobilnego ze stacjonarnymi sieciami teleinformatycznymi. Metoda badania sądów umożliwiła weryfikację obserwacji bezpośredniej oraz posłuży do określenia organizacyjnych i technicznych aspektów badanej sieci teleinformatycznej. Zakłada się zatem, że powyższa grupa specjalistów z dziedziny łączności, składająca się ze wskazanych powyżej przedstawicieli, posiada niezbędną wiedzę z obszaru resortowych rozwiązań teleinformatycznych.

Przyjmuję, że informacje uzyskane za pomocą badań sondażowych, odzwierciedlają faktyczny stan, jak również niezbędne potrzeby systemu dowodzenia w zakresie świadczenia usług teleinformatycznych.

Na potrzeby identyfikacji funkcjonalności stacjonarnej sieci teleinformatycznej, obecnie eksploatowanej przez siły zbrojne, wynikającej z przebiegu procesu dowodzenia, przyjmuję jako reprezentatywne, poddanie badaniom empirycznym metodą obserwacji biernej i uczestniczącej topologii sieci teleinformatycznej oraz generowanego ruchu w relacjach lokalnych oraz międzygarnizonowych.

Ze względu na konieczność budowania Węzłów Łączności poszczególnych strategicznych stanowisk dowodzenia na bazie stacjonarnej sieci teleinformatycznej sił zbrojnych, przy pomocy istniejących mobilnych środków teleinformatycznych oraz użytkowania niezbędnych Zintegrowanych Systemów Dowodzenia, określiłem przepływność sieci. Jednocześnie po dokonanej w roku 2007 restrukturyzacji Garnizonowych Węzłów Łączności oraz utworzeniu Regionalnych Węzłów

Łączności, wskazałem przebieg projektowanej sieci teleinformatycznej, bazując na kluczowych operatorach publicznych.

Wspomniana wyżej metoda została również wykorzystana w celu identyfikacji urządzeń i środków stacjonarnego systemu teleinformatycznego, które można wykorzystać opracowując koncepcję struktury organizacyjno-technicznej stacjonarnej sieci teleinformatycznej dla potrzeb systemu dowodzenia w czasie pokoju, kryzysu i zagrożenia militarnego państwa.

Zastosowanie przedstawionych w podrozdziale 1.4 metod teoretycznych w procesie badań naukowych, pozwoliło na skonsumowanie danych uzyskanych za pomocą badań empirycznych.

Efektem finalnym scharakteryzowanego procesu naukowo – badawczego jest autorska koncepcja struktury organizacyjno-technicznej sieci teleinformatycznej, zapewniająca realizację świadczenia podstawowych usług teleinformatycznych w procesie dowodzenia wojskami w czasie pokoju, kryzysu i zagrożenia militarnego państwa.

2. WIĘZI INFORMACYJNE SYSTEMU DOWODZENIA SIŁ ZBROJNYCH RZECZYPOSPOLITEJ POLSKIEJ GENERUJĄCE POTRZEBY NA USŁUGI TELEINFORMATYCZNE

Celem badań, których wyniki przedstawiono w tym rozdziale, jest próba odpowiedzi na pytania ***jakie wymagania i potrzeby w zakresie usług teleinformatycznych generuje system dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej w czasie pokoju, kryzysu i zagrożenia militarnego państwa oraz jaka jest rola stacjonarnej sieci teleinformatycznej w realizacji zadań łączności w toku dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej ?***

Aby osiągnąć tak sformułowany cel, autor dokonał szczegółowej analizy podstawowych potrzeb teleinformatycznych organów dowodzenia wojskami w celu zabezpieczenia procesu dowodzenia w czasie pokoju, kryzysu i zagrożenia militarnego państwa. Dokonał także analizy literatury przedmiotu i aktów prawnych (wykaz dokumentów formalno – prawnych – **zał. 2**) regulujących zagadnienia związane ze sposobem organizacji, wykorzystywania i utrzymania sieci teleinformatycznej.

2.1 System obronności Rzeczypospolitej Polskiej

Wszystkie działania na rzecz pokoju militarne i pozamilitarne zgodnie ze „Strategią Bezpieczeństwa..." nazywamy Systemem obronności Rzeczypospolitej Polskiej.

Są to wszystkie siły i środki przeznaczone do realizacji zadań obronnych, odpowiednio przygotowane do realizacji tych zadań[3]. „Zasadniczym elementem obrony narodowej są Siły Zbrojne Rzeczypospolitej Polskiej. Ich podstawowym zadaniem jest zapewnienie zdolności państwa do obrony oraz utrzymywanie gotowości do przeciwstawienia się agresji w ramach zobowiązań sojuszniczych. Polska będzie rozwijać zdolności bojowe sił zbrojnych dla zapewnienia skutecznej obrony i ochrony polskich granic w ramach działań prowadzonych samodzielnie oraz w ramach obrony kolektywnej, jak również poza jej granicami, zgodnie z artykułem V Traktatu Waszyngtońskiego. Siły Zbrojne Rzeczypospolitej Polskiej będą utrzymywały gotowość do udziału w działaniach o charakterze asymetrycznym,

[3] *Strategia obronności Rzeczypospolitej Polskiej,* Warszawa 2003 r.

w tym w wielonarodowych, połączonych operacjach zwalczania terroryzmu, prowadzonych zgodnie z prawem międzynarodowym, organizowanych przez NATO, UE lub doraźną koalicje państw".[4]

Siły Zbrojne Rzeczypospolitej Polskiej są przygotowane do wykonywania trzech rodzajów zadań strategicznych: ***zadań stabilizacyjnych i prewencyjnych w czasie pokoju***, ***zadań reagowania kryzysowego oraz zadań obronnych w razie wojny***. Ponadto są gotowe do udziału w reagowaniu na zagrożenia pozamilitarne. Siły Zbrojne Rzeczypospolitej Polskiej przygotowywane są zarówno do wykonywania zadań w ramach obrony kolektywnej NATO, jak i zadań reagowania kryzysowego. We wszystkich rodzajach Sił Zbrojnych utrzymywane będą wojska o wysokim stopniu gotowości do działania (wojska gotowości operacyjnej) zdolne do reagowania na każdy rodzaj zagrożeń zwłaszcza na terytorium Rzeczypospolitej Polskiej oraz wojska o zróżnicowanym stopniu gotowości bojowej (w tym gotowości mobilizacyjnej), przeznaczone do wspierania i kontynuowania już prowadzonych operacji. Obronność państwa to jeden z celów strategicznych, do którego wykorzystywane są najistotniejsze instrumenty i działania polityczne, gospodarcze, wojskowe i dyplomatyczne aby zapewnić szybkie i sprawne działanie w każdych warunkach oraz w reakcji na wszelkiego typu zagrożenia i kryzysy. Zgodnie ze „Strategią Obronności Rzeczypospolitej Polskiej" oraz dokumentem doktrynalnym „Doktryna Szkolna SZ RP" (DD/7) system obronności państwa to zbiór uporządkowanych wewnętrznie wzajemnie powiązanych elementów – ludzi, organizacji i urządzeń – działających na rzecz bezpieczeństwa państwa obejmując podsystemy :

1) podsystem kierowania;
2) podsystem – militarny (Siły Zbrojne Rzeczypospolitej Polskiej);
3) podsystem pozamilitarny (pozamilitarne ogniwa obronne).

Strukturę systemu obronnego państwa przedstawia rys. 2.1.

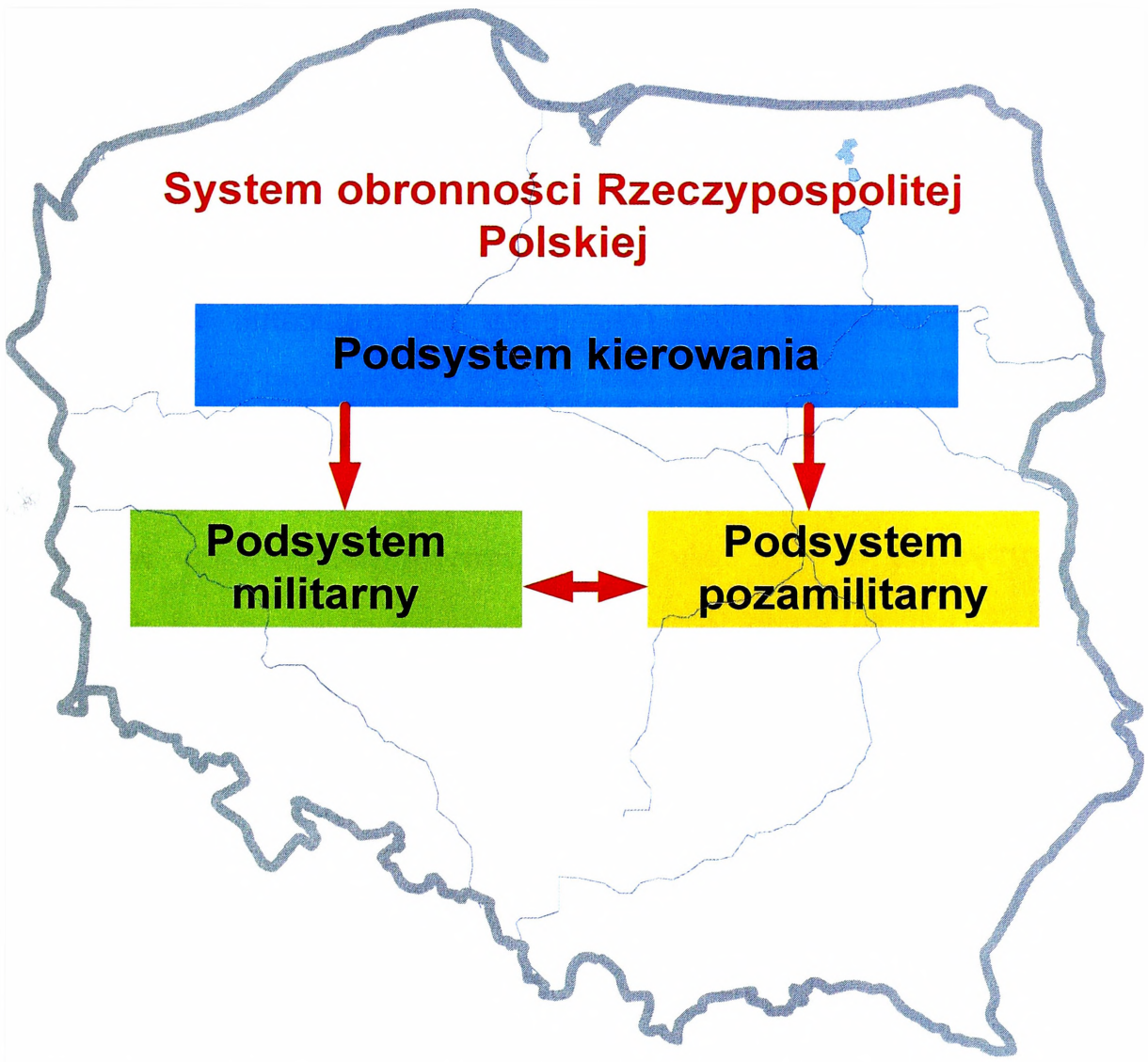
System obronności państwa funkcjonuje głównie na narodowym potencjale obronnym dysponując odpowiednimi siłami i środkami do realizacji niezbędnych zadań z dziedziny obronności oraz właściwego przygotowania **infrastruktury zabezpieczającej** jego funkcjonowanie. Istotą systemu obronności państwa, jest

---

[4] „Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej" Warszawa 2007

wykorzystanie całego posiadanego potencjału militarnego i niemilitarnego kraju do przeciwdziałania i ewentualnego odparcia zewnętrznego zagrożenia polityczno – militarnego, kryzysu i wojny, aby realizować działania, umacniające bezpieczeństwo państwa i jego obywateli oraz polepszać warunki rozwoju społeczeństwa. Należą do nich w szczególności[5]:

1) wzmacnianie suwerenności politycznej i ekonomicznej Polski;



Rys. 2.1 *Struktura systemu obronności Rzeczypospolitej Polskiej*

Źródło: Opracowanie własne: na podstawie„Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej"

2) zapewnienie wzrostu dobrobytu społeczeństwa i poprawy jakości życia obywateli;
3) unowocześnienie sił zbrojnych i rozwijanie ich zdolności współdziałania z armiami sojuszniczymi;

[5] „Strategia Bezpieczeństwa Narodowego RP" Warszawa 2007

4) umacnianie międzynarodowej pozycji i wizerunku Polski oraz zwiększanie jej udziału w kształtowaniu środowiska międzynarodowego.

2.1.1 Podsystem kierowania

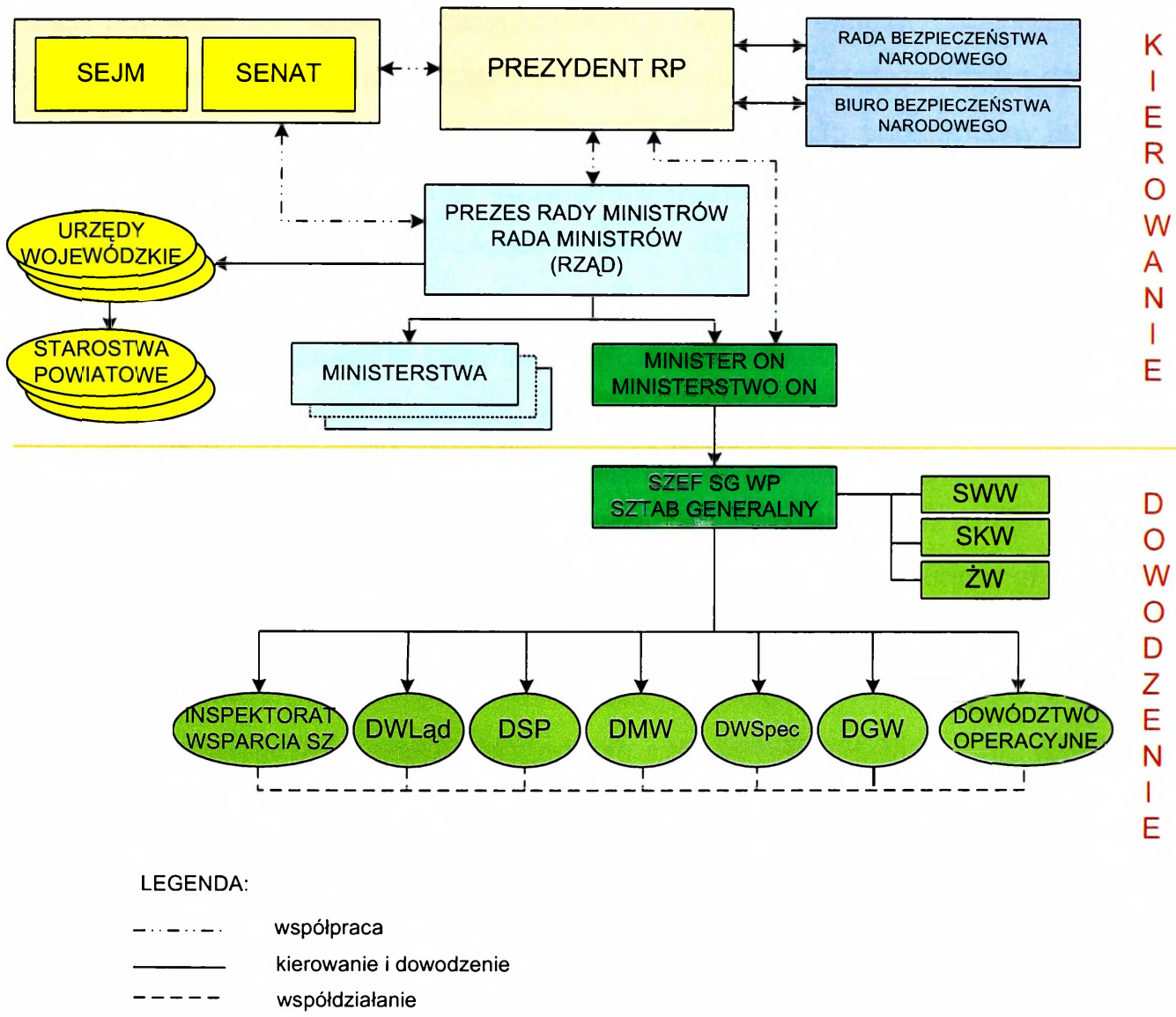
Podsystem kierowania tworzą ***organy władzy publicznej i kierownicy jednostek organizacyjnych***, które wykonują zadania związane z bezpieczeństwem narodowym oraz ***organy dowodzenia Sił Zbrojnych RP***. Naczelnym zadaniem podsystemu kierowania i dowodzenia jest zapewnienie ciągłości podejmowania decyzji i działań w celu utrzymania bezpieczeństwa narodowego. Podsystem kierowania i dowodzenia bezpieczeństwem narodowym realizuje ponadto przedsięwzięcia związane z monitorowaniem źródeł, rodzajów, kierunków i skali zagrożeń; zapobieganiem powstawaniu zagrożeń bezpieczeństwa narodowego na terytorium Rzeczypospolitej Polskiej oraz poza jej granicami; zapobieganiem skutkom tych zagrożeń oraz ich usuwaniem, a także kierowaniem obroną narodową. ***Dla zapewnienia sprawnego przekazu informacji w ramach procesów związanych z kierowaniem bezpieczeństwem narodowym organy władzy rządowej wykorzystują w tym celu miedzy innymi dedykowany wydzielony system łączności, będący w dyspozycji ministra właściwego do spraw wewnętrznych. System ten zapewnia bezpieczną i niezawodną komunikację pomiędzy podmiotami realizującymi zadania w zakresie kierowania bezpieczeństwem narodowym.***

Szczególna rola w kierowaniu bezpieczeństwem narodowym przypada Parlamentowi, Prezydentowi Rzeczypospolitej Polskiej i Radzie Ministrów. Prezydent Rzeczypospolitej Polskiej i Rada Ministrów - jako organy sprawujące władzę wykonawczą - są naczelnymi organami kierowania obronnością i wykonują swoje zadania w tym zakresie na podstawie Konstytucji Rzeczypospolitej Polskiej i innych ustaw. Zgodnie z Konstytucją[6] Rzeczypospolitej Polskiej, Prezydent stoi na straży suwerenności i bezpieczeństwa państwa oraz nienaruszalności i niepodzielności jego terytorium. Jest on też Najwyższym Zwierzchnikiem Sił Zbrojnych Rzeczypospolitej Polskiej. Jego organem doradczym w zakresie bezpieczeństwa wewnętrznego i zewnętrznego jest Rada Bezpieczeństwa

---

[6] Prezydent RP powołuje Radę Bezpieczeństwa Narodowego na podstawie § 2 ust. 2 Tymczasowego regulaminu Biura Bezpieczeństwa Narodowego – załącznika do Zarządzenia Nr 4 Prezydenta RP z dnia 29 września 2006 r. w sprawie organizacji oraz zakresu działania Biura Bezpieczeństwa Narodowego.

Narodowego. Rada Ministrów prowadzi politykę wewnętrzną i zagraniczną Rzeczypospolitej Polskiej, zapewnia jej bezpieczeństwo wewnętrzne i zewnętrzne oraz sprawuje ogólne kierownictwo w dziedzinie obronności.



Rys. 2.2 *Struktura systemu kierowania i dowodzenia „P”*

Źródło: Opracowanie własne: na podstawie „Strategii Bezpieczeństwa Narodowego RP”

Przedstawiona struktura systemu kierowania (rys. 2.2) jest nierozerwalną częścią składową Systemu Obronnego Rzeczypospolitej Polskiej. Na terytorium Rzeczypospolitej Polskiej zarządzanie kryzysowe sprawuje Rada Ministrów, a w przypadkach niecierpiących zwłoki zarządzanie kryzysowe sprawuje minister właściwy do spraw wewnętrznych, zawiadamiając niezwłocznie o swoich działaniach Prezesa Rady Ministrów, po czym podjęte decyzje przez ministra właściwego do spraw wewnętrznych podlegają rozpatrzeniu na najbliższym posiedzeniu Rady Ministrów. Organem opiniodawczo-doradczym właściwym w sprawach inicjowania

i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego jest Rządowy Zespół Zarządzania Kryzysowego utworzony przy Radzie Ministrów. W skład Zespołu wchodzą: Prezes Rady Ministrów jako przewodniczący, Minister Obrony Narodowej i minister właściwy do spraw wewnętrznych jako zastępcy przewodniczącego, Minister Spraw Zagranicznych, Minister Koordynator Służb Specjalnych - jeżeli został powołany. W posiedzeniach Zespołu, na prawach członka, biorą udział wyznaczone przez przewodniczącego, w zależności od potrzeb, organy administracji rządowej niezbędne do właściwego w danej sytuacji rozstrzygnięcia sytuacji kryzysowej. Również do prac Zespołu może skierować Prezydent Rzeczypospolitej Polskiej, na prawach członka, Szefa Biura Bezpieczeństwa Narodowego lub innego przedstawiciela. W zależności od potrzeb do danej sytuacji przewodniczący może zapraszać do udziału w posiedzeniach Zespołu, na prawach członka, inne osoby. Prezes Rady Ministrów z własnej inicjatywy, na wniosek właściwego ministra, kierownika urzędu centralnego lub wojewody, może wprowadzić na całym terytorium Rzeczypospolitej Polskiej albo jego części, w drodze zarządzenia, następujący stopień alarmowy. Z chwilą uznania przez władze państwowe, że zaistniała sytuacja kryzysowa, następuje uruchomienie prac planistyczno – wykonawczych, w tym wojskowego systemu planowania antykryzysowego. Sztab Antykryzysowy państwa opracowuje wytyczne dla poszczególnych organów państwowych w formie dyrektywy, w której wyraźnie określa stopień udziału sił zbrojnych.

Sztab Generalny Wojska Polskiego na podstawie dyrektywy władz państwowych planuje działania wojskowe, którego efektem są warianty użycia sił zbrojnych. Kolejnym etapem organów władz państwowych jest wybór działania w sytuacji kryzysowej oraz podjęcie decyzji o rozwiązaniu kryzysu, a w tym decyzji o zaangażowaniu i zadaniach sił zbrojnych. W dalszej kolejności następuje opracowanie planów działania sił zbrojnych. Etap ostatni rozpoczyna się z chwilą wydania rozkazu przez władze państwowe do podjęcia operacji. Rozkaz jest podstawą do uruchomienia przez Sztab Generalny Wojska Polskiego systemu dowodzenia i wykonania zadań antykryzysowych spoczywających na siłach zbrojnych.

W trakcie prowadzonych rozważań można stwierdzić, że ***proces kierowania związany jest nierozerwalnie z Radą Ministrów i podległymi mu centralnymi***

organami administracji rządowej, natomiast proces dowodzenia rozpoczyna się na poziomie Szefa Sztabu Generalnego Wojska Polskiego, podległych mu dowództw i rodzajów sił zbrojnych.

2.1.2 Podsystem pozamilitarny

Podsystem pozamilitarny, przeznaczony jest do realizacji podstawowych funkcji pozamilitarnych ogniw obronnych, należą do nich:

- ochrona ludności i struktur państwa w warunkach zagrożenia bezpieczeństwa państwa (kryzysu) i wojny;
- zapewnianie materialnych, informacyjnych i duchowych podstaw egzystencji ludności w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa (kryzysu) i wojny;
- zasilanie zasobami ludzkimi i materiałowymi Sił Zbrojnych Rzeczypospolitej Polskiej oraz pozamilitarne wsparcie wojsk własnych i sojuszniczych, prowadzących operacje na terytorium Polski.

Wśród ogniw pozamilitarnych występują trzy zasadnicze ogniwa: informacyjne, ochronne i gospodarcze.

Ogniwa informacyjne realizują zadania związane z ochroną i propagowaniem polskich interesów na arenie międzynarodowej, informacyjnym osłabianiem przeciwnika oraz umacnianie woli, morale, determinacji obronnej i wytrwałości własnego społeczeństwa w warunkach wojennych.

Ogniwa ochronne realizują zadania związane z zapewnieniem warunków bezpiecznego funkcjonowania struktur państwa oraz ochroną ludności i majątku narodowego przed skutkami zbrojnych i poza zbrojnych oddziaływań kryzysowych i wojennych.

Ogniwa gospodarcze realizują zadania związane z zapewnieniem materialnych podstaw realizacji zadań obronnych oraz przetrwania ludności w warunkach kryzysu i wojny. Wśród ogniw gospodarczo-obronnych istotne miejsce zajmuje przemysł obronny.

2.1.3. Podsystem militarny

Podsystem militarny zgodnie z treścią zawartą w „Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej" składa się z czterech misji (rys. 2.3).

W ramach każdej misji przewidziano określone zadania, które będą realizowane w różnych stanach gotowości obronnej państwa, w dwóch obszarach:

1) wewnętrznym (terytorium kraju);
2) zewnętrznym (poza jego obszarem).

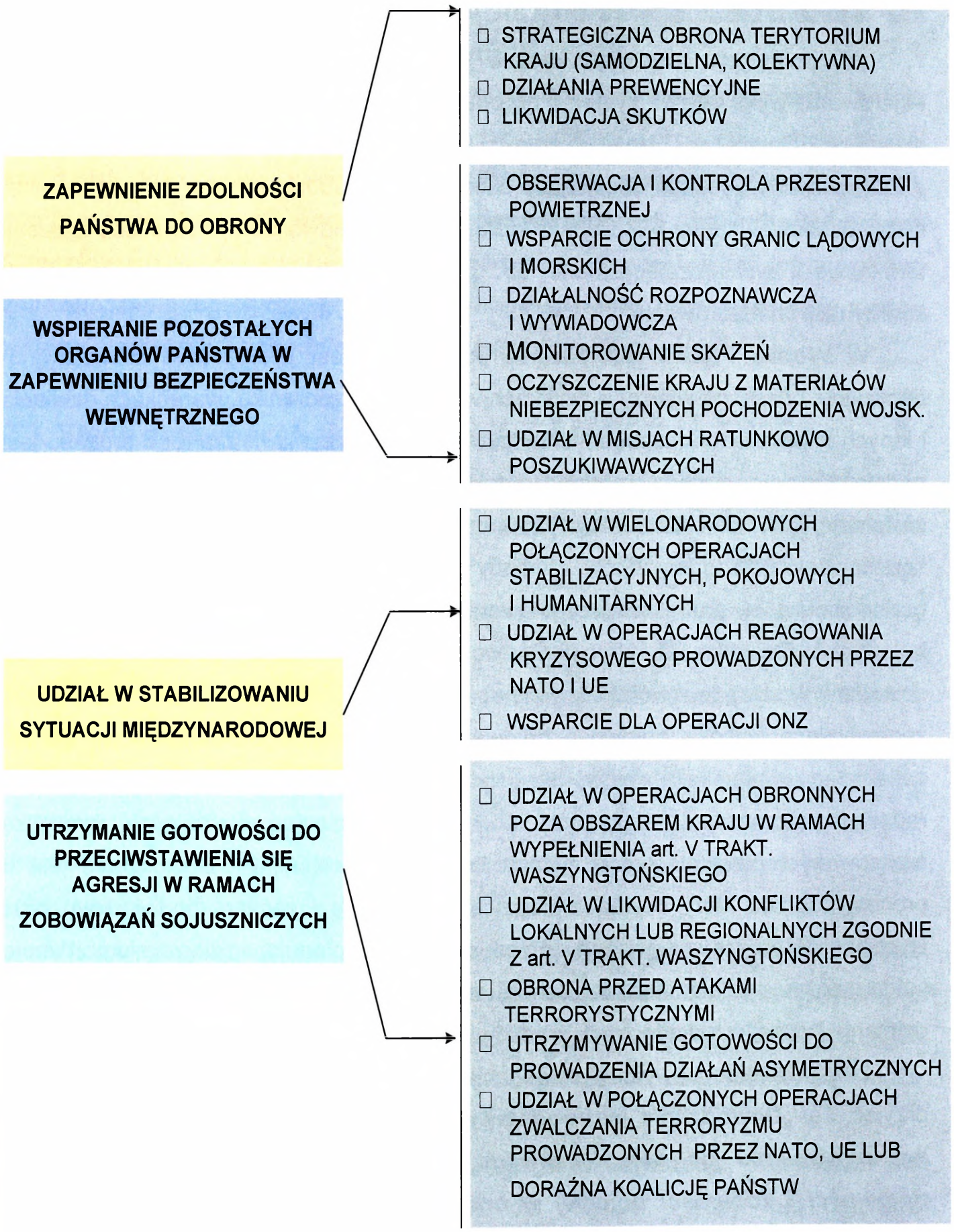
Podsystem militarny, **w czasie pokoju**, zgodnie z zasadą cywilnej i demokratycznej kontroli nad armią – całością Sił Zbrojnych Rzeczypospolitej Polskiej, łącznie z żołnierzami i jednostkami organizacyjnymi wydzielonymi do struktur sojuszniczych, kieruje minister obrony narodowej przy pomocy Ministerstwa Obrony Narodowej.

W razie zaistnienia polityczno-militarnych sytuacji kryzysowych stwarzających pośrednie zagrożenia dla bezpieczeństwa Polski, kierowanie obronnością, odbywać będzie się na ogólnych zasadach. Uruchomione zostaną wtedy jedynie dodatkowe środki i procedury kierowania reagowaniem kryzysowym. Kierowanie siłami zbrojnymi **w czasie kryzysu** odbywa się według zasad kierowania pokojowego, wojskami wydzielonymi do międzynarodowych zgrupowań, wykonujących zadania w ramach reagowania kryzysowego, dowodzi Dowództwo Operacyjnie.

W czasie wojny Siłami Zbrojnymi dowodzi Naczelny Dowódca Sił Zbrojnych Rzeczypospolitej Polskiej[7], mianowany przez Prezydenta Rzeczypospolitej Polskiej na wniosek Prezesa Rady Ministrów. Dla zapewnienia bezkolizyjnego rozwijania Sił Zbrojnych Rzeczypospolitej Polskiej oraz kierowania nimi w czasie wojny utworzony jest **Wojenny System Dowodzenia**. Proces dowodzenia odbywa się w systemie narodowym i sojuszniczym. System narodowy zapewnia pełne dowodzenie siłami nie wydzielonymi do struktur NATO oraz dowodzenie pozaoperacyjne wojskami wydzielonymi do zgrupowań sojuszniczych. Po przekazaniu wojsk operacyjnych dowództwom sojuszniczym dowództwa narodowe nadal odpowiadają za szkolenie rezerw oraz uzupełnienie i wsparcie logistyczne przekazanych wojsk, a także zapewniają warunki do przyjęcia sił wzmocnienia na terytorium kraju. Naczelny Dowódca Sił Zbrojnych dowodzi w pełni siłami zbrojnymi pozostającymi w narodowym podporządkowaniu.

---

[7] Zgodnie z art. 134, pkt 4, Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku.



Rys. 2.3 *Misje i zadania systemu militarnego*

Źródło: Opracowanie własne: na podstawie „Strategii Bezpieczeństwa Narodowego RP"

2.2 System dowodzenia Sił Zbrojnych Rzeczypospolitej Polskiej

Z podjętych rozważań można wywnioskować, że proces dowodzenia i kierowania wynikający z systemu obronnego Rzeczypospolitej Polskiej jest częścią składową ***systemu dowodzenia***, którą można scharakteryzować jako „ Zintegrowany system, obejmujący doktrynę, procedury, struktury organizacyjne, stany osobowe, sprzęt i łączność, która zapewnia dowódcom wszystkich szczebli terminowe i wystarczające dane do: planowania działań, kierowania nimi, ich koordynacji i nadzorowania" [8]

W Wojsku Polskim dowodzenie pojmowane jest jako proces informacyjno-decyzyjny, oparty na wiedzy o wojskach własnych, przeciwniku, warunkach działania i innych informacjach niezbędnych w procesie dowodzenia. Istotą tego procesu jest podejmowanie decyzji do działań. Po dokonaniu analizy literatury przedmiotu można stwierdzić, że dowodzenie wojskami jest to szczególny rodzaj kierowania, sprawowany przez dowódców i sztaby wobec podległych im wojsk, oddziałów, pododdziałów w zakresie przygotowania, zabezpieczenia, prowadzenia działań bojowych[9]. Dowodzenie, kierowanie wojskami – całokształt celowej działalności dowództw i sztabów realizowanych w ramach określonego systemu kierowania, zapewniającą wysoką gotowość bojową i właściwe przegotowanie wojsk do jak najlepszego osiągnięcia celów, bitwy lub operacji. Dowodzenie jest szczególnym rodzajem kierowania ze względu na strukturę organizacyjną sił zbrojnych i specyfikę realizowanych przez nie zadań, zwłaszcza w warunkach wojny[10]. Dowodzenie jest to proces, poprzez który dowódca narzuca swoją wolę i zamiary podwładnym oraz w ramach którego wspomagany przez swój sztab planuje organizuje, koordynuje i ukierunkowuje działania podległych mu wojsk przez użycie standardowych procedur działania i wszelkich dostępnych środków przekazywania informacji.[11]

Uwzględniając powyższe dywagacje i przedstawione różne definicje, można przyjąć, że: ***„Dowodzenie jest podstawową formą kierowania wojskami, opartą na uprawnieniu do kompleksowego kształtowania wszystkich elementów gotowości i zdolności bojowej w odniesieniu do bezpośrednio i pośrednio podległych żołnierzy, a więc wszechstronnego przygotowywania ich w czasie***

---

[8] NATO GLOSSARY AAP-6
[9] Psychologia walki i Dowodzenia J. Cendrowski, S. Swebocki wyd. 1973
[10] Leksykon wiedzy wojskowej
[11] Definicja prof. Józefa Michniaka, „ Dowodzenia i Łączność" Warszawa 2005

pokoju do wszelkiego rodzaju działań i do kierowania nimi podczas ich realizacji w okresie pokoju, kryzysu i wojny"[12].

Reasumując powyższe można stwierdzić, że ***„System dowodzenia jest to zespół elementów zorganizowanych w postaci organów dowodzenia, stanowisk dowodzenia, sieci telekomunikacyjnych, sieci teleinformatycznych, stacji i samodzielnych urządzeń telekomunikacyjnych, teleinformatycznych i pocztowych sprzężonych relacjami dowodzenia wraz z całą infrastrukturą zabezpieczenia logistycznego i operacyjnego systemu, współpracujący z sobą według przyjętych i uzgodnionych wcześniej zasad i wymagań"[13].***

2.3 Stany gotowości bojowej i kryzysowej

Stosownie do ***stanów gotowości obronnej*** państwa na podstawie Rozporządzenia Rady Ministrów w sprawie gotowości obronnej państwa *(Dz. U. 2004 r. Nr 219, poz. 2218)* Szef Sztabu Generalnego Wojska Polskiego wprowadza ***wyższe stany gotowości bojowej*** lub ***stany gotowości kryzysowej*** dla całych sił zbrojnych lub określonych dowództw i jednostek wojskowych na podstawie postanowienia Prezydenta Rzeczypospolitej Polskiej i decyzji Ministra Obrony Narodowej.

Dowództwa i jednostki wojskowe osiągają wyższe stany gotowości bojowej w ramach podnoszenia gotowości bojowej Sił Zbrojnych Rzeczypospolitej Polskiej. Uruchomienie procesu podnoszenia gotowości bojowej następuje w trybie nakazowym lub alarmowym:

- W trybie nakazowym – (sposób zasadniczy) – realizuje się przedsięwzięcia nakazane w rozkazie przez uprawnionego przełożonego lub wprowadza się kolejno wyższe stany gotowości bojowej dla określonych dowództw, jednostek wojskowych i systemów bojowych. Uzupełnienie do etatu stanu „W" może nastąpić już w Stałej Gotowości Bojowej;
- W trybie alarmowym – w sytuacjach nagłego zagrożenia, wprowadza się określony stan gotowości bojowej dla całości, grupy lub zestawu mobilizacyjnego jednostek wojskowych.

Po wprowadzeniu określonego stanu gotowości bojowej Sił Zbrojnych RP realizują przedsięwzięcia w ramach rozwijania **wojennego systemu dowodzenia Sił**

---

[12] „Dowodzenia i Łączność" J. Michniak, Warszawa 2005
[13] „Dowodzenia i Łączność" J. Michniak, Warszawa 2005

Zbrojnych Rzeczypospolitej Polskiej. Organy dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej szczebla strategicznego są integralną częścią systemu kierowania bezpieczeństwem narodowym we wszystkich stanach gotowości obronnej państwa.

Bardzo istotnym elementem w procesie Osiągania Wyższych Stanów Gotowości Bojowej jest **organizacja łączności**, który powinien zapewnić:

1. Terminowe i dokładne przekazywanie zadań, sygnałów i rozkazów oraz sprawne kierowanie mobilizacyjnym rozwinięciem jednostek;
2. Możliwość niezawodnego przekazywania informacji o skażeniach chemicznych, promieniotwórczych i zakażeniach biologicznych oraz sygnałów ostrzegania i alarmowania;
3. Warunki niezawodnego dowodzenia i współdziałania w MSD (miejsce stałej dyslokacji) oraz w wyznaczonych rejonach;
4. Łączność z garnizonem w MSD, pododdziałom przebywającym w rejonach alarmowych;
5. Do łączności z garnizonem wykorzystuje się środki łączności przewodowej i wojskowej poczty polowej z podległych pododdziałów łączności;
6. Łączność w rejonie alarmowym zapewnia się dowódcom, centrum dowodzenia, elementom bazy mobilizacyjnej i służbie dyżurnej sztabu oraz dowódcom pododdziałów. Do przekazania informacji wykorzystuje się przede wszystkim środki łączności przewodowej, radioliniowej i wojskowej poczty polowej. Dopuszcza się stosowanie radiotelefonów i radiostacji UKF małej mocy;
7. Siły i środki łączności niezaangażowane do utrzymania łączności w rejonie alarmowym rozmieszcza się w sposób umożliwiający szybkie przejście w ugrupowanie marszowe. Realizują one przedsięwzięcia wynikające z wprowadzonego stanu gotowości bojowej, mając na względzie sprawne przemieszczanie do zasadniczego rejonu alarmowego;
8. Po wprowadzeniu stanu Podwyższonej Gotowości Bojowej lub Gotowości „Zagrożenia Wojenne" jednostki wojskowe korzystają z systemu łączności stacjonarnej. Dodatkowo włącza się odbiorniki radiowe w sieciach i kierunkach radiowych zgodnie z wytycznymi sztabu nadrzędnego. Uruchomienie środków łączności radiowej na nadawanie może nastąpić w sytuacjach wyjątkowych, za zezwoleniem dowódcy lub szefa sztabu jednostki wojskowej;

STANY GOTOWOŚCI OBRONNEJ PAŃSTWA

STAŁA GOTOWOŚĆ OBRONNA PAŃSTWA	GOTOWOŚĆ OBRONNA PAŃSTWA CZASU KRYZYSU	GOTOWOŚĆ OBRONNA PAŃSTWA CZASU WOJNY
Zadania planistyczne, organizacyjne, szkoleniowe i kontrolne, mające na celu utrzymanie sprawności systemu obronnego państwa	Zadania zapewniające przygotowanie do przeciwdziałania zagrożeniom bezpieczeństwa państwa oraz usuwania skutków ich wystąpienia	Zadania umożliwiające przeprowadzenie powszechnej mobilizacji, wprowadzenie stanu wojennego oraz pełne rozwinięcie systemu obronnego państwa

STANY GOTOWOŚCI BOJOWEJ SZ RP

STAŁA GOTOWOŚĆ BOJOWA	PODWYŻSZONA GOTOWOŚĆ BOJOWA	GOTOWOŚĆ BOJOWA ZAGROŻENIE WOJENNE	PEŁNA GOTOWOŚĆ BOJOWA
Utrzymywać system służb operacyjnych i dyżurnych oraz sprawność systemu alarmowania i powiadamiania	Przygotować elementy Wojennego Systemu Dowodzenia	Zapoczątkować rozwijanie Wojennego Systemu Dowodzenai	W pełni rozwinąć Wojenny System Dowodzenia

STANY GOTOWOŚCI KRYZYSOWEJ SZ RP

STAŁA GOTOWOŚĆ KRYZYSOWA	PODWYŻSZONA GOTOWOŚĆ KRYZYSOWA	GOTOWOŚĆ ZAGROŻENIE KRYZYSOWEGO	PEŁNA GOTOWOŚĆ KRYZYSOWA
Wydzielenie struktur resortu obrony narodowej do rozwinięcia Systemu Zarządzania Kryzysowego j	Wydzielenie struktur Sił Zbrojnych do rozwinięcia Systemu Zarządzania Kryzysowego	Wprowadzenie szczegółowych zadania dla elementów Systemu Zarządzania Kryzysowego	Rozwinięcie pełnej obsady elementów Systemu Zarządzania Kryzysowego

Rys. 2.4 *Stany gotowości obronnej państwa i gotowości bojowej Sił Zbrojnych Rzeczypospolitej Polskiej*

Źródło: Opracowanie własne na podstawie : Biblioteka "Bezpieczeństwa Narodowego", kwartalnika wydawanego przez Biuro Bezpieczeństwa Narodowego, TOM 2/2007, wystąpienie Pana płk. Andrzeja Brzozy – Szefa Zarządu Planowania Systemów Dowodzenia i Łączności - P6 Sztabu Generalnego Wojska Polskiego (część jawna)nt „Stan obecny Sił Zbrojnych RP. System dowodzenia– problemy i wyzwania" oraz na podstawie Decyzji Ministra Obrony Narodowej Z-1z dnia 15.02.2007.

Obowiązkiem państwa, w tym głównie administracji rządowej i samorządowej, jest posiadanie adekwatnych do każdej sytuacji rozwiązań systemowych, odpowiedniego prawa oraz struktur i narzędzi pozwalających na sprawne zarządzanie w sytuacjach kryzysowych. Jest to tym ważniejsze, że działania w sytuacjach kryzysowych i stanach nadzwyczajnych, przebiegają zwykle w warunkach olbrzymiego napięcia, stresu, ograniczonej informacji i wysokiego ryzyka. Konstytucja Rzeczypospolitej Polskiej wprowadziła do wewnętrznego porządku prawnego pojęcia stanów nadzwyczajnych: wojennego, wyjątkowego i klęski żywiołowej, które mogą być wprowadzone w sytuacjach szczególnych zagrożeń, jeżeli zwykłe środki konstytucyjne są niewystarczające.

2.4 Elementy generujące wymagania organizacyjno – techniczne dla stacjonarnej sieci teleinformatycznej

W celu przeprowadzenia analizy potrzeb i wymagań wobec sieci teleinformatycznej wzięto pod uwagę sposób organizacji oraz technicznych uwarunkowań na stacjonarną sieć teleinformatyczną, która uzależniona jest od wymagań dowodzenia. Wymagania[14] jak podaje słownik języka polskiego jest to zespół związanych z czymś warunków, norm, żądań, oczekiwań, które ktoś lub coś ma spełniać; wymogi, potrzeby: skromne, wysokie, wygórowane wymagania. Natomiast wymagania dowodzenia[15] to całokształt warunków, wskaźników, wielkości i oczekiwań, którym powinno odpowiadać i do których należy dostosować dowodzenie. Za Profesorem Józefem Michniakiem wymagania dowodzenia odnoszą się do czterech zasadniczych obszarów tj.:

- wymagania w zakresie tworzenia struktur organizacyjnych (np.: jednolite struktury na taktycznych szczeblach dowodzenia);
- wymagania w zakresie proceduralnym (np.: jednakowe zrozumienie i interpretowanie znaków i skrótów taktycznych, procedur sztabowych itp.);
- wymagania w zakresie indywidualnych cech psychofizycznych dowódców i osób funkcyjnych organów dowodzenia (np. konsekwencja , inicjatywa, stanowczość);

---

[14] „Słownik współczesnego języka polskiego" - Warszawa 1998
[15] „Dowodzenia i łączność" Józef Michniak, AON Warszawa 2005

- wymagania techniczne (np. ciągłość, wierność i szybkość przekazu informacji, mobilność, itp.).

Reasumując powyższe można jednoznacznie stwierdzić, że sprawne dowodzenie siłami zbrojnymi w okresie pokoju, kryzysu i wojny odbywa się dzięki systemowi dowodzenia , w skład którego wchodzą następujące podsystemy[16]:

- organów i stanowisk dowodzenia;
- **łączność i informatyka** oraz *wspomagania procesu dowodzenia* ***(środki i urządzenia automatyzacji);***
- informacyjny, *na który składają się: elementy zintegrowanego rozpoznania i kontroli sytuacji.*

Każdy z powyższych podsystemów stanowi integralną funkcjonalno – informacyjną całość. Dobrze funkcjonującą rozległą sieć teleinformatyczną na terytorium Rzeczypospolitej Polskiej stanowi integralny podsystem, który jest niezbędnym elementem w systemie dowodzenia siłami zbrojnymi.

Do rozważań autor przyjął, że najważniejszymi elementami generującymi wymagania na taką sieć teleinformatyczną są:

- system dowodzenia w czasie pokoju, kryzysu i wojny;
- rodzaje działań z użyciem wojska na terytorium kraju;
- rodzaj zastosowanych usług teleinformatycznych niezbędnych do sprawnego przesyłu informacji;
- sposób pozyskiwania niezbędnych informacji w czasie dowodzenia operacjami militarnymi.

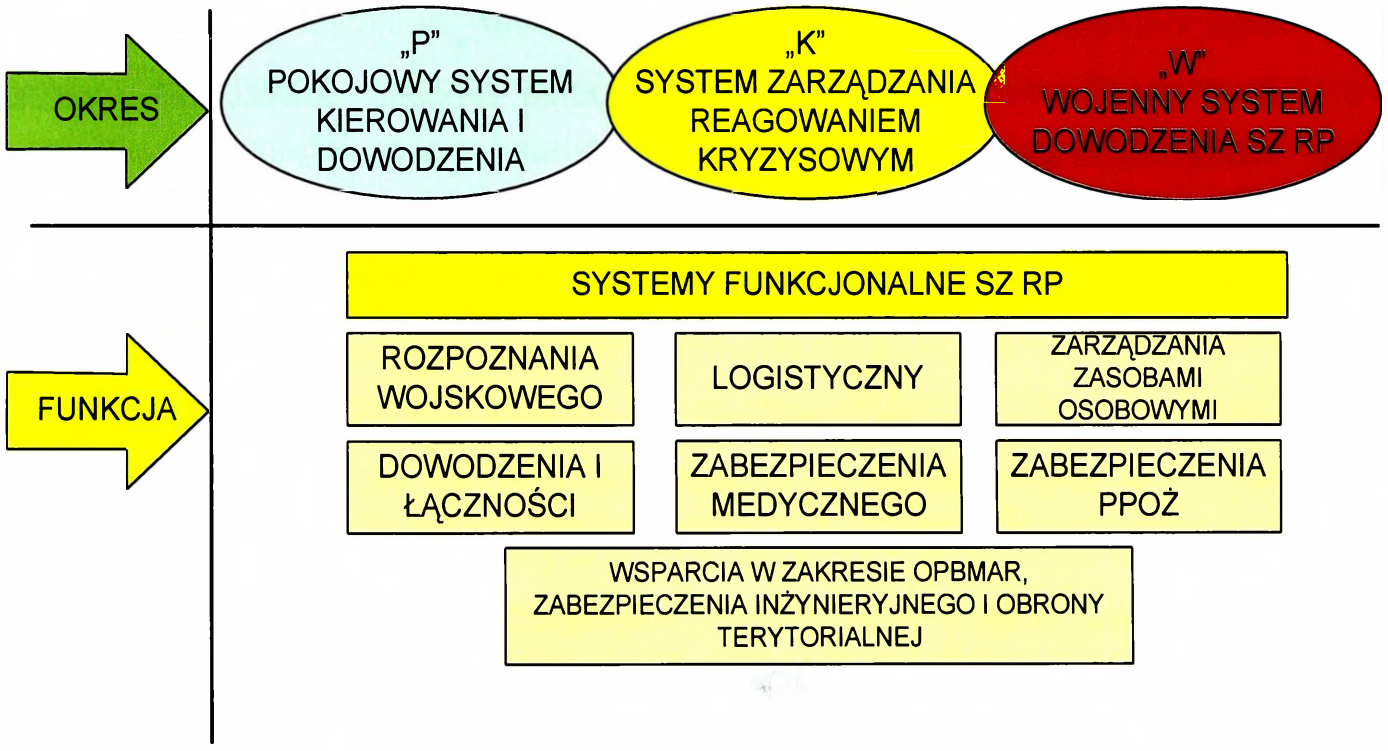
Z analizy literatury przedmiotu oraz aktów prawnych podsystemu kierowania obronnością, Siły Zbrojne Rzeczypospolitej Polskiej, realizując określone zadania wynikające ze „Strategii Obronnej Rzeczypospolitej Polskiej" w zależności od okresu w jakim się znajdują rozwijają dedykowane systemy:

- pokojowy system kierowania i dowodzenia;
- system zarządzania reagowaniem kryzysowym;
- wojenny system dowodzenia SZ RP.

W zależności od charakteru systemu rozwijanego w danym okresie, równolegle realizowany jest proces wspomagania przez systemy funkcjonalne, których głównym zadaniem jest zaspokajanie generowanych przez znamionowy system dowodzenia

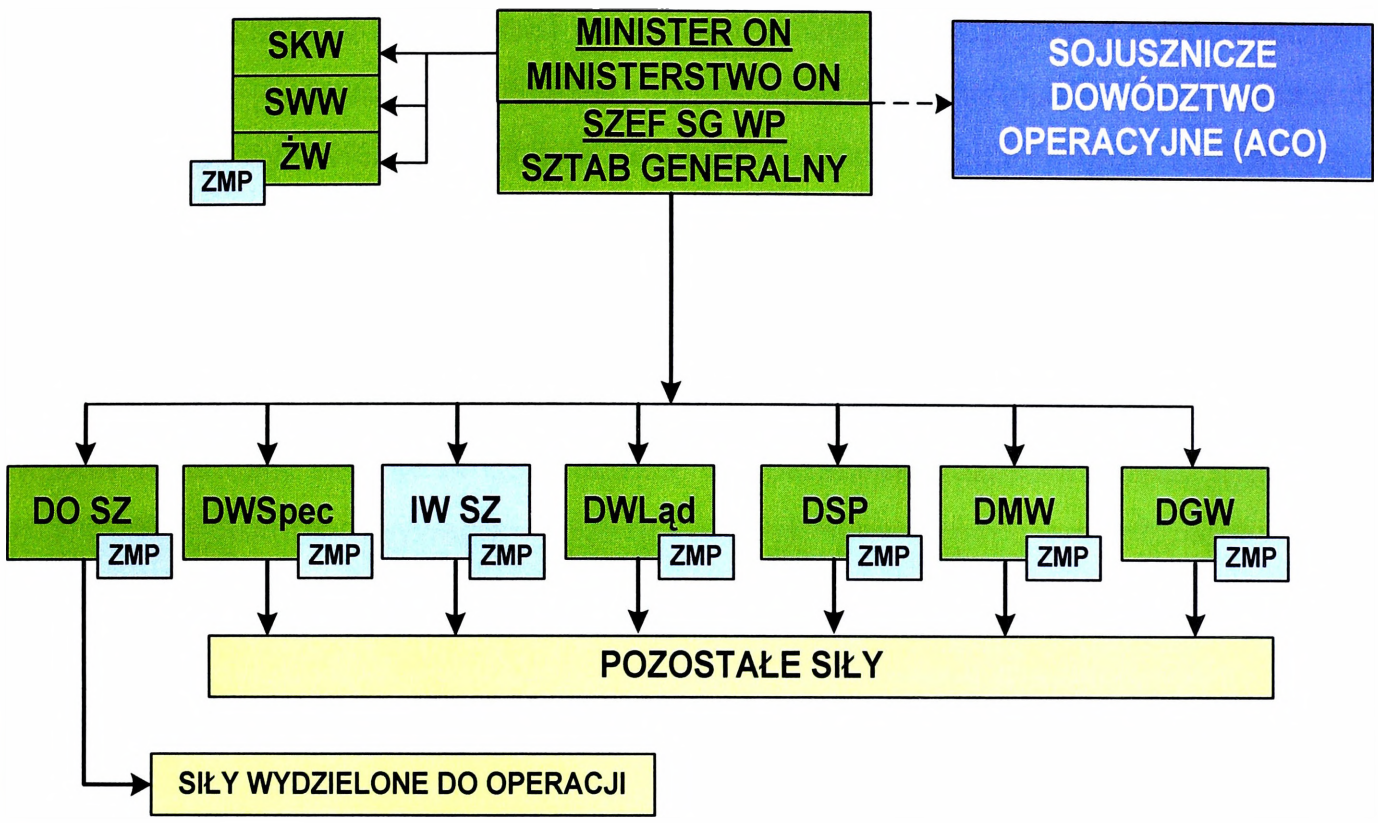
[16] „Dowodzenie i Łączność" Józef Michniak, AON Warszawa 2005

potrzeb z uwzględnieniem jego wyspecjalizowanych funkcji. Generowane potrzeby, jak również funkcje świadczone przez wyspecjalizowane systemy wspomagające przekładają się bezpośrednio na strukturę organizacyjno – techniczną systemu łączności.



Rys. 2.5 *Struktura podsystemu militarnego*
Źródło: Opracowanie własne: na podstawie „Zgrywanie systemu walki" AON Warszawa 2006

W okresie pokoju, kiedy funkcjonuje ***pokojowy system kierowania i dowodzenia***, system łączności resortu Obrony Narodowej zorganizowany jest zgodnie z potrzebami systemu dowodzenia i współdziałania. Głównym i zasadniczym zadaniem systemu jest zapewnienie przekazywania informacji w relacjach dowodzenia i współdziałania. **Na szczeblu strategicznym łączność organizowana jest w całości w oparciu o system stacjonarny**. Dotyczy to zarówno części transmisyjnej jak i węzłów łączności obsługujących stanowiska dowodzenia wyższych szczebli. Część teletransmisyjną systemu łączności resortu tworzą eksploatowane trakty cyfrowe dzierżawione od TP S.A., EXATEL oraz innych operatorów.



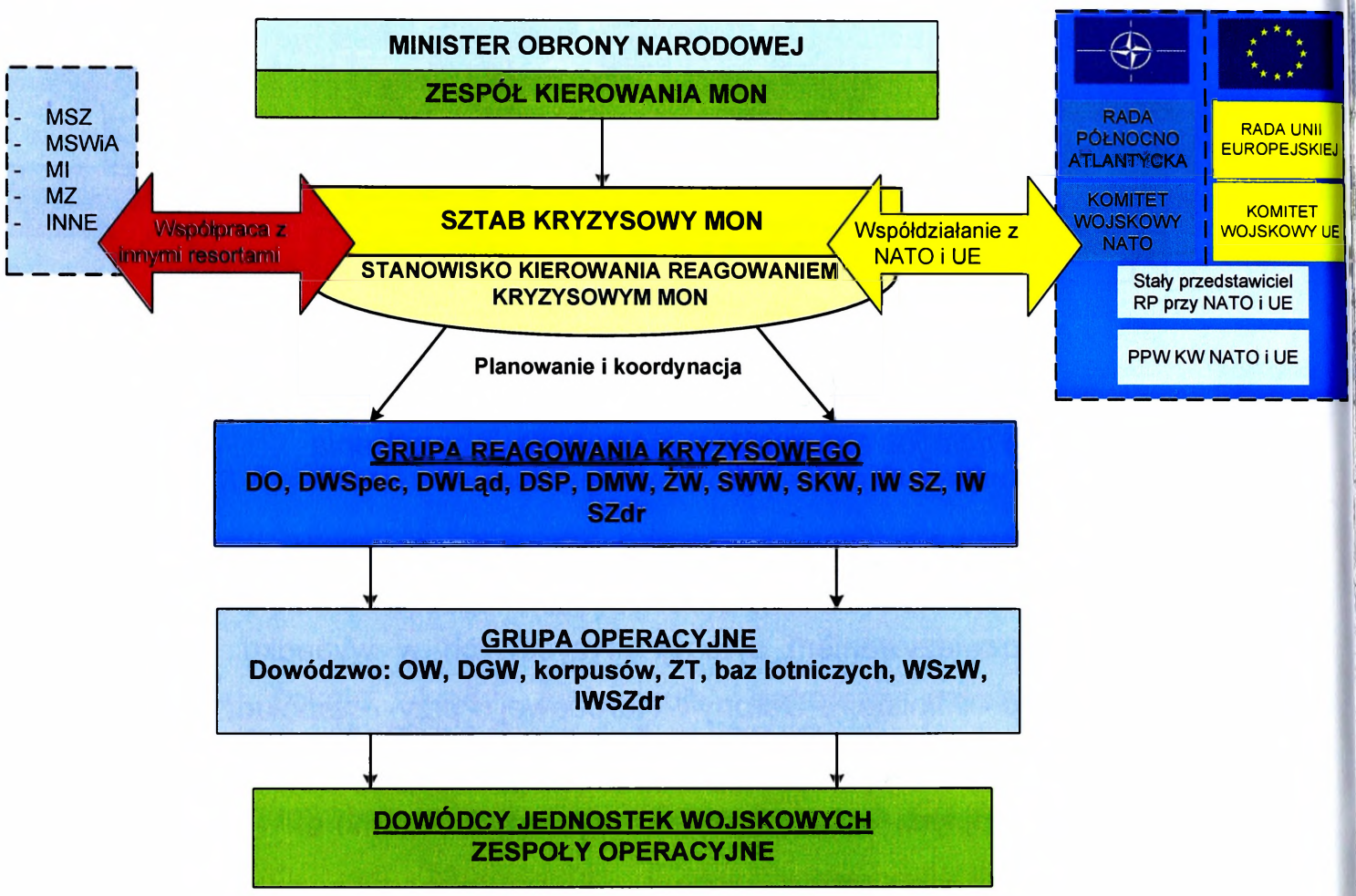
Rys. 2.6 *Struktura pokojowego systemu kierowania i dowodzenia*
Źródło: Opracowanie własne: na podstawie „Strategii Bezpieczeństwa Narodowego RP"

W okresie kryzysu, rozwijany jest ***system zarządzania reagowaniem kryzysowym***. Rozwiązywaniem sytuacji kryzysowych w wypadku występowania zagrożeń kieruje Minister Obrony Narodowej przy współudziale Zespołu Kierownictwa MON, w razie potrzeby poszerzonego odpowiednio o dowódców rodzajów sił zbrojnych oraz szefów wybranych komórek organizacyjnych Ministerstwa Obrony Narodowej.

W skład Systemu Kierowania Reagowaniem Kryzysowym resortu ON oprócz Zespołu Kierownictwa MON wchodzą: Sztab Kryzysowy MON, Grupy Reagowania Kryzysowego RSZ, Grupy Operacyjne dowództw okręgów wojskowych, Dowództwa Garnizonu Warszawa, korpusów, dowództw związków taktycznych oraz Wojewódzkich Sztabów Wojskowych. System Kierowania Reagowaniem Kryzysowym resortu ON aktywuje się w sytuacji narastania kryzysu. Ocena sytuacji kryzysowej jest procesem ciągłym, który w działalności bieżącej realizowany jest przez odpowiednie systemy monitorujące zarówno wojskowe jak i cywilne. Decyzje Ministra ON lub Szefa Sztabu Generalnego WP stanowią podstawę rozwinięcia ***Sztabu Kryzysowego MON***.

Informacja o rozwinięciu Sztabu Kryzysowego (SzK) MON przekazywana jest do Dyżurnej Służby Operacyjnej (DSO) Sił Zbrojnych Rzeczypospolitej Polskiej, która odpowiada za powiadomienie obsady Sztabu Kryzysowego MON.

W zależności od potrzeb w dalszej kolejności rozwija się podległe elementy Systemu Kierowania Reagowaniem Kryzysowym resortu ON i uruchamia niezbędne siły i środki wojska do udziału w operacji kryzysowej.



Rys. 2.7 *Struktura systemu zarządzania reagowaniem kryzysowym*
Źródło: Opracowanie własne: na podstawie „Decyzji Ministra Obrony Narodowej Z-1 z dnia 15.02.07"

Kierowanie siłami zbrojnymi odbywa się według ***zasad kierowania pokojowego***, wojskami wydzielonymi do międzynarodowych zgrupowań, wykonujących zadania w ramach reagowania kryzysowego, dowodzi Dowództwo Operacyjnie.

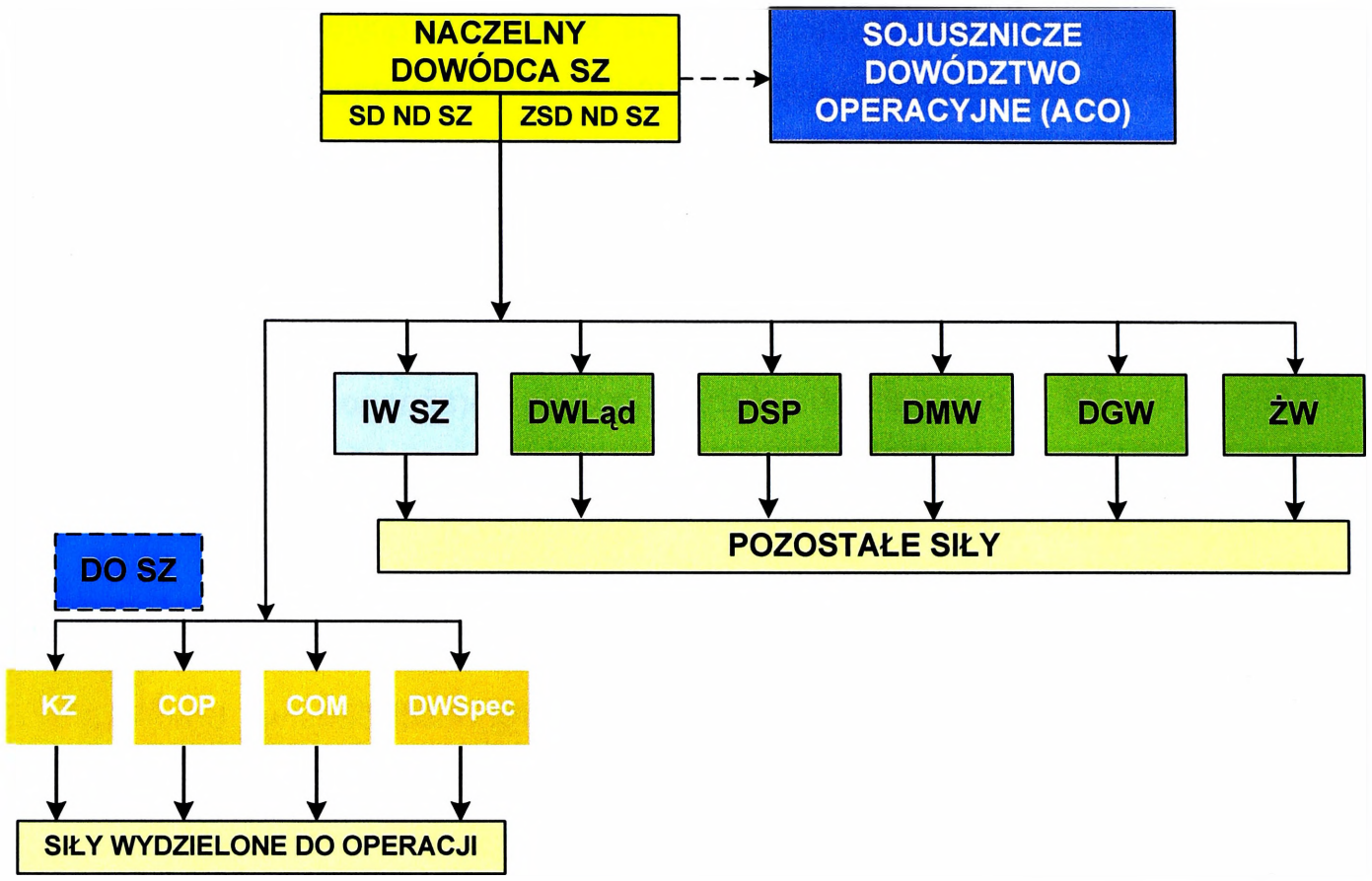
W okresie osiągania WSGB, system łączności wzmacniany jest wydzielanym dodatkowo potencjałem z zasobów TP S.A., EXATEL i innych operatorów. Węzły łączności obsługujące stanowiska dowodzenia wyższych szczebli są zawczasu

wytypowanymi i przygotowanymi obiektami telekomunikacyjnymi, uzupełnianymi w urządzenia końcowe. Środki mobilne są środkami rezerwującymi niektóre elementy stacjonarnego systemu łączności szczebla strategicznego. W razie potrzeby tworzą odrębne relacje dalekosiężne lub obejścia uszkodzonej w dużej skali sieci stacjonarnej. Za pomocą środków mobilnych rozwijane mogą być odrębne sieci w wybranym rejonie kraju, np. na obszarze o słabo rozwiniętej infrastrukturze telekomunikacyjnej. Środki węzłowe służyć mogą do doraźnego rozwijania polowych węzłów łączności stanowisk dowodzenia w operacyjnie uzasadnionych sytuacjach lub do dokompletowywania węzłów stacjonarnych po wystąpieniu strat spowodowanych oddziaływaniem przeciwnika lub klęsk żywiołowych. Na terenie kraju rozmieszczenie wojskowych węzłów łączności jest nierównomierne. Dlatego też przy planowaniu systemu łączności na potrzeby obronności państwa brane są pod uwagę również węzły telekomunikacyjne operatorów publicznych.

W czasie wojny Siłami Zbrojnymi dowodzi Naczelny Dowódca Sił Zbrojnych Rzeczypospolitej Polskiej[17], mianowany przez Prezydenta Rzeczypospolitej Polskiej na wniosek Prezesa Rady Ministrów. Dla zapewnienia bezkolizyjnego rozwijania Sił Zbrojnych Rzeczypospolitej Polskiej oraz kierowania dowodzenia nimi w czasie wojny utworzony jest **Wojenny System Dowodzenia** (WSyD), który jest integralną wykonawczą częścią Systemu Kierowania Obroną Państwa.

WSyD jest to plan rozmieszczenia oraz przemieszczania stanowisk dowodzenia na terytorium kraju w trakcie rozwijania się konfliktu zbrojnego. Plan zawiera także szczegółowe wytyczne do organizacji łączności na stanowiskach dowodzenia i w trakcie przemieszczania się pomiędzy kolejnymi położeniami stanowiskach dowodzenia.

[17] Zgodnie z art. 134, pkt 4, Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku.



Rys. 2.8 *Struktura wojennego systemu dowodzenia SZ RP*
Źródło: Opracowanie własne na podstawie „Ustawa z dnia 24 maja 2007 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej".

W strukturę Stanowiska Kierowania Obroną Państwa (SKOP) wchodzi Stanowisko Kierowania (SK) Prezydenta RP, który jest najwyższym zwierzchnikiem Sił Zbrojnych RP (art. 134 pkt 1 Konstytucji RP) oraz SK Prezesa Rady Ministrów i wskazanych przez niego ministrów, w tym SK MON.

Stanowisko Kierowania Ministra Obrony Narodowej spełnia rolę organu planistycznego i koordynującego wsparcie i zabezpieczenie działań Sił Zbrojnych Rzeczypospolitej Polskiej, wojsk sojuszniczych uczestniczących w operacji. Siłami Zbrojnymi dowodzi Naczelny Dowódca Sił Zbrojnych ze Stanowiska Dowodzenia lub Zapasowego SD.

Na czas wojny zostanie rozwinięty Wojenny System Dowodzenia, a Naczelny Dowódca Sił Zbrojnych Rzeczypospolitej Polskiej (po jego mianowaniu) będzie realizował decyzje organów kierowania obronnością państwa, sprawując pełne dowodzenie w stosunku do całych Sił Zbrojnych Rzeczypospolitej Polskiej. Dotychczasowy Wojenny System Dowodzenia jest tak skonstruowany, że komórki organizacyjne tworzące Sztab Generalny Wojska Polskiego oraz Dowództwo

Operacyjne wydzielają obsadę operacyjną na SD i ZSD Naczelnego Dowództwa Sił Zbrojnych.

- Dowództwo Operacyjne całość sił wydziela do Centrum Dowodzenia znajdującym się na SD ND SZ;
- Inspektorat Wsparcia z Szefostwami Inżynierii i OPBMR wydziela oficerów do Centrum Wsparcia, które również znajduje się na SD ND SZ;
- Dowództwa RSZ uzupełniają, w niezbędnym zakresie, obsadę operacyjną SD i ZSD ND SZ;
- Dowództwo Wojsk Specjalnych podlega pod ND SZ i bezpośrednio dowodzi siłami wydzielonymi do operacji;
- Dowództwo 2KZ, COP i COM, bezpośrednio podporządkowane pod ND SZ, dowodzą wydzielonymi komponentami z Rodzajów Sił Zbrojnych.

Przedstawiona powyżej struktura organizacyjno – funkcjonalna powinna umożliwić realizację celów na stanowiskach dowodzenia, być wystarczająco trwałą strukturą aby umożliwić jej nieprzerwane funkcjonowanie oraz ułatwić przystosowanie dowództw do zmieniających się warunków zewnętrznych. Po dokonaniu analizy struktury systemu dowodzenia widzimy jak wielkimi wymaganiami powinna być obarczona organizacja stacjonarnej sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej dla zapewnienia kierowania i dowodzenia na każdym szczeblu organizacyjnym.

Na podstawie przeprowadzonych badań, których opis, narzędzia badawcze i wyniki zamieszczono w **zał. 3** sporządzono tabelę 2.1 umożliwiającą podsumowanie dotychczasowych rozważań w celu określenia podstawowych potrzeb na **usługi telekomunikacyjne** i informatyczne w procesie dowodzenia w okresie pokoju, kryzysu i zagrożenia militarnego państwa, które w znaczący sposób przekładają się na wymagania organizacyjno - technicznych sieci teleinformatycznej (Usługi telekomunikacyjne i informatyczne – **zał. 1**).

Systemy teleinformatyczne umożliwiają przesyłanie szerokiej gamy usług głosowych, transmisji danych oraz obrazu.

Problem szczegółowych rozwiązań techniczno – organizacyjnych na Stanowiskach Dowodzenia lub Stanowisku kierowania reagowaniem kryzysowym szczebla strategicznego w literaturze przedmiotu poruszany jest bardzo rzadko i ogólnie. Jednak na podstawie doświadczeń zawodowych, często prowadzonych

i organizowanych ćwiczeń wojskowych oraz dysertacji literatury przedmiotu autor przedstawi ogólną koncepcję organizacji Stanowiska Dowodzenia szczebla strategicznego.

Na podstawie przeanalizowanej literatury na temat więzi informacyjnych, możemy zastosować kryterium przepływu informacji w relacji stanowisko dowodzenia – otoczenie, gdzie można wyróżnić trzy rodzaje więzi informacyjnych[18].

- Zewnętrzne wchodzące – związane ze zbieraniem informacji z szeroko rozumianego „otoczenia" (służbowe i współdziałanie, a więc np. dla rozkazów, meldunków czy też komunikatów);
- Wewnętrzne – związane z wytwarzaniem i przekazywaniem informacji wewnątrz stanowiska dowodzenia;
- Zewnętrzne wychodzące – związane z przekazywaniem informacji poza stanowisko dowodzenia.

Reasumując powyższe w systemie dowodzenia przekazywanie informacji wewnątrz stanowiska dowodzenia może odbywać się poprzez kontakt osobisty lub poprzez techniczne środki łączności, natomiast przekazywanie informacji na zewnątrz stanowiska dowodzenia musi odbywać się poprzez techniczne środki łączności. Węzeł łączności na stanowiskach dowodzenia w celu wymiany informacji powinien zapewniać następujące rodzaje usług telekomunikacyjnych we wszystkich rodzajach prowadzonych operacji wojskowych na terytorium kraju:

1. Łączność telefoniczną jawną i faksową;
2. Łączność telefoniczną niejawną i faksową;
3. Wideokonferencję;
4. Transmisję danych;
5. Zautomatyzowane systemy dowodzenia;

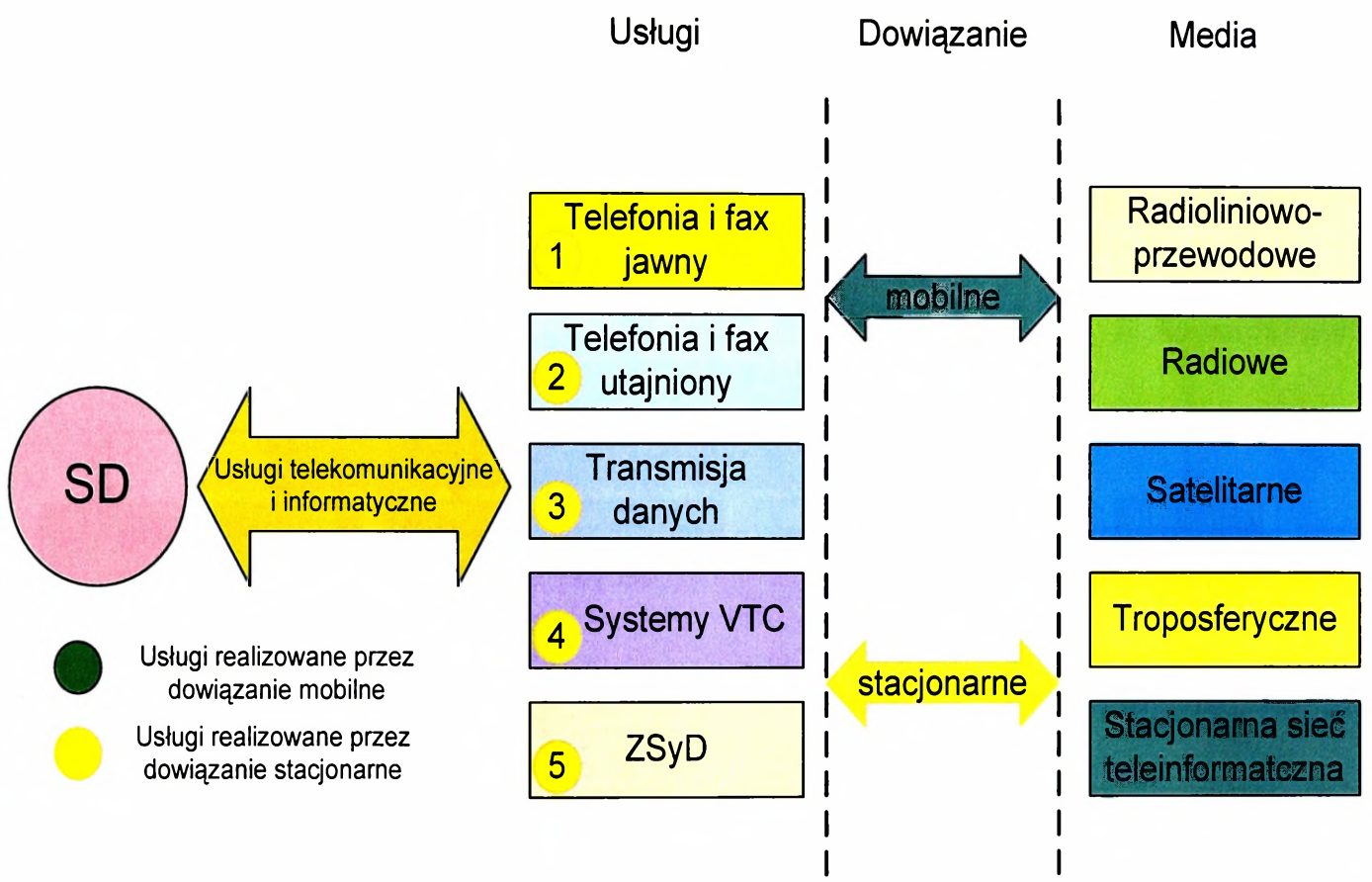
Poprzez następujące media:

1. Drogą satelitarną;
2. Stacjonarną siecią teleinformatyczną;
3. Drogą radiową (rezerwową);
4. Drogą troposferyczną;
5. Drogą radioliniowo – Kablową (przewodową i światłowodową);
6. Wojskową pocztę polową.

---

[18] „Dowodzenia i łączność" Józef Michniak, AON Warszawa 2005.

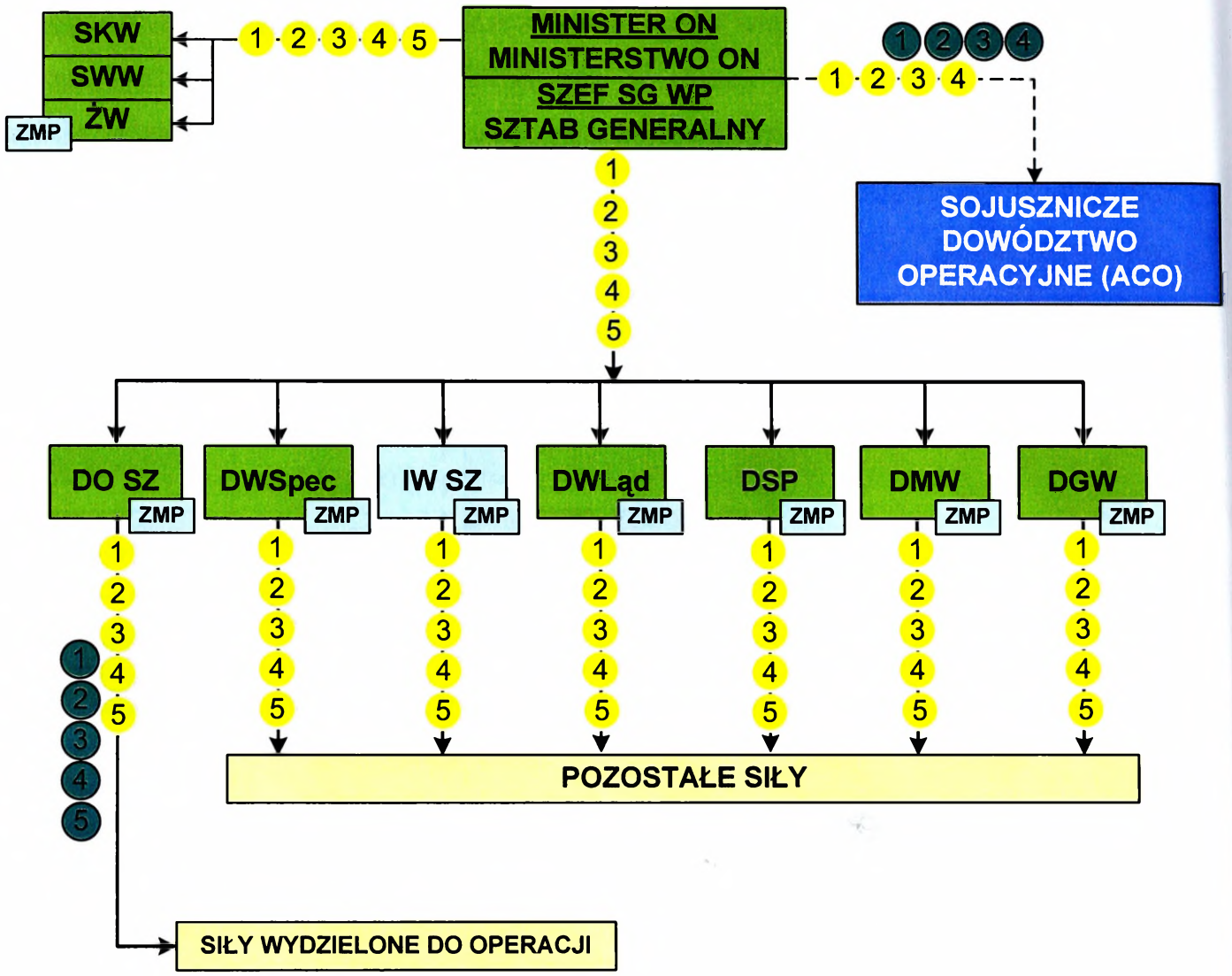
Powyższe zależności przedstawia (rys. 2.9)



Rys. 2.9 *Rodzaje usług i mediów na SD szczebla strategicznego*

Źródło: Opracowanie własne

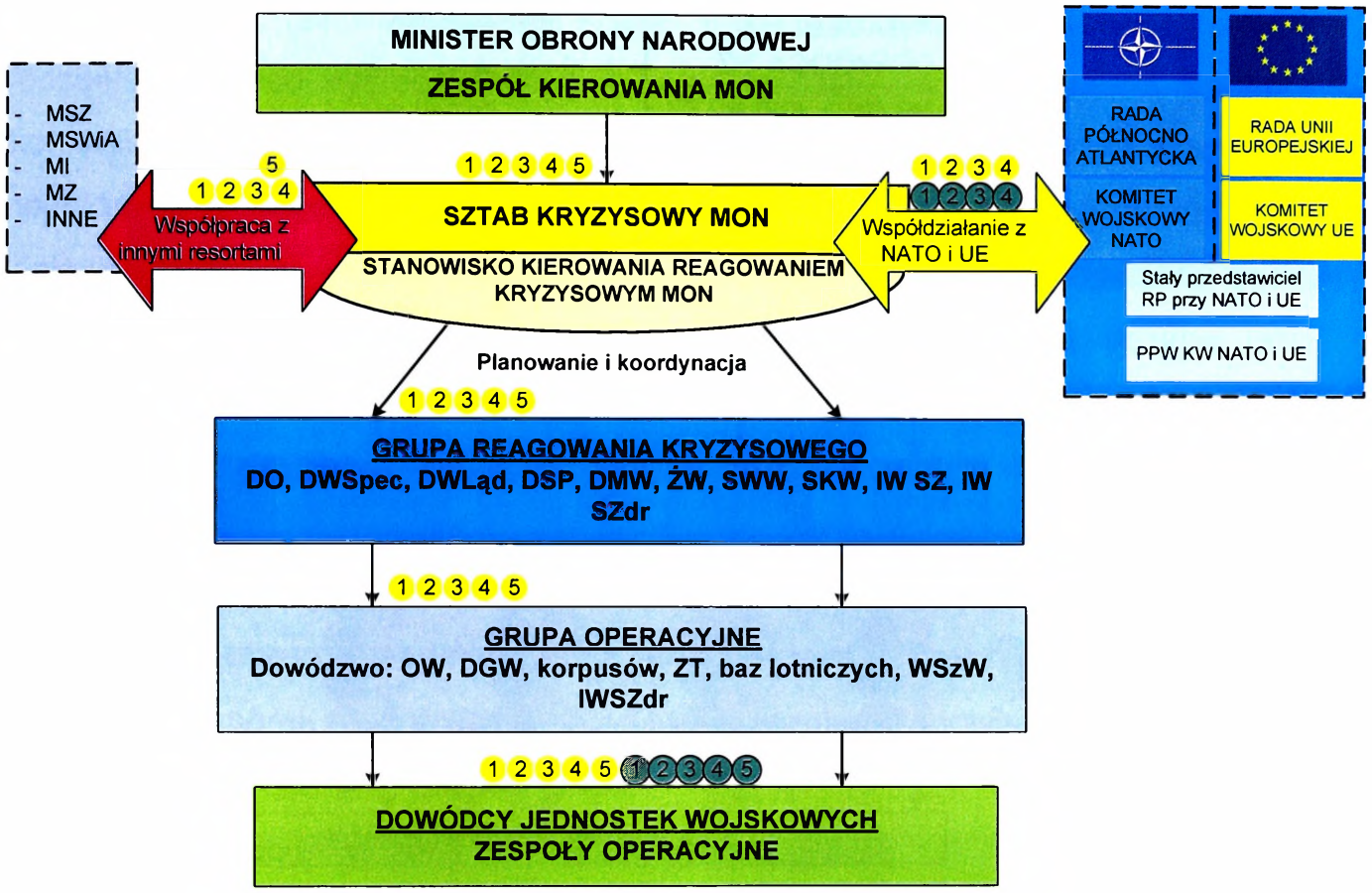
Po określeniu niezbędnych usług telekomunikacyjnych i informatycznych, czyli zadań łączności oraz więzi informacyjnych możliwe jest wykonanie analizy wymagań wobec sieci teleinformatycznej na podstawie modelu wyżej opisanych struktury systemów kierowania i dowodzenia.



Rys. 2.10 *Rodzaje mediów wykorzystywanych w pokojowym systemie kierowania i dowodzenia*
Źródło: Opracowanie własne

Po przeprowadzeniu analizy powyższego systemu można stwierdzić, że obciążenie oraz ilość usług telekomunikacyjnych oraz informatycznych w okresie pokoju nie wzrasta. Funkcjonująca sieć teleinformatyczna pracuje na stałym poziomie bez zwiększonych wymagań.

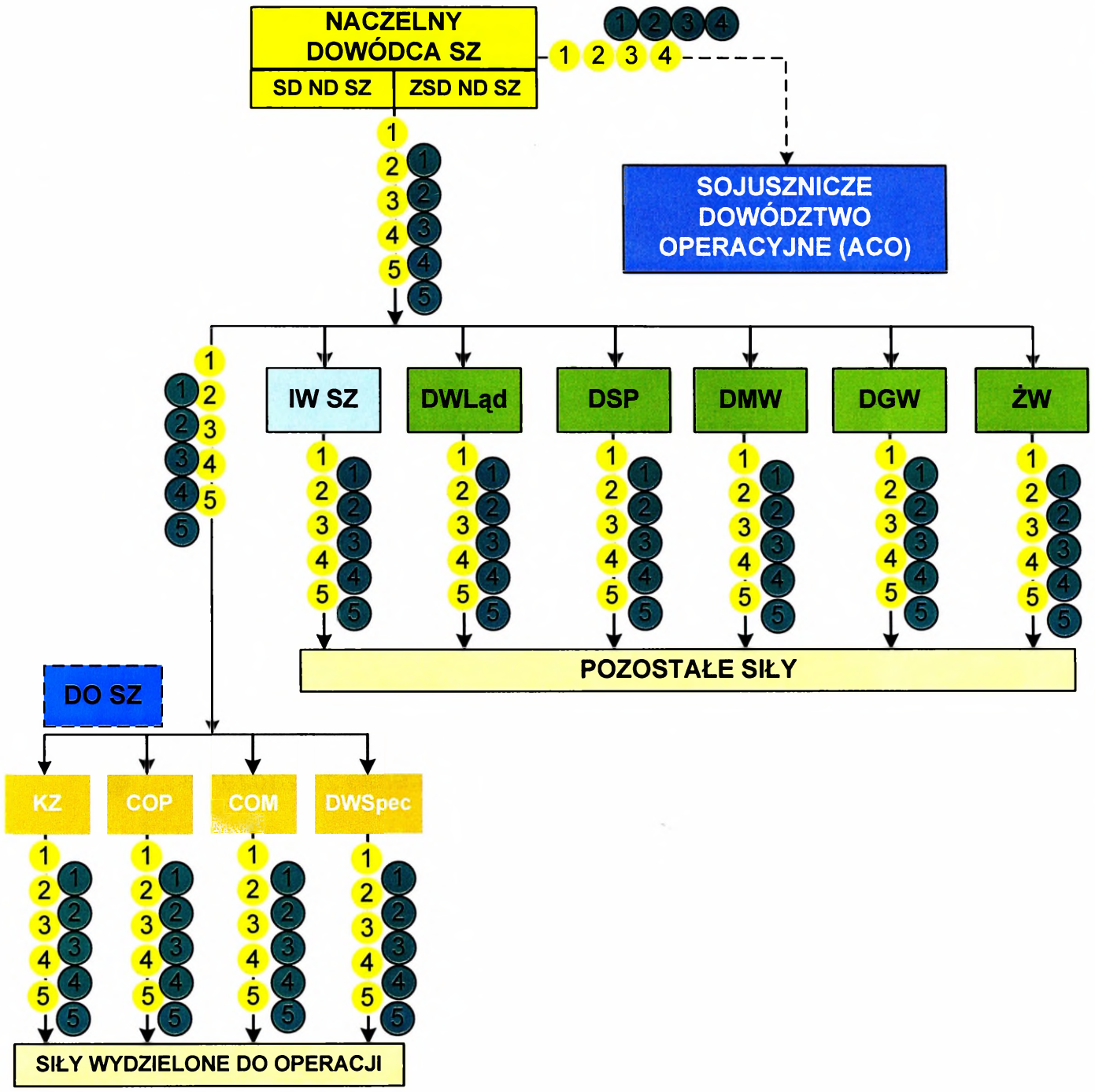
System zarządzania reagowaniem kryzysowym



Rys. 2.11 *Rodzaje mediów wykorzystywanych w systemie zarządzania reagowaniem kryzysowym*
Źródło: Opracowanie własne

W okresie stanów kryzysowych, system zarządzania reagowaniem kryzysowym generuję zmianę struktur dowodzenia i kierowania, organizowane jest stanowisko kierowania reagowaniem kryzysowym. Stanowisko kryzysowe jest obiektem stacjonarnym zawczasu przygotowanym. Z powyższej struktury oraz organizacji łączności widać, że w tym okresie wymagania wobec stacjonarnej sieci teleinformatycznej wzrastają nieznacznie. Dodatkowe wymagania generowane są na poziomie współdziałania z innymi ministerstwami oraz jednostkami wojskowymi biorącymi bezpośredni udział w usuwaniu skutków kryzysu.

Wojenny system dowodzenia SZ RP



Rys. 2.12 *Rodzaje mediów wykorzystywanych w wojennym systemie dowodzenia*
Źródło: Opracowanie własne

W okresie osiągania wyższych stanów gotowości bojowej organizowany jest Wojenny System Dowodzenia, który jak widać na rysunku 2.12. w znaczny sposób generuje zwiększone wymagania na stacjonarną sieć teleinformatyczną.

Analizując strukturę organizacyjną stanowisk dowodzenia (strategicznych), funkcjonujących w okresie organizacji wojennego systemu dowodzenia oraz przyjmując określoną organizację jego pracy można dokonać szacunkowych obliczeń

obejmujących obciążenie stacjonarnej sieci teleinformatycznej przenoszącej usługi świadczone przez podsystem łączności dla stanowisk dowodzenia.

Przy przyjęciu założenia, że węzeł łączności strategicznych stanowisk dowodzenia powinien być rozwinięty na bazie zawczasu wytypowanych obiektów telekomunikacyjnych (regionalny węzeł łączności lub garnizonowy węzeł łączności), wzmocnionych polowymi środkami łączności i informatyki i poniższych kryteriów:

- głównym parametrem przydziału urządzeń końcowych będą zadania danej osoby (komórki organizacyjnej) realizowane na stanowisku dowodzenia oraz możliwości techniczne sprzętu łączności i informatyki;
- największe nasycenie w urządzenia łączności i informatyki występować będzie w nw. komórkach organizacyjnych stanowiska dowodzenia:
  - połączony zespół operacyjny (PZO);
  - zespół oficerów kierunkowych z jednostek wydzielonych do operacji.
- gradacja komórek organizacyjnych na strategicznym stanowisku dowodzenia:
  - centrum, ośrodek, zespół, grupa;
  - dodatkowo Połączony Zespół Operacyjny (PZO);
  - każdy zespół składa się z trzech grup i na zamianie liczy 10 osób (szef + 3 grupy po 3 osoby).

Obsada operacyjna pracująca na jednej zmianie strategicznego stanowisku dowodzenia wynosi 450 osób.

Zapotrzebowanie na urządzenia końcowe zapewniające całkowite zaspokojenie potrzeb generowanych przez elementy stanowisku dowodzenia kształtuje się na poziomie przedstawionym w poniższej tabeli:

Tabela 2.2

Urządzenia końcowe na stanowisku dowodzenia

Lp.	Urządzenie końcowe	Ilość
1	Aparat systemowy jawny	8
2	Telefon jawny CA	30
3	Fax jawny	2
4	Telefon z ind. utajnianiem i faxem (NATO SECRET)	10
5	Telefon niejawny (ATS-2p)	108
6	Fax niejawny ILEX	2

7	Zestaw wideokonferencyjny	4
8	Telefon IP	20
9	Komputer MIL-WAN	69
10	Komputer Internet	30
11	Komputer SZAFRAN	2
12	Komputer DUNAJ	2
13	Komputer ŁEBA	2
14	Komputer NATO	10
15	Komputer SEC-WAN	20

Uwzględniając wymagania powyżej zestawionych urządzeń wobec systemu teleinformatycznego w celu zapewnienia ciągłej bezawaryjnej ich pracy, minimalny podział traktów stanowiących infrastrukturę dowiązania stanowisk dowodzenia do sieci teleinformatycznej Sił Zbrojnych przedstawia się w następujący sposób:

1. ***Trakty wchodzące:***

1) Stacjonarne:

- 1 trakt o przepływności 2 Mbit/s dla systemów jawnej łączności telefonicznej i faksowej;
- 1 trakt o przepływności 2 Mbit/s dla niejawnej sieci informatycznej (SEC-WAN);
- 2 trakty o przepływności 1 Gbit/s dla systemów teleinformatycznych (MIL-WAN) oraz Zautomatyzowanych Systemów Wsparcia Dowodzenia (SZAFRAN, DUNAJ, ŁEBA);

2) Mobilne:

- 1 trakt (kierunek radioliniowy) o przepływności 2 Mbit/s dla systemów niejawnej łączności telefonicznej i faksowej (PCŁU);
- 1 trakt (kierunek radioliniowy) o przepływności 2 Mbit/s dla niejawnej sieci informatycznej (SEC-WAN);
- 1 trakt (kierunek radioliniowy) o przepływności 2 Mbit/s dla niejawnej sieci informatycznej (MIL-WAN);
- 1 kierunek satelitarny do łączności z NATO na okres działań w układzie sojuszniczym.

2. ***Trakty wychodzące:***

   Ilość traktów i ich przepływność zależy od wyposażenia i możliwości technicznych stacjonarnego węzła łączności na bazie którego rozwijany jest WŁ strategicznego SD – generalnie jest zbliżona do ilości traktów wchodzących.

3. ***Łączność radiowa:***

   - 4 sieci radiowe (mobilne).

Analizując powyższe dane pod kątem organizacji łączności w okresie WSyD należy stwierdzić, systemy polowe są w pełni kompatybilne z systemami stacjonarnymi a w szczególności styki typu G703 oraz protokołami TCP/IP. Pełne wykorzystanie możliwości technicznych polowych aparatowni teleinformatycznych możliwe będzie dopiero wówczas, gdy Regionalne Węzły Łączności będą w stanie wydzielić łącze o odpowiedniej przepływności nie mniejsze jednak niż 1Gbit/s.

Dla usprawnienia procesu dowodzenia, w sieciach teleinformatycznych zostaną osadzone aplikacje informatyczne w celu wsparcia dowodzenia jako Zautomatyzowane Systemy Dowodzenia (ZSyD). Autor na potrzeby niniejszego rozdziału przedstawił trzy najważniejsze systemy informatyczne użytkowane w rodzajach sił zbrojnych (Opis aplikacji ZSyD – **zał. 4**).

2.5 Rodzaj stanowisk dowodzenia

System dowodzenia tak jak zostało to opisane w podrozdziale 2.2 są to elementy składowe takie jak:

- organy dowodzenia;
- stanowisk dowodzenia;
- sieci telekomunikacyjnych;
- sieci teleinformatycznych;
- stacji i samodzielnych urządzeń telekomunikacyjnych i teleinformatycznych;
- oraz innych,

i dlatego podczas ustalania rejonu stanowisk dowodzenia należy przestrzegać określonych wymogów, które muszą być spełnione pod względem stacjonarnej infrastruktury telekomunikacyjnej pozwalającej na przygotowanie sieci łączności stanowisk dowodzenia w poszczególnych miejscach dyslokacji z wykorzystaniem:

1) resortowych sieci telekomunikacyjnych;
2) sieci telekomunikacyjnych przedsiębiorstw telekomunikacyjnych;
3) dedykowanych sieci telekomunikacyjnych;
4) infrastruktury operatorów pocztowych;
5) wojskowej poczty polowej, poczty specjalnej podległej ministrowi właściwemu do spraw wewnętrznych oraz poczty kurierskiej podległej ministrowi właściwemu do spraw zagranicznych.

W systemie dowodzenia stanowiska dowodzenia są ważnym elementem, 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 ważnym elementem całego systemu dowodzenia.

W zależności od przygotowania infrastruktury terenowej oraz urządzenia miejsc pracy stanowiska dowodzenia można podzielić na:

- stacjonarne;
- stacjonarno-mobilne;
- mobilno-stacjonarne;
- mobilne.

Tabela 2.3

Rodzaj Stanowisk Dowodzenia

Szczebel dowodzenia	RODZAJ STANOWISK DOWODZENIA					
	SD	ZSD	TSD	WSD	PPD	PDO
Dywizja	X	X	X	X	X	
Brygada	X		X****	X**		X***
Pułk	X		X****			X
Batalion	X					X

** alternatywnie z PDO

*** część składowa SD

**** w miarę potrzeb i możliwości

2.5.1 Stanowisko dowodzenia (SD)

Na wszystkich szczeblach dowodzenia przeznaczone są do planowania działań operacyjnych i taktycznych oraz do bezpośredniego dowodzenia wojskami i stanowią zasadnicze miejsca pracy dowódcy i jego sztabu. Na stanowisku dowodzenia powinny być zorganizowane następujące elementy:

- łączność dowodzenia ze wszystkimi elementami ugrupowania taktycznego (operacyjnego) oraz z WSD i PPD;
- łączność z przełożonym i sąsiadami;
- ciągłe przygotowywanie informacji potrzebnych dowódcy do oceny sytuacji i podejmowania decyzji;
- przygotowywanie planów i rozkazów;
- koordynację prowadzenia rozpoznania i analizę informacji rozpoznawczych ze wszelkich dostępnych źródeł;
- organizację i koordynację wsparcia ogniowego;
- koordynację potrzeb zabezpieczenia logistycznego;
- przegotowywanie przesyłanie meldunków do przełożonego;
- dowodzenie wojskami i sterowanie środkami rażenia w toku działań;
- nadzór nad realizacją zadań;
- planowanie kolejnych działań operacyjnych.

2.5.2 Zapasowe stanowisko dowodzenia (ZSD)

Organizowane są w celu zapewnienia ciągłości i trwałości dowodzenia wojskami oraz przejęcia dowodzenia w wypadku obezwładnienia SD. ZSD nie ujawniają swojej działalności, gdy dowodzenie odbywa się z SD. Zajmują się głównie monitorowaniem rozwoju sytuacji, pozyskiwaniem dokumentów dowodzenia opracowanych na SD. Struktura organizacyjna ZSD powinna być taka, aby zapewnić realizację powyższych zadań. O wielkości obsady operacyjnej decyduje dowódca danego szczebla dowodzenia.

2.5.3 Tyłowe stanowisko dowodzenia (TSD)

Organizowane są w celu zapewnienia realizacji funkcji dowodzenia w obszarze tyłowym oraz sytuacji, gdy nie organizuje się ZSD, podtrzymania zasadniczych funkcji dowodzenia w ograniczonym czasie w wypadku obezwładnienia SD. Zajmują

się głównie koordynacją wsparcia personalnego i zabezpieczenia logistycznego, monitorowaniem rozwoju sytuacji w obszarze sił głównych, pozyskiwaniem dokumentów dowodzenia opracowanych na SD oraz realizacją planu działania w obszarze tyłowym.

2.5.4 Wysunięte stanowisko dowodzenia (WSD)

Rozwija się okresowo, stosownie do potrzeb w celu zapewnienia dowódcy bezpośredniego wglądu w sytuację i skrócenia czasu reakcji w relacjach dowodzenia podległymi wojskami w decydujących fazach operacji. Obsada operacyjna tych stanowisk wydzielana jest z SD w zależności od potrzeb dowodzenia i decyzji dowódcy.

Powinny one zapewnić:

- nadzór nad prowadzonymi działaniami bojowymi;
- nadzór i koordynację manewru wsparcia ogniowego;
- koordynację wsparcia powietrznego i obrony przeciwlotniczej;
- przekazywanie potrzeb zabezpieczenia logistycznego do SD;
- możliwość szybkiej zmiany rejonu rozmieszczenia stanowisk;
- ciągłą łączność z podległymi wojskami, głównym, zapasowym i tyłowym SD oraz z przełożonym i sąsiadami.

2.5.5 Punkt dowódczo-obserwacyjny (PDO)

Organizuje się w zależności od potrzeb, na szczeblu brygada, pułk, batalion w celu zapewnienia dowódcy bezpośredniego wglądu w sytuację oraz skrócenia czasu reakcji w relacjach dowodzenia podległymi pododdziałami.

2.5.6 Powietrzny punkt dowodzenia (PPD)

Stanowią element składowy SD i wykorzystywane są do zapewnienia dowodzenia w czasie: przemieszczania się dowódcy, przegrupowania związków operacyjnych i taktycznych, wyprowadzania wojsk z rejonów zmasowanych uderzeń przeciwnika.

2.6 Charakterystyka operatorów telekomunikacyjnych o szczególnym znaczeniu

Tak jak zostało to przedstawione wcześniej system obronny Rzeczypospolitej Polskiej oparty jest między innymi o system dowodzenia siłami zbrojnymi. System dowodzenia siłami zbrojnymi to zbiór wielu elementów niezbędnych do prawidłowego dowodzenia, jednym z istotnych elementów zgodnie z tematem pracy autora jest stacjonarna sieć teleinformatyczna sił zbrojnych Rzeczypospolitej Polskiej. Organizacja sieci teleinformatycznej w czasie pokoju, kryzysu i zagrożenia militarnego państwa regulowana jest wieloma aktami prawnymi (Zbiór dokumentów formalno – prawnych – **zał. 2**) w postaci ustaw, rozporządzeń oraz wytycznych właściwych sobie ministrów. Zgodnie z rozporządzenie Rady Ministrów (Dz. U. 2007 r. Nr 214, poz. 1571) został opracowany wykaz przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym podporządkowanych organom organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa przez **ministra właściwego do spraw łączności.**

Wojskowy System Telekomunikacyjny jest to zespół węzłów łączności, węzłów telekomunikacyjnych, stacji i samodzielnych urządzeń łączności i informatyki połączonych ze sobą w ściśle określony sposób torami transmisyjnymi wraz z urządzeniami zwielokratniającymi, komutacyjnymi, końcowymi, wzmacniakowymi, regenerującymi, łączności specjalnej, sprzętem specjalistycznym i pomocniczym oraz całą infrastrukturą zabezpieczenia logistycznego i bojowego, współpracujący ze sobą według wcześniej opracowanych i przyjętych zasad oraz procedur.

System łączności resortu Obrony Narodowej zorganizowany jest zgodnie z potrzebami systemu dowodzenia i współdziałania. Głównym i zasadniczym zadaniem systemu jest zapewnienie przekazywania informacji w relacjach dowodzenia i współdziałania. Na szczeblu strategicznym łączność organizowana jest w całości w oparciu o system stacjonarny. Dotyczy to zarówno części transmisyjnej jak i węzłów łączności obsługujących stanowiska dowodzenia na poziomie strategicznym.

Na podstawie przeprowadzonych badań, wykorzystując do tego celu metody teoretyczne takie jak: analizę, syntezę, porównanie, uogólnienie, abstrahowanie i wnioskowanie, wyselekcjonowano oraz opisano dwóch kluczowych operatorów współpracujących z Ministerstwem Obrony Narodowej. Część transmisyjną systemu

łączności resortu tworzą eksploatowane trakty cyfrowe dzierżawione od TP S.A., EXATEL oraz innych operatorów. W okresie osiągania WSGB oraz na czas wojny system łączności wzmacniany jest wydzielanym potencjałem z zasobów TP S.A., EXATEL i innych operatorów. Węzły łączności obsługujące stanowiska dowodzenia wyższych szczebli są zawczasu przygotowanymi obiektami telekomunikacyjnymi, uzupełnianymi w urządzenia końcowe. Środki mobilne (Wykaz sprzętu mobilnego – **zał. 5**) są środkami rezerwującymi niektóre elementy stacjonarnego systemu łączności. W razie potrzeby tworzą odrębne relacje dalekosiężne lub obejścia uszkodzonej w dużej skali sieci stacjonarnej na szczeblu strategicznym.

Za pomocą środków mobilnych rozwijane mogą być odrębne sieci w wybranym rejonie kraju, np. na obszarze o słabo rozwiniętej infrastrukturze telekomunikacyjnej. Środki węzłowe służyć mogą do doraźnego rozwijania polowych węzłów łączności stanowisk dowodzenia w operacyjnie uzasadnionych sytuacjach lub do dokompletowywania węzłów stacjonarnych po wystąpieniu strat spowodowanych oddziaływaniem przeciwnika lub klęsk żywiołowych. Na terenie kraju rozmieszczenie wojskowych węzłów łączności jest nierównomierne. Dlatego też przy planowaniu systemu łączności na potrzeby obronności państwa brane są pod uwagę również węzły telekomunikacyjne operatorów publicznych.

Zasadniczym zadaniem Wojskowego Systemu Telekomunikacyjnego jest zapewnienie terminowej, wiernej i skrytej łączności dla potrzeb dowodzenia wojskami i sterowania środkami rażenia, współdziałania i powiadamiania (ostrzegania). Jest niezwykle złożoną strukturą organizacyjną, znajdującą się aktualnie w fazie intensywnej rekonfiguracji, funkcjonującą na zasadach określonych w Rozporządzeniu Ministra Obrony Narodowej z dn. 12.10.2005 r. w sprawie szczegółowych warunków wykonywania działalności telekomunikacyjnej (Dz. U. Nr 207 z 2005 r. poz. 1736). Od początku 2006 r. trwają intensywne prace zmierzające do wdrożenia nowej struktury organizacyjnej Wojskowego Systemu Telekomunikacyjnego, umożliwiającej sprawne i dynamiczne zarządzanie posiadanym potencjałem telekomunikacyjnym w czasie rzeczywistym z jednego powołanego w tym celu ośrodka tj. Centrum Zarządzania Systemami Teleinformatycznymi resortu obrony narodowej.

Aby wskazać jakie wyzwania stoją przed powołaną instytucją konieczne staje się scharakteryzowanie pojęcia zarządzania.

Terminy „zarządzanie" i „zarządzanie sieciami" obejmują zagadnienia związane z eksploatacją, administrowaniem, utrzymaniem i uruchamianiem (ang. *Operations, Administration,, Maintenance, and Provisioning*) sieci telekomunikacyjnych i teleinformatycznych.

Opracowywane przez ITU-T (ang. *International Telecommunication Union-Telecommunication Standardization Sector*) zalecenia dotyczące zarządzania systemami otwartymi zawierają między innymi architekturę sieci zarządzania telekomunikacją TMN (ang. *Telecommunications Management Network*), styki między składnikami tej architektury oraz usługi i funkcje zarządzania siecią telekomunikacyjną.

W zaleceniach tych wyodrębniono pięć funkcjonalnych obszarów zarządzania:

- **zarządzanie uszkodzeniami** (ang. *Fault Management*);
  Polega ono na wykrywaniu, izolowaniu i naprawie nieprawidłowo funkcjonujących (uszkodzonych) zasobów;
- **zarządzanie konfiguracją** (ang. *Configuration Management*);
  Polega ono na identyfikowaniu (definiowaniu) zarządzanych zasobów i ich wzajemnych powiązań oraz sterowaniu tymi zasobami (eksploatacja);
- **zarządzanie rozliczeniami** (ang. *Accounting Management*);
  Polega ono na określaniu kosztów korzystania z zasobów na podstawie ustalonych taryf;
- **zarządzanie wydajnością** (ang. *Performance Management*);
  Polega ono na przeprowadzaniu oceny funkcjonowania zasobów z punktu widzenia efektywności ich wykorzystania;
- **zarządzanie bezpieczeństwem** (ang. *Security Management*).
  Polega ono na zapewnianiu ochrony zarządzanych zasobów i danych. Do zadań zarządzania bezpieczeństwem należy także prowadzenie dzienników bezpieczeństwa (ang. *Security Logs*), w których przechowywane są meldunki i informacje dotyczące bezpieczeństwa zasobów i danych.

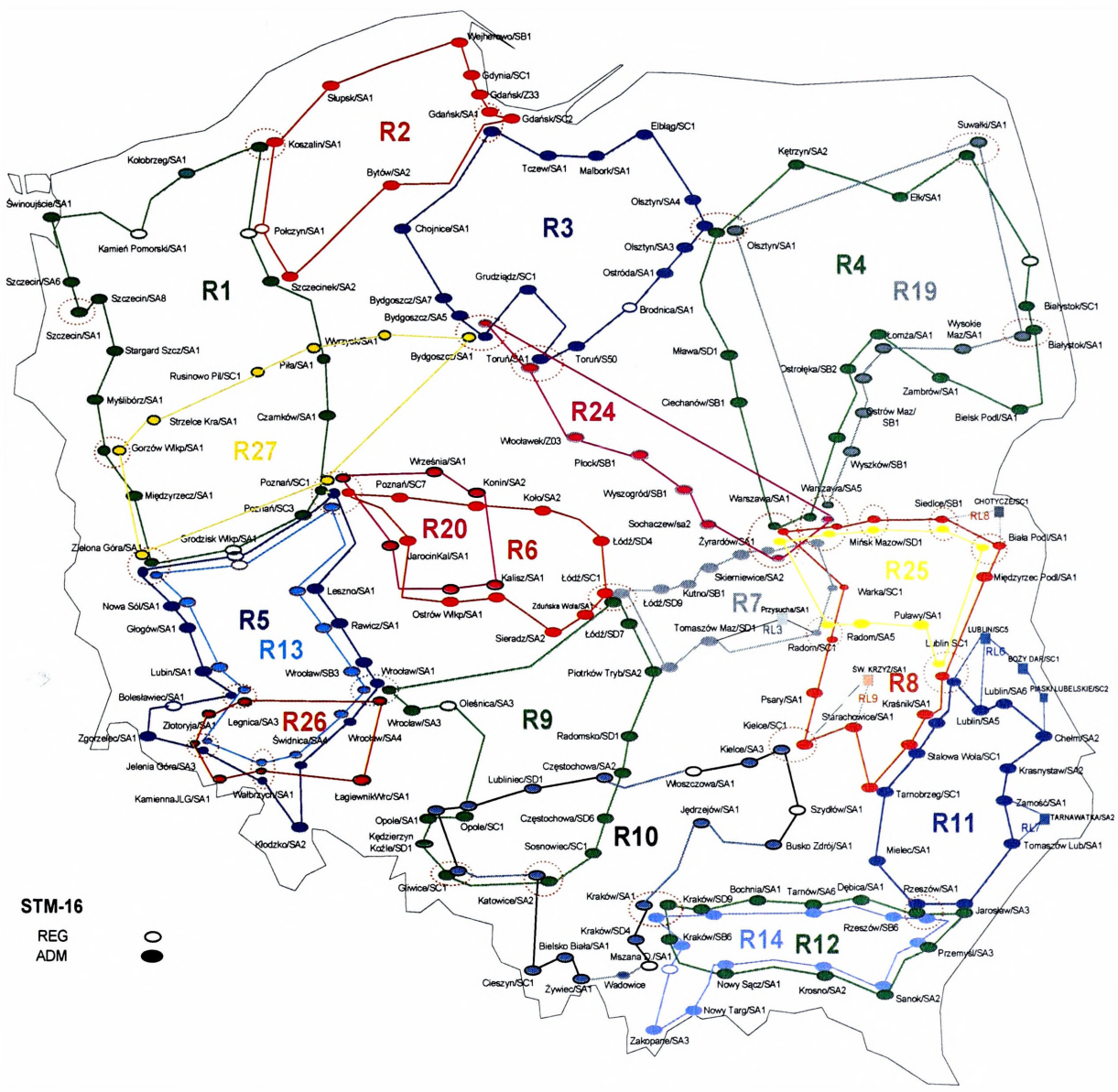
Poniżej została przedstawiona charakterystyka dwóch operatorów telekomunikacyjnych, których udział w tworzeniu sieci teleinformatycznej w siłach zbrojnych na potrzeby budowania systemu dowodzenia ma kluczowe znaczenie.

2.6.1 Telekomunikacja Polska S.A.

Telekomunikacja Polska S.A. obecnie jest największym operatorem krajowym. Obecnie znajduje się w rękach obcego kapitału, jednak w dalszym ciągu sprzedaje usługi oraz ściśle współpracuje z Ministerstwem Obrony Narodowej na rzecz obronności kraju. Posiada bardzo rozległą sieć teleinformatyczną w relacjach krajowych i międzynarodowych. Obszar Polski jest pokryty szkieletową siecią łączy telekomunikacyjnych oraz regionalnymi sieciami łączy telekomunikacyjnych. Łącza te są własnością resortu ON lub też są dzierżawione od przedsiębiorców telekomunikacyjnych. Łącza własne resortu ON są administrowane przez wojskowe węzły łączności.

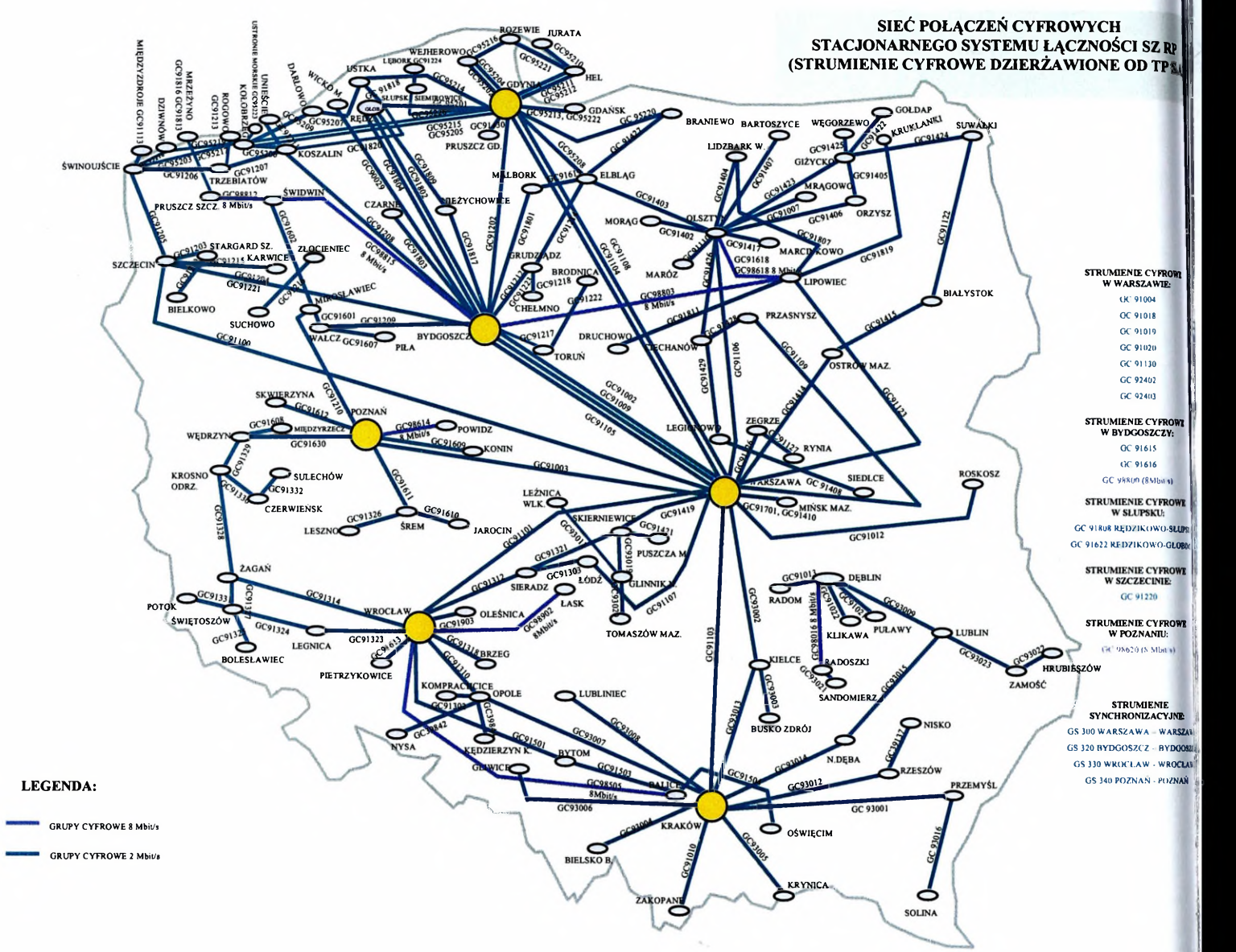
Sieć łączy telekomunikacyjnych w obszarze odpowiedzialności wojskowych węzłów łączności realizowana jest na bazie własnych i dzierżawionych zasobów sieci teletechnicznych MON i przedsiębiorców telekomunikacyjnych, oraz urządzeń stacjonarnych, radiowych i radioliniowych systemu teletransmisyjnego.

System teletransmisyjny stanowi istotny składnik Wojskowego Systemu Telekomunikacyjnego, który obejmuje zespół wyspecjalizowanych linii telekomunikacyjnych i urządzeń teletransmisyjnych rozwiniętych na danym obszarze. W systemie teletransmisyjnym zawarty jest potencjał typowych kanałów telekomunikacyjnych, rozdysponowany do eksploatacji w ramach poszczególnych wyspecjalizowanych sieci usługowych.



Rys. 2.13 *Ogólnopolska sieć teleinformatyczna firmy TP S.A.*

Źródło: Materiał reklamowe firmy



Rys. 2.14 *Sieć połączeń cyfrowych stacjonarnego systemu łączności sił zbrojnych dzierżawionych od firmy TP S.A.*

Źródło: Strategia informatyzacji Sił Zbrojnych RP

2.6.2 EXATEL S.A.

EXATEL SA jest jednym z największych operatorów telekomunikacyjnych w Polsce. Oferuje swoim Klientom kompleksowe rozwiązania i usługi teleinformatyczne - głosowe, internetowe, transmisji danych, a także hosting i kolokację. Ponad 15-letnie doświadczenie firmy na rynku, szerokie kompetencje

oraz rozwinięta infrastruktura techniczna w postaci nowoczesnej sieci światłowodów o długości ponad 19 tysięcy kilometrów gwarantują najwyższą jakość świadczonych usług oraz bezpieczeństwo biznesu. EXATEL SA powstał z połączenia dwóch polskich operatorów telekomunikacyjnych (2004 r.) o ponad 10-letniej tradycji: Tel-Energo i Telbanku, specjalizujących się w obsłudze wymagających i strategicznych branż, w tym operatorskiej, bankowo-finansowej i energetycznej. Osiągnięty efekt synergii umożliwił poszerzenie oferty spółki, zwiększenie potencjału technologicznego oraz pełniejsze wykorzystanie wiedzy i umiejętności pracowników. Dziś EXATEL to poważny, doświadczony oraz godny zaufania partner biznesowy. Gwarantuje najwyższą jakość połączeń, profesjonalną obsługę i dostęp do szerokiego wachlarza usług teleinformatycznych. Nowoczesna sieć teletransmisyjna Exatel powstała w wyniku połączenia infrastruktury telekomunikacyjnej Tel-Energo i Telbanku. Jest drugą co do wielkości platformą telekomunikacyjną w Polsce, gwarantującą najwyższy poziom jakości i bezpieczeństwa oferowanych usług.

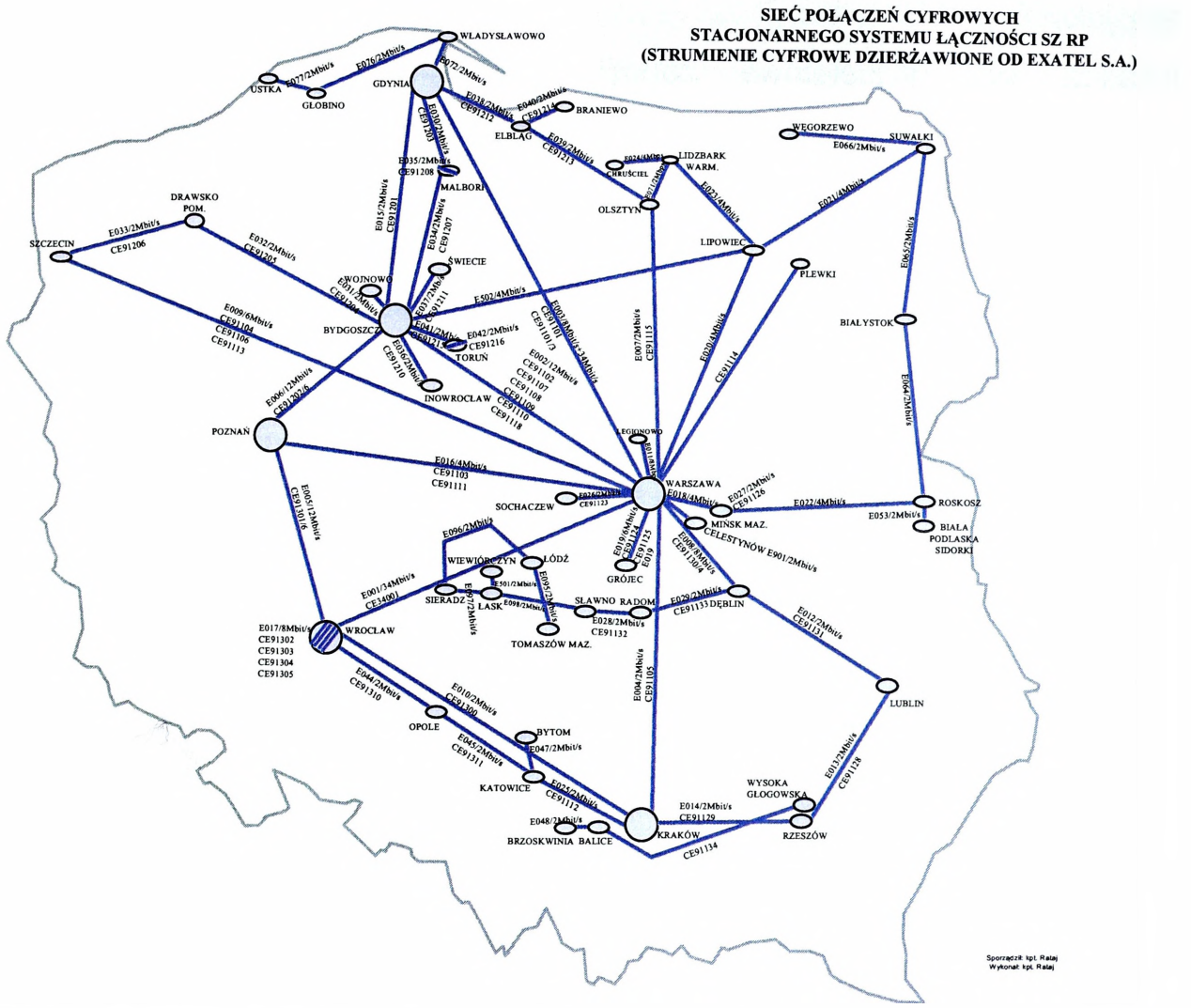
Ogólnopolska sieć teleinformatyczna wyróżnia się:

- długością ponad 19.000 km obejmującą około 400 miast i miejscowości;
- pokryciem wszystkich obszarów biznesowych w Polsce;
- przepustowością sieci szkieletowej sięgającą do 320 Gbit/s;
- połączeniem z sieciami internetowymi największych operatorów polskich i zagranicznych, umożliwiającym najszybszy dostęp do wszystkich zasobów globalnej sieci Internet;
- punktami styku z operatorami na granicach Polski zachodniej, południowej i wschodniej, umożliwiającymi tranzyt i terminowanie ruchu przechodzącego przez centralną Euro.

Sieć teletransmisyjną Exatel S.A. charakteryzuje niezawodność, elastyczność i możliwość zaspokojenia nawet najbardziej wyspecjalizowanych wymagań Klientów. Exatel S.A. stale rozbudowuje swoją sieć szkieletową i sieci miejskie w oparciu o sprzęt i oprogramowanie renomowanych producentów krajowych i zagranicznych. Wykorzystujemy najnowocześniejsze rozwiązania dostępowe oraz rozwiązania z zakresu transmisji danych i głosu.

Rys. 2.15 *Ogólnopolska sieć teleinformatyczna firmy EXATEL S.A.*

Źródło: Materiał reklamowe firmy



Rys. 2.16 *Sieć połączeń cyfrowych stacjonarnego systemu łączności sił zbrojnych dzierżawionych od firmy EXATEL S.A.*

Źródło: Strategia informatyzacji Sił Zbrojnych RP

EXATEL oferuje łącza cyfrowe o poniższych przepustowościach oraz wielokrotności.

Wykaz łączy EXATEL Tabela 2.4

Przepustowość	**Interfejs**	**Charakterystyka techniczna**
2 Mbit/s	2 Mbit/s, G703	120 lub 75 Ohm elektryczny
34 Mbit/s	34 Mbit/s, G703	75 Ohm elektryczny lub optyczny w STM-1
155 Mbit/s	155 Mbit/s, G703 155 Mbit/s, G957	75 Ohm elektryczny jednomodowy optyczny
622 Mbit/s	622 Mbit/s, G957	jednomodowy optyczny

Usługa dzierżawy łączy jest dostępna w ogólnopolskiej sieci światłowodowej o długości ponad 11 000 kilometrów. Ogólnokrajowy zasięg sieci umożliwia dostarczanie usługi poprzez węzły dostępowe znajdujące się we wszystkich większych miastach w Polsce.

Wysoką jakość oraz niezawodność transmisji gwarantuje w pełni redundantna i nowoczesna sieć szkieletowa zbudowana w strukturze pierścieniowej z zastosowaniem cyfrowej hierarchii synchronicznej SDH. W przypadku awarii drogi podstawowej funkcje sieciowe zapewniają przesyłanie danych drogami zastępczymi eliminując przerwy w komunikacji.

Szkielet sieci jest oparty na systemie DWDM, umożliwiającym uzyskanie przepływności do 320 Gbit/s.

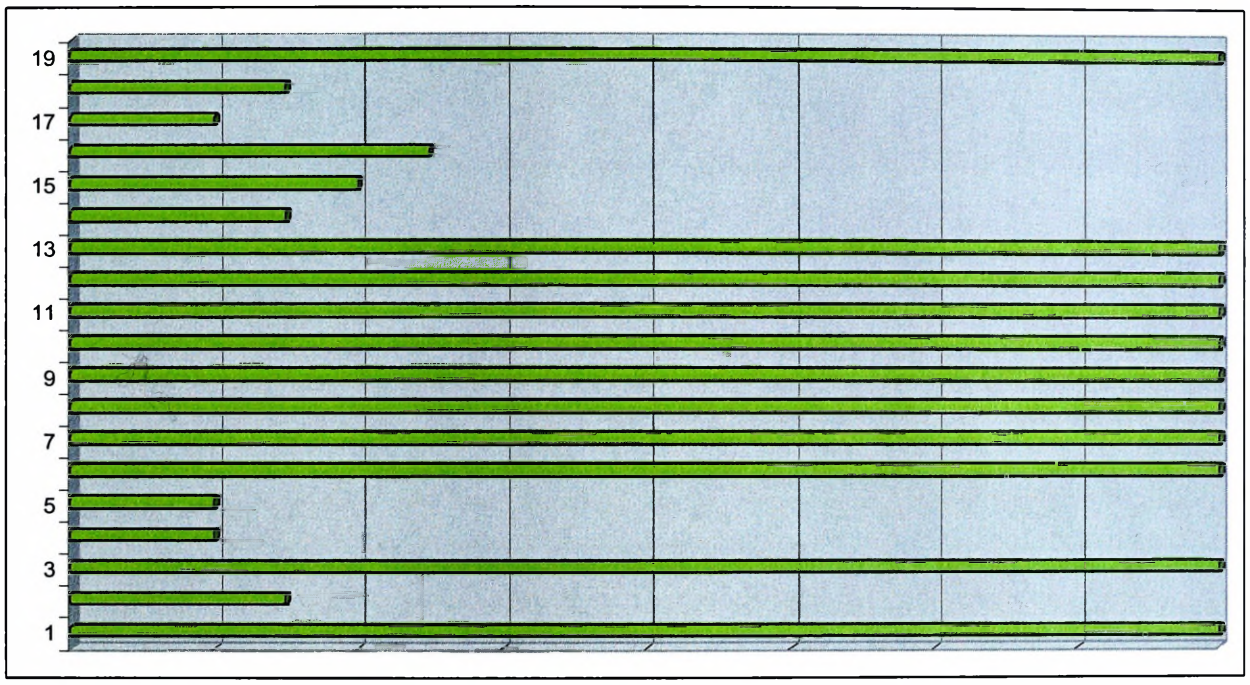
2.7 Synteza wyników badań

Po przeprowadzeniu analizy oraz syntezy badanych dokumentów oraz aktów prawnych próba odpowiedzi na dwa zasadnicze problemy badawcze ściśle związane z tym rozdziałem, czyli ***jakie wymagania i potrzeby w zakresie usług teleinformatycznych generuje system dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej w czasie pokoju, kryzysu i zagrożenia militarnego państwa oraz jaka jest rola stacjonarnej sieci teleinformatycznej w realizacji zadań łączność w toku dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej***, jest bardzo złożona, jednak w trakcie dysertacji literatury przedmiotu oraz badań sondażowych wśród kadry zawodowej oraz pracowników wojska Departamentu Informatyki i Telekomunikacji, Centrum Zarządzania Systemami Teleinformatycznymi oraz Centralnego Węzła Łączności, w celu zapewnienia skutecznej realizacji procesu dowodzenia w czasie pokoju, kryzysu oraz zagrożenia militarnego państwa z punktu widzenia użytkowników systemu teleinformatycznego, niezbędna jest realizacja następujących wymagań i potrzeb na usługi telekomunikacyjne:

- **telefonia;**
- **transmisja faksów;**
- **telekonferencja dla wybranych grup użytkowników;**
- **transmisja danych między użytkownikami;**
- **wyszukiwanie informacji,** w tym:
    - dostęp do centralnych baz danych,
    - dostęp do lokalnych baz danych,
    - dostęp do różnych zasobów danych z wykorzystaniem Internetu.
- **multimedia** (w tym np. wideokonferencja),

- **inne** (w tym np. szeroka gama usług sieci ISDN oraz usługi związane z tzw. sieciami inteligentnymi),

Wyżej wymienione usługi zostały wyselekcjonowane na podstawie badań sondażowych (Wyniki badań dotyczących określenia wymagań i potrzeby w zakresie usług teleinformatycznych które generuje system dowodzenia siłami zbrojnymi – **zał. 3**) które z macierzy 2.1 przetransponowano na wykres zamieszczony na rysunku 2.17.



Rys. 2.17 *Ilościowy układ odpowiedzi na pytania, które z wymienionych usług teleinformatycznych uważa Pani/Pan za potrzebne w celu zapewnienia właściwego funkcjonowania systemu dowodzenia siłami zbrojnymi*
Źródło: opracowanie własne na podstawie zebranych wyników

Powyższe wymagania i potrzeby realizowane będą w oparciu o następujące sieci teleinformatyczne o zasięgu lokalnym oraz globalnym:

- sieć ZASTRZEŻONA MIL-LAN ,w której osadzone będą Zintegrowane Systemy Dowodzenia SZAFRAN, DUNAJ, ŁEBA;
- sieć NATO SECRET PL_NOAN, MCCIS, ICC;
- sieć TAJNA SEC-LAN (po wdrożeniu do SZ RP);
- sieć JAWNA Internet.

Autor na podstawie wyników przeprowadzonych badań stwierdził, że organizacja stacjonarnej sieci teleinformatycznej jest priorytetowym elementem prawidłowego funkcjonowania całego systemu dowodzenia siłami zbrojnymi i dlatego sieć teleinformatyczna powinna sprostać odpowiednim zadaniom, czyli do roli stacjonarnej sieci teleinformatycznej autor zalicza następujące elementy składowe:

- zapewnienie swobodnego wielokierunkowego przepływu informacji pomiędzy wszystkimi elementami systemu dowodzenia;
- zapewnienie przepływu informacji wewnątrz poszczególnych elementów systemu dowodzenia;
- posiadanie w swojej strukturze interfejsów do współpracy z publicznymi stacjonarnymi i ruchomymi (mobilnymi) operatorami telekomunikacyjnymi – umożliwienie użycia publicznych systemów teleinformatycznych dla potrzeb systemu wojskowego;
- zapewnienie warstwy transportowej dla systemów teleinformatycznych funkcjonujących na potrzeby procesu dowodzenia oraz wojskowych systemów mobilnych;
- dostarczanie narzędzi wspomagających proces dowodzenia (ZSyD, dedykowane sieci informatyczne);
- zapewnienie dostępu do wiarygodnych i aktualnych danych niezbędnych do zabezpieczenia procesu dowodzenia.

Podsystemem teleinformatycznym działającym na potrzeby obronności państwa przyjęło się nazywać zbiór elementów funkcjonalnych wydzielanych z zasobów systemu telekomunikacyjnego państwa, powiązanych ze sobą w sposób umożliwiający świadczenie usług telekomunikacyjnych o wymaganej jakości. Sieć teleinformatyczna, w zależności od typu sytuacji kryzysowej i jej lokalizacji, może być wydzielana z zasobów publicznych systemów teleinformatycznych, operatorów prywatnych lub organizowana w oparciu o urządzenia teleinformatyczne stanowiące wyposażenie ewidencyjne sił zbrojnych.

Z uwagi na nieokreśloność i brak obiektywnych danych dotyczących organizacji systemów teleinformatycznych dla potrzeb obronności państwa – wynikających z nieokreślonego rodzaju zagrożenia oraz miejsca jego wystąpienia – nie jest możliwe określenie ich docelowej struktury techniczno – organizacyjnej.

System teleinformatyczny powinien obejmować obszar całego kraju. Wymaganie to powinno być realizowane etapami, począwszy od szczebla centralnego poprzez pośrednie szczeble kierowania do zapewnienia wojennego systemu dowodzenia SZ RP. Konieczne jest osiągnięcie stanu wyprzedzającego gotowość systemu teleinformatycznego w stosunku do systemu kierowania obroną państwa i działania wojsk.

Skład i struktura powinny odpowiadać składowi i strukturze systemu kierowania państwem w czasie pokoju, kryzysu i wojny oraz strukturze dowodzenia SZ RP w tym ujmować rejony stanowisk dowodzenia jednostek organizacyjnych SZ RP rozwijanych w DMP i ZMP.

Konfiguracja (rozmieszczenie) węzłów powinna być taka, by każda zmiana systemu dowodzenia nie wymagała rekonfiguracji tego systemu.

W systemie powinny występować węzły o jednolitym przeznaczeniu, tzn. węzły końcowo-tranzytowe spełniające również funkcję węzłów dostępowych dla mobilnych środków łączności MON. Węzły stanowisk kierowania i dowodzenia w ZMP przeznaczone do wykorzystania w czasie wojny i w sytuacjach kryzysowych powinny być utrzymywane w pełnej gotowości do użycia.

Na podstawie przeprowadzonych badań można założyć kształt sieci teleinformatycznej na poziomie strategicznym. Biorąc pod uwagę wymagania dla systemu dowodzenia w czasie pokoju, kryzysu i wojny można założyć, że przepływność sieci teleinformatycznej powinna zabezpieczyć przepływność ponad 1Gbit/s, także ze względu na możliwości sprzętu polowego. We wszystkich przypadkach Regionalne Węzły Łączności dzierżawią od operatorów publicznych trakty o przepływności 2Mbit/s, co w żadnym wypadku nie zabezpiecza potrzeb związanych z organizacją sieci teleinformatycznych na Stanowisku Dowodzenia szczebla strategicznego. Kontynuując poprzednią myśl odnośnie potrzeb należy także wspomnieć, że na dzień dzisiejszy siły zbrojne nie dysponują odpowiednimi mediami do organizacji sieci teleinformatycznej, zarówno stacjonarnej jak i polowej. Przedstawiona organizacja sieci teleinformatycznych na SD szczebla strategicznego wymaga dodatkowych urządzeń polowych takich jak: aparatownie troposferyczne, urządzenia satelitarne oraz dobrze zorganizowana stacjonarna sieć teleinformatyczna o odpowiedniej przepływności.

Realizacja powyższych przedsięwzięć wynika z zakresu kompetencyjnego Ministra Obrony Narodowej, określonego w „Rozporządzeniu Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym”[19].

[19] Wykaz wszystkich aktów prawnych opisujący problematykę obronności oraz związanych z tym obszarów działalności telekomunikacyjnej zawarto w zał. 2 do niniejszego opracowania.

3. STRUKTURA ORGANIZACYJNO-TECHNICZNA STACJONARNEJ SIECI TELEINFORMATYCZNEJ UŻYWANEJ PRZEZ SIŁY ZBROJNE

Celem badań, których wyniki przedstawiono w tym rozdziale, była próba odpowiedzi na dwa pytania: ***w jakim stopniu aktualne regulacje prawne określają zasady współpracy operatorów telekomunikacyjnych z Siłami Zbrojnymi oraz w jakim stopniu zmiany organizacyjno – techniczne w obszarze stacjonarnej sieci teleinformatycznej Sił Zbrojnych, podjęte w latach 1995 – 2005, wpłynęły na realizację potrzeb dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej w czasie pokoju, kryzysu i zagrożenia militarnego państwa***. Aby osiągnąć powyższy cel, autor dokonał szerokiej analizy literatury przedmiotu i aktów prawnych dotyczących badanego obszaru, a także analizy a następnie syntezy informacji zebranych w wyniku przeprowadzonego sondażu diagnostycznego techniką wywiadu z przedstawicielami, którzy w swoich zakresach działań mają zapisane zadania związane z pełnieniem obowiązków organizatora wojskowego systemu teleinformatycznego, w świetle aktualnych regulacji prawnych. Analizie poddano także elementy struktury organizacyjno-technicznej sieci teleinformatycznej, użytkowanej przez Siły Zbrojne Rzeczypospolitej Polskiej na terenie kraju. (Arkusz wywiadu dotyczący identyfikacji struktur organizacyjno – technicznych stacjonarnej sieci teleinformatycznej używanej przez siły zbrojne – **zał. 6**)

3.1 Organy zarządzające stacjonarną siecią teleinformatyczną SZ RP – umiejscowienie, struktura i zadania

Wojskowy system teleinformatyczny podlega w szczególności procesom planowania, organizowania i realizacji przedsięwzięć umożliwiających kierowanie państwem w warunkach zagrożenia bezpieczeństwa państwa i w czasie wojny lub dowodzenie Siłami Zbrojnymi Rzeczypospolitej Polskiej.

Wymienione procesy powinny być realizowane poprzez[20]:

- precyzowanie potrzeb w zakresie łączności;

[20] Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2005 r. w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa, §5 Dz.U. z 2004 r. Nr 180 poz. 1855.

- analizę możliwości przedsiębiorców telekomunikacyjnych i operatorów pocztowych w zakresie ich wykorzystania na potrzeby obronne państwa;
- planowanie wykorzystania istniejących systemów łączności na potrzeby obronne państwa;
- wytypowanie osób odpowiedzialnych za planowanie, wdrażanie, zarządzanie i eksploatację obronnych systemów łączności;
- utworzenie bazy danych o przedsiębiorcach telekomunikacyjnych i operatorach pocztowych, niezbędnej do przygotowania i wykorzystania obronnych systemów łączności;
- precyzowanie standardów wyposażenia stanowisk kierowania;
- wykonywanie inwestycji;
- wykonywanie inwestycji postulowanych.

Ponadto przez:

- opracowywanie zasad współpracy sieci przedsiębiorców telekomunikacyjnych z resortowymi sieciami telekomunikacyjnymi;
- dostosowywanie obiektów i infrastruktury telekomunikacyjnej przedsiębiorców telekomunikacyjnych do współpracy z ruchomymi urządzeniami telekomunikacyjnymi zgodnie z potrzebami określanymi w szczególności przez Ministra Obrony Narodowej lub ministra właściwego do spraw wewnętrznych;
- wskazywanie potrzeb w zakresie rozbudowy infrastruktury telekomunikacyjnej przedsiębiorców telekomunikacyjnych w ramach inwestycji postulowanych;
- zapewnianie bezpieczeństwa systemów łączności specjalnej;
- precyzowanie potrzeb w zakresie współdziałania operatorów pocztowych z wojskową pocztą polową, z pocztą specjalną podległą ministrowi właściwemu do spraw wewnętrznych oraz z pocztą kurierską podległą ministrowi właściwemu do spraw zagranicznych.

Z ramienia Ministra Obrony Narodowej, za realizację powyższych przedsięwzięć odpowiada organizator wojskowego systemu telekomunikacyjnego.

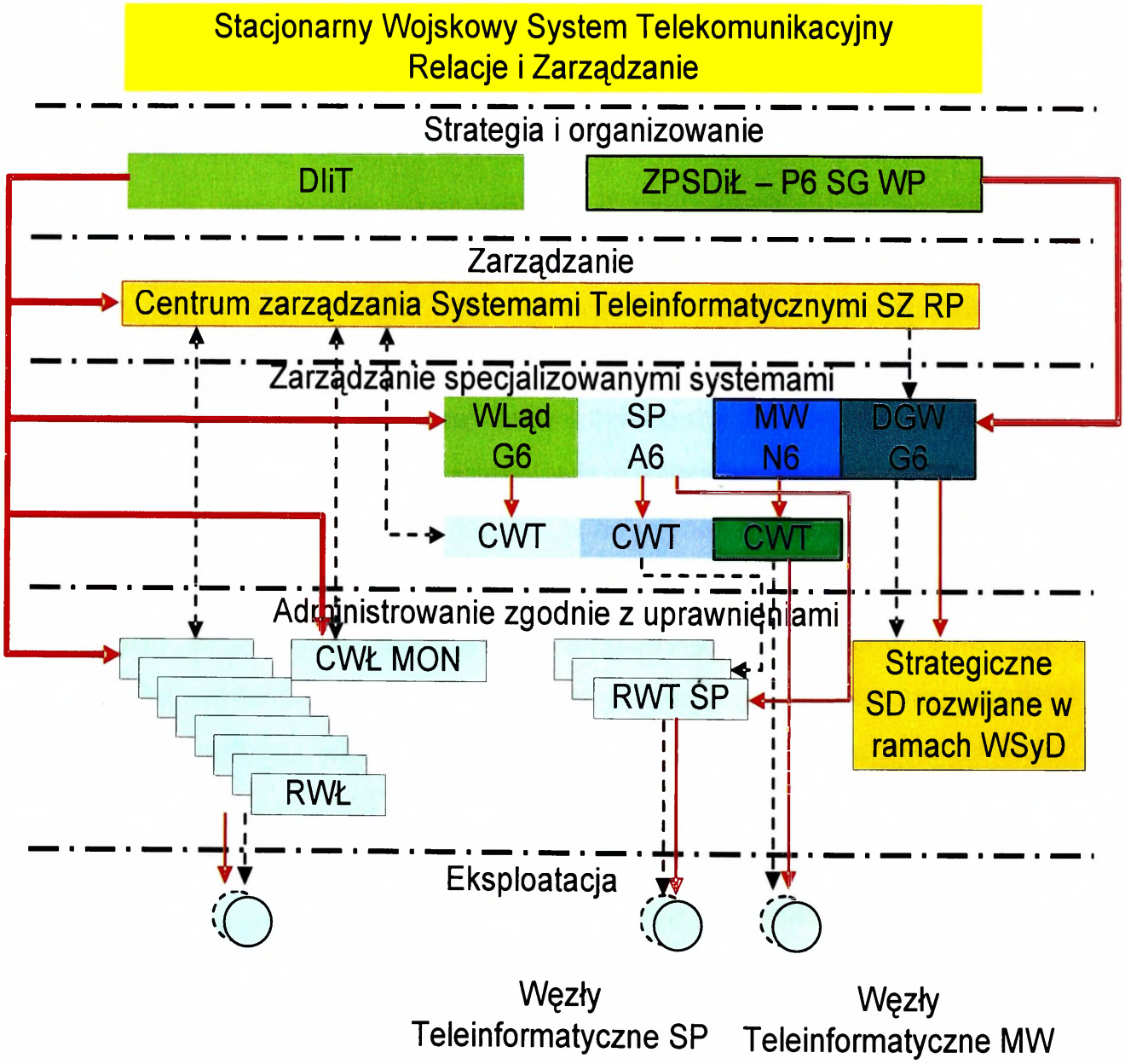
Organizatorem wojskowego systemu telekomunikacyjnego[21] jest komórka organizacyjna Ministerstwa Obrony Narodowej właściwa w zakresie normowania, kierowania, nadzorowania i koordynowania całokształtu zagadnień związanych

[21] Rozporządzenie Ministra Obrony Narodowej z dnia 12 października 2005 r. w sprawie szczególnych warunków wykonywania działalności telekomunikacyjnej, §2 pkt. 2.

z rozwojem, organizacją, funkcjonowaniem oraz rozbudową i modernizacją wojskowego systemu telekomunikacyjnego oraz wykorzystywaniem sieci telekomunikacyjnej operatorów publicznych dla potrzeb tego systemu.

Zgodnie z Zarządzeniem Nr 40/MON Ministra Obrony Narodowej z dnia 22 listopada 2006 r. w sprawie regulaminu organizacyjnego Ministerstwa Obrony Narodowej powołano dwie komórki organizacyjne mające w swoich zadaniach uprawnienia organizatora wojskowego systemu telekomunikacyjnego.

Pierwszą jest podległy bezpośrednio Ministrowi Obrony Narodowej, Departament Informatyki i Telekomunikacji (DIiT). Drugą Zarząd Planowania Systemów Dowodzenia i Łączności P-6, będący integralną komórką Sztabu Generalnego Wojska Polskiego.



Rys.3.1 *Schemat wzajemnych relacji i zarządzania w stacjonarnym systemie telekomunikacyjnym SZ RP*

Źródło: Opracowanie własne

3.1.1 Departament Informatyki i Telekomunikacji Ministerstwa Obrony Narodowej.

W myśl regulaminu będącego załącznikiem do zarządzenia Nr 40/MON z 22.11.2006 r.[22] – Departament Informatyki i Telekomunikacji planuje, nadzoruje, koordynuje i wytycza kierunki rozwoju informatyki i telekomunikacji w resorcie oraz pełni funkcję organizatora wojskowego systemu telekomunikacyjnego. Odpowiada za funkcjonowanie systemów informatycznych i telekomunikacyjnych w resorcie oraz za współpracę systemów resortowych z systemami NATO, UE oraz administracji publicznej. Jest komórką właściwą w zakresie określania standardów technologicznych dla systemów informatycznych i telekomunikacyjnych resortu oraz opracowywania i wdrażania aktów normatywnych, a także dokumentów regulujących procesy projektowania, wdrażania, funkcjonowania, użytkowania i utrzymania tych systemów.

Do zakresu zadań Departamentu należy:

- opracowywanie strategii informatyzacji resortu i nadzór nad jej realizacją;
- współpraca z organami administracji publicznej w zakresie opracowania i realizacji strategii informatyzacji państwa;
- wytyczanie kierunków rozwoju systemów informatycznych, infrastruktury telekomunikacyjnej, szkolenia specjalistycznego specjalistów informatyki i łączności oraz wdrażanie nowych technologii w tych obszarach;
- nadzór nad funkcjonowaniem systemów informatycznych i telekomunikacyjnych resortu oraz kierowanie działalnością administratorów systemów informatycznych w Urzędzie Ministra;
- opracowywanie jednolitej architektury organizacyjno-technicznej systemów informatycznych i telekomunikacyjnych w resorcie, w tym określanie norm oraz standardów technologicznych dla tych systemów oraz opracowywanie własnych lub uzgadnianie otrzymanych wymagań taktyczno-technicznych dla sprzętu i oprogramowania;
- wytyczanie kierunków rozwoju technologii informatycznych w Zautomatyzowanych Systemach Dowodzenia (ZSyD) i Kierowania Środkami Walki (KŚW) oraz nadzór i koordynacja nad ich wdrażaniem;

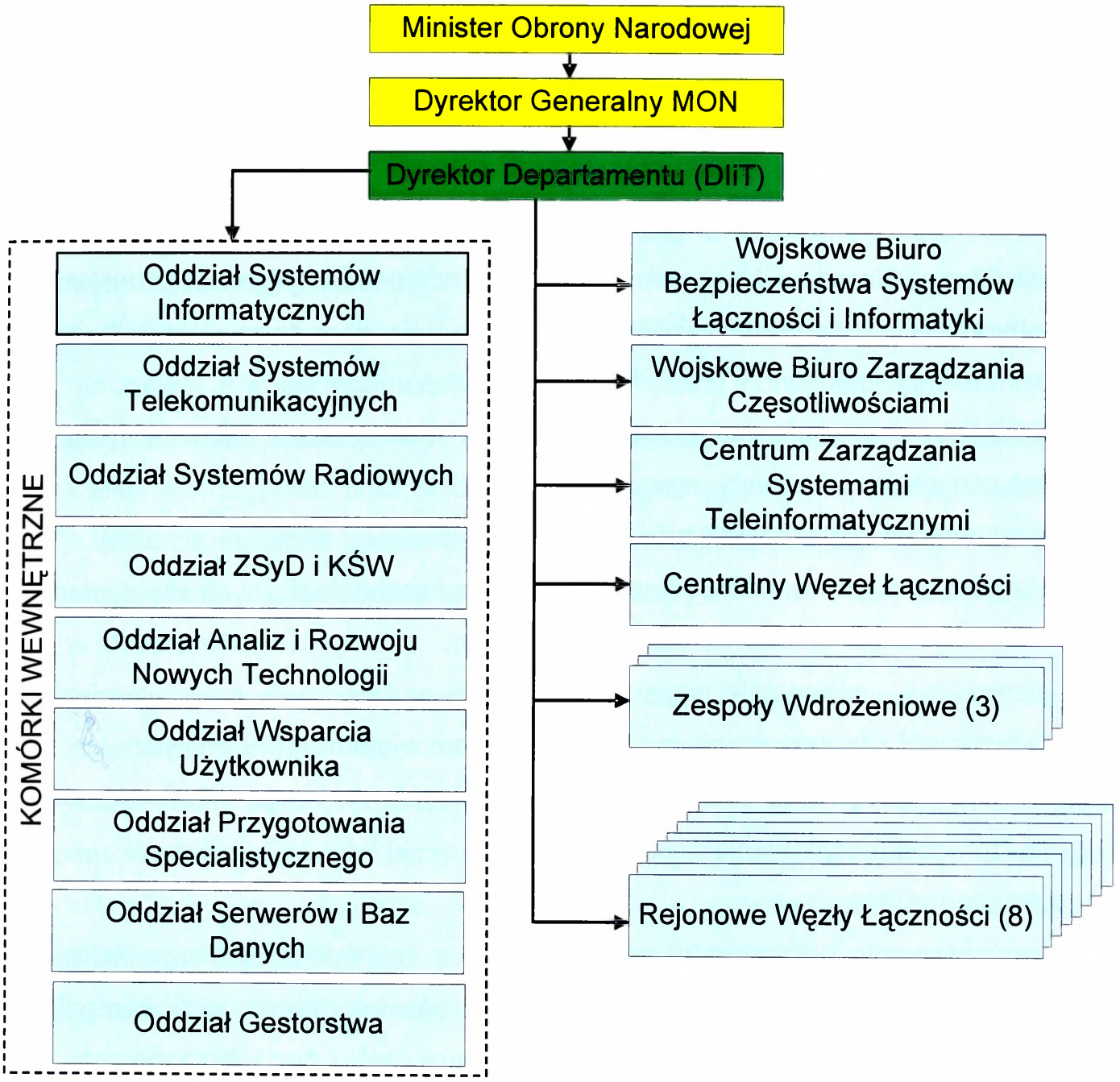
---

[22] Zarządzenie Nr 40/MON Ministra Obrony Narodowej z dnia 22 listopada 2006 r. w sprawie regulaminu organizacyjnego Ministerstwa Obrony Narodowej, Dziennik Urzędowy Ministra Obrony Narodowej z 2006 r. Nr 21 Poz. 269, 270, §23 ust.1.

- pełnienie funkcji organizatora wojskowego systemu telekomunikacyjnego oraz opracowywanie koncepcji jego rozwoju, w tym systemów ochrony kryptograficznej, bezpieczeństwa łączności i informatyki, a także koordynowanie oraz inicjowanie prac naukowo-badawczych i rozwojowo-wdrożeniowych w tym zakresie;
- koordynowanie i nadzorowanie działalności podporządkowanych jednostek organizacyjnych oraz organów wykonawczych informatyki i telekomunikacji w resorcie, w tym zabezpieczających Ministerstwo;
- planowanie i koordynowanie współpracy zagranicznej w zakresie odpowiedzialności Departamentu;
- inicjowanie, koordynowanie i nadzorowanie przedsięwzięć związanych z projektowaniem, budową, wdrażaniem i eksploatacją systemów informatycznych oraz technik symulacyjnych;
- realizowanie przedsięwzięć związanych z osiąganiem interoperacyjności technicznej i technologicznej w układzie narodowym, sojuszniczym i koalicyjnym w zakresie automatyzacji dowodzenia oraz systemów łączności i informatyki.

Departamentowi Informatyki i Telekomunikacji podlegają bezpośrednio Centrum Zarządzania Systemami Teleinformatycznymi (CZST), Centralny Węzeł Łączności MON (CWŁ MON) i osiem regionalnych węzłów łączności (RWŁ), Centrum Informatyki i Łączności Obrony Narodowej (CIiŁON), trzy Zespoły Wdrożeniowe (Warszawa, Bydgoszcz, Wrocław) Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki, Wojskowe Biuro Zarządzania Częstotliwościami (WBZC).

Pośrednio Departament ma również wpływ na działanie centrów teleinformatycznych poszczególnych sił zbrojnych: Wojska Lądowe – Centrum Wsparcia Mobilnych Systemów Teleinformatycznych Wojsk Lądowych, któremu są przyporządkowane – nowo powstające – Zespoły Wsparcia Teleinformatycznego Dywizji i Brygad, Centrum Wsparcia Teleinformatycznego Sił Powietrznych oraz Centrum Wsparcia Teleinformatycznego Marynarki Wojennej.



Rys.3.2 *Struktura organizacyjna Departamentu Informatyki i Telekomunikacji*
Źródło: Opracowanie własne.

Najważniejsze projekty w obszarze teleinformatyki i telekomunikacji Sił Zbrojnych RP zainicjowane przez DIiT to:

- modernizacja sieci MIL-WAN;
- rekonfiguracja sieci INTER-MON;
- wdrożenie systemu elektronicznego obiegu dokumentów;
- wdrożenie podpisu elektronicznego w MON;
- wdrożenie telefonii IP i VTC funkcjonującej w sieci MIL-WAN;
- budowa bramy międzysystemowej;
- wdrożenie systemu informatycznego wsparcia eksploatacji samolotów F-16;

- wdrożenie systemu łączności zabezpieczającego funkcjonowanie attachatów wojskowych;
- budowa resortowego portalu informacyjnego;
- budowa resortowego centrum backupów.

W szczegółowym zakresie głównymi realizatorami zadań jakie nałożył na DiiT Minister Obrony Narodowej są wewnętrzne komórki specjalistyczne departamentu – zorganizowane w formie oddziałów. Łącznie w departamencie Informatyki i Telekomunikacji funkcjonuje 9 takich struktur organizacyjnych.

Oddział systemów informatycznych jest komórką właściwą w zakresie systemów informatycznych resortu obrony narodowej.

Do zakresu zadań oddziału należy:

- określanie norm, standardów programowych i technologicznych dla systemów informatycznych w resorcie obrony narodowej;
- planowanie, inicjowanie, koordynowanie i nadzór nad przedsięwzięciami związanymi z projektowaniem oraz wdrażaniem systemów informatycznych;
- udział w pracach organizacji NATO i UE w zakresie systemów informatycznych;
- nadzór nad eksploatacją i rozwojem systemów informatycznych w resorcie obrony narodowej;
- opracowywanie dokumentów normatywnych w zakresie zasad organizowania, projektowania, wdrażania i eksploatacji systemów informatycznych oraz polityki bezpieczeństwa informacyjnego;
- analizowanie struktur systemów obiegu informacji w resorcie obrony narodowej pod kątem możliwości ich optymalizacji i informacji;
- analizowanie i opiniowanie potrzeb z zakresu systemów informatycznych zgłaszanych przez użytkowników instytucjonalnych oraz indywidualnych;
- wytyczanie kierunków prowadzenia prac naukowo-badawczych w obszarze systemów informatycznych;
- udział w tworzeniu polityki bezpieczeństwa informacyjnego resortu obrony narodowej w zakresie systemów informatycznych.

Oddział systemów telekomunikacyjnych jest komórką właściwą w zakresie realizacji funkcji organizatora wojskowego systemu telekomunikacyjnego oraz wytyczania kierunków rozwoju systemów telekomunikacyjnych w resorcie obrony narodowej.

Do zadań oddziału należy:

- współpraca z krajowym operatorem telekomunikacyjnym oraz agencjami NATO i UE w zakresie rozbudowy, modernizacji oraz zarządzania systemami telekomunikacyjnymi;
- opracowywania planów modernizacji systemów telekomunikacyjnych i sieci telekomunikacyjnych resortu obrony narodowej;
- nadzór nad funkcjonowaniem systemów telekomunikacyjnych w resorcie obrony narodowej, a w szczególności w urzędzie Ministra;
- nadzór nad rozwojem i funkcjonowaniem systemów komutacyjnych i teletransmisyjnych oraz sieci teleinformatycznych resortu obrony narodowej, a także zapewnienie bezpieczeństwa sieci i przesyłanych informacji;
- planowanie i nadzorowanie rozbudowy sieci teleinformatycznych w Ministerstwie;
- organizacja zarządzania systemami i sieciami telekomunikacyjnymi resortu obrony narodowej;
- realizowanie zadań organizatora wojskowego systemu telekomunikacyjnego w zakresie dzierżawy łączy teletransmisyjnych oraz planowania i nadzoru inwestycji w zakresie rozbudowy i modernizacji infrastruktury telekomunikacyjnej;
- opiniowanie planów rozwoju i modernizacji krajowej sieci telekomunikacyjnej oraz pocztowej pod kątem spełnienia wymogów obronności państwa.

Oddział ZSyD i KŚW jest komórką właściwą w zakresie wytyczania kierunków rozwoju, wdrażania i funkcjonowania zautomatyzowanych systemów dowodzenia i kierowania środkami walki (ZSyD i KŚW) w resorcie obrony narodowej.

Do zadań oddziału m.in. należy:

- określanie kierunków rozwoju oraz integracji ZSyD i KŚW, w tym wynikających z koncepcji osiągania sieciocentryczności przez Siły Zbrojne (SZ RP);
- ustalanie norm i standardów technicznych oraz technologicznych dla ZSyD i KŚW a także nadzór i koordynacja działań związanych z ich wdrażaniem;
- określenie modeli oraz procedur NATO wymagających implementacji w narodowych ZSyD i KŚW w celu zapewnienia ich interoperacyjności z systemami NATO;

- inicjowanie, planowanie i koordynowanie przedsięwzięć związanych z projektowaniem i wdrażaniem ZSyD i KŚW w SZ RP, w tym współudział w zarządzaniu projektami;
- współpraca z państwami członkowskimi i organizacjami NATO w zakresie wymiany doświadczeń związanych z budową, wdrażaniem i eksploatacją ZSyD i KŚW;
- współpraca z komórkami organizacyjnymi Ministerstwa, jednostkami organizacyjnymi resortu obrony narodowej oraz firmami komercyjnymi w zakresie wymagań systemowych i technicznych na ZSyD i KŚW.

Oddział analiz i rozwoju nowych technologii jest komórką właściwą w zakresie prowadzenia wszechstronnych analiz technologii informatycznych i telekomunikacyjnych pod kątem ich wykorzystania na potrzeb resortu obrony narodowej.

Do zadań oddziału m.in. należy:

- analiza zapotrzebowania resortu obrony narodowej na usługi informatyczne i telekomunikacyjne;
- analiza kierunków i trendów rozwoju technologii informatycznych i telekomunikacyjnych, a także jej wykorzystania przez inne państwa;
- analiza metodologii projektowania systemów oraz zarządzania projektami informatycznymi i telekomunikacyjnymi;
- analiza możliwości wykorzystania nowych technologii informatycznych i telekomunikacyjnych do budowy systemów informatycznych, telekomunikacyjnych oraz ZSD i KŚW;
- opracowywanie ekspertyz i prowadzanie skutków realizowalności systemów informatycznych, telekomunikacyjnych oraz ZSyD i KŚW;
- przygotowywanie propozycji zasadniczych kierunków prac badawczo-rozwojowych teleinformatyki i telekomunikacji prowadzonych w resorcie obrony narodowej oraz nadzór nad ich realizacją;
- opracowywanie wykazu obowiązujących w resorcie obrony narodowej standardów technologii teleinformatycznej oraz nadzór nad ich przestrzeganiem;
- opracowywanie planów rozwoju i modernizacji systemów informatycznych, telekomunikacyjnych oraz ZSyD i KŚW;

- opiniowanie i uzgadnianie planów rozwoju i modernizacji SZ RP w zakresie leżącym w kompetencji Departamentu;
- współudział w opracowywaniu analiz i ekspertyz w zakresie realizacji programów o wymiarze narodowym;
- prowadzenie ewidencji oprogramowania źródłowego i dokumentacji systemów teleinformatycznych resortu obrony narodowej oraz rejestru wszystkich systemów teleinformatycznych resortu ON.

Oddział systemów radiowych jest komórką właściwą w zakresie planowania, wdrażania funkcjonowania i rozwoju systemów radiowych w resorcie obrony narodowej.

Do zadań oddziału m.in. należy:

- opracowanie planów modernizacji i rozwoju systemów radiowych resortu obrony narodowej;
- inicjowanie, koordynowanie oraz udział w planowaniu i realizowaniu przedsięwzięć związanych z osiąganiem interoperatywności systemów radiowych resortu obrony narodowej z systemami NATO i UE, a także administracji publicznej;
- organizacja i wykorzystanie systemów satelitarnych;
- organizacja radiowych systemów KF i UKF;
- wdrażanie i koordynowanie wykorzystania bezprzewodowych technologii w sieciach teleinformatycznych resortu obrony narodowej;
- formułowanie wymagań na prace-rozwojowe, oraz organizowanie i nadzór funkcjonowania radiowych systemów łączności;
- udział w pracach zespołów ekspertów powoływanych w ramach przetargów dotyczących wyboru nowych typów środków łączności;
- koordynowanie, nadzorowanie wdrażania i eksploatacji sieci radiowych w resorcie obrony narodowej.

Oddział serwerów i baz danych jest komórką właściwą w zakresie określania zasad budowy i utrzymania baz danych oraz administrowania infrastrukturą programowo-sprzętową resortowych serwerów baz danych.

Do zadań oddziału m.in. należy:

- administrowanie platformą sprzętową serwerów baz danych eksploatowanych w urzędzie Ministra;

- administrowanie platformą programową (systemową oraz systemami baz danych) eksploatowaną w urzędzie Ministra;
- nadzór nad administrowaniem platformą programowo – sprzętową serwerów baz danych resortu obrony narodowej eksploatowaną poza urzędem Ministra;
- realizacja zadań w obszarze polityki bezpieczeństwa informacyjnego w zakresie: praw dostępu użytkowników do baz danych, archiwizacji oraz kopii bezpieczeństwa danych i niezawodności serwerów;
- współpraca z komórkami wewnętrznymi Departamentu w zakresie standaryzacji, rozwoju i zarządzania systemami opartymi na bazach danych;
- opracowywanie planów awaryjnych odzyskiwania danych w sytuacjach kryzysowych;
- współpraca z komórkami wewnętrznymi Departamentu w zakresie zapewnienia użytkownikom dostępu do baz danych oraz prowadzenia niezbędnych szkoleń.

Oddział przygotowania specjalistycznego jest komórką właściwą w zakresie planowania, kształtowania i koordynowania procesu szkolenia oraz doskonalącego szkolenia specjalistycznego specjalistów informatyki i telekomunikacji, realizacji współpracy zagranicznej Departamentu, planowania działalności bieżącej Departamentu oraz realizacji zadań gestora korpusu osobowego łączności i informatyki.

Do zadań oddziału m.in. należy:

- opracowywanie we współpracy z komórkami wewnętrznymi Departamentu zasadniczych kierunków i wymagań szkolenia specjalistycznego specjalistów informatyki i telekomunikacji;
- planowanie, koordynowanie i określanie w uzgodnieniu z komórkami wewnętrznymi Departamentu i innymi komórkami organizacyjnymi MON potrzeb, w zakresie doskonalącego szkolenia specjalistycznego;
- opiniowanie założeń do programów szkoleni realizowanych w resortowych uczelniach lub centrach szkolenia;
- realizowanie współpracy zagranicznej w obszarze odpowiedzialności Dep.;
- opiniowanie projektów struktur organizacyjnych organów wykonawczych informatyki i telekomunikacji resortu w tym projektów dokumentów kompetencyjno-etatowych;
- prowadzenie obsługi personalnej kadry i pracowników Departamentu;

- prowadzenie bazy danych stanu korpusu osobowego łączności i informatyki;
- weryfikowanie prognoz rozwoju służbowego kadry oficerskiej w korpusie osobowym łączności i informatyki stosownie do potrzeb SZ RP oraz określanie potrzeb naboru kandydatów do służby w tym korpusie;
- realizowanie zadań zapewniających bieżące funkcjonowanie Dep.

Oddział gestorstwa jest komórką właściwą w zakresie opracowywania i koordynowania realizacji zadań w zakresie rozwoju, organizacji oraz wdrożeń sprzętu informatyki łączności i oprogramowania oraz realizacji zadań określonych dla gestora sprzętu.

Do zadań oddziału m.in. należy:

- znajomość stanu ilościowego i jakościowego, a także perspektyw użytkowania uzbrojenia i sprzętu wojskowego, z uwzględnieniem i wykorzystaniem informacji Centralnego Organu Logistycznego (COL);
- określanie norm obsad etatowych oraz należności sprzętu informatyki, łączności i oprogramowania, z uwzględnieniem i wykorzystaniem informacji COL;
- opracowywanie z komórkami wewnętrznymi Departamentu wymagań taktyczno-technicznych na sprzęt informatyki, łączności i oprogramowania wyprowadzany na wyposażenia SZ RP;
- określanie w uzgodnieniu z komórkami wewnętrznymi Departamentu oraz jednostkami organizacyjnymi resortu obrony narodowej potrzeb SZ RP w zakresie dostaw sprzętu informatyki, łączności i oprogramowania;
- uzgadnianie projektów planów dostaw sprzętu informatyki, łączności i oprogramowania opracowywanych w ramach realizacji Centralnych Planów Rzeczowych;
- współudział w określaniu zasad prowadzenia ewidencji i sprawozdawczości w zakresie sprzętu informatyki, łączności i oprogramowania na poszczególnych szczeblach organizacyjnych resortu obrony narodowej;
- opracowywanie, we współpracy z komórkami wewnętrznymi Departamentu oraz jednostkami organizacyjnymi resortu obrony narodowej, projektów poleceń i rozkazów o wprowadzeniu do Sił Zbrojnych RP sprzętu informatyki i telekomutacji nowego typu;
- współudział w opracowywaniu dokumentów związanych z wycofywaniem i zagospodarowywaniem zbędnego sprzętu informatyki i telekomunikacji;

- planowanie działalności kodyfikacyjnej sprzętu w zakresie właściwości Departamentu.

Oddział wsparcia użytkownika jest komórką właściwą w zakresie udzielania pomocy technicznej związanej z używaniem sprzętu teleinformatycznego przez użytkowników w urzędzie Ministra i attachatach wojskowych oraz rozwiązanie zaistniałych problemów technicznych.

Do zakresu zadań oddziału m.in. należy:

- organizacja szkoleń użytkowników w zakresie podstawowej i zaawansowanej obsługi aplikacji oraz sprzętu, określenie tematów szkoleń a także ich przygotowywanie;
- przyjmowanie zgłoszeń o problemach z użytkowanym sprzętem teleinformatycznym bądź oprogramowaniem, niezależnie od źródeł kłopotów (zarówno w sytuacji awarii sprzętu jak i braku odpowiedniej wiedzy użytkownika);
- udzielanie pomocy technicznej użytkownikom sprzętu teleinformatycznego na miejscu tym naprawa komputerów i urządzeń peryferyjnych, wymiana części i rekonfiguracja oprogramowania;
- ewidencjonowanie najczęściej spotykanych problemów i braków umiejętności użytkowników w celu przygotowania tematyki szkoleń.

Poza komórkami wewnętrznymi DIiT zadania w zakresie organizacyjno-technicznym realizują instytucje podległe Dyrektorowi DIiT.

Instytucją zarządzającą bezpośrednio czynnym WST jest Centrum Zarządzania Systemami Teleinformatycznymi (CZST). Centrum odpowiada za poprawne funkcjonowanie systemu teleinformatycznego Sił Zbrojnych. Jego głównym zadaniem jest zarządzanie i monitorowanie systemów teleinformatycznych, sprawowanie centralnego nadzoru nad bezpieczeństwem tych systemów i reagowanie na zaistniałe incydenty komputerowe.

Ponadto Centrum jest głównym realizatorem procesu budownictwa specjalnego łączności i remontów wojskowej struktury telekomunikacyjnej. Ważnym zadaniem jest również sprawowanie nadzoru merytorycznego nad Regionalnymi Węzłami Łączności i Centrami Wsparcia Technicznego RSZ.

Kolejną instytucją podporządkowaną Dyrektorowi DIiT jest Centrum Informatyki i Łączności Obrony Narodowej. CIiŁON odpowiada za prowadzenie prac projektowo-

wdrożeniowych systemów teleinformatycznych resortu obrony narodowej, eksploatację systemów teleinformatycznych Ministerstwa Obrony Narodowej oraz szkolenia kursowe w zakresie informatyki.

Przedmiotem działalności Centrum Informatyki i Łączności Obrony Narodowej jest:

- projektowanie systemów teleinformatycznych na potrzeby resortu obrony narodowej;
- testowanie i uczestniczenie we wdrażaniu systemów teleinformatycznych;
- eksploatacja systemów teleinformatycznych szczebla centralnego, w tym użytkowanych przez komórki organizacyjne MON;
- planowanie, organizowanie i prowadzenie szkolenia kursowego w zakresie informatyki żołnierzy zawodowych i pracowników resortu obrony narodowej;
- realizowanie zadań na potrzeby Dyrektora Departamentu Informatyki i Telekomunikacji związanych ze sprawowaną przez niego funkcję gestora sprzętu informatyki, łączności i oprogramowania.

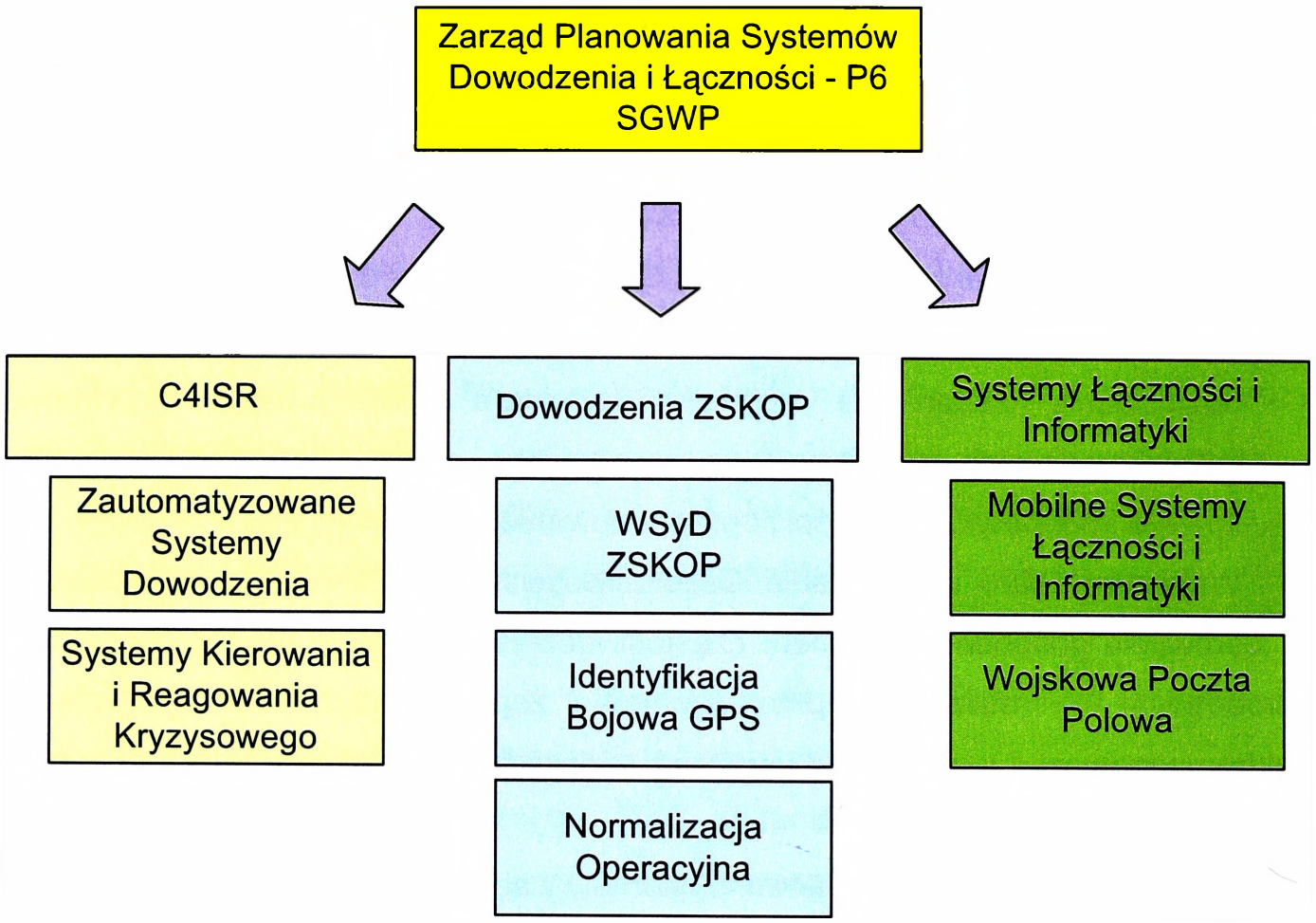
Wojskowe Biuro Zarządzania Częstotliwościami – komórka odpowiedzialna za kierowanie gospodarką widmem częstotliwości fal radiowych w resorcie Obrony Narodowej i realizację przedsięwzięć zapewniających kompatybilność elektromagnetyczną wojskowych urządzeń radiokomunikacyjnych i innych urządzeń radioelektronicznych.

Wojskowe Biuro Bezpieczeństwa Systemów Łączności i Informatyki – komórka pełniąca rolę krajowego organu operacyjnego w zakresie bezpieczeństwa teleinformatycznego. Realizuje przedsięwzięcia w zakresie bezpieczeństwa teleinformatycznego oraz sprawowania nadzoru nad eksploatacją techniczną i programową środków ochrony systemów łączności i informatyki.

Centralny Węzeł Łączności MON jest instytucją zapewniającą techniczną współpracę stacjonarnego systemu łączności SZ RP ze stacjonarnym systemem łączności państw NATO oraz organizację systemu łączności z jednostkami przebywającymi poza obszarem kraju.

3.1.2 Zarząd Planowania Systemów Dowodzenia i Łączności P-6 SG WP

Jak już wspomniano drugą komórką organizacyjną funkcjonującą w resorcie ON będącą organizatorem wojskowego systemu telekomunikacyjnego jest Zarząd Planowania Systemów Dowodzenia i Łączności P-6 SG WP.



Rys.3.3 *Zadania Zarządu Planowania Systemów Dowodzenia i Łączności P-6*

Źródło: Opracowanie własne

Zarząd Planowania Systemów Dowodzenia i Łączności P-6 jest komórką organizacyjną Sztabu Generalnego Wojska Polskiego właściwą w zakresie planowania i organizacji systemów dowodzenia i kierowania w czasie pokoju, kryzysu i wojny w tym jego funkcjonalnego powiązania z systemami kierowania bezpieczeństwem państwa, a także określania wymagań operacyjnych dla systemów teleinformatycznych i infrastruktury telekomunikacyjnej[23].

[23] Zarządzenie Nr 40/MON Ministra Obrony Narodowej z dnia 22 listopada 2006 r. w sprawie regulaminu organizacyjnego Ministerstwa Obrony Narodowej, Dziennik Urzędowy Ministra Obrony Narodowej z 2006 r. Nr 21 Poz. 269, 270, §44 ust.1.

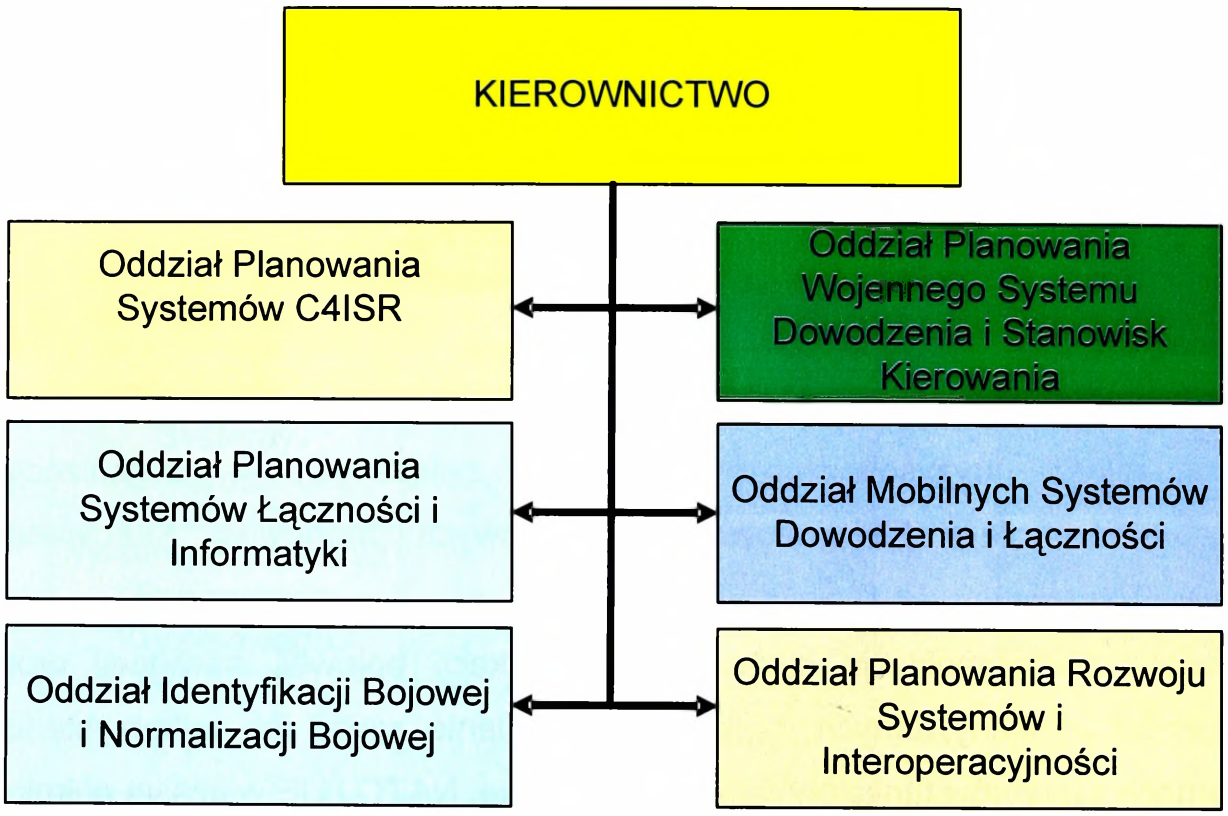
Do zakresu zadań Zarządu należy w szczególności[24]:

- kierowanie w resorcie realizacją przedsięwzięć związanych z budową, implementacją i integracją systemów dowodzenia, kontroli, komunikacji, łączności oraz wywiadu, obserwacji i dozoru (ang. Command, Control, Communication, Computers and Intelligence, Surveillance, Reconnaissance - C4ISR);
- określanie wymagań operacyjnych dla ZSyD oraz wytyczanie zasadniczych kierunków prac normalizacyjnych, kierowanie procesem ratyfikacji „Porozumień Standaryzacyjnych NATO" z obszaru interoperacyjności, a także procedur kierowania i dowodzenia w Siłach Zbrojnych i udział w procesie wdrażania postanowień dokumentów doktrynalnych NATO;
- realizacja zadań związanych z opracowywaniem koncepcji i dokumentów normatywnych dotyczących planowania, organizacji, rozwijania i funkcjonowania wojennego systemu dowodzenia, kierowania w czasie pokoju i sytuacjach kryzysowych oraz zadań związanych z organizacją i zabezpieczeniem funkcjonowania Zapasowych Stanowisk Kierowania Obroną Państwa;
- planowanie i organizacja systemów identyfikacji bojowej, nawigacji oraz systemów wymiany danych (Link) oraz określanie zasad ich wykorzystania w ramach systemów funkcjonujących w państwie, NATO i UE w czasie pokoju, kryzysu i wojny;
- planowanie wykorzystania resortowego systemu telekomunikacyjnego i określanie jego wymagań na potrzeby wojennego systemu dowodzenia, planowanie i organizacja systemów teleinformatycznych na potrzeby polskich kontyngentów wojskowych, polskich jednostek wojskowych, misji i operacji specjalnych poza granicami kraju, ćwiczeń szczebla strategicznego oraz udział w wytyczaniu kierunków szkolenia specjalistów informatyki i łączności;
- wykonywanie zadań wynikających z funkcji organizatora wojskowej poczty polowej;

---

[24] Zarządzenie Nr 40/MON Ministra Obrony Narodowej z dnia 22 listopada 2006 r. w sprawie regulaminu organizacyjnego Ministerstwa Obrony Narodowej, Dziennik Urzędowy Ministra Obrony Narodowej z 2006 r. Nr 21 Poz. 269, 270, §44 ust.2.

- opracowywanie wymagań operacyjnych na rozbudowę i modernizację infrastruktury telekomunikacyjnej w tym sieci teleinformatycznych;
- planowanie wykorzystania mobilnych systemów łączności i informatyki Sił Zbrojnych na potrzeby dowodzenia;
- planowanie i opracowywanie normatywnych systemów dowodzenia i łączności dla poszczególnych szczebli dowodzenia.



Rys.3.4 *Struktura organizacyjna Zarządu Planowania Systemów Dowodzenia i Łączności*
Źródło: Opracowanie własne

3.2 Przeznaczenie i cechy Wojskowego Systemu Teleinformatycznego

W celu realizacji tego przedsięwzięcia autor dokonał wnikliwej analizy pojęć ściśle związanych z systemem łączności:

- ***Łączność*** – dział komunikacji dotyczący przekazywania informacji (poczta, sygnalizacja, telegraf, telefon, radio, telewizja).

- ***Komunikacja*** [łac.], przewożenie ludzi i ładunków (transport) oraz przekazywanie wiadomości (łączność, telekomunikacja).
- ***Telekomunikacja*** – dziedzina nauki i techniki oraz działalności ludzkiej dotycząca przesyłania **wiadomości** na odległość za pomocą sygnałów elektrycznych kanałami telekomunikacyjnymi to także każde przesyłanie, nadawanie lub odbiór znaków, sygnałów, pisma, obrazów, dźwięków lub wszelkiego rodzaju wiadomości drogą przewodową, optyczną radiową, lub za pomocą innych systemów energetycznych[25].

  Telekomunikację ze względu na rodzaj przesyłanych wiadomości dzieli się na:

  1. Telefonię (przekazywanie dźwięków gł. Mowy),
  2. Radiofonię (przekazywanie dźwięków mowy i muzyki),
  3. Telegrafię (przekazywanie znaków pisma),
  4. Symilografię (przekazywanie obrazów nieruchomych),
  5. Telewizję (przekazywanie obrazów ruchomych wraz z towarzyszącym im dźwiękiem),
  6. Telemetrię (przekazywanie danych pomiarowych),
  7. Telemechanikę (przekazywanie impulsów sterujących),
  8. Teledację (przekazywanie danych cyfrowych).

- ***Transmisja*** [łac.], teletransmisja, przekazywanie sygnałów elektrycznych za pośrednictwem urządzeń elektronicznych z miejsc ich wytwarzania do miejsc ich odbioru.

- ***Teletransmisja*** [gr.-łac.], dział telekomunikacji zajmujący się techniką przesyłania sygnałów na odległość za pomocą przewodów, światłowodów lub fal radiowych lub dział telekomunikacji zajmujący się techniką przesyłania sygnałów na odległość za pomocą torów telekomunikacyjnych.

W zależnie od rodzaju użytego toru telekomunikacyjnego rozróżnia się teletransmisję:

- przewodową (za pomocą przewodów napowietrznych lub kabli),
- radiową (za pomocą fal radiowych),

[25] definicja własna J. Michniak

- optyczną (przeważnie za pomocą fal świetlnych przesyłanych przez światłowody,).

- ***Informatyka*** – zespół dyscyplin naukowych i technicznych zajmujących się przetwarzaniem informacji, zwłaszcza przy użyciu środków automatycznych (np.: komputerów).
- ***Teleinformatyka*** – dział informatyki dotyczący realizacji jej zadań na odległość z zastosowaniem środków telekomunikacji.

System *(gr. Systema)* oznacza połączenie, całość, system jest to pewna całość tworzona przez określony zbiór elementów i relacji między nimi, rozpatrywana z określonego punktu widzenia[26].

Według L. Von Bertalauffy „System jest to kompleks elementów znajdujących się we wzajemnej interakcji" , według A. Hall „System jest to zbiór obiektów wraz z relacjami między nimi i między ich właściwościami". S. Beer – „System jest to zorganizowana ilość elementów powiązanych wzajemnie i pełniących określone funkcje" ora według P. Rivett i R. Ackoff – „System jest to zespół obiektów i czynności, mający cztery podstawowe cechy charakterystyczne – treść, strukturę, łączność i sterowanie".

W przytoczonych powyżej definicjach, a także innych występujących w literaturze, zauważamy pewne cechy wspólne, tj.:

- *system jest zespołem powiązanych elementów;*
- *system jest związany z otoczeniem;*
- *element systemu może być systemem niższego rzędu.*

Podstawowe właściwości systemu:

1) zachowanie każdego elementu wpływa na zachowanie całości, ale żaden element nie ma wyłączności w oddziaływaniu na całość;
2) każdy, wyodrębniony wg dowolnego kryterium, podzbiór elementów ma wpływ na funkcjonowanie systemu, ale żaden z podzbiorów nie ma wyłącznego wpływu (system jest więc niepodzielną całością).

Systemem nazywa się również: zespół sposobów (metod) działania, wykonywania złożonych czynności, a także całokształt zasad organizacyjnych, ogół norm i reguł obowiązujących w danej dziedzinie (p. system finansowy, system

[26] T i K. Jajuga; K. i S. Wrzosek - Elementy teorii systemów i analizy systemowej, Wrocław, 1993 s.10

moralny); także całościowy i uporządkowany zespół zdań powiązanych ze sobą określonymi stosunkami logicznymi, w szczególności stosunkiem logiki wynikania, s*ystemem* w tym znaczeniu jest nazywana każda teoria metodologicznie poprawna i dotycząca dostatecznie obszernego fragmentu rzeczywistości. Za profesorem Michniakiem ***system jest to wyodrębniony zbiór elementów (materialnych lub abstrakcyjnych) wzajemnie sprzężonych, rozważany jako całość z określonym wyraźnie celem i z określonego punktu widzenia, mający przy tym takie właściwości, których nie posiadają jego pojedyncze elementy składowe***[27].

Rozróżnia się m.in. następujące systemy telekomunikacyjne:

- teletransmisyjne;
- telekomutacyjne (systemy central telekomunikacyjnych);
- przetwórcze (aparatów nadawczych i odbiorczych).

- ***System telekomunikacyjny*** to: zespół współpracujących ze sobą **urządzeń telekomunikacyjnych** spełniających określone wspólne zadanie, to także zbiór zasad działania danego urządzenia telekomunikacyjnego (określony jego właściwościami elektrycznymi i konstrukcyjnymi), odróżniających je od innych urządzeń spełniających to samo zadanie; np. określony system telewizyjny.

  Urządzenia telekomunikacyjne[28] *to urządzenia do przetwarzania zapisu informacji na sygnały, transmisji sygnałów, zestawiania i rozłączania łączy oraz do kontroli powyższych czynności.*

- ***System teletransmisyjny*** to zespół urządzeń teletransmisyjnych wraz z tworzonymi drogami telekomunikacyjnymi oraz ze sposobem ich działania określonym zakresem częstotliwości pracy, rodzajem modulacji, liczbą realizowanych kanałów telekomunikacyjnych, itp.

System teletransmisyjny, to rodzaj systemu telekomunikacyjnego gdzie rozróżnia się systemy teletransmisyjne **naturalne** (jednokrotne), w których tor służy do przesyłania sygnałów pochodzących tylko z jednego nadajnika, oraz systemy teletransmisyjne **wielokrotne**, w których tor służy do przesyłania sygnałów z wielu nadajników (każdemu sygnałowi przydziela się określone pasmo częstotliwości lub szczelinę czasową, udostępnianą w regularnych odstępach czasu).

Linia telekomunikacyjna (teletransmisyjna) to tor[29] (przewodowy, światłowodowy, falowodowy, świetlny lub zespół takich torów, łącznie ze stacjami teletransmisji

[27] Definicja własna J. Michniak
[28] Por. Leksykon naukowo-techniczny, ed. op. cit., s. 1040

przelotowymi, odgałęźnymi i końcowymi) oraz łącznie ze wszelkimi akcesoriami konstrukcyjnymi służącymi do przesyłania informacji na odległość, rozmieszczonych wzdłuż określonej trasy.

- **Infrastruktura** – to podstawowe urządzenia, budynki i instytucje usługowe, których istnienie jest niezbędne do prawidłowego funkcjonowania gospodarki i społeczeństwa. Wyróżnia się infrastrukturę **społeczną** oraz **techniczną.** Słowo *infrastruktura* oznacza dosłownie „konstrukcja pod spodem".

Infrastruktura techniczna to urządzenia, sieci przesyłowe i związane z nimi obiekty świadczące niezbędne i podstawowe usługi dla określonej jednostki przestrzenno-gospodarczej (osiedla, dzielnicy, miasta, zakładu przemysłowego, jednostki wojskowej, itp.) w zakresie energetyki, dostarczania ciepła, wody, usuwania ścieków i odpadów, transportu, teletechniki itp.[30]

Każdy system teleinformatyczny, a szczególnie jego urządzenia transmisyjne, komutacyjne, ochrony informacji niejawnej czy terminale końcowe instalowane są w uprzednio przygotowanych obiektach, budynkach, pomieszczeniach lub pojazdach mechanicznych, które nazywamy ***infrastrukturą.***

W związku z przedstawioną powyżej definicją infrastruktury technicznej, można przyjąć na potrzeby naszych zajęć, że:

- ***Infrastruktura wojskowych systemów teleinformatycznych*** to urządzenia systemu teleinformatycznego, sieci teletransmisyjnej (przesyłowej) i związane z nimi obiekty świadczące dla potrzeb określonej organizacji (jednostki wojskowej) niezbędne i podstawowe usługi w zakresie przetwarzania, przechowywania i przesyłania informacji jawnych lub niejawnych w sposób zapewniający ich ochronę przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania.
- ***System teleinformatyczny*** to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego[31]. ***System teleinformatyczny*** tworzą urządzenia, narzędzia, metody

---

[29] Tor telekomunikacyjny to konstrukcja techniczna będąca układem biernym, w zasadzie linearnym, umożliwiająca realizację kanału telekomunikacyjnego transmisyjnego przestrzennego – Biuletyn informacyjny Nr 2-3 (276-277), IŁ Warszawa-Międzeszyn, 1990, s. 31

[30] http://pl.wikipedia.org/wiki/Infrastruktura

[31] Ustawa z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną (Dz.U.2002.144.1204)

postępowania i procedury stosowane przez wyspecjalizowanych pracowników, w sposób zapewniający wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji. System teleinformatyczny jednostki organizacyjnej przetwarza, przechowuje oraz przesyła informacje niezbędne do prawidłowego jej funkcjonowania[32].

- ***Sieć*** *(ang. Network)* – ogólny termin używany do opisu systemu połączeń urządzeń peryferyjnych za pomocą kanałów telekomunikacyjnych.
- ***Sieć teleinformatyczna***[33] jest to organizacyjne i techniczne połączenie systemów teleinformatycznych.

Mając do czynienia z nowoczesnymi sieciami zintegrowanymi i dysponując zaawansowanymi technicznie terminalami abonenckimi, korzysta się w zasadzie *(praktycznie poza klasyczną usługą telefoniczną)* z usług teleinformatycznych.

Z analizy literatury i przede wszystkim dokumentów normatywnych (ustawy i rozporządzenia) regulujących tę materię wynika, że elementy współczesnego wojskowego systemu lub sieci teleinformatycznej to:

- infrastruktura teleinformatyczna;
- elementy (urządzenia) telekomutacyjne;
- elementy (urządzenia) informatyczne;
- aplikacje (oprogramowanie) systemowe;
- personel techniczny i użytkownicy systemu.

Współczesna infrastruktura teleinformatyczna obejmuje dwie do niedawna odrębne, a obecnie coraz bardziej przenikające się hierarchiczne struktury komunikacyjne:

- **sieci telekomunikacyjne**, dla których centralnym punktem nadal pozostają cyfrowe systemy komutacji (centrale) wraz z różnorodnymi sieciami dostępu abonenckiego;
- **cyfrowe sieci komputerowe** oparte na strukturach sieciowych typu LAN, MAN i WAN.

Oferowanie usług informatycznych przez sieć telekomunikacyjną nie czyni ją automatycznie siecią teleinformatyczną.

Sieć telekomunikacyjna to zespół aparatów przetwórczych, linii i stacji

---

[32] K. Liederman, Bezpieczeństwo teleinformatyczne, BEL Studio, 2001
[33] Ustawa z dnia 15 kwietnia 2005 r. o zmianie ustawy o ochronie informacji (Dz. U. Nr 85, poz.727),

teletransmisyjnych, central komutacyjnych, radiostacji i innych urządzeń telekomunikacyjnych znajdujących się na określonym obszarze, powiązanych ze sobą technicznie i przeznaczonych do świadczenia usług telekomunikacyjnych to także zespół wszystkich łączy telekomunikacyjnych otwartych dla korespondencji publicznej z wyjątkiem łączy telekomunikacyjnych służb ruchomych.

- ***Wojskowy System Teleinformatyczny*** to zespół współpracujących ze sobą urządzeń telekomunikacyjnych, informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych oraz głosu poprzez sieci teletransmisyjne (telekomunikacyjne) za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego.

Wojskowa sieć teleinformatyczna to zespół węzłów stanowisk dowodzenia, węzłów telekomunikacyjnych sieci, samodzielnych stacji i urządzeń telekomunikacji oraz informatyki połączonych ze sobą w ściśle określony sposób drogami telekomunikacyjnymi wraz z urządzeniami kryptograficznymi, sprzętem specjalistycznym i pomocniczym a także całą infrastrukturą wsparcia logistycznego i bojowego, współpracujący ze sobą według zawczasu przyjętych zasad i w ściśle określonym celu.

Umiejscowienie wojskowego systemu teleinformatycznego w strukturze systemu obronnego Polski jest zadaniem trudnym do zdefiniowania. Wynika to z faktu, iż jego elementy występują w każdym z podsystemów systemu obronnego i w każdym odgrywają znaczącą rolę.

Wojskowy system telekomunikacyjny[34] to zbiór urządzeń i linii telekomunikacyjnych, metod i procedur przekazywania informacji dla potrzeb Ministerstwa Obrony Narodowej oraz Sił Zbrojnych Rzeczypospolitej Polskiej za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną, zarządzanych przez organizatora wojskowego systemu telekomunikacyjnego.

Wojskowy system telekomunikacyjny zapewnia wymianę informacji dla użytkowników będących w strukturach:

- komórek organizacyjnych ministerstwa Obrony Narodowej;
- jednostek organizacyjnym podległym Ministrowi Obrony Narodowej lub przez niego nadzorowanym, będącym jednostkami budżetowymi, w tym również

[34] Rozporządzenie Ministra Obrony Narodowej z dnia 12 października 2005 r. w sprawie szczególnych warunków wykonywania działalności telekomunikacyjnej, §2 pkt. 7.

jednostkom Sił Zbrojnych Rzeczypospolitej Polskiej w czasie ich użycia lub pobytu poza granicami państwa;

- gospodarstwom pomocniczym komórek i jednostek organizacyjnych MON bądź nadzorowanych przez MON.

Ponadto w świetle obowiązujących przepisów[35] zezwala się na wykorzystanie wojskowego systemu telekomunikacyjnego przez jednostki sił zbrojnych obcych państw przebywające czasowo na terytorium Rzeczypospolitej Polskiej.

Oprócz, wyżej wymienionych beneficjentów wojskowego systemu telekomunikacyjnego w Rozporządzeniu Rady Ministrów z dnia 3 sierpnia 2005 r. w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa wymieniono następujące obszary wykorzystania WST[36]:

- system kierowania bezpieczeństwem narodowym;
- proces zapewnienia funkcjonowania państwa w razie zagrożenia bezpieczeństwa i w czasie wojny;
- system dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej;
- system współpracy z systemami łączności państw sojuszniczych;
- proces utrzymywania w stałej gotowości jednolitych systemów obserwacji, pomiarów, analiz, prognozowania i powiadamiania.

Ze względu na powyższe wojskowy system telekomunikacyjny powinien cechować się w szczególności:

- niezawodnością;
- odpornością na zakłócenia;
- zdolnością zapewnienia użytkownikom specjalnym[37] bezpiecznego przekazywania informacji;
- zdolnością zachowania ciągłości łączności podczas zmian miejsc pracy, w ramach stanowisk kierowania;
- zdolnością do elastycznej rekonfiguracji systemu;
- zdolnością do preferencyjnej obsługi użytkowników specjalnych.

---

[35] Rozporządzenie Ministra Obrony Narodowej z dnia 12 października 2005 r. w sprawie szczególnych warunków wykonywania działalności telekomunikacyjnej, §4 pkt. 2.

[36] Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2005 r. w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa, §10 pkt. 1, Dz.U. z 2004 r. Nr 180 poz. 1855

[37] użytkownik specjalny - organ władzy publicznej, Siły Zbrojne Rzeczypospolitej Polskiej lub przedsiębiorca o szczególnym znaczeniu gospodarczo-obronnym, o którym mowa w art. 3 ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców (Dz. U. Nr 122, poz. 1320 oraz z 2002 r. Nr 188, poz. 1571.

System telekomunikacyjny SZ RP zapewnia świadczenie usług w sposób ciągły w warunkach pokoju, kryzysu, jak również w sytuacjach związanych z Osiąganiem Wyższych Stanów Gotowości Bojowej. W celu sprostania stawianym wymogą w ramach WST planuje się użycie nw. sieci telekomunikacyjnych:

- własnej sieci telekomunikacyjnej (resortowa sieć MON);
- innych sieci administracji rządowej (np. resortowa sieć MSWiA);
- sieci telekomunikacyjnych NATO oraz Unii Europejskiej;
- sieci operatorów komercyjnych.

Ostatnie lata przyniosły istotne zmiany w wojskowych systemach łączności i informatyki. Zmiany te mają swoje uwarunkowania w wielu czynnikach, spośród których najistotniejszymi są:

- rozwój techniki cyfrowej oraz integracja urządzeń telekomunikacyjnych i informatycznych w system teleinformatyczny;
- zmiany w sztuce operacyjnej i taktyce, będące konsekwencją zmiany doktryny obronnej naszego kraju.

Rozwój techniki cyfrowej niemal całkowicie wyeliminował sprzęt wykonany w technice analogowej i stworzył podwaliny do organizacji systemu teleinformatycznego.

Działania na własnym terytorium zmieniły na strategiczno – operacyjnych szczeblach dowodzenia dotychczasową rolę polowego i stacjonarnego systemu łączności w zapewnieniu dowodzenia – nadając priorytet temu drugiemu.

Przy założeniu, że stanowiska dowodzenia szczebla strategicznego i operacyjnego będą z reguły rozmieszczane w obiektach stacjonarnych, łączność na ich potrzeby zapewniona będzie głównie poprzez stacjonarne węzły łączności, powiązane liniami stałymi, wzmacniane bądź uzupełniane środkami polowymi.

Istotny udział w zabezpieczeniu łączności dla potrzeb stanowisk dowodzenia szczebla strategicznego pełnić będą jednostki i pododdziały łączności (dowodzenia), których zadaniem będzie – rozwinięcie WŁ SD w układzie:

- stanowisko dowodzenia stacjonarne rozmieszczone jest obiektach w pełni przygotowanych i dostosowanych pod każdym względem do potrzeb dowodzenia w dotychczasowych miejscach dyslokacji lub innych obiektach wojskowych czy specjalnych;

- stanowisko dowodzenia stacjonarno – mobilne rozmieszczane jest w wybranych i przygotowanych wcześniej obiektach, a środki mobilne łączności uzupełniają tylko docelowe potrzeby dowodzenia w zakresie usług łączności i informatyki;
- stanowisko dowodzenia mobilno – stacjonarne rozmieszczane jest 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;
- stanowisko dowodzenia mobilne (aeromobilne) – przygotowane do rozmieszczenia w każdych warunkach i rejonach, z wykorzystaniem i bez, obiektów stacjonarnych, a praca sztabowa prowadzona będzie na środkach mobilnych lub aeromobilnych, autonomicznych pod względem usług łączności i informatyki.

3.3 Charakterystyka struktur organizacyjnych stacjonarnego systemu telekomunikacyjnego SZ RP.

3.3.1 Dotychczas funkcjonujący stacjonarny system telekomunikacyjny Sił Zbrojnych Rzeczypospolitej Polskiej

Do pierwszego stycznia 2007 r. stacjonarny system łączności SZ RP zbudowany był w oparciu o sieć Garnizonowych Węzłów Łączności (GWŁ) powiązanych ze sobą dalekosiężnymi traktami będącymi własnością resortu ON bądź też dzierżawionymi od operatorów telekomunikacyjnych.

Garnizonowe Węzły Łączności objęte były podziałem na kategorie (pięć kategorii) w zależności od szczebla organizacyjnego i liczebności jednostek wojskowych będących w rejonie odpowiedzialności danego GWŁ.

Garnizonowy Węzeł Łączności znajdował się w podporządkowaniu Dowódcy Garnizonu, w którym funkcjonował dany węzeł. W dniu 31 grudnia 2006 liczba Garnizonowych Węzłów Łączności funkcjonujących w Siłach Zbrojnych RP wynosiła 82.

Działalność instytucji centralnych Ministerstwa Obrony Narodowej zabezpieczał Centralny Węzeł Łączności MON, który stanowił główne ogniwo w stacjonarnym systemie telekomunikacyjnym państwa.

Dotychczas funkcjonujący system GWŁ umożliwiał ***kierowanie*** procesem planowania, organizowania, motywowania i kontrolowania działalności oraz ***dowodzenie*** poprzez kształtowanie wszystkich elementów gotowości i zdolności bojowej Sił Zbrojnych RP dla osiągnięcia ustalonych celów oraz dla wszechstronnego przygotowania w czasie pokoju i wszystkich fazach konfliktu, a także współdziałanie, alarmowanie i powiadamianie. Zapewniał on następujące rodzaje łączności:

a) telefoniczną łączność jawną i utajnioną;
b) telefaksową łączność jawną i utajnioną;
c) transmisję na potrzeby zautomatyzowanych systemów dowodzenia i systemów informatycznych;
d) łączność kodową i szyfrową;
e) wymianę korespondencji pisemnej.

Do zapewnienia dużej niezawodności pracy i ciągłości systemu telekomunikacyjnego wykorzystywane były następujące środki :

a) przewodowe;
b) optyczne;
c) radioliniowe;
d) radiowe;
e) satelitarne.

W skład system telekomunikacyjnego SZ RP wchodziły trzy wzajemnie powiązane ze sobą podsystemy telekomunikacyjne :

a) wojsk lądowych;
b) sił powietrznych;
c) marynarki wojennej.

W skład stacjonarnego podsystem telekomunikacyjnego Wojsk Lądowych wchodziły siły i środki łączności przewodowej i optycznej, radioliniowej i radiowej. W okresie stałej gotowości bojowej w podsystemie tym utrzymywana była całodobowa łączność przewodowa do wszystkich jednostek (instytucji) wojskowych, radiowa tylko w sieciach dowodzenia i alarmowania Sztabu Generalnego WP.

Uruchamianie pozostałych kierunków radiowych planowane było w ramach seansów lub po wprowadzeniu wyższych stanów gotowości bojowej (WSGB).

Podsystem stacjonarnej łączności Sił Powietrznych zorganizowany był na bazie wzajemnie uzupełniających się środków łączności przewodowej, optycznej i radiowej. Dalekosiężne trakty i łącza przewodowe miedzy poszczególnymi stanowiskami dowodzenia dzierżawiono od operatorów publicznych, natomiast elementy ugrupowania bojowego były połączone mediami teletransmisyjnymi miedzianymi lub światłowodowymi będącymi własnością Ministerstwa Obrony Narodowej.

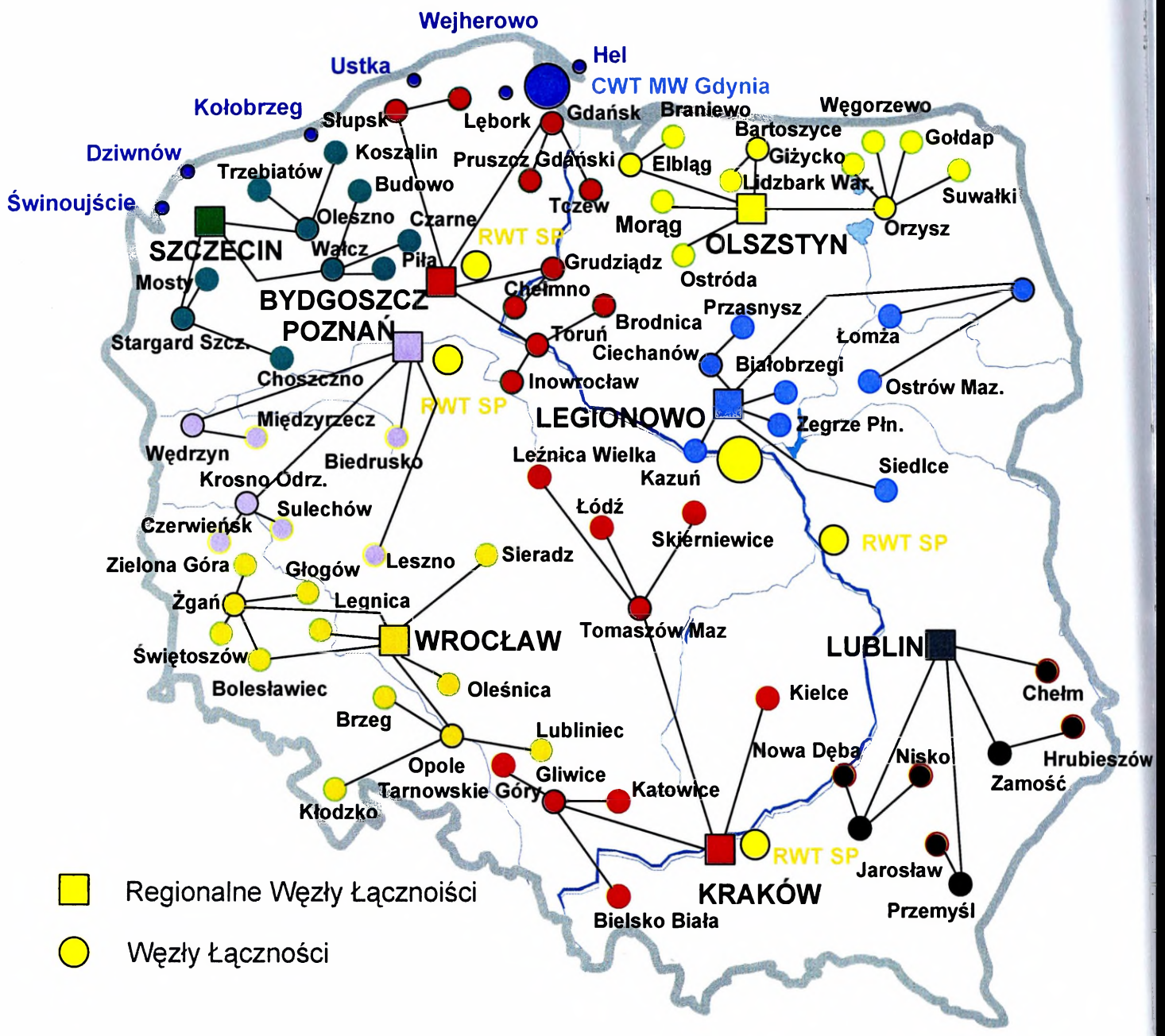
Podsystem stacjonarnej łączności Marynarki Wojennej zorganizowany był na bazie środków przewodowych w tym optycznych i radiowych. Środki przewodowe i optyczne wykorzystywane były do dowodzenia siłami marynarki wojennej wzdłuż wybrzeża morskiego. W relacjach dowodzenia „brzeg-okręt" i między jednostkami pływającymi podstawowym środkiem łączności wykorzystywano łączność radiową i satelitarną.

Wszystkie Garnizonowe Węzły Łączności podporządkowane były danemu dowódcy Rodzaju Sił Zbrojnych.

3.3.2 Aktualna struktura organizacyjno - techniczna stacjonarnej sieci teleinformatycznej SZ RP

Na podstawie przeprowadzonych badań, wykorzystując do tego celu takie metody empiryczne, jak sondaż diagnostyczny techniką obserwacji (Arkusz obserwacji dotyczący czynników powodujących niedomagania w zakresie prawidłowego funkcjonowania sieci teleinformatycznej – **zał. 7**) oraz metody teoretyczne, jak analizę syntezę, porównanie, uogólnienie, abstrahowanie poparte doświadczeniem zawodowym autora wyodrębniono grupę czynników powodujących niedomagania funkcjonowania sieci teleinformatycznej Sił Zbrojnych, powodujących znaczne osłabienie systemu dowodzenia.

Z dniem 1 stycznia 2007 r., zgodnie z Decyzją Ministra Obrony Narodowej Nr Z-63/Org/P1 z dnia 06.12.2005 r. w sprawie zmian organizacyjnych i etatowych stacjonarnego systemu łączności Wojsk Lądowych, Wojskowy System Telekomunikacyjny rozpoczął funkcjonowanie w nowej strukturze organizacyjnej.



Rys. 3.5 *Stacjonarny system łączności SZ po reorganizacji od 01.01.2007 r.*

Źródło: Opracowanie własne na podstawie „ Strategii Informatyzacji Sił Zbrojnych RP"

Z dotychczasowych 82 GWŁ pozostających w podporządkowaniu Inspektoratu Wsparcia Sił Zbrojnych Rzeczypospolitej Polskiej i Dowództwa Wojsk Lądowych utworzono osiem Regionalnych Węzłów Łączności obejmujących swym zasięgiem działania obszar całego kraju.

Natomiast w Marynarce Wojennej i Siłach Powietrznych powołano Centra Wsparcia Teleinformatycznego (CWT) odpowiedzialne wyłącznie za eksploatację systemów dowodzenia i łączności wykorzystywanych przez dany Rodzaj Sił Zbrojnych.

Celem reorganizacji stacjonarnego systemu łączności było zbudowanie struktury zapewniającej sprawne planowanie, budowę i zarządzanie eksploatowanymi siłami i środkami szeroko rozumianej sieci teleinformatycznej resortu Obrony Narodowej.

Przyjęta organizacja miała umożliwić również elastyczną ***rekonfigurację systemu wymuszoną sytuacjami kryzysowymi lub działaniami wojennymi.***

W trakcie prowadzonych ćwiczeń wojskowych pod kryptonimem : „Stokrotka 07", i „Ogniwo 07" zostały zaobserwowane zasadnicze niedomagania w funkcjonowaniu sieci teleinformatycznej Sił Zbrojnych, które można scharakteryzować na podstawie dwóch czynników:

1. Ograniczona przepływność łączy.

W trakcie ww. ćwiczeń wojskowych zestawiane były połączenia sieci teleinformatycznej MIL-WAN w relacjach:

- CWŁ MON – GWŁ Sieradz;
- GWŁ Sieradz – RgWŁ Wrocław;
- RgWŁ Wrocław – RgWŁ Kraków;
- CWŁ MON – RgWŁ Wrocław;
- CWŁ MON – RgWŁ Kraków.

Teoretyczna przepływność zestawianych łączy wynosiła 2Mbit/s, co w praktyce do przesyłania meldunków w trakcie procesu dowodzenia jest wielkością wystarczającą. Jednak po głębszej analizie okazało się, że na routerach brzegowych na poszczególnych węzłach łączności dokonano podziału pasma na różne instytucje w danych miejscowościach co w konsekwencji zmniejszyło przepływność na potrzeby dowodzenia w trakcie prowadzonych ćwiczeń do wielkości ***uniemożliwiającej czasowe przesyłanie meldunków w systemie dowodzenia***.

2. Brak odpowiednich interfejsów na węzłach regionalnych.

Aby możliwa była rekonfiguracja systemu teleinformatycznego wymuszona sytuacjami kryzysowymi lub działaniami militarnymi koniecznym staje się zastosowanie mobilnych środków teleinformatycznych, które jak zostało to opisane we wstępie niniejszej dysertacji służą do uzupełnienia stacjonarnej sieci teleinformatycznej na poziomie strategicznym. Szybkie, bezkolizyjne włączanie systemu mobilnego do systemu stacjonarnego w celu jej uelastycznienia możliwe jest dzięki zastosowaniu przyłączy liniowych niezbędnych interfejsów. Dla teleinformatycznych środków mobilnych konieczny jest np. interfejs G703.

Z obserwacji w trakcie ćwiczeń z użyciem środków polowych zaobserwowano brak tego typu przyłączy liniowych co zasadniczo utrudnia połączenie obu systemów. Sytuacja ta w zdecydowany sposób ***uniemożliwia dynamiczną rekonfigurację systemów polowych w miejscach występowania zagrożeń***.

Jednak dokonane zmiany na mocy ww. Decyzją Ministra Obrony Narodowej umożliwiły w znaczący sposób zmniejsza ilość ogniw decyzyjnych oraz wykonawczych uczestniczących w procesie zapewnienia łączności najwyższym organom Administracji Państwowej oraz SZ RP.

Po dokonaniu zmian organizacyjnych obejmujących stacjonarną sieć teleinformatyczną funkcjonującą w SZ RP w systemie tym wyróżnia się niżej wymienione podsystemy:

a) <u>podsystem jawnej łączności telefonicznej</u>;

Jest to podsystem łączności przeznaczony do wymiany wiadomości jawnych na wszystkich szczeblach dowodzenia. Częściowo oparty jest on na technice analogowej. Część cyfrowa jest rozwijana w oparciu o nowoczesne centrale tranzytowo – końcowe i terminale abonenckie. Obecnie podsystem cyfrowy zrealizowany jest głównie w postaci sieci cyfrowej z integracją usług ISDN zapewnia on miedzy innymi łączność z utajnianiem indywidualnym źródła, a także cyfrową łączność faksową;

b) <u>podsystem cyfrowej łączności utajnionej (PCŁU)</u>;

PCŁU obejmuje swoim zasięgiem komórki organizacyjne i instytucje centralne MON, Dowództwa RSZ, ZT, brygady i samodzielne pułki. Podsystem łączności utajnionej przeznaczony jest do automatycznego zestawiania połączeń, przekazywania informacji fonicznych oraz transmisji danych (o klauzuli do TAJNE włącznie) pomiędzy osobami funkcyjnymi i komórkami organizacyjnymi SZ RP. Stanowi sieć bazową umożliwiająca dowiązanie mobilnych środków łączności zabezpieczających dowodzenie na poszczególnych szczeblach dowodzenia;

c) <u>podsystem powiadamiania i alarmowania</u>;

Podsystem jest przeznaczony do powiadamiania i alarmowania jednostek wojskowych oraz kadry w miejscach zamieszkania. Do alarmowania i powiadamiania jednostek wojskowych jest wykorzystywany Komputerowy Telefoniczny System Alarmowania (KTSA), oraz będący w fazie rozwoju System Alarmowania Resortu Obrony Narodowej (SARON);

d) podsystem łączności radiowej KF;

Podsystem łączności radiowej KF jest przeznaczony do zapewnienia wymiany informacji na potrzeby dowodzenia, współdziałania, alarmowania i powiadamiania na szczeblu strategicznym, operacyjnym i taktycznym, zarówno w okresie stałej jak i wyższych stanów gotowości bojowej. Na szczeblu strategicznym oraz w Wojskach Lądowych w czasie pokoju łączność radiowa KF stanowi system rezerwowy. W Marynarce Wojennej, zwłaszcza w relacjach brzeg-okręt oraz okręt (grupa okrętów) – okręt środki radiowe KF stanowią część składową infrastruktury technicznej stacjonarnych węzłów łączności;

e) podsystem łączności satelitarnej;

Obecnie jednostki wojskowe (pododdziały) znajdujące się poza krajem, wykorzystują łączność satelitarną, opartą na komercyjnych stacjach naziemnych zapewniających przepływności kanałowe rzędu 2,4 lub 4,8 kbit/s. Kanały satelitarne o ww. przepływności zapewniają przekazywanie informacji fonicznych, a po ukompletowaniu terminali naziemnych w dodatkowe urządzenia końcowe, również przesyłanie dokumentów. Wzrastające zaangażowanie SZ RP w operacjach wojskowych prowadzonych zarówno w ramach Sił Pokojowych ONZ, koalicyjnych jak i NATO determinuje konieczność wdrożenia własnego systemu łączności satelitarnej;

Docelowo, satelitarny system łączności SZ RP będzie zabezpieczał łączność operacyjną na potrzeby dowodzenia:

- wojskami stacjonującymi na terenie kraju;
- wojskami realizującymi zadania poza terytorium kraju – np. polskimi kontyngentami wojskowymi biorącymi udział w operacjach międzynarodowych;
- okrętami MW RP wydzielonymi do sił NATO.

f) podsystem łączności szyfrowo-kodowej;

Łączność szyfrowo - kodowa przeznaczona jest do wymiany dokumentów niejawnych stanowiących tajemnicę państwową o klauzulach „ŚCIŚLE TAJNE" i „TAJNE". W podsystemie łączności szyfrowo-kodowej wykorzystywane są urządzenia elektromechaniczne i szyfr klasyczny. Charakteryzuje się on dużą mocą kryptograficzną i jest jednym z podstawowych systemów łączności z jednostkami wykonującymi zadnia poza granicami kraju w ramach operacji ONZ i NATO;

g) lokalne i rozlegle sieci komputerowe;

W resorcie obrony narodowej kontynuowana jest budowa lokalnych i rozległych sieci komputerowych typu:

- SEC-WAN - przeznaczonej do przetwarzania, przechowywania i przesyłania informacji niejawnych;
- MIL-WAN - przeznaczonej do przetwarzania, przechowywania i przesyłania informacji jawnych;
- INTER-MON - przeznaczonej do dostępu do światowej sieci INTERNET i wymiany wiadomości jawnych z NATO.

3.4 Synteza wniosków z badań

Odpowiedź na pytanie zawarte w początkowej części tego rozdziału, w jakim stopniu zmiany organizacyjno – techniczne w obszarze stacjonarnej sieci teleinformatycznej Sił Zbrojnych, podjęte w latach 1995 – 2005, wpłynęły na realizację potrzeb dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej w czasie pokoju, kryzysu i zagrożenia militarnego państwa, po przyprowadzonej analizie oraz syntezy dokumentów normatywnych należy stwierdzić, że na realizację procesu dowodzenia wpłynęły w następujący sposób:

1) dokonano transformacji technologicznej stacjonarnego systemu teleinformatycznego z techniki analogowej na technikę cyfrową dzięki czemu wzrosła dokładność oraz jakość przekazywanych danych;
2) zwiększyła się sprawność i przepustowość systemów teleinformatycznych, co umożliwia zwiększenie ilości danych przetwarzanych w systemie dowodzenia;
3) stworzono warunki do projektowania nowoczesnej w pełni zarządzanej jednolitej technologicznie struktury wojskowego stacjonarnego systemu teleinformatycznego, zdolnego do realizacji zadań systemu dowodzenia SZRP w czasie pokoju, kryzysu i zagrożenia militarnego państwa;
4) wdrożono w poszczególnych Rodzajach Sił Zbrojnych Zautomatyzowane Systemów Dowodzenia, co z kolei usprawnia i unowocześnia system dowodzenia SZ RP;
5) wskutek wdrożenia nowoczesnych rozwiązań technologicznych stworzono możliwość do funkcjonowania struktur organizacyjnych posiadających możliwości zdalnego zarządzania elementami stacjonarnej sieci teleinformatycznej;

6) budowana struktura organizacyjna dąży w kierunku powstawania elementów zarządzania zapewniających sprawne planowanie i elastyczną rekonfigurację systemu wymuszoną sytuacjami kryzysowymi lub działaniami wojennymi, znacznie zmniejsza ilość ogniw decyzyjnych oraz wykonawczych uczestniczących w procesie zapewnienia łączności;

Stacjonarna sieć teleinformatyczna zorganizowana jest zgodnie z potrzebami systemu dowodzenia i współdziałania tak podaje „ Strategia Informatyzacji Sił Zbrojnych RP". Zmiany doktrynalne, organizacyjne i techniczne w obszarze jej funkcjonowania mają na celu zapewnienie zaspokojenia oczekiwań związanych z procesem dowodzenia SZ RP. Przywoływane zmiany podyktowane są szeregiem czynników z których najważniejsze to:

- konieczność działania w środowisku sojuszniczym i koalicyjnym (zobowiązania wobec NATO i Unii Europejskiej, udział SZ RP w międzynarodowych komponentach militarnych, udział w misjach pokojowych i stabilizacyjnych);
- potrzeba osiągnięcia zdolności sieciocentrycznej;
- osiągnięcie przewagi informacyjnej;
- dynamiczny rozwój dostępnych technologii teleinformatycznych oraz sytuacji geopolitycznej.

Podjęte przez resort obrony narodowej działania dążą do konstruowania modelu systemu telekomunikacyjnego uwzględniającego organizację i topologię spełniającą nowoczesne wymogi poszczególnych klas systemów dowodzenia, wynikających z zasad Net Centric Warfare (NCW), tzn.:

- C4I2 (ang. Command, Control, Communication, Computers, Intelligence and Information) – sieć dowodzenia;
- C2IS (ang. Command, Control, Information System) – sieć wspomagania dowodzenia;
- C4ISR (ang. Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance) – sieć pozyskiwania i przetwarzania danych (sensorowa sieć rozpoznania).

Na podstawie analizy podjętych działań można również przyjąć tezę, że funkcjonująca stacjonarna sieć teleinformatyczna SZ RP jest systemem otwartym. W praktyce wiąże się to z procesem ciągłej weryfikacji i aktualizowania zasobów systemu oraz jego struktur organizacyjnych. Działania podejmowane na rzecz

rozwoju sieci teleinformatycznej w obecnej chwili i tak są spóźnione do nowych wyzwań jakie nam przynosi dynamiczny rozwój nowych technologii.

Zmiany technologiczne i coraz większe zapotrzebowanie użytkowników wojskowego systemu telekomunikacyjnego na nowoczesne usługi teleinformatyczne, wymusza modelowanie systemu w kierunku coraz silniejszego osadzenia go w publicznej przestrzeni telekomunikacyjnej z zastrzeżeniem pełnego zdefiniowania charakteru resortowe sieci telekomunikacyjnej.

Na szczeblu strategicznym łączność organizowana jest w całości w oparciu o system stacjonarny. Dotyczy to zarówno węzłów łączności obsługujących stanowiska dowodzenia jak również powiązań teleinformatycznych. W czasie kryzysu i zagrożenia militarnego państwa stacjonarny system będzie wzmacniany potencjałem z zasobów komercyjnych operatorów telekomunikacyjnych.

Reorganizacja organów zarządzających systemem telekomunikacyjnym SZ RP oraz elementów tworzących stacjonarną sieć teleinformatyczną SZ RP przeprowadzona w roku 2007 w znaczący sposób stwarza warunki do uelastycznienia funkcjonowania stacjonarnego systemu teleinformatycznego w wymuszonych sytuacjach kryzysowych lub działaniach wojennych. ***Jednak w celu pełnej realizacji założonych celów koniecznym staje się podjęcie działań w celu budowy szkieletu sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej oraz budowy przyłączy liniowych niezbędnych interfejsów na węzłach łączności sił zbrojnych i kluczowych operatorów telekomunikacyjnych***.

Istotną zmianą jest odbiegnięcie od ścisłego powiązania rozmieszczenia elementów systemu stacjonarnego ze strukturami organizacyjnymi SZ RP na rzecz uwarunkowań geograficznych. Powyższa zmiana zapewnia możliwość rekonfigurowania systemu dowodzenia bez konieczności modyfikowania systemu łączności oraz ma zapewnić równomierne nasycenie elementami systemu całego obszaru Polski.

Stworzenie jednolitych struktur organizacyjno-technicznych Rejonowych Węzłów Łączności oraz utrzymywanie ich w pełnej gotowości do użycia zabezpiecza podnosi skuteczność funkcjonowania rozwijanych w ZMP stanowisk dowodzenia i kierowania.

Przyjęta struktura organizacyjna organów kierujących i zarządzających stacjonarną siecią teleinformatyczną rozdziela kompetencje w tym zakresie pomiędzy:

1) Departament Informatyki i Telekomunikacji MON - obszar związany z techniczną eksploatacją, implementacją i rozwojem stacjonarnej sieci teleinformatycznej SZ RP;
2) Zarząd Planowania Systemów Dowodzenia i Łączności P-6 – obszar związany z planowaniem organizacji i funkcjonowania systemów teleinformatycznych funkcjonujących w ramach WSyD.

Obszarem wspólnych działań obydwu komórek organizujących Wojskowy System Telekomunikacyjny jest działalność w zakresie budowy modelowego systemu teleinformatycznego. Szczegółowe kompetencje zarządzania stacjonarnym systemem teleinformatycznym SZ RP skupione zostały w jednym punkcie – Centrum Zarządzania Systemami Teleinformatycznymi (CZST). W CZST zaplanowano narzędzia umożliwiające działania związane ze sterowaniem, monitorowaniem i rejestrowaniem użycia zasobów sieci, w celu zapewnienia jej efektywnego wykorzystania zgodnie z przeznaczeniem i adaptacją do warunków występujących w jej otoczeniu.

Po przeprowadzeniu głębokiej analizy oraz syntezy przedstawionych aktów prawnych przedstawionych w załączniku (Zbiór dokumentów formalno – prawnych – **zał. 2**) próba odpowiedzi na pytanie **w jakim stopniu aktualne regulacje ustawowe określają zasady współpracy operatorów telekomunikacyjnych z Siłami Zbrojnymi Rzeczypospolitej Polskiej w czasie pokoju, kryzysu i zagrożenia militarnego państwa**, należy stwierdzić, że odpowiedzialnym za przygotowanie i utrzymanie zapasowych stanowisk kierowania dla: Prezydenta Rzeczypospolitej Polskiej, Prezesa Rady Ministrów oraz ministrów i centralnych organów administracji rządowej (wskazanych przez Prezesa Rady Ministrów) jest **Minister Obrony Narodowej**.

Z racji odpowiedzialności Ministra Obrony Narodowej za przygotowanie i utrzymanie zapasowych stanowisk kierowania dla wskazanych organów władzy publicznej wynika fakt przygotowania utrzymania wewnętrznych sieci teleinformatycznych danego stanowiska kierowania.

Pomimo podjęcia szeregu decyzji organizacyjnych wpływających na kształt struktury oraz organizacji stacjonarnego systemu teleinformatycznego SZ RP daje się zauważyć coraz większy dystans i rozdźwięk pomiędzy funkcjonowaniem nowoutworzonej struktury a zbiorem aktualnie obowiązujących zasad świadczenia

usług przez publicznych operatorów telekomunikacyjnych na rzecz systemu wojskowego.

Powyższa teza nie oznacza jednak „totalnego chaosu" organizacyjnego, ma podkreślać jednak pogłębiającą się dysharmonię pomiędzy faktycznymi oczekiwaniami stacjonarnego systemu teleinformatycznego w zakresie jego uzupełnienia (wsparcia) przez operatorów publicznych w czasie pokoju, kryzysu i zagrożenia militarnego.

4. ZAGROŻENIA I CZYNNIKI WPŁYWAJĄCE NA FUNKCJONOWANIE STACJONARNEJ SIECI TELEINFORMATYCZNEJ UŻYTKOWANEJ PRZEZ SIŁY ZBROJNE RZECZYPOSPOLITEJ POLSKIEJ

Celem badań, których wyniki przedstawiono w tym rozdziale, było określenie, ***jakie zagrożenia i czynniki wpływają na funkcjonowanie stacjonarnej sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej?***

Aby osiągnąć tak sformułowany cel, gruntownej analizie poddano warunki oraz środowisko, w których funkcjonuje sieć teleinformatyczna sił zbrojnych RP. Następnie po określeniu elementów, czynników wpływających na bezpieczeństwo, możliwe stanie się wskazanie najistotniejszych zagrożeń, które odgrywać będą rolę decydującą. Autor przeprowadził sondaż diagnostyczny techniką obserwacji (Arkusz wywiadu dotyczący zagrożeń i czynników wpływających na poprawne funkcjonowanie stacjonarnej sieci teleinformatycznej – **zał. 7**)

4.1 Czynniki wpływające na funkcjonowanie sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej

W otoczeniu sieci teleinformatycznej można zidentyfikować wiele czynników charakterystycznych i wpływających na funkcjonowanie sieci teleinformatycznej.

Badania literatury przedmiotu pozwalają na przytoczenie różnych punktów widzenia na wspomniane zbiory czynników. W pracach Krystiana Baniaka przedstawiciela Alcatel – Lucent Polska zastały precyzyjnie zdefiniowane obszary zagrożeń w ramach infrastruktury telekomunikacyjnej :

Organizacja – formalny podmiot sprawujący kontrolę nad daną infrastrukturą telekomunikacyjną.

Personel – pracownicy zarządzający, korzystający i utrzymujący daną infrastrukturę.

Polityka Bezpieczeństwa – założenia, standardy, procedury, wytyczne, normatywy bezpiecznego korzystania z infrastruktury w ramach danej organizacji.

Placówki – obiekty fizyczne należące do organizacji (budynki, obiekty techniczne).

Infrastruktura – środki technologiczne – elementy zapewniające funkcjonowanie organizacji, przetwarzanie i przesyłanie informacji.

Powyższy podział elementów składowych infrastruktury pozwala na wyłonienie najważniejszych zbiorów czynników, które są wynikiem obserwacji i analiz, bardzo często opisywanych w zestawieniach zagrożeń telekomunikacyjnych[38] [39] [40].

Środowisko/Energia – systemy zasilania, wentylacji, klimatyzacji, uzdatniania powietrza (ang. HVAC) oraz bezpieczeństwa fizycznego.

Technologia – sprzęt oraz oprogramowanie.

Dane/transmisja – sieci transmisyjne ich topologie, redundancja, synchronizacja. W przypadku transmisji są to metody przechowywania, reprezentacji oraz przesyłania danych.

Czynnik Ludzki – polityka bezpieczeństwa, świadomość personelu jak i użytkownika końcowego, wpływ regulacji prawnych, zagadnienia związane z etyką pracy. Jest to najważniejszy obszar zagrożeń gdyż jest on najbardziej nieprzewidywalny.

Zagrożenia obszaru środowiskowego

- Występowanie katastrof naturalnych: powodzi, huraganów, trzęsień ziemi;
- Zawodność systemów energetycznych oraz zasilania zapasowego (dostępność paliwa, zagrożenie pożarowe składów paliwa);
- Sabotaż oraz zagrożenia terrorystyczne instalacji i obiektów fizycznych;
- Odporność na włamania i szczelność systemów kontroli dostępu - bezpieczeństwo lokalizacji:
    - łatwość obserwacji przez osoby postronne;
    - polityczne i kryminalne uwarunkowania danej lokalizacji geograficznej (np. występowanie zamieszek, niestabilność polityczna regionu);
    - odległość od zabudowań i terenów publicznych – dostępność;
    - ogrodzenia, czujniki, monitoring środki ochrony bezpośredniej;
    - ochrona fizyczna, szkolenie i zaufanie do kadry.
- Nieskuteczny system monitorowania i analizy logów;

---

[38] *Availability and Robustness of Electronic Communications Infrastructures, January 2007, Report for European Commission prepared by Alcatel-Lucent.*

[39] *Rauscher, Karl F., Protecting Communications Infrastructure, Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2, 2004;*

[40] *Rauscher, Karl F., Krock, Richard E., Runyon, James P., Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2, 2004*

- Zależność od zasobów i wsparcia, które nie są trwałe.

Możliwość wykorzystania słabości ochrony fizycznej jest o tyle niebezpieczne, iż eliminacja dobrze wybranej placówki może oznaczać powstanie szkód o zakresie globalnym dla danej organizacji. Związane jest przez występowanie skomplikowanych powiązań i zależności pomiędzy systemami korzystającymi z infrastruktury krytycznej.

Bezpieczeństwo energetyczne polega na zapewnieniu wielu źródeł zasilania w niezbędne do funkcjonowania elementy. Jednym z poważniejszych zagrożeń fizycznych jest często zależność od jednej elektrowni lub systemu dostaw (w przypadku procesów produkcji).

Zagrożenia obszaru technologicznego

- brak mechanizmów zwielokrotniania i redundancji sprzętowej i logicznej (np. brak alternatywnych torów transmisyjnych);
- występowanie błędów produkcyjnych lub konstrukcyjnych (błędy logiczne trudne do wykrycia), które mogą być szczególnie niebezpieczne w przypadku uzależnienia od jednego dostawcy sprzętu;
- jakość oprogramowania - występowanie błędów, kosztowne procedury testowania poprawek i wdrażania ich w życie. Poprawki oprogramowania mogą doprowadzić do destabilizacji pracy systemu poprzez zmianę lub unieruchomienie logiki działania aplikacji;
- bezpieczeństwo oprogramowania – występowanie błędów pozwalających na przejęcie kontroli nad aplikacją/sprzętem;
- odporność technologii transmisji na przechwycenie i zakłócenia elektromagnetyczne oraz na warunki środowiskowe;
- cykl życia urządzeń i czas do pierwszej awarii;
- odporność na warunki pracy i wpływ środowiska.

Odpowiednio zaprojektowany i wykonany sprzęt oraz oprogramowanie jest kluczem do sukcesu w tym obszarze. Niestety rzeczywistość jest inna i należy zwrócić dużą uwagę na poprawne podejście do kwestii wyboru i procedur użytkowania. Ważnym aspektem jest też posiadanie rozwiązań alternatywnych (dywersyfikacja dostawców) oraz odpowiedni cykl życiowy wyposażenia. Nie należy

wprowadzać nowych rozwiązań bez uprzednich testów zgodności ze standardami i deklaracjami producenta. Wewnętrzne standardy organizacji powinny mieć najwyższy priorytet w tej kwestii gdyż wiążą się bezpośrednio z sprawnością operacyjną instytucji.

W przypadku rozwiązań telekomunikacyjnych istotną kwestią jest także odporność na zakłócenia elektromagnetyczne oraz niski poziom strat w postaci emisji wtórnej. Istotne podsystemy przetwarzające informację poufną i tajną powinny unikać technologii otwartego dostępu typu WiFi bez dodatkowych zabezpieczeń (lub w ogóle). Należy brać pod uwagę możliwości podsłuchania lub zapisania transmisji poprzez emisję elektromagnetyczną lub nielegalne podpięcie się do systemu i przedsięwziąć odpowiednie środki kontroli na wyższych warstwach kanału informacyjnego (na poziomie transportowej lub aplikacyjnej modelu OSI).

Odporność technologii wykorzystywanych w infrastrukturze powinna uwzględniać warunki pogodowe i kalkulować sytuacje ekstremalne występujące w regionie użytkowania. Radiolinie – planowanie radiowe, dla przykładu, powinno uwzględniać zmienne warunki takie jak deszcz, śnieg i zapewniać odpowiedni margines tolerancji. Wiąże się to z odpowiednim procesem planowania i określania warunków brzegowych dla infrastruktury (bezpieczna metodologia).

Zagrożenia obszaru danych i sieci

- techniki transmisji (np. bezprzewodowe) oraz protokoły przesyłania danych (nieszyfrowane) nie zawsze umożliwiają poufny, integralny oraz uwierzytelniony przekaz (potwierdzenie deklarowanego źródła lub odbiorcy przekazu);
- topologie projektowanych sieci mogą nie zapewniać odporności na uszkodzenia lub pracować z mniejszą niż szacowana wydajnością – problem poprawnego projektowania i skalowalności;
- jakość implementacji standardów w szczególności jest przyczyną braku kompatybilności pomiędzy sprzętem różnych dostawców;
- synchronizacja (niepoprawna, uszkodzona) sieci i elementów toru transmisji może być źródłem problemów;
- zarządzanie i aktualizacja oprogramowania oraz konfiguracji urządzeń sieciowych (bezpieczeństwo);

- stopień skomplikowania stanowi zagrożenie dla funkcjonowania – łatwość popełnienia pomyłki.

Sieci komputerowe i telekomunikacyjne są podstawą systemów wymiany informacji. Projektowanie i opieka nad wdrożeniem i utrzymaniem tych systemów jest więc kluczowa. Dziurawy i nieefektywny system wymiany danych będzie łatwo kompromitowany i mało użyteczny. W krytycznym momencie jest tym co ma działać pewnie i efektywnie. Istotnym zagadnieniem jest etap planowania, zwłaszcza w kontekście pojemności i wydolności sieci, która ma zapewnić parametry w sytuacji kryzysowej, która często wiąże się ze znacznym wzmożeniem ruchu.

Infrastruktura krytyczna w postaci sieci transmisyjnych powinna więc zapewniać następujące wymogi:

- topologia charakteryzuje się odpornością na uszkodzenia (redundantny sprzęt oraz alternatywne trasy) i adaptacją do zmieniających się warunków (występowanie awarii);
- transmisja jest bezpieczna – informacje są przesyłane w poufny nienaruszony sposób. Osoby trzecie nie są w stanie wprowadzić zakłóceń lub uzyskać dostępu;
- konfiguracja i zarządzanie siecią jest zdefiniowanym cyklicznym oraz udokumentowanym procesem;
- personel jest przygotowany i przeszkolony w obsłudze sytuacji kryzysowych – każdy wie co ma robić i do kogo raportuje – sytuacje te są regularnie ćwiczone w praktyce;
- zdefiniowano plan współpracy z partnerami polegający na wzajemnej pomocy w sytuacjach kryzysowych (wykorzystanie zasobów innej organizacji).

Zagrożenia obszaru czynnika ludzkiego

- zagrożenia fizyczne – kradzież, sabotaż, terroryzm;
- zagrożenia mentalne – intencja oszukania, wprowadzenia w błąd, zmiany opinii publicznej na temat podmiotu;
- zagrożenia etyczne – niezadowoleni obywatele, pracownicy, zemsta;
- zagrożenia organizacyjne – nieświadome działanie szkodliwe wynikające z niewiedzy użytkownika systemu;
- brak Polityki Bezpieczeństwa;

- nierealistyczna lub niejednoznaczna Polityka Bezpieczeństwa (PB);
- brak wsparcia kardy menedżerskiej dla egzekucji PB;
- nierealistyczne regulacje prawne i luki prawne;
- brak szkoleń i kampanii uświadamiających użytkowników.

Czynnik ludzki jest odpowiedzialny za niedoskonałość rozwiązań jak i za wykorzystywanie systemów w celach nieprzewidzianych jak i niedozwolonych. Jest on źródłem ustawicznych problemów w każdym systemie informacyjnym. Kluczowym jest więc uprzedzanie faktów oraz precyzyjne definiowanie przeznaczenia systemu na etapie przygotowywania Polityki Bezpieczeństwa. Polityka Bezpieczeństwa, będąc zbiorem dozwolonych czynności w ramach systemu, w konsekwencji tłumaczy się na ustalenia, dobór standardów, procedur, wytycznych i regulacji, które znowu realizowane są przy pomocy środków kontroli. Zawodności czynnika ludzkiego nie jesteśmy w stanie wyeliminować więc realistyczny i w pełni wdrożony projekt Polityki Bezpieczeństwa jest jedynym optymalnym rozwiązaniem tego problemu.

Analiza zagrożeń opiera się na wiedzy odnośnie problemów i zachowań ludzi, którzy je powodują. Wiedza ta pochodzi z doświadczeń i obserwacji wynikających z użytkowania systemów komunikacyjnych. Jednakże metoda ta nie pozwala przewidzieć nowych elementów, nie jest w stanie zgłębić ludzkiej pomysłowości.

Natomiast Andrzej Machnacz dyrektor Biura Łączności i Informatyki w Komendzie Głównej Policji do czynników wpływających na bezpieczne funkcjonowanie systemów teleinformatycznych zalicza przede wszystkim czynnik ludzki:

Zagrożenia ludzkie zewnętrzne spowodowane poprzez celowe lub przypadkowe działanie ze strony osób nieuprawnionych mogą być wynikiem:

- ataku terrorystycznego na obiekty, w których zainstalowane są podstawowe urządzenia systemów teleinformatycznych, zdalnego wprowadzenia do systemu oprogramowania złośliwego, zdalnego uzyskania uprawnień, ataku impulsem elektromagnetycznym, użycia materiałów wybuchowych;
- zdalnego lub bezpośredniego skopiowania danych lub kradzieży nośników, na których dane te są przechowywane;

- podsłuchu łączy teletransmisyjnych, telekomutacyjnych i bezprzewodowych, podszycia się pod uprawnionego użytkownika, skopiowania wydruków, przejmowania ulotu elektromagnetycznego;
- zablokowania linii teletransmisyjnej lub telekomutacyjnej, przeciążenia systemu informacyjnego w wyniku generowania dużej ilości wiadomości lub niedostępności usług telekomunikacyjnych wynikających z zaniechania działań po stronie dostawcy usługi lub awarii łączy telekomunikacyjnych;
- odcięcia zasilania podstawowych urządzeń systemów teleinformatycznych w wyniku przerwy w dostawach energii elektrycznej, spowodowanej zaniechaniem działań po stronie dostawcy lub awarii infrastruktury;
- celowego modyfikowania informacji w czasie ich przesyłania łączami teletransmisyjnymi lub telekomutacyjnymi, generowania zakłóceń w liniach przesyłowych;
- celowego wykorzystania błędów oprogramowania urządzeń zabezpieczających np. typu zapora sieciowa.

Zagrożenia ludzkie wewnętrzne *spowodowane poprzez celowe lub* przypadkowe działanie ze strony osób uprawnionych mogą być wynikiem:

- uszkodzenia urządzeń lub oprogramowania systemów teleinformatycznych w wyniku działań sabotażowych lub błędów obsługi (błędy utrzymania i eksploatacji), wprowadzenia oprogramowania złośliwego, uzyskania przez uprawnionego użytkownika nieprzysługujących mu uprawnień, np. uzyskanie uprawnień administratora, a także użycia oprogramowania przez nieautoryzowanych użytkowników, niewłaściwego użycie zasobów, tzn. niezgodnego z właściwymi procedurami eksploatacyjnymi;
- nieautoryzowanego skopiowania wszystkich lub wybranych informacji z systemów teleinformatycznych przez nieuprawnionego do takich działań użytkownika, lub skopiowania danych z nośników, na których dane są archiwizowane, wprowadzenia oprogramowania złośliwego lub modyfikacji oprogramowania w sposób umożliwiający zdalny dostęp do informacji przechowywanych w systemach teleinformatycznych;
- przejmowania informacji przesyłanych siecią teletransmisyjną lub telekomutacyjną, uzyskania nieuprawnionego dostępu do terminala innego użytkownika, przypadkowego wysłania niezaszyfrowanych danych;

- zmodyfikowania zasobów systemów teleinformatycznych przez uprawnionego użytkownika, uzyskania nieprzysługujących uprawnień do wszystkich lub wybranych zasobów systemów teleinformatycznych;
- uzyskania nierejestrowanego dostępu do zasobów systemu teleinformatycznych, podszycia się pod innego uprawnionego użytkownika, zniszczenia lub modyfikacji rejestrów aktywności określonych składowych systemu teleinformatycznych przez uprawnionego użytkownika lub nieuprawnionego dostępu do tych rejestrów;
- nielegalnego instalowania oprogramowania niezwiązanego z działalnością MSWiA i funkcjami systemów teleinformatycznych, a także użycia narzędzi sieciowych lub innego oprogramowania w nieautoryzowany sposób;
- celowego lub spowodowanego błędem obsługi unieruchomienia systemów teleinformatycznych lub wybranych ich składowych, np. urządzeń systemu łączności, zasilania itp.;
- przejmowania i następnie modyfikowania informacji przesyłanych siecią teletransmisyjną lub telekomutacyjną.

Zagrożenia wywołane czynnikami środowiskowymi również mogą być wynikiem utraty dostępności informacji i usług systemów teleinformatycznych, spowodowanej wystąpieniem powodzi, pożaru, wyładowań atmosferycznych itp. Na przykład uderzenie pioruna w budynek, w którym znajdują się elementy systemu teleinformatycznego może spowodować pożar lub awarię infrastruktury teleinformatycznej na skutek wystąpienia przepięć w sieci energetycznej. Zagrożenia spowodowane ***czynnikami środowiskowymi i technicznymi*** są związane przede wszystkim z możliwością utraty lub uszkodzenia danych dostępnych w systemach teleinformatycznych. Na przykład awaria komputerów, serwerów, pamięci masowych, elementów sieci komputerowej lub innych urządzeń teleinformatycznych wynikająca z wad sprzętu, a także awarie spowodowane błędami programistów nie wykryte podczas realizacji testów, mogą spowodować brak dostępu do zasobów krytycznej infrastruktury teleinformatycznej.

Z kolei Jacek Matyszczak przedstawiciel Departamentu Spraw Obronnych Urzędu Komunikacji Elektronicznej do najważniejszych elementów mających wpływ

na bezpieczeństwo zalicza przede wszystkim czynnik ludzki, czyli działania głównie działania o charakterze terrorystycznym. Mogą być one realizowane w formie bezpośredniego fizycznego ataku na elementy infrastruktury telekomunikacyjnej, albo pośrednio poprzez oddziaływanie na inne elementy infrastruktury krytycznej. Pod pojęciem infrastruktury krytycznej rozumiemy kluczowe elementy gospodarki narodowej, których uszkodzenie lub zniszczenie miałoby negatywny wpływ na funkcjonowanie społeczeństwa, zagrażając bezpieczeństwu lub gospodarce państwa.

W atakach terrorystycznych mogą być wykorzystywane:

- konwencjonalne ładunki wybuchowe lub broń biologiczna i chemiczna;
- urządzenia wytwarzające wysokoenergetyczne impulsy elektromagnetyczne;
- środki informatyczne do zdobywania kodów i haseł;
- sieć Internetowa - za jej pomocą wykonuje się działania blokujące, niszczące.

4.2 Zagrożenia wpływające na funkcjonowanie sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej

Podejmując próbę dokonania podziału oraz charakterystyki zagrożeń bezpieczeństwa informacji w sieci teleinformatycznej należy scharakteryzować, a następnie zdefiniować, co rozumiemy pod pojęciem zagrożenia bezpieczeństwa informacji.

W myśl dokumentów sojuszniczych[41] ogólne pojecie zagrożenia bezpieczeństwa *(ang. breach of security*[42]*)* przyjmowane jest jako każde postępowanie sprzeczne z ogólnymi lub miejscowymi przepisami bezpieczeństwa bądź pomijanie tych przepisów, w wyniku czego rośnie ryzyko nieuprawnionego ujawnienia informacji niejawnych NATO i może dojść do ich utraty.

W ujęciu amerykańskim[43] zagrożeniem jest każdy „dokuczliwy" atak, który potencjalnie może wpłynąć na powstanie ryzyka utraty bezpieczeństwa narodowego.

---

[41] CM-55(final), Polityka bezpieczeństwa NATO, cz.IX, § 4
[42] Dokument NATO serii AMSG 524 – „Słownik pojęć i definicji z zakresu bezpieczeństwa łączności i informatyki"
[43] R.H Anderson, Securing the U.S. Defense Information Infrastructure: A Proposed Approach, National Defense Research Institute, RAND 1999, s. 5

Przedstawione definicje traktują omawiany problem w sposób ogólny, ale pozwalają na wyrobienie poglądu czym jest i jak rozumiane jest pojęcie zagrożenia bezpieczeństwa zarówno narodowego (USA) jak i sojuszniczego (NATO).

Zagadnienia związane z zagrożeniami bezpieczeństwa informacji w sieciach informatycznych, telekomunikacyjnych czy teleinformatycznych w tym kontekście są pojęciem bardziej szczegółowym.

Ogólnie rzecz ujmując, z zagrożeniem systemów lub sieci mamy do czynienia wówczas, gdy istnieje możliwość narażenia na szwank ich bezpieczeństwa na skutek utraty poufności, utraty integralności bądź utraty dostępu do systemu lub sieci. Słabe punkty można określić jako brak kontroli lub niewystarczającą kontrolę, w wyniku czego zwiększa się ryzyko zagrożenia bezpieczeństwa zasobów informacyjnych systemu bądź sieci. Słaby punkt to np. pomijanie lub upraszczanie procedur kontroli. Słaby punkt może mieć charakter techniczny, proceduralny czy operacyjny.

Informacje niejawne przechowywane w systemach i sieciach teleinformatycznych w sposób zintegrowany i w postaci gotowej do szybkiego przetworzenia, przekazania i użytku mogą stanowić słaby punkt ze względu na ryzyko ich nieuprawnionego ujawnienia bądź wykorzystania przez osoby nieupoważnione lub nie posiadające prawa dostępu. Ponadto gromadzone w ten sposób informacje są narażone na kradzież, zniekształcenie treści i zniszczenie. Co więcej, sprzęt teleinformatyczny (łączności i informatyki), podatny na uszkodzenia i niekiedy bardzo skomplikowany technologicznie, jest kosztowny i często trudno go szybko naprawić czy wymienić. Dlatego takie systemy i sieci teleinformatyczne stanowią atrakcyjny cel działań potencjalnego przeciwnika[44].

Opisane w poprzednim rozdziale czynniki mające zasadniczy wpływ na bezpieczeństwo sieci teleinformatycznej przekładają się bezpośrednio na występowanie opisanych zagrożeń. Należy podkreślić, że im bardziej rozwinięta jest infrastruktura teleinformatyczna, czyli im większe jest nasycenie urządzeniami aktywnymi oraz im większa jest sieć połączeń tym bardziej narażona jest na różnego rodzaju zagrożenia. Choć węzły łączności aktywnie uczestniczą w budowie Wojskowego Systemu Telekomunikacyjnego opartego na szkielecie systemu teletransmisyjnego Sił Zbrojnych jako podstawowego elementu organizacji różnej klasy systemów dowodzenia (od sieci dowodzenia poprzez sieci wspomagania

[44] Dyrektywa bezpieczeństwa AD-70/PL, cz.5, § 1

dowodzenia do sieci pozyskiwania i przetwarzania danych) to aktualnie budowana struktura teletransmisyjna zapewniająca wszechstronne i optymalne warunki do funkcjonowania „klasycznego" systemu komutacyjnego Sił Zbrojnych jest w małym stopniu narażona na incydenty lub różnego rodzaju zdarzenia w sieci teleinformatycznej.

W celu zapewnienia wysokiego priorytetu bezpieczeństwa Wojskowego Systemu Telekomunikacyjnego oraz osiągnięcia zdolności szybkiej rekonfiguracji i dostosowania szkieletu do potrzeb dowodzenia systemem, koniecznym staje się wykorzystanie nowoczesnych technologii teletransmisyjnych bazujących na fizycznej warstwie kabli optotelekomunikacyjnych i linii radiowych wzmocnionych komponentami łączy satelitarnych oraz cyfrowym systemem radiowej łączności KF – z zachowaniem hierarchicznej architektury systemu.

Aktualne działania modernizacyjne zachodzące w stacjonarnym systemie teleinformatycznym Sił Zbrojnych w pełni uwzględniają charakter i przeznaczenie systemu telekomunikacyjnego do doktryny wojny sieciocentrycznej, która stawia olbrzymie wymagania dla skutecznej organizacji systemu dowodzenia i łączności kładąc nacisk na umożliwienie szerokiego dostępu stanowisk dowodzenia do pozyskiwania danych, szybkiego ich przetwarzania i wykorzystania w procesach decyzyjnych.

Ten tak bardzo szybki rozwój technologiczny powoduje, że w krótkim czasie wszelkiego rodzaju zagrożenia będą dotyczyły także naszej sieci teleinformatycznej i dlatego jak wspomniałem wcześniej rozpoznawanie zagrożeń jest bardzo konieczne dla zachowania ciągłości funkcjonowania sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej. Możemy wyróżnić dwa zasadnicze rodzaje zagrożeń dla systemów teleinformatycznych[45]:

- mających miejsce w cyberprzestrzeni;
- ataki fizyczne na systemy informatyczne.

W dokumentach NATO [46] [47], można znaleźć m.in. następujące definicje dotyczące zdarzeń i incydentów komputerowych mających ścisły związek z cyberprzestrzenią.

---

[45] *Cybrterroryzm i problemy informacyjne we współczesnym świecie.*
[46] *NATO Computer Incident Response Capability (DCI-CC5), Annex 1, AC/322-WP/0223-REV1-CIRC.*
[47] *NATO Computer Incident Response Capability, Annex 1, AC/322-N/0648.*

Zdarzenia (ang. event) – to każde widoczne wydarzenie w systemach teleinformatycznych. Przykłady zdarzeń obejmujących m.in. zakłócenia w pracy systemu oraz „zalanie" sieci pakietami danych. Zdarzenia przyciągają coraz większą uwagę głównie z powodu rozpowszechniania zastosowań sieci komputerowych (Internet i Intranet), które narażone są na nieautoryzowany dostęp oraz na ogromną ilość kodów złośliwych. Wystąpienie zdarzenia czasem może wskazywać na pojawienie się incydentu i wymaga właściwej reakcji.

Incydent (ang. incident) – pojęcie to odnosi się do niekorzystnych zdarzeń w systemach teleinformatycznych lub do zagrożenia wystąpienia takiego zdarzenia. Przykłady incydentów obejmują m.in. utratę poufności danych, zakłócenie (ang. disruption) danych lub integralności system, lub zakłócenie – odmowę dostępności, np. nieautoryzowane użycie konta innego użytkownika, nieautoryzowane użycie prawa dostępu (ang. system privileges) oraz wprowadzenie złośliwych kodów, które niszczą informacje. Inne niekorzystne zdarzenia obejmują: powodzie, pożary, zakłócenia w zasilaniu elektrycznym, nadmierną temperaturę powodującą uszkodzenia systemu. Pojęcie incydentu obejmuje następujące przykłady kategorii niekorzystnych zdarzeń: ataki kodów złośliwych (wirusy, konie trojańskie robaki, skrypty używane przez crakerów, hackerów), nieautoryzowanych dostęp do zasobów, nieautoryzowane wykorzystanie usług, odmowa – przerwa wykonania usługi, nadużycie, szpiegostwo, itd. Opisane powyżej zjawiska są najprostszą i najczęściej występującą formą zagrożeń. Występują jeszcze inne, bardziej złożone zagrożenia wywołujące olbrzymie negatywne skutki w pracy systemów teleinformatycznych. Generalnie można stwierdzić, że wszelkiego rodzaju zagrożenia powodują w systemach teleinformatycznych szereg negatywnych zjawisk mających wpływ na ich funkcjonowanie:

- utratę usług albo ograniczenie ich dostępności spowodowane pojedynczymi lub wieloma zagrożeniami;
- ujawnienie informacji lub korupcję spowodowane przez wyzyskiwanie, sabotaż, wojnę elektroniczną, itp.;
- utratę kontroli operacyjnej nad siecią spowodowane wyzyskiwaniem, sabotażem albo fizycznym uszkodzeniem;
- konieczność uruchamiania łączy redundantnych;

- stopniowe obniżanie jakości usług spowodowane coraz bardziej dotkliwym brakiem kadr odpowiedzialnych za obsługę i serwisowanie.

Sytuacje opisane powyżej mogą poważnie zakłócić działania państwa poprzez zakłócanie zarządzania kryzysowego chyba, że zostaną podjęte odpowiednie działania mogące zagwarantować ciągłe wykorzystanie najważniejszych usług telekomunikacyjnych. Organizacje terrorystyczne doskonale zdają sobie sprawę ze znaczenia informacji we współczesnym świecie i wiedzą, że atak paraliżujący infrastrukturę teleinformatyczną może przenieść większy efekt , niż zwykły atak zbrojny. Nie wszystkie organizacje mają jednak możliwość, środki finansowe i umiejętności w wykorzystaniu nowoczesnych technologii do własnych celów. Dlatego dochodzi często do łączenia starych i nowych metod działania.

Zgodnie z opisem w literaturze[48] opisującą problematykę terroryzmu organizacje terrorystyczne można podzielić na trzy grypy:

- kategoria I – nowe techniki są używane do prowadzenia tradycyjnej działalności; wykorzystywane są do zbierania informacji, komunikacji, zdobywania środków finansowych i komunikacji;
- kategoria II – stare techniki wykorzystywane do nowej działalności; użycie siły fizycznej w celu zniszczenia systemów teleinformatycznych;
- kategoria III – nowe techniki użyte do nowych działań; atak w cyberprzestrzeni na system informacyjny.[49]

Tak więc dla utrzymania możliwości ciągłości świadczenia podstawowych usług telekomunikacyjnych, musimy cały czas rozpoznawać wszelkiego rodzaju zagrożenia, studiować tę problematykę i spisywać wszystkie zdarzenia aby państwo mogło dokonać niezbędnych przygotowań, oraz podjąć niezbędne działania (w tym regulacje prawne uwzględniające finansowanie) w celu wyeliminowania wpływu wyżej wymienionych zagrożeń. W czasie pokoju operatorzy telekomunikacyjni powinni uwzględniać w codziennej działalności wiele zdarzeń, które mogą mieć wpływ na możliwości obsługi ruchu i świadczenia usług. Sposób działania operatorów w czasie pokoju niewątpliwie powinien być kontynuowany w sytuacjach kryzysowych i stanie wojny tak dalece jak tylko jest to możliwe. Jednakże operatorzy muszą

---

[48] *Agnieszka Bógdał-Brzezińska, Marcin Florian Gawrycki, Cyberterrorym i problemy bezpieczeństwa informacyjnego we współczesnym świecie, Warszawa 2003*
[49] *A. Rathmell, Cyber- terrorism.., op.cit.,ss.3-4*

zaplanować i przygotować już w czasie pokoju swoje działania na wypadek szczególnych zagrożeń, które mogą wystąpić stosownie do eskalacji sytuacji kryzysowej.

Po dokonaniu analizy ilości, wielkości i rodzaju czynników oraz zagrożeń dla poprawnego funkcjonowania sieci teleinformatycznej Sił zbrojnych Rzeczypospolitej Polskiej możliwe jest wykorzystanie uzyskanych rezultatów poznawczych do opracowania autorskiej koncepcji stacjonarnej sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej.

4.3 Współczesne zagrożenia militarne i niemilitarne

Współczesna rzeczywistość – kreowana procesami globalizacji – stawia przed siłami zbrojnymi, coraz większe wymagania kompetencyjne. Wzrastający stopień utechnicznienia i zorganizowania sił zbrojnych, ich nowe funkcje w państwie i środowisku międzynarodowym, a zarazem zmiana stosunków społecznych, zarówno w skali mikro, jak i makro, sprawiają, że siły zbrojne muszą sprostać wielu zagrożeniom o różnym charakterze.

W tym kontekście celem rozdziału jest zidentyfikowanie czynników wpływających na transformacje zagrożeń.

W przeprowadzonym procesie badawczym przyjęto założenie, że zmiana elementów w zbiorze warunkującym modyfikację zbioru zagrożeń spowodowana jest szeregiem zjawisk zachodzących w siłach zbrojnych postrzeganych zarówno w wymiarze zewnętrznym (otoczenie międzynarodowe) jak i wewnętrznym (reorganizacja wojsk i zasad ich wykorzystania). Ponadto dostrzegano w procesie badawczym fakt, że kierunki zmian w strukturze zagrożeń są pochodną zmian zachodzących w systemie polityczno-militarnym oraz stanowią wypadkową postępu technicznego. Uwzględniono także zasadność twierdzenia, że właściwa identyfikacja zagrożeń jest uwarunkowana przebiegiem przyszłej operacji w układzie wielonarodowym i koalicyjnym, w ramach działań zarówno militarnych jak i pokojowych.

Zagrożenie jest terminem najczęściej używanym w rozważaniach poświęconych problemom bezpieczeństwa. Istota pojęcia zagrożenie oznacza możliwe niebezpieczeństwo, przewidywanie, iż określone zjawiska będą przebiegały w sposób stanowiący pewien poziom ryzyka. Przy czym należy zaznaczyć, że

pojęcie „ryzyko" zawiera w sobie emocjonalny ładunek, skrytego domniemanego niebezpieczeństwa, a więc niepomyślnego rozwoju sytuacji w otoczeniu określonego obiektu. Ryzyko charakteryzuje się zróżnicowanym stopniem prawdopodobieństwa wystąpienia i w momencie pojawienia się określonych, sprzyjających ku temu warunków przeradza się w rzeczywiste zagrożenie. Aby jednak nie dopuścić do tego, podmiot powinien podjąć odpowiednie działania prewencyjne, które zredukują lub wyeliminują przyczyny zagrożenia.

Wyniki analizy literatury wskazują, że w rozumieniu terminu zagrożenie wskazuje się na możliwość niepowodzenia planowanych działań lub utraty posiadanych wartości materialnych czy intelektualnych. Zatem stan zagrożenia jest elementem inicjującym proces decyzyjny. Z jednej strony wypływa z konieczności wyboru określonej opcji postępowania, z drugiej zaś wymusza wybór ze zbioru możliwych rozwiązań.

Zgodnie z zasadą, obniżanie poziomu zagrożenia polega na wyodrębnieniu w nim wielu elementów składowych, określanych jako czynniki lub symptomy. Zgodnie ze stanem przygotowania podmiotu (państwa, organizacji, firmy) do sytuacji zagrożenia, można wyróżnić zagrożenie nie przewidywane (nieuświadomione) i przewidywane (uświadomione).

W skali międzynarodowej stan zagrożenia może odnosić się na przykład do utraty suwerenności kraju. Natomiast w odniesieniu do określonego państwa (systemu) zagrożenie może powodować ryzyko utraty życia obywateli, destabilizacje rozwoju politycznego, zaburzenia procesu zmian demokratycznych itp.

Pojęcie zagrożenia jest definiowane na różne sposoby:

- zagrożenie to stan psychiki lub świadomości wywołany postrzeganiem zjawisk, które oceniane są jako niekorzystne lub niebezpieczne;
- zagrożenie to czynniki powodujące stan niepewności i obaw: mogą to być rzeczywiste działania innych uczestników życia społecznego niekorzystne i niebezpieczne dla żywotnych interesów i podstawowych wartości danego podmiotu (jednostkowego lub zbiorowego[50]);
- zagrożenie to sytuacja, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia.

---

[50] R. Zięba, Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych. [w:] D.B Bobrow, E. Haliżak, R. Zięba, Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku, Warszawa 1997, s. 4.

Reasumując, zatem można wnioskować, że zagrożenie to z jednej strony pewien stan psychiczny lub świadomościowy wywołany postrzeganiem zjawisk, które subiektywnie ocenia się jako niekorzystne lub niebezpieczne, a z drugiej strony czynniki obiektywne powodujące stany niepewności i obaw[51].

Pojęcie zagrożenie, w swej istocie to stan, który odnosi się do sfery świadomości konkretnego podmiotu (elementu lub systemu). W aspekcie społecznym, podmiotem może być osoba, grupa społeczna lub całe społeczeństwo. Zagrożenie jest często w związku z tym definiowane w odniesieniu do aspektu społecznego, jako określony stan psychiki lub świadomości kształtujący się lub ukształtowany na podstawie postrzegania zjawisk otoczenia, które dla podmiotu są negatywne, niekorzystne, niebezpieczne itp. Tak ujmowane zagrożenie mieści się w sferze świadomości i ma charakter subiektywny albowiem najistotniejszymi są tu oceny formułowane przez konkretny podmiot a leżą one u podstaw przedsięwzięć podejmowanych w celu podniesienia stopnia jego bezpieczeństwa[52]. Z drugiej strony zagrożenie jest zjawiskiem wywołującym stan niepewności i obaw. Tak więc zagrożeniem może być sytuacja, w której narażone jest bezpieczeństwo osobowe, żywotny interes, podstawowe wartości lub postępowanie części uczestników życia społecznego.

Zagrożenia mogą powstawać zarówno niespodziewane, jako produkt uboczny działań podjętych w celu osiągnięcia konkretnych pozytywnych korzyści, jak i zamierzone, jako wytwór podmiotu dla wykorzystania ich jako instrumentu do umyślnego oddziaływania na inny podmiot, celem osiągnięcia konkretnych negatywnych dla niego zjawisk. Zagrożenia mogą mieć także charakter ciągły, będąc np. zjawiskami przyrodniczymi lub elementami programu pewnej grupy społecznej przekazywanego z pokolenia na pokolenie. W takiej sytuacji społeczeństwo często akceptuje zagrożenia jako zjawiska niepożądane, ale realnie istniejące, nie możliwe do wyeliminowania[53]. Zagrożenie jako zjawisko można w zależności od jego charakteru w sposób mniej lub bardziej precyzyjny opisać, używając zasadniczo takich parametrów jak czas, przestrzeń czy skala oddziaływania, a więc poziom szkód (zniszczeń).

---

[51] S. Korycki, System bezpieczeństwa Polski, Warszawa 1994, s. 54.

[52] Szerzej: R. Zięba, Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych [w:]: D.B Bobrow, E. Haliżak, R. Zięba, Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku, Warszawa 1997, s. 4.

[53] Na przykład świadome zamieszkiwanie na terenach aktywnych sejsmicznie lub w pobliżu wulkanów.

Zagrożeniem dla bezpieczeństwa podmiotu (państwa, narodu, organizacji, instytucji, związku) będzie utrudnienie lub utrata warunków do swobodnego bytu i rozwoju. Zagrożenia te mogą powstawać w dziedzinie politycznej (np. izolacja polityczna, szantaż polityczny), społecznej (np. ograniczenie lub zerwanie współpracy kulturalnej, naukowo-technicznej, turystycznej), gospodarczej (np.: ograniczenie lub zerwanie wymiany handlowej, pomocy finansowej lub jednocześnie w kilku dziedzinach - w dowolnej konfiguracji[54].

Przez **zagrożenie militarne** bezpieczeństwa państwa zwykle rozumie się taki splot zdarzeń polityczno-militarnych, w których może nastąpić utrudnienie lub utrata warunków do niezakłóconego bytu i rozwoju narodu (państwa) albo naruszenie bądź utrata jego suwerenności i integralności terytorialnej w wyniku oddziaływania militarnego (napaści zbrojnej)[55].

Zagrożenie niemilitarne jest splotem zdarzeń (występujących w stanie kryzysu), w wyniku, którego może nastąpić utrudnienie lub utrata warunków do niezakłóconego bytu i rozwoju państwa (narodu) lub naruszenie bądź utrata jego suwerenności i integralności terytorialnej, przy czym cel działania (wymuszenie uległości lub ustępstw) zamierza się osiągnąć przez wywieranie nacisku i stosowanie sankcji politycznych lub ekonomicznych, bez uciekania się do stosowania przemocy fizycznej (zbrojnej)[56].

Nie wszystkie zjawiska zagrażające bezpieczeństwu są zagrożeniem. Część z nich nie zawsze jest groźna i nie zawsze stanowi pełny wymiar terminu zagrożenie. Jeśli stan zagrożenia jest związany ze świadomością podmiotu będącego obiektem zagrożenia to można wnioskować, że tylko brak należytej wiedzy o istocie zjawiska zagrożenia prowadzi do określonego stanu psychicznego. Zatem poznanie i zrozumienie zjawiska zagrożenia powoduje ograniczenie poziomu niebezpieczeństwa. Wówczas zamiast terminu zagrożenie trafniej wydaje się określać zaistniały stan ryzykiem, które należy eliminować, lub wyzwaniem, które można lub trzeba podejmować[57].

Termin „ryzyko" jest definiowany najczęściej w teorii organizacji i zarządzania oraz naukach politycznych, gdzie rozpatrywane są problemy bezpieczeństwa.

---

[54] S. Dworecki, Od konfliktu do wojny. Warszawa 1996, s.21
[55] Tamże, s.23.
[56] Por. tame s.25.
[57] Wyzwanie jest to zjawisko, które wypływa z sytuacji, zmusza podmiot do podjęcia działania.

Pojęcie to jest określane jako sytuacja, gdy co najmniej jeden z elementów składających się na nią nie jest znany, ale znane jest prawdopodobieństwo jego wystąpienia (lub ich - jeżeli tych elementów jest więcej). Prawdopodobieństwo to może być albo wymierne, albo tylko odczuwane przez podejmującego działanie (decyzję). Warunki ryzyka występują tylko wtedy, kiedy istniejące doświadczenia z przeszłości dotyczące podobnych zdarzeń można porównać z obecną sytuacją. Problemy występujące w sytuacji ryzykownej można w przypadku wymierności jej elementów rozwiązać, wykorzystując np. rachunek prawdopodobieństwa lub metody statystyczne[58]. W kontekście przytoczonej definicji można wnioskować, że w odniesieniu do państwa lub społeczności, stan ryzykowny to sytuacja, w której dostępność poszczególnych możliwości i związane z każdą z nich potencjalne korzyści są znane z pewnym szacunkowym prawdopodobieństwem[59].

4.4 Wymagania bezpieczeństwa teleinformatycznego

Wojskowy system teleinformatyczny to zbiór złożonych oraz zespolonych ze sobą obiektów (urządzeń), które rozmieszczone są na określonym obszarze, a także narzędzi, metod postępowania i procedur stosowanych przez określone dowództwa celem zapewnienia wytwarzania, przetwarzania, przechowywania lub przekazywania informacji dla potrzeb dowodzenia wojskami i sterowania środkami rażenia. Natomiast wojskowa sieć teleinformatyczna to organizacyjne i techniczne połączenie systemów teleinformatycznych[60].

System taki czy też sieć, funkcjonuje w specyficznym otoczeniu, którego odzwierciedleniem zarówno w warunkach pokoju, kryzysu czy też konfliktu zbrojnego jest stała możliwość oddziaływania na niego przez potencjalnego przeciwnika.

Oddziaływanie takie ma wieloraki charakter i może być stosowane na wiele sposobów przy użyciu różnych sił i środków, których zasadniczym zadaniem jest uniemożliwienie realizacji podstawowego celu funkcjonującego systemu tj. **przekazywania informacji w systemie dowodzenia wojskami i sterowania systemami uzbrojenia**. Utrudnienie lub wręcz sparaliżowanie systemu dowodzenia wojskami można osiągnąć m.in. poprzez rażenie ogniowe we wszelkich dostępnych formach i metodach stanowisk dowodzenia (SD), ale także węzłów łączności

---

[58] *Encyklopedia organizacji i zarządzania*, Warszawa 1982, s. 456.
[59] R.W. Gryffin, *Podstawy zarządzania organizacjami*, Warszawa 1996, s. 271.
[60] Definicje J.Michniak

stanowisk dowodzenia (WŁ SD), pomocniczych węzłów łączności (PWŁ) czy węzłów sieciowych (WS) oraz innych wrażliwych elementów systemu teleinformatycznego, których zniszczenie bądź obezwładnienie elektroniczne będzie miało zasadniczy wpływ na sprostanie wymaganiom stawianym tym systemów.

Dla osiągnięcia celu bezpieczeństwa teleinformatycznego należy zaplanować i zrealizować szereg zadań, których wykonanie zagwarantuje spełnienie wymagań, jakie stawia się przed takimi systemami. Z celu jaki stawia się teleinformatyce wojskowej do osiągnięcia, wynikają jej zadania[61]:

- zapewnienie dowódcy i sztabowi możliwości skrytego, ciągłego i realnego czasowo dowodzenia wojskami oraz sterowania środkami rażenia;
- zapewnienie współdziałania pomiędzy związkami taktycznymi (oddziałami, pododdziałami) organicznymi, przydzielonymi i wspierającymi oraz z sąsiadami;
- zapewnienie przekazywania sygnałów dowodzenia, powiadamiania ostrzegania i alarmowania;
- zapewnienie wymiany wiadomości dla potrzeb kierowania organami regulacji ruchu, przekazywania i otrzymywania danych o sytuacji meteorologicznej, a także sygnałów wzajemnego rozpoznania i służby czasu.

Zadania powyższe realizowane są w następstwie wymagań stawianych przez dowodzenie, które winno być ciągłe, trwałe, operatywne i skryte. Poprzez analizę przedstawionych powyżej wymagań w stosunku do systemu dowodzenia można wykazać, że są one ściśle związane z wymaganiami stojącymi przed systemami teleinformatycznymi, do których zalicza się[62]:

- ***terminowość przekazywania informacji*** pod każdą postacią, która wpływa na ciągłość dowodzenia; w przypadku dowodzenia za pomocą technicznych środków dowodzenia, jest też miernikiem gotowości organów dowodzenia do realizowania procesów dowodzenia; zachowanie wymogu terminowości przekazu informacji wpływa na operatywność dowodzenia tzn. szybkie reagowanie na zmiany sytuacji na polu walki jest uzależnione od zdolności systemu teleinformatycznego do przekazywania rozkazów, zarządzeń, meldunków itp.;

---

[61] J. Michniak, A. Wisz, Bezpieczeństwo i ochrona informacji w wojskowych sieciach telekomunikacyjnych
i zautomatyzowanych systemach dowodzenia....op. cit., s. 9
[62] J. Michniak, Bezpieczeństwo i ochrona...., op. cit., s. 10

- ***wierność przekazu przez środki teleinformatyczne*** jest niezbędna do zapewnienia ciągłości i operatywności dowodzenia, oddziaływanie przeciwnika może powodować zmniejszenie wierności przekazu - tylko zdolność do odtworzenia u odbiorcy poprawnych treści przekazywanych wiadomości może zapewnić wykonanie zadania, a tym samym wpływa na efektywność dowodzenia;
- ***skrytość przekazu informacji i pracy środków teleinformatycznych*** – **to** utrzymanie w tajemnicy treści przekazywanych wiadomości oraz samego faktu i miejsca ich przekazywania, w dużym stopniu zapewnia osiąganie skrytości dowodzenia.

Syntetyzując wszystkie trzy wymienione cechy przekazu informacji przez systemy teleinformatyczne można przypisać im jedno wspólne pojęcie nazwane jakością przekazu informacji przez środki i systemy teleinformatyczne.

Rys.4.1 *Jakościowe cechy wojskowych systemów (sieci) teleinformatycznych*

Źródło: J. Michniak, A. Wisz, Bezpieczeństwo i ochrona informacji w wojskowych sieciach telekomunikacyjnych i zautomatyzowanych systemach dowodzenia, AON, Warszawa 2000

W takim ujęciu jakościowe cechy wojskowych systemów teleinformatycznych są wzajemnie od siebie uzależnione, przy czym relacje te zależne są od konkretnych sytuacji i warunków.

Biorąc pod uwagę najbardziej uznawane wymagania wobec teleinformatyki wojskowej oraz uwzględniając wpływ otoczenia, można określić wymagania jakie musi spełniać wojskowy system teleinformatyczny.

Zgodnie z danymi przedstawionymi na rysunku 4.2. wymagania stawiane wojskowemu systemowi teleinformatycznemu to:

- ***stała gotowość bojowa*** - rozumiana jako zdolność przystąpienia do zapewnienia dowodzenia wojskami i sterowania środkami rażenia w czasie określonym przez dowództwo, po zmianie struktury systemu spowodowanej przejściem w wyższy stan gotowości bojowej lub wymuszonej sytuacją operacyjno – taktyczną;
- ***trwałość*** - rozumiana jako zdolność do zapewnienia dowodzenia wojskami i sterowania środkami rażenia w warunkach intensywnego oddziaływania ogniowego i elektronicznego przeciwnika;

Rys.4.2 *Wymagania stawiane wojskowemu systemowi teleinformatycznemu*
Źródło: J. Michniak, A. Wisz, Bezpieczeństwo i ochrona informacji w wojskowych sieciach telekomunikacyjnych i zautomatyzowanych systemach dowodzenia, AON, Warszawa 2000

- ***mobilność*** - rozumiana jako zdolność systemu do zmiany struktury oraz do rozwijania i przenoszenia elementów systemu, gwarantującą osiągnięcie gotowości całego systemu w nowych warunkach i w założonym czasie;
- ***przepustowość*** - rozumiana jako zdolność do transmisji określonych strumieni wiadomości w wyznaczonym czasie;
- ***bezpieczeństwo*** - rozumiana jako zdolność do poprawnego funkcjonowania w warunkach prowadzenia przez przeciwnika różnorodnych form walki elektronicznej.

Analizując wymienione wymagania stawiane wojskowemu systemowi teleinformatycznemu, można pozwolić sobie na stwierdzenie, że sumarycznie

stanowią one jedną integralną całość w tym sensie, że występuje pomiędzy nimi określona korelacja. Przykładem potwierdzającym tę tezę może być choćby zależność między przepustowością a bezpieczeństwem. Jest bowiem ogólnie znanym faktem, że zastosowanie urządzeń ochrony kryptograficznej (bezpieczeństwo) ma bezpośrednie przełożenie na prędkość transmisji (przepustowość). Zatem jednoczesna realizacja wszystkich cytowanych wymagań pozwala na spełnienie wymagań stawianych przez system dowodzenia.

Dotychczasowe usystematyzowanie wiedzy w zakresie określenia wymagań stawianych zarówno wojskowej sieci telekomunikacyjnej (a de facto teletransmisyjnej), jak i wojskowemu systemowi teleinformatycznemu pozwala na zidentyfikowanie miejsca i roli bezpieczeństwa w procesie dowodzenia realizowanego poprzez techniczne środki dowodzenia (systemy i sieci teleinformatyczne).

Wiedza ta jednocześnie stanowi podstawę dalszych rozważań, których oczekiwanym rezultatem będzie identyfikacja wymagań bezpieczeństwa informacji w systemie czy sieci teleinformatycznej w toku działań z użyciem wojsk.

4.5 Środowisko pracy sieci teleinformatycznej

Ostatnie dziesięciolecie dla resortu obrony narodowej to okres wielu przeobrażeń i zmian, które w jednakowym stopniu dotyczą aspektów doktrynalnych i organizacyjnych oraz technicznych. Potrzeba współdziałania w środowisku sojuszniczym i koalicyjnym jest doskonałym katalizatorem zmian w zakresie wyposażenia naszych wojsk w nowoczesne urządzenia i systemy o zaawansowanym poziomie technologicznym. Również potrzeba osiągania zdolności wojsk do działań sieciocentrycznych, w których zasadniczym celem jest osiągniecie przewagi informacyjnej, bezpośrednio wpływa na sposób postrzegania nowoczesnych technologii, jako narzędzia do realizacji zamierzonych celów. Nie sposób nie zauważyć dziś prostego związku pomiędzy efektywnością i skutecznością działania wojsk, a poziomem ich technologicznego zaawansowania.

Znaczącą rolę w postępującym procesie modernizacji sił zbrojnych spełnia informatyka, która dostarcza coraz to nowszych i bardziej zaawansowanych narzędzi, zarówno dowódcom, jak i kadrze zarządzającej resortem obrony narodowej, która zapewnia dostęp do informacji w każdych warunkach i na znaczne

odległości. Wykorzystując najnowsze technologie, staje się nieodłącznym elementem wszelkich działań.

Środowisko i warunki funkcjonowania wojskowych systemów teleinformatycznych wymagają zdefiniowania grupy podstawowych pojęć, umożliwiających przeprowadzenie analizy systemu teleinformatycznego w aspekcie jego bezpieczeństwa. Przed przystąpieniem do rozważań w zakresie określenia wymagań stawianych bezpiecznej sieci teleinformatycznej w działaniach z użyciem wojsk należy zauważyć, że pojęcia występujące w temacie, tzn. bezpieczeństwo, informacja oraz sieć teleinformatyczna są różnorako interpretowane. Dlatego też celowym jest przedstawienie na bazie dostępnych źródeł różnych definicji wymienionych pojęć, by wyodrębnić z nich te, które posłużą zdefiniowaniu podstawowego celu, którym jest określenie wymagań bezpieczeństwa informacji w sieci teleinformatycznej.

W literaturze poświęconej zagadnieniom ochrony systemów informatycznych czy zapewnieniu bezpieczeństwa informacji w nich przetwarzanych, przechowywanych i przesyłanych nie wydzielane jest z pojęcia wojskowego systemu teleinformatycznego pojęcie sieci telekomunikacyjnej. Fakt ten jest bardzo łatwy do wytłumaczenia, gdyż sieć telekomunikacyjna jest integralną częścią, elementem sieci teleinformatycznej spinającą lokalne sieci informatyczne w jedną rozległą całość, a z dotychczas zebranej i usystematyzowanej wiedzy wynika, że proces zapewnienia bezpieczeństwa systemowi musi być realizowany w sposób kompleksowy i obejmować wszystkie jego elementy funkcjonalne i organizacyjne. Podobnie rzecz ma się w odniesieniu do samego bezpieczeństwa systemu czy sieci, bowiem nie mają zasadniczego znaczenia miejsce i struktura organizacyjna systemu, w której powstał stan niepożądany polegający na ujawnieniu lub niekontrolowanym wypływie chronionej informacji. Zdarzenie to świadczy jedynie o tym, że zastosowane środki i metody ochrony nie spełniły stawianych przed nimi wymagań i nie uwzględniały wszystkich czynników wpływających na zapewnienie wymaganego poziomu bezpieczeństwa.

Uogólniając tok powyższego rozumowania w trakcie dalszych rozważań będących tematem dywagacji wymagania stawiane bezpieczeństwu wojskowego systemu teleinformatycznego będą traktowane jako równoznaczne tym wymaganiom, które stawiane są wojskowej sieci teleinformatycznej.

Pierwszym z wymienionych pojęć jest „bezpieczeństwo" (*ang. Security*[63]). Jest ono bardzo szerokim pojęciem, zawierającym w sobie wszystkie aspekty i pojęcia wchodzące w zakres ochrony informacji, do których zalicza się między innymi podatność, zagrożenia, ryzyko, aspekty zarządzania i zabezpieczenia. W Słowniku Języka Polskiego[64] jest definiowane jako „***stan nie zagrożenia, spokoju, pewności***". W ujęciu technicznym pojecie bezpieczeństwa określane jest jako stopień[65] pewności (wytrzymałości) konstrukcji na działania obciążające (niszczące) daną konstrukcję. Z jednej strony definicje te są bardzo proste i zwięzłe, ale jednocześnie ich zakres znaczeniowy jest bardzo szeroki. O wiele bardziej interesującą pod kątem naszych rozważań będzie definicja zawarta w treści zaczerpniętej z Myśli Wojskowej[66] mówiąca, że bezpieczeństwo to jedna z podstawowych potrzeb człowieka i określa to jako „*stan, który daje poczucie pewności i gwarancję jego zachowania oraz szansę na doskonalenie. Sytuacja odznaczająca się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni, na przykład zdrowia, pracy, szacunku, uczuć, dóbr materialnych*".

W odniesieniu do systemu telekomunikacyjnego bezpieczeństwo[67] pojmowane jest jako „*stan osiągany, gdy określone informacje, materiały, personel czynności i obiekty zostają zabezpieczone przed szpiegostwem, sabotażem, dywersją i terroryzmem, a także przed utratą lub nieautoryzowanym dostępem*".

Inaczej problem postrzegany jest i definiowany w odniesieniu do bezpieczeństwa łączności[68], gdzie traktowany jest on jako „*zdolność systemu do ochrony przesyłanych informacji oraz stacji (aparatowni), urządzeń i dokumentów kluczowych przed rozpoznaniem*". Definicja powyższa w cytowanej już wcześniej „Normie Obronnej NO-01-A003 poszerzona jest o środki bezpieczeństwa mające na celu zapobieżenie nieautoryzowanemu dostępowi lub w celu zapewnienia ich autentyczności.

W dokumentach normatywnych[69] Paktu Północnoatlantyckiego pojęcie bezpieczeństwa łączności (ang. Communication Security – COMSEC[70]) traktowane

---

[63] Dokument NATO serii AMSG 524 – „Słownik pojęć i definicji z zakresu bezpieczeństwa łączności i informatyki"
[64] „Słownik Języka Polskiego"- PWN, Warszawa 1978
[65] „Encyklopedia popularna PWN", Warszawa 1982
[66] „Myśl Wojskowa"- Bellona, Warszawa Listopad-Grudzień 2002, 6 (623)
[67] Systemy telekomunikacyjne i informatyczne – terminologia, Norma Obronna, NO-01-A003
[68] Tymczasowe zasady organizacji, funkcjonowania i bezpieczeństwa łączności utajnionej w SZ RP – Szefostwo Wojsk Łączności sygn. Łączn. 988/88 s. 49
[69] Dyrektywa Bezpieczeństwa AD 70-1 PL, część V, § 13
[70] Dokument NATO serii AMSG 524 – „Słownik pojęć i definicji z zakresu bezpieczeństwa łączności i informatyki"

jest jako *„zespół zabezpieczeń wynikających z używania środków ochrony kryptograficznej, środków zabezpieczenia transmisji i emisji na okres połączenia (sesji), a także z zastosowań fizycznych środków zabezpieczenia informacji. Podejmuje się je w celu ochrony przed dostępem osób nieautoryzowanych do informacji lub w celu zapewnienia autentyczności takiego połączenia".*

Podstawowym wymaganiem dla zapewnienia bezpieczeństwa teleinformatycznego jest bezpieczeństwo informacji.

Do zasadniczych i zarazem wymaganych atrybutów bezpiecznego[71] przesyłania informacji przesyłanych w wojskowych sieciach teleinformatycznych należą:

- **POUFNOŚĆ** - oznacza ochronę przed ujawnieniem informacji nieuprawnionemu odbiorcy;
- **INTEGRALNOŚĆ** - oznacza ochronę przed modyfikacją lub zniekształceniem aktywów przez osobę nieuprawnioną;
- **DOSTĘPNOŚĆ** - oznacza gwarancję uprawnionego dostępu do aktywów przy zachowaniu określonych rygorów czasowych;
- **ROZLICZALNOŚĆ** - oznacza określenie i weryfikowanie odpowiedzialności za działania, usługi i funkcje realizowane za pośrednictwem systemu;
- **AUTENTYCZNOŚĆ** - oznacza weryfikację tożsamości podmiotów lub prawdziwość aktywów systemu teleinformatycznego;
- **NIEZAWODNOŚĆ** - oznacza gwarancję odpowiedniego zachowania się systemu teleinformatycznego i otrzymanych wyników.

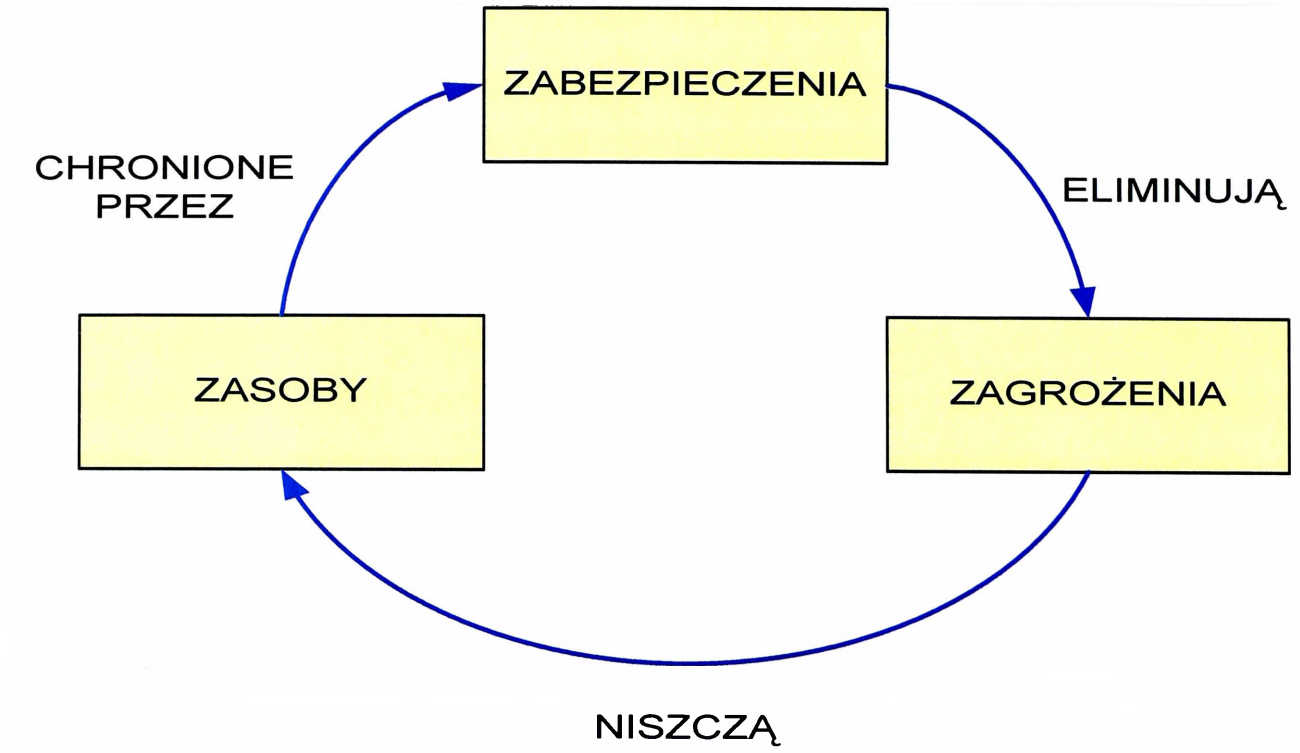
Jak każda sieć teleinformatyczna również i wojskowa posiada powiązane zależnościami elementy składowe wpływające na organizację i docelowy kształt sieci. Do podstawowych elementów składających się na całość systemu teleinformatycznego zaliczyć można:

- **AKTYWA** *(systemu teleinformatycznego)* - wszelkie oprogramowanie, dane, sprzęt, zasoby administracyjne, fizyczne, komunikacyjne lub ludzkie niezbędne do funkcjonowania systemu teleinformatycznego;
- **ZAGROŻENIA** - przyczyny niepożądanych zdarzeń, których efektami są szkody w systemie teleinformatycznym;

---

[71] *PN –I -13335-1 Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcie i modele bezpieczeństwa systemów informatycznych.*

- **MECHANIZMY ZABEZPIECZEŃ** - do zadań mechanizmów zabezpieczeń należy: ochrona przed zagrożeniami, eliminowanie słabości, ograniczanie wpływu niepożądanych zdarzeń, wykrywanie niepożądanych zdarzeń i realizowanie wyjścia z sytuacji kryzysowych;
- **SŁABOŚCI** - podatność systemu teleinformatycznego na zagrożenia jest wyrażona łatwością, z jaką dane zagrożenie może wyrządzić szkodę.



Rys. 4.3 *Zależności między elementami systemu teleinformatycznego*
Źródło: Opracowanie własne

Poza powyższymi elementami w środowisku funkcjonowania systemów teleinformatycznych do zdefiniowania pozostają:

- **ZDARZENIE** - możliwa, aczkolwiek niepożądana konsekwencja posiadania i użytkowania systemu teleinformatycznego, spowodowana wystąpieniem zagrożenia. Konsekwencją może być zniszczenie systemu teleinformatycznego poprzez uszkodzenie systemu zabezpieczenia, utratę poufności, integralności lub dostępności albo inne pośrednie szkody;
- **RYZYKO** - określa prawdopodobieństwo sytuacji, w której dane zagrożenie wykorzystuje określone słabości, powodując utratę zasobów lub uszkodzenie systemu teleinformatycznego, a zatem, pośrednią lub bezpośrednią szkodę dla jednostki organizacyjnej. Ryzyko charakteryzują dwa czynniki: prawdopodobieństwo jego wystąpienia oraz miara zdarzenia.

Wszelkie zmiany w układzie wzajemnych zależności między zagrożeniami, słabościami i wprowadzanymi mechanizmami zabezpieczeń mogą mieć duże znaczenie dla ryzyka. Określenie poziomu ryzyka dla każdej kategorii dostrzeżonych zagrożeń, słabości oraz wpływów na system teleinformatyczny jest **analizą ryzyka**.

Analiza ryzyka - systematyczna metoda identyfikowania aktywów systemu przetwarzania danych, zagrożeń tych aktywów i podatności systemu na te zagrożenia (risk analysis)[72].

Podstawowymi celami prowadzenia analizy ryzyka są:

- wypunktowanie istniejących zagrożeń;
- pokazanie bieżącego stanu bezpieczeństwa;
- podniesienie wzrost świadomości na wszystkich poziomach organizacji;
- pomoc w zebraniu podstawowych faktów niezbędnych do wyboru efektywnych środków zaradczych.

Analiza ryzyka nie jest zadaniem, które może być wykonane jednorazowo, powinna być wykonywana periodycznie, w celu utrzymania bieżącego stanu zgodnego ze zmianami zagrożeń, nowymi zadaniami stojącymi przed jednostką organizacyjną, nowymi udogodnieniami i wyposażeniem.

Należy mieć świadomość, że ryzyko można oszacować i zredukować, ale nie da się go wyeliminować całkowicie. Mechanizmy zabezpieczeń mogą jedynie zmniejszać ryzyko. Całkowita eliminacja jest zwykle niemożliwa lub zbyt kosztowna. Powoduje to konieczność oszacowania ryzyka szczątkowego i określenia poziomu jego akceptacji na podstawie przyjętej stopniowalności ryzyka. Stopień ryzyka jest funkcją wielu zmiennych, ale przede wszystkim zależy od stanu wiedzy o systemie i procesach w nim zachodzących. W zależności od ilości i jakości informacji możemy mówić o ryzyku:

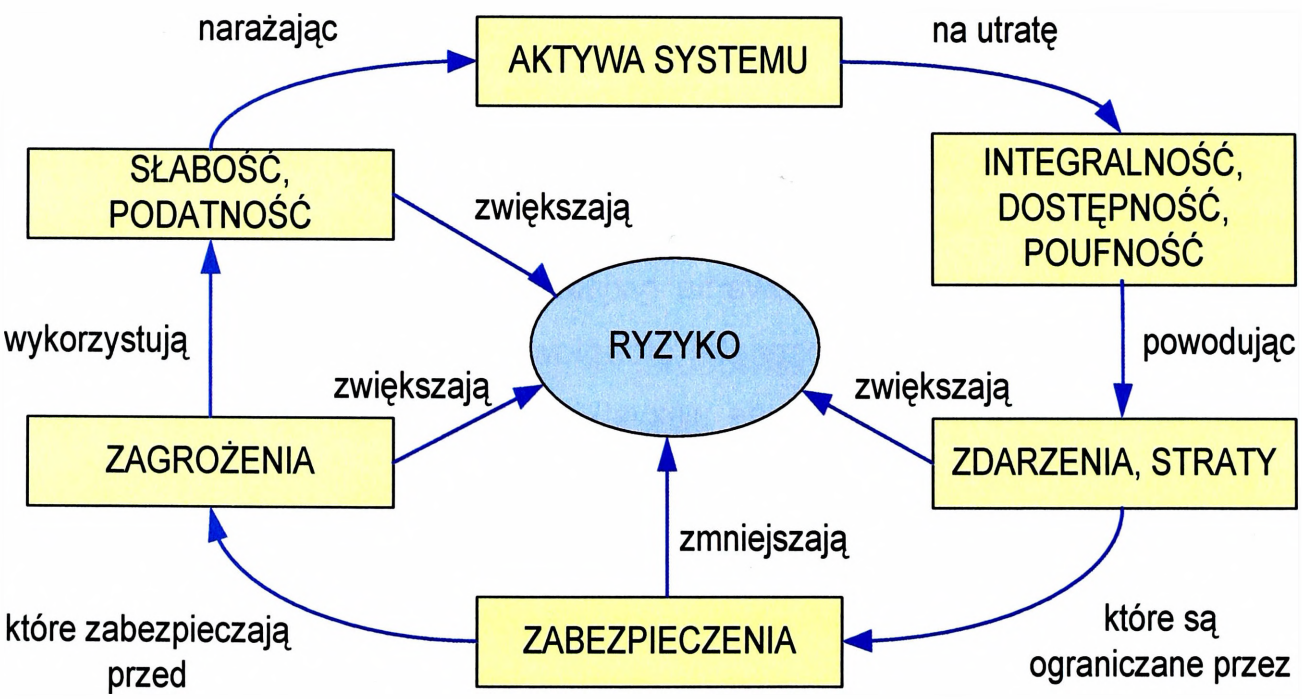
- NORMALNYM - takie, które musimy podjąć, bo jest ono naturalne;
- NIEZBĘDNYM - takie, które musimy podjąć, bo jest to minimum;
- DOPUSZCZALNYM - takie, na które możemy sobie pozwolić
- (RYZYKO SZCZĄTKOWE);
- NIEDOPUSZCZALNYM - takie, które przekracza poziom dopuszczalny.

---

[72] *Polska norma PN-I-02000 Technika informatyczna.*

Ze względu na dużą objętość problematyki poświęconej analizie ryzyka i zarządzaniu ryzykiem nie będę przedstawiał szerzej zagadnień (np. zautomatyzowane systemy ryzyka, metody zarządzania ryzykiem) związanych z tą dziedziną bezpieczeństwa sieci teleinformatycznych, podam jednak nasuwające się wnioski końcowe:

- zabezpieczenie systemów teleinformatycznych będzie się ciągle zmieniać jako, że zmieniają się również systemy teleinformatyczne;
- ochrona systemów teleinformatycznych jest ciągłym wyborem między tym co dozwolone i niedozwolone, jest ustawicznym przesuwaniem granicy między tymi dwoma obszarami;
- system zabezpieczeń powinien być kreowany w ten sposób by korzyści bezprawnej ingerencji w systemy teleinformatyczne były niższe niż koszty które intruz musi ponieść na zniszczenie zabezpieczeń;
- zabezpieczenie systemów teleinformatycznych jest problemem technicznym i organizacyjnym.



Rys. 4.4 *Zależności w środowisku funkcjonowania sieci teleinformatycznej*
Źródło: Opracowanie własne

Wraz z rozwojem ilościowym i technologicznym systemów teleinformatycznych przeznaczonych do przechowywania przetwarzania oraz przesyłania informacji istotnych dla codziennego funkcjonowania jednostek wojskowych i instytucji

cywilnych, wzrasta zainteresowanie tymi systemami ze strony potencjalnych przeciwników jak również zwykłych intruzów.

Można więc stwierdzić, że w znaczny sposób wzrasta ryzyko poprawnego funkcjonowania sieci teleinformatycznej Sił Zbrojnych, czyli pojawiają się różnego rodzaju zagrożenia. Badania literatury przedmiotu pozwalają na przytoczenie różnych definicji zagrożeń oraz ich kwalifikacji.

Zagrożenie - zjawisko wywołane działaniem sił natury bądź człowieka, które powodują, że poczucie bezpieczeństwa maleje bądź zupełnie zanika. Zagrożenia dzielimy na naturalne (np. klęski żywiołowe) i związane z działalnością człowieka (te dzielimy na: zagrożenia cywilizacyjne, np. imprezy masowe, choroby; zagrożenia destrukcyjne, np. terroryzm, przestępczość, sabotaż; zagrożenia gospodarcze, np. zanieczyszczenie środowiska, wadliwe konstrukcje). Zagrożenie możemy jeszcze podzielić ze względu na rozmiary (terytorium) na którym ono zachodzi tzn. zagrożenia globalne, regionalne jak i lokalne.[73]

Zagrożenia ekologiczne: eksperci wyróżniają cztery główne rodzaje zagrożenia ekologicznego o globalnym charakterze:

- rozprzestrzenianie się substancji toksycznych nie dających się biologicznie
- rozłożyć – chemicznych lub radioaktywnych;
- niszczenie lasów i zakwaszanie akwenów wodnych przez trucizny przemysłowe;
- zanieczyszczenie górnych warstw atmosfery przez chlorofluorowęglowodory, które powodują uszkadzanie warstwy ozonu (dziura ozonowa) i na skutek tego wzrost przenikania szkodliwych promieni ultrafioletowych;
- cieplarniany efekt, efekt szklarniowy, zjawisko wzrostu temperatury atmosfery spowodowane istnieniem w jej składzie tzw. gazów cieplarnianych (szklarniowych), które przepuszczają znaczną część promieniowania słonecznego (promieniowanie krótkofalowe) do powierzchni Ziemi, zmniejszając wypromieniowanie ciepła (promieniowanie długofalowe) przez powierzchnię Ziemi i dolne warstwy atmosfery.

Zagrożenie cywilizacyjne: podstawowe problemy trapiące współczesny świat, o zasięgu tak wielkim, że mogą spowodować załamanie globalnego ładu gospodarczego i politycznego oraz zagrozić egzystencji ludzi; np. nieprzestrzeganie

---

[73] *Źródło internetowe*

praw człowieka, terroryzm, walki etniczne, zachwianie równowagi ekologiczne, zagrożenie epidemiami, przeludnienie, nędza.

Zagrożenia, to zmiany występujące w otoczeniu, które mogą podważyć pozycję przedsiębiorstwa. Zagrożenie to zdarzenie lub trend w otoczeniu, możliwe lecz trudne do przewidzenia, powodowane głównie działaniami lub reakcjami nabywców, dostawców, kontrahentów, a zwłaszcza konkurentów, które - jeśli nie zostaną szybko dostrzeżone i nie wywołają odpowiedniego przeciwdziałania - mogą spowodować straty, a nawet zachwianie sytuacji przedsiębiorstwa. Zagrożenia powstają bądź z przyczyn zewnętrznych, bądź wewnętrznych przedsiębiorstwa niezdolnego do sprostania konkurencji, dokonania koniecznej zmiany segmentów i dostosowania do nich produkcji, marketingu i sprzedaży, a także na skutek pojawienia się nowych krajowych lub zagranicznych konkurentów, potrafiących lepiej i taniej pozyskiwać nabywców i zaspokajać ich potrzeby.

Zagrożenie bezpieczeństwa, atak na bezpieczeństwo, atak na system komputerowy, (angielskie *security attack, security threat*), działanie mające na celu przeniknięcie do chronionego systemu komputerowego w celu przechwycenia lub zniekształcenia przechowywanych w nim informacji. Rozróżnia się następujące rodzaje ataków na bezpieczeństwo:

- przerwanie (*interruption*), czyli zniszczenie części systemu lub jej unieruchomienie, np. przecięcie linii łączności;
- przechwycenie (*interception*), czyli uzyskanie dostępu do zasobów systemu przez czynnik postronny (osobę, komputer), np. podsłuch;
- modyfikacja (*modification*), tj. zmiana zasobów przez osobę nieupoważnioną, np. modyfikacja programu lub komunikatów sieciowych;
- podrobienie (*fabrication*), czyli atak na autentyczność, np. dodanie fałszywych danych do pliku.

Naruszenia bezpieczeństwa (nadużycia) systemu można podzielić na przypadkowel rozmyślne (złośliwe). Łatwiej jest chronić system przed nadużyciami przypadkowymi niż przed złośliwymi.[74]

Zagrożenia (threats) : wszystkie czynniki zewnętrzne, które są postrzegane przezfirmę jako bariery, utrudnienia, niebezpieczeństwa, dodatkowe koszty, wysiłki, wyrzeczenia itp. Ph. Kotler zagrożenia płynące ze strony otoczenia definiuje jako

---

[74] *Zdzisław Płoski, "Słownika Encyklopedycznego - Informatyka" Wydawnictwa Europa. ISBN 83-87977-16-0. Rok wydania 1999.*

"wyzwania powstałe w związku z niekorzystnym trendem lub rozwojem wypadków w otoczeniu, które doprowadziłyby w przypadku braku odpowiedniej akcji marketingowej do spadku wielkości sprzedaży i zysku"[75]. Istnienie zagrożeń zmniejsza potencjał rozwojowy firmy, ogranicza jej ekspansję rynkową i pomniejsza możliwości wykorzystania jej silnych stron w procesie obsługi rynku.

W pracy Krystiana Baniaka[76] zgodnie z definicją zagrożenie jest wydarzeniem, którego wystąpienie ma niepożądany wpływ na poprawny stan obiektu. Przykładem zagrożenia będzie np. huragan lub kradzież. W procesie wymiany informacji pożądanym rezultatem jest bezpieczeństwo przesyłanych danych, gwarancja dostarczenia w niezmodyfikowanej formie i w odpowiednim czasie. Zagrożenia dla tych celów będą związane z zamierzonymi lub przypadkowymi incydentami zmodyfikowania, podsłuchania lub uniemożliwienia transmisji.

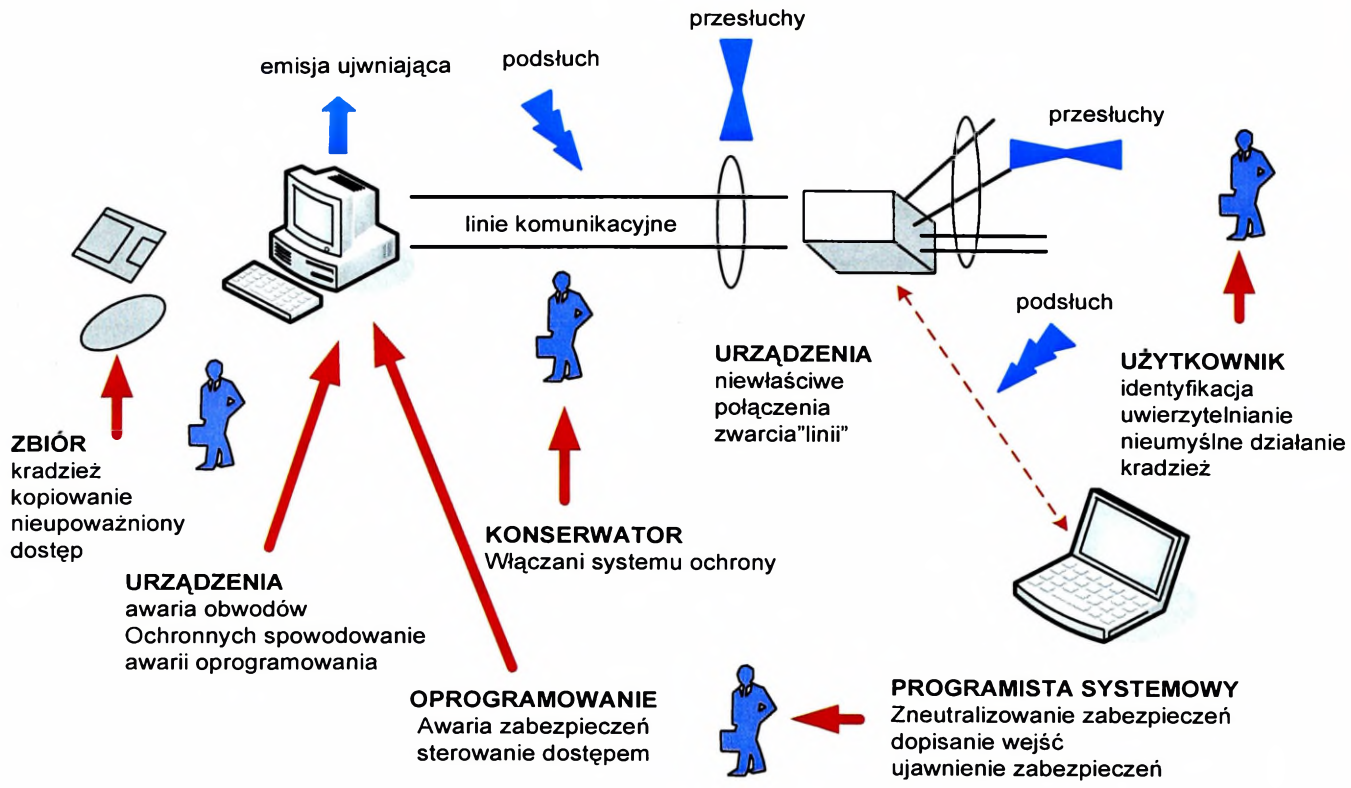
Incydenty niezamierzone są reprezentowane przez katastrofy naturalne, anomalie pogodowe, działania wojenne, awarie systemów zasilanie lub awarie sprzętowe.

Incydenty zamierzone są ukierunkowanymi działaniami osób lub wrogich organizacji mającymi na celu nielegalne wykorzystanie zasobów, usług lub przechwycenie/zmodyfikowanie informacji.

---

[75] *Ph. Kotler, źródło internetowe*

[76] *Krystian Baniak, „Bezpieczeństwo w telekomunikacji i teleinformatyce", Biblioteka „Bezpieczeństwa Narodowego" Warszawa 2007*



Rys. 4.5 *Najbardziej powszechne zagrożenia dla sieci teleinformatycznych*
Źródło: Opracowanie własne

Do dalszych rozważań nad poprawnym funkcjonowaniem sieci teleinformatycznej autor przyjął, że:

Zagrożenia to zbiór wszystkich czynników wewnętrznych należących do środowiska działania systemu i zewnętrznych nienależących do środowiska systemu wywołanych działaniem człowieka bądź sił natury, które powodują, że poczucie bezpieczeństwa maleje bądź zupełnie zanika.

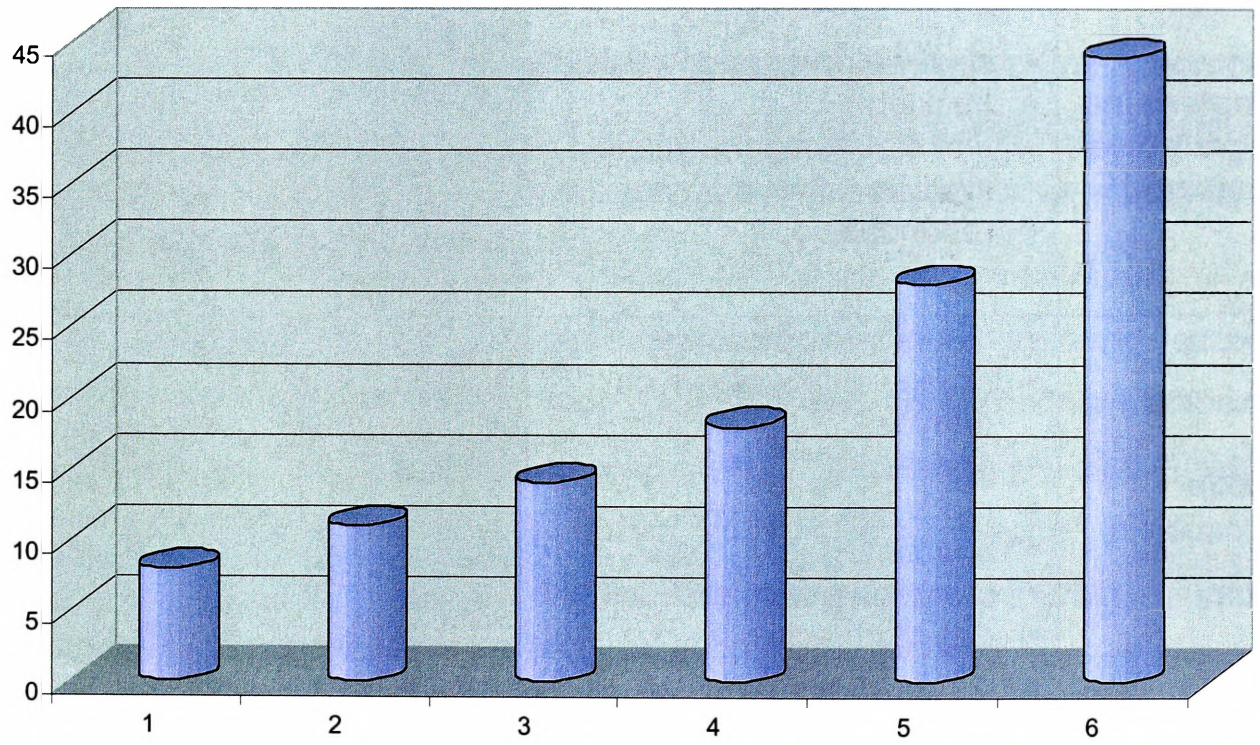
4.6 Synteza wniosków z badań

Próba odpowiedzi na pytanie zawarte w początkowej części rozdziału, jakie zagrożenia i czynniki wpływają na funkcjonowanie stacjonarnej sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej, jest bardzo skomplikowana, gdyż podziału czynników powodujących zagrożenia dla bezpieczeństwa sieci teleinformatycznych jak już wcześniej wspomniano można dokonywać w wielu aspektach i płaszczyznach. Jednak w trakcie dalszych rozważań opierając się na obowiązujących dokumentach normatywnych oraz na podstawie praktyki i doświadczeń przedstawiam próbę przyporządkowania najczęściej identyfikowanych i występujących czynników mających wpływ na zagrożenia

poprawnego funkcjonowania sieci teleinformatycznych Sił Zbrojnych Rzeczypospolitej Polskiej .

W świetle powyższych analiz oraz wyników przeprowadzonych badań, wykorzystując do tego celu takie metody empiryczne, jak sondaż diagnostyczny technika obserwacji w grupie kadry zawodowej i pracowników wojska Departamentu Informatyki i Telekomunikacji, Centrum Zarządzania Systemami Teleinformatycznymi oraz Centralnego Węzła Łączności (rys. 4.6.) można uznać, że poprawne funkcjonowanie sieci teleinformatycznej Sił Zbrojnych będą uzależnione od następujących czynników :

- materialne (fizyczne)
- niematerialne (programowe/ techniczne)
- ludzkie



Legenda:

1. Lokalizacja kluczowych elementów infrastruktury.
2. Wpływ środowiska naturalnego.
3. Niezawodność technologii oraz oprogramowania.
4. Czynnik ludzki (działania zamierzone i niezamierzone).
5. Czynniki niematerialne (programowe/techniczne).
6. Czynniki materialne (fizyczne).

Rys. 4.6 *Ilościowy układ odpowiedzi na pytania, które czynniki w zasadniczy sposób wpływają na bezpieczne funkcjonowanie sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej*

Źródło: opracowanie własne na podstawie zebranych wyników

Zidentyfikowany zbiór czynników wpływających na bezpieczne funkcjonowanie sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej przedstawiono w tabeli 4.1.

Tabela 4.1

Zbiór czynników

Czynniki powodujące zagrożenia	Rodzaje zagrożeń powodowanych przez czynniki	Mechanizmy zabezpieczeń
Materialne (Fizyczne)	▪ fizyczne ▪ ekologiczne ▪ cywilizacyjne ▪ terrorystyczne	▪ wybór „bezpiecznych" miejsc dla wrażliwych elementów infrastruktury systemu ▪ zapewnienie odtwarzania systemu; ▪ rezerwacja systemów utrzymania
Niematerialne (Programowe/ techniczne)	▪ złośliwe oprogramowanie ▪ hacking ▪ ulot elektromagnetyczny ▪ złośliwe kody ▪ redundancje	▪ stosowanie zabezpieczeń sprzętowych i programowych; ▪ monitoring sieci (analiza ruchu) ▪ separacja linii transmisyjnych; ▪ backup
Ludzkie	▪ nieuprawniony dostęp ▪ skasowanie wrażliwych danych ▪ podsłuch ▪ modyfikacja danych ▪ kradzież ▪ pomyłki i pominięcia ▪ dezinformacja	▪ dobór kadr ▪ stosowanie zabezpieczeń fizycznych ▪ przypisanie poziomów dostępu

Wymienione czynniki są ściśle związane z technologią oraz fizycznym lub cyberprzestrzennym naruszeniem strefy bezpieczeństwa. Ponieważ system teleinformatyczny Sił Zbrojnych RP jest wykorzystywany przez użytkowników przede wszystkim wojskowych zarówno w czasie pokoju, kryzysu oraz wojny, można oczekiwać dużego zainteresowania tymi obiektami ze strony potencjalnych przeciwników. Stąd też należy zakładać, że systemy teleinformatyczne mogą być jednym z głównych celów potencjalnego ataku. Poprawne funkcjonowanie systemu teleinformatycznego może zostać zakłócone przez czynniki innego rodzaju, które zostały opisane powyżej, a są to czynniki typowo militarne. Te czynniki można scharakteryzować jako:

- **Oddziaływanie walki elektronicznej**, która może mieć wpływ na wszystkie sieci i systemy telekomunikacyjne. Obejmuje proste zakłócanie pracy bardziej skomplikowanych urządzeń powodowane przez silne promieniowanie z urządzeń zakłócających. Takie promieniowanie może doprowadzić do uszkodzenia elementów sieci. Łącza radiowe (np. wysokich częstotliwości oraz komercyjne łącza satelitarne) oraz w szczególności łącza o stałych częstotliwościach są bardzo podatne na zakłócenia. Dodatkowym zagrożeniem mogą być ataki na elementy systemów satelitarnych znajdujące się na ziemi i w przestrzeni kosmicznej.
- **Broni konwencjonalnej**, która może być bardzo skuteczna przeciwko wszelkim rodzajom instalacji telekomunikacyjnych. Uszkodzenia systemów telekomunikacyjnych są powodowane bezpośrednimi atakami oraz efektami ubocznymi innych wybuchów (pożary, odłamki, itp.)
- **Broni chemicznej i biologicznej**, powodującej szczególne zagrożenie, ponieważ jest przeznaczona do niszczenia wybranych materiałów, terenów lub zabijania grup ludzi. Pomimo międzynarodowych ograniczeń dotyczących tego typu broni, istnieją jej różne odmiany.
- **Broni jądrowej**, która może mieć wieloraki wpływ na systemy łączności. Wybuchy na niskiej wysokości mogą spowodować bezpośrednie uszkodzenia instalacji przez siłę eksplozji, wysoką temperaturę oraz bliskość promieniowania. Wybuchy na dużych wysokościach mogą zakłócać lub uszkodzić instalacje telekomunikacyjne przez efekt impulsu elektromagnetycznego (Elektro Magnetic Pulse - EMP). Inne konsekwencje ataków jądrowych obejmują absorpcję transmisji satelitarnej oraz długodystansowych dróg propagacji, generowanie EMP skierowane przeciwko satelitom oraz efekty magnetyczno-hydrodynamiczne (MHD) skierowane przeciwko liniom długodystansowym oraz kablom podmorskim. Należy jednak pamiętać, że tego typu dużej skali ataki jądrowe są mało prawdopodobne w obecnej sytuacji politycznej.

Przedstawione czynniki są podstawą do opracowania strategii bezpieczeństwa systemów teleinformatycznych. Jednak podstawowym elementem w procesie zarządzania bezpieczeństwem jest zadanie sobie pytania, jaki poziom

bezpieczeństwa jest akceptowalny przez jednostki wojskowe i instytucje cywilne pracujących na rzecz obronności kraju. Właściwy poziom akceptowalnego ryzyka, a więc odpowiedni poziom bezpieczeństwa jest wykładnią do skutecznego zarządzania bezpieczeństwem.

Zabezpieczenie zasobów informacyjnych oraz systemów teleinformatycznych wymaga nie tylko implementacji i zarządzania środkami bezpieczeństwa, powinno również zapewnić możliwość skutecznego i szybkiego reagowania na incydenty zewnętrzne z bezpieczeństwem komputerowym, takie jak nieautoryzowane ingerencje, ataki kodów złośliwych i wirusów komputerowych. Potencjalny przeciwnik może zadać poważne straty bez użycia tradycyjnych sposobów walki, czyli użycia konwencjonalnej broni, czy w końcu mało prawdopodobnego użycia BMR, oraz narażenia na straty własnych sił i środków. Oddziaływująca tylko na systemy dowodzenia i zarządzania, przeciwnik może obezwładnić a nawet zniszczyć istotne elementy obronnej infrastruktury wojskowej i cywilnej. Walka informacyjna i cyberterroryzm stają się realnym zagrożeniem dla bezpieczeństwa narodowego. W poszukiwaniu sposobów ochrony, niezbędnym jest gromadzenie wiedzy o stanie otoczenia i rodzących się przesłankach zagrożeń, które z natury rzeczy będą utrzymywane przez zainteresowanego w jak największej tajemnicy. Zapewnienie bezpieczeństwa państwa w aspekcie zewnętrznym i wewnętrznym jest podstawowym obowiązkiem wszystkich szczebli zarządzania i kierowania państwem. Potrzeba ta wynika zarówno z uwarunkowań wewnętrznych, jak również z ewolucji otoczenia zewnętrznego. W obu tych obszarach powstają wyzwania i zagrożenia dla społeczeństwa i państwa. Zbieranie informacji o zagrożeniach prowadzą różne organizacje i instytucje posiadające odpowiednie siły i środki do ich wykrywania, likwidacji i zapobiegania. Brak systemu wczesnego ostrzegania może doprowadzić do szkodliwych zmian w środowisku, a w przypadku rozwoju zagrożenia na większą saklę, do powstania sytuacji kryzysowych.

5. IDENTYFIKACJA NOWOCZESNYCH TECHNOLOGII MOŻLIWYCH DO ZASTOSOWANIA W STACJONARNEJ SIECI TELEINFORMATYCZNEJ UŻYTKOWANEJ PRZEZ SIŁY ZBROJNE

Niniejszy rozdział stanowi próbę odpowiedzi na jedno z pytań problemowych, zawartych w rozdziale metodologicznym, a mianowicie, ***jakie współczesne urządzenia i technologie teleinformatyczne są możliwe do zastosowania w stacjonarnej sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej aby mogła sprawniej spełniać stawiane przed nią zadania łączności.***

W celu realizacji powyższego celu, autor założył rozwiązać go stosując następujące metody:

teoretyczne - analizę, syntezę, porównanie, uogólnienie, abstrahowanie i wnioskowanie,

empiryczne - sondaż diagnostyczny techniką analizy dokumentów.

5.1 Charakterystyka stacjonarnego sprzętu teleinformatycznego do organizacji węzłów łączności na Stanowiskach Dowodzenia.

W Wojskowym Systemie Telekomunikacyjnym wykorzystywane są systemy telekomunikacyjne, które wyspecyfikowano w tabeli nr 5.1. Informacje te zostały zebrane i opracowane przez oficerów Departamentu Telekomunikacji i Informatyki oraz opublikowane w „**Strategii Informatyzacji Resortu Obrony Narodowej"** na lata 2008-2012

Tabela 5.1

Wykaz sprzętu teletransmisyjnego

L.p.	Rodzaje systemów telekomunikacyjnych	Przykłady
1.	**Systemy teletransmisyjne**	
	Cyfrowe typu PDH, SDH i ATM	PDH (MUX-OLOTE), Cross Connect (DGT 3300), SDH (SMA – ¼), ATM
	bezprzewodowe	Radiolinie I radiostacje
2.	**Systemy komutacyjne**	
	Centrale abonenckie	DGT 3450, ALCATEL OCB – 283, ALCATEL 4400, HICOM

		300E Siemens
	Centrale tranzytowe	ALCATEL OCB - 283
	Centrale dyspozytorskie	ALCATEL (4400, 4100, BCN 5200), DGT Caro 2, DGT Caro 3
3.	**Dedykowane systemy łączności**	
	Systemy szybkiej łączności dyspozytorsko - konferencyjnej	CDK
	Podsystem cyfrowej łączności utajnionej	PCŁU
	Komputerowy Telefoniczny System Alarmowania	KTSA
	System radiowej łączności dowodzenia i powiadamiania	ASA
4.	**System łączności radiowej, radioliniowej i satelitarnej**	
	Radiowy system łączności dowodzenia	Zakresu KF, VHF
	Dyspozytorskie systemy łączności radiowej	TETRA
	Systemy łączności radioliniowej	RL – 432, R - 450
	Systemy łączności satelitarnej	WZŁ - 1

Systemy komutacyjne realizują telefoniczną łączności jawną dla użytkowników wojskowego systemu telekomunikacyjnego oraz zabezpieczają współpracę i wymianę usług w zakresie łączności telefonicznej z operatorami resortowymi i sektora publicznego.

Dedykowane systemy łączności służą realizacji wyodrębnionych i specyficznych funkcji Wojskowego Systemu Telekomunikacyjnego związanych z kierowaniem resortem obrony narodowej i dowodzeniem Siłami Zbrojnymi RP. Część z systemów eksploatowanych przez SZ RP może być wykorzystana jako element projektowanej stacjonarnej sieci teleinformatycznej na potrzeby dowodzenia siłami zbrojnymi.

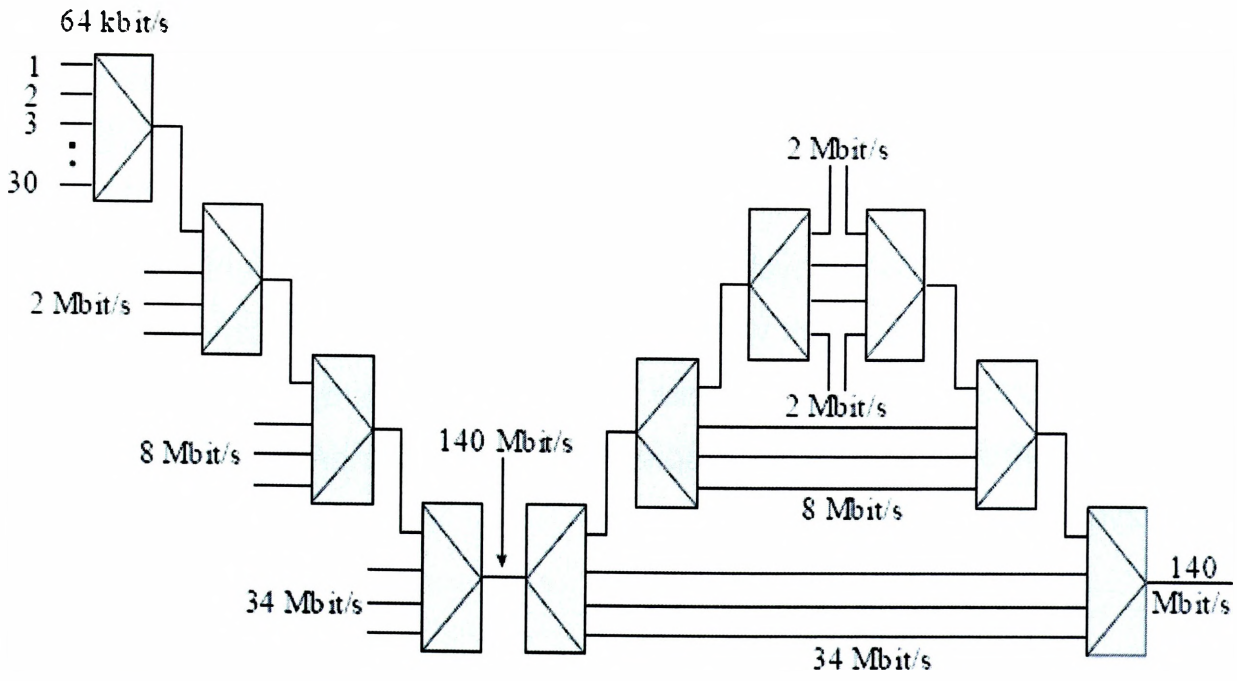
Kontynuując myśl przewodnią niniejszej rozprawy, związaną z opracowaniem autorskiej koncepcji stacjonarnej sieci teleinformatycznej na potrzeby dowodzenia siłami zbrojnymi, niezbędne jest przybliżenie czytelnikowi wybranych urządzeń

teletransmisyjnych, które potencjalnie można by zastosować w sieci teleinformatycznej na poziomie strategicznym.

Systemy transmisyjne pełnią rolę sieci ***dostępowej*** lub ***dostępowej i szkieletowej*** zapewniając szeroki zakres usług wymagany przez systemy teleinformatyczne zarówno w zakresie transmisji kanałów rozmównych jak i transmisji danych. W celu przybliżenia czytelnikowi systemów teletransmisyjnych autor dokonał sondażu diagnostycznego techniką analizy dokumentów (Arkusz analizy dokumentów dotyczący identyfikacji kluczowych technologii teleinformatycznych – **zał. 9**) a następnie porównania stosowanych w siłach zbrojnych i możliwych do zastosowania nw. systemów.

- **Krotnica PDH**

PDH – Pleziochroniczny system zwielokrotnienia (ang. Plesiochronous Digital Hierarchy) i transportu sygnałów cyfrowych, oparty jest na modulacji kodowo – impulsowej PCM. Technologia używana w sieciach telekomunikacyjnych. Elementy sieci PDH są ze sobą zsynchronizowane, ale nie idealnie gdyż każdy z elementów sieci posiada swój zegar. Pojedynczy kanał ma przepływność 64kbit/s co pozwala na przesyłanie jednej nieskompresowanej rozmowy telefonicznej. Systemy PDH przy multipleksacji wykorzystują zwielokrotnienie z podziałem czasu TDM (ang. Time Division Multiplexing).



Rys. 5.1 Europejska hierarchia zwielokrotnienia

Źródło :Opracowanie własne na podstawie Instrukcji obsługi PDH

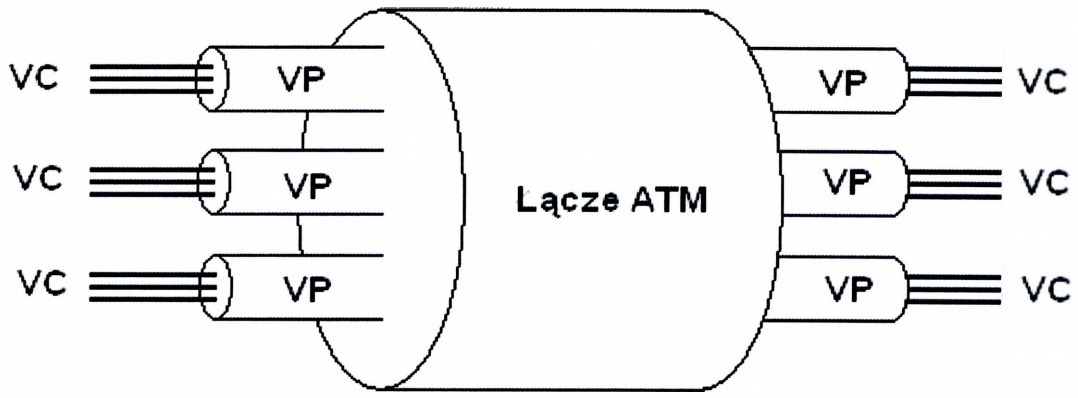
Wady i zalety systemów PDH

- w porównaniu do nowszych technologii mała przepływność sygnału liniowego;
- zawodność systemów PDH;
- energochłonność;
- konieczność stosowania hierarchii demultiplekserów kiedy chcemy wydzielić pojedynczy sygnał E1 z E4;
- brak standaryzacji ostatnich stopni zwielokrotniania (E5, T4);
- trzy różne standardy PDH na świecie (Europa, Ameryka, Japonia).

- **ATM** (ang. *Asynchronous Transfer Mode*) - to szerokopasmowa technologia komunikacyjna, dzięki której możliwe jest przesyłanie danych interakcyjnych, różnej wielkości plików, sygnału wizyjnego a także możliwa jest transmisja głosu. Jest to standard, który obecnie może być stosowany w sieciach lokalnych LAN, miejskich MAN a nawet rozległych WAN. Informacja w tym standardzie przesyłana jest w postaci krótkich pakietów zaopatrzonych w nagłówek o minimalnej wielkości (48 bajtów informacji + 5 bajtów nagłówka).

Pomiędzy stacją źródłową a docelową zostaje zestawione logiczne połączenie zwane kanałem wirtualnym VCC (ang. *Virtual Channel Connection*). Kanały o tym samym węźle docelowym tworzą tzw. wirtualną ścieżkę VPC (ang. *Virtual Path Connection*). W komutatorze ATM ma miejsce multipleksacja statystyczna poszczególnych kanałów. Kanały i ścieżki wirtualne są rozróżniane przez części nagłówka ATM - pole VPI (ang. *Virtual Path Identifier*) i pole VCI (ang. *Virtual Channel Identifier*).

Użycie ścieżek wirtualnych znacznie upraszcza zarządzanie całą siecią. Wynika to z faktu, że liczba ścieżek wirtualnych jest mniejsza od liczby kanałów wirtualnych. Dzięki temu zestawienie połączenia w węźle pośrednim, przez który przebiega dana ścieżka, wpływa na przyspieszenie zestawiania nowego połączenia, wykorzystującego ścieżki wirtualne.



Rys. 5.2 *Relacja pomiędzy kanałem wirtualnym, ścieżką wirtualną i łączem ATM*

Źródło :Opracowanie własne na podstawie Instrukcji obsługi ATM

- **DWDM** (*ang. Dense Wavelength Division Multiplexing*)

Jest to technika multipleksacji wielu sygnałów cyfrowych w jednym łączu światłowodowym z przydzieleniem każdemu sygnałowi innej długości fali świetlnej, innego kanału. Ze względu na ilość kanałów rozróżniamy takie technologie jak CWDM (*ang. Coarse Wavelength Division Multiplexing*) i WDM (ang. Wavelength Division Multiplexing).

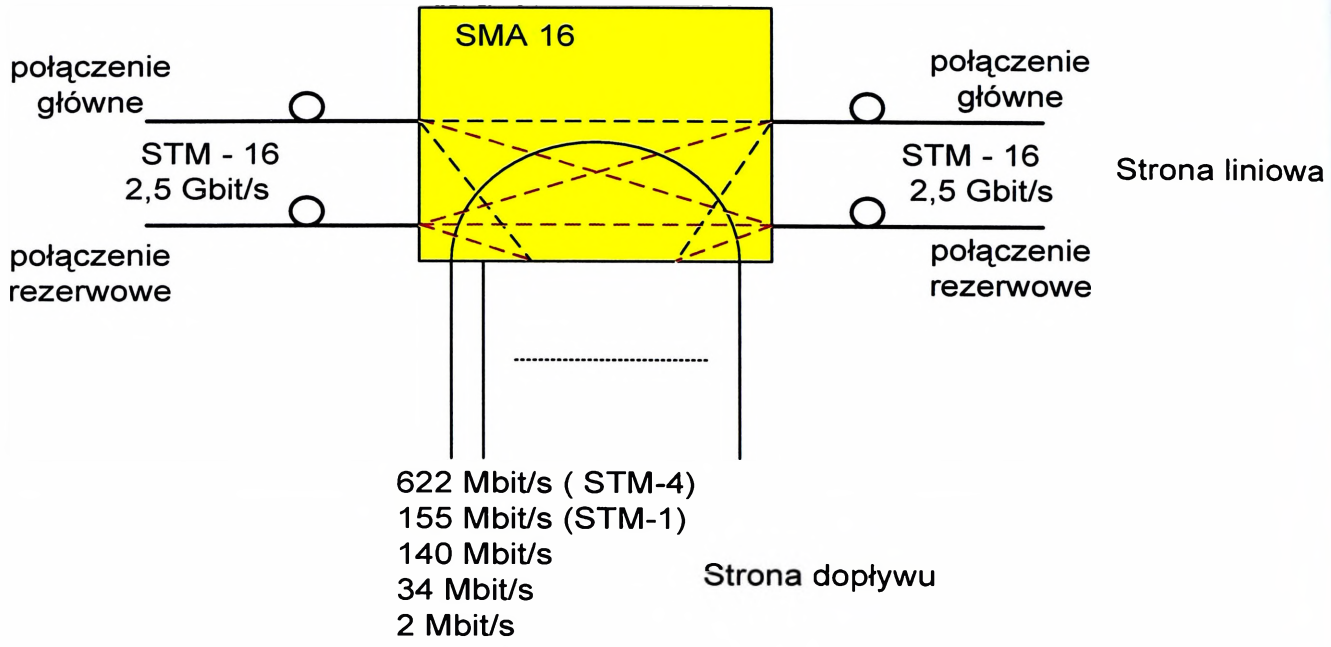
Ponieważ odstępy między kanałami są bardzo małe ok. 0,8nm, wygodnie jest charakteryzować falę poprzez jej częstotliwość, a nie długość fali. Siatka DWDM opracowana przez ITU opiera się na częstotliwości 193,1 THz, to jest 1552,52 nm. W istniejących światłowodach przy mało różniących się długościach fal można osiągać już krotności 400 kanałów DWDM, co odpowiada przepływności rzędu Tbit/s. Na przykład firma NEC w roku 2000, na odcinku 168 km osiągnęła szybkość transmisji 6,4 Tbit/s. Gęste zwielokrotnienie falowe DWDM jest jednym z rozwiązań dla superszybkich sieci szkieletowych, można zwiększyć przepustowość łączy bez inwestowania w nowe instalacje światłowodowe.

Inną odmianą technologii DWDM jest technologia UDWDM (*ang. Ultra Dense Wavelength Division Multiplexing*). Tutaj odstępy międzykanałowe są rzędu 0,4 nm (80 kanałów) lub mniejsze.

- **Krotnica SDH STM -16**

Na rysunku 5.3 przedstawiony jest model krotnicy SMA – 16 (karta katalogowa STM – 16 – **zał. 10**), która umożliwia tworzenie sieci szkieletowej o przepływności 2,5 Gbit/s po włóknach światłowodowych głównych lub w przypadku awarii

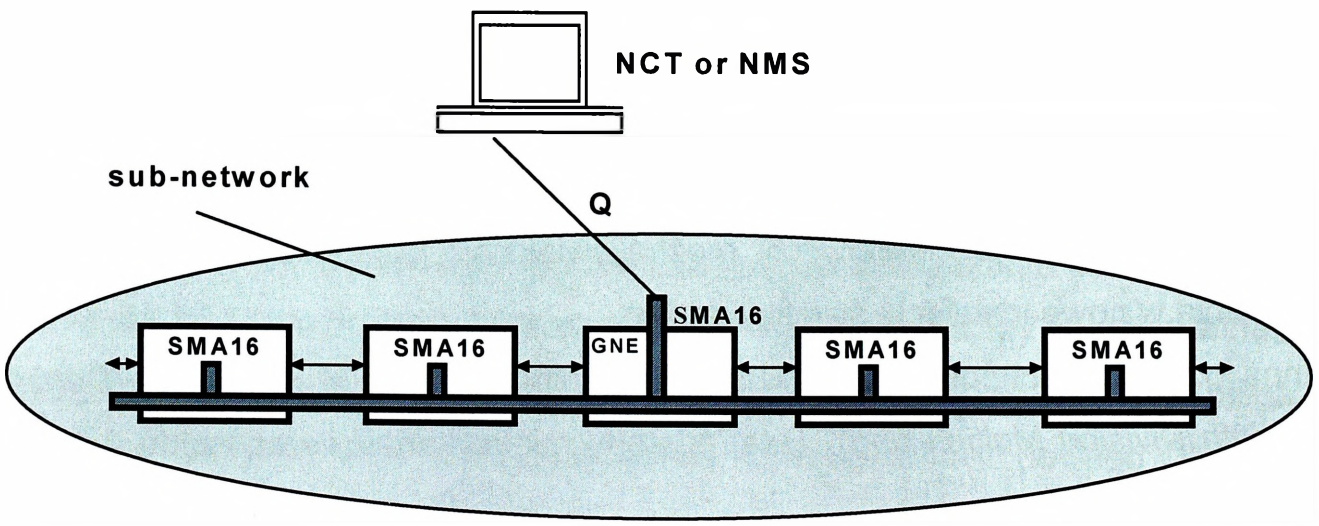
automatyczne przełącza się na włókna rezerwowe. Po stronie dopływu krotnica umożliwia utworzenia dwóch pierścieni SDH o przepływności 622 Mbit/s i 155 Mbit/s oraz trzech relacji PDH o przepływności 140 Mbit/s, 34 Mbit/s i 2Mbit/s.



Rys. 5.3 *Schemat krotnicy SMA – 16*

Źródło :Opracowanie własne na podstawie Instrukcji obsługi STM – 16

Utworzona sieć teleinformatyczna na bazie krotnic SDH daje nieograniczone możliwości konfiguracji sieci szkieletowej na potrzeby dowodzenia.

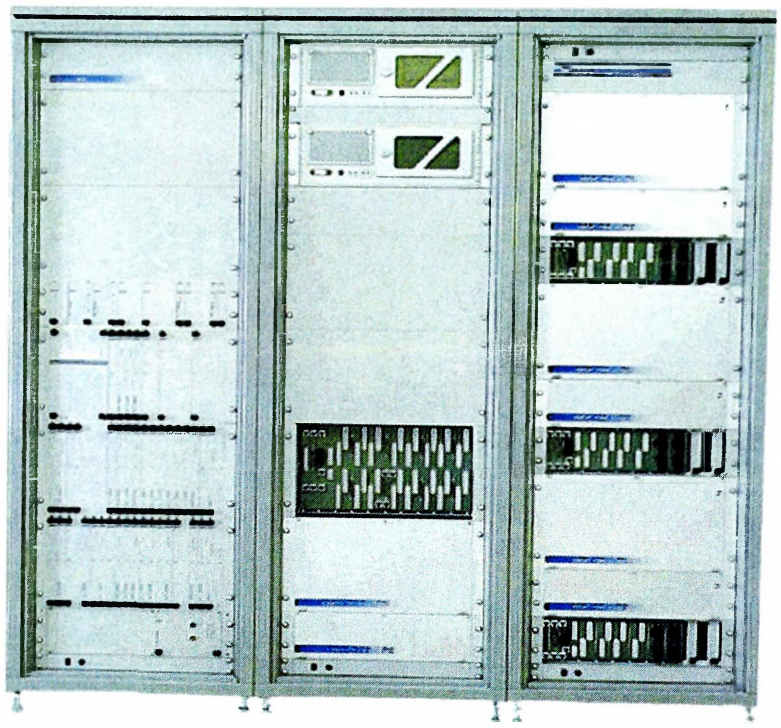


Rys. 5.4 *Schemat blokowy systemy zarządzania krotnicami SMA – 16*
Źródło :Opracowanie własne na podstawie Instrukcji obsługi STM – 16

Na rysunku 5.4 przedstawiony jest sposób zarządzania systemem krotnic SMA16. Zdalne zarządzanie systemem oparte jest na standardzie TMN i umożliwia serwisowanie systemu w czasie awarii oraz szybką rekonfigurację przepływności w zależności od potrzeb. Terminali zarządzających może być więcej niż jeden co

daje możliwość zwiększenia bezpieczeństwa systemu w przypadku uszkodzeń zarządzania.

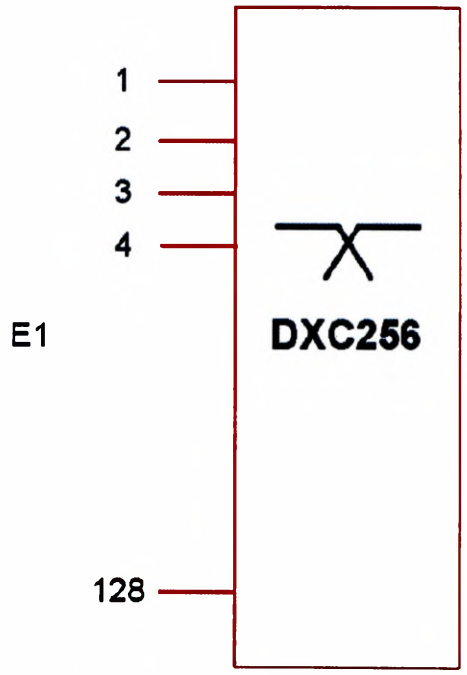
- **Cross Connect**



Rys. 5.5 *Zdjęcie systemu Cross Connect DGT 3300*
Źródło : Instrukcji obsługi Cross Connect

W skład systemu wchodzą następujące elementy:

- Automatyczna Przełącznica cyfrowa DXC256;
- Krotnica cyfrowa MX64;
- Koncentrator Łączy KŁ.



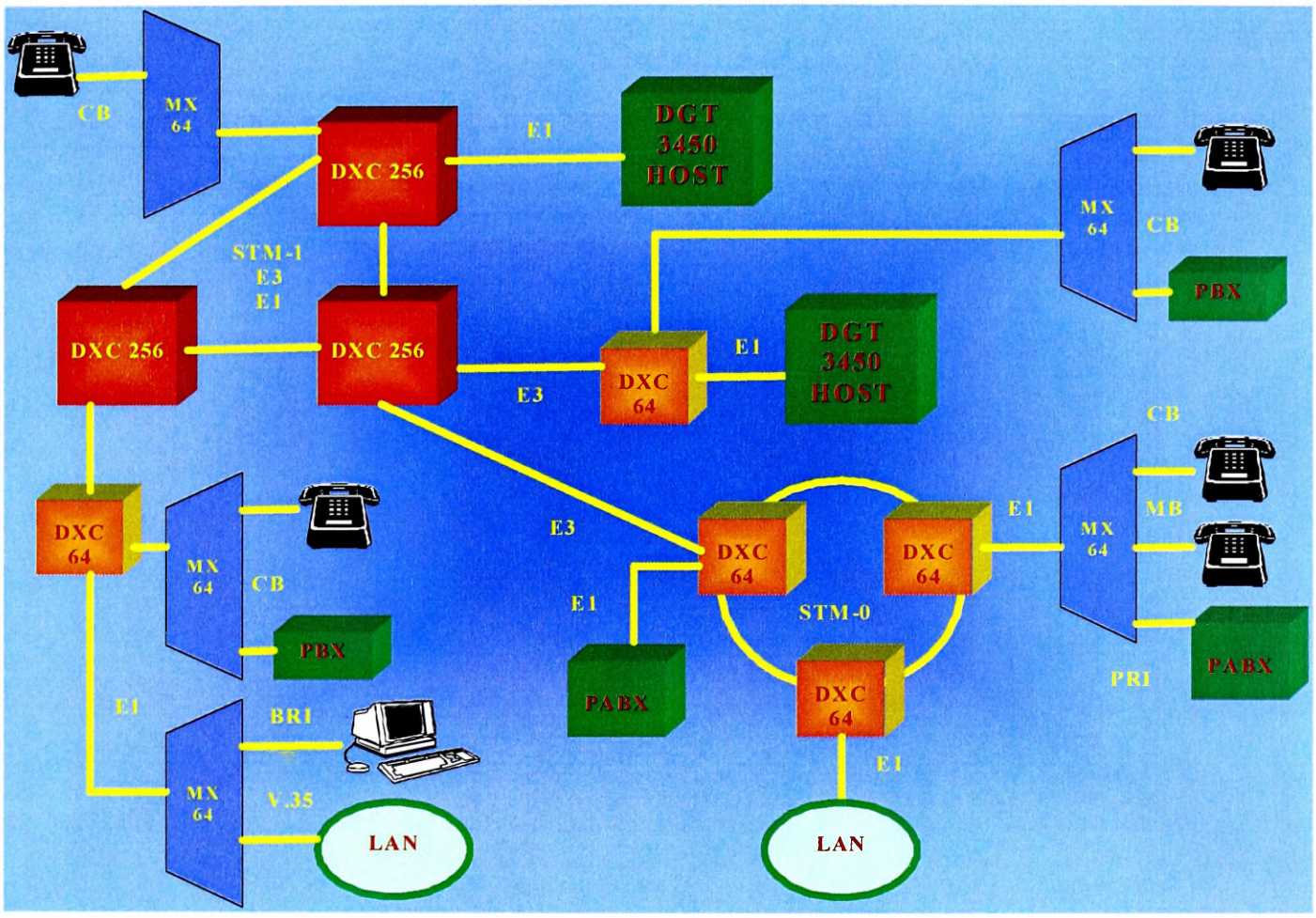
Przełącznica cyfrowa umożliwia:

- Komutacja na poziomie pojedynczych szczelin
- Interfejsy E1 - 2048kbit/s
- Dwukierunkowa, komutacja do 128 strumieni 2,048Mbit/s
- Komutacja na poziomie pojedynczego kanału 64kbit/s
- Transparentne przenoszenie sygnalizacji
- Możliwość grupowania kanałów
- Elastyczna i szybka rekonfiguracja dróg połączeniowych

System posiada wiele pozytywnych cech (karta katalogowa DXC – 256 – **zał. 11**), jednak do najważniejszych zaliczyć można komutowanie pojedynczych szczelin 64 kbit/s co bardzo ułatwia czynności przy podłączaniu pojedynczych urządzeń na węzłach a jednocześnie system Cross connect uzupełnia się z systemem SDH, który nie komutuje pojedynczych szczelin. Zarządzanie cross connectami również oparte jest na technologii TMN i daje nieograniczone możliwości:

- Hierarchiczny podział na domeny zarządzania;
- Zarządzanie siecią i elementami sieci;
- Zarządzanie centralne (TCP/IP) i za pośrednictwem terminala lokalnego;
- Możliwość zarządzania dowolnymi zasobami sieci z każdego terminala utrzymaniowego;
- Wirtualne stanowiska zarządzania;
- Definiowalne profile użytkowników;

- Graficzna prezentacja zarządzanej sieci;
- Rozproszony system zabezpieczeń;
- Nowoczesne środowisko oprogramowania (JAVA/CORBA);



Rys. 5.6 *Przykładowa konfiguracja sieci systemu DGT 3300*
Źródło : Instrukcji obsługi Cross Connect

5.2 Synteza wniosków z badań

Tabela 5.2

Charakterystyka urządzeń teleinformatycznych

L.p.	**System** **Możliwości**	**Krotnica PDH**	**ATM**	**DWDM**	**Krotnica SDH STM - 16**	**Cross - Connect**
1.	Przepływność	2Mbit/s 34Mbit/s 140Mbit/s	Dynamiczna Do2,5Gbit/s	Do 10Tbit/s	155Mbit/s 622Mbit/s 2,5Gbit/s	2Mbit/s 34Mbit/s 155Mbit/s
2.	Zawodność	0	1	1	1	1
3.	Zarządzanie	0	1	1	1	1
4.	Możliwość rozdziału	0	0	0	0	1

	przepływności poniżej 2Mbit/s					
5.	Energochłonność	0	1	1	1	1
6.	Redundancja połączeń	0	1	1	1	1
7.	Możliwość dynamicznej konfiguracji	0	1	1	1	1
8.	Interfejs TCP/IP	0	0	0	0	1
9.	Cena	1	0	0	1	1
	Podsumowanie	**1**	**5**	**5**	**6**	**8**

Przedstawione charakterystyki wybranych urządzeń teleinformatycznych oraz porównanie ich parametrów pozwoliło na jednoznaczne wskazanie z punktu widzenia organizacji stacjonarnego systemu teleinformatycznego na poziomie strategicznym najlepszych możliwych do zastosowania urządzeń. Biorąc pod uwagę cechy projektowanego systemu rozległej sieci teleinformatycznej (sieci WAN) opartej (od strony użytkownika) na technologii przełączania pakietów (protokół IP) i obejmującej wszystkie jednostki organizacyjne resortu można stwierdzić, że najlepszymi urządzeniami pod tym kątem są SDH oraz Cross Connect.

6. AUTORSKA KONCEPCJA STACJONARNEJ SIECI TELEINFORMATYCZNEJ SIŁ ZBROJNYCH RZECZYPOSPOLITEJ POLSKIEJ.

Niniejszy rozdział stanowi próbę odpowiedzi na pytania problemowe, przedstawione w rozdziale metodologicznym, a mianowicie, ***jaka powinna być struktura organizacyjno – techniczna stacjonarnej sieci teleinformatycznej aby mogła zapewnić świadczenie podstawowych usług teleinformatycznych w procesie dowodzenia Siłami Zbrojnymi.*** W celu realizacji powyższego celu, autor dokonał analizy i przedstawił, na bazie uzyskanych wyników badań, autorską koncepcję struktury organizacyjno-technicznej sieci teleinformatycznej, zapewniająca realizację świadczenia podstawowych usług teleinformatycznych w procesie dowodzenia wojskami w czasie pokoju, kryzysu i zagrożenia militarnego państwa.

6.1 Architektura proponowanego rozwiązania ogólnokrajowego

6.1.1 Wprowadzenie

Obowiązująca strategia bezpieczeństwa naszego kraju ma charakter typowo obronny i zakłada działania wojsk głównie na obszarze kraju, choć nie wyklucza działań zbrojnych poza granicami kraju np. w ramach operacji sojuszniczych NATO.

W związku z powyższym, można założyć, że na potrzeby wojennego systemu dowodzenia SZ RP na szczeblu strategicznym, udział stacjonarnych sieci teleinformatycznej będzie znacznie większy, niż polowych systemów teleinformatycznych. Przy czym jest oczywiste, że w warunkach prowadzenia działań zbrojnych na obszarze kraju, zakres oraz sposoby wykorzystania stacjonarnej sieci teleinformatycznej będą różne w zależności od rejonu obrony.

Ostatnie lata przyniosły istotne zmiany w wojskowych sieciach teleinformatycznych. Zmiany te mają swoje uwarunkowania w wielu czynnikach, spośród których najistotniejszymi są:

a) rozwój techniki cyfrowej oraz integracja łączności i informatyki w jeden system teleinformatyczny,
b) zmiany w sztuce operacyjnej i taktyce, będące konsekwencją zmiany doktryny obronnej naszego kraju.

Rozwój techniki cyfrowej niemal całkowicie wyeliminował sprzęt wykonany w technice analogowej i stworzył nową dziedzinę łączności - teleinformatykę.

Działania na własnym terytorium zmieniły na szczeblach strategiczno - operacyjnych dowodzenia dotychczasową rolę polowego i stacjonarnego systemu łączności w zapewnieniu dowodzenia – nadając priorytet temu drugiemu.

Przy założeniu, że stanowiska dowodzenia szczebla strategicznego i operacyjnego będą z reguły rozmieszczane w obiektach stacjonarnych, łączność na ich potrzeby zapewniona będzie głównie poprzez stacjonarne węzły łączności, powiązane liniami stałymi, wzmacniane bądź uzupełniane środkami polowymi.

6.1.2 Potrzeby a możliwości sieci teleinformatycznej SZ RP

Główny problem badawczy, który został przedstawiony w rozdziale metodologicznym polegał na zbadaniu, czy obecnie funkcjonująca sieć teleinformatyczna w siłach zbrojnych odpowiada potrzebom na usługi teleinformatyczne wynikające z procesu dowodzenia w czasie pokoju, kryzysu i zagrożenia militarnego państwa, a jeżeli nie to jaka powinna ona być. W celu odpowiedzi na główny problem badawczy w rozdziale 2. scharakteryzowano potrzeby na usługi telekomunikacyjne, gdzie stwierdzono, że z punktu widzenia użytkowników najważniejszymi usługami są:

- **telefonia;**
- **transmisja faksów;**
- **telekonferencja dla wybranych grup użytkowników;**
- **transmisja danych między użytkownikami;**
- **wyszukiwanie informacji,** w tym**:**
  - dostęp do centralnych baz danych,
  - dostęp do lokalnych baz danych,
  - dostęp do różnych zasobów danych z wykorzystaniem Internetu.
- **multimedia** (w tym np. wideokonferencja),
- **inne** (w tym np. szeroka gama usług sieci ISDN oraz usługi związane z tzw. sieciami inteligentnymi),

Powyższe zadania łączności realizowane będą w oparciu o sieć teleinformatyczną sił zbrojnych.

Jednak aby realizacja powyższych usług w systemie dowodzenia była możliwa, sieć teleinformatyczna musi być wydajna o odpowiedniej konfiguracji i przepływności. Możliwości sieci teleinformatycznej tak jak zostało to stwierdzone w

rozdziale 3. na podstawie badań jest ograniczona. Głównymi czynnikami ograniczającymi możliwości są:

- ograniczona przepływność łączy;
- brak odpowiednich interfejsów na węzłach regionalnych.

W trakcie dalszych badań w rozdziale 4. zastały wyselekcjonowane najważniejsze zagrożenia i czynniki wpływające na funkcjonowanie stacjonarnej sieci teleinformatycznej, które w znaczący sposób podwyższają wymagania na budowę i organizację takiej sieci. Reasumując, organizacja stacjonarnej sieci teleinformatycznej jest priorytetowym elementem prawidłowego funkcjonowania całego systemu dowodzenia siłami zbrojnymi i dlatego sieć teleinformatyczna powinna sprostać odpowiednim zadaniom, jednak aby mogła sprostać wszelkim potrzebom wynikającym z procesu dowodzenia, biorąc pod uwagę dzisiejsze możliwości ***koniecznym wydaje się wybudowanie rozległej, wydajnej sieci teleinformatycznej***.

Planowana przez autora wojskowa stacjonarna sieć teleinformatyczna oparta jest na jednej - wspólnej dla wszystkich usług i systemów informatycznych eksploatowanych w resorcie Obrony Narodowej – rozległej sieci teleinformatycznej (sieci WAN) opartej (od strony użytkownika) na technologii przełączania pakietów (protokół IP) i obejmującej wszystkie jednostki organizacyjne resortu. Oznacza to wykorzystanie tego samego urządzenia teletransmisyjnego do budowy łączy WAN, niezależnie od klauzuli informacji przesyłanych do/z jednostki. Celem uniezależnienia sieci WAN od zmian restrukturyzacyjnych w resorcie ON autor założył, że będzie ona zbudowana zgodnie z podziałem geograficznym a nie organizacyjnym. Szkielet sieci oparty jest na węzłach sieci szkieletowej zlokalizowanych w Regionalnych Węzłach Łączności. W celu zwiększenia niezawodności sieci, autor przyjął stosowanie zasady pełnej redundancji połączeń szkieletowych oraz urządzeń wchodzących w skład ww. węzłów. Z uwagi na przewidywane wymagania transmisyjne przyszłych aplikacji autor założył, że łącza WAN, do budowy których zamierza wykorzystać protokoły warstw niższych (SDH, Ethernet) mają przepływność 2,5 Gbit/s w szkielecie sieci.

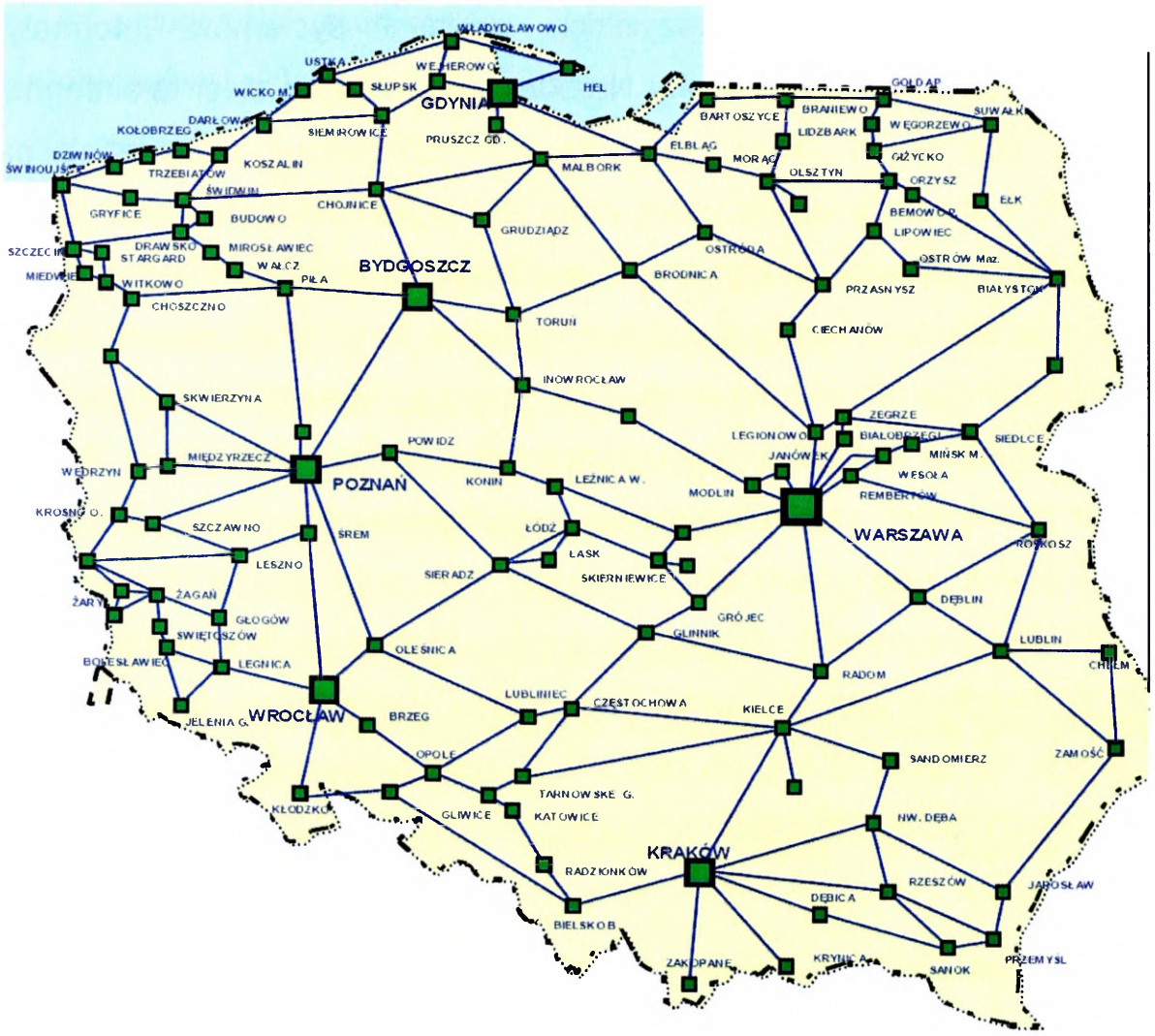
6.1.3 Topologia proponowanego rozwiązania

Przyjęte rozwiązanie sieci teleinformatycznej, dla potrzeb dowodzenia siłami zbrojnymi, rozpatrywane jest pod kątem funkcjonującą strukturę Departamentu Informatyki i Telekomunikacji oraz Centrum Zarządzania Systemami Teleinformatycznymi i charakteryzuje się dużą skalowalnością przepływności od 2 Mbit/s do 2,5 Gbit/s w zależności od możliwości urządzeń zwielokrotniających.

W czasie pokoju systemy dowodzenia SZ RP funkcjonują przy wykorzystaniu istniejącego potencjału stacjonarnej sieci teleinformatycznej MON.

6.1.3.1 Sieć PDH

Na potrzeby łączności dalekosiężnej (międzymiastowej, międzygarnizonowej) wojskowa stacjonarna sieć teleinformatyczna wykorzystuje dzierżawione od operatorów publicznych łącza cyfrowe (2 Mbit/s) zgodnie z załączonym poniżej rysunkiem, który powstał na podstawie przeanalizowanej literatury przedmiotu.



Rys. 6.1 *Schemat sieci PDH w relacjach międzygarnizonowych*

Źródło: „Strategia informatyzacji Sił Zbrojnych"

Tabela 6.1

Zestawienie ilości łączy PDH w istniejącym systemie teleinformatycznym

L.p.	Łącza	Ilość
1.	Strumienie cyfrowe < 2Mbit/s	55
2.	Strumienie cyfrowe 2Mbit/s	294
3.	Strumienie cyfrowe 8Mbit/s	10
4.	Strumienie cyfrowe 34Mbit/s	1
5.	Strumienie cyfrowe > 34Mbit/s	0

Na rysunku 6.1 przedstawiona została istniejąca topologia sieci teleinformatycznej opartej o technologię PDH, natomiast w tabeli 6.1 przedstawione zostało ilościowe zestawienie strumieni cyfrowych wraz z ich przepływnościami. Z przedstawionego materiału widać, że przeważająca ilość łączy nie przekracza 2Mbit/s. Jedynym możliwym sposobem poprawienia możliwości sieci teleinformatycznej jest zwiększenia przepływności łączy. Jednak autor przyjął, że technologia PDH jest nieperspektywiczna i nie ma sensu brnąć w przestarzałą technologię. System PDH nie posiada możliwości zarządzania, rezerwowania połączeń w przypadku awarii sieci oraz jest technologią energochłonną.

6.1.3.2 Sieć ATM

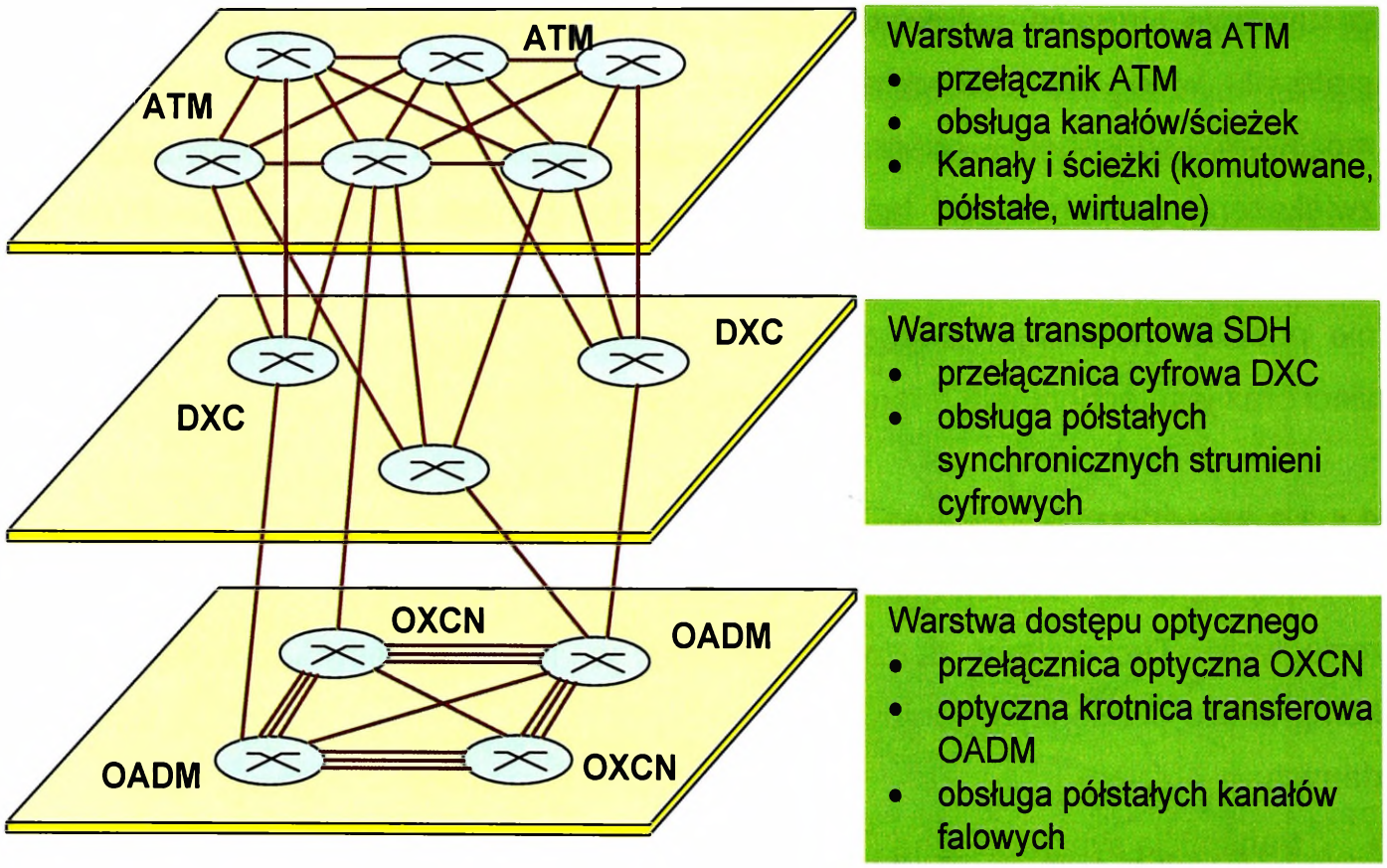
ATM oznacza asynchroniczny sposób transferu strumieni danych w sieciach rozległych. Technologia ta powstała aby w fundamentalny sposób dokonać kompromisu pomiędzy dwoma bardzo różniącymi się technikami cyfrowej transmisji danych:

- transmisją synchroniczną (stosowaną głównie w telekomunikacji);
- transmisją pakietową (stosowaną głównie w sieciach komputerowych).

Transmisja synchroniczna - Synchronous Transfer Mode STM, pozwala na zestawianie połączeń komutowanych, pomiędzy nadawcą a odbiorcą w czasie rzeczywistym. Transmisje STM są na ogół drogie w użytkowaniu, gdyż technologie działające w ramach STM są kosztowne.

Transmisja pakietowa - PTM Packet Transfer Mode nie przesyła danych w czasie rzeczywistym. Dzieli ona strumień cyfrowy na określonej długości bloki danych zwane pakietami i wysyła je do odbiorcy. Technologia ATM zapewnia podstawowy przekaz informacji w trybie połączeniowym, co oznacza, że przesyłaniem informacji

właściwej musi wystąpić faza zestawienia łączy (również wirtualnego) na podstawie parametrów deklarowanych przez abonenta. Technika ATM jest technika asynchroniczną, co oznacza, że szybkość transmisji w ramach kanału wirtualnego jest zmienna, zgodnie z szybkością źródła lub najbliższego węzła. W sieci ATM węzły nie sprawdzają poprawności przesyłanej informacji, a kontrola błędów jest prowadzona w systemach użytkowników końcowych. Jednak należy tutaj wspomnieć, że sieć ATM bardzo dobrze sprawuje się osadzona na warstwie transportowej SDH co ilustruje rys. 6.2. Koszty technologii ATM są bardzo wysokie i dlatego autor nie będzie się zajmował budową sieci teleinformatycznych opartej na ATM.



Rys. 6.2 *Schemat sieci ATM*

Źródło: Podstawy telekomunikacji

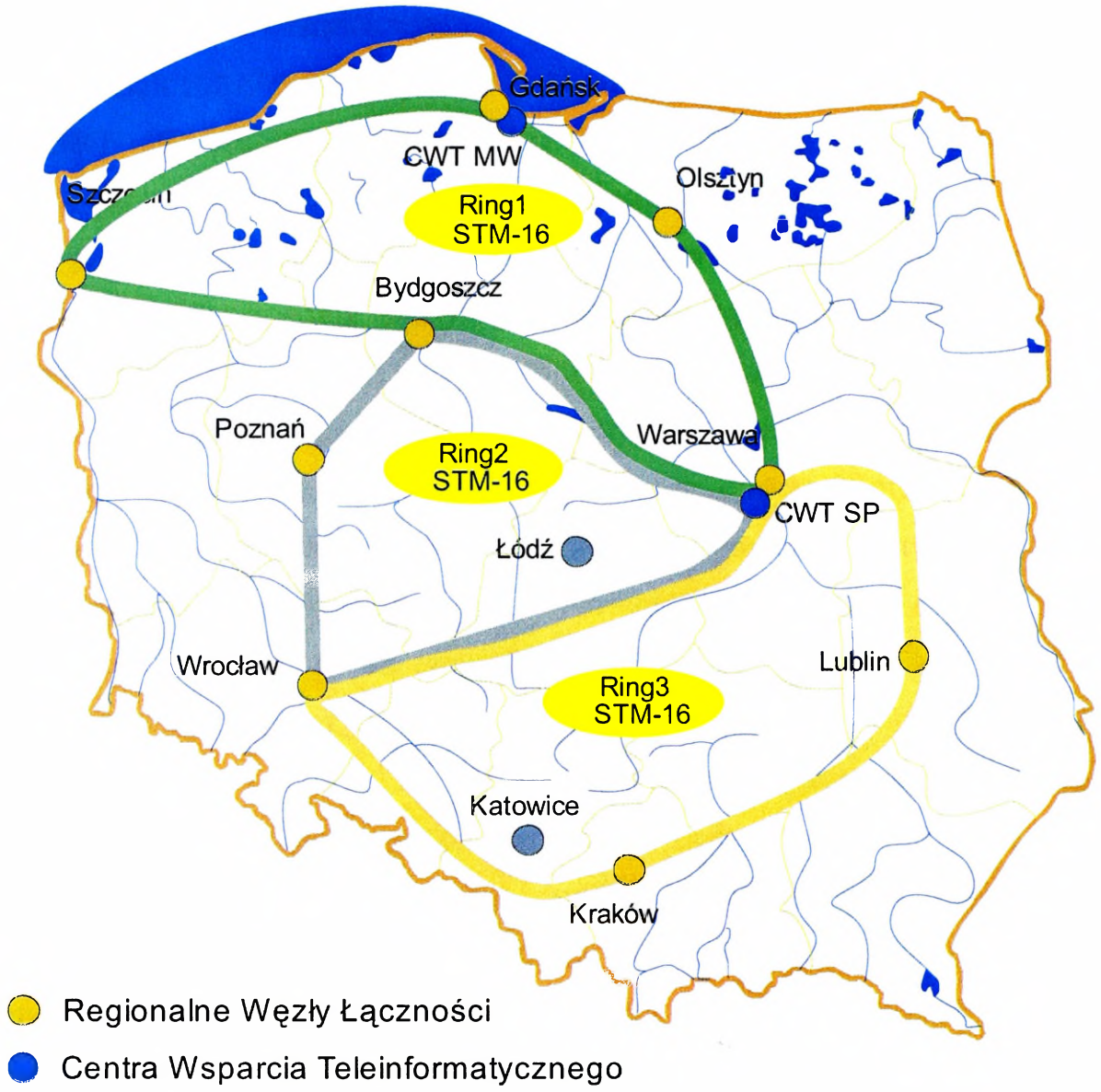
6.1.3.3 Sieć SDH

Reasumując powyższe oraz analizę przeprowadzoną i przedstawioną w 2. rozdziale elementów struktury organizacyjno-technicznej sieci teleinformatycznej, użytkowanej przez Siły Zbrojne Rzeczypospolitej Polskiej na terenie kraju, pod kątem spełnienia przez nią potrzeb wynikających z wymagań na określone rodzaje usług teleinformatyczne wskazuje jednoznacznie, że najlepszym rozwiązaniem budowy sieci teleinformatycznej będzie sieć oparta na **technologii SDH.** System synchroniczny SDH (Synchronous Digital Hierarchy) umożliwia nieograniczony wzrost przepływności (w zależności od potrzeb powyżej 10 Gbit/s) w sieciach teleinformatycznych z zastosowaniem linii optycznych. Podstawową cechą SDH jest synchroniczność przekazu, oparta na stałej ramce transmisyjnej, która jest generowana z głównym zegarem systemu czyli zegarem odniesienia PRC (Primary Reference Clock). System SDH zapewnia pełną redundancję wszystkich połączeń w systemie poprzez przełączanie na linie rezerwowe oraz poprzez przekierowanie ruchu w sposób programowy.

Krotnicy SMA 16 charakteryzuje się możliwością realizacji połączeń pomiędzy : strona liniowa – strona liniowa (line-line), strona dopływowa – strona liniowa (tributary-line), strona dopływowa – strona dopływowa ograniczonej jedynie pojemnością sieci przełączającej. Charakteryzuje się także pełną redundancją połączeń. Dla zapewnienia realizacji wymagań dla systemu dowodzenia, które zostały opisane w rozdziale 2. konieczne jest zapewnienie budowy sieci teleinformatycznej na dwóch poziomach: poziom węzłów regionalnych i centrów wsparcia teleinformatycznego (poziom 1 - STM-16) oraz poziom pozostałych węzłów łączności (poziom 2 - STM-4) . Poziom 1 dla utworzenia głównej sieci szkieletowej (rys. 6.3) sił zbrojnych powinien być wyposażone w następujące urządzenia teletransmisyjne:

- krotnice STM – 16 - 10;
- cross connect - 10;

Przedstawiona na rysunku 6.3 topologia sieci teleinformatycznej jest rozwiązaniem budowy sieci teleinformatycznej pracującej w trzech ringach fizycznych oraz wirtualnych, które są w stanie zapewnić pełną protekcję połączeń w całym systemie. W przypadku awarii urządzeń lub linii światłowodowych zaprogramowany system SDH, w sposób automatyczny przenosi się do pierścienia sąsiedniego zapewniając realizację wszystkich usług.



Rys. 6.3 S*chemat ideowy topologii sieci teleinformatycznej SZ RP na poziomie 1*
Źródło: opracowanie własne

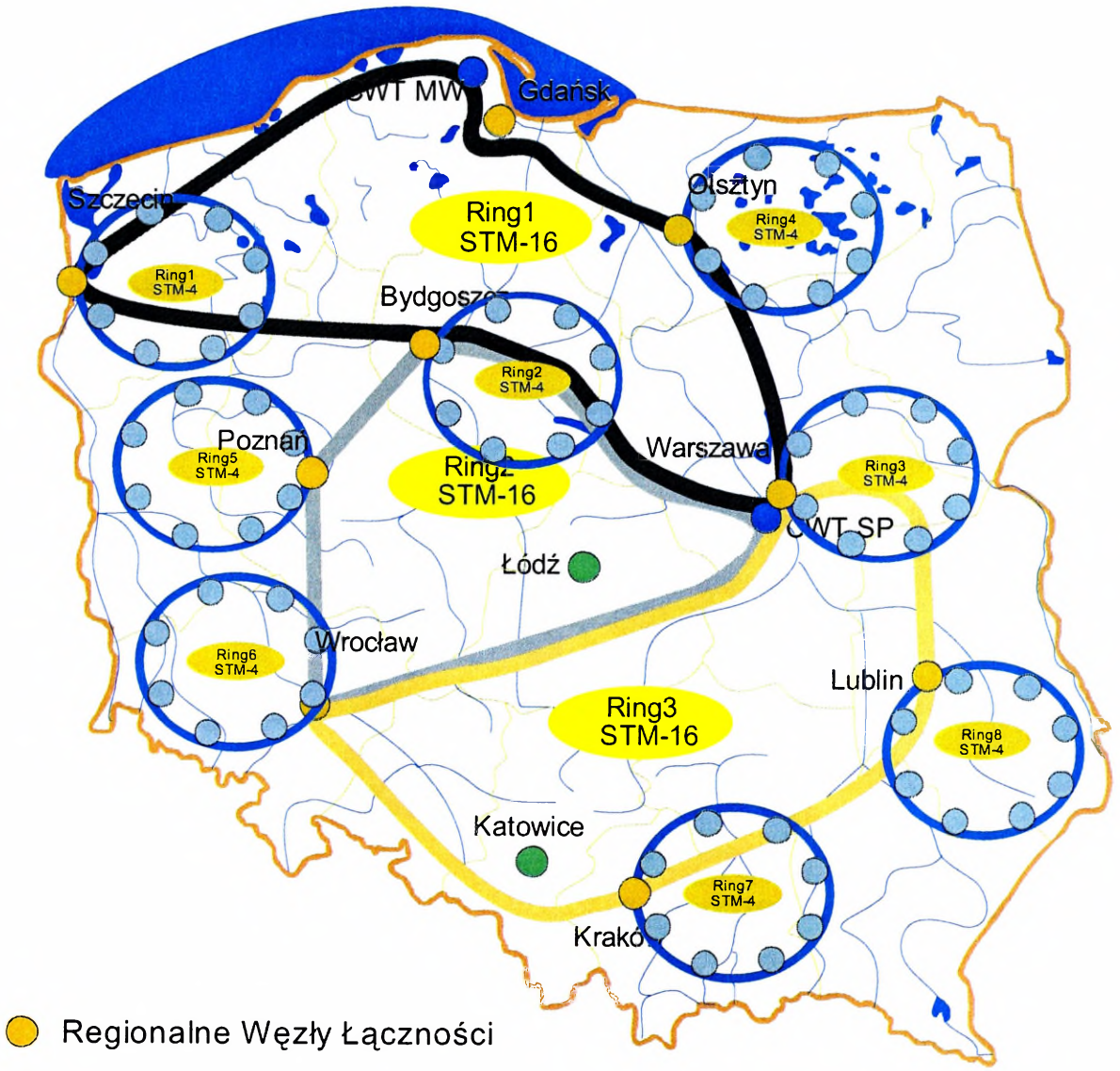
Poziom 2 to osiem sieci szkieletowych na poziomie STM – 4 łączących garnizonowe węzły łączności, które są rozlokowane wokół Węzłów Regionalnych.

Na rysunku 6.4 przedstawiona jest topologia sieci teleinformatycznej na poziomie 2, która pod względem bezpieczeństwa posiada podobne rozwiązania jak sieć na wyższym poziomie.

Poziom 2 powinien być wyposażony w następujące urządzenia teletransmisyjne:

- około 78 krotnic STM – 4;
- około 78 cross connect;

Podane wielkości sprzętu teleinformatycznego oraz topologia sieci są wielkościami przybliżonymi, które w każdym momencie w zależności od potrzeb dowodzenia mogą ulec zmianie.



Rys. 6.4 S*chemat ideowy topologii sieci teleinformatycznej SZ RP na poziomie 2*
Źródło: opracowanie własne

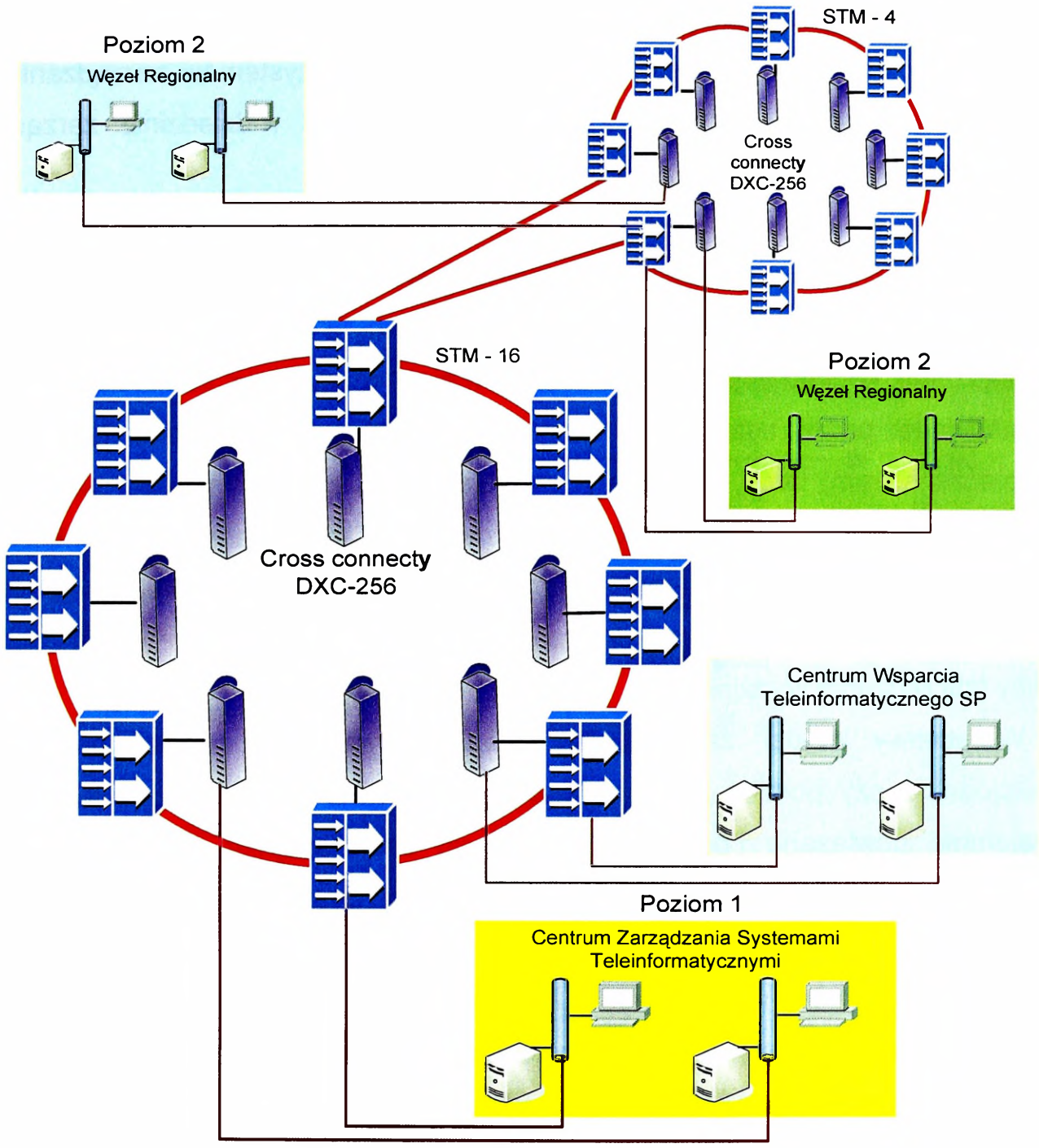
Przyjęcie projektowanego rozwiązania na podstawie analizy dokumentów umożliwi:

- implementację centralnego, sprawnie działającego (z uwagi na przejrzystość struktury technicznej) systemu zarządzania;
- realizację usług na zakładanym poziomie jakości, w niezawodny i bezpieczny sposób oparty na jednolitej infrastrukturze teletransmisyjnej (niezależność od klauzuli i rodzaju ruchu);
- realizację usług w wymaganym przez użytkowników miejscu i czasie;
- niezależność struktury (konfiguracji) sieci od zmian organizacyjnych w resorcie;
- korzystny (w stosunku do obecnie stosowanych rozwiązań) wskaźnik: *nakłady finansowe / stopień wykorzystania;*
- wykorzystywanie ogólnie przyjętych standardów poprzez prostą adaptację najnowszych technologii transmisji;
- budowę centralnych serwerowni o wymaganym poziomie niezawodności;
- realizację (prostą pod względem technicznym) gateway-ów między systemami o różnych klauzulach;
- zwiększenie bezpieczeństwa przesyłania dokumentów stanowiących tajemnice państwową opracowywanych w trybie off-line.

6.2 Zarządzanie systemem

Zarządzania systemem teleinformatycznym zlokalizowane jest w Centrum Zarządzania Systemami Teleinformatycznymi na poziomie 1.

Natomiast poziom 2 obsługiwany jest przez Węzły Regionalne w obrębie swojej odpowiedzialności systemowej i terytorialnej. Tak rozproszony system zarządzania daje większe gwarancje poprawnego funkcjonowania systemu teleinformatycznego w przypadku awarii.



Rys. 6.5 *Przykładowy model zarządzania systemem teleinformatycznym*
Źródło : opracowanie własne

Dla zabezpieczenia poprawności działania systemu zarządzania w przypadku awarii serwerów lub innych urządzeń niezbędnych w procesie zarządzania systemem teleinformatycznym, pod uwagę autor założył rezerwowe terminale zarządzania. Po przeprowadzonej analizie rezerwowy system zarządzania na poziomie 1 autor umiejscowił w Centrum Wsparcia Teleinformatycznego Sił Powietrznych. Natomiast poziom 2 obsługiwany jest przez sąsiedni Węzeł Regionalny.

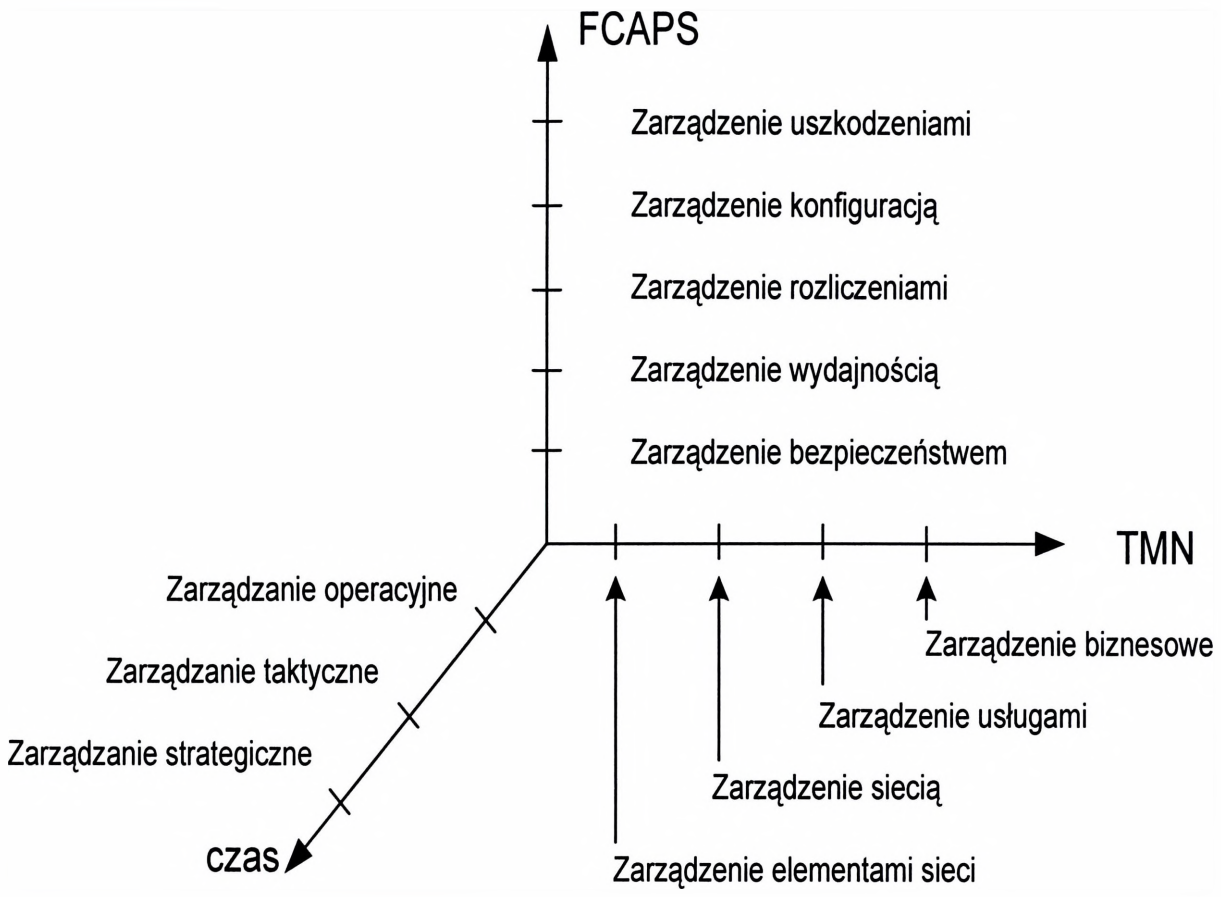
Przykładowy model zarządzania systemem teleinformatycznym obrazuje rysunek 6.5.

Dla tak zaprojektowanej topologii sieci teleinformatycznej (rys.6.3 i 6.4) w celu pełnej automatyzacji procesu zarządzania i integracji systemów zarządzania leży przyjęcie odpowiednich ogólnoświatowych standardów w dziedzinie zarządzania sieciami takich jak TMN.

W celu zobrazowania znaczenia zarządzania autor założył hipotetyczne uszkodzenie węzła komutacyjnego sieci. Po wykryciu uszkodzenia (zarządzanie uszkodzeniami) węzeł ten zostaje wyłączony z sieci, a ruch skierowany inną drogą (zarządzanie konfiguracją). Jednocześnie w sieci rozsyła się komunikat, że dane komutowane przez uszkodzony węzeł mogły ulec przekłamaniu (zarządzanie bezpieczeństwem) oraz, że opłaty za połączenia, które obsługiwał uszkodzony węzeł, mają zostać odpisane z kont użytkowników (zarządzanie rozliczeniami). Po naprawieniu uszkodzenia (zarządzanie uszkodzeniami) węzeł zostaje włączony do sieci (zarządzanie konfiguracją) oraz zostają przeprowadzone testy wydajności jego pracy (zarządzanie wydajnością).

Warstwowy model zarządzania teleinformatyką czyli podział na obszary funkcjonalne czy podział na zarządzanie operacyjne, taktyczne i strategiczne są wzajemnie powiązane i pozwalają z różnych stron spojrzeć na skomplikowaną dziedzinę, jaką jest zarządzanie siecią teleinformatyczną rys. 6.4. Zaproponowany model sieci teleinformatycznej wymaga kilku platform zarządzania siecią teleinformatyczną ze względu na rozwiązania sieci teleinformatycznej na dwóch poziomach oraz ze względu na zastosowanie, co najmniej dwóch typów urządzeń teletransmisyjnych. Wykaz platform zarządzania siecią teleinformatyczną :

- zarządzanie siecią szkieletową na poziomie 1 – STM -16;
- zarządzanie urządzeniami Cross-Connect na poziomie 1;
- zarządzanie siecią szkieletową na poziomie 2 – STM - 4;
- zarządzanie urządzeniami Cross-Connect na poziomie 2;



Rys. 6.6 *Zarządzanie siecią widziane z różnych perspektyw*
Źródło :Opracowanie własne

FCAPS – (ang. Fault, Configuration, Accounting, Performance,Security) – usterki, konfiguracja , rozliczenie, wydajność, bezpieczeństwo.

6.3 Działanie systemu w sytuacjach zagrożenia bezpieczeństwa państwa

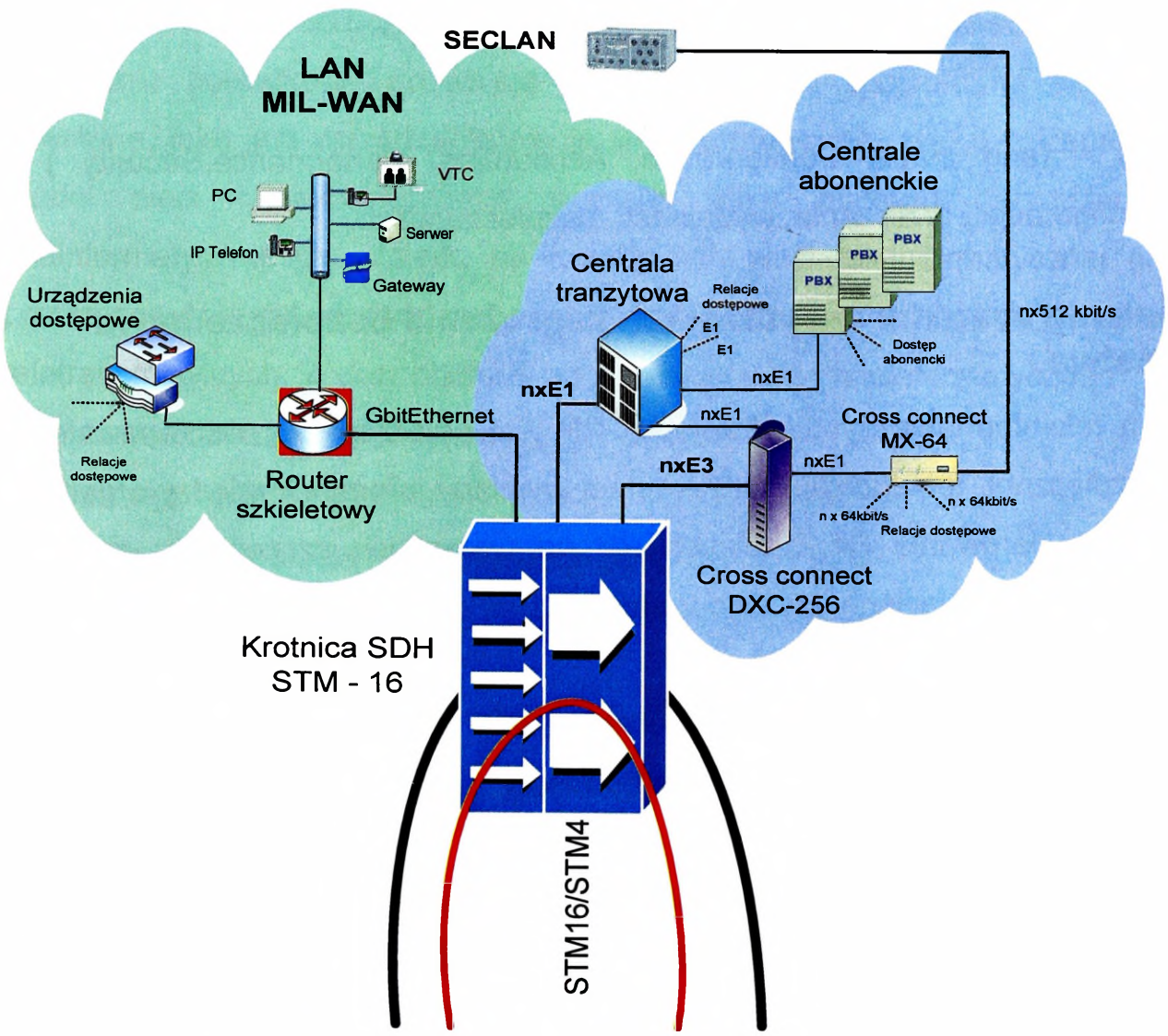
System teleinformatyczny Sił Zbrojnych RP jest przeznaczony do zapewnienia ciągłej, bezpiecznej, terminowej i niezawodnej wymiany informacji między organami dowodzenia i kierowania Sił Zbrojnych RP na wszystkich szczeblach, zarówno w czasie pokoju, sytuacjach kryzysowych, jak i w czasie zagrożenia militarnego państwa.

Zapewnia współdziałanie organów dowodzenia i kierowania Sił Zbrojnych RP z naczelnymi organami kierowania obronnością państwa, jednostkami układu pozamilitarnego oraz organami dowodzenia i kierowania Sojuszu Północnoatlantyckiego. Ponadto system powinien zapewnić wymianę informacji na potrzeby jednostek sił koalicyjnych czasowo przebywających na terenie Polski, a także jednostek Sił Zbrojnych RP poza terenem kraju. Gwarantuje on wymianę informacji przy pomocy środków technicznych.

W celu realizacji zadań system teleinformatyczny SZ RP jest organizacyjnie i technicznie powiązany z systemami różnych operatorów telekomunikacyjnych działającymi zarówno w Polsce, jak i za granicą.

W czasie pokoju zadanie zapewnienia łączności spoczywa na **systemie stacjonarnym**. W sytuacjach zagrożenia bezpieczeństwa państwa w czasie kryzysu lub wojny jest on uzupełniany - stosownie do potrzeb - **mobilnymi środkami jednostek dowodzenia i łączności**. W okresie zagrożenia bezpieczeństwa państwa warunki funkcjonowania systemu łączności ulegają radykalnym zmianom ze względu na to, że:

- może on stać się obiektem bezpośredniego ataku przeciwnika i tym samym mogą ulec znacznemu zmniejszeniu jego możliwości,
- wzrośnie obciążenie większości elementów i ogniw systemu, w czasie wojny bowiem nasila się proces informacyjny, wzrastają wymagania wobec tajności i sprawności pozyskiwania, przetwarzania i przekazywania informacji.



Rys. 6.7 *Przykładowa organizacja Węzła Regionalnego*
Źródło: opracowanie własne

W okresie zagrożenia bezpieczeństwa państwa kryzysami i zagrożeniami niemilitarnymi (ekologicznymi, społecznymi itp.) oraz wynikającymi z konfliktów polityczno - militarnych w sąsiedztwie Polski, system łączności i informatyki SZ RP będzie funkcjonował w zasadzie według reguł okresu pokojowego, przy czym dla doraźnych potrzeb organizacyjnych i w zależności od zaistniałej sytuacji może być rozbudowywany (uzupełniany) **środkami polowymi**. Aby przedstawione powyżej zadania mogły być realizowane każdy Węzeł Regionalny powinien być zorganizowany tak jak przedstawia to rysunek 6.7.

W celu realizacji procesu dowodzenia proponowane rozwiązanie kształtu węzła zapewnia możliwość elastycznej rozbudowy węzłów środkami polowymi w razie nagłej potrzeby. Przy projektowaniu węzła uwzględniono wszystkie potrzeby i wymogi jakie system stacjonarny musi spełnić w celu dynamicznej rozbudowy środkami polowymi włącznie ze specjalnymi przyłączami linowymi zapewniającymi przenoszenie interfejsu G703. Krotnica SDH i Cross Connecty poprzez szerokie możliwości oraz zaplanowaną nadmiarowość przepływności jest w stanie przyjąć wszystkie środki polowe zgodnie z organizacją wszystkich rodzajów węzłów.

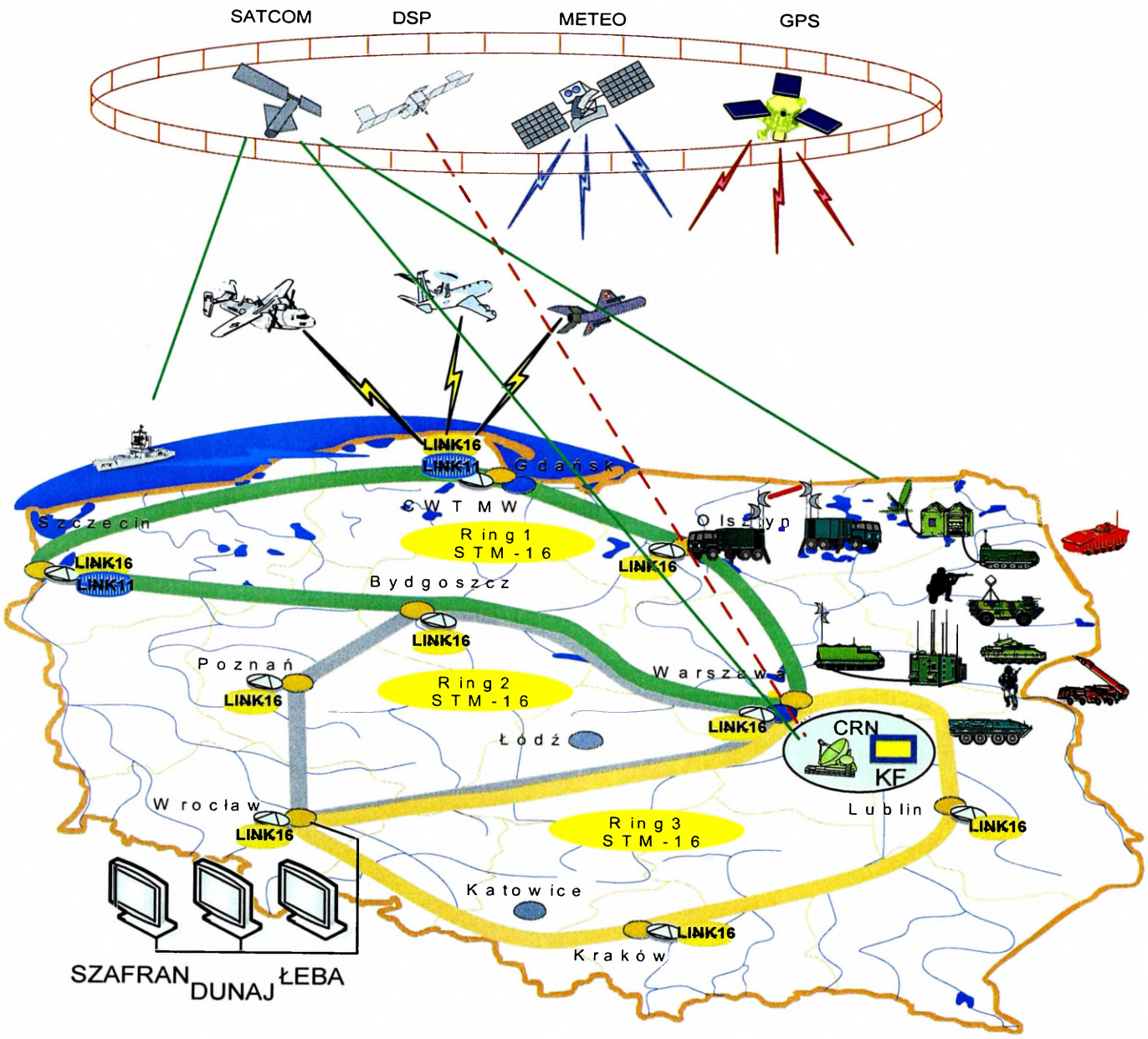
6.4 Synteza wyników badań

Przedstawiona organizacyjno – techniczna koncepcja sieci teleinformatycznej Sił Zbrojnych ukazała całe spektrum zagadnień związanych z problematyką stacjonarnej sieci teleinformatycznej dla potrzeb kierowania i dowodzenia Siłami Zbrojnymi RP. Z przeprowadzonej analizy literatury przedmiotu oraz dokumentów formalno – prawnych wynika że rozległa sieć teleinformatyczna oraz jej organizacja jest wstępem do organizacji sytemu dowodzenia. Jednocześnie jest to tylko jeden z elementów składający się na dobrze zorganizowany system dowodzenia. Reasumując powyższe można wnioskować, że bardzo ważnym elementem dowodzenia jest także komponent mobilny.

Elementy taktycznego cyfrowego systemu łączności, w powiązaniu ze stacjonarną siecią teleinformatyczną, zabezpieczają potrzeby w zakresie wymiany informacji dla wszystkich elementów ugrupowania, zarówno na szczeblu taktycznym jak i strategicznym.

Wymiana informacji oraz pozyskiwaniem niezbędnych informacji w czasie dowodzenia siłami zbrojnymi to jedno z zasadniczych wymagań na stacjonarną sieć

teleinformatyczną SZ RP. Autor podjął próbę przedstawienia sposobu pozyskiwania informacji zgodnie doktryną NCW.



Rys. 6.8 *Przykładowe zastosowanie rozległej sieci teleinformatycznych do zbierania informacji niezbędnych w procesie dowodzenia*
Źródło: opracowanie własne

Legenda:

GIG – Global Information Grid

SATCOM – Satellite Communication

DSP – Defence Support Program */Amerykańskie Satelity Wywiadowcze/*

METEO – Meteorological

GPS – Ground Positioning System

ISR – Intelligent Surveillance Reconnaissance

HUB – Koncentrator

UAV – Unmaned Aerial Vehicle

Walka sieciocentryczna (ang. Network Centric Warfare NCW)[77] jest definiowana jako „opierająca się na ***przewadze informacyjnej*** koncepcja prowadzenia operacji, według której wzrost siły bojowej jest generowany poprzez połączenie w sieć informacyjną sensorów, decydentów i systemów walki w celu osiągnięcia wspólnej świadomości, zwiększenia szybkości dowodzenia oraz tempa operacji, zwiększenia skuteczności uzbrojenia, wzrostu odporności na uderzenia przeciwnika oraz zwiększenia stopnia synchronizacji działań". NCW przekłada zatem przewagę informacyjną na zdolności bojowe poprzez efektywne łączenie na polu walki różnego typu jednostek organizacyjnych i wykorzystywanie ich wiedzy.

Doświadczenia z ostatnich konfliktów zbrojnych (w tym z wojny w Iraku) potwierdziły że, miliardowe inwestycje w systemy dowodzenia, wykrywania i śledzenia pozwoliły na efektywne wykorzystanie sił oraz na łączenie elementów pola walki i eliminowanie luk między nimi. W poprzednich działaniach, w ramach operacji połączonych, jednostki poszczególnych RSZ realizowały zadania raczej równolegle niż wspólnie.

Dzięki działaniom sieciocentrycznym wojska osiągają zdolności operacyjne, które można zdefiniować poprzez następujące elementy:

- wspólny obraz operacyjny (Common *Operational Picture/Joint Operational Picture - COP/JOP);*
- wspólne (współbieżne) planowanie *(collaborativeplanning);*
- oddziały Zadaniowe *(Mission-organized force elements);*
- działania ukierunkowane na efekt *(effect-based operations);*
- zwiększone tempo *(enhanced tempo).*

Rozwój systemu dowodzenia powinien uwzględniać założenia koncepcji „walki sieciocentrycznej", która wymaga jednoczesnego prowadzenia działań w domenach fizycznej, informacyjnej i decydowania.

Domenę fizyczną tworzy zdolność bojowa posiadanych sił i środków w połączeniu z zasadami sztuki operacyjnej. Obejmuje działania tradycyjne: uderzenia, obrona i manewr we wszystkich wymiarach (lądowym, morskim i powietrznym).

Głównymi parametrami oceny efektywności działań bojowych w tej domenie będą dwie zasadnicze miary zdolności bojowej: skuteczność rażenia i odporność (zdolność do przetrwania).

---

[77] Warsztaty strategicznego przeglądu obronnego WIŁ Zegrze 2005;

Domena informacyjna obejmuje tworzenie, przetwarzanie i współużytkowanie informacji. W domenie informacyjnej następuje wymiana informacji między siłami biorącymi udział w walce, komunikowanie się odpowiednich ośrodków dowodzenia i sztabów oraz przekazywanie decyzji dowódców.

Domena decydowania to domena umysłów walczących i wspomagającej ich narzędzi technicznych, a nawet socjologicznych. Tym samym zawiera bardzo niewymierne elementy, takie jak: umiejętność przewodzenia, morale, jedność oddziałów i pododdziałów, poziom wyszkolenia i doświadczenia, świadomość sytuacji, opinię publiczną itp.

Koncepcja wojny sieciocentrycznej może zostać zrealizowana tylko wtedy, gdy zostanie zbudowana odpowiednia **infrastruktura sieciowa**, tzw. Globalna Sieć Informacyjna (GIG - *Global Information Grid).* Głównym zadaniem GIG jest dostarczenie i udostępnienie infrastruktury technicznej w celu połączenia sił zbrojnych w jedną sieć. GIG dostarcza usługi w dziedzinie łączności, bezpieczeństwa, przetwarzania, zarządzania i dystrybucji informacji; umożliwia połączenia typu „każdy z każdym" oraz interoperacyjność poszczególnych komponentów połączonych sił zbrojnych -własnych i sojuszniczych.

W celu zabezpieczenia dowodzenia Sił Zbrojnych Rzeczypospolitej Polskiej planowany jest jednolity system sieciocentryczny, który zintegruje systemy dowodzenia i kierowania środkami walki funkcjonujące we wszystkich rodzajach sił zbrojnych na wszystkich szczeblach dowodzenia, począwszy od szczebla strategicznego.

Podstawą funkcjonowania systemu sieciocentrycznego będą:

- sieć teleinformatyczna SDH;
- łączność satelitarna;
- łączność transmisji danych LINK-16;
- łączność transmisji danych LINK-11
- łączność radioliniowa;
- łączność radiowa.

Jednolita sieć teleinformatyczna zapewni wymianę informacji na potrzeby zautomatyzowanych systemów dowodzenia wojskami oraz systemów identyfikacji bojowej i monitorowania położenia wojsk.

ZAKOŃCZENIE

W ramach niniejszej rozprawy autor przeprowadził badania teoretyczne i empiryczne na temat stacjonarnej sieci teleinformatycznej Sił Zbrojnych, próbując odpowiedzieć na wszystkie pytania problemowe, zawarte w rozdziale metodologicznym. Celem badań było wypracowanie, naukowo uzasadnionych, założeń organizacyjno – technicznych stacjonarnej sieci teleinformatycznej niezbędnej do zabezpieczenia procesu dowodzenia siłami zbrojnymi w okresie pokoju, kryzysu i zagrożenia militarnego państwa. Następnie na podstawie uzyskanych wyników badań należało określić, jakie należy podjąć niezbędne działania techniczno - organizacyjne, w celu osiągnięcia pełnej zdolności części stacjonarnej sieci teleinformatycznej do organizacji i eksploatacji wszystkich klas sieci na potrzeby dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej.

Pierwszy problem badawczy, a więc udzielenie odpowiedzi na następujące pytanie problemowe:

Jakie wymagania i potrzeby w zakresie usług teleinformatycznych generuje system dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej w czasie pokoju, kryzysu i zagrożenia militarnego państwa oraz jaka jest rola stacjonarnej sieci teleinformatycznej w realizacji zadań łączności w toku dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej, autor rozwiązał w rozdziale 2. niniejszej rozprawy.

Z przeprowadzonych badań wypływają następujące wnioski:

1. Organizacja stacjonarnej sieci teleinformatycznej jest priorytetowym elementem prawidłowego funkcjonowania całego systemu dowodzenia siłami zbrojnymi;
2. Aby system dowodzenia siłami zbrojnymi funkcjonował należycie sieć teleinformatyczna powinna sprostać odpowiednim wymaganiom;
3. Do roli stacjonarnej sieci teleinformatycznej należy zaliczyć następujące elementy składowe:
   - zapewnienie swobodnego, wielokierunkowego przepływu informacji pomiędzy wszystkimi elementami systemu dowodzenia;
   - zapewnienie przepływu informacji wewnątrz poszczególnych elementów systemu dowodzenia;
   - posiadanie w swojej strukturze interfejsów do współpracy z publicznymi stacjonarnymi i ruchomymi (mobilnymi) operatorami

telekomunikacyjnymi – umożliwienie użycia publicznych systemów teleinformatycznych dla potrzeb systemu wojskowego;

- zapewnienie warstwy transportowej dla systemów teleinformatycznych funkcjonujących na potrzeby procesu dowodzenia oraz wojskowych systemów mobilnych;
- dostarczanie narzędzi wspomagających proces dowodzenia (ZSyD, dedykowane sieci informatyczne);
- zapewnienie dostępu do wiarygodnych i aktualnych danych niezbędnych do zabezpieczenia procesu dowodzenia.

4. Należy brać pod uwagę możliwość wykorzystania infrastruktury operatorów telekomunikacyjnych, niezbędnej dla obronności państwa, należy mieć na uwadze planowanie, budowę oraz ciągłe utrzymywanie i modernizowanie spójnego i centralnie zarządzanego systemu teleinformatycznego. Powinien on stanowić integralną część **systemu kierowania bezpieczeństwem narodowym.**
5. Realizacja powyższych przedsięwzięć wynika z zakresu kompetencyjnego Ministra Obrony Narodowej, określonego w „Rozporządzeniu Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym".
6. Z uwagi na nieokreśloność i brak obiektywnych danych dotyczących organizacji systemów telekomunikacyjnych dla potrzeb obronności państwa – wynikających z nieokreślonego rodzaju zagrożenia oraz miejsca jego wystąpienia - nie jest możliwe określenie ich docelowej struktury organizacyjno – funkcjonalnej.
7. System teleinformatyczny powinien objąć obszar całego kraju. Wymaganie to powinno być realizowane etapami, począwszy od szczebla centralnego poprzez pośrednie szczeble kierowania do zapewnienia wojennego systemu dowodzenia SZ RP. Konieczne jest osiągnięcie stanu wyprzedzającego gotowość systemu teleinformatycznego w stosunku do systemu kierowania obroną państwa i działania wojsk.
8. Skład i struktura powinna odpowiadać składowi i strukturze systemu kierowania państwem w czasie pokoju, kryzysu i zagrożenia militarnego państwa oraz strukturze dowodzenia SZ RP, w tym powinny obejmować rejony stanowisk dowodzenia jednostek organizacyjnych SZ RP rozwijanych w DMP i ZMP.

9. Konfiguracja (rozmieszczenie) węzłów powinna być podatna na każdą zmianę systemu dowodzenia, nie powinna wymagać rekonfiguracji tego systemu.
10. W systemie powinny występować węzły o jednolitym przeznaczeniu, tzn. węzły końcowo-tranzytowe spełniające również funkcję węzłów dostępowych dla mobilnych środków łączności MON. Węzły stanowisk kierowania i dowodzenia w ZMP przeznaczone do wykorzystania w czasie wojny i w sytuacjach kryzysowych powinny być utrzymywane w pełnej gotowości do użycia.
11. Kontynuując poprzednią myśl w zakresie potrzeb, należy również wspomnieć, że na dzień dzisiejszy siły zbrojne nie dysponują odpowiednimi mediami do organizacji sieci teleinformatycznej zarówno stacjonarnej jak i polowej. Przedstawiona organizacja sieci teleinformatycznych na SD szczebla strategicznego wymaga dodatkowych urządzeń polowych takich jak: aparatownie troposferyczne, urządzenia satelitarne oraz dobrze zorganizowana stacjonarna sieć teleinformatyczna o odpowiedniej przepływności.
12. Niezbędne są następujące usługi telekomunikacyjne:
    - telefonia;
    - transmisja faksów;
    - telekonferencja dla wybranych grup użytkowników;
    - transmisja danych między użytkownikami;
    - wyszukiwanie informacji, w tym:
        - dostęp do centralnych baz danych,
        - dostęp do lokalnych baz danych,
        - dostęp do różnych zasobów danych z wykorzystaniem Internetu,
    - multimedia (w tym np. wideokonferencja);
    - inne (w tym np. szeroka gama usług sieci ISDN oraz usługi związane z tzw. sieciami inteligentnymi).

Drugi szczegółowy problem badawczy, tj. udzielenie odpowiedzi na pytanie problemowe: *„W jakim stopniu aktualne regulacje prawne określają zasady współpracy operatorów telekomunikacyjnych z Siłami Zbrojnymi oraz w jakim stopniu zmiany organizacyjno – techniczne w obszarze stacjonarnej sieci teleinformatycznej Sił Zbrojnych, podjęte w latach 1995 – 2005, wpłynęły na realizację potrzeb*

dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej w czasie pokoju, kryzysu i zagrożenia militarnego państwa?", został rozwiązany w rozdziale 3.

Należy stwierdzić, że na realizację procesu dowodzenia wpłynęły w następujący sposób:

1. Dokonano transformacji technologicznej stacjonarnego systemu teleinformatycznego z techniki analogowej na technikę cyfrową, dzięki czemu wzrosła dokładność oraz jakość przekazywanych danych.
2. Zwiększyła się sprawność i przepustowość systemów teleinformatycznych, co umożliwia zwiększenie ilości danych przetwarzanych w systemie dowodzenia.
3. Stworzono warunki do projektowania nowoczesnej, w pełni zarządzanej, jednolitej technologicznie struktury wojskowego stacjonarnego systemu teleinformatycznego, zdolnego do realizacji zadań systemu dowodzenia SZ RP w czasie pokoju, kryzysu i zagrożenia militarnego państwa.
4. Wdrożono w poszczególnych rodzajach Sił Zbrojnych Zautomatyzowane Systemy Dowodzenia, co z kolei usprawnia i unowocześnia system dowodzenia SZ RP.
5. W skutek wdrożenia nowoczesnych rozwiązań technologicznych stworzono możliwość do funkcjonowania struktur organizacyjnych, posiadających możliwości zdalnego zarządzania elementami stacjonarnej sieci teleinformatycznej.
6. Budowana struktura organizacyjna ewoluuje w kierunku powstawania elementów zarządzania, zapewniających sprawne planowanie i elastyczną rekonfigurację systemu, wymuszoną sytuacjami kryzysowymi lub działaniami wojennymi, znacznie zmniejsza ilość ogniw decyzyjnych oraz wykonawczych uczestniczących w procesie zapewnienia łączności.
7. Zmiany doktrynalne, organizacyjne i techniczne w obszarze jej funkcjonowania mają na celu zaspokojenie oczekiwań związanych z procesem dowodzenia SZ RP.

Przywoływane zmiany podyktowane są szeregiem czynników, z których najważniejsze to:

- konieczność działania w środowisku sojuszniczym i koalicyjnym (zobowiązania wobec NATO i Unii Europejskiej, udział SZ RP w międzynarodowych komponentach militarnych, udział w misjach pokojowych i stabilizacyjnych);

- potrzeba osiągnięcia zdolności sieciocentrycznej;
- osiągnięcie przewagi informacyjnej;
- dynamiczny rozwój dostępnych technologii teleinformatycznych oraz sytuacji geopolitycznej.

8. Podjęte przez resort obrony narodowej działania dążą do konstruowania modelu systemu telekomunikacyjnego uwzględniającego organizację i topologię spełniającą nowoczesne wymogi poszczególnych klas systemów dowodzenia, wynikających z zasad Net Centric Warfare (NCW), tzn.:
   - C4I2 (ang. Command, Control, Communication, Computers, Intelligence and Information) – sieć dowodzenia;
   - C2IS (ang. Command, Control, Information System) – sieć wspomagania dowodzenia;
   - C4ISR (ang. Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance) – sieć pozyskiwania i przetwarzania danych (sensorowa sieć rozpoznania).
9. Na podstawie analizy podjętych działań można również przyjąć tezę, że funkcjonująca stacjonarna sieć teleinformatyczna SZ RP jest systemem otwartym. W praktyce wiąże się to z procesem ciągłej weryfikacji i aktualizacji zasobów systemu oraz jego struktur organizacyjnych. Działania podejmowane w obecnej chwili na rzecz rozwoju sieci teleinformatycznej i tak są opóźnione w stosunku do nowych wyzwań jakie przynosi nam dynamiczny rozwój nowych technologii.
10. Zmiany technologiczne oraz coraz większe zapotrzebowanie użytkowników wojskowego systemu telekomunikacyjnego na nowoczesne usługi teleinformatyczne, wymusza modelowanie systemu w kierunku osadzenia go w publicznej przestrzeni telekomunikacyjnej, z zastrzeżeniem pełnego zdefiniowania charakteru resortowej sieci telekomunikacyjnej.
11. Na szczeblu strategicznym łączność w całości organizowana jest w oparciu o system stacjonarny. Dotyczy to zarówno węzłów łączności obsługujących stanowiska dowodzenia, jak również powiązań teleinformatycznych. W czasie kryzysu i zagrożenia militarnego państwa stacjonarny system będzie wzmacniany potencjałem z zasobów komercyjnych operatorów telekomunikacyjnych.

12. Reorganizacja organów zarządzających systemem telekomunikacyjnym SZ RP oraz elementów tworzących stacjonarną sieć teleinformatyczną SZ RP przeprowadzona w roku 2007, w znaczący sposób uelastycznia funkcjonowanie stacjonarnego systemu teleinformatycznego w wymuszonych sytuacjach kryzysowych lub działaniach wojennych.
13. Istotną zmianą jest odejście od ścisłego powiązania rozmieszczenia elementów systemu stacjonarnego ze strukturami organizacyjnymi SZ RP na rzecz uwarunkowań geograficznych. Powyższa zmiana zapewnia możliwość rekonfigurowania systemu dowodzenia bez konieczności modyfikowania systemu łączności oraz ma zapewnić równomierne nasycenie elementami systemu całego obszaru Polski.
14. Stworzenie jednolitych struktur organizacyjno-technicznych Rejonowych Węzłów Łączności oraz utrzymywanie ich w pełnej gotowości do użycia, zabezpiecza i podnosi skuteczność funkcjonowania rozwijanych w ZMP stanowisk dowodzenia i kierowania.
15. Przyjęta struktura organizacyjna organów kierujących i zarządzających stacjonarną siecią teleinformatyczną rozdziela kompetencje w tym zakresie pomiędzy:
    - Departament Informatyki i Telekomunikacji MON - obszar związany z techniczną eksploatacją, implementacją i rozwojem stacjonarnej sieci teleinformatycznej SZ RP.
    - Zarząd Planowania Systemów Dowodzenia i Łączności P-6 – obszar związany z planowaniem organizacji i funkcjonowania systemów teleinformatycznych funkcjonujących w ramach WSyD.

Obszarem wspólnych działań obydwu komórek organizujących Wojskowy System Telekomunikacyjny jest działalność w zakresie budowy modelowego systemu teleinformatycznego. Szczegółowe kompetencje zarządzania stacjonarnym systemem teleinformatycznym SZ RP skupione zostały w jednym punkcie – Centrum Zarządzania Systemami Teleinformatycznymi (CZST), gdzie zaplanowano narzędzia umożliwiające działania związane ze sterowaniem, monitorowaniem i rejestrowaniem użycia zasobów sieci, w celu zapewnienia jej efektywnego wykorzystania, zgodnie z przeznaczeniem i adaptacją do warunków występujących w jej otoczeniu.

Po przeprowadzeniu analizy przedstawionych aktów prawnych, należy stwierdzić, że odpowiedzialnym za przygotowanie i utrzymanie zapasowych stanowisk kierowania dla: Prezydenta Rzeczypospolitej Polskiej, Prezesa Rady Ministrów oraz ministrów i centralnych organów administracji rządowej (wskazanych przez Prezesa Rady Ministrów) jest **Minister Obrony Narodowej**.

Z racji odpowiedzialności Ministra Obrony Narodowej za przygotowanie i utrzymanie zapasowych stanowisk kierowania dla wskazanych organów władzy publicznej, wynika fakt przygotowania i utrzymania wewnętrznych sieci teleinformatycznych danego stanowiska kierowania.

Kolejny szczegółowy problem badawczy, czyli udzielenie odpowiedzi na pytanie: *Jakie zagrożenia i czynniki wpływają na funkcjonowanie stacjonarnej sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej?,* został rozwiązany w kolejnym 4. rozdziale.

Rozwiązanie tego problemu badawczego doprowadziło do stwierdzenia, że podziału czynników powodujących zagrożenia dla bezpieczeństwa sieci teleinformatycznych można dokonywać w wielu aspektach i płaszczyznach.

W świetle przeprowadzonych analiz oraz wyników badań można uznać, że poprawne funkcjonowanie sieci teleinformatycznej Sił Zbrojnych jest uzależnione od czynników ściśle związanych z technologią oraz fizycznym lub cyberprzestrzennym naruszeniem strefy bezpieczeństwa. Ponieważ system teleinformatyczny Sił Zbrojnych RP jest wykorzystywany przez użytkowników przede wszystkim wojskowych zarówno w czasie pokoju, kryzysu oraz wojny, można oczekiwać dużego zainteresowania tymi obiektami ze strony potencjalnych przeciwników. Stąd też należy zakładać, że systemy teleinformatyczne mogą być jednym z głównych celów potencjalnego ataku. Poprawne funkcjonowanie systemu teleinformatycznego może zostać zakłócone przez czynniki typowo militarne:

- oddziaływanie walki elektronicznej, która może mieć wpływ na wszystkie sieci i systemy telekomunikacyjne. Dodatkowym zagrożeniem mogą być ataki na elementy systemów satelitarnych znajdujące się na ziemi i w przestrzeni kosmicznej;
- broni konwencjonalnej, która może być bardzo skuteczna przeciwko wszelkim rodzajom instalacji telekomunikacyjnych;

- broni chemicznej i biologicznej, powodującej szczególne zagrożenie, ponieważ jest przeznaczona do niszczenia wybranych materiałów, terenów lub zabijania grup ludzi;
- broni jądrowej, która może mieć wieloraki wpływ na systemy łączności.

Czynniki mające wpływ na zagrożenia są podstawą do opracowania strategii bezpieczeństwa systemów teleinformatycznych, właściwy poziom akceptowalnego ryzyka, a co za tym idzie odpowiedni poziom bezpieczeństwa jest wykładnią do skutecznego zarządzania bezpieczeństwem.

Zabezpieczenie zasobów informacyjnych oraz systemów teleinformatycznych wymaga nie tylko implementacji i zarządzania środkami bezpieczeństwa, ale również powinna zapewnić możliwość skutecznego i szybkiego reagowania na incydenty zewnętrzne z bezpieczeństwem komputerowym, takie jak nieautoryzowane ingerencje, ataki kodów złośliwych i wirusów komputerowych. Potencjalny przeciwnik może zadać poważne straty bez użycia tradycyjnych sposobów walki, czyli użycia konwencjonalnej broni, czy w końcu mało prawdopodobnego użycia BMR, oraz narażenia na straty własnych sił i środków. Oddziaływając tylko na systemy dowodzenia i zarządzania, przeciwnik może obezwładnić a nawet zniszczyć istotne elementy obronnej infrastruktury wojskowej i cywilnej. Walka informacyjna i cyberterroryzm stają się realnym zagrożeniem dla bezpieczeństwa narodowego. W poszukiwaniu sposobów ochrony, niezbędnym jest gromadzenie wiedzy o stanie otoczenia i rodzących się przesłankach zagrożeń, które z natury rzeczy będą utrzymywane przez zainteresowanego w jak największej tajemnicy. Zapewnienie bezpieczeństwa państwa w aspekcie zewnętrznym i wewnętrznym jest podstawowym obowiązkiem wszystkich szczebli zarządzania i kierowania państwem. Potrzeba ta wynika zarówno z uwarunkowań wewnętrznych, jak również z ewolucji otoczenia zewnętrznego. W obu tych obszarach powstają wyzwania i zagrożenia dla społeczeństwa i państwa. Zbieranie informacji o zagrożeniach prowadzą różne organizacje i instytucje posiadające odpowiednie siły i środki do ich wykrywania, likwidacji i zapobiegania. Brak systemu wczesnego ostrzegania może doprowadzić do szkodliwych zmian w środowisku, a w przypadku rozwoju zagrożenia na większą skalę, do powstania sytuacji kryzysowych.

Odpowiedź na pytanie: *Jakie współczesne urządzenia i technologie teleinformatyczne są możliwe do zastosowania w stacjonarnej sieci*

teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej aby mogła sprawniej spełniać stawiane przed nią zadania łączności?, zamieszczono w rozdziale 5.

1. Biorąc pod uwagę wymagania dla systemu dowodzenia w czasie pokoju, kryzysu i zagrożenia militarnego, możemy założyć, że przepływność sieci teleinformatycznej o wartości 1Gbit/s powinna zabezpieczyć, pełne wykorzystanie możliwości technicznych urządzeń mobilnych.
2. We wszystkich przypadkach Regionalne Węzły Łączności dzierżawią od operatorów publicznych trakty o przepływności 2Mbit/s, co w żaden sposób nie zabezpiecza potrzeb związanych z organizacją sieci teleinformatycznych na Stanowisku Dowodzenia szczebla strategicznego.
3. W celu zapewnienia skutecznej realizacji procesu dowodzenia w czasie pokoju, kryzysu i zagrożenia militarnego na Stanowisku Dowodzenia powinny być zorganizowane następujące sieci teleinformatyczne :
   - sieć ZASTRZEŻONA MIL-LAN ,w której osadzone będą Zintegrowane systemy Dowodzenia SZAFRAN, DUNAJ, ŁEBA;
   - sieć NATO SECRET PL_NOAN, MCCIS, ICC;
   - sieć TAJNA SEC-LAN (po wdrożeniu do SZ RP);
   - sieć JAWNA Internet.
5. Z punktu widzenia organizacji systemu teleinformatycznego na poziomie strategicznym najlepszymi możliwymi do wykorzystania urządzeniami są krotnice SDH oraz Cross Connect.

Ostatni szczegółowy problem badawczy a więc udzielenie odpowiedzi na pytanie: *Jaka powinna być struktura organizacyjno – techniczna stacjonarnej sieci teleinformatycznej aby mogła zapewnić świadczenie podstawowych usług teleinformatycznych w procesie dowodzenia Siłami Zbrojnymi ?, został określony w rozdziale 6.*

Rozwiązanie tego problemu badawczego doprowadziło do przekonania, że obecna struktura organizacyjno – techniczna nie jest w stanie zapewnić odpowiednich warunków dla systemu dowodzenia ze szczególnym wskazaniem na okres zagrożenia militarnego państwa w czasie organizacji stanowisk dowodzenia, a więc potrzeb podmiotów systemu na usługi telekomunikacyjne, wynikających z więzi informacyjnych procesu dowodzenia, które autor przedstawił w rozdziale 2.

Rozległa sieć teleinformatyczna oraz jej organizacja jest podstawą do organizacji sytemu dowodzenia. Bardzo ważnym elementem dowodzenia jest także komponent mobilny, dlatego w ramach prowadzonych od wielu lat prac badawczo-rozwojowych zaprojektowano od podstaw w sposób kompleksowy taktyczny cyfrowy system łączności, który został przebadany w warunkach poligonowych i aktualnie jest wdrażany do Sił Zbrojnych RP. Jest on nowoczesnym systemem odpowiadającym aktualnym standardom światowym. Został zbudowany w oparciu o urządzenia oraz obiekty mobilne (polowe aparatownie łączności).

Elementy taktycznego cyfrowego systemu łączności, w powiązaniu ze stacjonarną siecią teleinformatyczną, powinny zabezpieczyć potrzeby w zakresie wymiany informacji dla wszystkich elementów ugrupowania, zarówno na szczeblu taktycznym jak i strategicznym, umożliwiając automatyczne zestawianie połączeń (z komutacją kanałów i pakietów) we wszystkich relacjach dowodzenia i współdziałania oraz wymianę utajnionych informacji (fonicznych, danych, tekstowych, wolnozmiennych obrazów) pomiędzy jego użytkownikami.

System powinien być wyposażony w obiekty pozwalające tworzyć polową (radioliniowo-przewodową) infrastrukturę telekomunikacyjną na obszarze działań. Jej głównym elementem powinna być obszarowa sieć łączności, której podstawowa funkcja powinna polegać na obsłudze skoncentrowanego ruchu telekomunikacyjnego (wychodzącego i przychodzącego) od/do węzłów łączności stanowisk dowodzenia. Powinna zapewnić realizację automatycznych połączeń telekomunikacyjnych po trasach alternatywnego wyboru, dla wszystkich użytkowników systemu dowodzenia. Stanowi ona również bazę komutacyjno-teletransmisyjną dla innych użytkowników i podsystemów, w tym dla:

- podsystemu łączności radiowej,
- podsystemów zautomatyzowanego dowodzenia,
- podsystemów zautomatyzowanego kierowania środkami walki (systemami broni).

Obszarowa sieć łączności powinna być rozwijana w oparciu o powiązane ze sobą (fizycznie i logicznie), według określonego planu: pomocnicze węzły łączności, wielokanałowe, cyfrowe linie międzywęzłowe oraz linie dowiązania do innych systemów telekomunikacyjnych (w tym interfejsowe linie międzysystemowe).

W sensie technicznym, taktyczny cyfrowy system łączności powinien stanowić zestaw polowych węzłów łączności zbudowanych z mobilnych obiektów, powiązanych ze sobą polowymi międzywęzłowymi liniami łączności.

Rozwiązanie tych problemów stanowiło finalną próbę głównego problemu badawczego, którego treść jest następująca: ***„Czy obecna struktura organizacyjno – techniczna stacjonarnej sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej, zabezpiecza potrzeby na usługi teleinformatyczne wynikające z procesu dowodzenia wojskami w czasie pokoju, kryzysu i zagrożenia militarnego państwa, a jeżeli nie, to jaka powinna ona być?"***

Efektem końcowym przeprowadzonych badań było wypracowanie *autorskiej koncepcji struktury organizacyjno-technicznej sieci teleinformatycznej, zapewniającej realizację świadczenia podstawowych usług teleinformatycznych w procesie dowodzenia wojskami w czasie pokoju, kryzysu i zagrożenia militarnego państwa.*

Wnioski jakie nasunęły się w wyniku rozwiązywania problemów szczegółowych i głównego problemu badawczego są następujące.

Przyjęta struktura organizacyjna organów kierujących i zarządzających stacjonarną siecią teleinformatyczną rozdziela kompetencje na dwa podmioty:

- Departament Informatyki i Telekomunikacji MON - obszar związany z techniczną eksploatacją, implementacją i rozwojem stacjonarnej sieci teleinformatycznej SZ RP;
- Zarząd Planowania Systemów Dowodzenia i Łączności P-6 – obszar związany z planowaniem organizacji i funkcjonowania systemów teleinformatycznych funkcjonujących w ramach WSyD.

Obszarem wspólnych działań obydwu komórek organizujących Wojskowy System Telekomunikacyjny jest budowa modelowego systemu teleinformatycznego. Szczegółowe kompetencje zarządzania stacjonarnym systemem teleinformatycznym SZ RP skupione zostały w jednym punkcie – Centrum Zarządzania Systemami Teleinformatycznymi (CZST), gdzie zaplanowano narzędzia umożliwiające działania związane ze sterowaniem, monitorowaniem i rejestrowaniem użycia zasobów sieci, w celu zapewnienia jej efektywnego wykorzystania zgodnie z przeznaczeniem i adaptacją do warunków występujących w jej otoczeniu.

Reorganizacja organów zarządzających systemem telekomunikacyjnym SZ RP oraz elementów tworzących stacjonarną sieć teleinformatyczną SZ RP przeprowadzona w roku 2007, w znaczący sposób uelastycznia funkcjonowanie

stacjonarnego systemu teleinformatycznego w wymuszonych sytuacjach kryzysowych lub działaniach wojennych.

Istotną zmianą jest odejście od ścisłego powiązania rozmieszczenia elementów systemu stacjonarnego ze strukturami organizacyjnymi SZ RP na rzecz uwarunkowań geograficznych. Powyższa zmiana zapewnia możliwość rekonfigurowania systemu dowodzenia bez konieczności modyfikowania systemu łączności oraz ma zapewnić równomierne nasycenie elementami systemu całego obszaru Polski.

Pomimo podjęcia szeregu decyzji organizacyjnych wpływających na kształt struktury oraz organizacji stacjonarnego systemu teleinformatycznego SZ RP daje się zauważyć coraz większy dystans i rozdźwięk pomiędzy funkcjonowaniem nowoutworzonej struktury a zbiorem aktualnie obowiązujących zasad świadczenia usług przez publicznych operatorów telekomunikacyjnych na rzecz systemu wojskowego.

Powyższa teza nie oznacza jednak „totalnego chaosu" organizacyjnego, ma podkreślać jednak pogłębiającą się dysharmonię pomiędzy faktycznymi oczekiwaniami stacjonarnego systemu teleinformatycznego w zakresie jego uzupełnienia (wsparcia) przez operatorów publicznych w czasie pokoju, kryzysu i zagrożenia militarnego.

W ostatnich latach dokonano transformacji technologicznej stacjonarnego systemu teleinformatycznego z techniki analogowej na technikę cyfrową, dzięki czemu wzrosła dokładność oraz jakość przekazywanych danych, zwiększyła się również sprawność i przepustowość systemów teleinformatycznych, co umożliwia zwiększenie ilości danych przetwarzanych w systemie dowodzenia.

Stworzono warunki do projektowania nowoczesnej w pełni zarządzanej jednolitej technologicznie struktury wojskowego stacjonarnego systemu teleinformatycznego, zdolnego do realizacji zadań systemu dowodzenia SZ RP w czasie pokoju, kryzysu i zagrożenia militarnego państwa. Jednak z uwagi na nieokreśloność i brak obiektywnych danych dotyczących organizacji systemów telekomunikacyjnych dla potrzeb obronności państwa – wynikających z nieokreślonego rodzaju zagrożenia oraz miejsca jego wystąpienia – nie jest możliwe określenie ich docelowej struktury organizacyjno – technicznej, biorąc pod uwagę powyższe w systemie powinny występować węzły o jednolitym przeznaczeniu, tzn. węzły końcowo-tranzytowe spełniające również funkcję węzłów dostępowych dla mobilnych środków łączności

MON. Węzły stanowisk kierowania i dowodzenia w ZMP przeznaczone do wykorzystania w czasie wojny i w sytuacjach kryzysowych powinny być utrzymywane w pełnej gotowości do użycia.

Kontynuując poprzednią myśl w zakresie potrzeb należy także wspomnieć, że aktualnie siły zbrojne nie dysponują odpowiednimi mediami do organizacji sieci teleinformatycznej, zarówno stacjonarnej jak i polowej. Przedstawiona organizacja sieci teleinformatycznych na SD szczebla strategicznego wymaga dodatkowych urządzeń polowych takich jak: aparatownie troposferyczne, urządzenia satelitarne oraz dobrze zorganizowana stacjonarna sieć teleinformatyczna o odpowiedniej przepływności.

System teleinformatyczny powinien objąć obszar całego kraju, wymaganie to powinno być realizowane etapami, począwszy od szczebla centralnego poprzez pośrednie szczeble kierowania do zapewnienia wojennego systemu dowodzenia SZ RP. Konieczne jest osiągnięcie stanu wyprzedzającego gotowość systemu teleinformatycznego w stosunku do systemu kierowania obroną państwa i działania wojsk.

Na podstawie analizy podjętych działań można również przyjąć tezę, że funkcjonująca stacjonarna sieć teleinformatyczna SZ RP jest systemem otwartym. W praktyce wiąże się to z procesem ciągłej weryfikacji i aktualizacji zasobów systemu oraz jego struktur organizacyjnych, a także ciągłym zwiększaniem bezpieczeństwa. Zabezpieczenie zasobów informacyjnych oraz systemów teleinformatycznych wymaga nie tylko implementacji i zarządzania środkami bezpieczeństwa, powinno również zapewnić możliwość skutecznego i szybkiego reagowania na incydenty zewnętrzne z bezpieczeństwem komputerowym, takie jak nieautoryzowane ingerencje, ataki kodów złośliwych i wirusów komputerowych.

Działania podejmowane na rzecz rozwoju sieci teleinformatycznej w obecnej chwili i tak są opóźnione w stosunku do nowych wyzwań jakie nam przynosi dynamiczny rozwój nowych technologii.

Biorąc pod uwagę wymagania dla systemu dowodzenia w czasie pokoju, kryzysu i zagrożenia militarnego możemy założyć, że przepływność sieci teleinformatycznej o wartości przekraczającej 1Gbit/s, powinna zabezpieczyć pełne wykorzystanie możliwości technicznych urządzeń mobilnych. W związku z tym z punktu widzenia organizacji systemu teleinformatycznego na poziomie strategicznym najlepszymi możliwymi do użytku urządzeniami są krotnice SDH i Cross Connect.

W obecnej chwili we wszystkich przypadkach Regionalne Węzły Łączności dzierżawią od operatorów publicznych trakty o przepływności 2Mbit/s, co w żaden sposób nie zabezpiecza potrzeb związanych z organizacją sieci teleinformatycznych na Stanowisku Dowodzenia szczebla strategicznego. Analizując powyższe można stwierdzić, że ***obecna struktura organizacyjno – techniczna stacjonarnej sieci teleinformatycznej Sił Zbrojnych Rzeczypospolitej Polskiej, zabezpiecza potrzeby w zakresie usług teleinformatycznych wynikających z procesu dowodzenia wojskami w czasie pokoju i kryzysu, ale w ograniczonym zakresie, co spowodowane jest ograniczoną przepływnością łączy. W okresie zagrożenia militarnego państwa sieć teleinformatyczna nie zabezpiecza potrzeb w zakresie usług teleinformatycznych, co spowodowane jest brakiem odpowiednich interfejsów na węzłach regionalnych, ograniczoną przepływnością łączy oraz niemożnością dynamicznego rekonfigurowania systemów polowych w miejscach występowania zagrożeń***.

Uwieńczeniem powyższej dysertacji w toku prowadzonych badań naukowych jest autorska koncepcja struktury organizacyjno-technicznej sieci teleinformatycznej, zapewniająca realizację świadczenia podstawowych usług teleinformatycznych w procesie dowodzenia wojskami w czasie pokoju, kryzysu i zagrożenia militarnego państwa.

Zaproponowane rozwiązanie struktury organizacyjno-technicznej sieci teleinformatycznej powinno w zasadniczy sposób zniwelować czynniki wpływające negatywnie na realizację świadczenia podstawowych usług teleinformatycznych w procesie dowodzenia wojskami w czasie pokoju, kryzysu i zagrożenia militarnego państwa.

Wynika z tego, że cel badań jaki przyświecał autorowi w momencie rozpoczęcia procesu badawczego został w sposób zadawalający osiągnięty. Czyli postawiona w początkowej fazie badań ***hipoteza robocza została zweryfikowana pozytywnie***.

WYKAZ RYSUNKÓW I TABEL

BIBLIOGRAFIA

A B C D E F G H I J K L M N O P R S T U W Z

LITERATURA PRZEDMIOTU

1. Barczak A. i in. "*Planowanie systemu łączności*", Bellona, Warszawa 1999.
2. Barjasz W. "*Normalizacja systemów transmisyjnych*", Przegląd Telekomunikacyjny nr 5, Warszawa 1993.
3. Bielski M., „*Organizacje: istota, struktury, procesy*", Uniwersytet Łódzki, Łódź 1997.
4. Bógdoł-Brzezinska A.., Florian Gawrycki M.,„*Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*", Warszawa 2003.
5. Czarnecki P., Jajszczyk A., Lubacz J., „*Standardy zarządzania sieciami OSI/NM, TMN, WEFP*", Poznań 1995.
6. Bojarski R., „*Operacja obronna*", AON, Warszawa 1999.
7. Dudek Z.T., Zagrobelny T., „*Ewolucja sieci telekomunikacyjnych od analogowych do szerokopasmowych*", Przegląd Telekomunikacyjny
8. nr 6, Warszawa 1992.
9. Griffin R.W., „*Podstawy zarządzania organizacjami*", PWN, Warszawa 1999.
10. Janczak J. i in., „*Mobilne sieci łączności*", AON, Warszawa 2003.
11. Janczak J. i in., „*Środki dowodzenia*, AON", Warszawa 2003.
12. Janczak J., „*Właściwości organizacji łączności w specyficznych środowiskach i warunkach walki*", AON, Warszawa 2004.
13. Janczak J., Świdzikowski G., „*Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*", AON, Warszawa 2004.
14. Jajszczyk A., Roszkiewicz M., „*Węzły komutacji w sieciach szerokopasmowych ATM*", POLMAN'95, Poznań 1995.
15. Knetki J., Wołejszo J., „*Więzi informacyjne stanowisk dowodzenia szczebla taktycznego wojsk lądowych SZ RP*", AON, Warszawa 2002.
16. Kitler W., „*Wybrane aspekty kierowania państwem w sytuacjach kryzysowych w obronie narodowej RP wobec wyzwań i zagrożeń współczesności*", AON, Warszawa 1999.

17. Kościelnik D., „*ISDN Cyfrowe sieci zintegrowane usługowo”*, WKŁ 1997.
18. *Kompendium CCPC, NATO.*
19. Piątek Z., „*Świadczenia na rzecz obrony realizowane w sytuacjach kryzysowych”*, Ruch Wspólnot Obronnych, Warszawa 2006.
20. Praca zbiorowa, „Mobilne sieci łączności – album schematów”, AON, Warszawa 2003.
21. Krasuski A., „*Prawo telekomunikacyjne – komentarz”*, Lexis Nexis, Warszawa 2005
22. Wołejszo J., „*Wybrane aspekty projektowania struktur organizacyjno-funkcjonalnych ośrodków decyzyjnych”*, AON, Warszawa 2002.
23. Stachowiak Z., „*Metodyka i metodologia pisania prac kwalifikacyjnych”*, AON, Warszawa 2001.
24. Piedziuk E., „*Słownik pojęć z zakresu telekomunikacji”*
25. Nowicki W., „*Glosarium telekomunikacji, zalecane terminy, ich definicje, odpowiedniki obcojęzyczne, komentarze”*, z. 2, „Biuletyn informacyjny” nr 2–3 (276–277) IŁ, Warszawa – Miedzeszyn, 1990.
26. „Materiały konferencji Instytutu Zarządzania i Dowodzenia, Łączność w operacjach reagowania kryzysowego”, AON, Warszawa 2003.
27. „Materiały konferencji Zakładu Systemów Łączności i Informatyki, Łączność w sytuacjach w kryzysowych o charakterze niemilitarnym na obszarze kraju”, AON, Warszawa, 2004.
28. „Materiały konferencji międzynarodowej konferencji naukowej, Sieci teleinformatyczne w działaniach sieciocentrycznych”, AON, Warszawa 2007.
29. Michniak J., Wołejszo J., „*Determinanty skutecznego organizowania struktur dowództw* cz. III. *Transformacja dowództwa szczebla operacyjnego na stanowiska dowodzenia”*, AON, Warszawa 2002.
30. Michniak J., „*Dowodzenie i łączność”*, AON, Warszawa 2003.
31. Michniak J., „*Dowodzenie w operacjach antykryzysowych i połączonych”*, AON, Warszawa 2005.
32. Michniak J., „*Dowodzenie w teorii i praktyce wojsk”*, AON, Warszawa 2003.
33. Michniak J., „*Kierowanie mobilnymi systemami łączności wojsk lądowych”*, cz. I. *Główne problemy*, AON, Warszawa 2002.
34. Michniak J., „*Kompendium łączności”,* AON, Warszawa 1994.

35. Michniak J., Fiołna Z., *„Sieć łączności państwa”*, AON, Warszawa 2001.
36. Mazurkiewicz J.W., *„Leksykon łączności wojskowej”*, AON, Warszawa 1996.
37. Majewski T., *„Ankieta i wywiad w badaniach wojskowych”*, AON, Warszawa 2002.
38. Majewski T., *„Etapy projektowania struktur organizacyjnych”*, AON, Warszawa 2004.
39. *„Mobilne sieci łączności – album schematów”,* Praca zbiorowa pod kierunkiem płk dr hab. inż. Józefa Janczaka, Warszawa 2003.
40. Norris Mark, *„Teleinformatyka”*, WKŁ , Warszawa 2002.
41. ppłk Fiołna Z. *,,Podsystem łączności w systemie kierowania reagowaniem kryzysowym”*
42. Sienkiewicz P., *„Metodyka zastosowania współczynników jakości w kalkulacjach operacyjno-taktycznych”,* AON, Warszawa 1993.
43. *„Sieci teleinformatyczne w działaniach sieciocentrycznych – materiały z międzynarodowej konferencji naukowej*”. Redakcją naukową płk dr hab. inż. Józef Janczak, ppłk dr inż. Andrzej Wisz, Warszawa 2007.
44. *„Secure 2003” VII Konferencja bezpieczeństwa IT pod patronatem Ministra Nauki Michała Klebera,* Warszawa 2003.
45. *„Secure 2004” VIII Konferencja bezpieczeństwa IT,* Warszawa 2004.
46. *„Secure 2005” IX Konferencja bezpieczeństwa IT,* Warszawa 2005.
47. *„Technika informatyczne – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych”* , Raport Techniczny 1998.
48. *„Technika informatyczna- Praktyczne zasady zarządzania bezpieczeństwem informacji”, Polska Norma,* Warszawa 2003.
49. Wojnarowski J., *„System obronności państwa”*, AON, Warszawa 2005.

S/7246

Czyt. Rozprawa elektorska