SZTAB GENERALNY WP

AKADEMIA

OBRONY NARODOWEJ

KIEROWANIE OBRONNOŚCIĄ PAŃSTWA W ASPEKCIE WYKORZYSTANIA TECHNICZNYCH ŚRODKÓW NAJNOWSZEJ GENERACJI

Materiały z konferencji naukowej przeprowadzonej w Centrum Konferencyjnym WP w dniach 19÷20 grudnia 2001 roku

WARSZAWA Grudzień

SZTAB GENERALNY WP

AKADEMIA
OBRONY NARODOWEJ

KIEROWANIE OBRONNOŚCIĄ PAŃSTWA W ASPEKCIE WYKORZYSTANIA TECHNICZNYCH ŚRODKÓW NAJNOWSZEJ GENERACJI

Materiały z konferencji naukowej przeprowadzonej w Centrum Konferencyjnym WP w dniach 19÷20 grudnia 2001 roku

WARSZAWA Grudzień 2001

Konferencja
„Kierowanie obronnością państwa w aspekcie wykorzystania technicznych środków najnowszej generacji"
pod patronatem
MINISTRA OBRONY NARODOWEJ

RADA PROGRAMOWA KONFERENCJI

gen. bryg. prof. dr hab. Michał KRAUZE – przewodniczący rady programowej

gen. dyw. Lech KONOPKA – z-ca przewodniczącego

płk rez. dr inż. Eugeniusz PIEDZIUK – sekretarz

płk dr inż. Stanisław KRYSIŃSKI

gen. bryg. dr Julian MAJ

płk mgr inż. Roman PAŁKA

płk dr hab. Jacek PAWŁOWSKI

płk mgr inż. Marian PŁAWIAK

płk dr hab. inż. Grzegorz RÓŻAŃSKI

płk dr hab. Ryszard STĘPIEŃ

płk dr inż. Zbigniew TADEUSIAK

gen. bryg. dr inż. Wojciech WOJCIECHOWSKI

KOMITET ORGANIZACYJNY KONFERENCJI

płk rez. dr inż. Eugeniusz PIEDZIUK – przewodniczący

mgr inż. Jerzy JAKUBOWSKI - z-ca przewodniczącego

mgr Urszula JARASZEK – sekretarz

kpt. mgr inż. Jan SOŁYGA

por. mgr inż. Stanisław KAŁAMARZ

por. mgr inż. Grzegorz NAZAREWICZ

por. rez. mgr inż. Wojciech BURDECKI

mgr inż. Andrzej DOBOSZ

Iwona POŻOGA

SEKRETARIAT KONFERENCJI

mgr Urszula JARASZEK

ZRZESZENIE FIRM DZIAŁAJĄCYCH
NA RZECZ OBRONNOŚCI RP

ul. E. Gierczak 8, (bl.112)
00 – 910 Warszawa
tel.: (22) 612 84 98
tel./fax: 681 33 91; 681 35 71

Redakcja:

płk rez. dr inż. Eugeniusz PIEDZIUK
płk rez. mgr inż. Antoni SKUBIS

Adiustacja i korekta:

mgr Urszula JARASZEK

Nakład: 150 egz. Skład komputerowy: Arkadiusz HOŁOWNIA
Druk i oprawa: *Zrzeszenie Firm Działających na rzecz Obronności RP*
ul. E. Gierczak 8, (bl.112) 00 – 910 Warszawa

MINISTER OBRONY NARODOWEJ

Warszawa, dn. 12.12.2001 r.

Szanowni Panowie

płk rez. dr inż. Eugeniusz Piedziuk
Przewodniczący
Komitetu Organizacyjnego
Konferencji

mgr inż. Jerzy Jakubowski
Dziekan Korpusu Firm
Działających na rzecz
Obronności RP

Wielce Szanowni Panowie !

Uprzejmie dziękuję za propozycję objęcia honorowego patronatu nad konferencją naukową na temat „Kierowanie obronnością państwa podczas stanów nadzwyczajnych z wykorzystaniem technicznych środków najnowszej generacji". Honorowy patronat nad Panów konferencją traktuję jako osobisty zaszczyt i wyróżnienie dla Ministerstwa Obrony Narodowej.

Jednocześnie pragnę wyrazić najwyższe uznanie dla Prezesów działających na polskim rynku firm, którzy z taką troską i odpowiedzialnością uczestniczą w procesie budowania systemu bezpieczeństwa państwa.

Życzę organizatorom konferencji powodzenia i sukcesów w jej przygotowaniu i przeprowadzeniu, zaś wszystkim uczestnikom - aby okazała się interesująca i pożyteczna. Z przyjemnością zapoznam się również z materiałami pokonferencyjnymi.

Z poważaniem

Jerzy Szmajdziński

WYKAZ FIRM

UCZESTNICZĄCYCH W KONFERENCJI

1. ALCATEL- Warszawa
2. ATM S.A. – Warszawa
3. ADVICE COMMUNICATION Sp. z o.o. – Warszawa
4. W. BURDECKI Sp. z o.o. – Warszawa
5. CISCO SYSTEMS POLAND – Warszawa
6. CNPEP RADWAR S.A. – Warszawa
7. DGT Sp. z o.o. - Gdańsk
8. EBS Ltd. - Warszawa
9. EFECTA Sp. z o.o. – Warszawa
10. EMAX S.A. - Poznań
11. EPIT & KRWZ – Warszawa
12. ERA GSM – Warszawa
13. NETIA NETWORK S.A. – Warszawa
14. OPTIMUS Sp. z o.o. – Nowy Sącz
15. OPTO Sp. z o.o. – Warszawa
16. PROVISION Sp. z o.o. – Warszawa
17. RWT TELEFONY POLSKIE S.A. - Warszawa
18. SOLIDEX S.A. – Warszawa
19. SPRINT Sp. z o.o. – Olsztyn
20. STEKOP S.A. - Białystok
21. TAC - POLSKA – Gdynia
22. TELKOM - TELOS S.A. – Kraków
23. TELZAS Sp. z o.o. – Szczecinek
24. TELEKOMUNIKACJA POLSKA S.A. – Warszawa
25. WIKING – Wesoła
26. ZWUT S.A. & SIEMENS COMPANY – Warszawa

WYKAZ

FIRM UCZESTNICZĄCYCH W WYSTAWIE

PODCZAS KONFERENCJI

1. DGT Sp. z o.o. - Gdańsk
2. EMAX S.A. – Poznań
3. CNPEP RADWAR S.A. – Warszawa
4. OPTO Sp. z o.o. - Warszawa
5. OPTIMUS Sp. z o.o. – Nowy Sącz
6. POLSKA TELEFONIA CYFROWA Sp. z o.o. Warszawa
7. PROVISION Sp. z o.o. - Warszawa
8. RWT TELEFONY POLSKIE S.A. – Radom
9. STEKOP S.A. - Białystok
10. TAC – POLSKA Sp. z o.o. – Gdynia
11. TELZAS Sp. z o.o. – Szczecinek
12. WOJSKOWY INSTYTUT ŁĄCZNOŚCI - Zegrze
13. WOJSKOWE ZAKŁADY ŁĄCZNOŚCI Nr 1 – Zegrze
14. ZWUT S.A.& SIEMENS COMPANY - Warszawa

SPIS TREŚCI

WSTĘP

„Wyobraźnia pozwala człowiekowi wyjść poza ustalone schematy, poza systemy, wniknąć w świat nieznany i narzucić im porządek ludzkich kategorii"

Jan Szczepański

Szanowni Państwo !

Wszyscy doskonale pamiętamy rok 1989. Miał on przełomowe znaczenie w najnowszej historii Polski. To właśnie w roku 1989 zapoczątkowana została gruntowna przebudowa systemu polityczno – społecznego i gospodarczego naszego państwa. Następowało, wraz z upływem czasu, stopniowe zbliżanie się różnych dziedzin jego funkcjonowania do standardów obowiązujących w państwach o rozwiniętej i ugruntowanej demokracji. Efektem tego było między innymi przyjęcie Polski do Paktu Północnoatlantyckiego oraz coraz lepsze perspektywy związane z włączeniem naszego kraju do struktur politycznych, a zwłaszcza gospodarczych, Europy Zachodniej.

W ramach ogólnych przeobrażeń, dotyczących państwa w całości, następowały istotne zmiany w dziedzinach niezwykle ważnych, wręcz fundamentalnych, dla pokojowego bytu i wszechstronnego rozwoju narodu. Do dziedzin tych należy zaliczyć między innymi bezpieczeństwo i obronność państwa, których ważnym gwarantem są siły zbrojne.

Nowe uwarunkowania zewnętrzne i wewnętrzne sprawiły, że również w obszarze czysto wojskowym musiały nastąpić istotne zmiany. Proces reformowania sił zbrojnych nie został zakończony. Choć jest on już mocno zaawansowany, nie należy sądzić, że jego pełne urzeczywistnienie nastąpi w najbliższej perspektywie. Reformowanie sił zbrojnych jest bowiem procesem trudnym, szczególnie kosztownym i dlatego w warunkach polskich – długotrwałym.

Głównym problemem są stosunkowo niskie, choć mające tendencje wzrostowe, nakłady na przezbrojenie i modernizację techniczną armii. Zatem jej unowocześnienie i zbliżenie się do standardów technicznych obowiązujących w czołowych armiach NATO następować będzie stopniowo i stosownie do wzrostu gospodarczego, odnotowywanego w kolejnych latach.

Z nieukrywaną satysfakcją możemy stwierdzić, że po roku 1989 sprawy bezpieczeństwa i obronności państwa nabrały nowego wymiaru. Stały się one w szerszym zakresie problemem publicznym, a więc ogólnopaństwowym, nie zaś tylko resortów tzw. „siłowych", a zwłaszcza ludzi noszących mundury – żołnierzy, policjantów, funkcjonariuszy straży granicznej, strażaków, itp. Sprawami bezpieczeństwa i obronności zaczęły zajmować się także różnego rodzaju organizacje, formalne i nieformalne. Z racji profilu swojej działalności mogły one w stosownym zakresie, wpłynąć na postęp i rozwój w różnych dziedzinach bezpieczeństwa i obronności państwa – legislacyjnej, strukturalnej, organizacyjnej, szkoleniowej, a zwłaszcza technicznej.

Do tego rodzaju organizacji z całą pewnością należy zaliczyć ukonstytuowane w roku 2000, ciągle jednak nieformalne, *ZRZESZENIE FIRM DZIAŁAJĄCYCH NA RZECZ OBRONNOŚCI RP*.

ZRZESZENIE..., wyrażając swoją głęboką troskę o sprawy bezpieczeństwa i obronności państwa, oddając do dyspozycji jego właściwych organów swój potencjał naukowy, techniczny i wykonawczy, postanowiło przejąć i kontynuować tradycję konferencji naukowych, połączonych z wystawą osiągnięć, których rodowód sięga roku 1993. Miejscem organizowania tego rodzaju corocznych imprez była w latach 1993 ÷ 1997 Akademia Obrony Narodowej, a głównych ich animatorem Zakład Zarządzania Systemami Informacyjnymi tejże uczelni. Konferencje naukowe były wówczas organizowane pod patronatem ministrów obrony narodowej i łączności oraz charakteryzowały się dużym rozmachem naukowym i wystawienniczym.

Na skutek zmian personalnych i restrukturyzacyjnych, w tym rozwiązania Zakładu Zarządzania Systemami Informacyjnymi, organizowanie Konferencji Systemu Obronnego i Łączności (KSOŁ) zostało zaniechane, a idea integrowania różnego rodzaju środowisk, w tym zwłaszcza firm teleinformatycznych, wokół spraw i działań mających na celu podwyższanie efektywności systemu bezpieczeństwa i obronności państwa, zaczęła powoli obumierać. Firmy oraz osoby reprezentujące różne środowiska, wspierające tę niezwykle ważną i potrzebną działalność, dostrzegły to pogłębiające się zagrożenie.

Efektem twórczej refleksji oraz, jak wcześniej wspomniałem, zatroskanie o sprawy bezpieczeństwa i obronności państwa, a także, nie ukrywajmy, zabieganie przez firmy o dobrze pojmowany interes biznesowy, było reaktywowanie konferencji ale w zmodyfikowanej formule organizacyjnej i merytoryczno – naukowej. Zainteresowane firmy „wzięły sprawy w swoje ręce", powołując wspomniane *ZRZESZENIE...* i wyłaniając jego władze. Skutkiem tego działania oraz urzeczywistnienia idei, które odżyły, było

właśnie zorganizowanie w Centrum Konferencyjnym WP, w kwietniu 2001r. - seminarium, a w grudniu tegoż roku - konferencji na temat: „Kierowanie obronnością państwa w aspekcie wykorzystania technicznych środków najnowszej generacji". Do inicjatywy *ZRZESZENIA*... pozytywnie odniósł się minister obrony narodowej przyjmując honorowy patronat nad tym przedsięwzięciem oraz wykazując zainteresowanie jego rezultatami.

Dorobek ostatniej dwudniowej konferencji to sześć referatów merytorycznych dotyczących zagadnień ogólnych i szczegółowych. Zagadnienia ogólne obejmowały przede wszystkim prezentację – systemu obronności RP, infrastruktury teleinformatycznej sił zbrojnych i zarządzania nią w stanach nadzwyczajnych oraz psychologicznych aspektów zachowań jednostek i grup społecznych w obliczu zagrożeń.

Referaty szczegółowe, które możemy nazwać „specjalistycznymi", dotyczyły działalności normalizacyjnej w resorcie obrony narodowej, bezpieczeństwa i ochrony informacji, realizowania zadań obronnych przez operatorów telekomunikacyjnych, itp. Referaty na powyższe tematy wygłosili przedstawiciele instytucji centralnych MON, Sztabu Generalnego WP, Akademii Obrony Narodowej i Wojskowej Akademii Technicznej.

W konferencji aktywnie uczestniczyli przedstawiciele firm, którzy zaprezentowali nie tylko własne osiągnięcia techniczne, ale także wygłosili niezwykle interesujące referaty merytoryczne dotyczące problematyki telekomunikacyjnej, ekologicznej, bezpieczeństwa obiektów i informacji, itp.

Konferencji towarzyszyła wystawa osiągnięć firm, która cieszyła się dużym zainteresowaniem zwiedzających. W wystawie uczestniczyło czternaście firm prezentując, w oparciu o zgromadzone eksponaty, swoje najnowsze osiągnięcia, możliwe do wykorzystania w strukturach organizacyjno – technicznych systemu bezpieczeństwa i obronności państwa.

Na zakończenie konferencji odbyła się żywa dyskusja, podsumowująca jej osiągnięcia, której rezultatem było także przyjęcie ustaleń dotyczących spożytkowania uzyskanego dorobku.

Uczestnicy konferencji zgodnie stwierdzili, że reaktywowane przedsięwzięcia naukowe należy kontynuować i rozwijać w przyszłości, zapoznając z ich dorobkiem i konkluzjami odpowiednie gremia kierownicze i decydenckie naszego kraju.

Michał Krauze

REFERATY

PROGRAMOWE

MINISTERSTWO
OBRONY NARODOWEJ

Stanisław KOZIEJ

SYSTEM OBRONNOŚCI RZECZPOSPOLITEJ POLSKIEJ W STANACH NADZWYCZAJNYCH

CENTRUM KONFERENCYJNE WP Grudzień 2001

Dziękuję za zaproszenie na dzisiejszą konferencję. Jestem przekonany o jej istotnym znaczeniu dla obronności naszego państwa. Wierzę ponadto, że będzie ona również bardzo interesująca, zważywszy na listę zaproszonych referentów.

Moim zadaniem, jako inaugurującego dyskusję, jest przedstawienie najbardziej generalnych wymagań i pożądanych założeń budowy systemu kierowania obronnością państwa w sytuacjach nadzwyczajnych zagrożeń. Użycie przeze mnie słowa „budowa", a nie np. „doskonalenie" lub „rozwijanie" nie jest tu przypadkowe. Niestety. Jesteśmy bowiem obecnie z pewnością jedynym państwem w NATO i chyba jednym z nielicznych państw w świecie, które nie mają prawnie uregulowanych spraw kierowania państwem w najbardziej krytycznych warunkach zagrożenia i wojny, a tym samym nie mamy w praktyce systemu kierowania państwem w czasie kryzysu i wojny. W razie zaistnienia takich sytuacji możemy liczyć co prawda na znaną w świecie naszą wyjątkową zdolność do improwizacji w trudnych sytuacjach, ale mimo wszystko to chyba nie jest rozwiązanie najlepsze. Mówiąc poważnie – brak czytelnego, jednoznacznie i zawczasu określonego systemu kierowania państwem w warunkach zagrożenia (kryzysu) i wojny jest największą słabością naszego systemu bezpieczeństwa narodowego. Usunięcie tej słabości musi być zadaniem priorytetowym.

Ukazują to z całą mocą ostatnie klęski żywiołowe, wnioski z narodowej strategicznej gry wojennej i z udziału w ćwiczeniach kryzysowych NATO, przygotowania do nadchodzącego ćwiczenia CMX 2002, dyskusje i kontrowersje w toku prac nad ustawą o gotowości cywilnej i zarządzaniu kryzysowym a wreszcie praktyczne doświadczenia z reagowania na obecną sytuację kryzysową spowodowaną atakiem terrorystycznym na naszego sojusznika.

Przystępując do omówienia podstawowych wymagań w tym zakresie chciałbym rozpocząć od stwierdzenia, że w projektowaniu założeń narodowego systemu kierowania nie można stosować częściowych rozwiązań, wprowadzać półśrodków, ani też tworzyć struktur doraźnych, np. tylko na potrzeby ćwiczeń, jak to, niestety, ma wciąż miejsce obecnie w stosunku do nadchodzącego ćwiczenia CMX 2002. Konieczne jest podejście całościowe, strategiczne, zintegrowane. Od kilku lat staram się przekonać do takiego podejścia kolejnych decydentów. W samym MON to się udało i po dwóch latach różnych „przepychanek" i dziwnych pomysłów zbudowany został resortowy system kierowania reagowaniem kryzysowym odpowiadający logice współczesnych wymagań. Niestety, na szczeblu krajowym wciąż jesteśmy „w lesie". Z uporem godnym lepszej sprawy forsowane

są rozwiązania nie mające wiele wspólnego z racjonalną organizacją systemu kierowania w szczególnych warunkach zagrożenia bezpieczeństwa państwa i wojny.

Pracując nad własnym systemem, który winien być interoperacyjny z systemem sojuszniczym, warto wziąć pod uwagę, że w NATO trwają obecnie prace nad dostosowaniem dotychczasowego systemu pogotowia (NATO Precautionary System) do nowych warunków w celu uczynienia zeń skutecznego instrumentu sojuszniczego system reagowania kryzysowego (NATO Crisis Response System), zapewniającego reagowanie na całe spektrum zagrożeń – od najmniej niebezpiecznych zagrożeń cywilnych do wojny nuklearnej na pełną skalę włącznie. Jako członek sojuszu uczestniczymy w tych pracach. Nakłada to na nas jednocześnie obowiązek budowania analogicznego, kompatybilnego z sojuszniczym, narodowego systemu kierowania szeroko rozumianym reagowaniem kryzysowym. W dotychczasowych pracach w tym zakresie nie udało się niestety zapewnić takiego właśnie, zintegrowanego podejścia. Rozwiązania zawarte w ostatnio procedowanej ustawie o gotowości cywilnej i cywilnym zarządzaniu kryzysowym nie były kompatybilne z rozwiązaniami sojuszniczymi. Zostały one ograniczone – w wyniku przyjęcia zawężonych definicji podstawowych kategorii, takich jak: kryzys, gotowość cywilna, planowanie cywilne – wyłącznie do spraw związanych z tzw. kryzysami cywilnymi czasu pokoju. Stoi to w sprzeczności z rozumieniem „Crisis Managament" w NATO. Dlatego istnieje potrzeba przygotowania rozwiązań zapewniających zbudowanie systemu zintegrowanego, cywilno-wojskowego. Konieczne są do tego regulacje, które należałoby wprowadzić w jednej ustawie o zintegrowanym kierowaniu bezpieczeństwem narodowym (reagowaniem kryzysowym i obroną państwa). Projekt takiej ustawy został przygotowany przez Departament Systemu Obronnego MON i jest obecnie wstępnie konsultowany i uzgadniany w ramach resortu.

W projektowaniu zintegrowanego systemu kierowania należałoby uwzględniać następujące podstawowe założenia:

a) Reagowanie kryzysowe traktować szeroko (tak jak w NATO) – jako reagowanie na zagrożenia o charakterze militarnym i pozamilitarnym. Myślę, że ostatni atak terrorystyczny z 11 września 2001 r. oraz trwająca obecnie kampania antyterrorystyczna świadczą najpełniej o konieczności takiego właśnie podejścia. Na szczeblu państwa (czyli na poziomie ponadresortowym, ponaddziałowym) potrzebny jest zatem jeden zintegrowany system zajmujący się obydwoma rodzajami (typami) sytuacji kryzysowych.

b) Konieczne jest zapewnienie ciągłości kierowania przygotowaniami pokojowymi, reagowaniem kryzysowym i obroną państwa w czasie wojny. Stąd też system kierowania przygotowaniami pokojowymi winien być podstawą do rozwinięcia systemu kierowania reagowaniem kryzysowym, ten zaś – podstawą do rozwinięcia wojennego systemu kierowania.

c) Problematyka pokojowych przygotowań na sytuacje nadzwyczajne, reagowania kryzysowego i obrony państwa w razie wojny, czyli problematyka bezpieczeństwa narodowego, ma ponadresortowy (ponaddziałowy) charakter. Konieczne jest zatem zapewnienie odpowiednich organizacyjnych warunków do efektywnego jej koordynowania na szczeblu administracji rządowej i całego państwa. Pora najwyższa, aby wreszcie zakończyć z kultywowaniem Polski resortowej w obszarze bezpieczeństwa. Zatrzymanie się na poziomie działów i traktowanie obrony narodowej jako jednego z działów jest nieporozumieniem. Obrona narodowa, a tym bardziej bezpieczeństwo narodowe, to sprawa całego państwa, a nie tylko jednego działu czy resortu. Działem mogą być siły zbrojne, ale nie obronność państwa.

d) W projektowaniu systemu kierowania bezpieczeństwem narodowym (w tym kierowania reagowaniem kryzysowym i obroną państwa) należy przede wszystkim uwzględnić ogólne (uniwersalne) zasady budowy systemów kierowania (szkic nr 1), obowiązujące ustalenia Konstytucji RP oraz konieczność interoperacyjności z istniejącym sojuszniczym systemem kierowania reagowaniem kryzysowym.

Decydent

W odniesieniu do pierwszego elementu każdego systemu kierowania, tj. decydenta, należy oczywiście uwzględnić, że zgodnie z Konstytucją organami władzy wykonawczej są prezydent i Rada Ministrów. Forum ich współdziałania jest Rada Gabinetowa (nie posiadająca jednakowoż żadnych kompetencji władczych). Prezes Rady Ministrów zapewnia realizację decyzji RM i – ewentualnie uzgodnionych na forum Rady Gabinetowej – decyzji prezydenta.

Co do funkcjonowania państwowego ogniwa decydenckiego w czasie *pokoju* istnieje potrzeba ustawowego sprecyzowania relacji kompetencyjnych prezydenta i Rady Ministrów w zakresie bezpieczeństwa narodowego. Należałoby zwłaszcza zdecydowanie doprecyzować w ustawie rolę i zasady działania w tym zakresie Rady Gabinetowej (włącznie z ewentualnym zapraszaniem na jej posiedzenia marszałków Sejmu i Senatu). Jednym z istotnych zadań powinno być m.in. wskazanie przez prezydenta, na wniosek

Prezesa Rady Ministrów, osoby przewidzianej do wyznaczenia na stanowisko Naczelnego Dowódcy Sił Zbrojnych RP w razie wojny.

W odniesieniu do kierowania w czasie *kryzysu* należałoby przyjąć generalną zasadę, że odbywa się ono wedle procedur i struktur czasu pokojowego. Bezpośrednie kierowanie wykonawcze reagowaniem kryzysowym sprawuje premier, który w zależności od rodzaju i skali kryzysu może powierzyć część swoich zadań innemu członkowi Rady Ministrów. Sprawy o podstawowym znaczeniu uzgadniane winny być z Prezydentem RP w ramach kryzysowych posiedzeń Rady Gabinetowej, odbywanych ewentualnie z udziałem osób reprezentujących także inne organy państwowe.

Wprowadzenie dodatkowych nadzwyczajnych rozwiązań konieczne byłoby na czas *wojny*. Proponuje się, aby przyjąć, że w takiej sytuacji prezydent na wniosek premiera dokonuje zmian w składzie Rady Ministrów (na podstawie ustawy o działach), w wyniku czego tworzona jest Rada Ministrów w wojennym składzie. Prezydent i Rada Ministrów w wojennym składzie stanowią z kolei „wojenną" Radę Gabinetową („Gabinet Wojenny"). Na wniosek Prezesa Rady Ministrów Prezydent RP powołuje Naczelnego Dowódcę Sił Zbrojnych RP, który jednocześnie pełni funkcję szefa Sztabu Generalnego WP. Naczelny dowódca uczestniczy również w posiedzeniach „wojennej" Rady Gabinetowej oraz reprezentuje Polskę w naczelnych gremiach wojskowych NATO (wchodzi w skład Komitetu Wojskowego NATO).

Organ doradczy

Organem doradczym prezydenta jest Rada Bezpieczeństwa Narodowego. Natomiast organem doradczym Rady Ministrów w sprawach bezpieczeństwa narodowego winien być stały komitet na czele z premierem (np. Rządowy Komitet Bezpieczeństwa Narodowego – RKBN). Skład komitetu powinien być tożsamy z przewidywanym na czas wojny składem Rady Ministrów (rządową częścią "Gabinetu Wojennego").

W czasie *pokoju* należałoby utworzyć RKBN na mocy rozporządzenia Rady Ministrów. W pracach RKBN powinien uczestniczyć także przedstawiciel Prezydenta RP. Ważne jest ustalenie współdziałania RKBN z Radą Bezpieczeństwa Narodowego. RKBN winna mieć powierzone kompetencje do rozpatrywania i rekomendowania Radzie Ministrów całości problemów bezpieczeństwa narodowego o skali państwowej (polityki zagranicznej, obronności, bezpieczeństwa wewnętrznego). Wskazane byłoby wprowadzenie zasady systematycznych posiedzeń Komitetu – np. nie mniej niż raz w miesiącu.

W razie kryzysu RKBN powinien zbierać się stosownie do potrzeb i rozpatrywać, uzgadniać oraz rekomendować Radzie Ministrów sprawy wymagające decyzji na szczeblu państwa.

Na czas wojny należałoby założyć, że RKBN przestaje funkcjonować – w praktyce przekształcając się w „wojenną" Radę Ministrów (stając się częścią „Gabinetu Wojennego").

Organ sztabowy

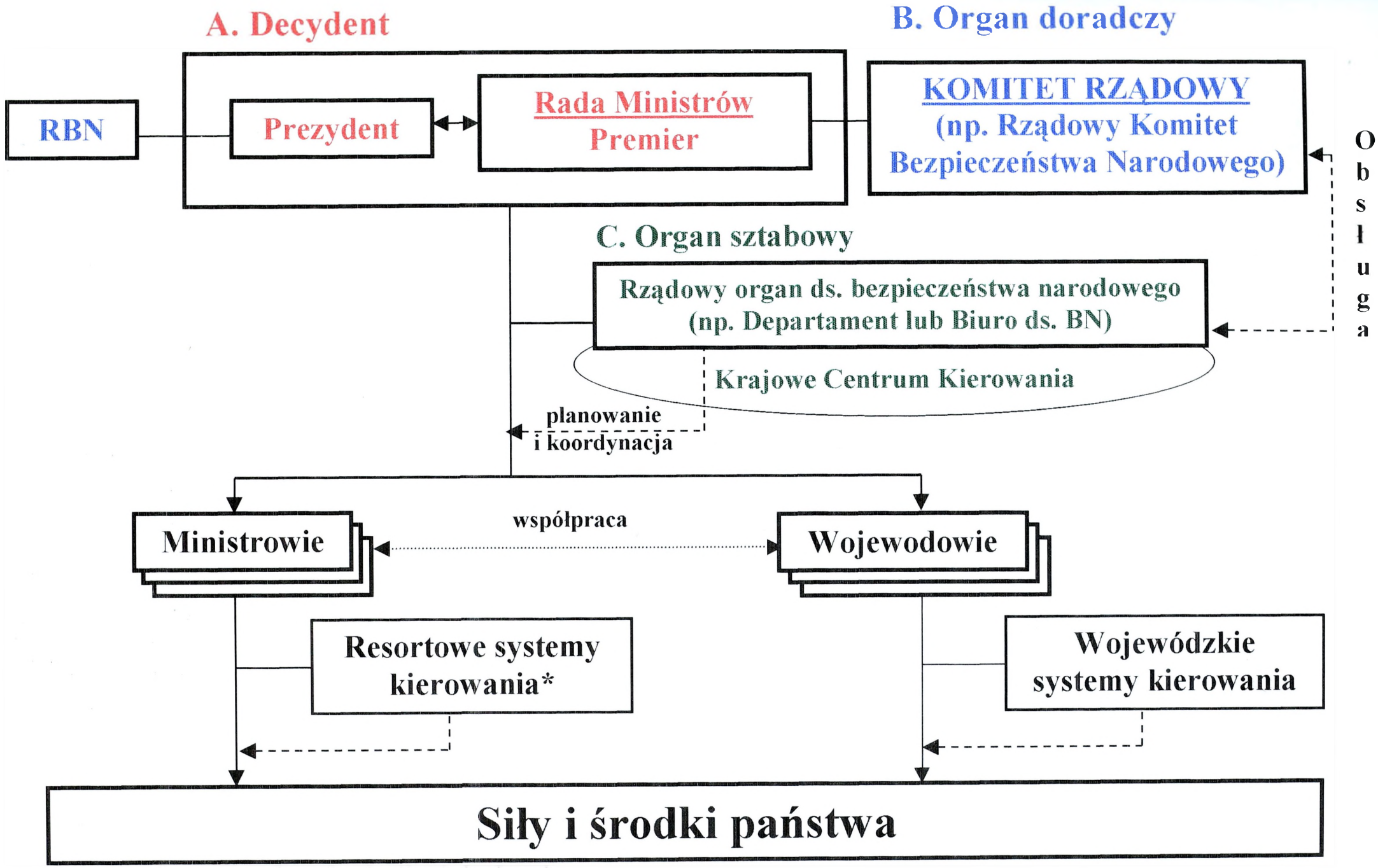
Organem sztabowym – odpowiedzialnym za bieżące, codzienne, wykonawcze planowanie i koordynowanie realizacji decyzji rządowych w zakresie bezpieczeństwa narodowego (w tym w zakresie reagowania kryzysowego), a także obsługę RKBN - powinien być zintegrowany organ rządowy, podległy bezpośrednio premierowi. Taki organ – np. Departament lub Biuro Systemu Bezpieczeństwa Narodowego (DSBN) – utworzony mógłby być na bazie istniejących obecnie: Departamentu Spraw Obronnych kancelarii premiera, Departamentu Systemu Obronnego MON (obecnie w likwidacji), części urzędu szefa OCK, etatów i specjalistów z MSZ, MSWiA, UOP, RCSS oraz ewentualnie z innych struktur rządowych.

W czasie *pokoju* głównym zadaniem Departamentu (Biura) Systemu Bezpieczeństwa Narodowego byłoby przygotowywanie projektów ogólnopaństwowych (ponadresortowych, ponaddziałowych) koncepcji, planów i programów strategicznych w zakresie bezpieczeństwa narodowego oraz koordynowanie (monitorowanie, nadzorowanie) realizacji decyzji Rady Ministrów w tym zakresie. Komórka ta zapewniałaby także obsługę RKBN (jej szef mógłby być jednocześnie sekretarzem RKBN). Ważnym jej zadaniem powinno być również utrzymywanie Krajowego Centrum (Stanowiska) Kierowania i zapewnianie bieżącego monitorowania sytuacji bezpieczeństwa państwa. Zbudowanie i bieżące utrzymywanie zintegrowanego (ponadresortowego) Centrum (Stanowiska) Kierowania na potrzeby premiera jest obecnie jednym z najpilniejszych zadań praktycznych w tworzeniu systemu kierowania kryzysowego i obronnego. Nie może być tak, jak jest obecnie u nas, aby premier był zdany wyłącznie na korzystanie ze stanowisk swoich ministrów. Jest to rozwiązanie kuriozalne i nigdzie w świecie nie spotykane.

W czasie kryzysu organ sztabowy zapewnia konieczne warunki zintegrowanego kierowania reagowaniem kryzysowym na szczeblu państwa. Rozwija – stosownie do potrzeb – Krajowy Sztab Kryzysowy na Krajowym Centrum (Stanowisku) Kierowania Kryzysowego.

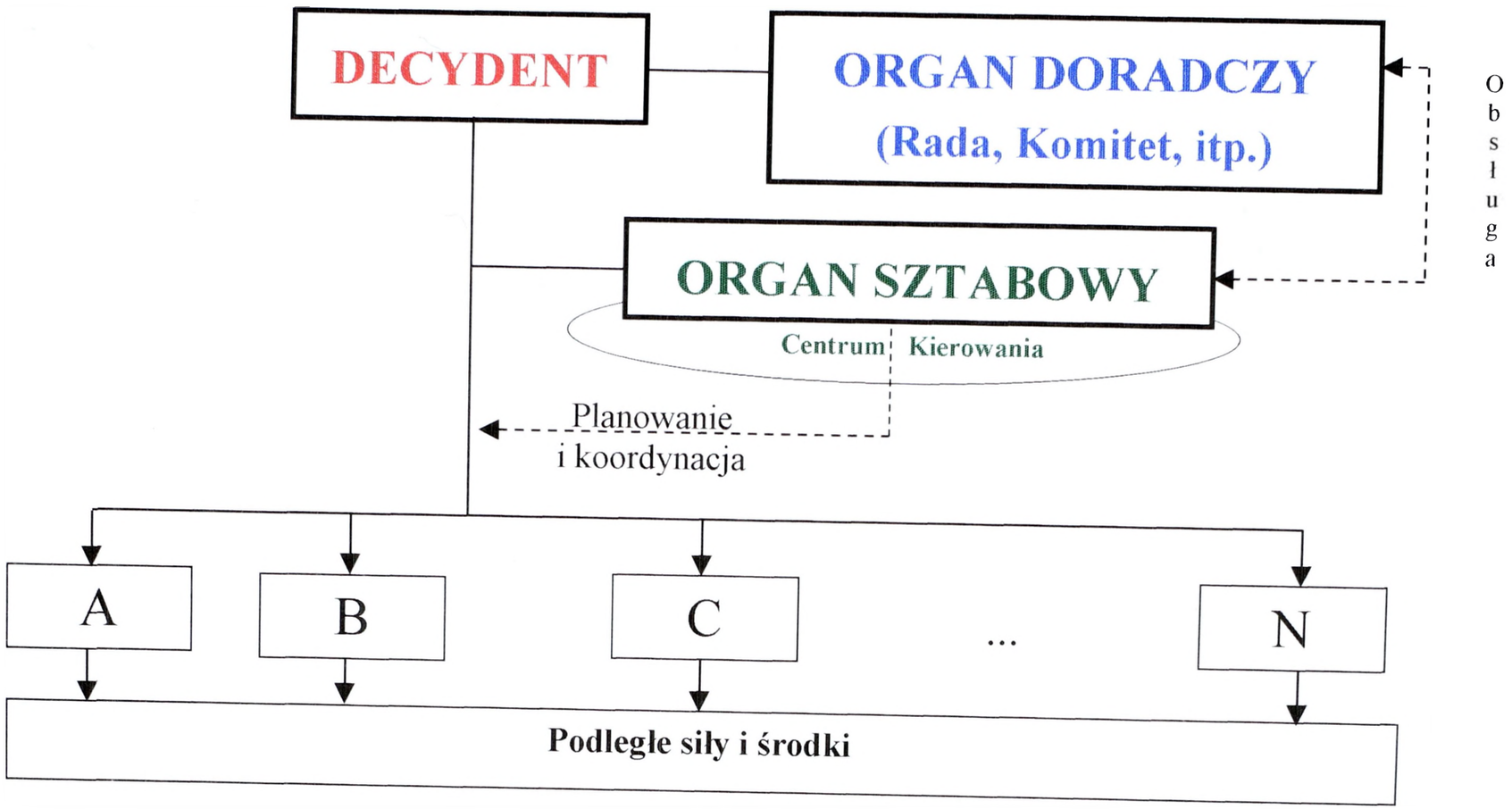
W razie wojny proponowany organ sztabowy powinien odpowiadać za zapewnienie operacyjnych i organizacyjno-technicznych warunków kierowania obroną państwa przez Prezydenta RP i Radę Ministrów, w tym rozwinięcie Centralnego Stanowiska Kierowania Obroną Państwa.

W zakończeniu chciałbym szczególnie mocno podkreślić konieczność zintegrowanego, cywilno-wojskowego podejścia do budowy systemu kierowania bezpieczeństwem narodowym w czasie pokoju, kryzysu i wojny. Już dawno skończyła się era podejścia wyłącznie specjalistycznego, resortowego. Sądzę, że ostatecznie powinny nas o tym przekonać wnioski z reagowania na obecną sytuację kryzysową spowodowaną atakiem terrorystycznym z 11 września. Jeśli będziemy chcieli sprawami szeroko rozumianego reagowania kryzysowego kierować w skali państwa przy pomocy struktur Straży Pożarnej, a sprawami obrony państwa przy pomocy wyłącznie struktur Sił Zbrojnych RP – to, z całym szacunkiem dla tych dwóch bardzo ważnych instytucji państwa, nic dobrego z tego nie wyniknie. To „ćwiczyliśmy" w ostatnich latach z miernymi skutkami. Pora zbudować na szczeblu krajowym strukturę zintegrowaną, cywilno-wojskową, pracującą na rzecz decydenta państwowego i spinającą w jedną spójną całość wysiłki wszystkich specjalistycznych sił i środków państwa. Mam nadzieję, że tego typu przesłanie z tej konferencji znajdzie swój oddźwięk w pracach nad konkretnymi rozwiązaniami prawnymi i organizacyjnymi.



*) w tym także system dowodzenia siłami zbrojnymi

Model kierowania bezpieczeństwem narodowym w czasie pokoju, kryzysu i wojny



Uniwersalny model kierowania

SZTAB GENERALNY WP

Julian MAJ
Jan BLAJER

KIEROWANIE I DOWODZENIE SIŁAMI ZBROJNYMI RP W STANACH NADZWYCZAJNYCH

CENTRUM KONFERENCYJNE WP Grudzień 2001

SZTAB GENERALNY WOJSKA POLSKIEGO

ZARZĄD SYSTEMÓW DOWODZENIA SG WP

KIEROWANIE I DOWODZENIE SZ RP W STANACH NADZWYCZAJNYCH

Referujący: płk Jan BLAJER

ZAGADNIENIA

- przyczyny budowy nowej struktury dowodzenia i kierowania SZ RP;
- dowodzenie i kierowanie w czasie „P";
- dowodzenie i kierowanie w czasie kryzysu i wojny.

GŁÓWNE PRZYCZYNY ZMIAN

- **zmiany doktrynalne;**
- **przynależność do NATO;**
- **wymogi wewnętrzne;**

GŁÓWNE PRZYCZYNY ZMIAN

(cd)

- **ZMIANY DOKTRYNALNE:**
  - nowa ocena zagrożeń;
  - wymagania na SZ lżejsze, mobilne, o wysokiej gotowości;
  - użycie nowych technologii;
  - dostosowane użycia SZ do zagrożeń i osiągnięć technologicznych;
  - zmniejszenie SZ.

GŁÓWNE PRZYCZYNY ZMIAN

(cd)

- **PRZYNALEŻNOŚĆ DO NATO:**
  - zgodność organizacyjna struktury systemu dowodzenia i kierowania;
  - zgodność struktur wewnętrznych dowództw isztabów;
  - sprawne dowodzenia i kierowanie w ramach wspólnej obrony Sojuszu wg Art. 5 TPA:
    - przejęcie dowodzenia przez dowództwa NATO (TOA);
    - wszechstronne zabezpieczenie operacyjnych wojsk;
    - realizacja zadań państwa gospodarza (HNS);
    - zastosowanie zintegrowanych zautomatyzowanych systemów dowodzenia.

GŁÓWNE PRZYCZYNY ZMIAN

(cd)

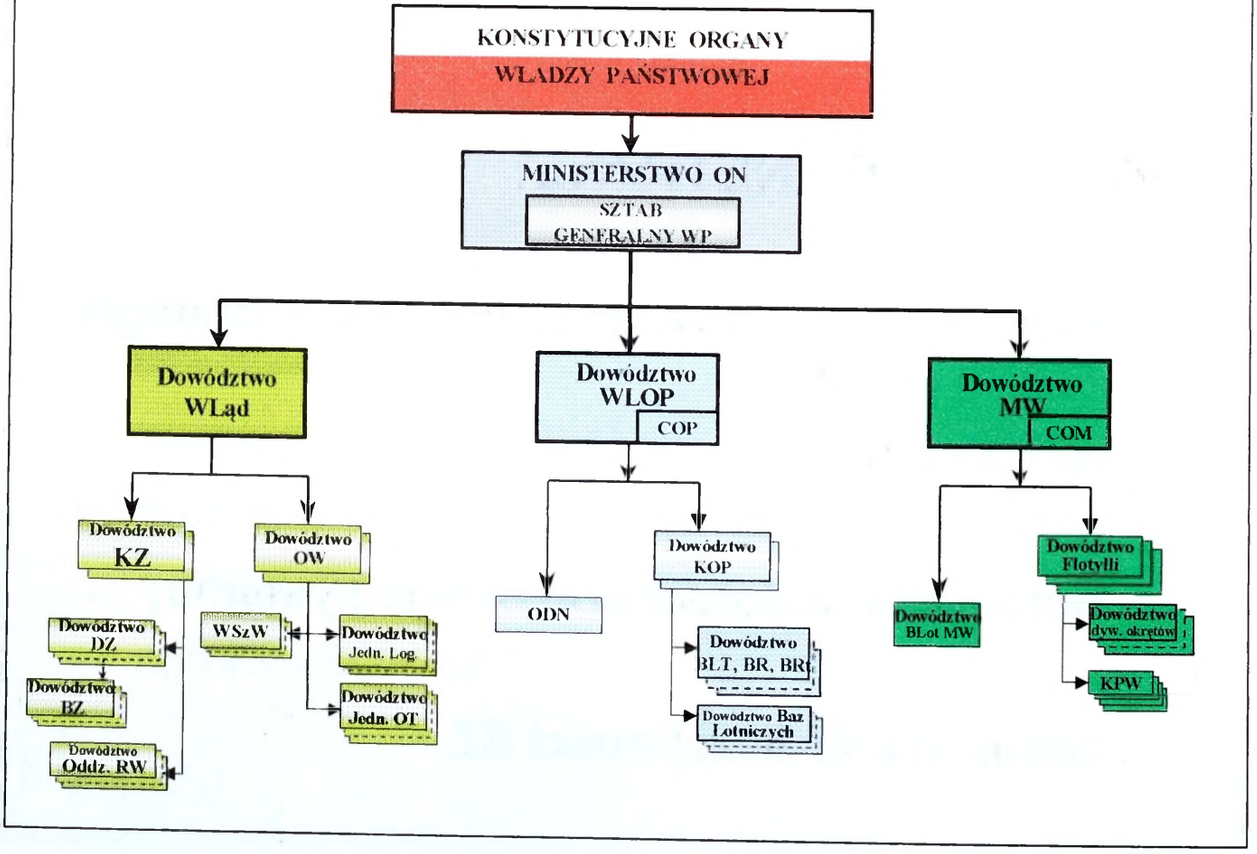
- **WYMOGI WEWNĘTRZNE:**
  - strategia bezpieczeństwa państwa i strategia obronna RP;
  - ograniczenia dotychczasowego systemu;
  - zmniejszenie liczebności SZ.

ZAŁOŻENIA ZMIAN SYSTEMU DOWODZENIA

- zbieżność struktur i zadań cz. „P" i „W";
- skrócenie linii dowodzenia;
- zgodność ze strukturami NATO;
- łatwość przejścia od dowodzenia narodowego do sojuszniczego;
- optymalizacja struktury i funkcjonowania - efekty ekonomiczne.

SYSTEM DOWODZENIA SIŁAMI ZBROJNYMI RP czasu „P"

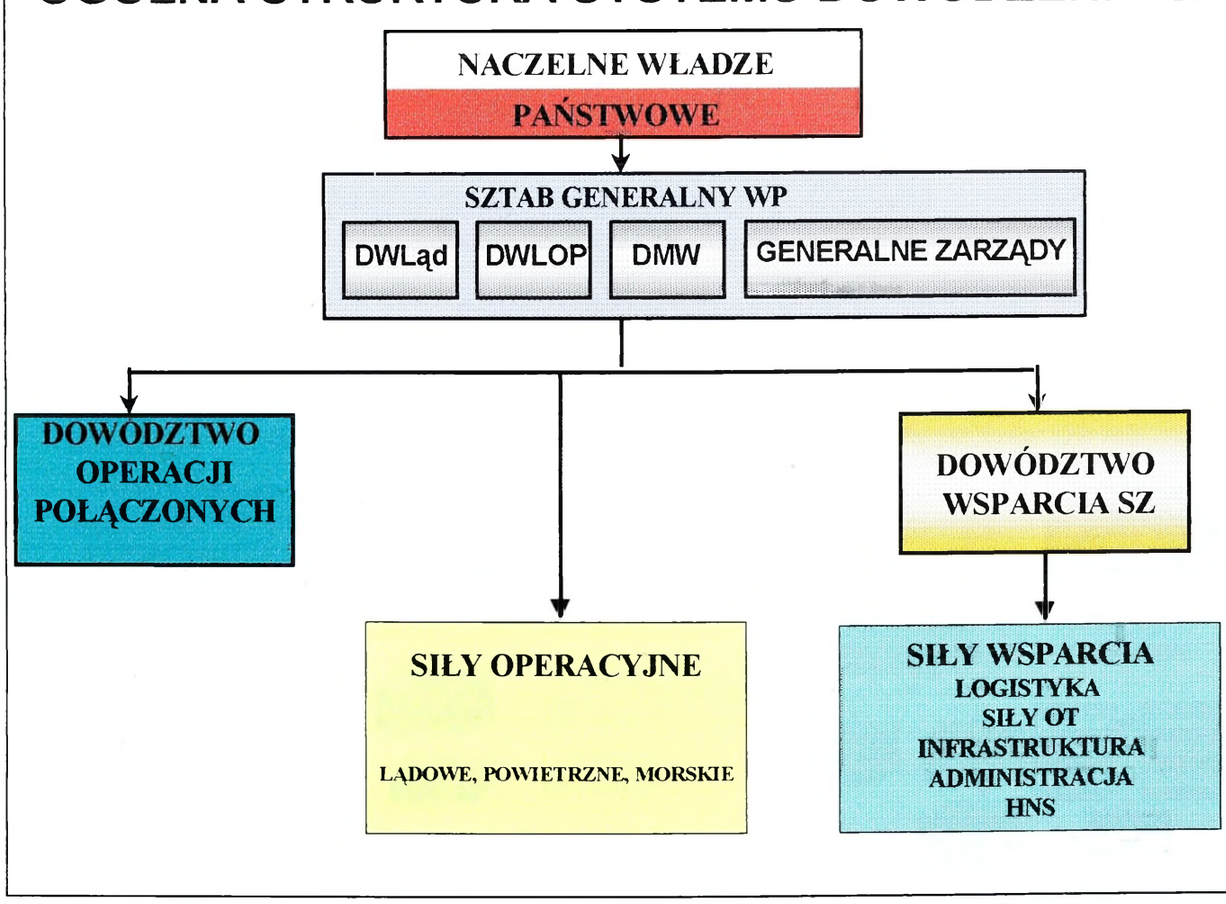
/stan aktualny/

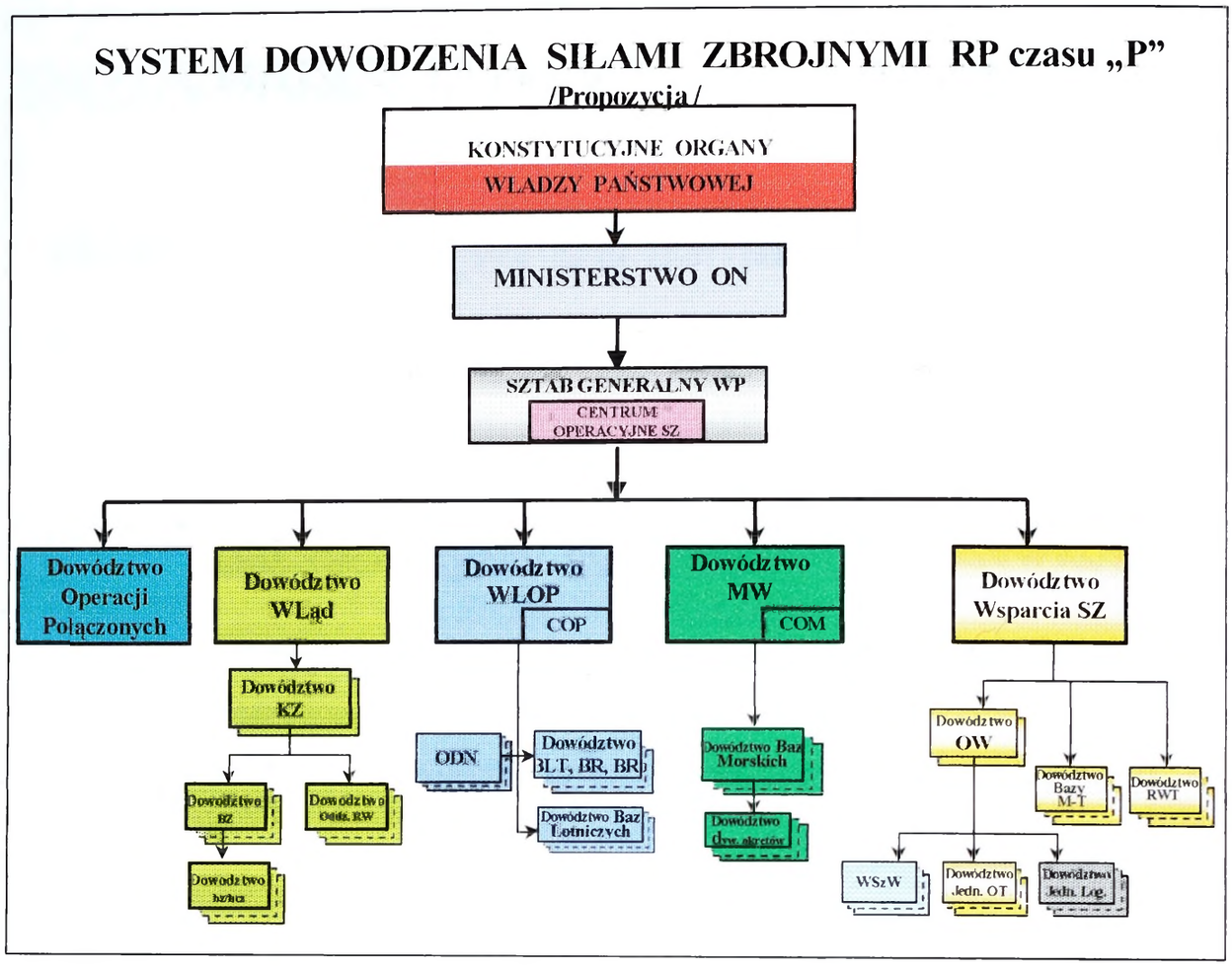


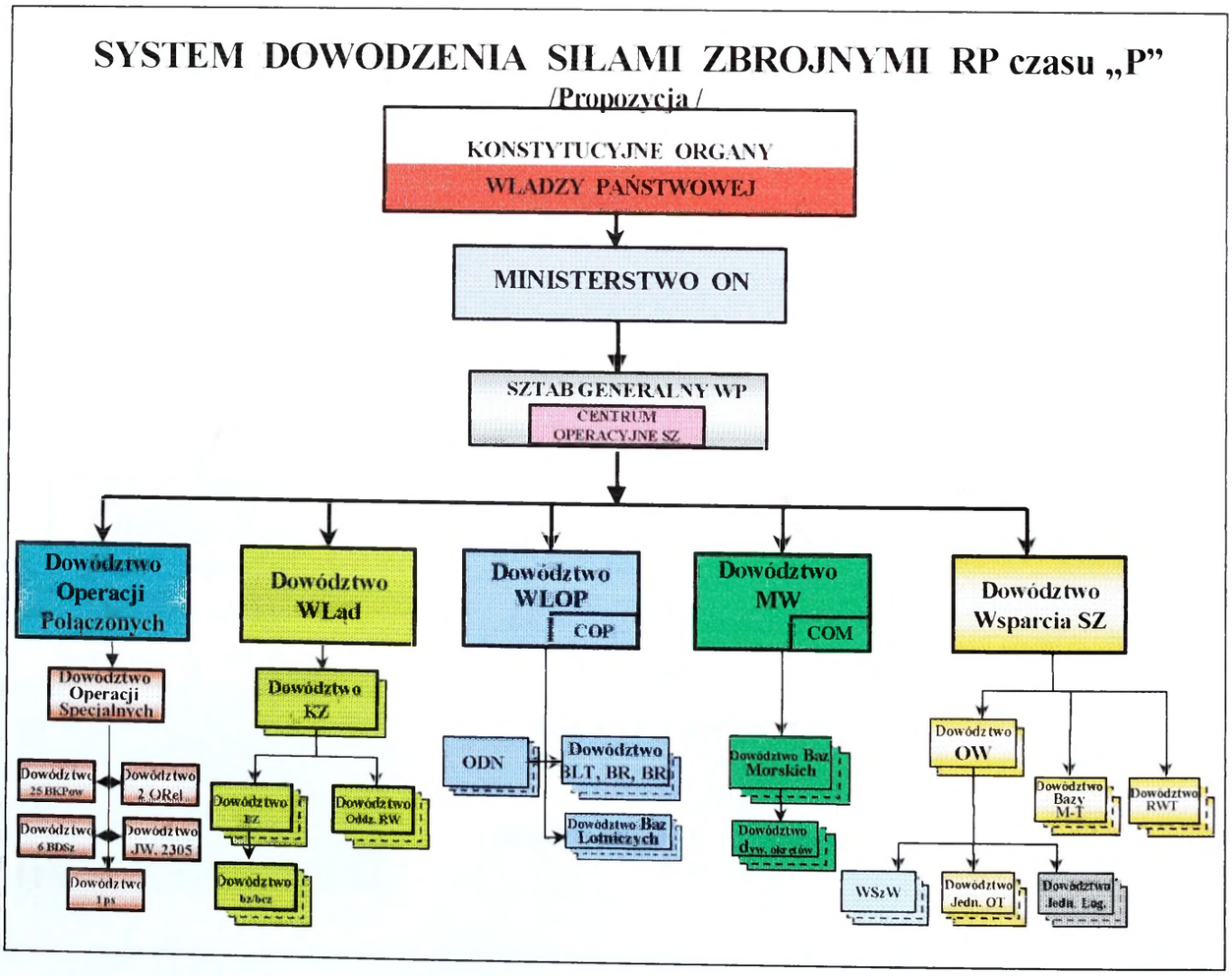
KIERUNKI GŁÓWNYCH ZMIAN

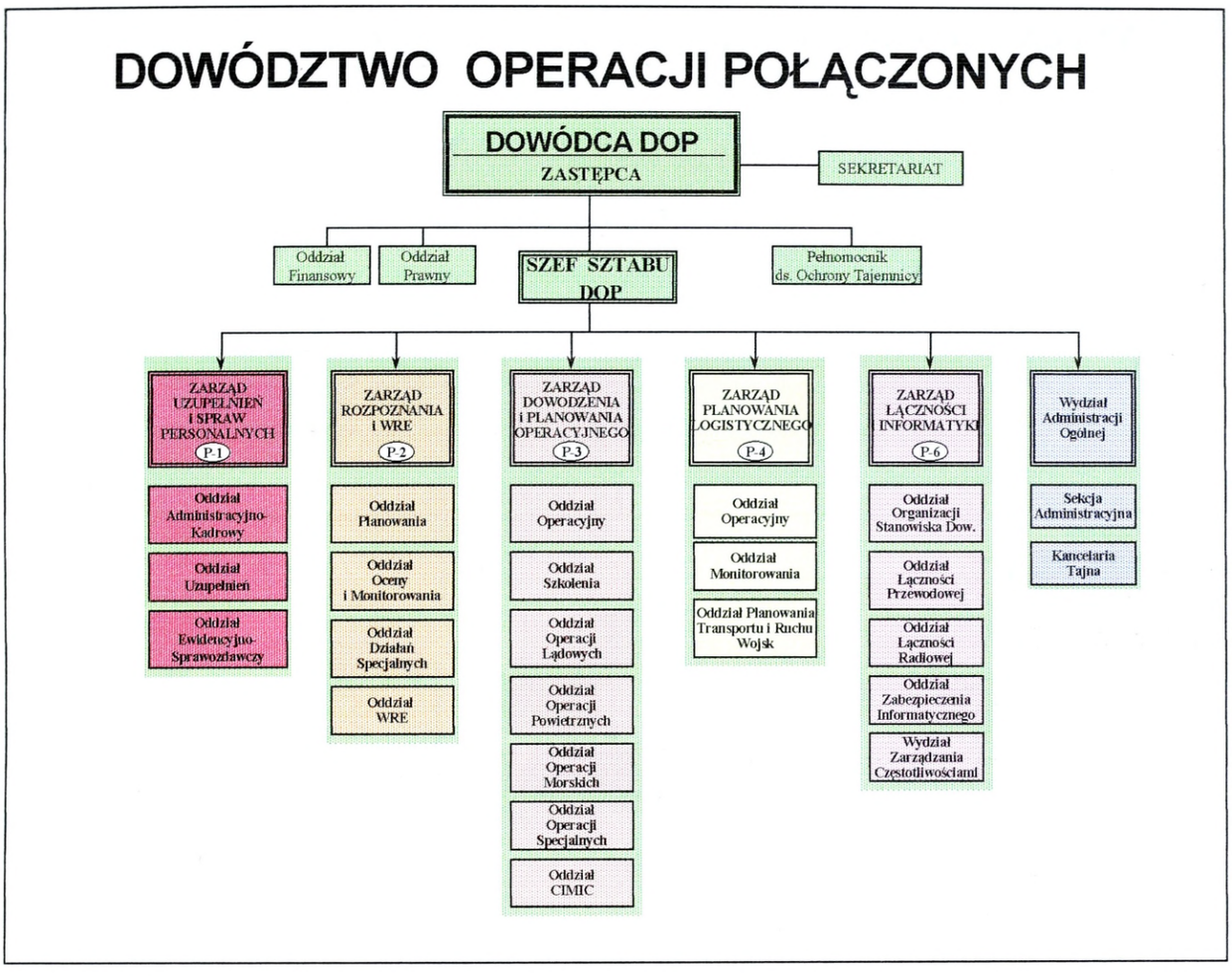
- zmiana kompetencji SG WP;
- utworzenie Dowództwa Operacji Połączonych (DOP);
- utworzenie Dowództwa Wsparcia SZ;
- zmiana roli i miejsca dowództw RSZ;
- likwidacja co najmniej jednego z niższych szczebli dowodzenia.

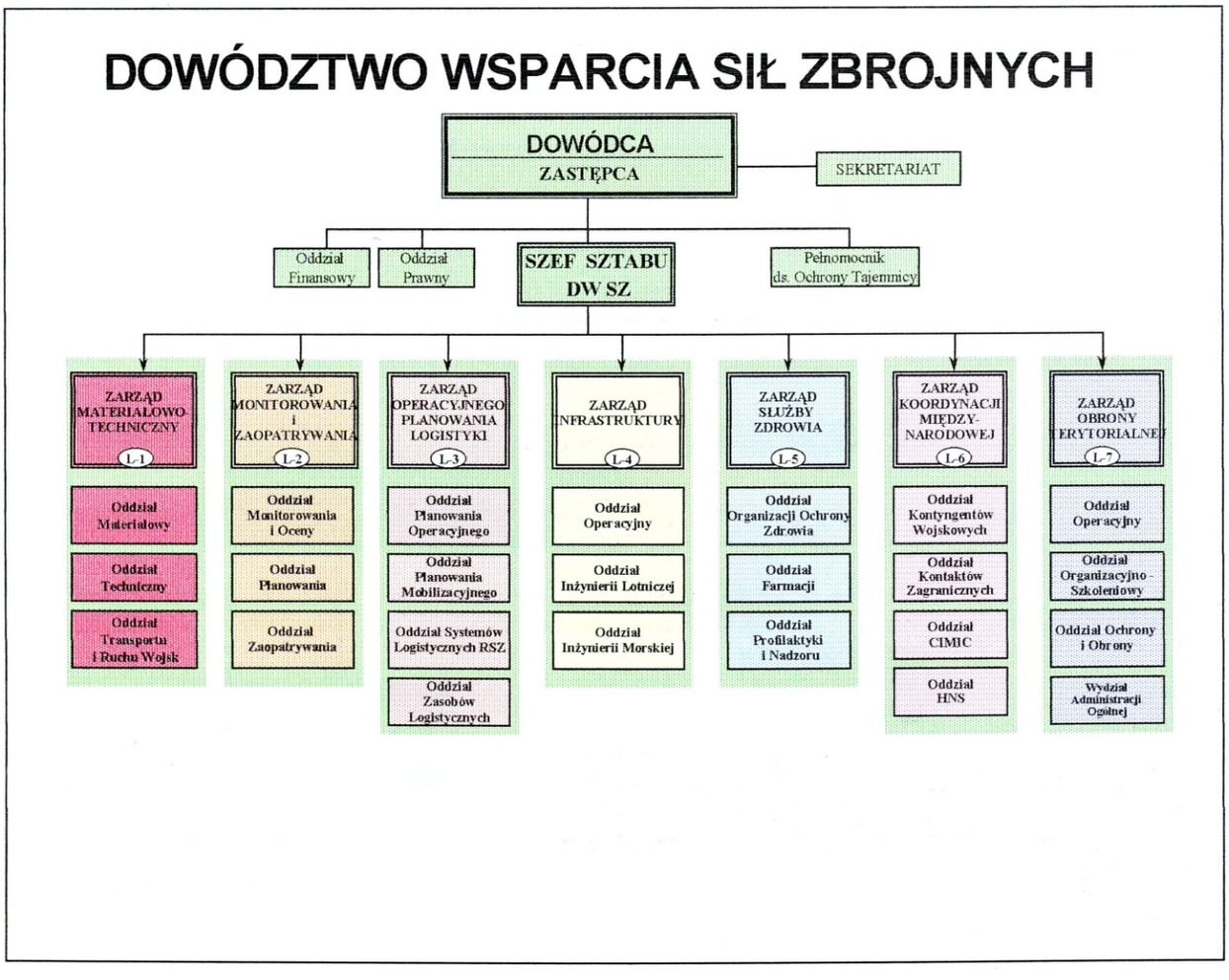
OGÓLNA STRUKTURA SYSTEMU DOWODZENIA SZ

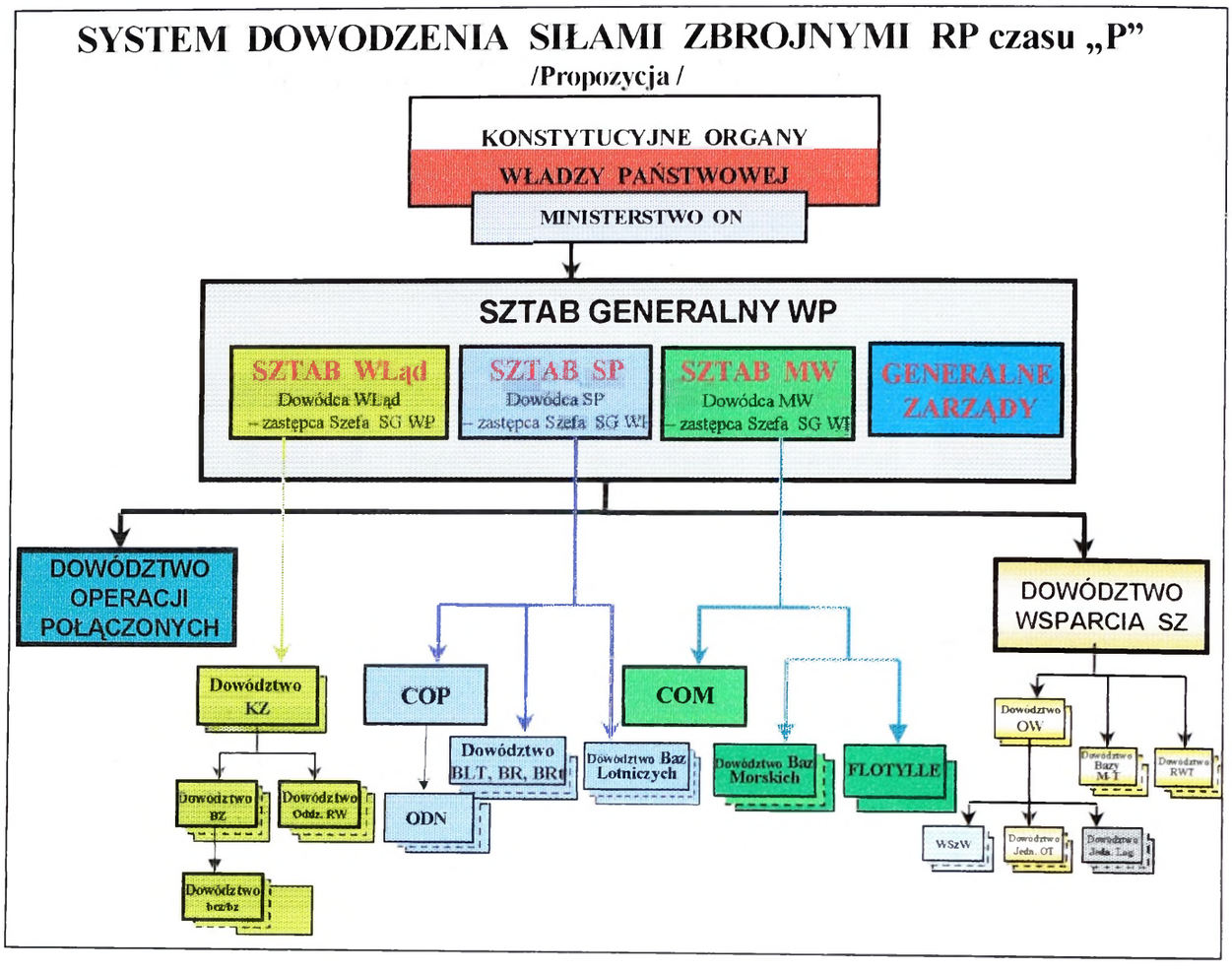


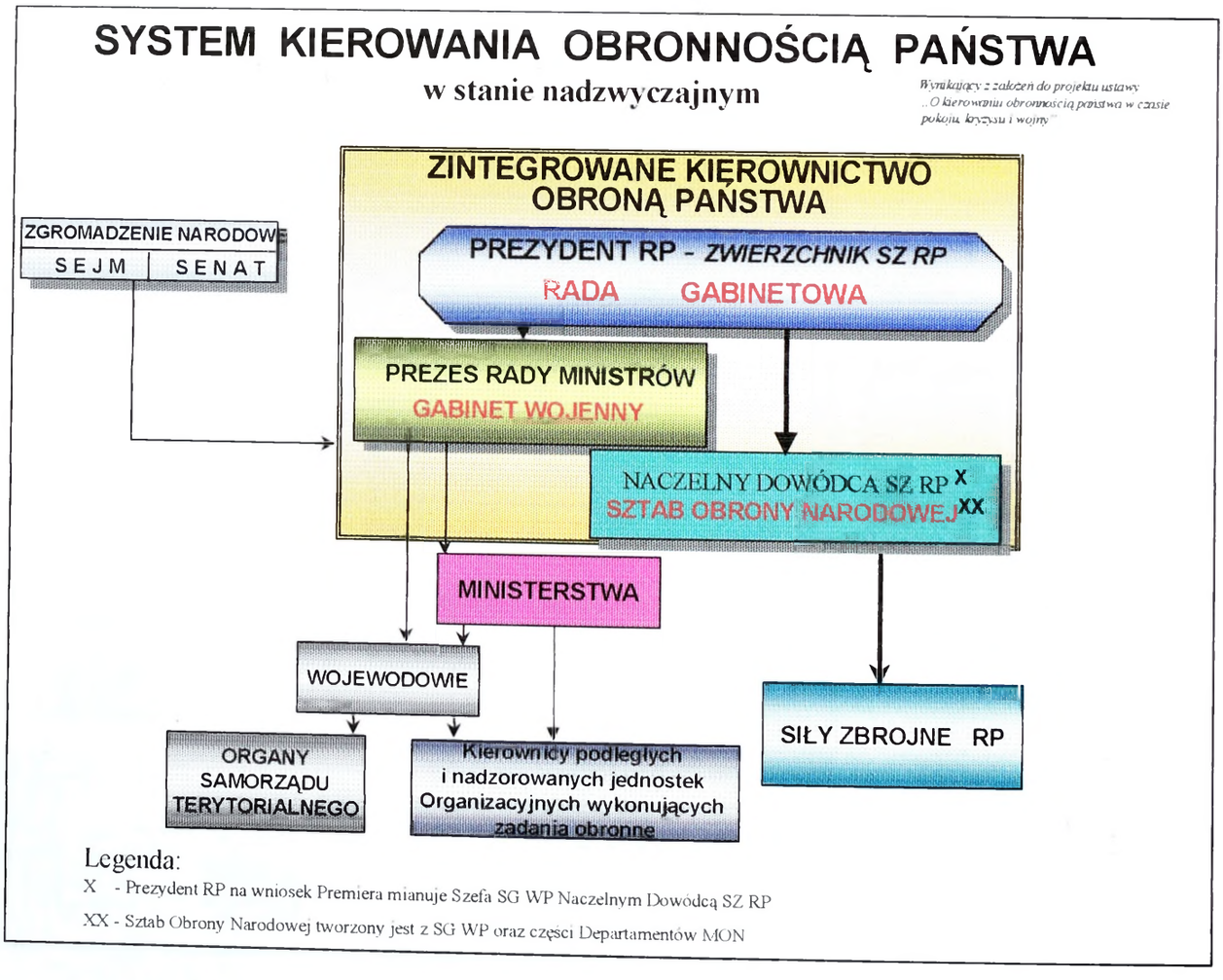

SYSTEM DOWODZENIA SIŁAMI ZBROJNYMI RP czasu „P”
/Propozycja/
KONSTYTUCYJNE ORGANY
WŁADZY PAŃSTWOWEJ
MINISTERSTWO ON
SZTAB GENERALNY WP
CENTRUM OPERACYJNE SZ
Dowództwo Operacji Połączonych
Dowództwo WLąd
Dowództwo WLOP
COP
Dowództwo MW
COM
Dowództwo Wsparcia SZ
Dowództwo KZ
ODN
Dowództwo BLT, BR, BRz
Dowództwo Baz Lotniczych
Dowództwo Baz Morskich
Dowództwo dyw. okrętów
Dowództwo OW
Dowództwo Bazy M-T
Dowództwo RWT
WSzW
Dowództwo Jedn. OT
Dowództwo Jedn. Log.
Dowództwo BZ
Dowództwo Oddz. RW
Dowództwo bz/bcz

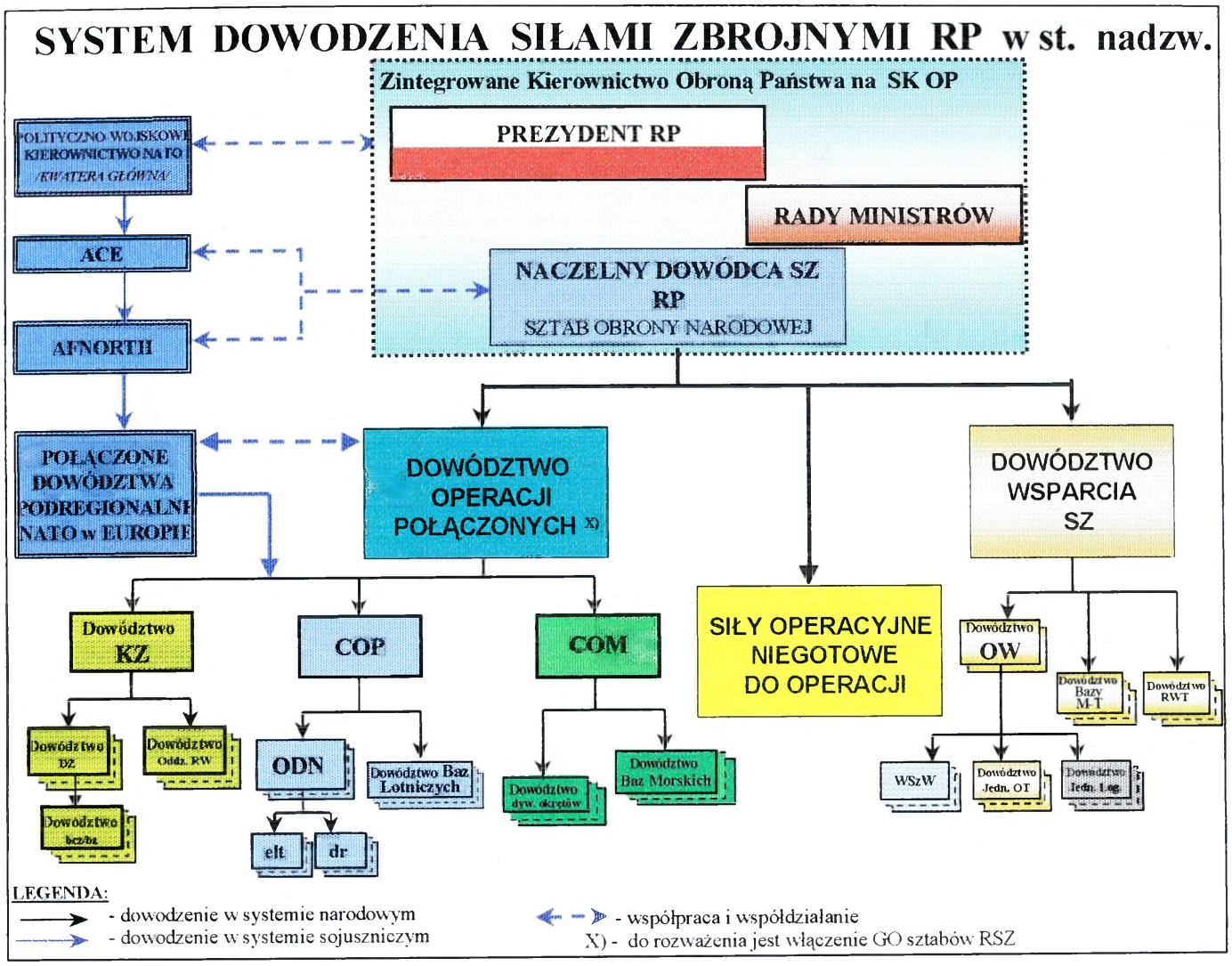

SYSTEM DOWODZENIA SIŁAMI ZBROJNYMI RP czasu „P”
/Propozycja/
KONSTYTUCYJNE ORGANY
WŁADZY PAŃSTWOWEJ
MINISTERSTWO ON
SZTAB GENERALNY WP
CENTRUM OPERACYJNE SZ
Dowództwo Operacji Połączonych
Dowództwo WLąd
Dowództwo WLOP
COP
Dowództwo MW
COM
Dowództwo Wsparcia SZ
Dowództwo Operacji Specjalnych
Dowództwo KZ
Dowództwo 25 BKPow
Dowództwo 2 ORel
Dowództwo 6 BDSz
Dowództwo JW. 2305
Dowództwo 1 ps
ODN
Dowództwo BLT, BR, BRz
Dowództwo Baz Lotniczych
Dowództwo Baz Morskich
Dowództwo dyw. okrętów
Dowództwo OW
Dowództwo Bazy M-T
Dowództwo RWT
WSzW
Dowództwo Jedn. OT
Dowództwo Jedn. Log.
Dowództwo BZ
Dowództwo Oddz. RW
Dowództwo bz/bcz


DOWÓDZTWO OPERACJI POŁĄCZONYCH
DOWÓDCA DOP
ZASTĘPCA
SEKRETARIAT
Oddział Finansowy
Oddział Prawny
SZEF SZTABU DOP
Pełnomocnik ds. Ochrony Tajemnicy
ZARZĄD UZUPEŁNIEŃ i SPRAW PERSONALNYCH P-1
Oddział Administracyjno-Kadrowy
Oddział Uzupełnień
Oddział Ewidencyjno-Sprawozdawczy
ZARZĄD ROZPOZNANIA i WRE P-2
Oddział Planowania
Oddział Oceny i Monitorowania
Oddział Działań Specjalnych
Oddział WRE
ZARZĄD DOWODZENIA i PLANOWANIA OPERACYJNEGO P-3
Oddział Operacyjny
Oddział Szkolenia
Oddział Operacji Lądowych
Oddział Operacji Powietrznych
Oddział Operacji Morskich
Oddział Operacji Specjalnych
Oddział CIMIC
ZARZĄD PLANOWANIA LOGISTYCZNEGO P-4
Oddział Operacyjny
Oddział Monitorowania
Oddział Planowania Transportu i Ruchu Wojsk
ZARZĄD ŁĄCZNOŚCI INFORMATYKI P-6
Oddział Organizacji Stanowiska Dow.
Oddział Łączności Przewodowej
Oddział Łączności Radiowej
Oddział Zabezpieczenia Informatycznego
Wydział Zarządzania Częstotliwościami
Wydział Administracji Ogólnej
Sekcja Administracyjna
Kancelaria Tajna


DOWÓDZTWO WSPARCIA SIŁ ZBROJNYCH
DOWÓDCA
ZASTĘPCA
SEKRETARIAT
Oddział Finansowy
Oddział Prawny
SZEF SZTABU DW SZ
Pełnomocnik ds. Ochrony Tajemnicy
ZARZĄD MATERIAŁOWO-TECHNICZNY L-1
Oddział Materiałowy
Oddział Techniczny
Oddział Transportu i Ruchu Wojsk
ZARZĄD MONITOROWANIA i ZAOPATRYWANIA L-2
Oddział Monitorowania i Oceny
Oddział Planowania
Oddział Zaopatrywania
ZARZĄD OPERACYJNEGO PLANOWANIA LOGISTYKI L-3
Oddział Planowania Operacyjnego
Oddział Planowania Mobilizacyjnego
Oddział Systemów Logistycznych RSZ
Oddział Zasobów Logistycznych
ZARZĄD INFRASTRUKTURY L-4
Oddział Operacyjny
Oddział Inżynierii Lotniczej
Oddział Inżynierii Morskiej
ZARZĄD SŁUŻBY ZDROWIA L-5
Oddział Organizacji Ochrony Zdrowia
Oddział Farmacji
Oddział Profilaktyki i Nadzoru
ZARZĄD KOORDYNACJI MIĘDZY-NARODOWEJ L-6
Oddział Kontyngentów Wojskowych
Oddział Kontaktów Zagranicznych
Oddział CIMIC
Oddział HNS
ZARZĄD OBRONY TERYTORIALNEJ L-7
Oddział Operacyjny
Oddział Organizacyjno - Szkoleniowy
Oddział Ochrony i Obrony
Wydział Administracji Ogólnej

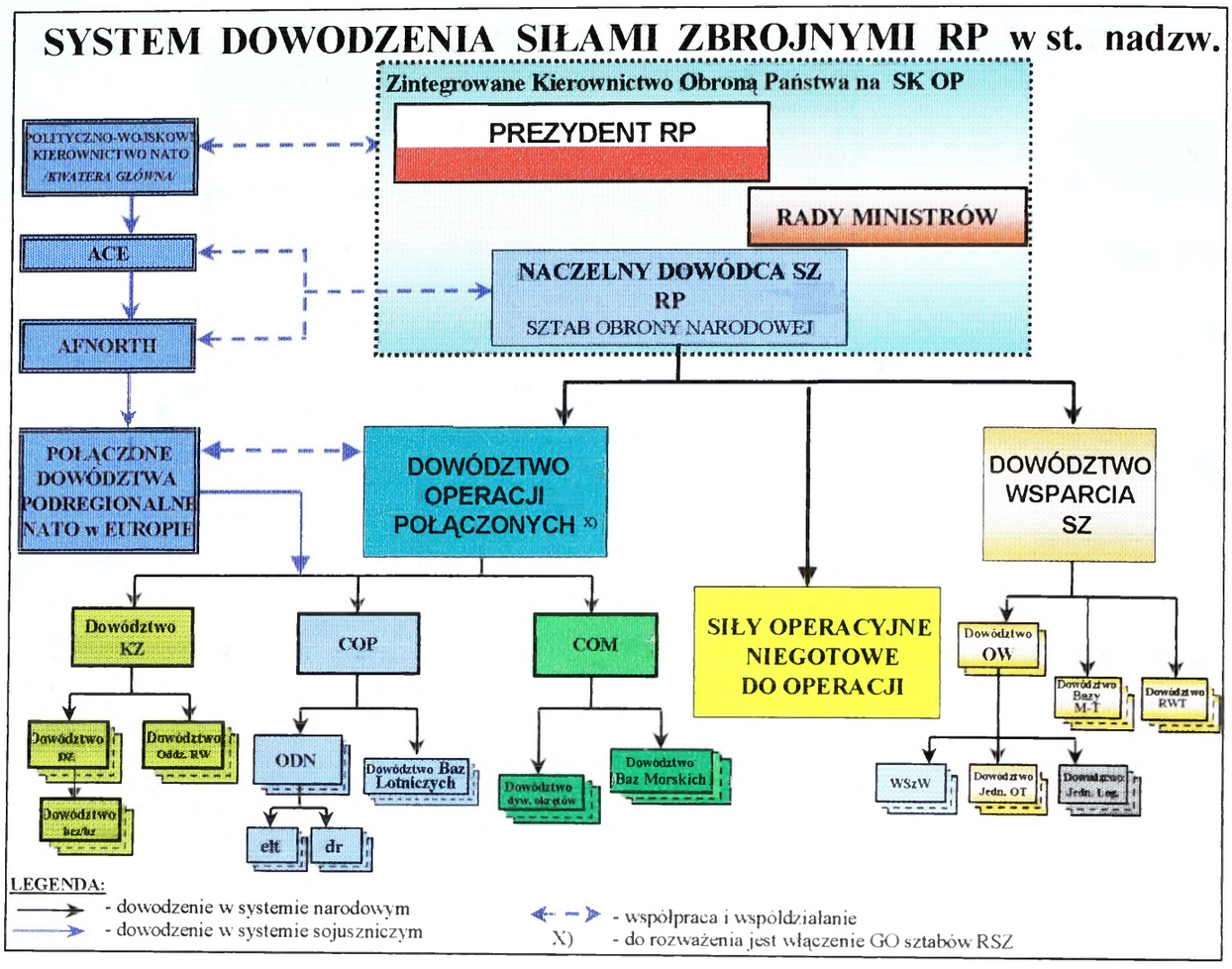

SYSTEM DOWODZENIA SIŁAMI ZBROJNYMI RP czasu „P”
/Propozycja /
KONSTYTUCYJNE ORGANY
WŁADZY PAŃSTWOWEJ
MINISTERSTWO ON
SZTAB GENERALNY WP
SZTAB WLąd
Dowódca WLąd
– zastępca Szefa SG WP
SZTAB SP
Dowódca SP
– zastępca Szefa SG WP
SZTAB MW
Dowódca MW
– zastępca Szefa SG WP
GENERALNE ZARZĄDY
DOWÓDZTWO OPERACJI POŁĄCZONYCH
DOWÓDZTWO WSPARCIA SZ
Dowództwo KZ
COP
COM
Dowództwo BLT, BR, BRt
Dowództwo Baz Lotniczych
Dowództwo Baz Morskich
FLOTYLLE
Dowództwo OW
Dowództwo Bazy M.T
Dowództwo RWT
Dowództwo BZ
Dowództwo Oddz. RW
ODN
WSzW
Dowództwo Jedn. OT
Dowództwo Jedn. Log
Dowództwo bez/bz


SYSTEM KIEROWANIA OBRONNOŚCIĄ PAŃSTWA
w stanie nadzwyczajnym
Wynikający z założeń do projektu ustawy
„O kierowaniu obronnością państwa w czasie pokoju, kryzysu i wojny”
ZINTEGROWANE KIEROWNICTWO OBRONĄ PAŃSTWA
ZGROMADZENIE NARODOWE
SEJM
SENAT
PREZYDENT RP - ZWIERZCHNIK SZ RP
RADA GABINETOWA
PREZES RADY MINISTRÓW
GABINET WOJENNY
NACZELNY DOWÓDCA SZ RP X
SZTAB OBRONY NARODOWEJ XX
MINISTERSTWA
WOJEWODOWIE
ORGANY SAMORZĄDU TERYTORIALNEGO
Kierownicy podległych i nadzorowanych jednostek Organizacyjnych wykonujących zadania obronne
SIŁY ZBROJNE RP
Legenda:
X - Prezydent RP na wniosek Premiera mianuje Szefa SG WP Naczelnym Dowódcą SZ RP
XX - Sztab Obrony Narodowej tworzony jest z SG WP oraz części Departamentów MON



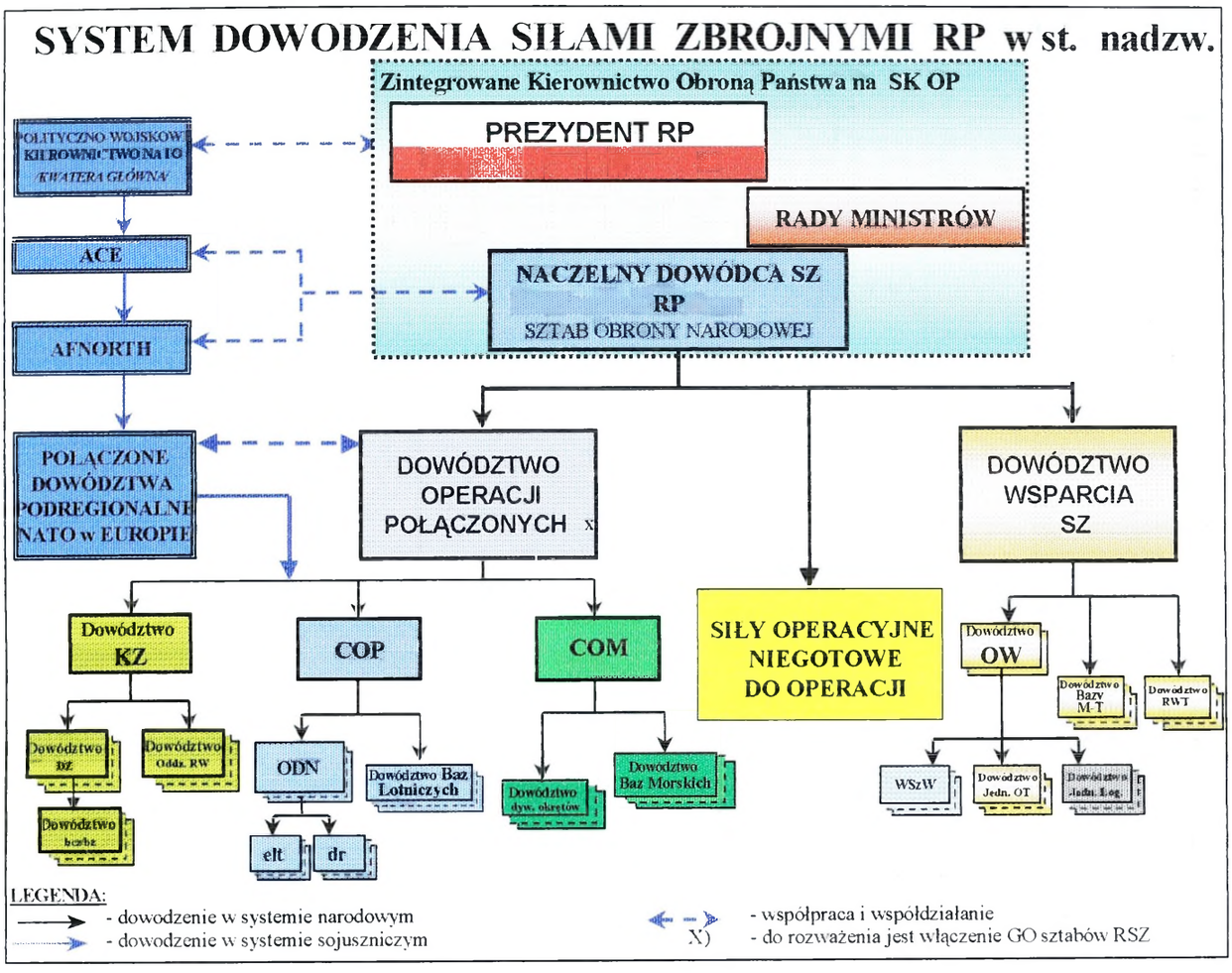
ZADANIA SZTABU OBRONY NARODOWEJ

- ocena sytuacji i wypracowanie decyzji dla naczelnych władz;
- kierowanie całością działań SZ w układzie narodowym;
- współdziałanie z wojskowymi władzami NATO;
- mobilizacyjne i operacyjne rozwinięcie SZ;
- realizacja TOA;
- kierowanie HNS;
- określanie potrzeb obronnych, współdziałanie z resortami;
- odtwarzanie zdolności bojowej SZ.



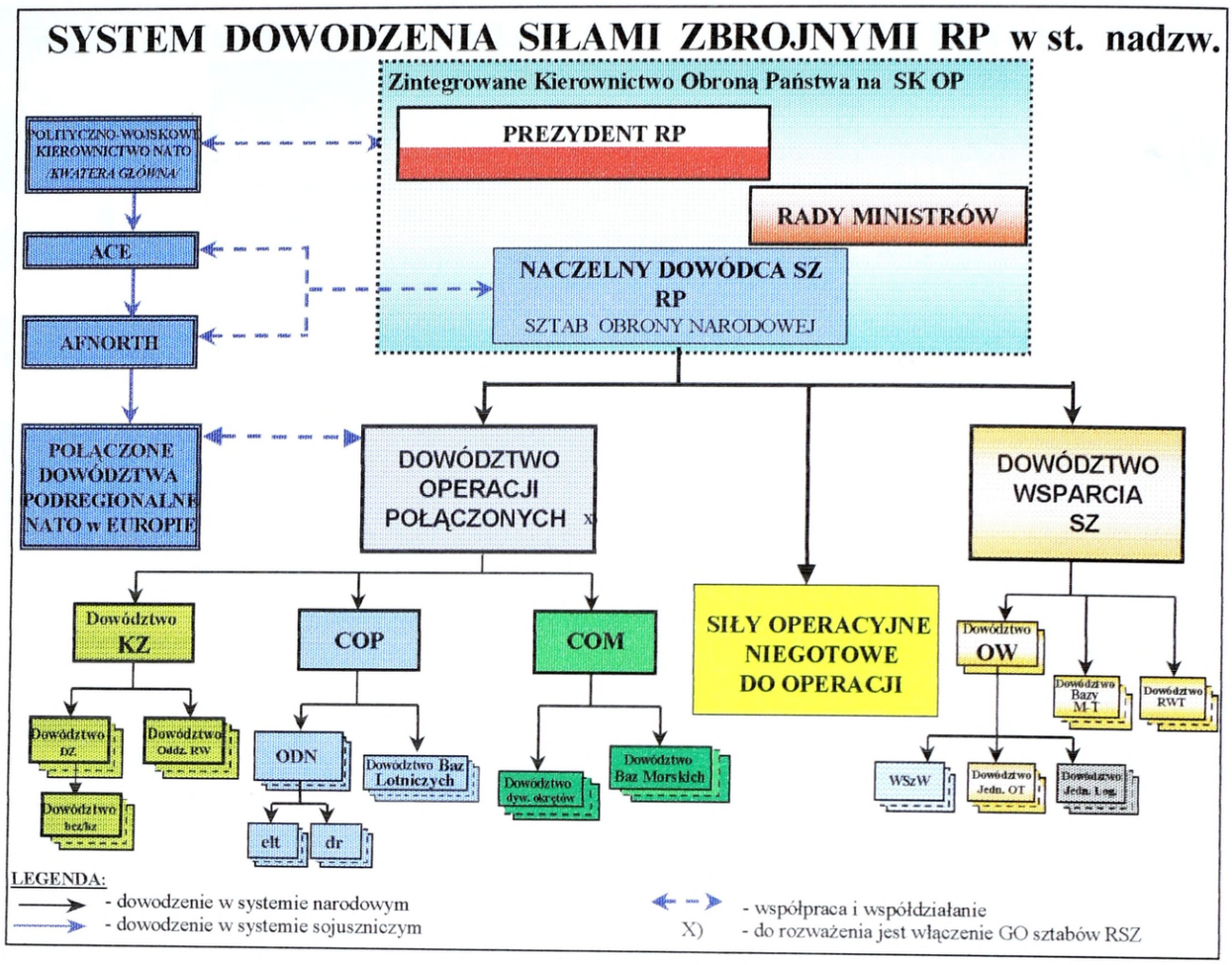
ZADANIA DOWÓDZTWA OPERACJI POŁĄCZONYCH

- realizacja zadań dyrektywnych Naczelnego Dowódcy SZ;
- planowanie i prowadzenie operacji połączonej na obszarze RP;
- dowodzenie wydzielonymi siłami operacyjnymi i sprawne ich przekazanie dowództwu sojuszniczemu;
- współudział w planowaniu użycia SZ w systemie sojuszniczym;
- zdolność do włączenia się do sojuszniczego łańcucha dowodzenia.



ZADANIA DOWÓDZTWA WSPARCIA SZ

- wsparcie logistyczne;
- obrona terytorialna;
- zarządzanie infrastrukturą;
- administracja ;
- HNS;
- dowodzenie strefą tyłową w strukturze dowodzenia sojuszniczego.


SYSTEM DOWODZENIA SIŁAMI ZBROJNYMI RP w st. nadzw.
Zintegrowane Kierownictwo Obroną Państwa na SK OP
POLITYCZNO-WOJSKOWE KIEROWNICTWO NATO
KWATERA GŁÓWNA
PREZYDENT RP
RADY MINISTRÓW
ACE
NACZELNY DOWÓDCA SZ RP
SZTAB OBRONY NARODOWEJ
AFNORTH
POŁĄCZONE DOWÓDZTWA PODREGIONALNE NATO w EUROPIE
DOWÓDZTWO OPERACJI POŁĄCZONYCH X)
DOWÓDZTWO WSPARCIA SZ
Dowództwo KZ
COP
COM
SIŁY OPERACYJNE NIEGOTOWE DO OPERACJI
Dowództwo OW
Dowództwo Bazy M-T
Dowództwo RWT
Dowództwo DZ
Dowództwo Oddz. RW
Dowództwo bez/lot
ODN
Dowództwo Baz Lotniczych
elt
dr
Dowództwo dyw. okrętów
Dowództwo Baz Morskich
WSzW
Dowództwo Jedn. OT
Dowództwo Jedn. Log.
LEGENDA:
- dowodzenie w systemie narodowym
- dowodzenie w systemie sojuszniczym
- współpraca i współdziałanie
X) - do rozważenia jest włączenie GO sztabów RSZ

AKADEMIA
OBRONY NARODOWEJ

Jacek PAWŁOWSKI

MODEL SYSTEMU KIEROWANIA REAGOWANIEM KRYZYSOWYM W SYTUACJACH NADZWYCZAJNYCH ZAGROŻEŃ DLA LUDNOŚCI I ŚRODOWISKA

CENTRUM KONFERENCYJNE WP Grudzień 2001

Każdego niemal dnia media informują o występujących w różnych częściach naszego globu tragediach spowodowanych klęskami żywiołowymi, katastrofami technicznymi lub ekologicznymi oraz różnego rodzaju epidemiami. Również Polska w ostatnich latach doświadczyła klęski powodzi. Wszystkie te zdarzenia potęgują w nas poczucie zagrożenia bezpieczeństwa, które odgrywa niezmiernie ważną rolę w rozwoju ludzi i społeczeństw.

Poczucie bezpieczeństwa dotyczy wszystkich dziedzin życia i działalności człowieka tworząc wielowymiarowy wektor komfortu psychicznego ludzi „czujących się bezpiecznymi", stąd też i zagrożenia tegoż bezpieczeństwa obejmują całe spektrum zjawisk odbierających ten komfort w poszczególnych dziedzinach życia i działalności, bądź ich różnorodnej konfiguracji. Z większością zagrożeń zmuszeni jesteśmy radzić sobie sami, jednakże są zagrożenia, które przekraczają nie tylko możliwości pojedynczych osób, ale całych społeczeństw. Przeciwdziałanie tym zagrożeniom i usuwanie ich skutków wzbudza w ostatnich latach duże zainteresowanie wśród polityków i decydentów, którzy tym społeczeństwom przewodzą.

Nie ma zatem w dziedzinie bezpieczeństwa powszechnego równie dynamicznego, a zarazem zawiłego zjawiska jak zarządzanie w sytuacjach kryzysowych. Niepewność sytuacji międzynarodowej, konflikty i spory społeczne, przestępczość, awarie techniczne i klęski żywiołowe zmuszają do podejmowania kroków zaradczych w trybie pilnym, często bez dostatecznego przygotowania i zorganizowania się do działania.

Zgodnie z Konstytucją Rzeczypospolitej Polskiej jednym z podstawowych celów funkcjonowania naszego państwa i jego struktur jest zapewnienie bezpieczeństwa bytu i warunków rozwoju obywateli przy jednoczesnym poszanowaniu ich osobistej wolności[1]. Realizacji tego celu służą istniejące w Polsce systemy nastawione na przeciwdziałanie konkretnym zagrożeniom i reagowanie w sytuacjach ich wystąpienia. Utrzymywanie takiego stanu rzeczy przy poszerzaniu się spektrum uświadamianych zagrożeń może skutkować powstawaniem kolejnych systemów przeciwdziałania, a w konsekwencji powodować marnotrawienie wysiłków i zasobów. Dlatego też istnieje potrzeba wypracowania jednego, spójnego systemu przeciwdziałania nadzwyczajnym zagrożeniom, który byłby w stanie sprostać dotychczasowym i mogącym pojawić się w przyszłości nowym wyzwaniom.

---

[1] Artykuł 5 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997r.

Najbardziej widocznym przejawem skuteczności systemu przeciwdziałania nadzwyczajnym zagrożeniom jest system kierowania reagowaniem kryzysowym. Dlatego też niniejsze rozważania i wyniki dotychczasowych badań poświęcone są modelowi systemu kierowania reagowaniem kryzysowym, który mógłby skutecznie działać w przyjętym w Polsce systemie prawnym i ustrojowym.

Analiza systemów kierowania reagowaniem kryzysowym w innych państwach pozwala wnioskować, że zazwyczaj systemy te są tworzone na bazie systemów obrony militarnej i stanowią kolejny etap ich ewolucji. Etap ten został zapoczątkowany stosunkowo niedawno, zwłaszcza w czasie gdy zmalało zagrożenie wojną powszechną, a wzrosło poczucie zagrożenia katastrofami technicznymi i terroryzmem. W dzisiejszym kształcie systemy kierowania reagowaniem kryzysowym nie mają wiele wspólnego z obroną militarną kraju w swojej klasycznej postaci. Jednakże wzrost świadomości społecznej i zdecydowanie lepsze przygotowanie aparatu władzy i administracji do sprawnego kierowania państwem w sytuacjach kryzysowych przyczyniają się do wzrostu potencjału obronnego tych państw.

Filarami, które utrzymują systemy kierowania reagowaniem kryzysowym w poszczególnych państwach, są: system prawny, struktura organizacyjna i edukacja dla bezpieczeństwa.

Struktura prawna tych systemów zazwyczaj składa się z trzech zasadniczych grup aktów prawnych uporządkowanych w sposób hierarchiczny. Najważniejszą grupę stanowią ustawy określające ustrój państwa oraz występujący w nim podział władzy i uprawnienia poszczególnych jej ośrodków oraz akty prawne tworzące system administracji i określające jej podstawowe zadania. Ta część systemu prawnego państwa definiuje strukturę systemu kierowania nim, czyli systemu nadrzędnego w stosunku do systemu kierowania reagowaniem kryzysowym. Określa ona również, chociaż zazwyczaj w sposób bardzo ogólny, podstawowe zadania głównych elementów systemów kierowania państwem w dziedzinie szeroko rozumianego bezpieczeństwa.

Drugą grupę w hierarchii aktów prawnych stanowią ustawy ukierunkowane na przeciwdziałanie nadzwyczajnym zagrożeniom. Tworzą ją dwa, spójne pod względem prawnym, zbiory ustaw. Pierwszy z nich stanowią ustawy kompetencyjne określające zadania poszczególnych organów władzy i administracji w zakresie przeciwdziałania nadzwyczajnym zagrożeniom oraz definiujące rodzaje stanów zagrożenia. Drugi natomiast stanowią akty prawne regulujące problematykę przeciwdziałania poszczególnym rodzajom zagrożeń. Zazwyczaj dotyczą one ochrony przeciwpożarowej, przeciwpowodziowej,

transportu i przechowywania materiałów niebezpiecznych lub cywilizacyjnych zagrożeń nuklearnych. Występowanie w tej grupie dwóch, w pewnym sensie niezależnych zbiorów aktów prawnych jest uwarunkowane historycznie. Pierwszy z nich (ustawy kompetencyjne) powstał w wyniku modyfikacji aktów prawnych dotyczących obrony militarnej danego państwa, wtedy gdy istniały już akty należące do drugiego zbioru i nie było sensu ich zastępować jakimś jednym uniwersalnym aktem, a dokonano jedynie ich modyfikacji w celu zapewnienia spójności systemu prawnego.

Wymienione powyżej dwie grupy aktów prawnych wyczerpują ustawową część struktury systemu prawnego w dziedzinie bezpieczeństwa narodowego. Określają one bowiem kompetencje poszczególnych organów władzy i administracji, zarówno w zakresie kierowania państwem, w sensie ogólnym, jak również w zakresie przeciwdziałania nadzwyczajnym zagrożeniom i kierowania reagowaniem w sytuacjach ich wystąpienia.

Ostatnią grupę tworzą akty wykonawcze do części ustawowej, obejmujące wytyczne i dyrektywy rządowe oraz przygotowane na ich podstawie plany działania w sytuacjach kryzysowych i programy przygotowania społeczeństwa wraz z aparatem władzy i administracji do realizacji opracowanych planów.

Opisany powyżej system prawny determinuje istnienie struktur organizacyjnych w systemie kierowania reagowaniem kryzysowym. Ich tworzenie podporządkowane jest kilku podstawowym zasadom. Pierwsza z nich mówi o zapewnieniu ciągłości systemu kierowania państwem niezależnie od rodzaju zaistniałej sytuacji. Druga wynika z potrzeby zapewnienia wolności i swobody jednostki w państwie demokratycznym i mówi o tym, iż w przypadku zagrożenia reaguje najniższy, kompetentny poziom władzy. Trzecia wynikająca również z podstaw demokracji i stanowiąca uzupełnienie poprzedniej, ogranicza kompetencje szczebla rządowego w sytuacjach nadzwyczajnych zagrożeń dla ludzi i środowiska jedynie do wsparcia władz lokalnych (regionalnych) i udzielania im stosownej do skali zagrożenia pomocy.

Z zasad tych wynika, że tworzone na mocy prawa struktury administracyjne systemu kierowania reagowaniem kryzysowym powstają przy poszczególnych organach władzy w celu pełnienia roli doradczej dla tych organów oraz przygotowywania w ich imieniu i za ich przyzwoleniem, planów reagowania kryzysowego i realizacji programów wdrażających te plany.

Konkretyzując, struktura organizacyjna systemu kierowania reagowaniem kryzysowym oparta jest o ustawowe organy władzy i wydzielone struktury administracyjne stanowiące w sytuacjach zagrożenia rdzeń sztabów kryzysowych tych

organów. Natomiast w czasie braku zagrożeń, te wydzielone struktury administracyjne przygotowują plany reagowania kryzysowego i programy ich wdrażania, dbają o utrzymanie na właściwym poziomie gotowości do reagowania podległych danemu organowi władzy instytucji, służb i struktur administracyjnych oraz stanowią organ opiniodawczy w dziedzinie zapewnienia bezpieczeństwa społeczności, w imieniu której władzę sprawuje dany organ.

Systemy kierowania reagowaniem kryzysowym w innych państwach posiadają jeszcze jedną wspólną, niezmiernie ważną dla zrozumienia ich istoty cechę związaną z traktowaniem bezpieczeństwa jako wspólnego dobra wszystkich obywateli. Takie podejście do problemu uwidacznia się szczególnie w systemie kanadyjskim, gdzie podkreśla się wagę dobrowolnych porozumień pomiędzy departamentami i agencjami rządowymi oraz *Memoranda Zrozumienia*. Również w systemie amerykańskim mówi się o problemie dobrowolnych porozumień na szczeblu lokalnym. Aby można było skutecznie realizować przedsięwzięcie oparte w znacznej mierze na dobrowolności wzajemnej współpracy poszczególnych podmiotów, musi istnieć wspólna platforma tej współpracy. Taką płaszczyznę porozumienia można osiągnąć jedynie w czasie wspólnych szkoleń, ćwiczeń i treningów zmierzających do wymiany i ujednolicania poglądów na kwestie zapewnienia wspólnego dobra jakim jest bezpieczeństwo powszechne obywateli. Stąd też ogromną rolę przywiązuje się do prowadzenia ćwiczeń, treningów i szkoleń na wszystkich szczeblach kierowania państwem angażując w nie również, w niezbędnym zakresie, zwykłych obywateli. Problematyka szkolenia ujmowana jest w programach wdrażania planów reagowania kryzysowego.

Innym ważnym czynnikiem wpływającym na kształt systemu kierowania reagowaniem kryzysowym w Polsce są uwarunkowania wynikające z przynależności do organizacji międzynarodowych w tym do Sojuszu Północnoatlantyckiego oraz podpisanych konwencji i umów międzynarodowych. Analiza dokumentów źródłowych pozwala stwierdzić, że z formalnego punktu widzenia Polska spełnia wymagania wynikające z zaleceń i wytycznych organizacji międzynarodowych oraz ratyfikowanych konwencji międzynarodowych. Pozwala to na podjęcie wspólnych z innymi państwami prac zmierzających do ujednolicania polityki prewencyjnej w zakresie przeciwdziałania nadzwyczajnym zagrożeniom. Problem kompatybilności w tej dziedzinie funkcjonowania państwa z innymi krajami europejskimi jest szczególnie istotny w obecnej sytuacji, kiedy Polska stara się o jak najszybsze wstąpienie do Unii Europejskiej. Jednakże pomimo ogólnego spełnienia tych wymogów w Polsce nadal brak jest krajowego koordynatora

odpowiedzialnego za robocze kontakty z innymi krajami, zarówno w czasie niesienia pomocy innym, jak przyjmowania jej od nich. Wyznaczani „ad hoc" koordynatorzy nie mogą w rzeczywistych warunkach wystąpienia nadzwyczajnych zagrożeń pełnić właściwie swej roli, ponieważ brak im jest pełnego rozeznania, zarówno co do możliwości naszego kraju w zakresie udzielenia pomocy innym, jak i do ewentualnych potrzeb naszego kraju. Ponadto tak wyznaczony koordynator potrzebuje pewnego czasu na właściwe przygotowanie się do pełnienia wyznaczonej mu roli, co powoduje szczególnie w pierwszym, najważniejszym okresie reagowania, chaos organizacyjny. Przykładem takiego stanu rzeczy były ćwiczenia międzynarodowe pod kryptonimem CMX - 98, CRISEX - 98 oraz CMX / CRISEX - 2000, w których Polska brała udział. W każdym z tych ćwiczeń, zarówno koordynator krajowy, jak i koordynator na szczeblu Ministerstwa (resortu) był indywidualnie wyznaczany ad hoc, co dowodzi brak stałych koordynatorów. O ile w ćwiczeniu wcześniej przygotowanym można sobie pozwolić na takie posunięcie, ponieważ wyznaczony koordynator ma czas na przygotowanie się do pełnienia wyznaczonej mu roli o tyle w sytuacjach rzeczywistych jest to niedopuszczalne.

Wnioski płynące z analizy systemów kierowania reagowaniem kryzysowym w innych państwach i systemu prawno - ustrojowego obowiązującego w Polsce prowadzą do twierdzenia, że do kierowania reagowaniem kryzysowym w sytuacjach nadzwyczajnych zagrożeń powinny być przygotowane wszystkie organy i szczeble administracji rządowej i samorządowej oraz przedsiębiorcy władający niebezpiecznymi instalacjami, każdy w zakresie swoich kompetencji. Powszechność odpowiedzialności za wspólne dobro jakim jest bezpieczeństwo nie może jednak oznaczać chaosu. Dlatego też, muszą istnieć ośrodki odpowiedzialne za koordynację, zarówno przygotowań do reagowania w sytuacjach kryzysowych, jak i samego procesu reagowania na zagrożenia. Zgodnie z polskim prawodawstwem oraz terytorialnością[2] nadzwyczajnych zagrożeń najlepszym rozwiązaniem jest przypisanie roli koordynatora systemu kierowania reagowaniem kryzysowym najwyższemu organowi władzy wykonawczej na danym obszarze. Organami tymi, w myśl polskiego ustawodawstwa, są:

- Zarząd Gminy,
- Zarząd Powiatu,
- Wojewoda,
- Rada Ministrów.

---

[2] Nadzwyczajne zagrożenia są zawsze ściśle związane z obszarem, na którym występują. Nie są to zagrożenia obejmujące tylko wybrane grupy społeczne, ale wszystkich mieszkańców danego terytorium, bez względu na jego wielkość oraz strukturę społeczeństwa.

Jak łatwo zauważyć w trzech przypadkach są to ciała kolegialne, co stoi w sprzeczności z często postulowaną zasadą jednoosobowego kierownictwa i odpowiedzialności za kierowanie reagowaniem kryzysowym. Należy jednak zauważyć, że organy te pełnią rolę koordynatorów, a nie bezpośrednio kierujących akcją zwalczania zagrożenia lub usuwania jego skutków.

Kierowanie obejmuje trzy procesy informacyjne:

1. Zbierania i przetwarzania informacji w celu uzyskania jak najbardziej wiernego obrazu dziejącej się rzeczywistości oraz kierunków i zakresu rozwoju sytuacji, a ponadto właściwej dystrybucji tych informacji.
2. Opracowania i analizowania różnych koncepcji działania, możliwych do realizacji w danych warunkach.
3. Decydowania, którą z wypracowanych koncepcji uznać za najbardziej optymalną i wdrożyć do realizacji.

Procesy te determinują sposób działania organu kierowania, a tym samym wpływają na jego wewnętrzną strukturę (rys. 2).

Elementem decyzyjnym w prezentowanej strukturze jest organ władzy wykonawczej i nie ma znaczenia dla istoty sprawy czy jest on organem jednoosobowym czy też ciałem kolegialnym. Natomiast funkcję informacyjną i sztabową realizuje urząd obsługujący decydenta (ciało decyzyjne). Oczywistą sprawą jest, że cały urząd nie może zajmować się przeciwdziałaniem nadzwyczajnym zagrożeniom. Stąd też konieczne jest powołanie w każdym urzędzie komórki lub stanowiska odpowiedzialnego za przygotowanie urzędu do kierowania reagowaniem kryzysowym oraz inicjowania tego procesu, kiedy zajdzie konieczność. Wielkość tych komórek uwarunkowana jest z jednej strony potrzebami, z drugiej zaś kosztami utrzymania.

W czasie normalnego funkcjonowania danej społeczności, gdy brak jest odczuwalnych zagrożeń, komórka ds. zarządzania kryzysowego może być niewielka lub zgoła jednoosobowa i rozszerzać się odpowiednio do rozwoju sytuacji (zagrożeń). W momencie dostrzeżenia pojawiających się zagrożeń szczególnego znaczenia nabiera w niej element informacyjny, który powinien zwiększyć swą efektywność oraz element sztabowy, który już w tej fazie powinien przygotowywać różne koncepcje działania adekwatne do prawdopodobnych scenariuszy rozwoju sytuacji.

W miarę narastania zagrożenia i rozwoju sytuacji w kierunku kryzysu efektywność funkcjonowania elementu informacyjnego i sztabowego musi dość gwałtownie rosnąć, osiągając maksimum swoich możliwości bezpośrednio przed wejściem sytuacji w fazę

kryzysu. Oczywiście wzrost efektywności ściśle jest związany z obsadą osobową tej komórki i stopniem jej uzbrojenia w narzędzia niezbędne do sprawnego i efektywnego przetwarzania informacji w celu uzyskania możliwie najbardziej wiarygodnego obrazu dziejącej się rzeczywistości, co stanowi podstawę trafności podejmowanych decyzji.

Reasumując, kierowanie reagowaniem kryzysowym wymaga wzrostu sprawności i efektywności działania organu kierowania w porównaniu z okresami funkcjonowania danego urzędu w sytuacjach stabilnych.

Nadzwyczajne zagrożenia można podzielić, przyjmując jako kryterium podziału zasięg ich oddziaływania, na trzy grupy:

- o ograniczonym zasięgu, czyli występujące na pewnym ograniczonym obszarze lub odnoszące się do wyodrębnionej dziedziny funkcjonowania państwa i nie powodujące powstania sytuacji kryzysowych poza tym obszarem lub dziedzinami;
- rozprzestrzeniające się, czyli stopniowo przeradzające się z sytuacji kryzysowych o ograniczonym zasięgu w sytuacje ogólnokrajowe;
- zasięgu ogólnokrajowym, czyli takie, które od samego początku ich zaistnienia obejmują znaczną część kraju lub większą część dziedzin jego funkcjonowania.

Wyodrębnione grupy sytuacji kryzysowych stanowią dobre tło do ukazania istoty funkcjonowania aparatu kierowania reagowaniem kryzysowym oraz roli jaką pełnią poszczególne jego szczeble (rys. 3).

W sytuacjach o ograniczonym zasięgu główny ciężar opanowywania sytuacji kryzysowych spoczywa na organach zarządzających danym obszarem lub dziedziną funkcjonowania państwa. Natomiast zadaniem organów wyższego (nadrzędnego) szczebla jest śledzenie rozwoju sytuacji oraz w miarę potrzeby wspieranie organów, aktualnie kierujących reagowaniem, siłami, środkami i zasobami będącymi w dyspozycji wyższego szczebla. Głównym celem działania nadrzędnych organów kierowania reagowaniem kryzysowym jest niedopuszczenie do rozprzestrzenienia się sytuacji kryzysowej poprzez takie wspieranie organów kierujących reagowaniem kryzysowym, aby mogły ją opanować. Organ nadrzędny nie powinien, bez wyraźnej potrzeby, przejmować kierowania reagowaniem w takiej sytuacji, ponieważ przejęcie reagowania zdejmuje również ciężar odpowiedzialności z organu niższego szczebla, a co za tym idzie nie sprzyja pogłębianiu jego wiedzy i doświadczenia, które jest podstawą sprawnego i skutecznego działania.

Można by takie rozważania uważać za nie racjonalne, ponieważ szczebel nadrzędny dysponując większymi możliwościami może łatwiej zapanować nad sytuacją.

Jednakże należy zwrócić uwagę na fakt, iż rozważany jest aparat kierowania reagowaniem kryzysowym, a nie jeden centralny organ odpowiedzialny za realizację tego zadania. Ponadto mogą zdarzyć się sytuacje, w których niezbędna będzie wytężona praca wszystkich szczebli, a wtedy doświadczenie i wiedza organów niższego szczebla zdobyte w trakcie opanowywania sytuacji rozpatrywanego typu zaowocuje zdecydowanie większą skutecznością całego aparatu kierowania reagowaniem kryzysowym.

W rozprzestrzeniających się sytuacjach kryzysowych rola nadrzędnych organów zarządzania kryzysowego w pierwszej fazie ich rozwoju, kiedy mają one ograniczony zasięg, jest podobna do opisanej powyżej. W fazie tej, im skuteczniej będą działać organy kierowania niższych szczebli tym więcej czasu będzie posiadał organ nadrzędny na przygotowanie się do przejęcia zarządzania rozwijającą się sytuacją, a tym samym łatwiej będzie mógł ją opanować.

W obydwu zaprezentowanych typach sytuacji kryzysowych bardzo ważna jest skuteczność działania aparatu kierowania najniższych szczebli, ponieważ od niej zależy czy dana sytuacja kryzysowa przeniesie się na inne obszary oraz jak długo będzie trwała. To one są odpowiedzialne za sprawne i szybkie opanowanie takich sytuacji. Nieco inną rolę w tych sytuacjach kryzysowych pełni aparat kierowania wyższych szczebli. Polega on na zapewnieniu doradztwa, pomocy technicznej i finansowej oraz koordynacji, a przede wszystkim na tworzeniu prawa, koncepcji i programów reagowania w sytuacjach kryzysowych oraz nadzorowaniu ich wdrażania. Na wyższych poziomach kierowania reagowaniem kryzysowym będzie organizowana pomoc szczeblom niższym, wtedy kiedy sytuacja powstała w wyniku zagrożenia przerasta ich możliwości.

Zdecydowanie odmienna, od przedstawionej, jest rola najwyższych szczebli kierowania reagowaniem kryzysowym w sytuacjach kryzysowych o zasięgu ogólnokrajowym. Przy tego typu zagrożeniach aparat kierowania reagowaniem kryzysowym rozwijany jest stopniowo od najwyższego do najniższego szczebla. Przeciwnie niż w poprzednio opisanych sytuacjach, w których aparat ten rozwijany był od najniższego do najwyższego szczebla. Ponadto w czasie występowania ogólnokrajowych zagrożeń najwyższy szczebel kierowania reagowaniem kryzysowym nie tylko rozwija się jako pierwszy, ale przede wszystkim steruje rozwijaniem niższych szczebli tego aparatu oraz określa i precyzuje zadania niezbędne do realizacji przez szczeble niższe. W sytuacjach tych szczebel nadrzędny pełni rolę koordynatora przygotowań całego systemu do reagowania kryzysowego i w rezultacie kieruje nim.

Podstawową właściwością polskiego systemu ustrojowego jest to, że najwyższym organem wykonawczym jest ciało kolegialne jakim jest Rada Ministrów. Natomiast poszczególni ministrowie, a tym bardziej organy centralne mają ograniczone możliwości oddziaływania na instytucje szczebla terenowego. Władza wykonawcza oparta na ciałach kolegialnych występuje również na niższych szczeblach – gminnym i powiatowym.

Zasadniczym zatem problemem jest budowa organu kierowania reagowaniem kryzysowym opartego na kolegialnym organie zarządzania państwem. Rozwiązanie tego problemu można znaleźć w raporcie studyjnym z ćwiczenia CMX/CRISEX 2000. Autorzy tego raportu proponują (rys. 4), aby wymaganą w funkcjonowaniu Rady Ministrów kolegialność zapewnić przez utworzenie w ramach systemu krajowego stałego komitetu Rady Ministrów do spraw Zarządzania w Sytuacjach Kryzysowych. Celem działania komitetu powinno być analizowanie sytuacji bezpieczeństwa, uzgadnianie stanowisk członków Rady Ministrów, inicjowanie, przygotowywanie i przedstawianie Radzie Ministrów oraz jej prezesowi projektów rozstrzygnięć, opinii lub udzielania rekomendacji w sprawie sposobu zapobiegania lub rozwiązywania kryzysu.

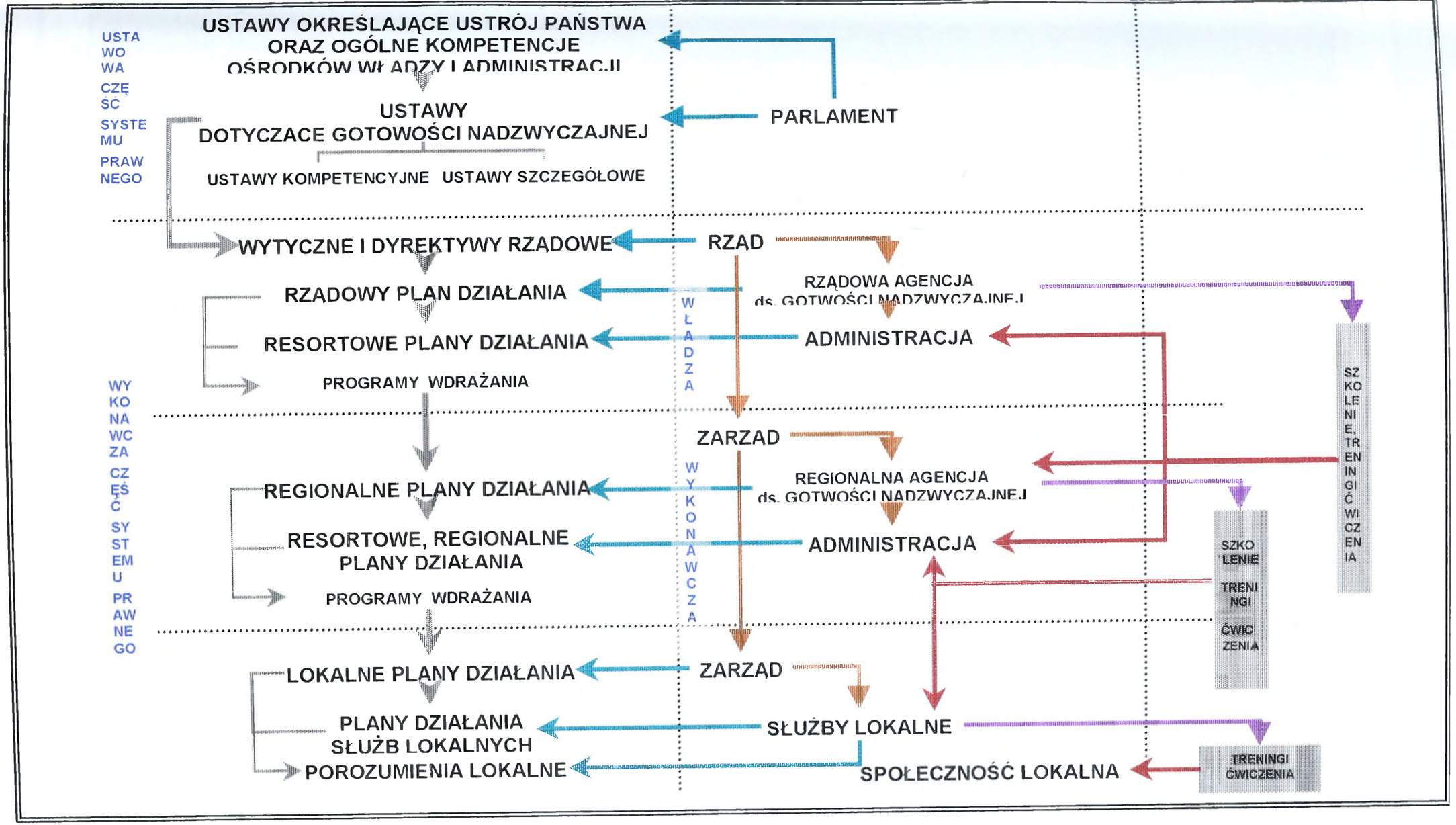
Podsumowując należy stwierdzić, że:

1. W Polsce należy budować trójszczeblowy aparat kierujący reagowaniem kryzysowym, adekwatnie do występującej struktury władzy wykonawczej i administracji.
2. Komórkę do spraw zarządzania kryzysowego, przeznaczoną do pełnienia roli sztabu w czasie reagowania kryzysowego, należy sytuować przy szefie władzy wykonawczej danego szczebla.
3. Każdy szczebel aparatu kierowania reagowaniem kryzysowym powinien posiadać jak największą autonomię w tworzeniu własnych struktur związanych z zarządzaniem kryzysowym, wynikającą ze stopnia niezależności danego szczebla kierowania państwem.
4. Możliwości eskalacji zagrożeń i implikacji przez dane zagrożenie innych wymusza tworzenie jednego aparatu kierowania reagowaniem kryzysowym dla wszelkich możliwych do przewidzenia sytuacji zagrożeń.
5. Poszczególne szczeble aparatu kierowania reagowaniem kryzysowym powinny być przygotowane do zarządzania w sytuacjach kryzysowych mogących wystąpić na ich poziomie oraz przygotowywać podległe instytucje do reagowania w takich sytuacjach i narzędzia reagowania kryzysowego.

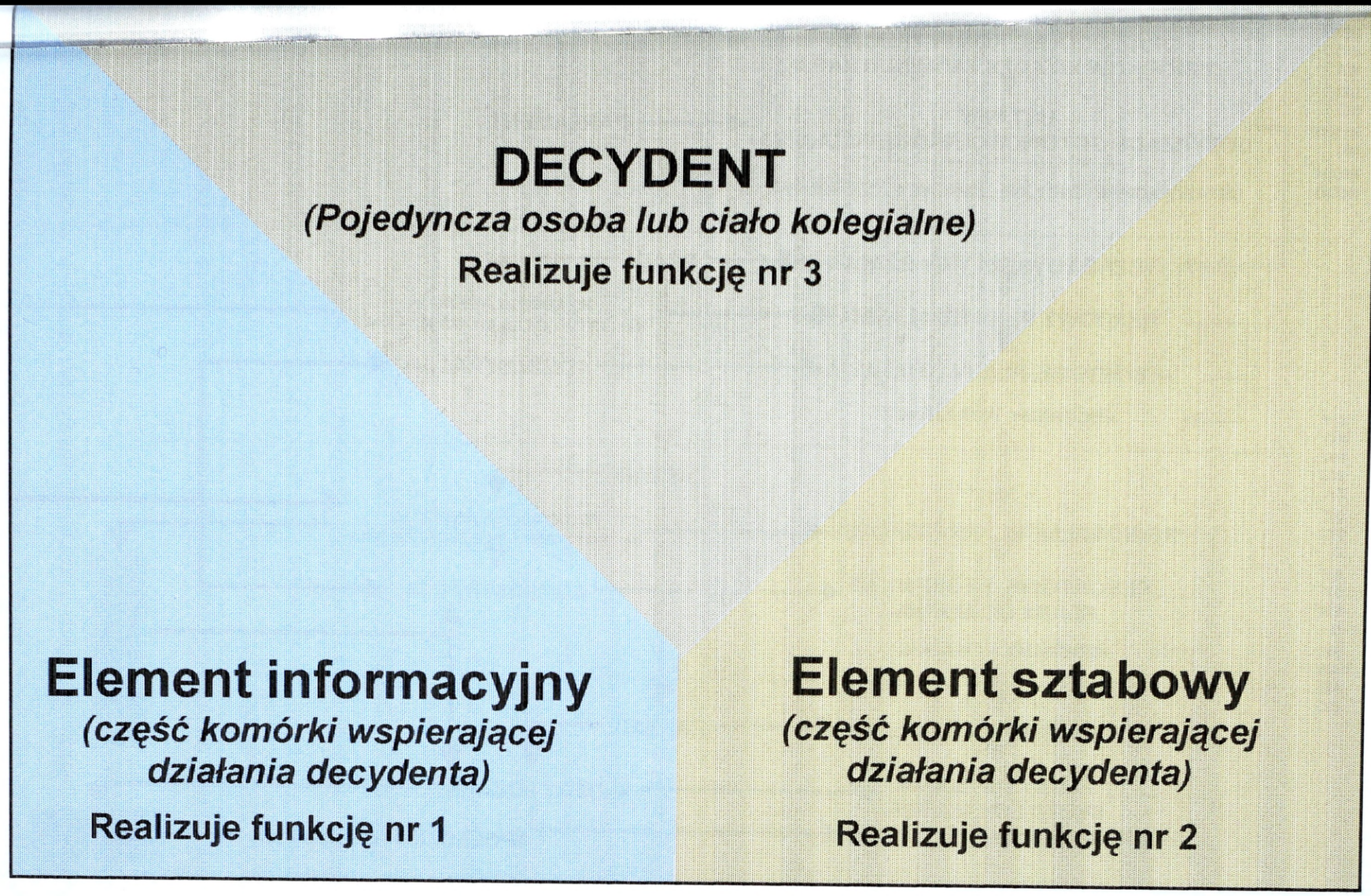
6. Organ kierowania reagowaniem kryzysowym pełni rolę doradczą w stosunku do organów niższego szczebla, w zakresie przygotowania ich do reagowania w sytuacjach zagrożeń adekwatnych dla tych szczebli, ponadto musi być przygotowany do udzielenia pomocy w siłach, środkach i zasobach szczeblom niższym w czasie ich reagowania na zagrożenia.

Przedstawiony model nie reprezentuje całego systemu reagowania kryzysowego w sytuacjach nadzwyczajnych zagrożeń, a jedynie jego część tworzącą podsystem kierowania reagowaniem kryzysowym. Jednakże owa część jest filarem na którym można zbudować cały system. Analiza aktów prawnych prowadzi do wniosku, iż w Polsce całkiem sprawnie funkcjonują pewne elementy systemu reagowania kryzysowego, zwłaszcza organy wykonawcze, natomiast system kierowania tym reagowaniem jest mało sprawny i nie spójny.

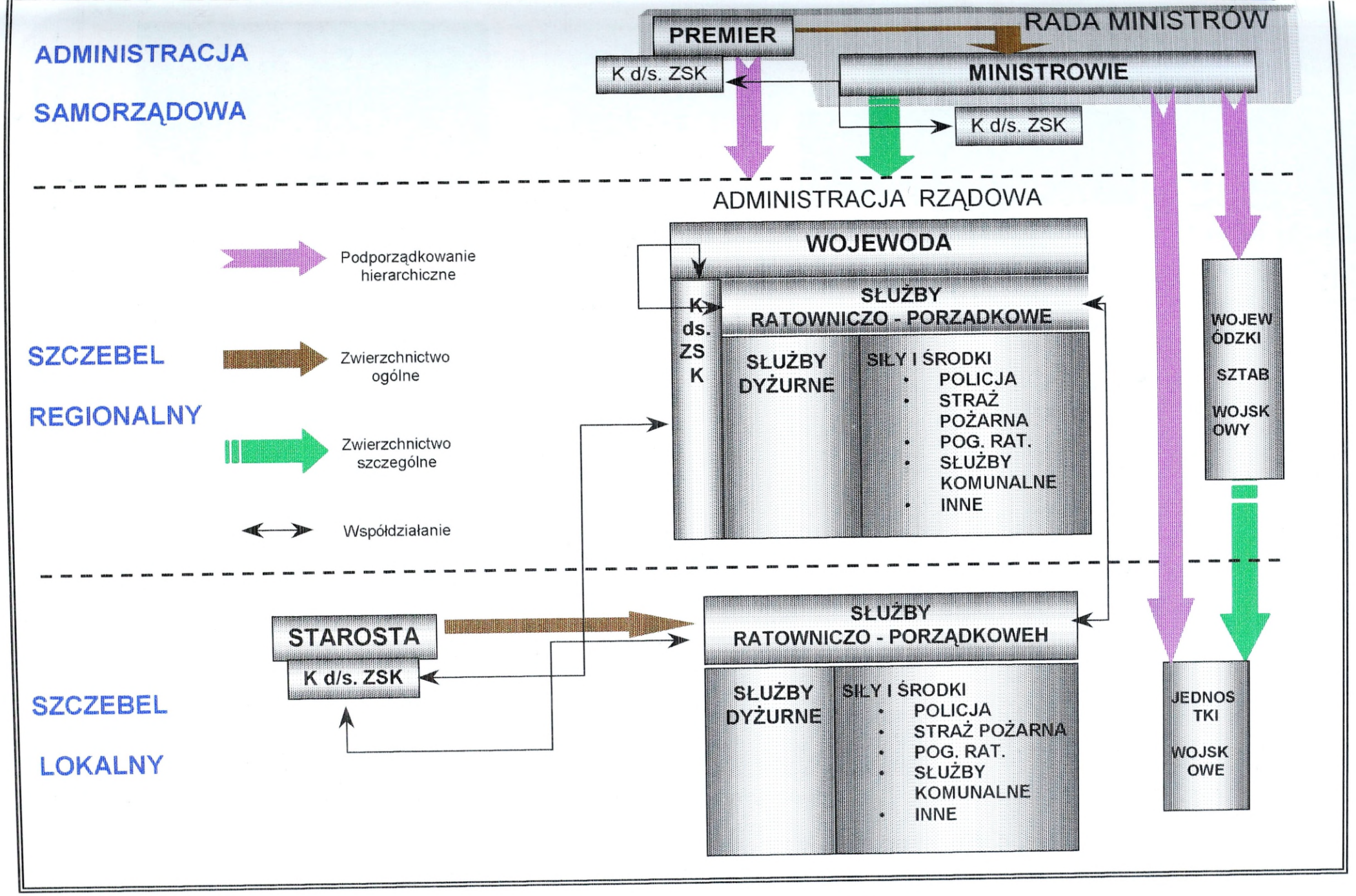
Przeprowadzone dotychczas badania uwidoczniły możliwość zbudowania nowoczesnego i skutecznego systemu kierowania reagowaniem kryzysowym uwzględniającego zobowiązania międzynarodowe Polski. Tworząc taki system należy znowelizować obowiązujące przepisy prawne oraz przyjąć i wprowadzić w życie ustawę kompetencyjną w dziedzinie bezpieczeństwa. Kolejnym krokiem w jego tworzeniu byłoby prowadzenie intensywnych szkoleń dla personelu odpowiedzialnego za tę problematykę na poszczególnych szczeblach administracji rządowej i samorządowej oraz przygotowanie przez każdy szczebel kierowania państwem, stosownie do kompetencji, wytycznych, planów i programów ich wdrażania. Zbudowany i scalony w ten sposób system kierowania reagowaniem kryzysowym w sytuacjach nadzwyczajnych zagrożeń w sposób samoistny i permanentny rozwijałby się zapewniając całemu społeczeństwu coraz większe poczucie bezpieczeństwa.



Rys. 1. Ogólna struktura systemu kierowania reagowaniem kryzysowym

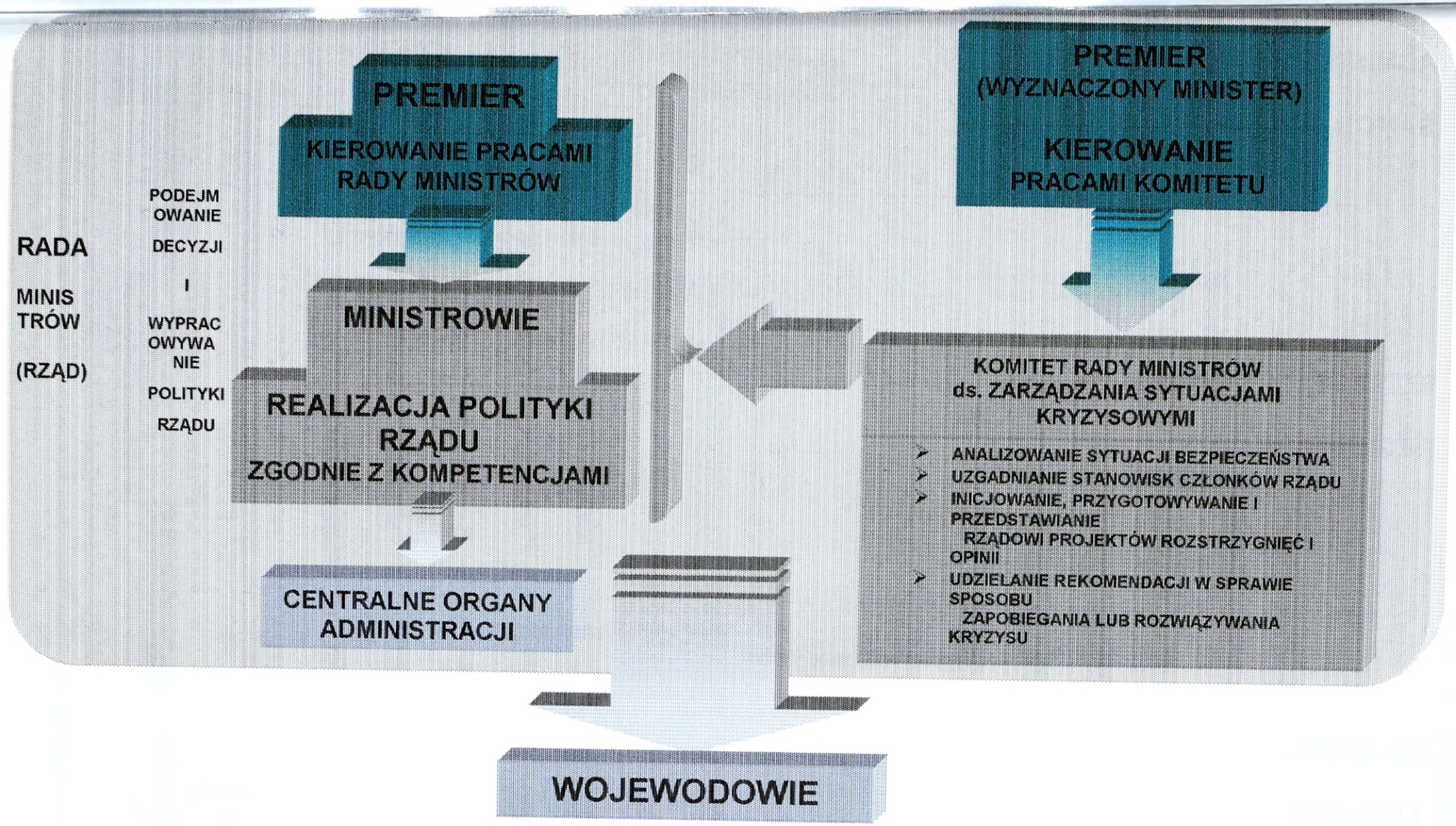


Rys. 2. Model organu kierowania reagowaniem kryzysowym



Rys. 3. Idea aparatu kierowania reagowaniem kryzysowym

(skrót ds. ZSK oznacza komórkę do spraw zarządzania kryzysowego)



Rys. 4. Model aparatu kierowania reagowaniem kryzysowym na szczeblu centralnym
(wg autorów raportu studyjnego z ćwiczenia CMX/CRISEX 2000)

WOJSKOWA
AKADEMIA TECHNICZNA

Grzegorz RÓŻAŃSKI

ROLA INFRASTRUKTURY TECHNICZNEJ W ZABEZPIECZENIU FUNKCJONOWANIA SYSTEMÓW INFORMACYJNYCH W STANACH NADZWYCZAJNYCH

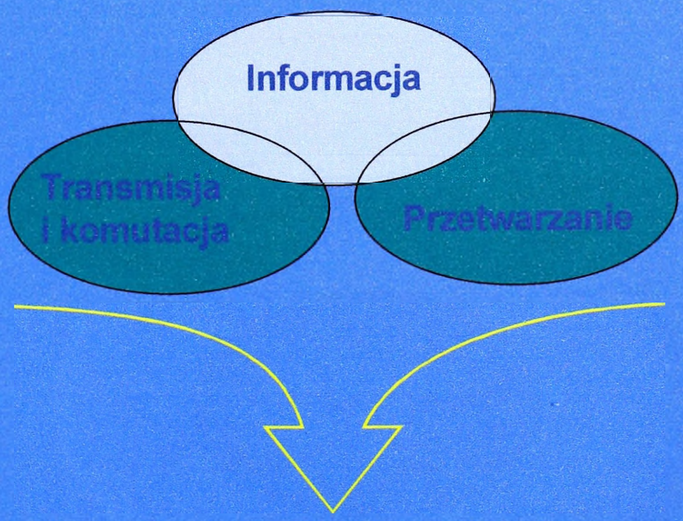
CENTRUM KONFERENCYJNE WP Grudzień 2001

Grzegorz RÓŻAŃSKI

ROLA INFRASTRUKTURY TECHNICZNEJ W ZABEZPIECZENIU FUNKCJONOWANIA SYSTEMÓW INFORMACYJNYCH W STANACH NADZWYCZAJNYCH

Wydział Elektroniki
Wojskowej Akademii Technicznej

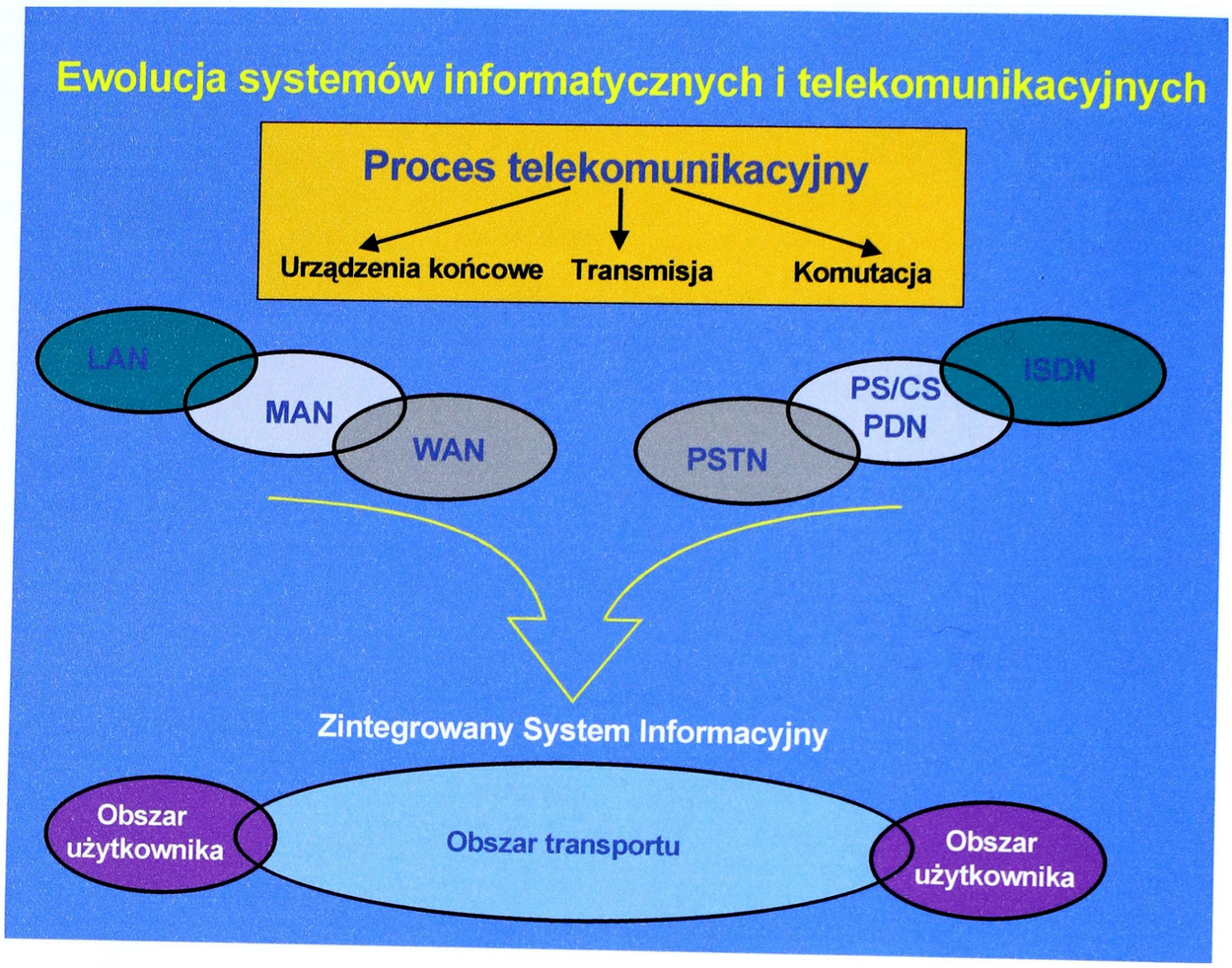
Technologia informacyjna i jej atrybuty

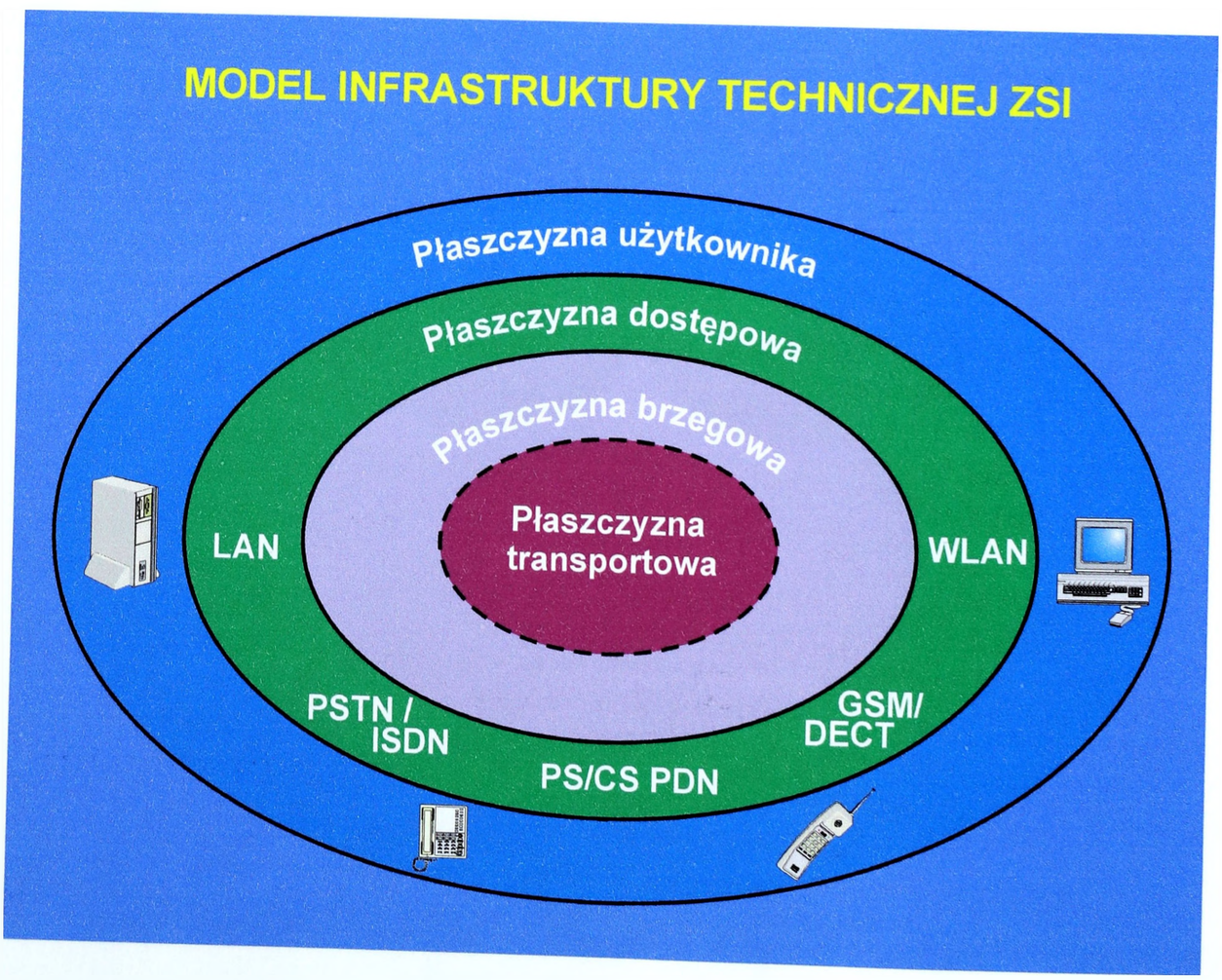


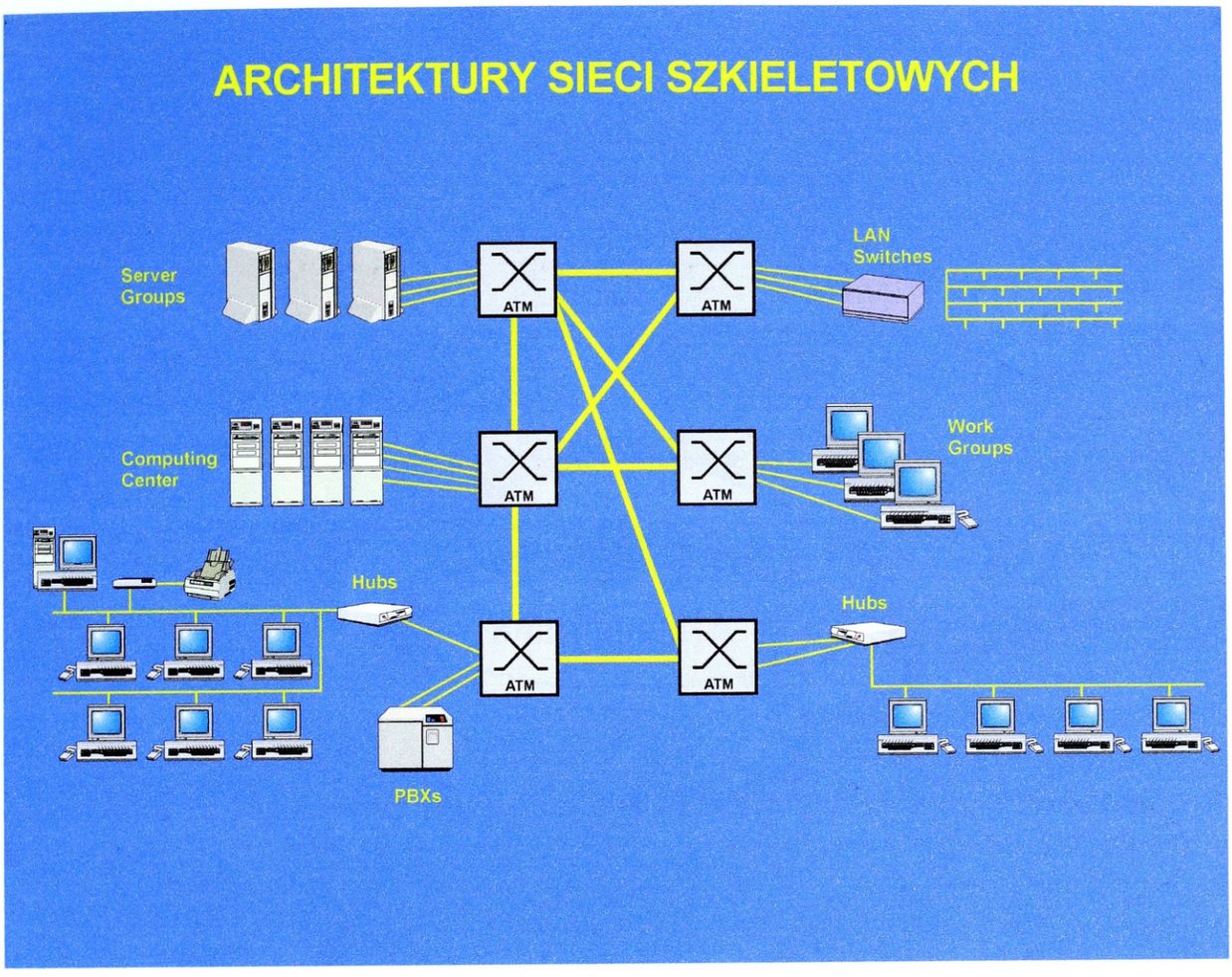
System informacyjny w sytuacjach nadzwyczajnych

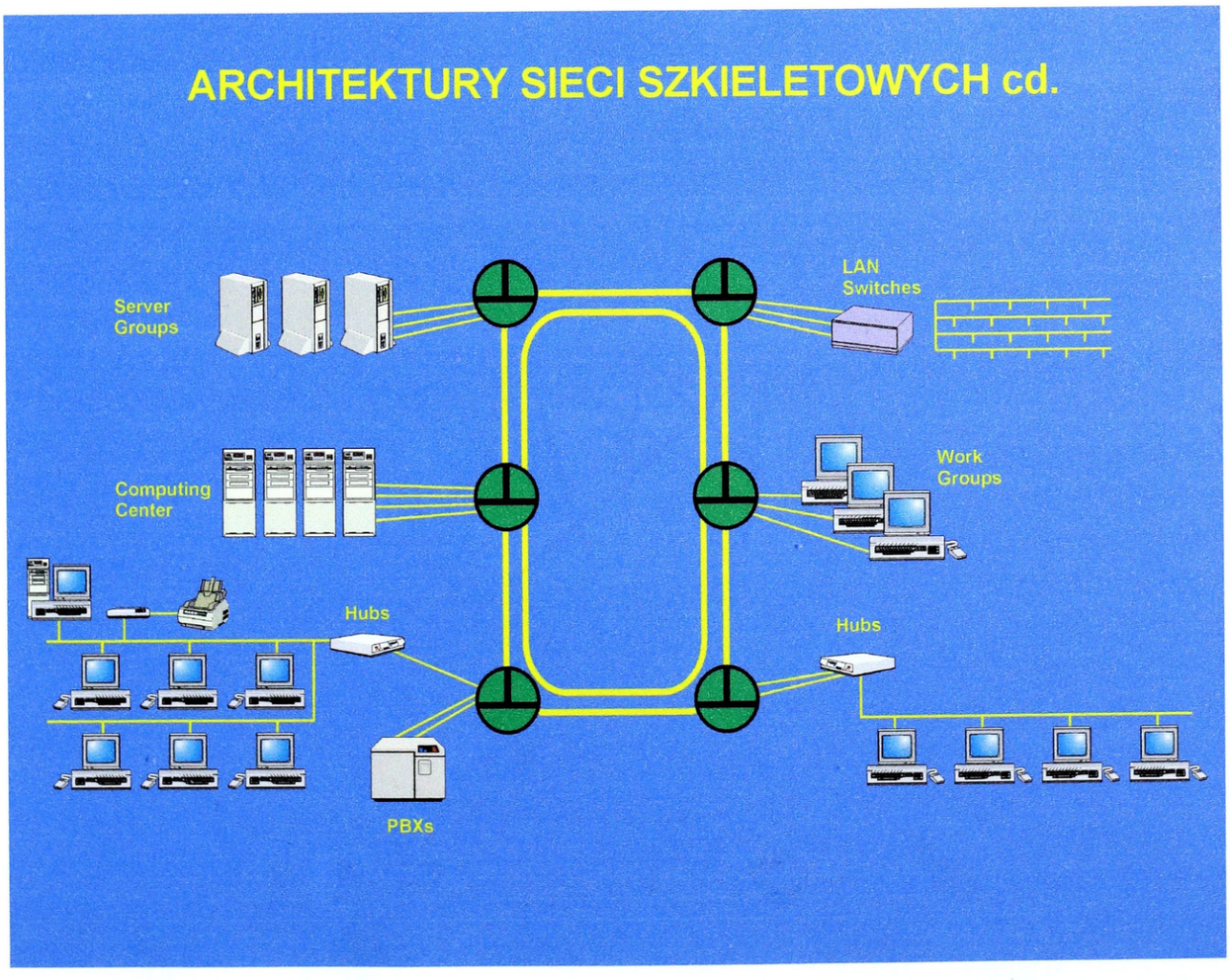
cel: Kierowanie, dowodzenie i zarządzanie

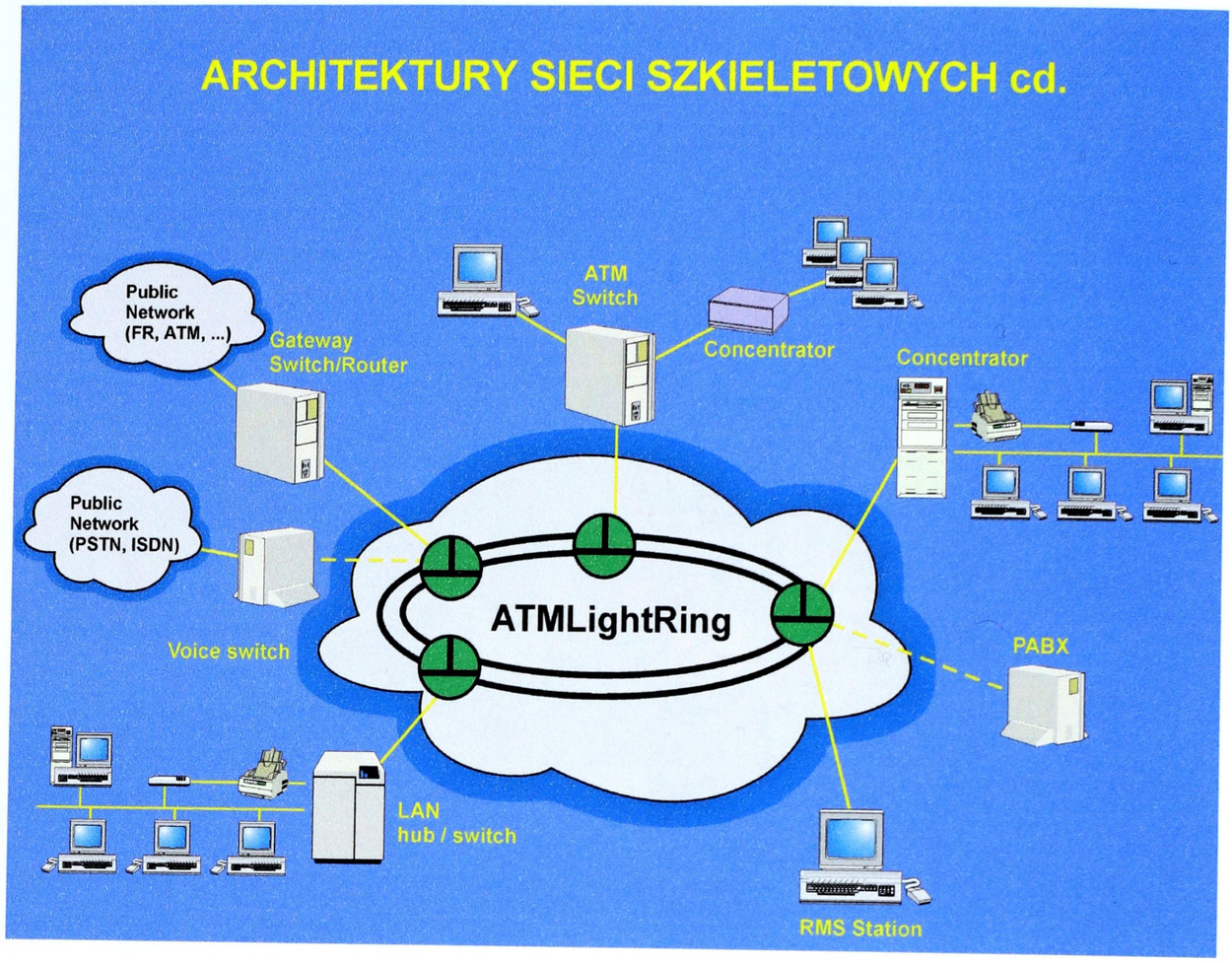
środki: Zintegrowany System Telekomunikacyjny i Informatyczny (CIS)

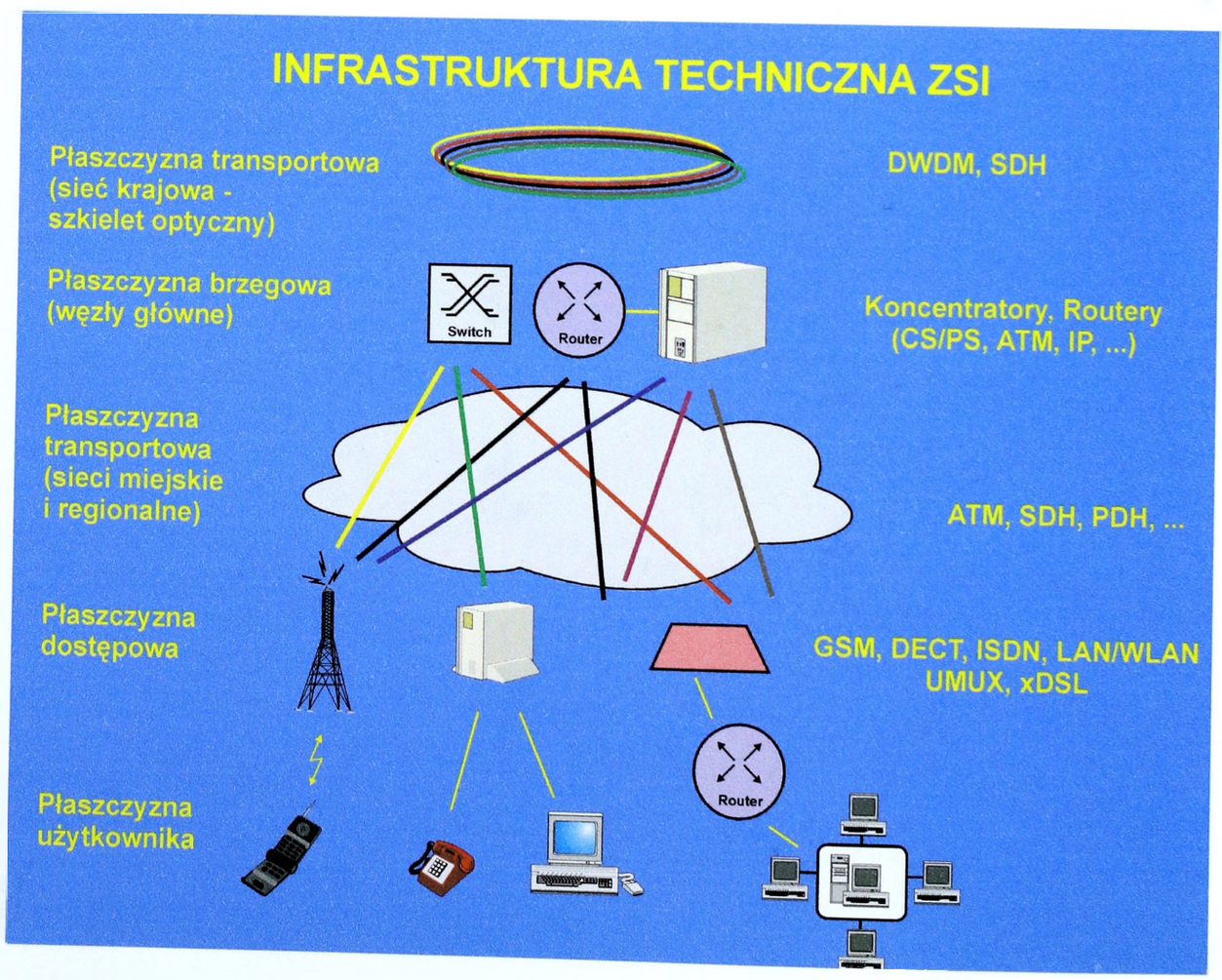

Ewolucja systemów informatycznych i telekomunikacyjnych
Proces telekomunikacyjny
Urządzenia końcowe
Transmisja
Komutacja
LAN
MAN
WAN
PSTN
PS/CS PDN
ISDN
Zintegrowany System Informacyjny
Obszar użytkownika
Obszar transportu
Obszar użytkownika

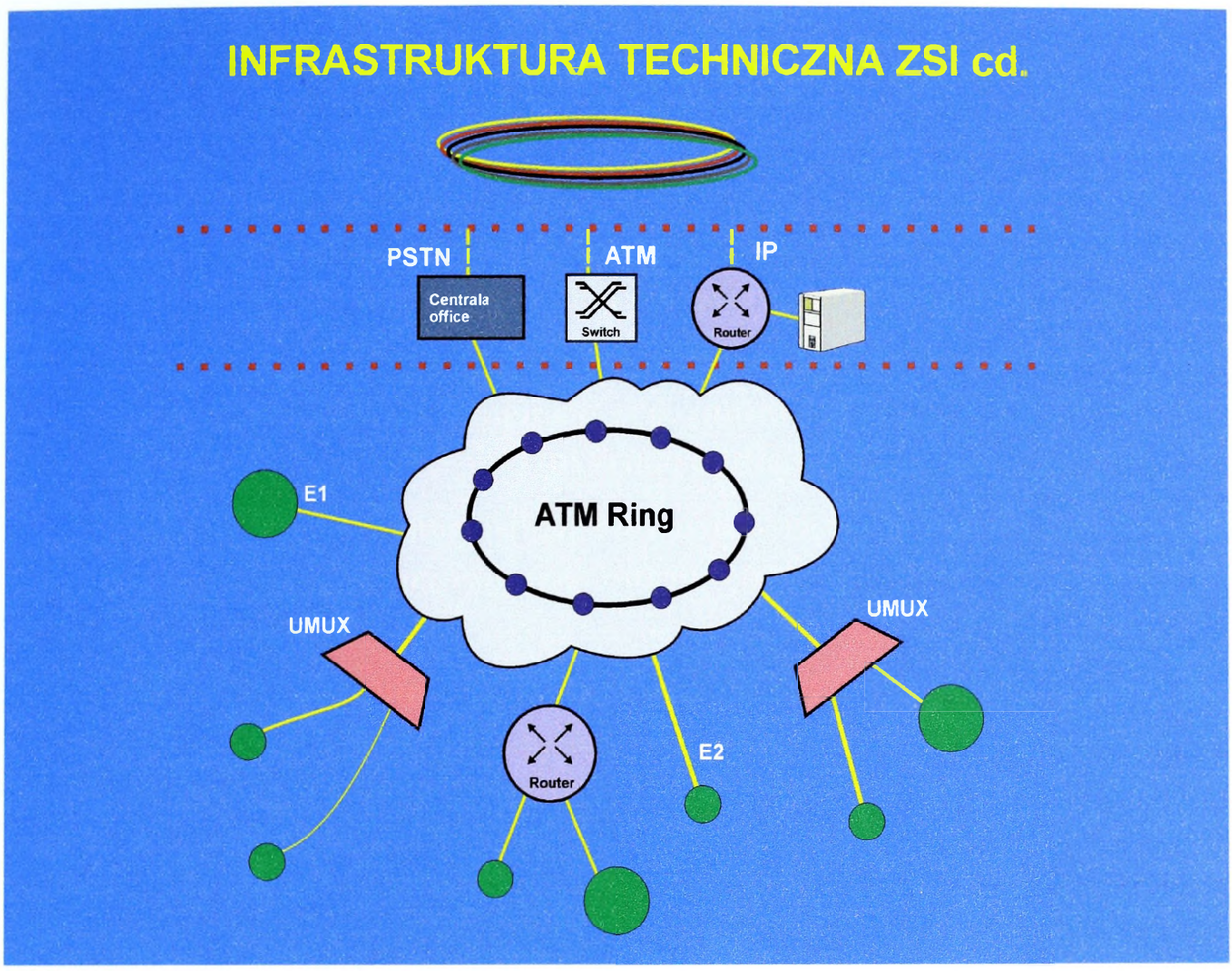

MODEL INFRASTRUKTURY TECHNICZNEJ ZSI
Płaszczyzna użytkownika
Płaszczyzna dostępowa
Płaszczyzna brzegowa
Płaszczyzna transportowa
LAN
WLAN
PSTN / ISDN
GSM/ DECT
PS/CS PDN

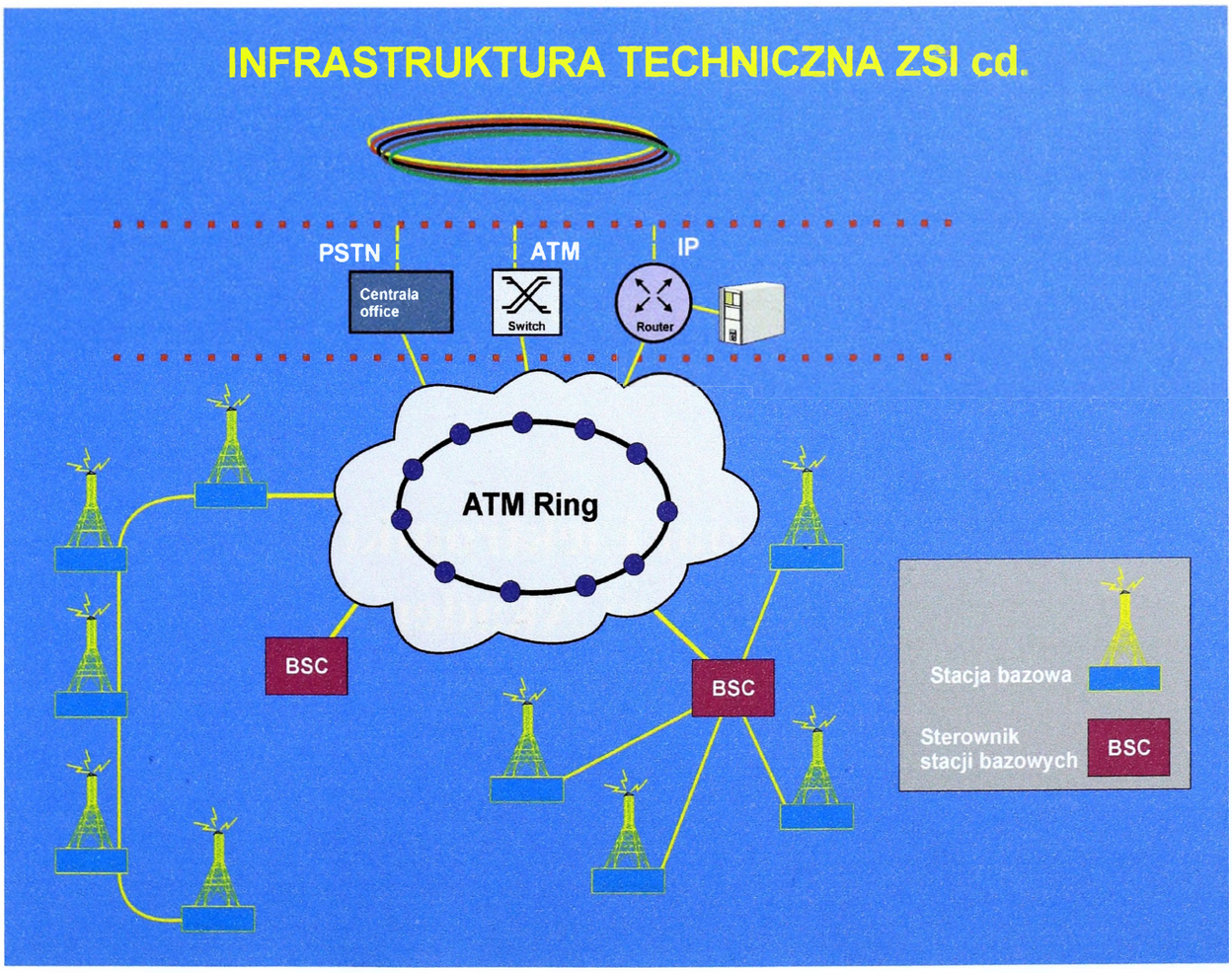

ARCHITEKTURY SIECI SZKIELETOWYCH
Server Groups
Computing Center
Hubs
PBXs
ATM
ATM
ATM
ATM
ATM
LAN Switches
Work Groups
Hubs


ARCHITEKTURY SIECI SZKIELETOWYCH cd.
Server Groups
Computing Center
Hubs
PBXs
LAN Switches
Work Groups
Hubs


ARCHITEKTURY SIECI SZKIELETOWYCH cd.
Public Network (FR, ATM, ...)
Gateway Switch/Router
ATM Switch
Concentrator
Concentrator
Public Network (PSTN, ISDN)
ATMLightRing
Voice switch
PABX
LAN hub / switch
RMS Station


INFRASTRUKTURA TECHNICZNA ZSI
Płaszczyzna transportowa (sieć krajowa - szkielet optyczny)
DWDM, SDH
Płaszczyzna brzegowa (węzły główne)
Switch
Router
Koncentratory, Routery (CS/PS, ATM, IP, ...)
Płaszczyzna transportowa (sieci miejskie i regionalne)
ATM, SDH, PDH, ...
Płaszczyzna dostępowa
GSM, DECT, ISDN, LAN/WLAN UMUX, xDSL
Router
Płaszczyzna użytkownika


INFRASTRUKTURA TECHNICZNA ZSI cd.
PSTN
ATM
IP
Centrala office
Switch
Router
E1
ATM Ring
UMUX
UMUX
Router
E2


INFRASTRUKTURA TECHNICZNA ZSI cd.
PSTN
ATM
IP
Centrala office
Switch
Router
ATM Ring
BSC
BSC
Stacja bazowa
Sterownik stacji bazowych
BSC

WNIOSKI I UWAGI

⇒ Technologia informacyjna stanowi podstawę do organizacji i projektowania systemów informacyjnych dla kierowania obronnością państwa w stanach nadzwyczajnych.

⇒ Infrastruktura techniczna systemów informacyjnych musi bazować na rozwiązaniach stosowanych w projektowaniu systemów telekomunikacyjnych i informatycznych.

⇒ Szerokopasmowe sieci szkieletowe realizowane w technice ATM/IP są podstawowymi architekturami technicznymi płaszczyzny transportowej.

⇒ Istotne znaczenie w organizacji i projektowaniu architektur ZSI w płaszczyznach: użytkownika i dostępowej odgrywają bezprzewodowe systemy informacyjne, szczególnie w organizacji tzw. systemów "ad-hoc".

Grzegorz
RÓŻAŃSKI

Wydział Elektroniki
Wojskowej Akademii
Technicznej

SZTAB GENERALNY WP
ZARZĄD
ŁĄCZNOŚCI I INFORMATYKI

Wojciech WOJCIECHOWSKI
Marek ŻOCHOWSKI

ZARZĄDZANIE INFRASTRUKTURĄ TELEINFORMATYCZNĄ SIŁ ZBROJNYCH RP W STANACH NADZWYCZAJNYCH

CENTRUM KONFERENCYJNE WP Grudzień 2001

Sztab Generalny Wojska Polskiego

Zarząd Łączności i Informatyki

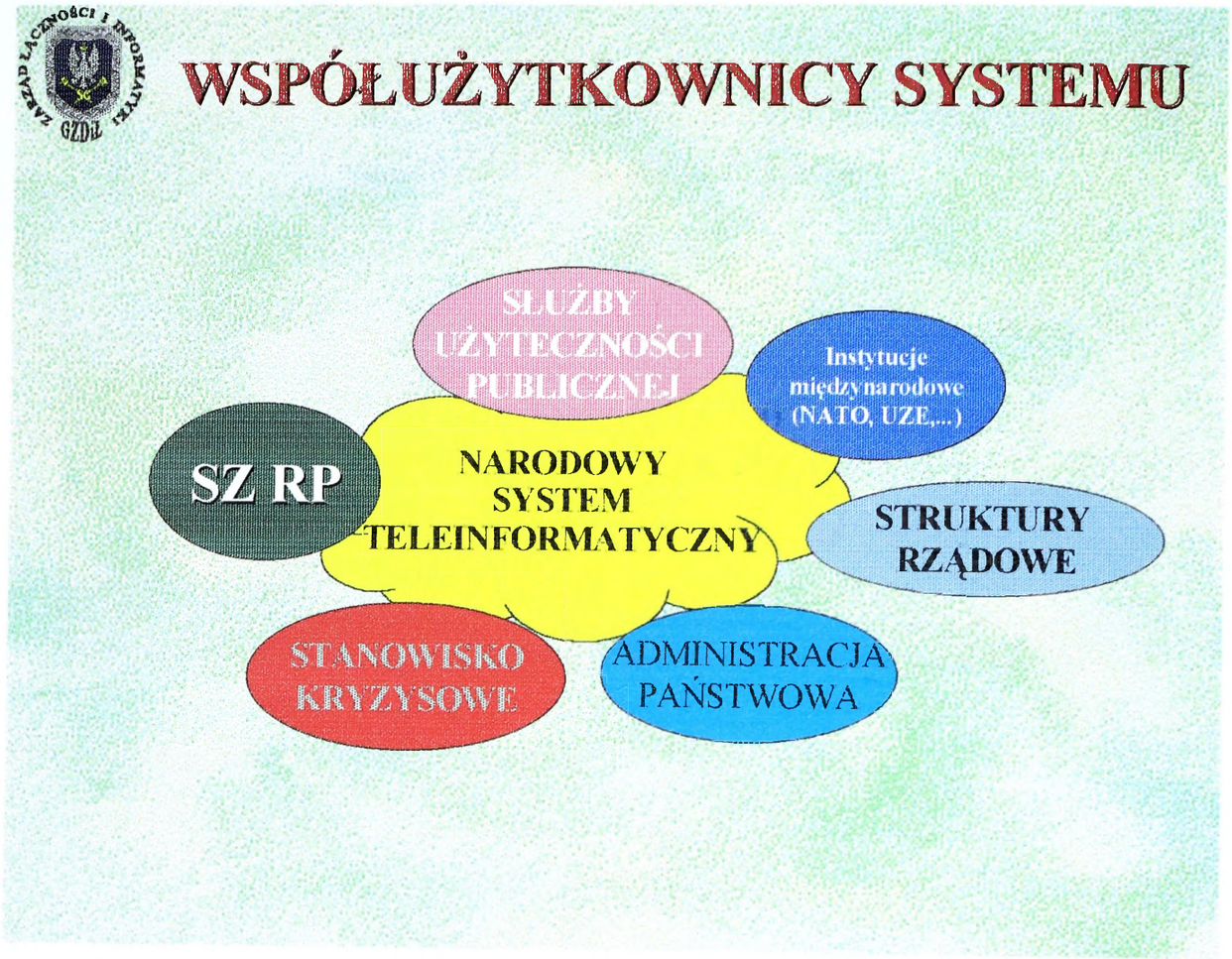
KONCEPCJA ZARZĄDZANIA INFRASTRUKTURĄ TELEINFORMATYCZNĄ SIŁ ZBROJNYCH W STANACH NADZWYCZAJNYCH

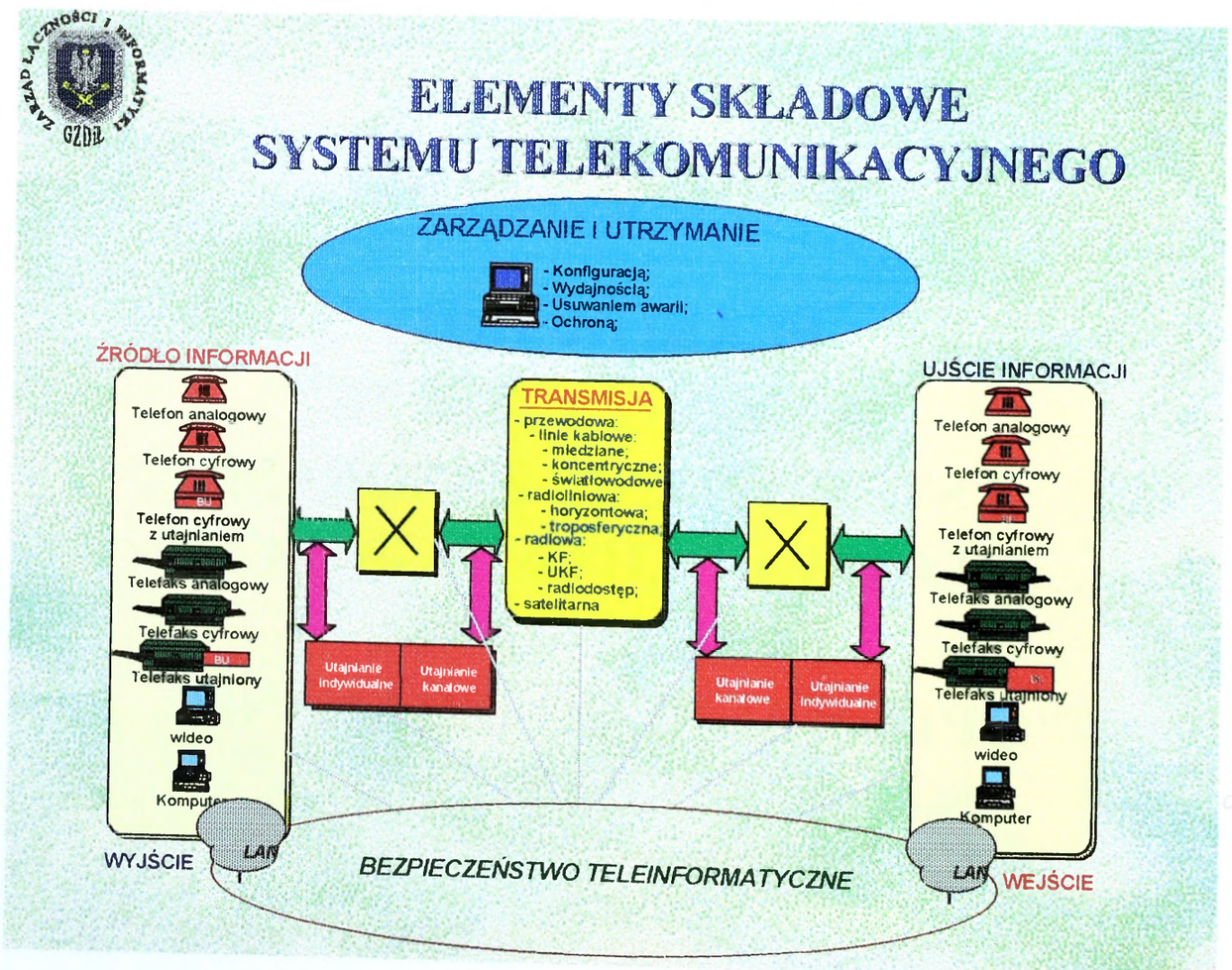
Referujący: ppłk Marek ŻOCHOWSKI

ZARZĄDZANIE

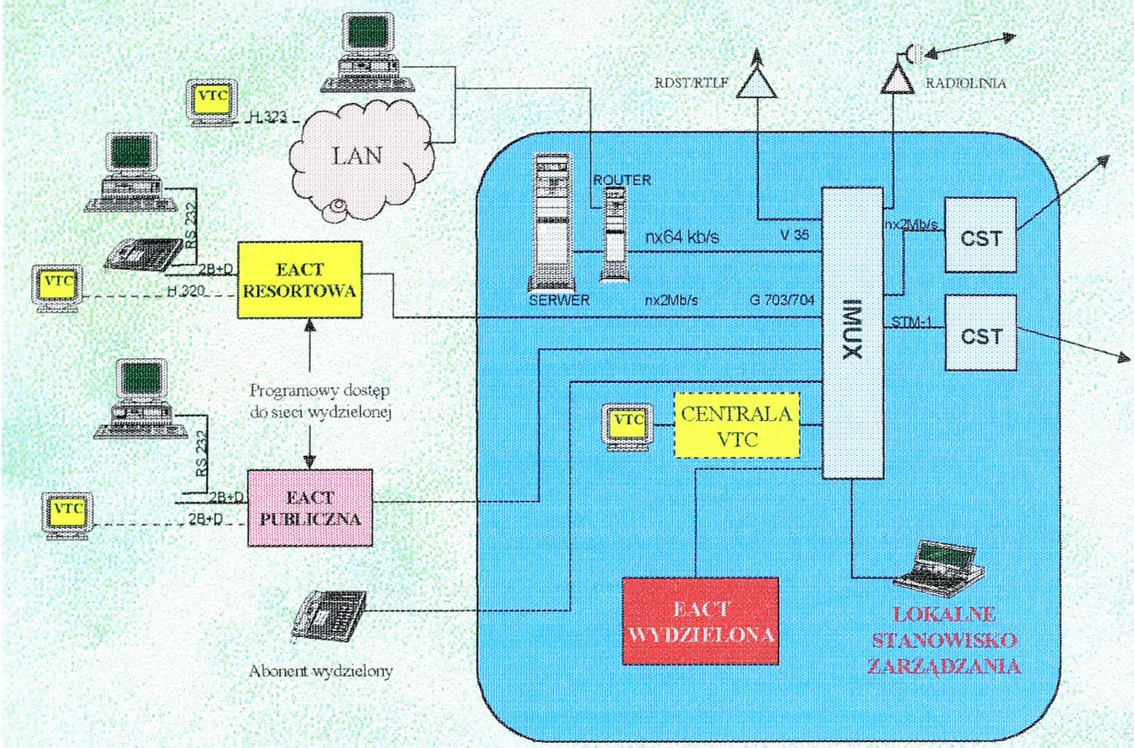
PLANOWANIE, WYKORZYSTANIE I STEROWANIE ZASOBAMI SIECI W CELU OSIĄGNIĘCIA I UTRZYMANIA OPTYMALNEGO DZIAŁANIA SIECI

wg. STANAG 5064 (AAP-31)


ZARZĄD ŁĄCZNOŚCI I INFORMATYKI
GZDŁ
WSPÓŁUŻYTKOWNICY SYSTEMU
SŁUŻBY UŻYTECZNOŚCI PUBLICZNEJ
Instytucje międzynarodowe (NATO, UZE,...)
SZ RP
NARODOWY SYSTEM TELEINFORMATYCZNY
STRUKTURY RZĄDOWE
STANOWISKO KRYZYSOWE
ADMINISTRACJA PAŃSTWOWA


ZARZĄD ŁĄCZNOŚCI I INFORMATYKI
GZDŁ
ELEMENTY SKŁADOWE SYSTEMU TELEKOMUNIKACYJNEGO
ZARZĄDZANIE I UTRZYMANIE
- Konfiguracją;
- Wydajnością;
- Usuwaniem awarii;
- Ochroną;
ŹRÓDŁO INFORMACJI
Telefon analogowy
Telefon cyfrowy
Telefon cyfrowy z utajnianiem
Telefaks analogowy
Telefaks cyfrowy
Telefaks utajniony
wideo
Komputer
WYJŚCIE
LAN
TRANSMISJA
- przewodowa:
- linie kablowe:
- miedziane;
- koncentryczne;
- światłowodowe
- radiolinia:
- horyzontowa;
- troposferyczna
- radiowa:
- KF;
- UKF;
- radiodostęp;
- satelitarna
Utajnianie indywidualne
Utajnianie kanałowe
Utajnianie kanałowe
Utajnianie indywidualne
UJŚCIE INFORMACJI
Telefon analogowy
Telefon cyfrowy
Telefon cyfrowy z utajnianiem
Telefaks analogowy
Telefaks cyfrowy
Telefaks utajniony
wideo
Komputer
LAN
WEJŚCIE
BEZPIECZEŃSTWO TELEINFORMATYCZNE

STRUKTURA TECHNICZNA WĘZŁA ŁĄCZNOŚCI



FUNKCJE ZARZĄDZANIA

- Zarządzanie konfiguracją;
- Zarządzanie bezpieczeństwem;
- Zarządzanie uszkodzeniami;
- Zarządzanie jakością;
- Zarządzanie finansowe.

OBSZARY FUNKCJONALNE

- transmisja;
- komutacja (kanałów i pakietów);
- widmo częstotliwości;
- kryptografia.

WARSTWY ZARZĄDZANIA

HIERARCHIA SYSTEMU ZARZĄDZANIA

- Poziom I - elementy nadzorowane;
- Poziom II - węzeł łączności (aparatownia);
- Poziom III - grupa węzłów łączności;
- Poziom IV - zespół węzłów łączności;
- Poziom V - system łączności SZ RP.

POZIOM I

ELEMENT NADZOROWANY

Wszystkie urządzenia znajdujące się na wyposażeniu węzła łączności (aparatowni) powinny posiadać własny, autonomiczny system zapewniający sterowanie i kontrolę nad nimi (urządzenia , pulpity własne urządzeń) oraz powinny mieć zaimplementowaną funkcję agenta (zalecany agent SNMP v3)

Powinien obejmować warstwę zarządzania elementami sieci.

POZIOM II

WĘZEŁ ŁĄCZNOŚCI

Węzeł łączności (aparatownia) powinien posiadać własny, autonomiczny **system utrzymania**, zapewniający sterowanie i kontrolę wszystkich urządzeń składowych węzła (aparatowni) jak również stwarzać dobre warunki pracy operatorowi. System ten powinien realizować funkcje: utrzymaniowe, operatorskie, reklamacyjne i pomocy abonenckiej.

Powinien obejmować warstwę zarządzania elementami sieci i zarządzania siecią.

POZIOM III

GRUPA WĘZŁÓW ŁĄCZNOŚCI

Realizuje funkcje związane z budową, uruchamianiem i bieżącą eksploatacją oraz rekonfigurowaniem systemu.

Powinien obejmować warstwę zarządzania elementami sieci, zarządzania siecią oraz zarządzania usługami.

POZIOM IV

ZESPÓŁ WĘZŁÓW ŁĄCZNOŚCI

Realizuje funkcje związane z uruchamianiem i bieżącą eksploatacją oraz rekonfigurowaniem systemu, w tym:

- automatyczne rozpowszechnianie rozkazów do - i zbieranie meldunków z - węzłów łączności;
- graficzną prezentację aktualnego stanu systemu łączności;
- gospodarkę widmem środków własnych, przeciwdziałania radioelektronicznego przeciwnika i stanu walki radioelektronicznej;
- dystrybucję danych kluczowych do urządzeń utajniających, uruchamianie kierunków;
- zarządzanie siecią łączności.

Powinien obejmować warstwę zarządzania bezpieczeństwem, zarządzania elementami sieci, zarządzania siecią oraz zarządzania usługami.

POZIOM V

SYSTEM ŁĄCZNOŚCI SZ RP

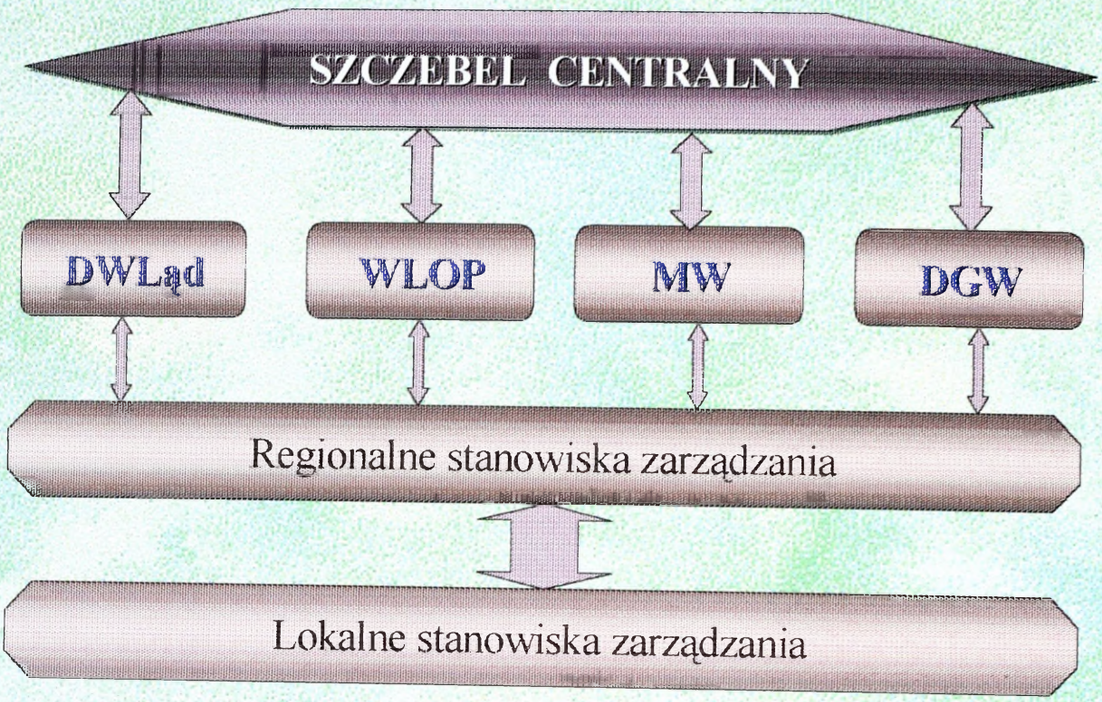
Realizuje funkcje związane z planowaniem systemu, w tym:

- struktury systemu łączności
- danych kluczowych do urządzeń utajniających;
- częstotliwości, danych do radiostacji, stacji radiodostępu, radiolinii;
- zabezpieczenia materiałowego;

oraz jego bieżącym nadzorem.

Powinien obejmować warstwę zarządzania bezpieczeństwem, zarządzania elementami sieci, zarządzania siecią oraz zarządzania usługami.

STRUKTURA SYSTEMU ZARZĄDZANIA SZ RP



Założenia systemowo-techniczne na system zarządzania SZ RP

- Obszar działania (terytorium RP, jednostki poza granicami);
- Skład i struktura (funkcjonuje w ramach systemu kierowania państwem w czasie pokoju, kryzysu i wojny);
- Zapewnienie:
  - ✓ Współpracy z systemami NATO (w ramach HNS, spełnienie STANAG-ów);
  - ✓ Współpracy z resortowymi sieciami łączności;
  - ✓ Usług (telefon, transmisja danych, videotelekonferencja);
  - ✓ Funkcjonowania zintegrowanego systemu informatycznego;
  - ✓ Systemów radiodostępu;
  - ✓ Łączności satelitarnej;
  - ✓ Bezpieczeństwa systemu i informacji.

Przykład zarządzania infrastrukturą telekomunikacyjną w ramach ćwiczeń „CRYSTAL EAGLE'2000"

STANDARYZACJA

Założenia: opracowanie STANAG-ów w ramach projektu TACOM POST-2000.

Stan realizacji:

- zakończenie prac nad STANAG-mi - koniec 2004 roku;
- uzgodnienia w ramach podkomitetów NC3B - 2005;
- rozpoczęcie procesu ratyfikacji i implementacji STANAG-ów - od 2006 roku.

AKADEMIA
OBRONY NARODOWEJ

Ryszard STĘPIEŃ

PSYCHOSPOŁECZNE ASPEKTY ZACHOWAŃ JEDNOSTEK I GRUP SPOŁECZNYCH W OBLICZU ZAGROŻEŃ

CENTRUM KONFERENCYJNE WP Grudzień 2001

Współczesny świat, mimo wielu działań rządów i państw zatroskanych zapewnieniem bezpieczeństwa swoim obywatelom, generuje coraz więcej zagrożeń. Poziom ryzyka, ściśle powiązanego z niepewnością i brakiem bezpieczeństwa, jest niekiedy tak duży, że wywołuje poczucie lęku uniemożliwiającego człowiekowi normalne funkcjonowanie.

Opublikowany w 1999 roku międzynarodowy raport pt.: Un Monde Nouveau, jako wynik gruntownych analiz różnych opracowań instytucji międzynarodowych, zawiera stwierdzenie, iż doświadczenia, jakie przyniósł XX wiek, świadczą o niebezpieczeństwie utraty humanistycznych wartości i wzrastającym zagrożeniu ludzkości, wręcz stawiającym pod znakiem zapytania możliwości przetrwania w XXI stuleciu gatunku Homo sapiens.[3]

Wśród podstawowych wyzwań, które powinny być podjęte zdaniem autorów raportu wymienia się:

- zapewnienie pokoju, który jest niezbędnym warunkiem pomyślnego rozwiązania pozostałych problemów;
- przezwyciężanie powiększających się w szybkim tempie nierówności w skali krajowej i międzynarodowej;
- zapewnienie trwałego rozwoju i rozsądnego gospodarowania środowiskiem ziemskim;
- podjęcie działań zorientowanych na przyszłość.

Obok przedstawionych globalnych wyzwań coraz częściej upowszechniana jest teza, iż takie uniwersalne wartości jak: wolność, równość prawa człowieka i demokracja pozostają w bezpośrednim związku z ich niedocenianiem w rzeczywistości społecznej. Stale obserwujemy upowszechnianie przemocy, wzrost liczby zachowań agresywnych i brutalizację życia. Zmieniają się także oczekiwania ludzkich zbiorowości i jednostek, w zakresie przeciwdziałania różnym zagrożeniom.

Zdaniem Teresy Borowskiej „odpowiedź na pytanie, w jakim kierunku powinna pójść edukacja, aby dzięki niej człowiek potrafił pokonywać zagrożenia dzisiejszego świata, wiąże się ściśle z problemami dobra i zła"[4].

Edukacja ma więc przygotować człowieka do kreowania własnej egzystencji. „Homo construens", człowiek budujący, o niezbędnej sile moralnej i zasobach kognitywno-emocjonalnych . Z badań G. Zimbardo wynika, że „ludzie, którzy nauczyli

---

[3] Zob. F. Mayor, J. Bindé Un Monde Nouveau, UNESCO 1999.

[4] T. Borowska, „Homo construens" – człowiek budujący. Edukacyjne przygotowanie do radzenia sobie z różnymi zagrożeniami, (w:) Pedagogika i edukacja wobec nadziei i zagrożeń współczesności, pod red. Janusza Gniteckiego i Joanny Rutkowiak, Warszawa – Poznań 1999, s. 351.

się, że mają mały wpływ na swoje życie, postrzegają rzeczywistość jako determinującą ich egzystencję. *Ten błąd w uczeniu* - twierdzi T. Borowska – *powoduje, że w sytuacji zagrożenia rezygnują oni często z aktywności – cechuje ich po prostu „bezradność". Natomiast ludzie o uwewnętrznionej kontroli są bardziej autonomiczni, optymistyczni, aktywni, gdyż ta rozwinięta wewnętrzna lokalizacja daje im większe poczucie odpowiedzialności*"[4].

Zagadnienia bezradności i poczucia bezradności wiążą się ściśle z psychospołecznymi uwarunkowaniami zachowań ludzi w sytuacji ryzyka, niepewności i zagrożenia.[5] Wśród głównych zagrożeń bezpieczeństwa państw i społeczeństw wymienia się: terroryzm i bioterroryzm, przestępczość zorganizowaną, kryzysy i konflikty lokalne, katastrofy technologiczne, naruszanie praw człowieka i ubóstwo wielu grup społecznych, napięcia etniczne wewnątrz państw i na ich granicach, żywiołowe migracje na dużą skalę, brak ochrony środowiska naturalnego, wzrost nacjonalizmów i schyłek państwa narodowego, niepewność co do wspólnego losu ludzkości, gromadzenie coraz to skuteczniejszej broni.

W obszarze zjawisk o charakterze ogólnospołecznym, które mogą powodować zagrożenia bezpieczeństwa psychospołecznego wymienia się dezintegrację wybranych elementów więzi społecznej, a głównie osłabienie systemu wartości i zanik społeczeństwa obywatelskiego. Można zadać sobie pytanie, czy ma szanse przetrwania człowiek jeśli jego władza nad środowiskiem w którym żyje, a także poczucie kompetencji ulegają nagłej destrukcji? Prawdopodobnie każda próba udzielenia możliwie jednoznacznej odpowiedzi na tak sformułowane pytanie byłaby niepełna i wątpliwa. Jednak dla potrzeb edukacyjnych zachowań w warunkach utraty bezpieczeństwa przyjmuje się na ogół, że człowiek utwierdzony w przekonaniu, iż może wywierać wpływ na środowisko, częściej niż inni będzie przejawiał wiarę w pomyślne wyjście z trudnej sytuacji i podejmie w tym celu określone działania. Podobnie zachowa się ten, kto w swoim działaniu kieruje się wolą osiągnięcia wyznaczonego celu i kto jest przekonany, iż beznadziejne sytuacje wymagają twórczych i aktywnych działań.

Obok takich pojęć, jak beznadziejność i bezradność, w sytuacjach zagrożeń pojawia się termin: lęk. Jest on definiowany jako „niejasny, nieprzyjemny stan emocjonalny charakteryzujący się przeżywaniem obaw, strachu, stresu i przykrości. Lęk jest często

---

[4] Tamże, s. 351-352.

[5] Zob. P.G. Zimbardo, F.L. Ruch, Psychologia i życie, Warszawa 1996, a także: M. Goszczyńska, Człowiek wobec zagrożeń. Uwarunkowania oceny i akceptacji ryzyka, Warszawa 1997; J. Szmagalski, Ofiary katastrof i klęsk żywiołowych, Warszawa 1996

przeciwstawiany strachowi ze względu na to, że *(zazwyczaj*, jak mówią niektórzy, bądź *zawsze,* jak utrzymują inni) lęk jest stanem pozbawionym obiektu, natomiast strach jest zawsze strachem przed czymś, kimś, lub jakimś zdarzeniem".[6]

Sytuacje wywołujące lęk różnie oddziałują na ludzi i często odmiennie wpływają na pojawianie się w ich działaniu negatywnych konsekwencji. Inaczej mówiąc, niektórzy potrafią wykazywać daleko idące tolerowanie lęku, co może wynikać zarówno z indywidualnych cech, jak i z pewnych wyuczonych zachowań (reakcji) w obliczu zagrożenia. Funkcjonalne zaburzenia lękowe traktowane ogólnie, charakteryzują się uporczywym, nieukierunkowanym lękiem i takimi reakcjami, jak drżenie ciała, nerwowość, napięcie nerwowe, pocenie się, zawroty głowy, uczucie niepokoju, drażliwość, szybkie oddychanie, gwałtowne bicie serca, itp.

Bardzo ważnym czynnikiem redukowania lęku, niepewności i bezradności, jest przewidywalność zdarzeń. Jej znaczenie w działaniu ludzi narażonych na różne zagrożenia jest tym większe, im bardziej potrafimy im stworzyć możliwość wcześniejszego znalezienia się w zbliżonej sytuacji.

Dlatego też współczesne rozumienie edukacji dla bezpieczeństwa nawiązuje do idei tworzenia takich sytuacji dydaktycznych, w których uczeń musi opanować wiadomości i umiejętności niezbędne w radzeniu sobie z nieoczekiwanymi zagrożeniami".[7] Im częściej uczeń staje wobec problemu wymagającego nie tylko posłużenia się znaną wiedzą i opanowanymi umiejętnościami, ale również zastosowania twórczo opracowanych rozwiązań, tym większe jest prawdopodobieństwo, że będzie go cechowała zdolność przewidywania zdarzeń. W ten sposób można skutecznie łagodzić strach i lęk wobec zagrożeń i stymulować aktywne i samodzielne działanie jednostki ludzkiej.

W obliczu coraz częściej występujących zagrożeń bardzo wiele uwagi poświęca się zagadnieniom *stresu,* rozumianego jako pewien stan napięcia psychicznego powodowany zakłóceniem równowagi pomiędzy zewnętrznym lub wewnętrznymi wymaganiami, a aktywnymi możliwościami jednostki w zakresie radzenia sobie z tymi wymaganiami.[8] Jak twierdzi Andrzej Augustynek, stres psychiczny wywołany przez silny bodziec (stresor), to „wzrost poziomu napięcia emocjonalnego, prowadzący do ogólnej mobilizacji

---

[6] A.S. Reber, Słownik psychologii, Warszawa 2000, s. 340. Zob. też: B. Rokicki, Lęk, (w:) J. Borkowski, M. Dyrda, L. Kanarski, B. Rokicki, Człowiek w organizacji. Podręczny słownik psychologii zarządzania i dziedzin pokrewnych, Warszawa 2001, s. 67

[7] Zob. R. Stępień, Edukacja szkolna, a bezpieczeństwo państwa, „Edukacja dla bezpieczeństwa", 2000, nr 1, s. 5.

[8] B. Rokicki, Stres, (w:) J. Borkowski, M. Dyrda, L. Kanarski, B. Rokickim, Człowiek..., op. cit., s 130-131.

sił organizmu, mogący przy długotrwałym działaniu doprowadzić do zaburzeń w funkcjonowaniu organizmu, wyczerpania i chorób psychosomatycznych".[9]

Na ogół nie klasyfikuje się czynników stresowych, ale wiadomo, że silne, nagłe i niezwykłe bodźce, szczególnie te, które zagrażają bezpieczeństwu, bądź życiu człowieka niemal zawsze wywołują stres. W rzeczywistości jednak o pojawieniu się stresu psychologicznego decyduje nie tylko siła stresora, ale także jego znaczenie dla podmiotów. Janusz Reykowski rozróżnia trzy klasy czynników obciążających psychologiczny system samoregulacyjny. Są to zakłócenia, zagrożenia i sytuacje deprywacji.[10]

Wśród zakłóceń wymienia Autor rozmaite elementy sytuacji, które utrudniają albo uniemożliwiają jednostce sprawne wykonywanie określonych czynności. Zagrożenia natomiast są rozumiane jako rozmaite niebezpieczeństwa o charakterze fizycznym lub społecznym. Stres jaki wiąże się z występowaniem zagrożeń jest następstwem antycypowania pewnej szkody, którą człowiek poniesie, jeśli w porę i skutecznie się nie zabezpieczy.

Z kolei deprywacja ma miejsce wówczas, gdy człowiek *„nie zaspokoił swoich potrzeb lub nie osiągnął zamierzonych przez siebie celów"*.[11]

Należy podkreślić, że stres powiązany na ogół z występowaniem silnego napięcia emocjonalnego, któremu mogą towarzyszyć: strach, irytacja, niepokój, panika, przerażenie, gniew lub złość, nie zawsze wiąże się wyłącznie ze stanami negatywnymi. W wielu przypadkach stan emocjonalny wywołany sytuacją stresową może spełniać rolę mobilizującą człowieka do zdwojonego wysiłku i w ten sposób uodporniać go na stres. Problem ten wiąże się bezpośrednio z emocjonalnością jednostki, a ściślej z pobudzaniem, hamowaniem, ruchliwością i równowagą procesów nerwowych.

Źródłem pogłębionej refleksji psychologów i pedagogów jest fakt, iż wielu ludzi, znajdując się w sytuacji stresowej i w stanie pobudzenia emocjonalnego, zachowuje zdolność racjonalnego myślenia i działania. Mówimy wówczas o wysokiej odporności na stres, co może mieć swoje uzasadnienie nie tylko w indywidualnych właściwościach, ale również w odpowiednim przygotowaniu edukacyjnym.

---

[9] A. Augustynek, Stres, (w:) Słownik psychologiczny, pod red. Włodzimierza Szewczuka, Warszawa 1985, s. 297.

[10] Zob. A. Frączek, M.Kofta, Frustracja i stres psychologiczny, (w:) Psychologia, pod red. red. Tadeusza Tomaszewskiego, Warszawa 1976, s. 656 i nast.

[11] Tamże, s. 657.

W Polsce od kilku lat podejmowane są określone działania mające na celu przygotowanie społeczeństwa do przeciwstawiania się różnym zagrożeniom bezpieczeństwa personalnego i strukturalnego. Wśród głównych instytucji odpowiedzialnych za fakty tak rozumianej edukacji wymienia się: rodzinę, szkołę, organizacje młodzieżowe i stowarzyszenia, środki masowego przekazu, wojsko, policję, staż pożarną (państwową i ochotniczą). W latach dziewięćdziesiątych w ramach badań naukowych na temat systemu bezpieczeństwa Polski, prowadzonych przez Akademię Obrony Narodowej, uzasadniono potrzebę wprowadzenia terminu: edukacja dla bezpieczeństwa, jako zaktualizowanego ujęcia zbyt tradycyjnego już przysposobienia obronnego (wcześniej przysposobienia wojskowego).[12]

W ten sposób rozpoczęto likwidowanie (osłabienie) dystansu między potrzebami obronności i tradycyjną edukacją oraz między zagrożeniami militarnymi a bezpieczeństwem obywateli.

Coraz szerzej upowszechnia się przekonanie, że zachowanie człowieka w sytuacji zagrożenia klęską żywiołową, bądź katastrofą ekologiczną będzie bardzo zbliżone do zachowań w okresie wojny czy działań innych niż wojna.

Równocześnie pojawiają się nowe obszary badań w zakresie edukacji dla bezpieczeństwa obejmujące:

- określenie istoty i zasadności poszerzania tolerancji na ryzyko i niepewność w sytuacji zagrożeń;
- kształtowanie i rozwijanie zdolności człowieka w zakresie pracy nad stresem i lękiem;
- poszerzanie wizji człowieka uwikłanego, narażonego na zagrożenia – (homo dupleks);
- przygotowanie człowieka zdolnego do twórczego, aktywnego i samodzielnego budowania własnej egzystencji (homo construens).

Współczesny człowiek powinien być świadomy swoich obowiązków obywatelskich, a jego wrażliwość na różnorodne sygnały o zagrożeniu i potrzebę stałego doskonalenia swoich kwalifikacji musi pozostawać w bezpośrednim związku ze współczesnością i wizją przyszłości.

---

[12] Zob. Edukacja dla bezpieczeństwa. Materiały z konferencji naukowej, pod red. Ryszarda Stępnia, Warszawa 1994.

REFERATY

INSTYTUCJI I FIRM

MINISTERSTWO
OBRONY NARODOWEJ

Ryszard JAKUBCZAK

SYSTEM OBRONNOŚCI RZECZPOSPOLITEJ POLSKIEJ WYMIAR STRATEGICZNY WSPARCIA NARODOWEGO

CENTRUM KONFERENCYJNE WP Grudzień 2001

Wsparcie narodowe to strategiczne, obok działań wojsk operacyjnych, przedsięwzięcia obronne na terytorium państwa-członka NATO – prowadzone przez system obrony terytorialnej wespół z logistyką stacjonarną na rzecz własnych i sojuszniczych wojsk operacyjnych oraz ludności w sytuacjach zagrożenia jej życia i mienia. Obejmuje ono instytucje odpowiedzialne za realizacje zadań wynikających z obowiązków państwa-gospodarza (HNS) oraz mobilizację wojsk i gospodarki narodowej, terytorialne organy dowodzenia, wojska obrony terytorialnej, formacje i organizacje pozamilitarnego układu obronnego podległe administracji rządowej, obronnie przygotowane społeczeństwo, infrastrukturę obronną, logistykę stacjonarną w części technicznej, materiałowej, transportu i hospitalizacji.

System wsparcia narodowego to zespół elementów posiadających właściwości aktywnego, zbrojnego i pozazbrojnego oddziaływania na przeciwnika oraz kompleksowego wsparcia sił własnych i sojuszniczych oraz ochrony i obrony ludności w sytuacjach zagrożenia jej życia i mienia na terytorium RP w ścisłym współdziałaniu z organami administracji rządowej i samorządowej.

Biorąc za podstawę powyższą definicję należy podkreślić, że istotą i celem utworzenia tego systemu jest wzmocnienie możliwości prowadzenia działań obronno-ochronnych na obszarze kraju oraz zapewnienie zintegrowanego wielorakiego wsparcia logistycznego na rzecz wojsk własnych i sojuszniczych w ramach realizacji zobowiązań wynikających z roli państwa-gospodarza, udziału w działaniach ratowniczych oraz likwidacji skutków klęsk żywiołowych, katastrof i awarii, realizacja zadań wynikających ze współpracy cywilno-wojskowej, a także patriotycznego i obronnego przygotowania społeczeństwa.

W ten sposób system wsparcia narodowego (terytorialnego) integrowałby działania w dziedzinie:

- zarządzania logistyką stacjonarną w części technicznej, materiałowej, transportu i służby zdrowia,
- przygotowania i zarządzania infrastrukturą obronną,
- administrowania zasobami rezerw osobowych, współudziału w pokojowym uzupełnianiu i mobilizacyjnym rozwinięciu SZ RP,
- realizacji zadań wynikających z roli państwa-gospodarza,
- udział w realizacji współpracy cywilno - wojskowej (CIMIC),
- obrony terytorialnej,

- topografii i hydrometeorologii wojskowej,
- części zadań obrony przed bronią masowego rażenia i inżynierii wojskowej.

Zatrzymajmy się nad sposobem realizacji zadań w wyżej wyspecyfikowanych dziedzinach w dziale „obrona narodowa".

Czynniki strategiczne warunkujące istnienie systemu obronnego są pochodną tego, czym dysponuje - jako atutami obronnymi - państwo. W każdym dobrze obronnie zorganizowanym państwie podstawę w tym względzie stanowią ludzie (ich zorganizowana społecznie organizacja - podstawa istnienia państwa[13] jako takiego) i terytorium[14] (stanowiące także bazę wypadową do agresji na innych), na którym mieszkają odpowiednio przygotowani do jego do obrony obywatele. Z tego wynika także, że podstawę systemu wsparcia narodowego (terytorialnego) wywodzić trzeba przede wszystkim z dwu źródeł – a mianowicie z uwarunkowań demograficznych i terytorialnych, a w tym kontekście zewnętrznych i wewnętrznych potrzeb państwa. Te pierwsze są znacząco zależne od uwarunkowań geopolitycznych i porozumień sojuszniczych, zaś te drugie – aktywnością obronną na rzecz utrzymania optymalnego poziomu bezpieczeństwa państwa w sferach militarnej i pozamilitarnej.

Historia wojskowości daje tylko jedno rozwiązanie na optymalne wykorzystanie potencjału zawartego w masowej formacji obywatelskiej do obrony państwa – tworzenie wojsk obrony terytorialnej[15], do obrony miejscowej w ramach powszechnego obowiązku (służby wojskowej) obronnego. W ten sposób można doprowadzić do „niepokonalności" narodu, społeczeństwa, państwa. A to już jest wartość strategiczna, ponieważ od szantażu nuklearnego ważniejsza jest niepokonalność przeciwnika – twierdzi E. Teller („ojciec" bomby wodorowej i autor koncepcji gwiezdnych wojen). Niepokonalność taką mogą współcześnie osiągnąć jedynie państwa demokratyczne, gdyż tylko w nich – w przeciwieństwie do totalitarnych - istnieje militarna możliwość (i to nie we wszystkich) wyzyskania całego potencjału społecznego do obrony państwa.

---

[13]To społeczności zorganizowane tworzą państwa, określając ich granice charakter i inne warunki jego funkcjonowania wewnętrznego i stosunki z państwami sąsiednimi.

[14]Podstawą materialną państwa jest jego terytorium. Nie ma państwa bez terytorium – o granice terytorium lub o nie same toczono - i wciąż się toczy - krwawe wojny, bowiem wielkość terytorium zaświadcza o znaczeniu państwa w stosunkach międzynarodowych. Ona stanowi też podstawę jego bogactwa i siły.

[15]Struktura narodowościowa obywateli w państwie także wpływa na charakter wojsk terytorialnych i system obrony terytorium państwa. W jednolitych narodowo państwach można budować system obrony terytorialnej, a w jego ramach wojska obrony terytorialnej. Tam natomiast, gdzie utworzenie wojsk obrony terytorialnej może uzbroić lokalną społeczność a tym samym przyczynić się do rozpadu państwa wielonarodowego, wprowadza się system obrony terytorium, a w miejsce wojsk obrony terytorialnych - przywiązanych do lokalnej społeczności - rozbudowuje znacznie wojska wewnętrzne (*aterytorialne* co do formowania, szkolenia i użycia operacyjnego) oraz bardzo podobne wojskom operacyjnym - regionalne wojska terytorialne.

Przy pomocy właściwie wykorzystanych na rzecz obronności zasobów (środków właściwych do obrony) państwo może doprowadzić do takiego stanu, kiedy wszelkie logicznie konstruowane strategie agresji ze strony potencjalnych przeciwników nie będą w stanie wykazać takich własnych walorów, na których podstawie przywódcy polityczni potencjalnego agresora będą w stanie zaakceptować je jako środek w stosunkach międzypaństwowych. Zatem osiągnie się wtedy stan, który polecał Sun Tzu: „zwyciężaj strategię strategią", zaś w innym miejscu własnej teorii walki dopowiadał - najwyższym osiągnięciem jest pokonać wroga bez walki[16]. Również Belizariusz (wódz bizantyjski z VI w.) wskazywał na to, że „najpełniejsze i najszczęśliwsze zwycięstwo to zmusić nieprzyjaciela do zrezygnowania z jego celów, nie ponosząc przy tym samemu żadnych strat"[17].

Takie wygranie wojny bez wojny jest możliwe głównie na płaszczyźnie politycznej w sferze stosunków międzynarodowych, gdzie liczy się tylko siła – bowiem (jak twierdzi Slessor – w „Strategia Zachodu") polityka zagraniczna bez siły jest bezsilna. W stosunkach międzynarodowych siła ma nie tylko wymiar agresywny, ponieważ stosunkowo wysoki stan potencjału obronnego jest także atutem w pozyskiwaniu sojuszników. Nawet zagrożone agresją państwo może pozyskiwać obrońców, tym bardziej jeśli tyko samo stanowi godną obrony wielkość – obrońca w ogólności więcej może liczyć na pomoc z zewnątrz niż nacierający. Będzie on mógł tym pewniej na to liczyć, im ważniejsze jest jego istnienie dla wszystkich innych, to znaczy im zdrowszy i silniejszy jest jego stan polityczny i wojskowy[18]. Stąd płynie także wskazanie, aby w budowaniu wielkości potencjału obronnego wykorzystywać także wojska o mniejszej mobilności operacyjnej dające dodatkową wartość potencjału obronnego.

Wyraźna przewaga liczebna wojsk operacyjnych nad wojskami obrony terytorialnej jednoznacznie świadczy o tym, że w państwie przedkłada się nad obronę na własnym terytorium interwencję zbrojną poza jego granicami. Stosunek wojsk operacyjnych do wojsk obrony terytorialnej może być miarodajnym wykładnikiem charakteru strategii wojennej państwa.

Jest to jednak prawdziwe tylko wtedy, kiedy strony nie prowadzą działań precyzyjnych przeciw sobie, ponieważ w wypadku ich zastosowania dysponujący małą

---

[16] „Sztuka wojny", Warszawa 1994, s. 35
[17] B. H. Liddell Hart, „Strategia: działania pośrednie", Warszawa 1959, s. XVI.
[18] Clausewitz C., „O wojnie", Lublin 1995, s. 445-446.

armią operacyjną (posiadającą najnowsze technologicznie środki walki) może pokonać w rozstrzygającej bitwie każdą - oprócz tej wystawionej w ramach obrony terytorialnej.

Przedmiotem strategii obronnej państwa demokratycznego budującego system obrony jest poszukiwanie sposobu zbudowania go na możliwie wysokim poziomie bezpieczeństwa ale jednocześnie po najniższych (na ile jest to możliwe) kosztach. Dlatego optymalnym wyjściem dla takiego państwa - o doktrynie defensywnej - jest (wzorem wielu państw Europy) stawianie na znaczącą liczebnie strukturę obrony terytorialnej.

W ostatnich wiekach daje się zauważyć w Europie, że w sytuacji kiedy jednolite narodowo państwo rezygnuje z wykorzystania systemu obrony terytorialnej do wzmocnienia własnej obronności, zachodzi podejrzenie, że sprawujący w nim władzę zamierzają prowadzić politykę obroną niezgodną z interesem narodowym. Historia dowodzi, że działanie przeciw bezpieczeństwu własnego państwa (wyrażające się nielogiczną strukturą systemu obrony państwa) jest przeważnie wynikiem naiwności lub nieodpowiedzialności[19] powodowanej innymi niż obronne przyczynami[20].

Analizując systemy obrony państw, można stwierdzić, że nie ma dwóch jednakowych systemów obrony terytorium państwa (w tym struktur wojsk obrony terytorialnej) w dwóch różnych państwach, ponieważ zależą one od charakteru strategii wojskowej państwa (defensywnej lub ofensywnej), charakteru strategii wojennej sąsiadów, położenia geopolitycznego i struktury narodowościowej.

1. UWARUNKOWANIA GEOPOLITYCZNE

Jest oczywistym, że geopolityka[21] określa główne problemy bezpieczeństwa narodowego Polski, a w tym i główne problemy obrony militarnej. Polska leży między największymi (obszarowo i ludnościowo państwami) Rosją i Niemcami – będącymi

---

[19]Por. Postępowanie marszałka J. Pilsudskiego - dla osłabienia przeciwników politycznych w armii „rozbił" terytorialną strukturę obronną państwa - poprzez likwidacje dowództw okręgów korpusów (DOK) i obsadzał najważniejsze stanowiska miernymi ale wiernymi „towarzyszami" - bezpośrednio po zamachu majowym w 1926 r. Zemściło się to tragicznie w 1939 r., zabrakło bowiem wtedy terytorialnych dowództw szczebla operacyjnego (typu)DOK, do przygotowania i kierowania obronnością państwa w skali regionalnej i operacyjno-taktycznej, a utworzone jednostki wojsk obrony terytorialnej (brygady, półbrygady i batalion Obrony Narodowej) - zamiast funkcjonować w podporządkowaniu DOK i bronić niemal każdej miejscowości - przydzielano do wykorzystania dowódcom wojsk operacyjnych, którzy wyjątkowo nie celowo wykorzystywali je w walce.

[20]W Polsce znane są przyczyny rozwiązywania wojsk terytorialnych w Rzeczypospolitej szlacheckiej, a także w okresie II RP i PRL. Często warunkowano to czynnikami ekonomicznymi – obciążeń finansowych budżetu państwa (skarbu) – jednak po doznanej klęsce militarnej stawało się jasne, że za takim działaniem stał głównie interes polityczny niektórych sąsiadów; zmierzający do militarnego osłabienia RP po to, aby w rozstrzygającej o niepodległości sytuacji móc łatwo pokonać jej wojska składające się jedynie z ograniczonej liczby słabych formacji wojsk operacyjnych.

[21]Geopolityka, teoria wyjaśniania zjawisk politycznych czynnikami geograficznymi ... rozwój państwa, jego bezpieczeństwo i trwanie jest pochodną czynników geograficznych takich jak położenie, ukształtowanie terytorium, granice, klimat i wielkość państwa, *Leksykon politologii,* Wrocław 1997, s. 103.

zresztą swego rodzaju mocarstwami światowymi (RFN – ekonomiczne, Rosja – nuklearne mocarstwo). Dysproporcja siły narodowej[22] na niekorzyść Polski, w połączeniu z kilkusetletnimi doświadczeniami „naporu" – nie tylko zresztą militarnego - ze strony Niemiec i Rosji jednoznacznie wskazują, że podstawą polskiej racji stanu jest skuteczna, zawczasu przygotowana obrona narodowa. Obrona, zdolna odstraszyć, zniechęcić przeważające potencjały przed użyciem przemocy przeciwko interesom Polski. Tak więc Polska winna realizować klasyczną tezę Clausewitza: „zdobywca zawsze jest usposobiony pokojowo (...), chętnie wkroczyłby do naszego państwa jak najspokojniej. Aby nie mógł tego zrobić, musimy sami pragnąć wojny, a więc ją też przygotowywać, czyli innymi słowy: sztuka wojenna wymaga aby właśnie słabi, skazani na obronę byli zawsze uzbrojeni, aby nie ulec napadowi"[23].

Współczesny historyk angielski, wielki przyjaciel Polski Norman Davies tak realnie ocenia położenie geopolityczne Polski: „jest oczywistym historycznym faktem, że aspołeczne posunięcia sąsiadów pozbawiły ich możliwości niepodległego bytu"[24]. Aktualny pozostaje więc postulat Romana Dmowskiego: „między Rosją a Niemcami nie ma miejsca na słabe państwo". Bowiem bezwzględne prawo historii państw brzmi: „ma prawo do życia tylko to co się potrafi obronić" (O. Balzer) lub w ujęciu marsz. J. Piłsudskiego: „historia jest ciągłą walką sił i że kto siły nie ma, ten się w historii nie liczy".

W położeniu geopolitycznym Polski obrona narodowa oznacza nie tylko obronę militarną ale przeciwdziałanie także innym zagrożeniom bezpieczeństwa narodowego – kulturowym, ekonomicznym, ideowym, politycznym, itp. Stąd też polska organizacja wojskowa, w tym szczególnie – masowy komponent wojska OT - winna, poprzez proces szkolenia wojskowego całej młodzieży, kształtować również świadomość narodową[25], postawę patriotyczną i obywatelską oraz współodpowiedzialność za bezpieczeństwo narodowe.

Potencjał państwa stanowią nie tylko jego zasoby środków trwałych i ludności oraz infrastruktury, ale także stan nauki i techniki oraz geopolityczne położenie. To wszystko może być odpowiednio wykorzystane na rzecz obronności, której charakter określa

---

[22]Fundamentalna kategoria politologii określająca zdolność oddziaływania państwa w środowisku międzynarodowym. Siłę narodową tworzą m.in.: „czynnik geograficzny, zasoby naturalne, potencjał przemysłowy, gotowość militarna, czynnik demograficzny, charakter narodowy, morale narodowe, jakość dyplomacji, jakość rządu". Wg H.J.Morgentaua, [w:] A.Bodnar, *Decyzje polityczne. Elementy teorii,* Warszawa 1985, s. 220.

[23]C.von Clausewitz, *O wojnie,* Lublin 1995, s. 441.

[24]N. Davies, *Boże igrzyska,* Kraków 1999, s. 1080.

[25]„Świadomość narodowa jest najlepszą ochroną granic", R.Umiastowski, czołowy geograf II RP.

polityka obronna. Prześledźmy więc jak te czynniki warunkują strategię państwa w zakresie tworzenia i wykorzystania systemu obrony terytorialnej. Pierwotnym w stosunku do strategii – rozumianej także jako droga przejścia od założeń do celów[26] (lub też metoda osiągania celów polityki) – jest decyzja polityczna. Zatem o charakterze obrony, systemie obrony państwa, skali wykorzystania jego potencjału na potrzeby obronne decyduje polityka – jako wola rządu-reprezentanta państwa (społeczeństwa, narodu; działającego na bazie ustawy zasadniczej państwa) - zawarta w dokumentach będących wykładnią polityki obronnej państwa.

W III Rzeczypospolitej Polskiej wola taka została wyrażona po raz pierwszy, kiedy państwo było u progu własnej niepodległości i nie należało do żadnego sojuszu militarno-politycznego. Wychodząc wtedy z polskiej racji stanu (nadrzędności interesu ogólnego państwa jako całości względem interesom szczegółowym ...) władze naczelne przyjęły (2.11.1992 r.) dwa dokumenty doktrynalne ujmujące podstawowe założenia polityki bezpieczeństwa narodowego. Były to „Założenia polskiej polityki bezpieczeństwa" i „Polityka bezpieczeństwa i strategia obronna Rzeczypospolitej Polskiej". Określono w nich, iż „celem Rzeczypospolitej Polskiej jest obrona i umacnianie niepodległej, suwerennej państwowości, gwarantującej respektowanie praw człowieka, wolności i swobód obywatelskich.

Trwały, niepodległy i bezpieczny byt państwa jest warunkiem ukształtowania sprawnego systemu demokratycznego, opartego na zasadach społeczeństwa obywatelskiego oraz pomyślnego przeprowadzenia reform systemowych, usprawniających gospodarkę narodową".

W najnowszych opracowaniach tego typu przyjmuje się w pierwszym rzędzie, że strategicznym celem polskiej polityki bezpieczeństwa jest zagwarantowanie niepodległości, suwerenności, integralności terytorialnej państwa oraz nienaruszalności jego granic[27]. Odniesiono się także do „otoczenia politycznego" Polski – wskazując na potrzebę wnoszenia wkładu w budowę trwałego, sprawiedliwego ładu pokojowego w Europie i na świecie - ale znalazło to swoje miejsce w czwartym punkcie rankingu celów strategicznych RP; m.in. za ochroną porządku demokratycznego oraz warunków dla wszechstronnego i stabilnego rozwoju (...) państwa. Również w ramach podstawowych zasad polskiej polityki bezpieczeństwa problematyka, zewnętrznej aktywności RP znajduje

---

[26] Strategia narodowa, „International Military Defense Encyclopaedia", New York 1993, t. 5, s. 2779-2581. Tłumaczenie polskie – „Słownik terminów z zakresu bezpieczeństwa narodowego", AON. Warszawa 1996, s. 110.

[27] „Strategia bezpieczeństwa RP" – przyjęta przez Rade Ministrów 4.01.2000 r.

się w kolejnych - a nie pierwszej - z przyjętych zasad. Podobnie priorytety – w zakresie tego co jest pierwsze: własne terytorium, czy aktywność państwa na zewnątrz? – są określone w treści „Traktatu Północnoatlantyckiego"[28] (Waszyngton 4.4.1949 r.), gdzie indywidualna ... zdolność do odparcia zbrojnej napaści wyartykułowana jest w art. 3, zaś udzielanie pomocy ... napadniętym (poprzez akcję jaką uzna się za konieczną) – w art. tegoż dokumentu.

Przyjmują, że strategia (np. bezpieczeństwa narodowego) jest teorią i praktyką działania państwa, ukierunkowaną na osiąganie celów założonych w dziedzinie bezpieczeństwa (...)[29] i odnosząc to do stanowiska A. Beaufre, który przyjmuje, że zadaniem strategii jest osiągnięcie celów ustalonych przez politykę, wykorzystując jak najlepiej posiadane środki[30] - to rodzi się pytanie: jak trzeba postępować aby właśnie tak przyjętą (w dokumentach rządowych i międzynarodowych) logikę przełożyć na właściwe działanie aby osiągnąć cele polityczne? Drogę do znalezienia odpowiedzi na tak sformułowane pytanie wskazuje prof. T. Kotarbiński opisując prakseologiczne rozumienie działania - w myśl czego działać ... to tyle ... co zmierzać do określonego celu w danych warunkach przy pomocy właściwych środków[31]. W odniesieniu do strategii obronnej państwa - rozumianej jako element strategii bezpieczeństwa narodowego państwa – właściwe osiągnięcie jej celu może następować jedynie pod warunkiem, że zadania zrealizowane w kontekście tego celu będą również brać pod uwagę priorytety wynikające ze stosownych postanowień (i logiki politycznej) prawnych zawartych w dokumentach typu strategia bezpieczeństwa państwa uwzględniająca także uwarunkowania i zobowiązania międzynarodowe.

W sytuacji III RP – jako państwa-członka NATO – zarówno „Strategia bezpieczeństwa RP"[32], jak również treść „Traktatu Północnoatlantyckiego" wskazują jednoznacznie na pierwszeństwo problematyki obronnej w odniesieniu do terytorium Polski przed gotowością państwa do zewnętrznej reakcji militarnej nawet w ramach sojuszu. Również wiele „zadań terytorialnych" (m.in. o charakterze infrastruktury obronnej) wynikających z roli RP jako „państwa-gospodarza" wskazuje na wagę

---

[28] NATO – vademecum, Bellona, Warszawa 1995, s. 261-264.

[29] Słownik terminów z zakresu bezpieczeństwa narodowego", AON. Warszawa 1996, s. 83-84.

[30] A. Beaufre: „Wstęp do strategii. Odstraszanie i strategia", Warszawa 1968, s. 30.

[31] T. Kotarbinski: „Traktat o dobrej robocie", Wrocław 1975, s.19.

[32] Jeśli spojrzeć pod tym kątem na „Strategie bezpieczeństwa Rzeczpospolitej Polskiej", przyjętej i ogłoszonej przez rząd RP, to musi budzić „strategiczny niepokój" założenie, że *w przewidywalnej przyszłości nic temu państwu nie zagraża.* Stwierdzenie tego rodzaju nie tylko niezasadnie usypia społeczeństwo i odstręcza je od łożenia na bezpieczeństwo (które jak na ironie jest coraz mniejsze – nawet widać to już na ulicach, a nie tylko na granicy państwa), ale kompromituje wręcz państwo zarówno w oczach opinii społecznej, jak również na zewnątrz.

i pierwszeństwo terytorium Polski w podejmowaniu spraw obrony państwa przed operacyjną gotowością części Sił Zbrojnych RP do działań na zewnątrz. Jest to zgodne z jedną z podstawowych zasad strategicznych, z której wynika, że chcąc wybierać się na interwencję zewnętrzną należy wpierw zabezpieczyć militarnie granicę i terytorium w takim stopniu aby:

- nie zachęcać słabością obronną do agresji na własne terytorium;
- w wypadku poniesienia klęski w działaniach poza granicami można było skutecznie chronić się przed odwetowym działaniem zbrojnym na własnym terytorium.

W sytuacji, kiedy pierwszoplanowego znaczenia nabiera obrona granicy państwa i przygotowanie jego terytorium do obrony przed innymi zadaniami obronnymi, w tym także sojuszniczymi realizowanymi poza granicami, pojawia się pytanie: jakimi siłami militarnymi można to czynić? Odpowiedź w zasadzie może być tylko jedna – zresztą kształtowana doświadczeniem zawartym w sztuce wojennej, zbieranym przez tysiąclecia funkcjonowania cywilizacji nie tylko europejskiej. Otóż mając określoną wielkość wojsk operacyjnych – limitowaną m.in. postanowieniami CFE i systematycznie zmniejszanym „wysiłkiem" budżetowym państwa na obronność – „rezerw na rzecz zwiększenia skuteczności obrony państwa" można poszukiwać jedynie w tworzeniu wojsk terytorialnych, z których najtańszymi są wojska lokalne funkcjonujące w strukturze terytorialnych dowództw obrony (terytorialnych organów dowodzenia) - czyli rozbudowanych do wymaganych wielkości wojsk obrony terytorialnej.

W początkach lat dziewięćdziesiątych przyjmowano, że rozwinięte wojska operacyjne RP są w stanie „panować" obronnie na obszarze nie większym niż 3% terytorium Polski. Obecnie wiele jednostek z tamtego okresu już na stałe rozwiązano, a i potencjał tych, które pozostały spadł znacząco. W tej sytuacji rola i strategiczna ważność wojsk obrony terytorialnej jest nie tylko istotna, ale wciąż rosnąca – jako jedynego środka militarnego RP, na który państwo polskie jeszcze stać i który w stosunkowo krótkim czasie można wykorzystać do znaczącego podniesienia wielkości jego potencjału obronnego na własnym terytorium. Na poziomie strategicznym państwo dysponuje w sferze militarnej - obok wojsk obrony terytorialnej - wojskami operacyjnymi. Używane są one zarówno do działań ofensywnych, w tym agresywnych, poza własnym terytorium, jak również do obrony własnego terytorium. Jednak kompleksowo ostrzegając

obronę państwa należy przyjąć, że środkami właściwymi do jego obrony – tworzącymi także strategiczne korzyści w obronie własnego terytorium - są[33]:

1. Wojska obrony terytorialnej (regionalne i lokalne – w systemie dowodzenia terytorialnego).
2. Przygotowane - przez terytorialne organy dowodzenia - do obrony terytorium.
3. Wola obronna narodu (a w tym szczególnie jego elit politycznych oraz ludzi kultury), co do zakresu przygotowania i współudziału społeczeństwa w obronie państwa.
4. Działania nieregularne w masowej skali.
5. Wojska operacyjne.
6. Pomoc innych państw (systemy zbiorowego bezpieczeństwa), sojusze.

Uznany strateg C. von Clausewitz, w swym dziele „O wojnie" poświęca wiele uwagi wykorzystaniu całego „zakresu środków obrony"[34] właściwych do obrony państwa, gdzie główne miejsce – obok „twierdz, narodu, powstań narodowych i sprzymierzeńców" – zajmuje „obrona krajowa", jako formacja zbrojna (we współczesnym rozumieniu - wojska obrony terytorialnej). Wskazuje on także, iż „sztuka wojenna wymaga aby właśnie słabsi, skazani na obronę byli zawsze uzbrojeni, aby nie ulec napadowi"[35]. To kompleksowe w skali państwa clausewitzowskie podejście do jego obrony zawsze wzbudzało pogardę u mocarstw militarnych, które swój rozwój terytorialny (podboje) osiągały działaniami agresywnymi wojsk operacyjnych. Stąd zarówno ich wyżsi dowódcy wojskowi, jak również cywilni stratedzy polityczni osłabiali wszelkie „inne tendencje obronne", które ograniczały nakłady na wojska operacyjne – niby uszczuplające środki finansowe możliwe do wchłonięcia przez wojska operacyjne i niepotrzebnie (ich zdaniem) przeznaczane (rozpraszane) na inne środki obrony państwa niż tylko te wojska. Również dyplomacja państw mocarstwowych dbała i dba o to, aby w państwach mniejszych od tych, które reprezentuje niezbyt rozwijano narodowe wojska terytorialne (niezależnie czy są to państwa sojusznicze, czy też niezwiązane układem militarnym). Zatem nie należy obciążać ambasadorów mocarstw pytaniami w stylu: jakie powinniśmy mieć wojska?, gdyż odpowiedź będzie ta sama od tysięcy lat – „jedynie ograniczone wielkością nowoczesne wojska operacyjne, do których sprzęt możecie u nas pozyskać". Zatem

---

[33]Por.: „Zakres środków obrony" (państwa - przyp. R. J.) w C. von Clausewitz, „O wojnie", Warszawa 1995, s. 443-450. Clausewitz uważany jest przez Amerykanów za „ojca współczesnej strategii" (A. i H. Toffler; „Wojna i antywojna", Warszawa 1997, s. 59) – w Polsce zaś często, za *niegodnego uwagi i przeżytek historii* - tak właśnie jak to uważał J. Stalin.

[34]C. von Clausewitz: „O wojnie": Lublin 1995, s. 443-450.

[35]C. von Clausewitz, tamże s. 441.

gloryfikowane pierwszeństwa nakładów i poniekąd super ważności (ponad inne środki obrony państwa) wojsk operacyjnych przez państwa mocarstwowe było i jest także propagandowo im wygodne, gdyż w momencie wmówienia słabszemu państwu konieczności budowy jego obrony jedynie (lub głównie) w oparciu o wojska operacyjne stawia się je w roli przegranego, ponieważ w takiej sytuacji nigdy nie było ono i wciąż nie będzie w stanie stawić skutecznie czoła armii potężnego (siłą i wielkością wojsk operacyjnych) „mocarza operacyjnego" – a często wkrótce, także agresora.

W XX wieku propagandowa działalność w tej dziedzinie wielu imperialnych państw europejskich wywarła dość istotny wpływ na poglądy teoretyków zajmujących się strategią obrony państwa. Jest to efektem dość agresywnego zwalczania myśli tych, którzy postulowali budowę obrony państwa w oparciu o kompleksowe wyzyskanie potencjału własnego terytorium i znajdujących się tam mieszkańców. Stalin wręcz zabraniał poznawania poglądów C. von. Clasewitza, gdyż logika tego teoretyka i praktyka strategii obrony państwa zagrażała m.in. planom stalinowskiej strategii agresji wobec Europy oraz wskazywała na zaniedbania w kompleksowym budowaniu bezpieczeństwa państwa radzieckiego „na miejscu". Wprawdzie Stalina już nie ma i o Clasewitzu można już mówić od dłuższego czasu, zarówno w wojskowych uczelniach radzieckich, jak również rosyjskich, to jednak rosyjski „kręgosłup" w sferze obronności jest wciąż stalinowski – cechuje go wręcz komunizm wojenny. Jest to jedna z przyczyn zasadniczych kłopotów ekonomicznych bezpowrotnie upadającego już imperium agresywnej ekspansji terytorialnej.

Filozofia w myśl, której wszystko (pierwszeństwo) było dla wojsk operacyjnych zdegenerowała społecznie państwo i zniszczyła jego podstawy ekonomicznego funkcjonowania. Rosja obecnie jest największym złomowiskiem sprzętu bojowego, którego ochrona pochłania tak znaczne nakłady środków finansowych, iż nie stać jej nie tylko na konserwację i podtrzymywanie sprawności bojowej posiadanego sprzętu oraz liczącą się produkcję nowego, lecz także wypłaty pensji dla kadry zawodowej i żołdu żołnierzom. Ochrona sprzętu specjalnego w Rosji – w tym strategicznych systemów broni masowego rażenia o zasięgu międzykontynentalnym - jest „sponsorowana" przez Zachód.

Kiedy równocześnie łoży się na oba komponenty sił zbrojnych – wojska obrony terytorialnej i wojska operacyjne – oraz inne elementy systemu obrony państwa (powszechne przeszkolenie wojskowe, utrzymanie infrastruktury obronnej na własnym terytorium, przygotowanie do działań nieregularnych na dużą skalę, szukanie sojuszników militarnych), to w sytuacji Polski – gdzie 70% to stary sprzęt bojowy i w większości mało

skuteczny[36] na współczesnym polu walki – można byłoby mieć wszystko pozostałe oprócz nowoczesnych wojsk operacyjnych. Stawiając przez ostanie dziesięć lat jedynie na wojska operacyjne[37] doprowadzono do stanu, gdzie państwo polskie ma tylko „kupę" ruchomego złomu bojowego i żadnego pomysłu na inne niż dotychczas tworzenie armii – prawie jak w Rosji.

Ten kto przyjmuje, że w strukturze jego sił zbrojnych znaczące miejsce mają wojska obrony terytorialnej, daje poniekąd do zrozumienia sąsiadom, że jego strategia wojskowa ma charakter defensywny. Tak postrzega to H. Mendershausen przyjmując, że „państwo, które kładzie nacisk na rozwój obrony terytorialnej będzie z reguły usiłowało przekonać inne kraje, że nie zagraża ich integralności terytorialnej, chociaż może zagrażać wojskom przeciwnika. (...) Rzeczywisty lub potencjalny agresor (...) będzie prawdopodobnie uważał, że skutecznie działające wojska obrony terytorialnej stanowią zagrożenie dla jego własnych działań"[38], kiedy przystąpi on do agresji. Kontynuując dodaje, że „zgodnie z opracowanymi doktrynami dla wojsk obrony terytorialnej konieczne jest wykonanie gwałtownego ataku jednak na terytorium własnego kraju. (...) Chociaż są one bierne pod względem strategicznym, to jednak aktywne pod względem taktycznym". Jeśli uwzględni się – za A. Beaufre - iż „wybór taktyki to strategia" (i w dodatku fakt – że wojska obrony terytorialnej taktyką stoją), to taka konstrukcja logiczna pozwoli przyjąć założenie o następującej treści: wojska obrony terytorialnej są prostą konsekwencją strategicznego wyboru i z tego względu mają znaczenie strategiczne – stąd też strategia obrony państwa określa ich charakter, zadania i struktury (a nie strategia wojskowa, która w wypadku Polski - za podstawę wielkości wojsk OT przyjmuje coraz mniejsze stany rezerwowej broni lekkiej - systematycznie wysprzedawanej od kilku lat przy akceptacji operacyjnych skutków takich działań przez kolejnych szefów Sztabu Generalnego).

Na istotę strategii w odniesieniu do potrzeb obrony wskazuje gen. A. Beaufre, twierdząc, że „wszystkie (...) względy przemawiają za zorganizowaniem we Francji prawdziwej służby terytorialnej obok stałych (...) oddziałów bojowych. (...) Taki system służby milicyjnej jest niezbędną częścią składową systemu wojskowego epoki jądrowej, ponieważ tylko on i to najmniejszym kosztem, potrafi przystosować się do nieskończonej liczby różnych okoliczności, których nie można przewidzieć (...). Jednostki milicyjne (...)

---

[36]Jest to niemal ta sama jakość środków, które Jugosłowianie mogli jedynie chować przed środkami walki NATO podczas wojny w Kosowie w 1999.

[37]Inne podejście w tym względzie jest ośmieszane już w fazie wstępnej i nie podlega nawet merytorycznemu osądzeniu przez spadkobierców imperialnych filozofii obrony państwa.

[38]H. Mendershausen: „Reflections on Territorial Defense" - RAND C., 1980.

mogłyby stanowić lokalną kuźnię obywatelską.[39] O wadze uwzględniania w strategii wielu potencjalnych zagrożeń wypowiada się także prof. T. Kotarbiński, przyjmuje on wręcz, że do istoty pojęcia strategii należy "wielowariantowość", czyli to, że uwzględnia ona wszelkie sytuacje[40] z jakim można się spotkać. Stąd wskazywał – „każdą swoją strategię oceniaj wedle najgorszej ewentualności jaka się może zdarzyć, gdy ją zastosujesz. Wybierz tę strategię, która z takiego właśnie punktu widzenia jest względnie najlepsza".[41] Wtóruje mu w tym gen. A. Beaufre, który zakładał, że w strategii nie należy obierać za punkt wyjścia tego, co jest możliwe, ale szukać tego, co jest konieczne i starać się to osiągnąć".[42]

Polski teoretyk wojskowości gen. F. Skibiński podejmując problem obrony terytorium odnosi się także do wojsk terytorialnych – pod którymi rozumie on zarówno regionalne, rezerwowe, jak i lokalne oraz inne wykorzystywane na terytorium państwa – i postuluje, że „już z samego faktu istnienia - i przeznaczenia do ściśle określonych zadań - uderzeniowych sił zbrojnych wynika automatycznie potrzeba dysponowania innym „gatunkiem" sił, które też organizuje się wszędzie pod taką czy inną wersją nazwy Terytorialnych Sił Zbrojnych".[43] Dodaje nawet, iż „wojska terytorialne nie mogą być traktowane jako ubogi krewny...", ponieważ uważa, że „gdyby bitwa przeniosła się na własny obszar krajowy..., wojska terytorialne musiałyby wtedy wystąpić w roli równorzędnego partnera w stosunku do własnych wojsk uderzeniowych, a w stosunku do nieprzyjaciela - w roli co najmniej równego przeciwnika".[44]

Starożytny strateg chiński Sun Tzu przyjmuje, że terytorium jest podstawą istnienia państwa. Jak można go odstąpić?[45] A na temat jego przygotowania do działań zbrojnych wyraża się następująco: ten kto pierwszy zajmuje pole bitwy i tam oczekuje wroga, jest w lepszej sytuacji niż ten kto później wkracza (...), zaś dalej dodaje, wskazując na przygotowanie do obrony lokalnej (na miejscu) - jeśli jesteś w stanie utrzymać wszystkie ważne strategiczne punkty (...) możesz nie obawiać się, że wróg wkroczy[46] (...) Przestępstwem jest (...) nie przygotować się do wojny. Przygotowanie się na wszystkie ewentualności jest powodem do dumy[47]. Aby chociażby częściowo przygotować się do

---

[39]A. Beaufre: „Wstęp do strategii. Odstraszanie i strategia", Warszawa 1968, s. 236.
[40]T. Kotarbinski, „Abecadło praktyczności", Warszawa 1972 r. s. 23.
[41]Op. cit., s. 24.
[42] Beaufre A., op. cit., s. 161.
[43]F. Skibinski: „Rozważania o sztuce wojennej", WIN, Warszawa 1990, s. 318.
[44]Tamże, s. 320.
[45]Sun Tzu: „Sztuka wojny", Warszawa 1994, s. 19.
[46]Jak wyżej , s. 65.
[47]Jak wyżej , s. 42.

tych bardziej prawdopodobnych „ewentualnościach" postrzeganych jako wyzwania i zagrożenia w sferze bezpieczeństwa, należy posiadać siły zbrojne, które byłyby w stanie „panować" wojskowo na obszarze przynajmniej kilkudziesięciokrotnie większym, niż gwarantują to czynić wojska operacyjne – zdolne jedynie do „sztampowej", a nie wszelakiej obrony na przestrzeni nie większej niż 3% terytorium państwa i w dostatku przedkładające bardziej zewnętrzną mobilność zagraniczną nad wewnętrznymi potrzebami RP. Teza Sun Tzu bezpośrednio koresponduje z tym na co wskazuje Clausewitz odnośnie t e r y t o r i u m, które w strategii jest podstawową kategorią przy osiąganiu celów polityki. Zatem ze strategicznych podstaw budowy obrony państwa wynika konieczność posiadania wojsk, które zagospodarują terytorium, czego w wypadku rozwijania jedynie wojsk operacyjnych nie bierze się pod uwagę w stopniu wymaganym dla odpowiedzialnego traktowania bezpieczeństwa obywateli i ich mienia znajdującego się w obrębie granic państwa polskiego. Nie uwzględnia się także ochrony i obrony dóbr kultury materialnej i majątku narodowego, gdyż wojska te nie powinny być rozdrabniane. W tej sytuacji konieczne są terytorialne formacje zbrojne masowo organizowane w każdym miejscu – stosownie do potrzeb. Mogą to być w wypadku Polski jedynie wojska OT.

Uogólniając powyższe rozważania można przyjmować, że przy budowie bezpieczeństwa państwa w obszarze stosowania czynnika militarnego na poziomie strategicznym[48] (w skali państwa) nie można go opierać jedynie na wojskach operacyjnych, lecz w jak największym stopniu wyzyskiwać do tego obronę wykorzystującą całe terytorium – teren (jego rzeźbę i pokrycie), a głównie zasoby osobowe i materialne, produkcję i usługi znajdujące się na nim. Aby tego dokonać wystarczy na to co funkcjonuje „w terenie" „nałożyć organizację", która najlepiej spośród innych funkcjonuje w warunkach zagrożenia. Jest nią bez wątpienia organizacja wojskowa – i od wieków nazywa się obroną terytorialną. Przy czym powinna ona funkcjonować

[48]Właściwie wykorzystując wojska obrony terytorialnej w skali strategicznej stwarza się podstawę do optymalnego wykorzystania wojsk operacyjnych. Oceniając strategię wojenną państwa można - bez większego błędu - określać jej charakter, m.in. przez rolę i znaczenie w niej wojsk obrony terytorialnej. Jeśli stanowią one podstawę podsystemu militarnego (sił zbrojnych) w ramach sytemu obronnego państwa, to należy przyjmować, że państwo to posiada defensywną strategię wojskową. Natomiast, gdy podstawę tę tworzą wojska wewnętrzne lub regionalne wojska terytorialne albo wojska rezerwowe (wojska terytorialne przeznaczone także do wspierania wojsk operacyjnych, interwencyjnych poza terytorium państwa) - nie ma już takiej pewności. Dominacja wojsk wewnętrznych w systemie wojskowym nie tylko świadczy o wewnętrznych problemach narodowościowych (tendencjach separatystycznych lub narodowo-wyzwoleńczych – i konieczności ich posiadania do przeciwdziałania takim zjawiskom) ale i o chęci „pełnego politycznego" wewnętrznego panowania rządzących - z pomocą także tych wojsk - w celu posiadania możliwości interweniowania poza granicami resztą sił zbrojnych (nawet regionalnymi wojskami terytorialnymi – co zresztą czynili już w XIX wieku Prusacy z Landwehrą; mimo, że w zasadniczej masie była to regionalna formacja terytorialna). Podobnie z wojskami terytorialnymi postępowali Niemcy podczas II wojny światowej i Chińczycy w wojnie przeciw Wietnamowi w 1979 r., a także Amerykanie w wojnie przeciw Irakowi.

w okresie braku zagrożeń w zalążkowej formie, lecz ze sprawnie działającym systemem kierowania nią – zarówno podczas zbierania informacji i ich przetwarzania, jak również podczas jej rozwijania do działań i w trakcie ich trwania.

Położenie geopolityczne państwa ma także istotny wpływ na jego strategiczne przygotowania obronne – niewystarczające uwzględnianie tego aspektu w strategii obronnej państwa zazwyczaj niekorzystnie wpływa na jego bezpieczeństwo. Przykładem tego jest polityka obronna (lub jej istotne niedomogi) bezpośrednio przed rozbiorami Polski – kiedy w małym stopniu brano pod uwagę wielkości sił zbrojnych agresywnych kolonialnie sąsiadów oraz centralne położenie Rzeczypospolitej wobec tychże, i w Europie. Nie uwzględniano także faktu przebiegu przez terytorium Polski strategicznych szlaków komunikacyjnych między mocarstwami europejskimi, a także szlaku międzykontynentalnego.

Będąc państwem średniej wielkości, sąsiadującym z mocarstwami (mocarstwem militarnym) - posiadającymi przewagę w wojskach operacyjnych - należy tworzyć taki system obrony państwa, który w maksymalnym stopniu umożliwiałby wykorzystanie potencjału mieszkańców i infrastruktury obronnej na rzecz obrony powszechnej.

Wszystkie państwa[49] demokratyczne Europy sąsiadujące z państwami wchodzącymi w skład sojuszy militarnych – zarówno NATO, jak i byłego Układu Warszawskiego – a nie będące ich członkami posiadały i posiadają z tego głównie powodu silnie rozbudowane systemy obrony terytorialnej, których wojska są podstawowym komponentem ich sił zbrojnych. Państwa demokratyczne będące członkami sojuszu, a znajdujące się na jego obrzeżu – jako państwo graniczne[50] - miały i mają także znacznie rozbudowane systemy obrony terytorialnej i funkcjonujące w nich liczne terytorialne wojska lokalne i regionalne.

W ten sposób wytworzono dodatkowy potencjał do obrony państwa, którego nie można było uzyskać nawet przy nowoczesnych i rozbudowanych wojskach operacyjnych. Niweczono więc podstawowe założenia skutecznej agresji - uniemożliwiając agresorowi wyzyskania jego przewagi, inicjatywy i zaskoczenia w rozstrzygającej bitwie pomiędzy ścierającymi się wojskami operacyjnymi. Innymi słowy, uchylając się od regularnych bitew i "rozmienianie" ich, wbrew temu do czego dąży agresor, na "tysiąc walk" - jak

[49] Austria, Finlandia, Szwecja, Szwajcaria.
[50] Norwegia, Dania, Niemcy.

twierdził Mossor[51] - stworzono warunki do „niepokonalności"[52]. Przykłady klasyczne to obrona Polski za Piastów i przed potopem szwedzkim w drugim etapie wojny.

P r z e s t r z e ń o b r o n n a P o l s k i to jeden z najważniejszych atutów obrony RP. Powinien on być uwzględniany w tworzeniu strategii bezpieczeństwa i obrony Polski. Rzeczpospolita przełomu tysiącleci to terytorium o średnich wymiarach 600×600 km, które po odpowiednim przygotowaniu do działań nieregularnych jest w stanie stworzyć niebezpieczne „grzęzawisko zbrojne" dla każdej armii - nie tylko, że nie do zdobycia, pokonania lub przejścia go ale także w wypadku wtargnięcia weń z krztą szansy na bezpieczne wycofanie się. O jej randze świadczy stwierdzenie gen. W. Sikorskiego „wszyscy ci wodzowie (Aleksander Wielki, Hannibal, Dżyngis-chan i Napoleon - przyp. aut.) nie uniknęli losu, który im zgotowała wchłaniająca ich siły i osłabiająca stopniowo ich energię działania, niezwyciężona ostatecznie (...) i nie podbita przez nich – p r z e s t r z e ń"[53]. Problem przestrzeni jest o tyle ważny iż niekiedy postrzega się jej znaczenie dopiero w działaniach na terytorium dużych państw (np. Rosja, itp.) – w kontekście ogromnych odległości do pokonania przez wojska. Małe znaczenie przywiązuje się jednak do przestrzeni w kontekście „zajętości terenu" (przez nakładające się na siebie działaniami różne struktury wojsk i coraz częściej cywilną działalność na rzecz logistyki wojskowej).

Współcześnie – kiedy to nasycenie terytorium państwa broniącego się „małą techniką walki" może być relatywnie mało kosztowne i masowe – problem pokonania przestrzeni nawet równinnej, przy dużym wskaźniku zabudowy trwałej (takiej m.in. jak w Polsce), jest nie mniej ważny i równie kłopotliwy dla agresora jak bywa to w górach i na bagnach albo rozciągniętym po horyzont stepie, czy też bezgranicznej pustyni. Po prostu „obcy" teren staje się zdradliwy w trakcie przemieszczania się wojsk, niebezpieczny dla żołnierzy nawet na ubezpieczonych postojach i w obozowiskach, i przez to wyjątkowo trudny do pokonania i utrzymania go.

Niedostateczne postrzeganie i rozwiązywanie problemów przestrzeni w zakresie zajętości terenu może nieść negatywne skutki w działaniach wojsk - równie tragiczne jak

---

[51] S. Mossor, op. cit. , s. 196.

[52] Taka strategia obronna Szwajcarii uchroniła ją przed agresją Hitlera, który bał się „ugrzęźnięcia zbrojnego" w tym małym ale doskonale obronnie zorganizowanym państwie. Współcześnie *groźba „ugrzęźnięcia" na obcym terytorium* - jak to określają taką niewydolność operacyjną wojsk lądowych amerykańscy wojskowi, po tragicznych doświadczeniach z Wietnamu i Somalii – odstrasza NATO przed interwencją w Jugosławii. Ten „obronnie grząski" teren wytwarzają masowo tworzone formacje terytorialne - przy ich zatem wykorzystaniu podniesiony niewiele poziom obronności na całym terytorium jest „grzęzawiskiem zbrojnym" nie do przebycia przez zwarte formacje operacyjnych wojsk lądowych agresora. Na takie terytorium można natomiast oddziaływać jedynie z powietrza, ale póki co bez zajęcia terytorium nikt do tej pory wojny nie wygrał.

[53] W. Sikorski: „Przyszła wojna", Warszawa 1984. S.255.

ogromne odległości. Niedobór bowiem środków zaopatrzeniowych i uzupełnianie przemęczonym oraz „zdziesiątkowanym" stanom osobowym wojsk lub ich chaotyczne dostarczanie jednakowoż jest dokuczliwe i opłakane w skutkach - niezależnie czy powstaję wskutek zakłóceń powodowanych dużymi odległościami, czy też z powodu blokady funkcji logistycznych powstającej wskutek nakładania się na siebie przedsięwzięć wzajemnie nieskoordynowanych. Powstające blokady w rytmiczności dostaw oraz straty materiałowe i osobowe - będące skutkiem uderzeń przeciwnika w miejsca nadmiernej koncentracji wysiłku logistycznego i manewru wojskami - są równie niekorzystne dla prowadzących walkę, jak zakłócenia wynikające z braku dostaw powodowanych koniecznością pokonania znacznych odległości.

W dobie coraz większej i szybo postępującej urbanizacji Europy oraz automatyzowania i pełnej mechanizacji procesów walki, a także nasycania logistyki wojskowej technicznymi środkami transportu ważne jest także „panowanie nad przestrzenią na potrzeby wojsk" - nad niemal każdym skrawkiem przestrzeni własnego terytorium (jego drogami, węzłami komunikacyjnymi i rejonami składowania środków walki oraz koncentracji i mobilizacji wojsk). Jest to coraz większym problemem nie tylko na rozległych przestrzeniach ale często w państwie średniej wielkości. Częstokroć waga przestrzeni w rejonach o dużej koncentracji zabudowy i różnorodności pokrycia terenu może mieć większe znaczenie dla działań wojsk (szczególnie w obronie) niż rozwiązywanie problemów wynikających z pokonywalności znacznie rozleglejszych przestrzeni – szczególnie jeśli uwzględni się możliwości rażenia przy pomocy rakiet manewrujących (dla których rozległość przestrzeni nie stanowi większego problemu).

2. UWARUNKOWANIA SOJUSZNICZE

Rozważanie tego problemu celowo jest przeprowadzić na podstawie dorobku prawnego (tzw. „NATO Acquis") i doświadczeń sojuszu z uwzględnieniem specyfiki położenia Polski na obszarze euroatlantyckim, zagrożeń z tego wynikających oraz roli Polski w NATO. W dokumencie przyjętym przez szefów państw i rządów uczestniczących w spotkaniu Rady Północnoatlantyckiej w dn. 23-24 kwietnia 1999 roku potwierdzony jest niezmienny cel sojuszu i wytyczone zasadnicze zadania w dziedzinie bezpieczeństwa. Koncepcja umożliwia przekształconemu NATO wnoszenie wkładu do zmieniającego się środowiska bezpieczeństwa oraz wspierania bezpieczeństwa i stabilności. Koncepcja

wyznacza kierunki polityki bezpieczeństwa i obrony sojuszu, jego doktryny operacyjne, kształt sił konwencjonalnych i nuklearnych oraz zasady kolektywnej obrony.

Podstawowym i niezmiennym celem NATO ustanowionym w Traktacie Waszyngtońskim jest zapewnienie wolności i bezpieczeństwa wszystkich państw członkowskich, przy użyciu politycznych i wojskowych środków. W oparciu o powszechnie uznawane wartości, jak demokracja, prawa człowieka i rządy prawa, sojusz dążył, od samego początku swojego istnienia, do stworzenia w Europie sprawiedliwego i trwałego porządku, opartego na pokoju. Cel ten w dalszym ciągu będzie realizowany. Jego osiągnięcie może być utrudnione przez kryzysy i konflikty mające wpływ na bezpieczeństwo przestrzeni euroatlantyckiej. Dlatego właśnie jest ważne, aby NATO nie tylko było w stanie bronić swych członków, lecz także mogło przyczynić się do bezpieczeństwa i stabilności w regionie.

Podstawową zasadą w oparciu, o którą funkcjonuje sojusz są wzajemne gwarancje i współpraca między suwerennymi państwami, mająca wspierać zasadę niepodzielności bezpieczeństwa wszystkich państw członkowskich. Dzięki solidarności i spójności NATO żaden z sojuszników nie będzie osamotniony w wypadku zagrożenia. Zasady, na których opiera się kolektywna współpraca znajdują odzwierciedlenie w praktycznych rozwiązaniach, pozwalających sojuszowi na maksymalne wykorzystanie środków politycznych, wojskowych, posiadanych przez niego zasobów oraz zapobiegają renacjonalizacji polityki obronnej nie pozbawiając sojuszników suwerenności. Rozwiązania te umożliwiają siłom sojuszu realizację operacji reagowania kryzysowego wykraczających poza artykuł 5, są również konieczne do tego, aby sojusz mógł reagować na wszystkie pozostałe zagrożenia.

Komunikat „szczytu waszyngtońskiego" wydany przez szefów państw i rządów uczestniczących w spotkaniu Rady Północnoatlantyckiej w Waszyngtonie 24 kwietnia 1999 r. w pkt. 42 stwierdza m.in.: Terroryzm stanowi poważne niebezpieczeństwo dla pokoju, bezpieczeństwa i stabilności, które może zagrozić terytorialnej integralności państw. Ponownie potępiamy terroryzm oraz potwierdzamy naszą wolę walki z nim zgodnie z naszymi międzynarodowymi zobowiązaniami i prawem narodowym. Zagrożenie terrorystyczne dla sił i baz NATO wymaga rozważenia i rozwoju odpowiednich środków dla ich stałej ochrony, biorąc w pełni pod uwagę obowiązki państwa-gospodarza.

Dla wszystkich tych rozwiązań podstawę stanowią uzgodnione procedury, zintegrowana struktura wojskowa oraz porozumienia o współpracy. Główne z tych rozwiązań to: wspólne planowanie sił, wspólne fundusze, wspólne planowanie operacyjne,

formacje wielonarodowe, dowództwa i systemy dowodzenia, zintegrowany system obrony powietrznej, zrównoważony podział ról i obowiązków wśród sojuszników, stacjonowanie i rozmieszczenie sił, gdy zachodzi taka potrzeba, poza ich rodzimym terytorium, rozwiązania umożliwiające rozwiązywanie kryzysów i wzmocnienie (łącznie z jego planowaniem), wspólne standardy i procedury związane z wyposażeniem sił, ćwiczeniami oraz logistyką, doktryny odnoszące się do wielonarodowych i połączonych ćwiczeń, infrastruktura, współpraca w zakresie uzbrojenia i logistyki.

W dokumentach NATO podkreśla się, że wielkość wszystkich sił sojuszu będzie utrzymana na najniższym poziomie niezbędnym do sprostania wymogom kolektywnej obrony i innych misji sojuszniczych. Ich gotowość będzie w odpowiedni sposób zróżnicowana. Zakłada się, że geograficzne rozmieszczenie sił sojuszu w czasie pokoju zapewniać będzie odpowiednią ich obecność na terytorium sojuszu, łącznie ze stacjonowaniem i rozmieszczeniem sił poza ich rodzimym terytorium i wodami oraz wysuniętą obecnością sił, wtedy i tam, gdzie to jest konieczne.

Koncepcja strategiczna sojuszu zakłada również, że w związku z redukcją sił NATO i kurczącymi się zasobami, coraz większe znaczenie dla efektywnej realizacji misji sojuszu odgrywa zdolność do współpracy między sojusznikami. W tym kontekście dużą rolę odgrywają rozwiązania zwiększające skuteczność kolektywnej obrony, jak np. zintegrowana struktura wojskowa. Istnieje potrzeba efektywnej koordynacji, na wszystkich poziomach poszczególnych elementów natowskiego planowania obronnego, w celu przygotowania sił i struktur NATO do realizacji pełnego spektrum misji sojuszu. Zwiększeniu dostępności sił i środków, które mogą być przeznaczone do realizacji tychże misji sprzyja wymiana informacji między sojusznikami na temat ich narodowego planowania sił. Członkowie paktu, chcąc elastycznie reagować na ewentualne zagrożenia i efektywnie realizować swoje misje, powinni dysponować odpowiednimi rozwiązaniami logistycznymi (w odniesieniu np. do transportu i wsparcia medycznego) oraz środkami umożliwiającymi im rozmieszczenie i skuteczne wsparcie wszystkich rodzajów posiadanych sił. Sprzyjać współpracy będzie również proces standaryzacji i obniżenie kosztów wsparcia logistycznego. Poważnym wyzwaniem logistycznym ma być podtrzymanie operacji wykraczających poza terytorium traktatowe, na obszarze z niewystarczająco rozwiniętą infrastrukturą państwa-gospodarza, lub jej całkowitym brakiem. Zdolność do wygenerowania na czas większych sił, odpowiednio wyposażonych i wyszkolonych, zdolnych do realizacji pełnego spektrum misji sojuszu będzie również stanowić istotny wkład do rozwiązywania konfliktów i obrony. Wiąże się to z gotowością

wzmocnienia każdego zagrożonego obszaru i ustanowienia tam, jeżeli zajdzie taka potrzeba, obecności międzynarodowej. Różnego rodzaju siły, o zróżnicowanych stopniach gotowości powinny być zdolne do rozmieszczenia, zarówno w ramach wzmocnienia w Europie, jak i z Ameryki do Europy. Wymagać to będzie kontroli linii komunikacyjnych oraz odpowiednich rozwiązań związanych ze wsparciem i ćwiczeniami.

Dla powodzenia operacji realizowanych przez NATO ogromne znaczenie mają również związki między siłami sojuszu i lokalnymi władzami cywilnymi (zarówno rządowymi, jak i pozarządowymi). Współpraca cywilno-wojskowa jest wzajemnie zależna: władze cywilne coraz częściej potrzebują środków wojskowych, z drugiej strony dla operacji militarnych ogromne znaczenie ma wsparcie cywilne, jak np. logistyka, komunikacja, wsparcie medyczne i poparcie społeczne. Jednocześnie duże znaczenie mieć będzie w dalszym ciągu współpraca między wojskowymi i cywilnymi strukturami sojuszu.

W „Koncepcji Strategicznej Sojuszu" (pkt. 60) przyjętej w Waszyngtonie (23-24 kwietnia 1999 r.) czytamy dla powodzenia operacji realizowanych przez NATO ogromne znaczenie mają związki między siłami sojuszu i lokalnymi władzami cywilnymi (zarówno rządowymi, jak i pozarządowymi). Współpraca cywilno-wojskowa jest wzajemnie zależna: władze cywilne coraz częściej potrzebują środków wojskowych, z drugiej strony dla operacji militarnych kapitalne znaczenie ma wsparcie cywilne, jak np. logistyka, komunikacja, wsparcie medyczne i poparcie społeczne.

W Polsce problematyka wsparcia wojsk sojuszniczych na terytorium naszego państwa wzbudza żywe zainteresowanie w szerokich kręgach administracji publicznej i gospodarczej oraz kadry sił zbrojnych[54], ale mimo to widoczny jest brak kompleksowego podejścia do zjawiska i zdaje się przeważać myślenie o HNS jedynie w kategoriach logistycznych, choć obszar jego problematyki jest znacznie szerszy. Wydaje się, że aktualny stan struktur resortowych próbujących realizować problematykę HNS nie w pełni odpowiada zidentyfikowanym w toku badań obowiązkom państwa-gospodarza i może mieć trudności w realizacji zadań wynikających z dokumentów normatywnych NATO. Nie wypracowano do tej pory na szczeblu kraju rozwiązań systemowych w tym względzie.

Podejmowane dotychczas prace mają charakter rozproszony, gdyż prowadzone są jednocześnie przez kilka instytucji resortu obrony narodowej, głównie logistycznych, zwłaszcza w zakresie przygotowania infrastruktury wojskowej. Jednocześnie dostrzegalny

---

[54]S. Filipiak, *Współpraca cywilno-wojskowa w ramach wsparcia wojsk sojuszu ze strony państwa-gospodarza (Host Nation Support – HNS)* [w:] „Współpraca cywilno-wojskowa" *(Civil Military Cooperation – CIMIC)*. Materiały z konferencji naukowej zorganizowanej w Departamencie Społeczno-Wychowawczym MON w dniu 23 marca 1999r.DW Bellona, Warszawa 1999, s.52-59.

jest brak w instytucjach wojskowych komórek wyspecjalizowanych w sprawach HNS, organizujących i koordynujących całokształt działalności w tej dziedzinie.

Zgodnie z ustawą z dnia 4 września 1997 r. o działach administracji rządowej, Ministerstwo Obrony Narodowej kieruje działem – obrona narodowa – obejmującym, w czasie pokoju, m.in. sprawy: obrony państwa oraz sił zbrojnych Rzeczypospolitej Polskiej a także udziału Rzeczypospolitej Polskiej w wojskowych przedsięwzięciach organizacji międzynarodowych oraz w zakresie wywiązywania się z zobowiązań militarnych, wynikających z umów międzynarodowych.

O miejscu i randze misji wsparcia państwa-gospodarza w zapewnieniu wiarygodności i skuteczności odstraszania i obrony wspólnej NATO najlepiej świadczy treść punktu 60. „Koncepcji strategicznej sojuszu" z 23-24.04.1999 roku: „dla powodzenia operacji realizowanych przez NATO ogromne znaczenie mają również związki między siłami sojuszu i lokalnymi władz cywilnych (zarówno rządowymi, jak i pozarządowymi).

Współpraca cywilno-wojskowa jest wzajemnie zależna i władze cywilne coraz częściej potrzebują środków wojskowych, z drugiej strony dla operacji militarnych ogromne znaczenie ma wsparcie cywilne, jak np.: logistyka, komunikacja, wsparcie medyczne i poparcie społeczne. Jednocześnie duże znaczenie mieć będzie w dalszym ciągu współpraca między wojskowymi i cywilnymi strukturami sojuszu.

Również narodowe strategie bezpieczeństwa i obronności przyjmują za strategicznie ważne przygotowania Polski do wypełnienia misji HNS. W „Strategii bezpieczeństwa Rzeczypospolitej Polskiej" z 4.01.2000 r. stwierdzono, iż „kluczowe znaczenie dla integracji z sojuszem ma podejmowanie komplementarnych działań na szczeblu władzy ustawodawczej i wykonawczej służących umacnianiu zdolności obronnych państwa, w tym w sferze prawnej i ekonomiczno-finansowej. Działania praktyczne w sferze gospodarczo-finansowej powinny koncentrować się przede wszystkim na: (...) umiejętności wykorzystania Programu Inwestycyjnego NATO w Dziedzinie Bezpieczeństwa (NSIP) do rozbudowy infrastruktury na terytorium Polski, wykorzystywanej również przez inne państwa NATO, w tym zwłaszcza w celu wypełnienia przez Polskę obowiązków państwa-gospodarza (HNS). Podjęcie skutecznych działań na rzecz dostosowania systemu obronności państwa umożliwiające współudział w ramach NATO będzie wymagało m.in. (...) przygotowania infrastruktury wojskowej i cywilnej do przyjęcia i wsparcia sił wzmocnienia sojuszu w ramach wypełnienia obowiązków państwa-gospodarza.

Z kolei w „Strategii obronności Rzeczypospolitej Polskiej" z 23.05.2000 roku – solidarność i integrację sojuszniczą – określono jako jedną z zasad polskiej strategii obronności. Istota strategicznej rangi przedmiotu badań wynika z powszechnego charakteru wojny, której uczestnikami czynnymi i biernymi są nie tylko siły zbrojne, ale również całe społeczeństwo, gospodarka, terytorium, infrastruktura, itd. Już blisko 200 lat temu, po narodzinach państw narodowych i ukształtowaniu się w epoce napoleońskiej powszechnego charakteru wojen C. von Clausewitz w swym fundamentalnym dziele „O wojnie" sformułował następującą tezę: „kraj, wraz ze swym obszarem i zaludnieniem, jest nie tylko źródłem właściwych sił zbrojnych, ale również i sam przez się stanowi nieodłączną część sił działających w wojnie, a mianowicie tę jego część, która tworzy teatr wojny albo wywiera nań znaczny wpływ"[55].

Tak, więc przygotowanie i funkcjonowanie Polski jako wiarygodnego członka wspólnoty obronnej NATO oraz realność i skuteczność ewentualnego wzmocnienia przez siły NATO obrony terytorium Polski będzie zależeć powtarzając określenie z „Koncepcji strategicznej sojuszu" – w ogromnym stopniu właśnie od przygotowania polskiego społeczeństwa, gospodarki i terytorium do obrony – w tym do realizacji misji wsparcia państwa-gospodarza (HNS).

Początkiem wdrażania problematyki HNS do systemu obronnego RP była realizacja zadań wynikających z celu TG 4123 „Wsparcie państwa-gospodarza". Zgodnie z ustaleniami KSORM z dnia 17.12.1998 r., do czasu uzyskania członkostwa w NATO tymczasowo rolę koordynatora HNS w obszarze sił zbrojnych RP pełnił Zarząd Planowania Logistyki SG WP, a DSO MON w zakresie koordynowania i nadzoru nad problematyką HNS w pozamilitarnych ogniwach systemu obronnego państwa. Rozbudowa i modernizacja tych obiektów obejmuje:

- lotniska – zwiększenie długości dróg startowych, montowanie nowych systemów hamowania (hakowych), wykonanie systemów oświetleniowych do nawigacji, budowę systemów łączności,
- bazy morskie – dostosowanie paliwowych systemów do zaopatrywania okrętów NATO, rozbudowę nabrzeży do celów remontowych oraz załadowczych i wyładowczych dla jednostek o dużym zanurzeniu, budowę lądowiska helikopterów,

[55] C.von Clausewitz, „O wojnie", Lublin 1995, s. 10.

- składnice paliw – dostosowanie obiektów i instalacji nalewczych do wymogów i standardów NATO.

Pomimo podjętych działań[56], wdrażanie systemu wsparcia państwa-gospodarza nadal napotyka na liczne utrudnienia z uwagi na brak odpowiednich struktur HNS na szczeblu rządowym i SZ RP, ograniczone przydziały środków finansowych, zbyt wolne dostosowywanie polskiego prawodawstwa do wymogów NATO oraz nowe jakościowo uwarunkowania dotyczące np. projektów prac budowlanych, kosztorysów, itp.

Na ministrze obrony narodowej z racji kierowania działem – obrona narodowa – spoczywa również kierowanie przygotowaniem Polski do realizacji przedsięwzięć organizacyjnych misji wsparcia państwa-gospodarza. Z kolei „Strategia obronności RP" określa, iż „koordynatorem przygotowań obronnych w państwie jest minister obrony narodowej". Stąd też przed urzędem Ministerstwa Obrony Narodowej stoi olbrzymiej rangi wyzwanie intelektualne i organizacyjne przygotowania i utrzymywania gotowości i sprawności Polski do realizacji misji wsparcia państwa-gospodarza.

HNS[57] jest definiowane w NATO jako cywilna i wojskowa pomoc świadczona w czasie pokoju, w sytuacjach kryzysowych i podczas konfliktów, przez państwo, na którego terytorium przemieszczają się (także w tranzycie) lub są rozmieszczone i działają siły i organizacje NATO. Zakres realizowanych przedsięwzięć (pomocy) regulują zobowiązania wynikające z porozumień w ramach sojuszu lub z dwustronnych bądź wielostronnych umów zawartych miedzy państwem-gospodarzem oraz organizacją NATO (dowódcami NATO) i państwem (państwami) wysyłającymi wojska.[58]

---

[56]W pierwszej połowie 2000 r., w ramach wdrażania systemu HNS, zasadniczo realizowano przedsięwzięcia zmierzające do określenia obszarów odpowiedzialności SZ RP i innych resortów w formie spotkań roboczych oraz warsztatów i szkoleń z udziałem ekspertów Królewskich Sił Zbrojnych Holandii. Ponadto, w ramach realizacji II etapu celu TG 4123 rozpoczęto przygotowania do budowy scentralizowanej bazy danych państwa-gospodarza, zawierającej dane o infrastrukturze obronnej i zasobach materiałowych wojska i sektora cywilnego. Formalnie, dopiero w drugiej połowie 2000 r. Minister Obrony Narodowej, w celu koordynacji zadań dotyczących wsparcia państwa–gospodarza oraz ich realizacji w układzie terytorialnym, infrastruktury, logistycznym i mobilizacyjnym powołał Pełnomocnika ministra obrony narodowej do spraw wsparcia przez państwo–gospodarza (HNS) i systemu obrony terytorialnej (Decyzja nr 150/MON z 24 sierpnia 2000 r.). Zgodnie z decyzją nr 44 sekretarza stanu – I zastępcy MON z dnia 13 września 2000 r. powołano zespół do opracowania „Koncepcji wykonywania przez MON oraz inne organa administracji rządowej zadań wynikających z obowiązków państwa–gospodarza", która została rozpatrzona i przyjęta na posiedzeniu kierownictwa MON w dniu 8 stycznia 2001 r.

[57]HNS, zgodnie z definicją zamieszczoną w MC 334/1, *jest cywilną i wojskową pomocą udzielaną przez państwo-gospodarza (HNS) w czasie pokoju, stanach wyjątkowych, kryzysu lub konfliktu siłom i organizacjom sojuszniczym rozmieszczanym, działającym na jego terytorium lub przemieszczającym się przez nie. Uzgodnienia dokonane pomiędzy stosownymi władzami państwa-gospodarza (HNS) i państwa wysyłającego (SN) oraz/lub NATO stanowią podstawę takiej pomocy.* „Sojusznicza doktryna i procedury połączonego wsparcia przez państwo-gospodarza" AJP-4.5, Sztab Gen. WP., s. 1-1.

[58]NATO AAP(U) – „Słownik terminów i definicji NATO (angielsko-polski)", MON BWSN 1998, s.154; MC 334/1: (*Zasady i polityka NATO odnośnie państwa goszczącego -gospodarza*), p.6; ALP-9 (B): „Doktryna logistyczna sił lądowych" (Stanag 2406), p.204a i 1001c.

Wsparcie udzielane przez państwo przyjmujące powinno objąć:

- udzielenie pomocy (ułatwień) w czasie przyjęcia na granicy państwa;
- zapewnienie swobody przegrupowania do rejonu operacji, rozmieszczenia wojsk w terenie i działań;
- dostarczenie niezbędnych materiałów, usług i pomocy.

Zgodnie z założeniami logistyki NATO wsparcie dla sojuszników realizuje się głównie siłami wojskowymi, z wykorzystaniem zasobów wojskowych. Równocześnie dąży się jednak do maksymalizacji wyzyskania możliwości środków cywilnych – jeśli jest to celowe, realne, dostępne na czas i korzystne finansowo. Użycie zasobów cywilnych wiąże się bowiem z angażowaniem gospodarki gospodarza (niekiedy z jej mobilizacją) i jest łatwo dostępne raczej w rejonach uprzemysłowionych, przy czym sięganie do cywilnych źródeł zasilania pozwala utrzymywać nienaruszone zasoby własne wojska i obniżać koszty podejmowanych działań.

HNS obejmuje nie tylko zadania wsparcia logistycznego. Jego celem jest podtrzymywanie zdolności bojowej i swobody działania wojsk sojuszniczych, zaspokojenie ich potrzeb oraz uchronienie przed brakami materiałowymi uniemożliwiającymi wykonanie zadań.

Ważne jest przy tym, aby potrzebne zaopatrzenie i urządzenia pomocnicze były dostarczane: w potrzebnych ilościach; we właściwym czasie; we wskazane miejsca; w należytej jakości (w stanie użyteczności). Zwłaszcza sprawa jakości zasługuje na szczególną uwagę, gdyż (jak mogliśmy się przekonać goszcząc w 1998 roku na poligonie Śląskiego Okręgu Wojskowego holenderską jednostkę artylerii) sojusznicy dopuszczają do eksploatacji (wykorzystania) w zasadzie tylko materiały posiadające certyfikat jakości z serii ISO 9000.

Oprócz funkcji logistycznej HNS jest równocześnie specyficzną formą współpracy cywilno-wojskowej[59]. Celem CIMIC jest uzyskanie kooperacji zapewniającej tworzenie warunków zabezpieczających materialną i militarną przewagę nad przeciwnikiem. Inna z dostępnych definicji określa, że CIMIC to „zasady i przedsięwzięcia, które wspierają [...]" działania wojsk sojuszu[60].

Artykuł 5 Traktatu Waszyngtońskiego zobowiązuje państwa - członkowskie NATO do wzajemnej i wspólnej obrony militarnej. Mamy tu na myśli operacje wspólnej obrony

---

[59]Drążczyk W., „Zasady, procedury i zakres udziału logistyki sił powietrznych państwa-gospodarza w zabezpieczeniu przyjmowanych wojsk NATO (Host Nation Support – HNS)". AON, Warszawa 1999, s.9.
[60]AJP-1(A), op.cit., p.2103.

(CDO – Common Defence Operations). Strategia sojuszu odwołuje się do ugruntowanych już pojęć, takich jak państwo wysyłające i państwo goszczące. Co więcej w ostatnich latach obserwujemy znaczący wzrost udziału sił zbrojnych NATO w operacjach pokojowych wykraczających poza formułę artykułu 5, tj. w działaniach prowadzonych w ramach „operacji reagowania kryzysowego" (CRO - Crisis Response Operations) organizowanych także przez organizacje cywilne (ONZ, OBWE).

Z obu wyżej wymienionych rodzajów operacji wynika, że siły zbrojne poszczególnych państw członkowskich muszą być zdolne do prowadzenia różnorodnych operacji także, poza terytorium własnego państwa, to znaczy na terytorium państwa przyjmującego. Doświadczenia wyniesione z licznych i różnorodnych działań przeprowadzonych w ostatnim dziesięcioleciu ujawniły jak wielką rolę odgrywa wparcie ze strony państwa, na obszarze którego te działania są realizowane. Między innymi z tych powodów, w stosunku do państwa przyjmującego utrwaliło się określenie państwa-gospodarza.

O powodzeniu, zarówno operacji, jak też całej misji, czy to z zakresu wspólnej obrony, czy też reagowania kryzysowego albo dla potrzeb ćwiczeń, w znacznej mierze decyduje przygotowanie wsparcia ze strony państwa-gospodarza. Przy czym szczególne znaczenie ma udostępnienie lokalnej infrastruktury, zapewnienie dostaw materiałów i usług, koordynacja ruchu oraz jego ochrona, a także osłona operujących sił. Wsparcie to coraz bardziej nabiera na znaczeniu, stając się kluczową funkcją zabezpieczenia logistycznego, decydującą o zdolności działania wojsk państw–członków NATO.

Głównym celem realizacji wsparcia ze strony państwa-gospodarza jest ekonomizacja logistyki tych sił, a tym samym wydatne zwiększenie możliwości planowania i prowadzenia operacji.

Zasoby logistyki wojskowej wchodzącej w skład sił zbrojnych służą przede wszystkim zabezpieczeniu własnych potrzeb narodowych. Dlatego też wsparcie sił sojuszu musi być realizowane przy wykorzystaniu określonej i odpowiednio przygotowanej części potencjału gospodarczo-obronnego oraz struktur własnych sił zbrojnych i administracji publicznej państwa-gospodarza (państwa przyjmującego). Praktyka współcześnie prowadzonych operacji NATO wskazuje, że sektor cywilny nie tylko wypełnia lukę powstałą z powodu zwiększonego zapotrzebowania sił zbrojnych na określone usługi, nazwijmy je „cywilne", ale niejednokrotnie jest w stanie świadczyć swoje usługi taniej niż robiłyby to siły zbrojne. Wychodzi to naprzeciw jednej z podstawowych zasad NATO dotyczących „efektywności kosztowej", która musi być brana pod uwagę przy planowaniu

zabezpieczenia logistycznego operacji czy też ćwiczeń. Zakres i sposób wykorzystywania zasobów cywilnych w ramach HNS zależy od tego, czy omawiane wsparcie jest realizowane w czasie pokoju, czy też będzie ono udzielane w obliczu zewnętrznego zagrożenia państwa. W trakcie budowy omawianego systemu należy wypracować zasady realizacji HNS zagrożenia wojennego i wojny, a częściowo wykorzystywać je w czasie pokoju. Wymaga to przygotowania kompleksowych regulacji prawnych na czas wojny, a także odpowiednich procedur uruchamiających tego rodzaju regulacje. Ważną rolę w przygotowaniu formalnych podstaw funkcjonowania krajowego (narodowego) systemu HNS będą spełniać te organy administracji rządowej, które będą uczestniczyć w planowaniu i wykonywaniu zadań wynikających z obowiązków państwa-gospodarza.

3. UWARUNKOWANIA MILITARNE

Biorąc pod uwagę powyższe reformy sił zbrojnych w czołowych europejskich państwach NATO celowym byłoby aby w Polsce sięgnięto po te doświadczenia - konsolidując rozdęte i rozdrobnione struktury dowodzenia oraz logistyki (na szczeblach centralnym i operacyjnym) - należy je istotnie zmniejszyć poprzez:

- Pozostawienie w Sztabie Generalnym WP jedynie planowania strategicznego, a realizacje zadań podzielonych na "terytorialne" i "operacyjne" przenieść do wojsk – „terytorialnych" w kompetencje Inspektoratu Wsparcia Terytorialnego (IWT), zaś „operacyjnych" do trzech dowództw rodzajów sił zbrojnych.
- Komasację komórek realizujących zadania terytorialnych na szczeblu strategicznym w ramach Inspektoratu WT.
- Rozdzielenie logistyki na terytorialną (stacjonarną - strukturach IWT) i operacyjną (ruchomą - przy wojakach).
- W pionie terytorialnym logistyki pozostawić jej część stacjonarną, zaś ruchomą podporządkować dowództwom rodzajów sił zbrojnych.
- Komórki dowodzenia operacyjnego pozostawić w trzech rodzajach sił zbrojnych i na poziomie korpusów (równorzędnych), wycofując je z okręgów wojskowych.
- Mobilizację sił zbrojnych i gospodarki narodowej w zakresie planowania pozostawić w Sztabie Generalny, zaś w sferze wykonania - przekazać w struktury podporządkowane ITW.
- Infrastrukturę obronną włączyć w struktury terytorialne.

- Zarządzanie HNS przebudować w skali państwa oraz MON i włączyć do obowiązków IWT.
- Docelowo przekształcić dowództwa rodzajów sił zbrojnych w inspektoraty funkcjonujące w ramach Dowództwa Operacji Połączonych, zaś IWT przebudować w narodowe Dowództwo Terytorialne.
- Okręgi wojskowe przekształcić z dowództw operacyjnych w dowództwa terytorialne obszarów, mniejszych obszarem od dzisiejszych (z dwu dzisiejszych w pięć w przyszłości), pozwoli to zredukować przynajmniej 30% etatów i usprawni zarządzanie.
- Utworzyć terytorialny system kierowania obroną państwa - poczynając od IWT poprzez dowództwa wojewódzkie, aż do dowództw obwodów (jedno dla kilku powiatów).
- Strukturę zarządzania logistyką włączyć w terytorialny system kierowania obroną państwa, podobnie uczynić z administracja zasobami.
- Utworzyć garnizony jako wojskowego właściciela (w imieniu Skarbu Państwa) koszar i bazy szkoleniowej oraz podporządkować je - poprzez dowództwa obwodów - strukturze zarządzania infrastrukturą obrony. Wojska operacyjne staną się wtedy jedynie dzierżawcą koszar i obiektów szkoleniowych, które będą chronione przez instytucje powoływane przez system OT. Pozwoli to odciążyć dowódców jednostek wojsk operacyjnych od wielu obecnie realizowanych zadań i skoncentrować się na szkoleniu bojowym.
- Przenieść realizację szeregu zadań wykonywanych przez wojska na rzecz ich zabezpieczenia pokojowego w sferę usług realizowanych przez firmy cywilne pozyskiwane w drodze przetargów.
- Zmienić dziesiątki tysięcy stanowisk wojskowych na pracowników wojska.
- Zmniejszyć bazę szkoleniową o 3/4 etatów obecnego stanu.
- Zmienić system szkolenia, pozyskiwania i służby kadry wojskowej.
- Zmienić funkcjonowanie służby zdrowia na potrzeby wojska.

Pierwszym krokiem w kierunku takiego działania jest utworzenie Inspektoratu WT (dowództwa wsparcia narodowego), który stanie się pomocnym ministrowi obrony narodowej w rozpoznawaniu faktycznego stanu zasobów zbędnej infrastruktury. Pozwoli to wykonać następne przedsięwzięcia, które mogą wykazać, że w czasie pokoju możemy mieć armie nie większą niż 50.000 kadry zawodowej i kilkadziesiąt żołnierzy służących w ramach krótkotrwałej służby obowiązkowej w strukturach obrony terytorialnej.

Zadania sił zbrojnych można także określić wg miejsca ich realizacji, a więc obszaru RP, obszaru państwa (państw) NATO i poza nimi. Mogą to być wreszcie zadania o charakterze bojowym (wojennym) lub niebojowym (w terminologii NATO – innym niż wojna). Podstawowym dokumentem określającym przeznaczenie SZ RP jest ustawa zasadnicza: „Art. 26.1. siły zbrojne Rzeczypospolitej Polskiej służą ochronie niepodległości państwa i niepodległości jego terytorium oraz zapewnieniu bezpieczeństwa i nienaruszalności jego granic".

Z zapisu tego nie wynikają zadania związane z wypełnieniem zobowiązań sojuszniczych oraz międzynarodowych. Można więc uznać, że wynikają one z faktu, iż źródłem prawa w Polsce są: konstytucja, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia, a także (na określonym obszarze) akty prawa miejscowego. Szereg aktów prawa państwowego, począwszy od ustawy o powszechnym obowiązku obrony RP, określa możliwe obszary i formy aktywności sił zbrojnych. Synteza postanowień zawartych potwierdza przedstawione powyżej formy, obszary i zakres aktywności sił zbrojnych RP.

Zobowiązania międzynarodowe, głównie w ramach NATO (sojusznicze), rozszerzają gamę aktywności poza obszarem narodowym, a więc daleko odbiegających od wykładni artykułu 26. ust. 1 Konstytucji RP. W Strategii obronności RP stwierdzono, że: siły zbrojne RP – działając w narodowym systemie obronności i systemie sojuszniczym NATO – są gotowe do wykonywania trzech rodzajów zadań strategicznych: zadań obronnych w razie wojny (odparcie bezpośredniej agresji na terytorium Polski lub udział w odparciu agresji na inne państwo sojusznicze, zadań reagowania (także w ramach misji organizacji międzynarodowych) oraz zadań stabilizacyjnych i prewencyjnych w czasie pokoju (...) siłom zbrojnym RP należy zapewnić odpowiednią zdolność do: odstraszania potencjalnego agresora, prowadzenia operacji obronnej przeciwko agresji na szeroką skalę, udziału w dwóch jednoczesnych większych operacjach reagowania kryzysowego spoza (Art. V Traktatu Północnoatlantyckiego) albo w kilku operacjach o mniejszej skali, w tym operacjach pokojowych w ramach sił międzynarodowych[61].

Przyjmuje się również, iż siły zbrojne RP służą do: skutecznego i elastycznego reagowania na zmiany sytuacji militarnej w otoczeniu Polski; gwarantowania realizacji zadań osłonowych; natychmiastowego podjęcia działań obronnych w razie zagrożenia

[61] *Strategia bezpieczeństwa Rzeczypospolitej* ...., s. 13.

bezpieczeństwa państwa i sojuszu; stałego udziału w międzynarodowych operacjach pokojowych i reagowania kryzysowego[62].

Za naiwne i lekkomyślne należy więc uznać twierdzenia o tym, że „sojusz musi nam pomóc", albo „natychmiast pomoże...". Zdaniem czołowego promotora wstąpienia Polski do NATO Jana Nowaka-Jeziorańskiego „nie ma tu mowy o tym, by napaść na Polskę automatycznie uruchomiła działania wojenne ... samo podjęcie takiego zbiorowego postanowienia będzie wymagało czasu, może kilka dni, a może więcej, a przyjście z pomocą może polegać na przykład na blokadzie agresora, a nie na wypowiedzeniu mu wojny. Aby uruchomić sojusz, potrzebne będą działania opóźniające, obliczone na zadawanie wrogowi jak największych strat, zarówno na froncie, jak i po zajęciu terytorium przez nieprzyjaciela". Tenże wielki polityk w ślad za m.in. Napoleonem, C. Clausewitzem[63], H. von Moltke i gen. W. Sikorskim formułuje kapitalną regułę:„Polska może liczyć na pomoc sojuszników tylko wtedy, gdy będzie chciała i mogła bronić się sama, jeśli zdobędzie własne możliwości odstraszania napastnika"[64]. Wiąże się też ściśle z realizacją zadań obrony terytorialnej obejmujących:

- zdobywanie i rozpowszechnianie informacji z pogranicza sektorów cywilnego i wojskowego;
- ochronę przeciwdywersyjną portów, lotnisk i stacji wyładowczych, rejonów rozmieszczenia wojsk i urządzeń logistycznych lotnisk, a także dróg przegrupowania sił NATO;
- zabezpieczenie przegrupowania i kierowanie ruchem wojsk na wyznaczonych ciągach komunikacyjnych;
- współpracę cywilno-wojskową w zakresie koordynacji przedsięwzięć związanych z realizacją przez państwo-gospodarza funkcji rządowych, ekonomicznych i socjalnych[65].

4. UWARUNKOWANIA POZAMILITARNE

Operacje inne niż wojna, ukazują pełnię ról, jakie mogą być powierzane siłom zbrojnym danego państwa. Czasem mogą to być zadania o znaczeniu priorytetowym,

---

[62] *Strategia obronności...* s. 11.

[63] W kwestii „liczenia" przez Polskę na pomoc innych państw: C. von Clausewitz *„... obrońca w ogólności więcej może liczyć na pomoc z zewnątrz niż nacierający. Będzie on mógł tym pewniej na to liczyć, im ważniejsze jest jego istnienie dla wszystkich innych, to znaczy im zdrowszy i silniejszy jest jego stan polityczny i wojskowy"* [w:] *O wojnie*, s.450.

[64] J. Nowak-Jeziorański, *Słoń i jeż*, Wprost nr 29 z 19.07.98 r.

[65] *Koncepcja rozwoju Obrony Terytorialnej (główne kierunki)*, MON, Warszawa 1999, s. 10; ALP-9(B), *Doktryna logistyczna sił lądowych* (Stanag 2406), p. 1003-1008.

innym zaś razem - o charakterze drugorzędnym. Żadnej z nich nie można jednak wykluczyć, tym bardziej w odniesieniu do państwa aktywnego w sojuszu NATO. Jedne i drugie określają zakres w s p a r c i a c y w i l n e g o [66] dla sił zbrojnych. Wsparcie to może mieć charakter (wymiar) materialno-energetyczny (w tym informacyjny) lub moralny. W innym ujęciu wsparcie cywilne dla sił zbrojnych może obejmować: wsparcie operacyjne; wsparcie logistyczne; wsparcie informacyjne; wsparcie moralne (religijne, psychologiczne, edukacyjne, wymiar sprawiedliwości, itd.).

Wsparcie operacyjne – to działania specjalistycznych sił i środków cywilnych, które wspierają siły wojskowe w osiąganiu ich głównego celu. Wsparcie to w zasadzie nie odbiega swą postacią od właściwych działań militarnych. Wiele sił cywilnych (służb, inspekcji, policji i straży) posiada zdolności do wykonania tych samych, lub podobnych, co siły wojskowe zadań. Mogą to być m.in.: siły i środki wywiadu i kontrwywiadu, siły medyczne, sanitarne i weterynaryjne, łączności, ochrony środowiska, policyjne, transportu, a także szereg innych reprezentujących sektor cywilny z pozarządowymi włącznie.

Istnieje delikatna granica pomiędzy wsparciem operacyjnym a pozostałymi rodzajami wsparcia. I tak, dla przykładu, w operacji wojennej wsparcie medyczne może być wsparciem rozumianym jako usługowe. W razie operacji niesienia pomocy humanitarnej zaś, cywilne siły i środki medyczne będą wspierały siły zbrojne, realizując wraz z nimi cel główny operacji, będzie to więc wsparcie operacyjne. Wsparcie operacyjne służy zatem wzmocnieniu działań sił wojskowych, a przedmiotem tegoż jest adresat danego typu działania. Pozostałe rodzaje wsparcia służą wzmocnieniu zdolności sił wojskowych, podmiotem wsparcia są zatem siły wojskowe.

Wsparcie logistyczne – to działania władz cywilnych mające na celu udostępnienie siłom wojskowym pomocy materialnej i usługowej w rejonie działań, by zapewnić pomyślne wykonanie ich misji.

Wsparcie informacyjne - to działania władz cywilnych mające na celu udostępnienie siłom wojskowym urządzeń i nośników informacji oraz niezbędnych wiadomości do wykonania ich misji.

Wsparcie moralne - to działania władz cywilnych mające na celu udzielenie wsparcia siłom wojskowym w zakresie edukacji, posług religijnych, uzyskania społecznej akceptacji, ochrony ofiar i poszkodowanych, a więc w całym obszarze społecznym celu i skutków działania sił zbrojnych.

---

[66] Wg W. Kitlera.

Wsparcie cywilne jako jedną z misji sektora cywilnego w obszarze obrony cywilnej – podsystemu obrony narodowej. Wsparcie to jest tylko częścią szerszego zjawiska, które w NATO określa się jako „Civil Emergency Planning", a w Polsce nazywano gotowością obronną sektora cywilnego. Często też narodowe zadania obronne utożsamia się z powinnościami sektora cywilnego określonymi ustawą o powszechnym obowiązku obrony RP i innymi przepisami szczegółowymi z uchwałami KOK włącznie[67]. Sektor cywilny realizuje przedsięwzięcia w zakresie obrony narodowej, które określono jako obronę cywilną lub – niemilitarną. Jednym z jej elementów jest wsparcie cywilne dla określonych ustawowo sił i środków rządowych (siły resortu obrony, spraw wewnętrznych i administracji, UOP ...). Elementem tego wsparcia będzie – wsparcie sił zbrojnych własnych i sojuszniczych.

W projekcie ustawy o powinnościach obronnych przewiduje się, że Rada Ministrów[68] planuje i realizuje przygotowania obronne zapewniające funkcjonowanie państwa w czasie zewnętrznego zagrożenia bezpieczeństwa (kryzysu) i wojny, w tym przedsięwzięcia gospodarczo-obronne oraz zadania wykonywane na rzecz sił zbrojnych RP i wojsk sojuszniczych. Każdy z ministrów zaś – w zależności od działu - podejmuje stosowne przedsięwzięcia. I tak w dziale:

- administracja publiczna: określa zadania obronne i organizuje ich wykonanie przez nadzorowane organy administracji rządowej oraz podległe, podporządkowane i nadzorowane jednostki organizacyjne i komórki organizacyjne;
- architektura i budownictwo: tworzy warunki do gromadzenia i przechowywania zasobów geodezyjnych i kartograficznych na potrzeby obronne państwa;
- finanse publiczne: określa zasady polityki celnej i skarbowej;
- gospodarka: opracowuje zasady i koordynuje funkcjonowanie gospodarki oraz kontroli obrotu z zagranicą w razie zagrożenia i w czasie wojny; opracowuje i aktualizuje CPMG; zapewnia bezpieczeństwo energetyczne; zapewnia wymagany stan rezerw państwowych i zapasów obowiązkowych paliw, opracowuje zasady utrzymania potencjału produkcyjnego i usługowego na

[67] J. Marczak (kier. nauk.) *Wykorzystanie potencjału pozamilitarnego w czasie kryzysu i wojny* [w:] B. Balcerowicz (kier. nauk.), *Przygotowanie i prowadzenie wojny obronnej przez Polskę po 2000 roku* „KAPPA", AON, Warszawa 1999.

[68] *Ustawa z dnia ... o obowiązku wojskowym i innych powinnościach obronnych.* Projekt, stan na kwiecień 2000, dział V – aneks do tekstu jednolitego ze stycznia 2000 (na prawach maszynopisu).

potrzeby obronne, nadzoruje realizację zadań obronnych przez spółki przemysłu obronnego;

- HNS w tym dziale to m.in.: charakterystyka systemu paliwowego (produkcja, przetwórstwo, przechowalnictwo, rurociągi), zasoby i źródła energii elektrycznej, regulowanie taryf celnych, obrotu towarów i technologii, zasady funkcjonowania i procedury współpracy z Agencją Rezerw Materiałowych;
- gospodarka morska: określenie zasad funkcjonowania transportu morskiego oraz portów i przystani morskich, a także korzystania z obszarów morskich; HNS w tym dziale to m.in.: charakterystyka techniczno-eksploatacyjna infrastruktury morskiej (porty, przystanie), środków transportowych oraz właściwości wybrzeża morskiego, a także sprawy ochrony środowiska morskiego;
- gospodarka wodna: określa zasady przygotowania śródlądowych dróg wodnych, obiektów hydrotechnicznych; zapewnia techniczne i nawigacyjne warunki śródlądowych dróg wodnych; gospodaruje rezerwami mobilizacyjnymi; HNS w tym dziale to m.in.: przeprawy – charakterystyka i konstrukcje, stałe i doraźne, usługi (prognozy, ostrzeżenia, monitorowanie) meteo-, aerohydrologiczne, pomiary wód;
- łączność: określa zasady funkcjonowania systemu telekomunikacyjnego i pocztowego w razie zewnętrznego zagrożenia bezpieczeństwa państwa (kryzysu) i w czasie wojny; ustala zasady organizacji łączności na potrzeby systemu obronności państwa; zapewnia wydzielanie zasobów krajowej infrastruktury telekomunikacyjnej na potrzeby kierowania; koordynuje usługi w tym zakresie; odpowiada za zapewnienie wymaganego stanu rezerw państwowych[69]; HNS w tym dziale to m.in.: usługi pocztowe i telekomunikacyjne, odtwarzanie łączności, charakterystyka dostępności do systemów łączności, telefonia cyfrowa;
- rolnictwo: ustala zasady produkcji roślinnej i zwierzęcej oraz skupu płodów rolnych w razie zewnętrznego zagrożenia bezpieczeństwa państwa (kryzysu) i w czasie wojny;
- rozwój wsi: opracowuje zasady przygotowania, zabezpieczenia i zapewnienia dostaw wody na potrzeby obronne;

[69]Zapewnienie odpowiedniego poziomu rezerw państwowych należy do powinności wielu ministrów.

- rynki rolne: tworzy warunki organizacyjne i techniczne do gromadzenia i przechowywania produktów rolno-spożywczych w ramach rezerw państwowych;
- HNS w tym dziale to m.in.: zaopatrywanie w żywność i produkty do jej produkcji, charakterystyka zasobów żywności, systemu jej magazynowania (magazyny, chłodnie, hurtownie, itd.), konserwacji i przetwarzania; usługi gastronomiczne, giełdy produktów rolnych; „liderzy" produkcji rolnej, stan prawny i organizacyjny oraz procedury współpracy z Agencją Rynku Rolnego, Inspekcją Skupu i Przetwórstwa Artykułów Rolnych;
- Skarb Państwa: gospodaruje mieniem Skarbu Państwa; organizuje zadania obronne w przedsiębiorstwach państwowych;
- transport: określa zasady funkcjonowania transportu i żeglugi śródlądowej oraz przepraw promowo-mostowych; HNS w tym dziale to m.in.: charakterystyka możliwości transportowych kraju z żeglugą śródlądową włącznie, świadczenie usług transportowych (z wyjątkiem transportu morskiego), charakterystyka przejść granicznych, węzłów komunikacyjnych, itd.;
- środowisko: ustala zasady wykorzystania lasów, parków narodowych, rezerwatów przyrody i innych zasobów naturalnych; HNS w tym dziale to m.in.: surowiec drzewny i inne zasoby naturalne, łowiectwo, bytowanie wojsk na terenach zalesionych;
- sprawy wewnętrzne: zapewnia warunki funkcjonowania określonych organów kierowania państwem w razie zagrożenia (kryzysu) i wojny; prowadzi bazę informacyjną rejestru pojazdów i kierowców (Centralna Ewidencja Pojazdów i Kierowców – CEPIK) planuje, organizuje i zapewnia realizację przedsięwzięć na rzecz mobilizacyjnego rozwinięcia sił zbrojnych; określa zadania obronne i organizuje ich wykonywanie przez nadzorowane organy administracji rządowej oraz podległe, podporządkowane i nadzorowane jednostki i komórki organizacyjne; HNS w tym dziale to m.in.: świadczenie usług z zakresu CEPIK, świadczenie wsparcia przez siły Policji, Straży Granicznej i Państwowej Straży Pożarnej i inne rodzaje wsparcia o operacyjnym charakterze;
- zdrowie: ustala zasady organizacji i funkcjonowania służby zdrowia w razie zagrożenia (kryzysu) i w czasie wojny; określa zasady wykorzystania kadr

medycznych. HNS w tym dziale to m.in. charakterystyka możliwości w zakresie świadczeń leczniczych, charakterystyka infrastruktury i urządzeń systemu opieki zdrowotnej (szpitale, sanatoria, lekarze, personel medyczny, łóżka, sale operacyjne, itd.), zasoby krwi, rezerwy środków farmaceutycznych, materiałów medycznych i innych, możliwości ruchomych oddziałów służby zdrowia i ich wykorzystanie;

- wszyscy ministrowie – organizują wykonywanie zadań przez podległe, podporządkowane i nadzorowane jednostki organizacyjne w zakresie dostaw, usług i świadczeń na rzecz sił zbrojnych; zapewniają realizację inwestycji przewidzianych do wykorzystania przez siły zbrojne[70].

Podstawę do udzielenia wsparcia wojskom sojuszniczym stanowi ratyfikowana w 1998 r. umowa między stronami Traktatu Północnoatlantyckiego dotycząca statusu ich sił zbrojnych[71], która w art. 1 ust.2 przewiduje zastosowanie umowy w stosunku do władz administracyjnych umawiających się stron w granicach administrowanych przez nie terenów. Zasadnicze znaczenie ma art. 9 tejże ustawy, w którym przewiduje się możliwość nabywania na miejscu towarów oraz usług na tych samych zasadach i – z zasady – przez te same organy, które dokonują zakupów na potrzeby SZ RP. Ust. 3 tego artykułu ustala, że udostępnienie przez „władze państwa przyjmującego" potrzebnych gruntów, budynków i urządzeń będzie się odbywało na zasadach dotyczących zakwaterowania SZ państwa przyjmującego. Z kolei ust. 4 reguluje sprawę świadczeń osobistych („cywilnej siły roboczej"), przewidując zastosowanie przepisów kraju goszczącego (Polski).

Wykładnię i uszczegółowienie trybu postępowania wobec goszczących wojsk daje ustawa z dnia 23 września 1999 r. o zasadach pobytu wojsk obcych na terytorium Rzeczypospolitej Polskiej oraz zasadach ich przemieszczania się przez to terytorium[72]. Także i ona odwołuje się do stosowania zasad przyjętych wobec SZ RP (np. w sprawach świadczeń zdrowotnych udzielanych przez publiczne zakłady opieki zdrowotnej, korzystania z dróg publicznych, przewozu materiałów niebezpiecznych oraz korzystania z linii i urządzeń telekomunikacyjnych, a także pasm częstotliwości).

---

[70]Szczegółowe informacje w projekcie ustawy.
[71]Tzw. SOFA, Dz U RP Nr 97 z 1998r., poz. 504.
[72]Dz U RP nr 93 poz. 1063. W szczególności reguluje ona sprawy szkolenia na polskich poligonach, choć może mieć zastosowanie do realizacji zadań HNS.

„Powyższe pozwala sądzić, że zabezpieczenie potrzeb jednostek NATO na terytorium Polski będzie odbywało się w ramach zadań realizowanych przez administrację publiczną na rzecz SZ RP i na tych samych zasadach (a już co najmniej do standardu tego powinno się dążyć)."[73]

1. Sojusz dysponuje przemyślaną, opartą na doświadczeniach praktyki przejrzystą koncepcją pozyskiwania potrzebnego wsparcia od państwa podejmującego wojska NATO na swoim terytorium (państwa-gospodarza).
2. Przyjęła ona postać doktryny, uporządkowanego systemu poglądów i założeń, zaakceptowanych przez władze sojuszu, które – w świetle doświadczeń historycznych i regularnego weryfikowania przyjętych rozwiązań podczas ćwiczeń, powinny spełnić oczekiwania NATO – zapewnić otrzymanie zapotrzebowanych materiałów, usług i pomocy. Zabezpieczeniem są tu gwarancje dostarczenia wsparcia udzielane przez rząd państwa-gospodarza.
3. Przyjęte aktualnie rozwiązania odpowiadają nowym uwarunkowaniom strategicznym, które zwiększają wymogi w zakresie zabezpieczenia mobilności i potrzeb logistycznych wojsk, w warunkach dużej nieprzewidywalności rejonu rozwijania wojsk, w stosunkowo krótkim czasie, do realizacji szerokiego spektrum możliwych misji:
   - udzielania pomocy w usuwaniu klęsk żywiołowych;
   - innych cywilnych działań ratunkowych;
   - wspierania misji humanitarnych;
   - prowadzenia wspólnej operacji obronnej;
   - operacji reagowania kryzysowego nie pozostającej w związku z artykułem 5 (Crisis Reaction Operations – CRO).
4. Ponieważ trudno dziś wskazywać z dostateczną pewnością i dokładnością rejony rozwinięcia wojsk i ich szczegółowy, narodowy skład – planowanie więc ma charakter ogólny i wielowariantowy, raczej wstępny. Precyzowanie podejmowanych przedsięwzięć nastąpi po podjęciu decyzji o realizacji konkretnej misji. W tej sytuacji wzrasta współcześnie rola dowódców NATO w przygotowaniu HNS. Ich przewidywania potrzeb muszą być głębsze,

[73] W. Kitler, H. Szafran, *wsparcie cywilne dla sił zbrojnych*, w: W. Kitler kier. nauk., *Współczesny wymiar obrony cywilnej RP w świetle integracji ze strukturami zachodnioeuropejskimi cz. II, Warszawa 2000*, na prawach maszynopisu (praca ta ukaże się niemal w tym samym terminie co niniejsze dzieło).

a przygotowywane rozwiązania – uniwersalne i przyszłościowe, wychodzące naprzeciw specyficznym potrzebom niektórych krajów członkowskich. Dowódcy NATO mają większe niż kiedyś prerogatywy w zakresie planowania przygotowania HNS, w tym – umów i porozumień, aby nie wydłużyć ponad miarę przygotowań do rozpoczęcia misji.

5. Sojusznicza doktryna HNS znacząco formalizuje wewnątrzsojusznicze procedury i dokumenty HNS dążąc do zawarcia w nich potrzebnych treści w celu zrozumienia intencji i zadań przez wszystkie strony oraz dla przeciwdziałania ewentualnym zakłóceniom w dostarczaniu wsparcia, w szczególności zaś zapobieżenia konkurowaniu przez różne państwa o trudno dostępne towary i usługi. Ustala też ogólną architekturę wewnętrznych sojuszniczych struktur zarządzania HNS tak aby zabezpieczyć obieg informacji i sterowanie realizacją wsparcia pod kontrolą dowódców NATO. Doktryna określa podstawowe ogólne obowiązki państwa-gospodarza w zakresie zapewnienia współpracy z właściwymi organami NATO i państw wysyłających wojska dla racjonalnego i sprawnego przygotowania oczekiwanego wsparcia.
   - Jednocześnie – żądając zapewnienia koordynacji i współpracy między wojskowymi i cywilnymi podmiotami państwa-gospodarza – wymaga przez to zbudowania określonych wewnętrznych struktur i relacji łączących działania obu sektorów.
   - Do zidentyfikowanych zasadniczych zadań państwa-gospodarza należą:
     - zapewnienie realizacji HNS;
     - utrzymanie współpracy z sojusznikami;
     - zarządzanie posiadanymi zasobami materiałowymi, potencjałem usługowym i transportowym;
     - koordynowanie przemieszczania wojsk NATO i ruchów (migracji) własnej ludności;
     - utrzymanie funkcjonowania państwa w obszarach działań wojsk NATO;
     - zapewnienie warunków bytowania i ochrony ludności oraz bezpieczeństwa i porządku publicznego w strefie działań bojowych oraz strefie komunikacji;

– prowadzenie rozpoznania terytorialnego oraz zapewnienie bezpieczeństwa wojskowego, w tym zwalczanie sabotażu i szpiegostwa.

6. Właściwe i zdolne do realizacji lub wsparcia sektora cywilnego w spełnianiu powyższych zadań są jedynie struktury terytorialne sił zbrojnych, w Polsce podobnie jak w wielu państwach NATO – obrona terytorialna.
7. Dla prac koncepcyjnych i zbudowania w ich rezultacie polskiego, narodowego systemu HNS konieczne i przydatne będzie zapoznanie się z doświadczeniami i rozwiązaniami praktyki sojuszników – szczególnie w układzie terytorialnym. Struktury wsparcia narodowego nie należy postrzegać jedynie w kontekście potrzeb wojsk operacyjnych, lecz głównie konieczności odbudowy nie istniejącej w RP terytorialnej części obronności państwa i nałożonej na nią logistyki stacjonarnej sił zbrojnych - a nie tylko wojsk operacyjnych.
8. W realizacji strategicznego celu polskiej polityki chodzi o osiągnięcie „jak najwyższego poziomu bezpieczeństwa”[74]. Podstawowe zasady działania NATO określają niepodzielność wspólnego bezpieczeństwa co oznacza, iż „żadne z państw członkowskich nie musi polegać wyłącznie na własnych, narodowych działaniach i zasobach ekonomicznych, aby przeciwstawić się zagrożeniom bezpieczeństwa”. Jednocześnie jednak „żadne z państw nie rezygnuje z prawa wypełnienia zobowiązań podjętych wobec swojego społeczeństwa. Każde państwo nadal odpowiada za własne potrzeby obronne. Poprzez zbiorowe działanie sojusz umożliwia państwom członkowskim wzmocnienie swoich zdolności realizacji koniecznych celów narodowych”[75].
9. Zasady te mają swoje odbicie w treści Traktatu Północnoatlantyckiego – głównego aktu politycznego NATO. W art. 3 stwierdza się, iż „Każda (Strona Traktatu – przyp. aut.) z osobna i wszystkie razem, przez stałą i skuteczną samopomoc i pomoc wzajemną będą utrzymywały i rozwijały swoją indywidualną i zbiorową zdolność do odparcia zbrojnej napaści”. Natomiast treść Art. 5 ujmuje kwestię udzielenia pomocy stronie lub stronom napadniętym „podejmując natychmiast indywidualnie w porozumieniu z innymi stronami taką akcję, jaką uzna za konieczną, nie wyłączając użycia siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru

[74] W. Bartoszewski [w:] *NATO. Vademecum*, Warszawa 1995, s. 5
[75] Tamże, s. 107.

północnoatlantyckiego". Konsekwencją tego artykułu są wymogi wobec tego państwa-gospodarza, który otrzyma taką pomoc sformułowane pod ogólnym tytułem HNS.

10. W sprawach wsparcia sił sojuszniczych przez państwo-gospodarza (HNS) w MON są dwa mało skoordynowane ze sobą ośrodki, które usiłują realizować ten problem na poziomie MON, natomiast poza tym ministerstwem nie ma żadnych konkretnych komórek, które w imieniu tychże chciałyby podjąć się tą problematyką ciążącą na nich. Sztab Generalny WP, który najwięcej czyni w tym obszarze na rzecz państwa nie chce za wszystko odpowiadać co ciąży na całym państwie - i ma ku temu podstawy prawne.
11. Analizując założenia strategiczne systemu wsparcia narodowego należy przyjąć, że rozległość problematyki objętej tym systemem jest na tyle rozległa, nowa i konieczna do opisania w sposób kompleksowy iż właściwie dobrze się stało, że doszło do naukowego rozpatrzenia problemu w gronie ponad dwudziestu naukowców i praktyków wojskowych. Biorąc pod uwagę uwarunkowania geopolityczne, sojusznicze, militarne i pozamilitarne, a także uwzględniając przesłanki do tworzenia systemu wsparcia narodowego (terytorialnego) oraz warunki determinujące organizację zintegrowanego zabezpieczenia i wsparcia sił zbrojnych RP należy założyć, że wsparcie sił zbrojnych (zarówno sojuszniczych, jak i polskich) nie powinno być troską jedynie struktur wojskowych - ich naczelnego organu - lecz przede wszystkim państwa i powinno być kierowane przez komórkę organizacyjną ministra obrony narodowej.
12. Powinno ono funkcjonować w ramach wyodrębnionej struktury MON – działając z wykorzystaniem struktur administracji wojskowej i terytorialnego kierowania obronnością państwa – poza strukturą dowodzenia wojskami operacyjnymi, w ścisłym współdziałaniu z administracją cywilną szczebla centralnego, regionalnego i lokalnego[76]. Nie może ono być tworzone jedynie w wymiarze logistyki stacjonarnej wojsk, lecz powinno stanowić spójny system terytorialnie organizowanej obrony narodowej z tą logistyką.

[76]Ostatnie dziesięciolecie to bezładne wyzbywanie się potencjału obronnego państwa, stąd istnieje konieczność odbudowy jego elementów, których funkcjonowania zaniechano lub ograniczono do wielkości niewspółmiernej do potrzeb. Zatem budowanie systemu wsparcia narodowego jest szansą na właściwe usytuowanie elementów systemu wojskowego w Polsce – stosownie do ich rangi w strukturze obronności państwa.

BIURO
WOJSKOWEJ SŁUŻBY
NORMALIZACYJNEJ

Marian PŁAWIAK
Bogusław ROGOWSKI

PRAKTYCZNE ZADANIA DZIAŁALNOŚCI NORMALIZACYJNEJ RESORTU OBRONY NARODOWEJ W STANACH NADZWYCZAJNYCH

CENTRUM KONFERENCYJNE WP Grudzień 2001

BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

PRAKTYCZNE ZASTOSOWANIE PRAC NORMALIZACYJNYCH MON W STANACH NADZWYCZAJNYCH

REFERUJĄCY
ppłk mgr inż. Bogusław ROGOWSKI

Warszawa, 19 – 20 grudnia 2001 r.

BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

PODSTAWY PRAWNE SYSTEMU

USTAWA
z dnia 3 kwietnia 1993 r. o normalizacji
(Art. 18 – ustawy)

ROZPORZĄDZENIE RADY MIINISTRÓW
z dnia 10 stycznia 1995 r.

- *wprowadzenie obowiązku stosowania Polskich Norm;*
- *zorganizowanie i wykonanie przeglądu dokumentów normalizacyjnych (31.12.1996r.);*
- *powołanie służb normalizacyjnych w resortach MON i MSWiA;*
- *zgłaszanie potrzeb w zakresie opracowywania Polskich Norm – do programu i planu PKN;*
- *zadania dla PKN w zakresie realizacji zadań na rzecz OiBP.*

BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

OBSZARY OBJĘTE STANDARYZACJĄ – PRZYKŁADY

ŚRODKI UZBROJENIA i WYPOSAŻENIA INŻYNIERYJNEGO;

SPRZĘT I ŚRODKI OCHRONY PRZECIWCHEMICZNEJ - W TYM NBC;

SPRZĘT RADIOTECHNICZNY, ŚRODKI ŁĄCZNOŚCI ORAZ SYSTEMY INFORMATYKI;

UZBROJENIE i SPRZĘT MARYNARKI WOJENNEJ;

STATKI POWIETRZNE ;

ZABEZPIECZENIE LOGISTYCZNE:

- sprzęt i wyposażenie;
- zaopatrywanie, w tym mundurowe, żywnościowe oraz MPS;
- transport naziemny, powietrzny i morski;
- zabezpieczenie medyczne.

BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

DOKUMENTY NORMALIZACYJNE – MOŻLIWE WYKORZYSTANIE

W ZAKRESIE ŚRODKÓW UZBROJENIA i WYPOSAŻENIA INŻYNIERYJNEGO

NORMY OBRONNE (NO)

NO-46-A500 Wojskowe stacje i zestawy uzdatniania wody. Parametry wody pitnej. Metody badań w warunkach polowych.

NO-46-A501 Wojskowe stacje i zestawy uzdatniania wody. Polowe laboratorium kontroli jakości wody. Pobieranie próbek w warunkach polowych.

NO-13-A212 Wykrywacze indukcyjne min.

DOKUMENTY STANDARYZACYJNE NATO

ATP-52 Doktryna Wojsk Inżynieryjnych Sił Lądowych:

- *usuwanie i niszczenie przedmiotów wybuchowych i niebezpiecznych;*
- *zabezpieczenie i utrzymanie urządzeń komunalnych i obiektów budowlanych.*

BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

DOKUMENTY NORMALIZACYJNE – MOŻLIWE WYKORZYSTANIE

W ZAKRESIE SPRZĘTU i ŚRODKÓW OCHRONY PRZECIWCHEMICZNEJ

NORMY OBRONNE (NO)

NO-42-A200 Indywidualny pakiet przeciwchemiczny.

NO-42-A501 Sprzęt ochrony układu oddechowego. Maski przeciwgazowe.

NO-42-A505 Przyrządy rozpoznania chemicznego.

NO-68-A209 Środki do likwidacji skażeń.

NO-04-A001 Zakres wiedzy i umiejętności z OPChem.

DOKUMENTY STANDARYZACYJNE NATO

STANAG 2061 Procedury rozmieszczania pacjentów z państw sprzymierzonych w placówkach medycznych.

AMedP-15 Wojskowe wsparcie medyczne i pomoc humanitarna w wypadku katastrof.

BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

DOKUMENTY NORMALIZACYJNE – MOŻLIWE WYKORZYSTANIE

W ZAKRESIE UZBROJENIA i SPRZĘTU MARYNARKI WOJENNEJ

NORMY OBRONNE (NO)

NO-07-A023 Uzupełnianie zapasów na morzu. Ładunki płynne.

NO-07-A028 Poszukiwanie i ratownictwo morskie. Łączność.

NO-07-A029 Obrona przed BMR. Obrona okrętów. Organizacja i procedury.

DOKUMENTY STANDARYZACYJNE NATO

ATP- 40 Sposób kontroli sytuacji w czasie kryzysu i w czasie wojny.

BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

DOKUMENTY NORMALIZACYJNE – MOŻLIWE WYKORZYSTANIE

W ZAKRESIE ZABEZPIECZENIA LOGISTYCZNEGO

NORMY OBRONNE (NO)

NO-91-A258-2 MPS. Paliwo F-34.

NO-89-A206 Indywidualna racja żywnościowa sucha „S".

DOKUMENTY STANDARYZACYJNE NATO

AJP- 4.5 Doktryna i procedury sojuszniczego wsparcia państwa gospodarza.

STANAG 2227 Wojskowe wsparcie medyczne w obszarze klęski żywiołowej.

BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

ZABEZPIECZENIE STANDARYZACYJNE SPRZĘTU I WYPOSAŻENIA TECHNICZNEGO SZ RP - PRZYKŁADY

Okręt wsparcia logistycznego – „KONTRADMIRAŁ X. CZERNICKI"

PUBLIKACJE
STANDARYZACYJNE NATO

AHP, ALP, AMedP, APP, ATP
(wyposażenie dokumentacyjne okrętu)

BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

ZABEZPIECZENIE STANDARYZACYJNE ĆWICZEŃ - PRZYKŁADY

ĆWICZENIE CMX / CRISEX 2000

- publikacje normalizacyjne MON i NATO;
- wydawnictwa normalizacyjne;
- normalizacyjne bazy danych;
- publikacje kodyfikacyjne;
- kodyfikacyjne bazy danych.

ĆWICZENIE STRONG RESOLVE 02

- publikacje standaryzacyjne NATO;
- publikacje NATO z zakresu łączności.

BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

KRAJOWE DOKUMENTY NORMALIZACYJNE

PN - Polska Norma

NO - Norma Obronna

ZN - Zakładowa Norma

WPN - Wojskowa Polska Norma

WBN - Wojskowa Branżowa Norma

BN - Branżowa Norma

A - zmiana do Polskiej Normy

Ad - dodatek do Polskiej Normy

AC - poprawka do Polskiej Normy

BN, WPN, WBN - są sukcesywnie zastępowane PN lub NO lub wycofywane „bez zastąpienia"

BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

DOKUMENTY W ZASOBACH BWSN

(stan na 20.12.2001r.)

STANDARYZACYJNE NATO

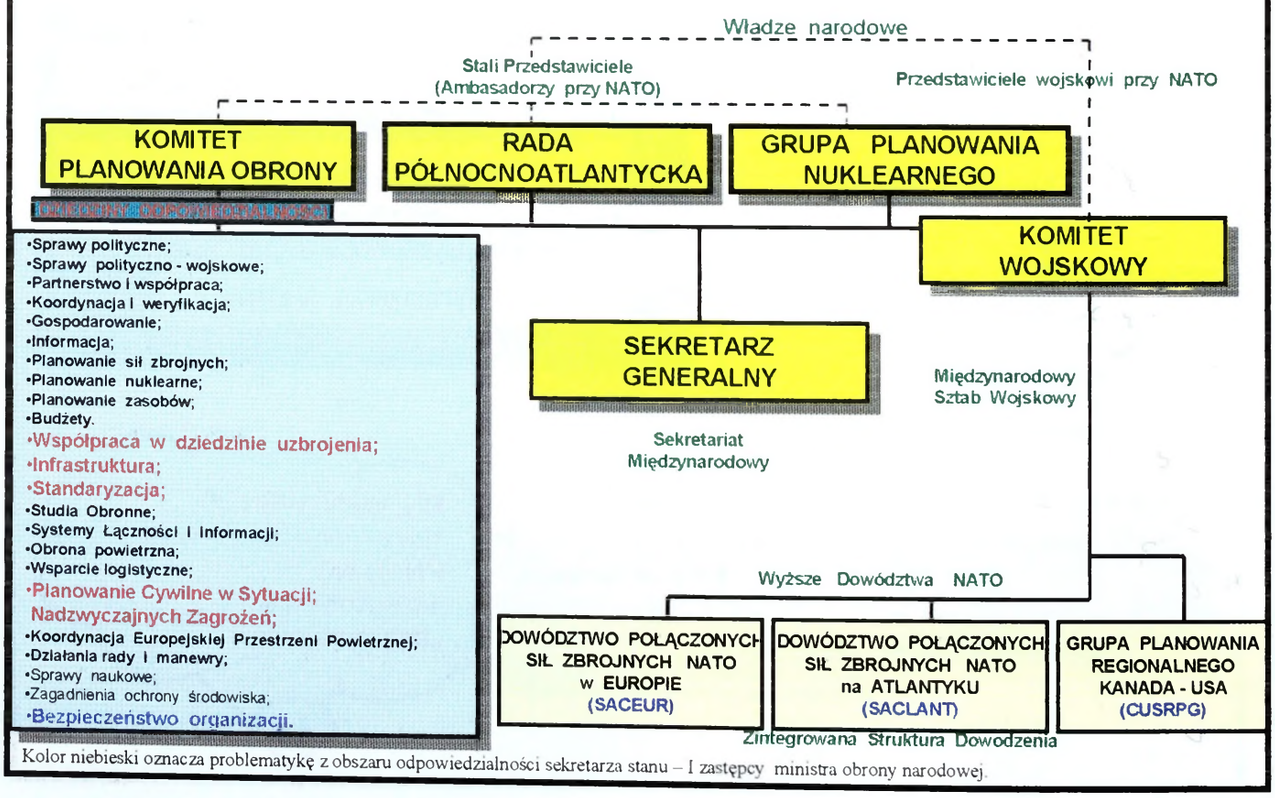
- STANAG i AP - 1345
- Przetłumaczone - 479

KRAJOWE

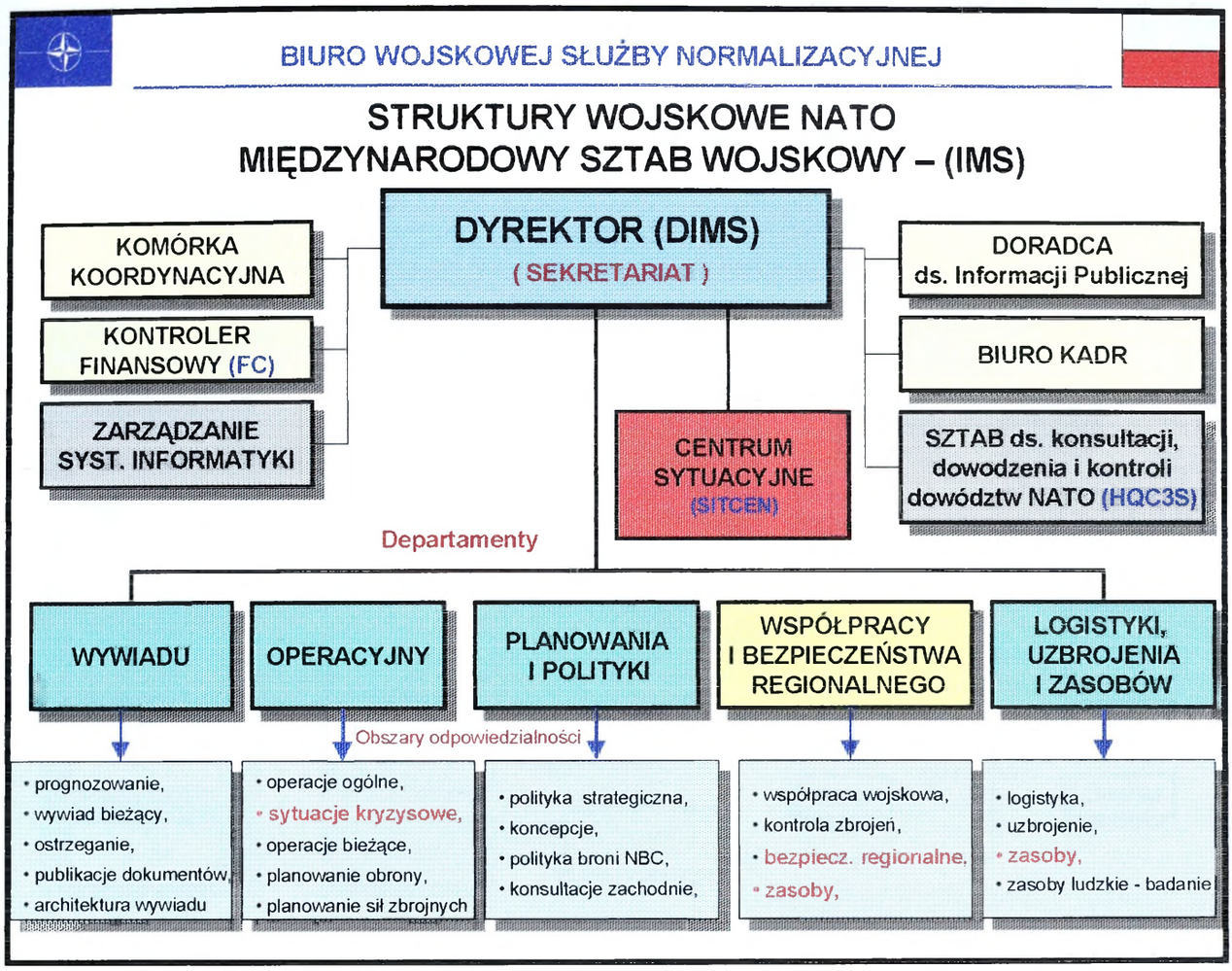
- Normy Obronne (NO) - 465
- Polskie Normy (PN-V) - 187
- Wojskowe Branżowe Normy (WBN) - 422
- Wojskowe Polskie Normy (WPN) - 57

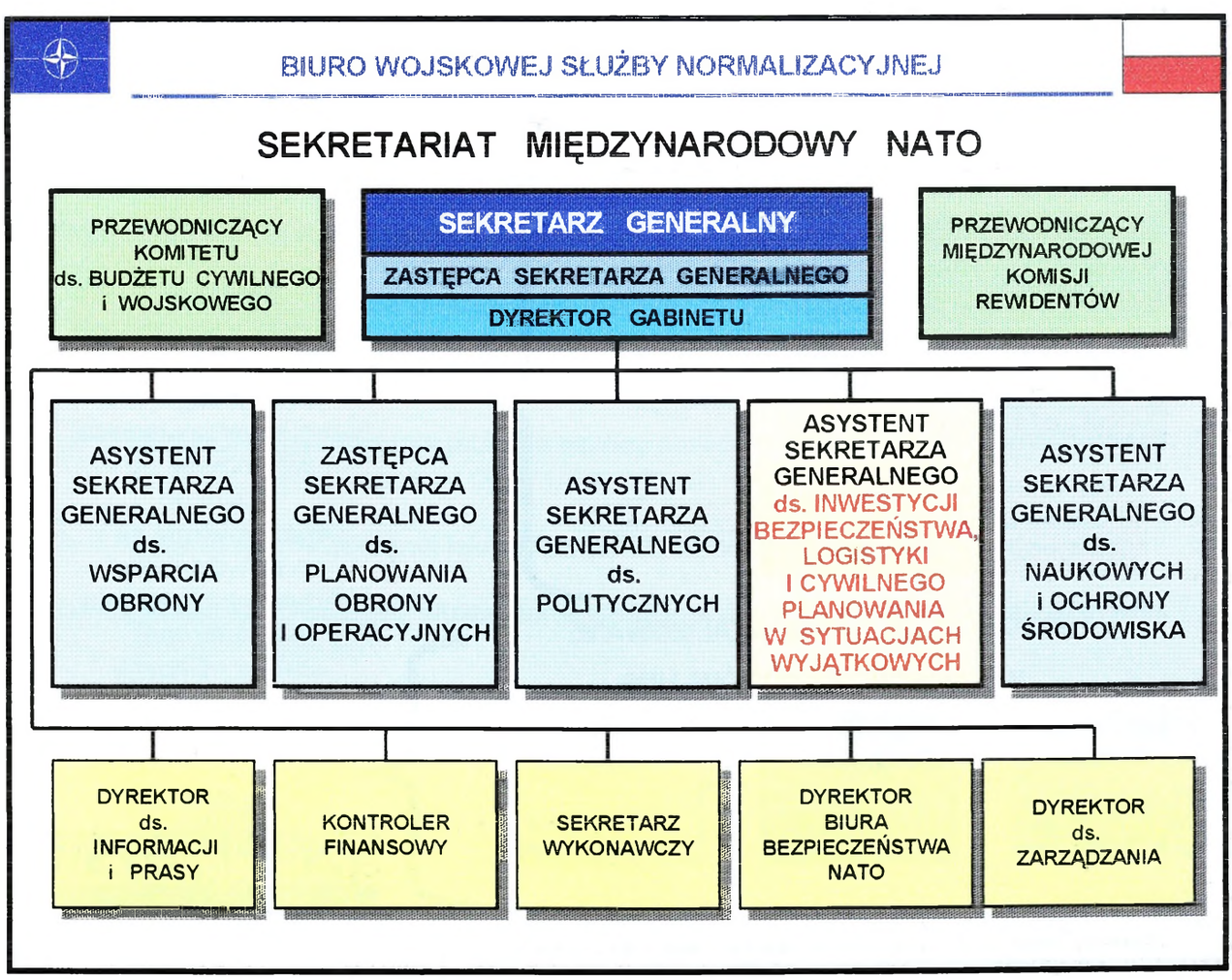
BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

STRUKTURA POLITYCZNA I WOJSKOWA NATO



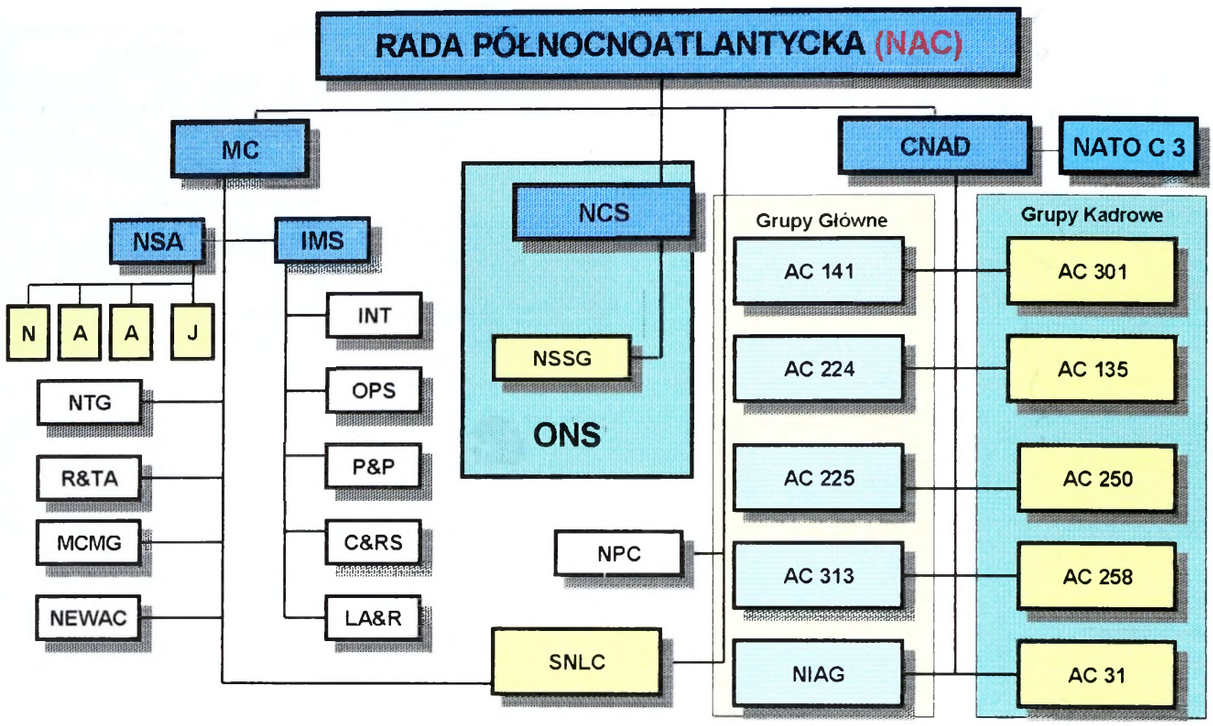
Kolor niebieski oznacza problematykę z obszaru odpowiedzialności sekretarza stanu – I zastępcy ministra obrony narodowej.


BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ
STRUKTURY WOJSKOWE NATO
MIĘDZYNARODOWY SZTAB WOJSKOWY – (IMS)
KOMÓRKA KOORDYNACYJNA
KONTROLER FINANSOWY (FC)
ZARZĄDZANIE SYST. INFORMATYKI
DYREKTOR (DIMS)
(SEKRETARIAT)
CENTRUM SYTUACYJNE (SITCEN)
DORADCA ds. Informacji Publicznej
BIURO KADR
SZTAB ds. konsultacji, dowodzenia i kontroli dowództw NATO (HQC3S)
Departamenty
WYWIADU
OPERACYJNY
PLANOWANIA I POLITYKI
WSPÓŁPRACY I BEZPIECZEŃSTWA REGIONALNEGO
LOGISTYKI, UZBROJENIA I ZASOBÓW
Obszary odpowiedzialności
• prognozowanie,
• wywiad bieżący,
• ostrzeganie,
• publikacje dokumentów,
• architektura wywiadu
• operacje ogólne,
• sytuacje kryzysowe,
• operacje bieżące,
• planowanie obrony,
• planowanie sił zbrojnych
• polityka strategiczna,
• koncepcje,
• polityka broni NBC,
• konsultacje zachodnie,
• współpraca wojskowa,
• kontrola zbrojeń,
• bezpiecz. regionalne,
• zasoby,
• logistyka,
• uzbrojenie,
• zasoby,
• zasoby ludzkie - badanie


BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ
SEKRETARIAT MIĘDZYNARODOWY NATO
PRZEWODNICZĄCY KOMITETU ds. BUDŻETU CYWILNEGO i WOJSKOWEGO
SEKRETARZ GENERALNY
ZASTĘPCA SEKRETARZA GENERALNEGO
DYREKTOR GABINETU
PRZEWODNICZĄCY MIĘDZYNARODOWEJ KOMISJI REWIDENTÓW
ASYSTENT SEKRETARZA GENERALNEGO ds. WSPARCIA OBRONY
ZASTĘPCA SEKRETARZA GENERALNEGO ds. PLANOWANIA OBRONY I OPERACYJNYCH
ASYSTENT SEKRETARZA GENERALNEGO ds. POLITYCZNYCH
ASYSTENT SEKRETARZA GENERALNEGO ds. INWESTYCJI BEZPIECZEŃSTWA, LOGISTYKI I CYWILNEGO PLANOWANIA W SYTUACJACH WYJĄTKOWYCH
ASYSTENT SEKRETARZA GENERALNEGO ds. NAUKOWYCH i OCHRONY ŚRODOWISKA
DYREKTOR ds. INFORMACJI i PRASY
KONTROLER FINANSOWY
SEKRETARZ WYKONAWCZY
DYREKTOR BIURA BEZPIECZEŃSTWA NATO
DYREKTOR ds. ZARZĄDZANIA

BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

ORGANIZACJA STANDARYZACJI W NATO



BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

WSPARCIE REALIZOWANE W RAMACH CIMIC

WSPARCIE (WZMOCNIENIE) TRANSATLANTYCKIE
(czas - ok. 3 m-cy, do pół roku)

WSPARCIE (WZMOCNIENIE) KONTYNENTALNE
(czas - od 1 m-ca do ok. 4 m-cy)

WSPARCIE (WZMOCNIENIE) REGIONALNE
(czas -od 2-u do 10-ciu tygodni)

Zdolność państwa zagrożonego kryzysem, sytuacją nadzwyczajną lub konfliktem/działaniami wojennymi, do własnego organizowania sił : przeciwdziałanie kryzysowi/zagrożeniu (samoobrona), obrona militarna

WSPARCIE MILITARNE REALIZOWANE W RAMACH WYMOGÓW HNS

Siły Główne Sojuszu
Zdolność reakcji - (kilka miesięcy)

+

Siły Szybkiego Wzmocnienia RRF
Zdolność reakcji - kilka tygodni (miesiąc)

+

Siły Natychmiastowego Reagowania IFR
Zdolność reakcji - kilka dni (tygodni)

STANDARYZACJA

STRATEGIA WZMOCNIENIA SIL (za: Bolesław Balcerowicz, "Strategiczne koncepcje obrony" - wykład AON)

BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

MIEJSCE WSPARCIA (HNS)

W OBSZARZE DZIAŁAŃ WSPÓŁPRACY CYWILNO-WOJSKOWEJ (NATO- UN)

BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

KIERUNKI ROZWOJU NORMALIZACJI

Nowelizacja ustawy o normalizacji i przepisów wykonawczych, zwłaszcza:

- **zobowiązanie PKN do prowadzenia działalności normalizacyjnej związanej z OiBP;**
- **wyodrębnienie obszaru związanego z OiBP;**
- **ustawowe upoważnienie ministra obrony narodowej do koordynacji działalności normalizacyjnej z obszaru OiBP w kontaktach międzynarodowych;**
- **uznanie normy obronnej jako dokumentu normalizacyjnego;**
- **obowiązek utworzenia służby normalizacyjnej przez MON i MSWiA i fakultatywnie w innych resortach.**

Włączenie się w proces tworzenia przez ISO Komitetu Technicznego ds. normalizacji obrony cywilnej z siedzibą w Moskwie.

BIURO WOJSKOWEJ SŁUŻBY NORMALIZACYJNEJ

00-911 WARSZAWA 62
Al. Niepodległości 218
POLSKA

Poczta elektroniczna: : bwsnmon@ wp.mil.pl
: (+48-22) 6 876 328
: (+48-22) 6 876 906

Telefony kontaktowe:
: (+48-22) 6 874 274
: (+48-22) 6 874 824
: (+48-22) 6 876 321

RWT TELEFONY POLSKIE S.A.
Radom

Andrzej BRZĘCZKOWSKI

SYSTEM ŁĄCZNOŚCI W NOWEJ STRUKTURZE ZADAŃ UTRZYMANIA ZDOLNOŚCI REAGOWANIA NA SYTUACJE KRYZYSOWE

CENTRUM KONFERENCYJNE WP Grudzień 2001

Andrzej BRZĘCZKOWSKI

Elementy systemu łączności w nowej strukturze zadań związanych z potrzebą utrzymywania zdolności reagowania na kryzysy

RWT Telefony Polskie S.A.

Warszawa, 19 / 20 grudnia 2001 r.

RWT Telefony Polskie S.A.

- Lokalizacja: Radom.
- Tradycje produkcji sprzętu telekomunikacyjnego od roku 1938.
- Wykonane projekty dla operatorów telekomunikacyjnych, administracji państwowej oraz biznesu, finansów i edukacji.
- Wyróżnienia MŁ i nagrody branżowe.
- 9 miejsce w rankingu najszybciej rozwijających się firm wg Home and Market za lata 1998-2000.

2

RWT Telefony Polskie S.A.

- Klienci z grupy administracji państwowej oraz urzędy centralne:
  - Zakład Ubezpieczeń Społecznych;
  - Ministerstwo Obrony Narodowej;
  - Ministerstwo Spraw Wewnętrznych i Administracji;
  - Akademia Obrony Narodowej;
  - Straż Graniczna;
  - Kancelaria Sejmu RP.

3

RWT Telefony Polskie S.A.

- Grupa produktów:
  - telefony analogowe;
  - urządzenia do sieci ISDN;
  - cyfrowe systemy teletransmisyjne;
  - systemy dostępu do sieci danych oraz Internetu;
  - systemy wideokonferencyjne;
  - projekty informatyczne.

4

Oferta RWT-TP S.A.

- Urządzenia do sieci ISDN:
  - zakończenia sieciowe NT;
  - karty komputerowe;
  - telefony cyfrowe;
  - faksy grupy IV;
  - wideotelefony;
  - testery linii ;
  - centralki.

5

RWT-TP S.A.

- Systemy dostępu do sieci danych oraz Internetu
  - wykorzystanie technologii xDSL do 8Mb/s;
  - tworzenie wirtualnych sieci prywatnych;
  - możliwość zdalnej pracy w domu z bezpiecznym dostępem do danych korporacyjnych;
  - możliwość szybkiego dostępu do Internetu.

6

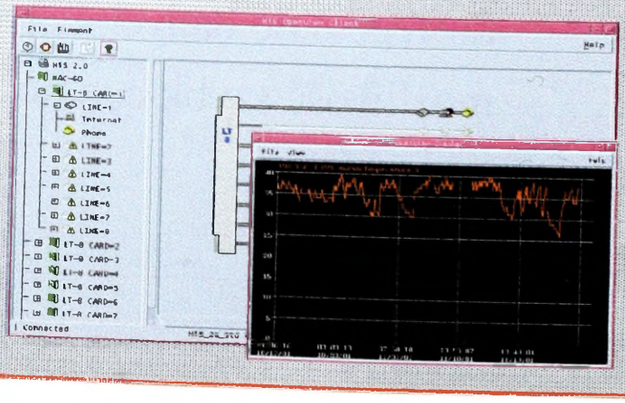
RWT-TP S.A.

- Systemy wideokonferencyjne:
  - zapewnienie komunikacji audio-wideo-dane z zagwarantowaniem jakości usług;
  - komunikacja wielopunktowa w sieciach ISDN i IP;
  - „wirtualne” spotkania wykluczające konieczność podróży, oszczędność czasu i kosztów;
  - doświadczona kadra inżynierska do realizacji każdego projektu.

7

RWT-TP S.A.

- Projekty informatyczne:
  - tworzenie oprogramowania w obszarze systemów zarządzania siecią teleinformatyczną;
  - tworzenie oprogramowania specjalistycznego.



Projekty RWT-TP S.A.

- System transmisji danych HiS:
  - wdrożenie w sieci TP S.A., obejmującej ponad 90 tysięcy zakończeń abonenckich, usługi SDI;
  - testowa instalacja systemu x DSL w Pomorskim Okręgu Wojskowym.

9

Projekty RWT-TP S.A.

- Wielopunktowy system wideokonferencyjny ZUS:
  - największa sieć wideokonferencyjna w Europie;
  - narzędzie zarządzania rozproszonymi jednostkami ZUS;
  - niezbędne medium szkoleń pracowników w trakcie wdrażania reformy ubezpieczeń społecznych;
  - redukcja kosztów operacyjnych.

10

Projekty RWT-TP S.A.

- Pilotażowy system wideokonferencyjny MSWiA:
  - kancelaria premiera RP, ministra MSWiA; Komenda Główna Policji oraz wojewodowie;
  - integracja rozproszonej struktury MSWiA;
  - przyspieszenie podejmowania decyzji;
  - narzędzie szybkiego reagowania w stanach nadzwyczajnych i kryzysowych;
  - system zgodny z modelem kierowania bezpieczeństwem narodowym w czasie pokoju, kryzysu, wojny.

11

Projekty RWT-TP S.A.

- Pilotażowy system wideokonferencyjny MSWiA:
  - realizacja wielopunktowej komunikacji między uczestnikami konferencji;
  - możliwość wymiany danych oraz pracy na wspólnej aplikacji i transferu plików;
  - możliwość rejestracji konferencji oraz odtwarzania materiałów audiowizualnych w jej trakcie.

12

Propozycja wdrożenia systemu wideokonferencyjnego w strukturze MON

- zapewnienie możliwości szybkiego reagowania na sytuacje wyjątkowe i kryzysowe;
- użyteczne narzędzie komunikacji na poziomie kierowania, dowodzenia i zarządzania obronnością kraju.

13

Propozycja wdrożenia systemu wideokonferencyjnego w strukturze MON

- zgodność ze standardami komunikacji przyjętymi w innych jednostkach administracji państwowej;
- zgodność z systemami komunikacji audiowizualnej stosowanymi w jednostkach dowodzenia NATO.

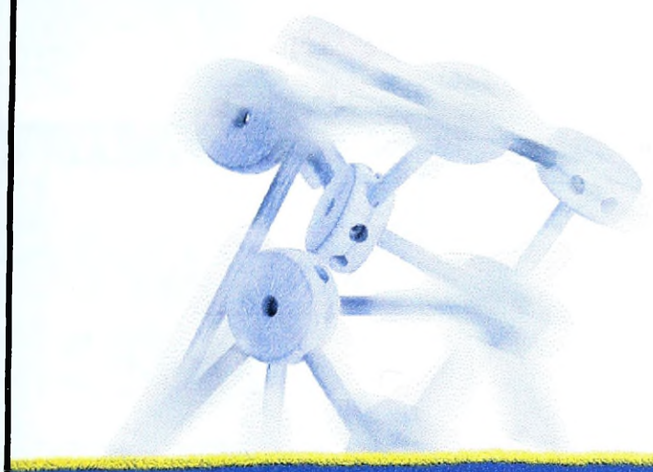
14

EMAX S.A.
Poznań

Maciej WACHOWSKI

SYSTEMY TELEINFORMATYCZNE W SYSTEMIE KIEROWANIA OBRONNOŚCIĄ PAŃSTWA

CENTRUM KONFERENCYJNE WP Grudzień 2001



Systemy teleinformatyczne w systemie kierowania obronnością państwa

ZEUS 2000

informatyka
sieci komputerowe
telekomunikacja

Maciej WACHOWSKI

Dział Produkcji Oprogramowania Emax SA

Konferencja pt. *„Kierowanie obronnością państwa podczas stanów nadzwyczajnych z wykorzystaniem technicznych środków najnowszej generacji"*
Warszawa, 19-20 grudnia 2001 r.

emax
MYŚL I TECHNOLOGIA

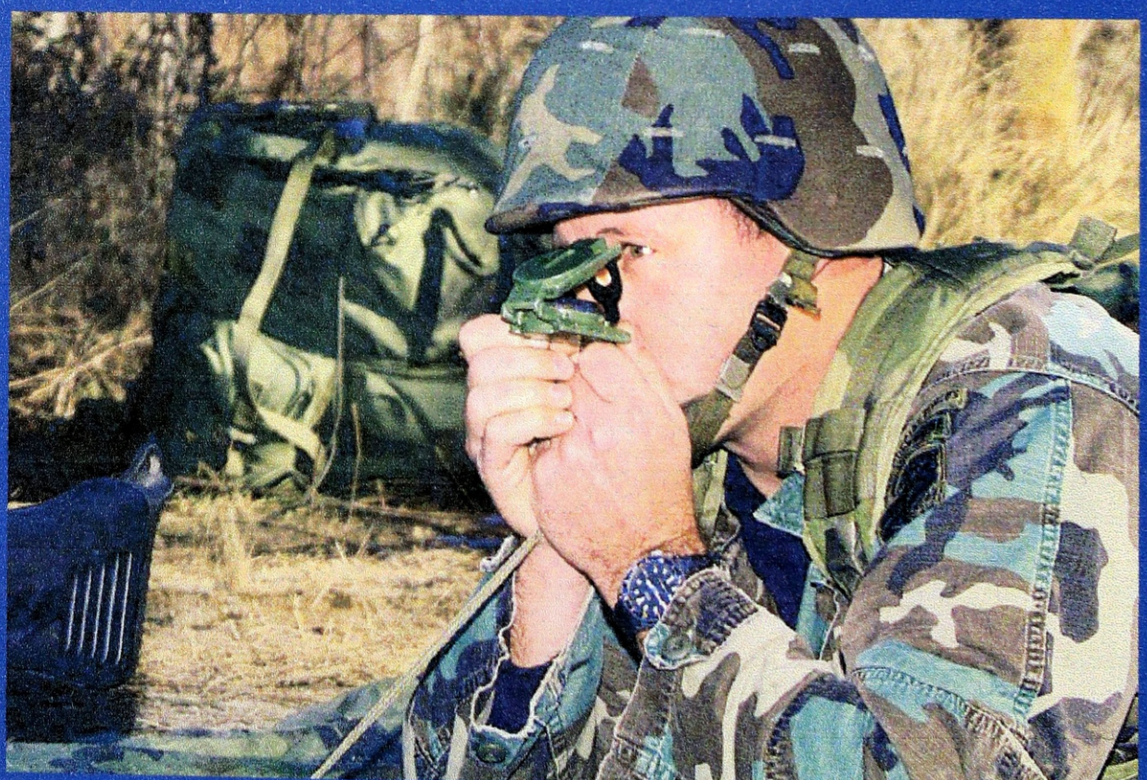
Plan prezentacji

- najpotężniejsza broń
- historia
- bezpieczna architektura systemów informatycznych
- aplikacje Emax SA

emax
MYŚL I TECHNOLOGIA

Najpotężniejsza broń?

Najpotężniejsza broń?

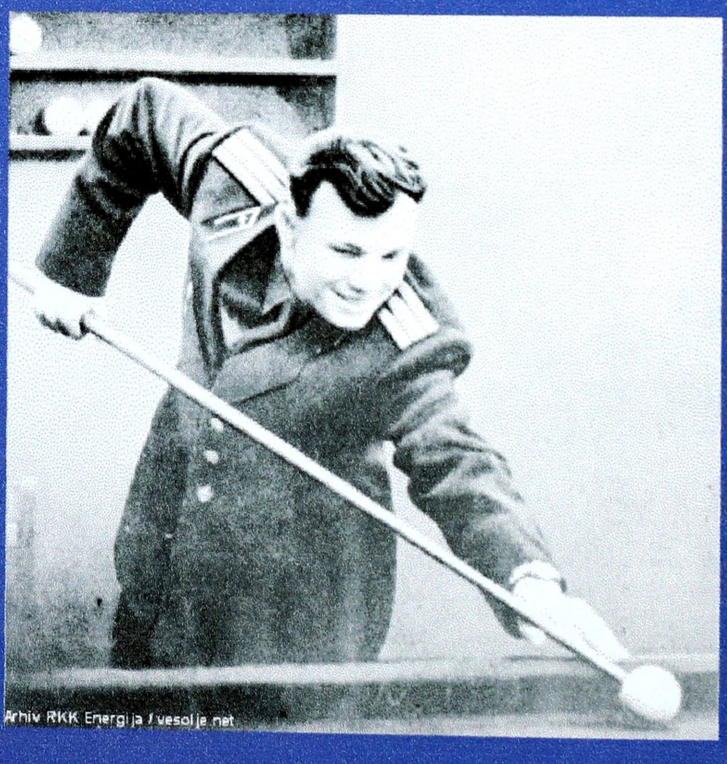


Najpotężniejsza broń?

Najpotężniejsza broń?

Najpotężniejsza broń?

Historia



emax
MYŚLI TECHNOLOGIA

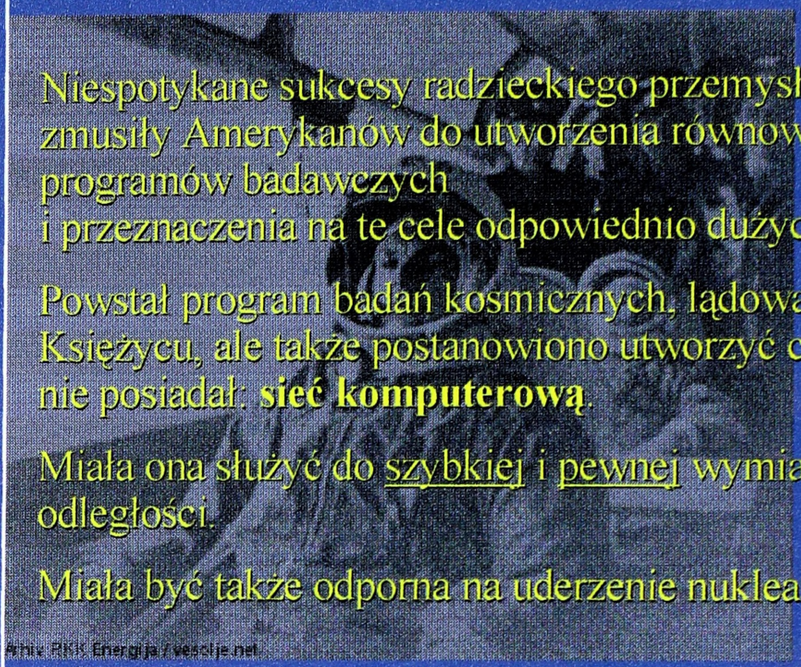
Historia

emax
MYSL I TECHNOLOGIA

Historia

emax
MYSL I TECHNOLOGIA

historia



Niespotykane sukcesy radzieckiego przemysłu kosmicznego zmusiły Amerykanów do utworzenia równoważących te sukcesy programów badawczych
i przeznaczenia na te cele odpowiednio dużych środków.

Powstał program badań kosmicznych, lądowania człowieka na Księżycu, ale także postanowiono utworzyć coś, czego przeciwnik nie posiadał: **sieć komputerową**.

Miała ona służyć do szybkiej i pewnej wymiany informacji na duże odległości.

Miała być także odporna na uderzenie nuklearne.

Arhiv PKS Energija / vesolje.net

emax
MYSL I TECHNOLOGIA

Historia

Pracami projektowymi w drugiej połowie lat sześćdziesiątych zajęła się amerykańska organizacja rządowa **ARPA** (ang. *Advanced Research Program Agency*).

W połowie roku **1968** ARPA zaprojektowała sieć czterech komputerów łączących:

- University of California in Los Angeles (UCLA);
- University of California in Santa Barbara (UCSB);
- Stanford Research Institute (SRI);
- University of Utah in Salt Lake City (UU).

W grudniu **1968** firma **BBN** (*Bolt, Beranek & Newman*) wygrała przetarg na wykonanie zaprojektowanej sieci.

emax
MYSL I TECHNOLOGIA

Historia

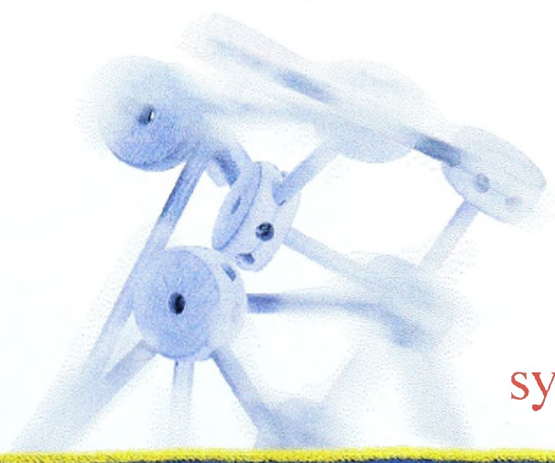
W grudniu **1969** roku sieć czterech komputerów została uruchomiona jako eksperyment, aby w 1971 roku stać się już normalną siecią użytkową. Zarządzał nią protokół NCP (ang. *Network Control Protocol*).

W **1972** roku ARPA stała się organizacją DARPA (ang. *Defense ARPA*) podległą Departamentowi Obrony USA.

W **1974** roku i kilku następnych została ukształtowana ostateczna postać architektury TCP/IP.

W roku **1985** prace nad architekturą TCP/IP uznano za zakończone i projekt został zamknięty.

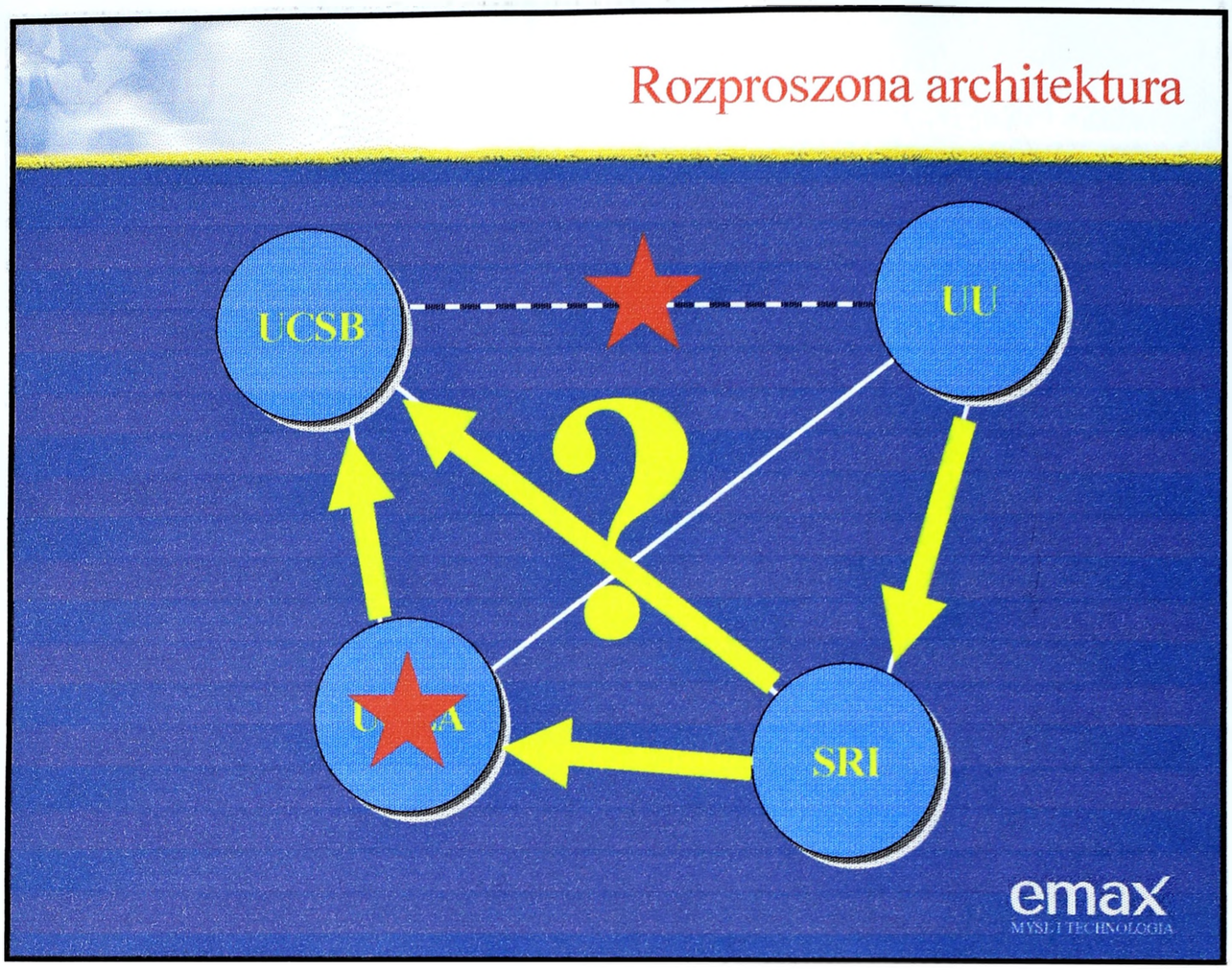
emax
MYSL I TECHNOLOGIA

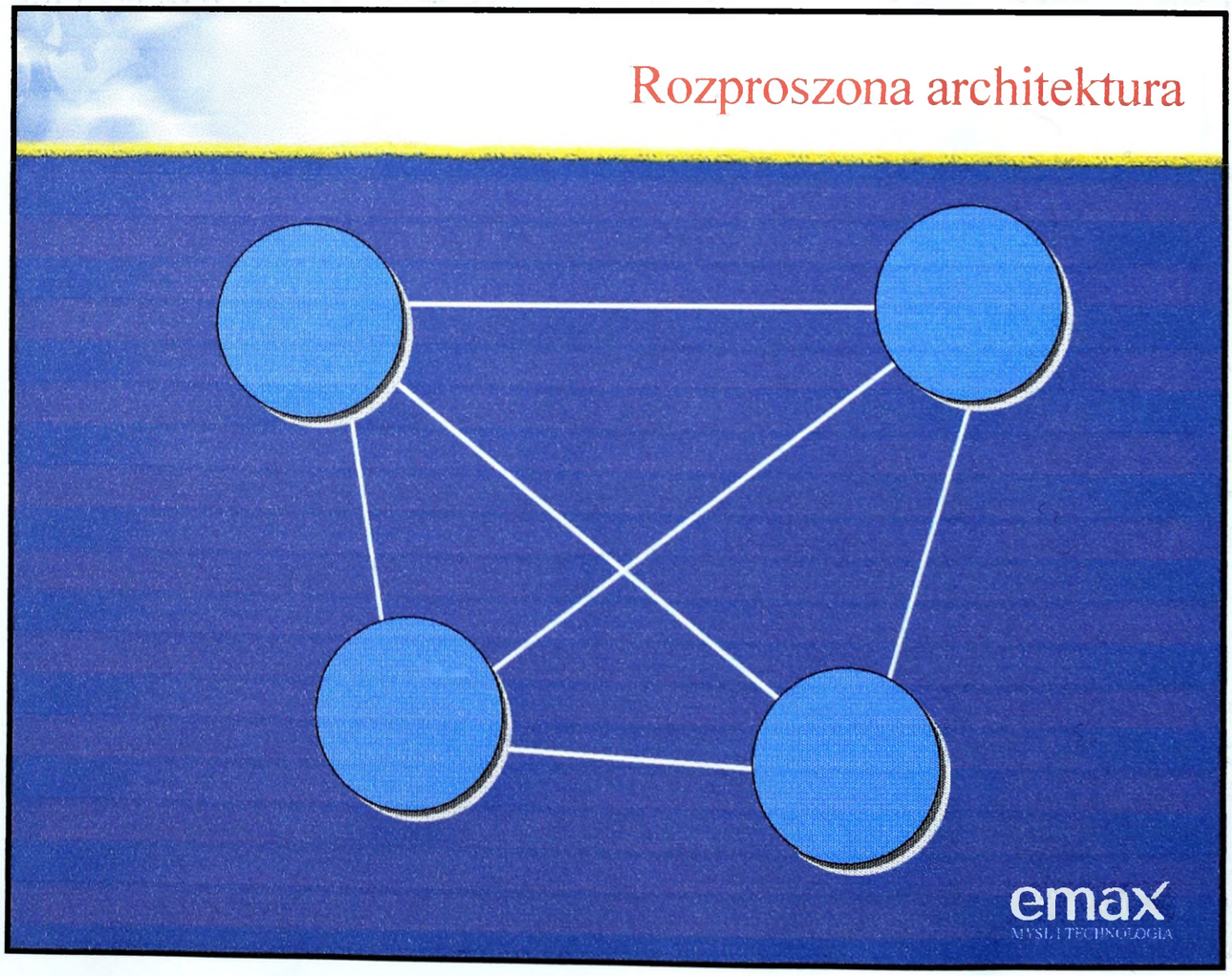


Bezpieczna architektura systemów informatycznych

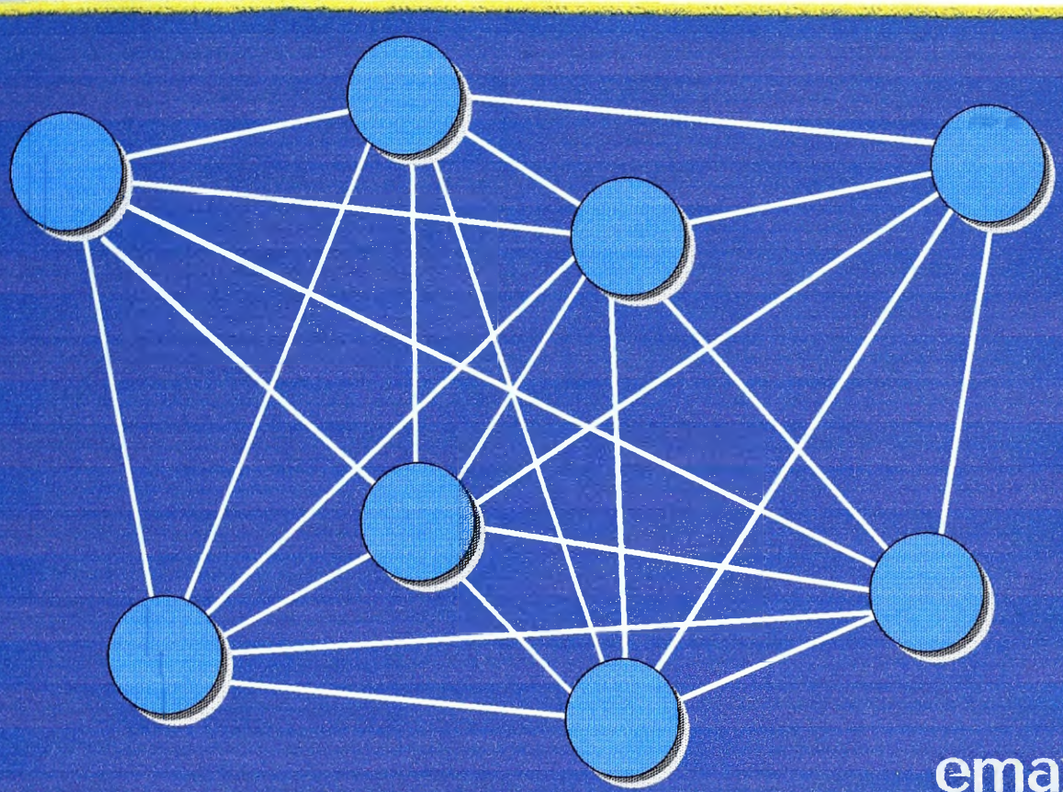
Co zadecydowało o sukcesie sieci ARPANET?

emax
MYSL I TECHNOLOGIA


Rozproszona architektura
UCSB
UU
SRI
emax
MYSLI TECHNOLOGIA

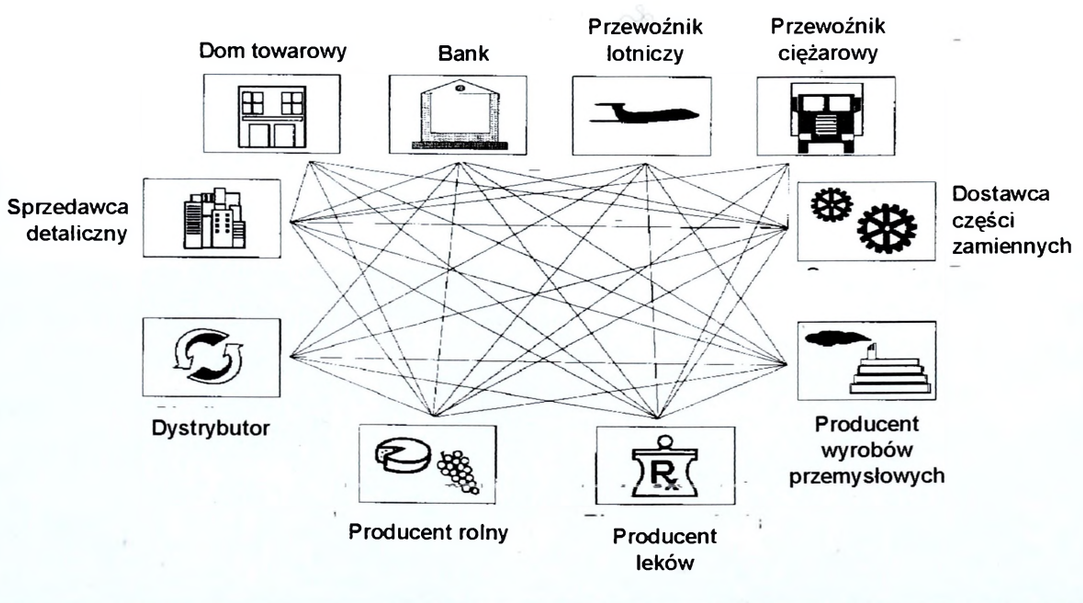

Rozproszona architektura
emax
MYSLI TECHNOLOGIA

Rozproszona architektura

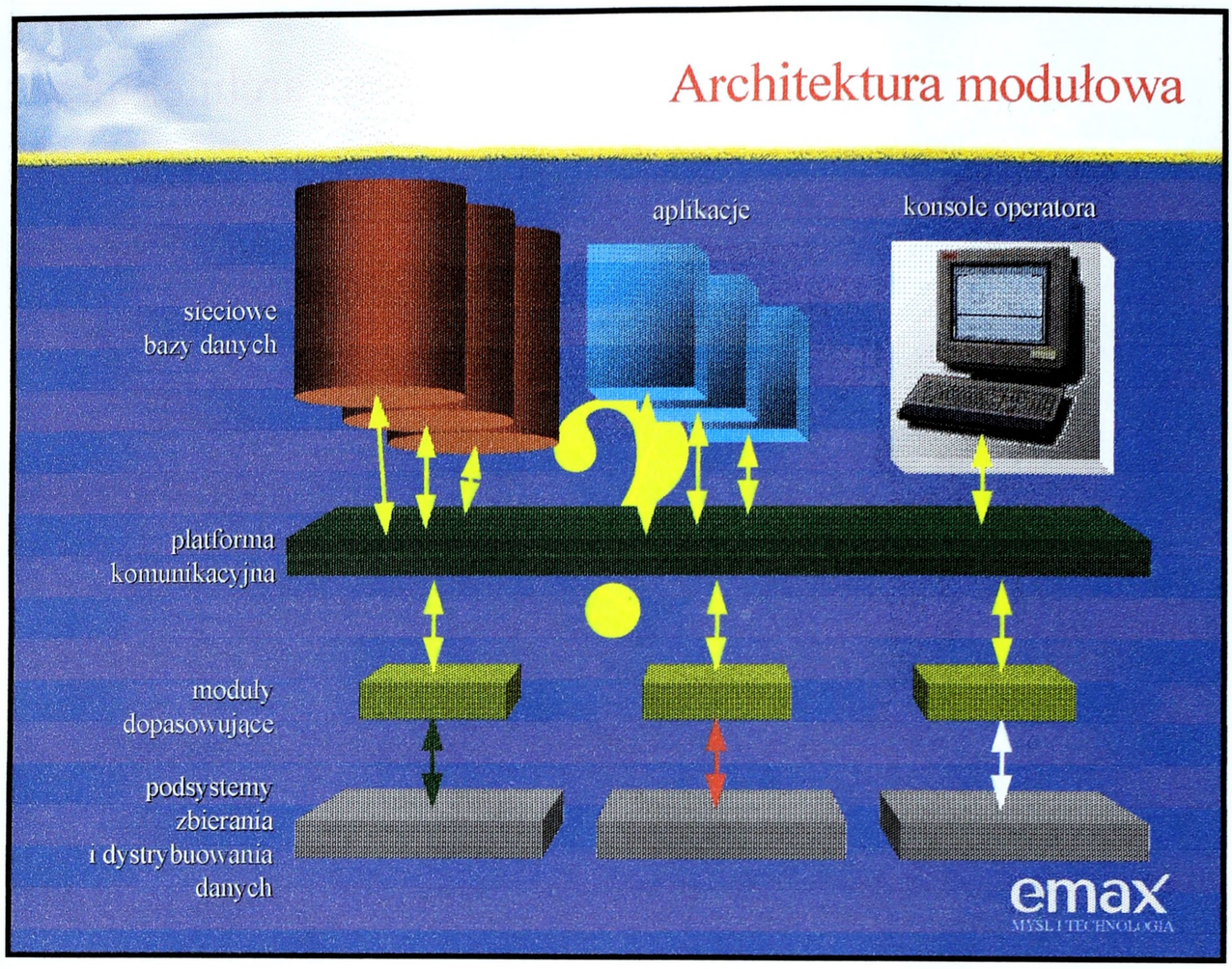


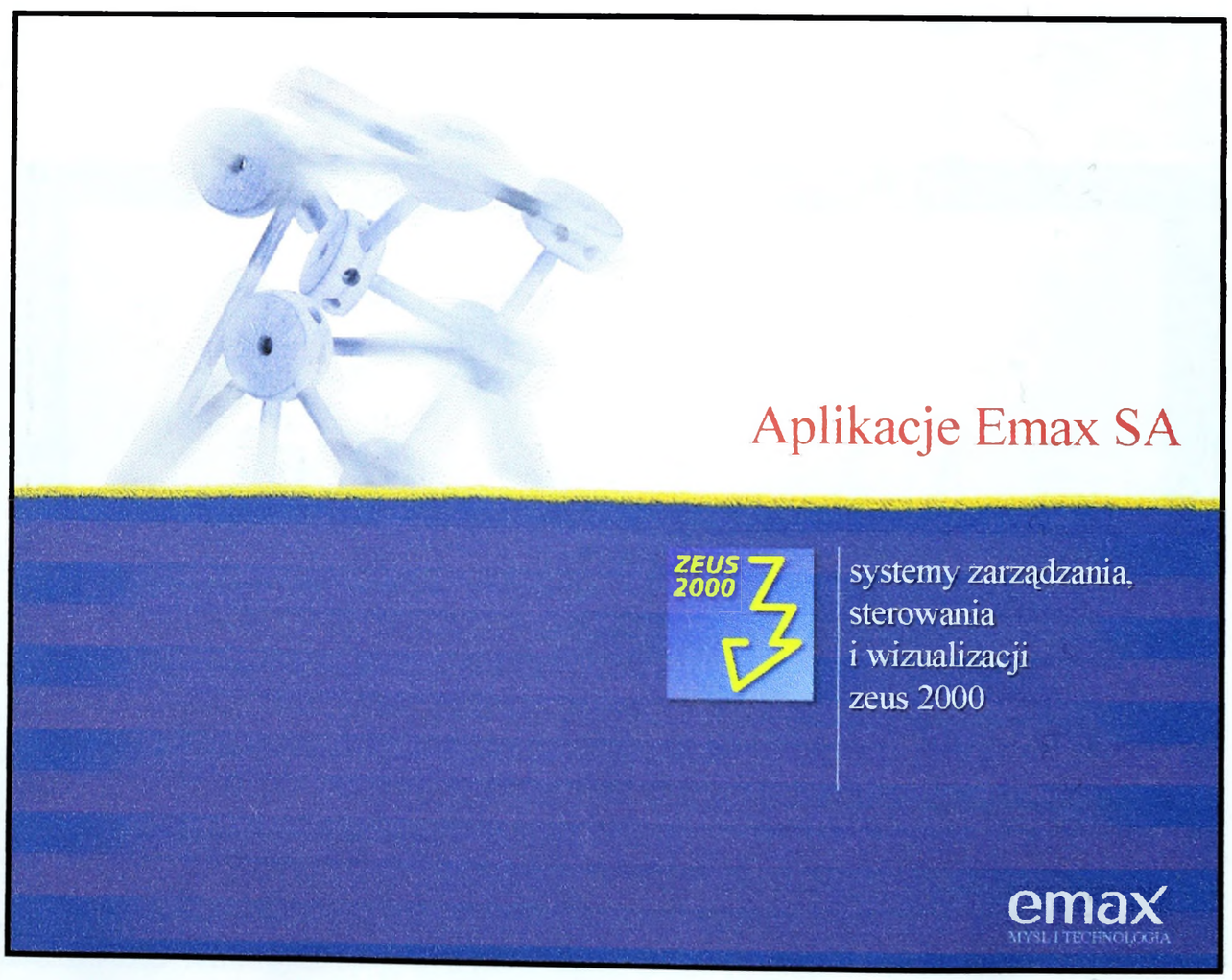
emax
MYSL I TECHNOLOGIA

Rozproszona architektura



emax
MYSL I TECHNOLOGIA


Architektura modułowa
aplikacje
konsole operatora
sieciowe
bazy danych
platforma
komunikacyjna
moduły
dopasowujące
podsystemy
zbierania
i dystrybuowania
danych
emax
MYŚL I TECHNOLOGIA


Aplikacje Emax SA
ZEUS
2000
systemy zarządzania,
sterowania
i wizualizacji
zeus 2000
emax
MYŚL I TECHNOLOGIA

Zintegrowany system zarządzania zeus 2000

- wizualizacja systemów zabezpieczeń;
- sterowanie systemami automatyki;
- rejestrowanie historii zdarzeń;

- otwartość i skalowalność;
- architektura sieciowa i modułowa;
- w całości produkt firmy Emax S.A..

emax
MYŚL I TECHNOLOGIA

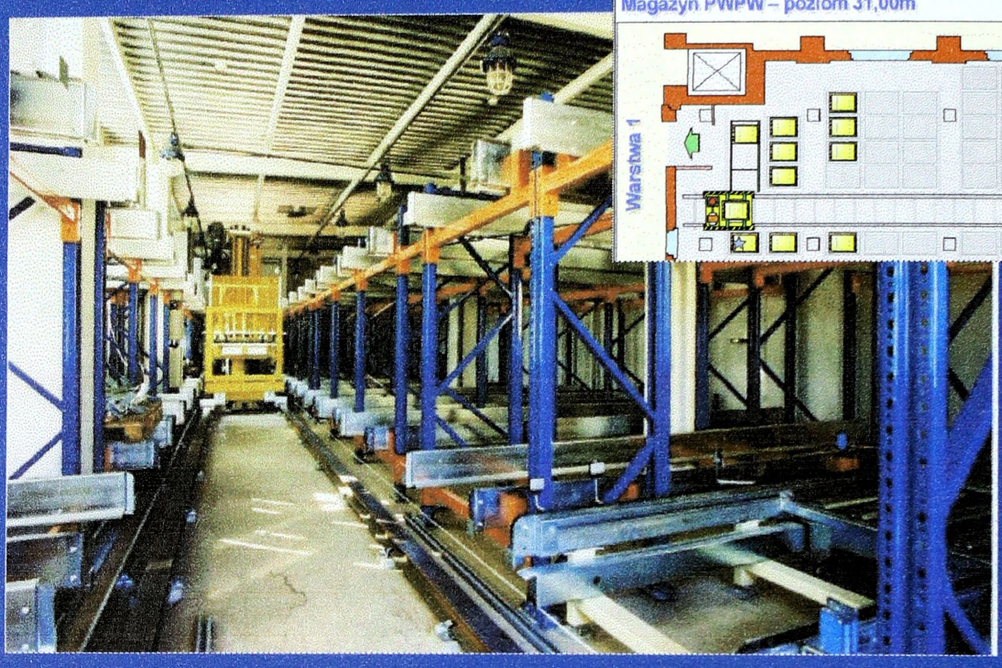
elektrownia bełchatów

rogowiec k. bełchatowa

emax
MYŚL I TECHNOLOGIA

polska wytwórnia papierów wartościowych

warszawa



emax
MYŚL I TECHNOLOGIA

szpital wojewódzki

jelenia góra

emax
MYŚL I TECHNOLOGIA

TUiR Warta

Warszawa

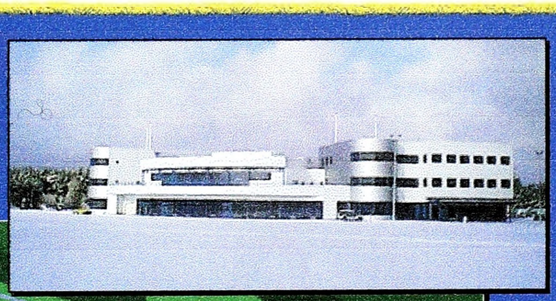
inteligentny biurowiec

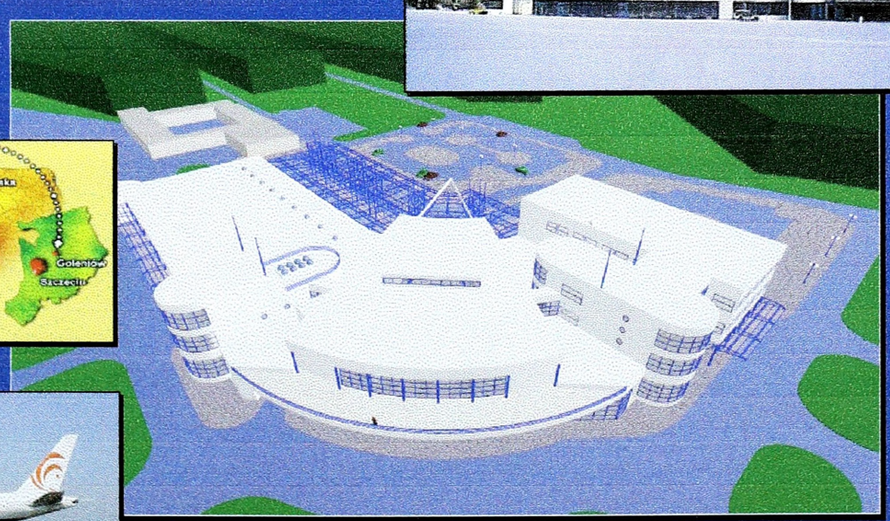
nadrzędny nadzór nad:
- sygnalizacją pożaru;
- sygnalizacją włamania;
- kontrolą dostępu;
- telewizją przemysłową;
- automatyką budynkową:
  . ogrzewanie;
  . klimatyzacja;
  . wentylacja;
  . oświetlenie;
  . zasilanie;
  . parkingi;
  itp.

emax
MYSL I TECHNOLOGIA

Lotnisko PPL Goleniów

Goleniów k. Szczecina





emax
MYSL I TECHNOLOGIA

Podsumowanie

- najpotężniejszą bronią jest dziś i zawsze była informacja;
- historia sieci komputerowych rozpoczęła się w 1968 roku – TCP/IP bez większych modyfikacji funkcjonuje do dziś;
- najlepszą obroną systemów informatycznych jest ich modułowość, decentralizacja i redundancja;
- zeus 2000 jest systemem firmy Emax S. A. zbudowanym zgodnie z ww. założeniami.

emax
MYŚL I TECHNOLOGIA

ZEUS 2000

Dział Produkcji Oprogramowania
Emax SA
ul. Niezłomnych 1C, 61-894 Poznań
tel. (0-61) 8717-281, fax (0-61) 8717-282
e-mail: dpo@emax.com.pl
http://www.emax.com.pl

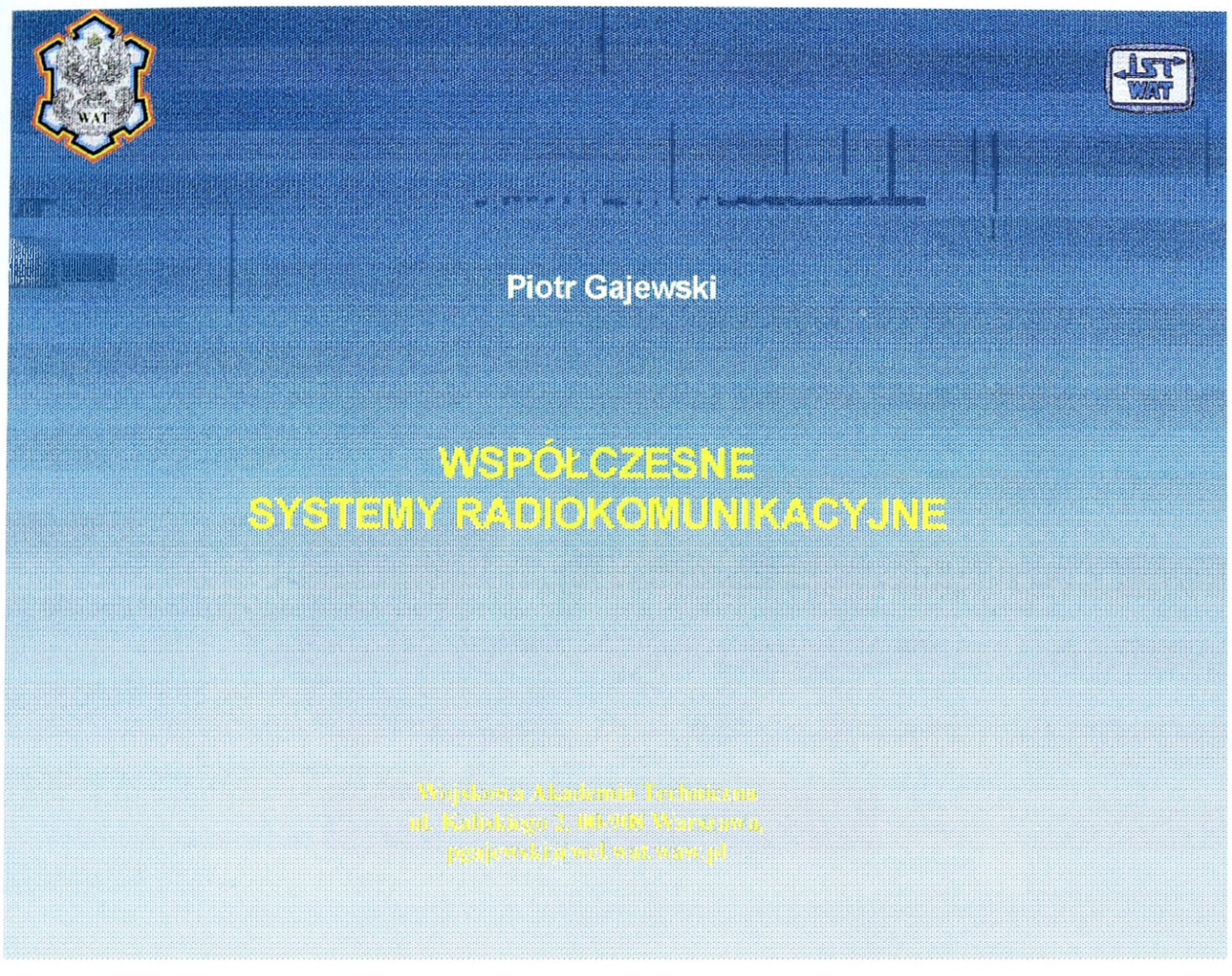
emax
MYŚL I TECHNOLOGIA

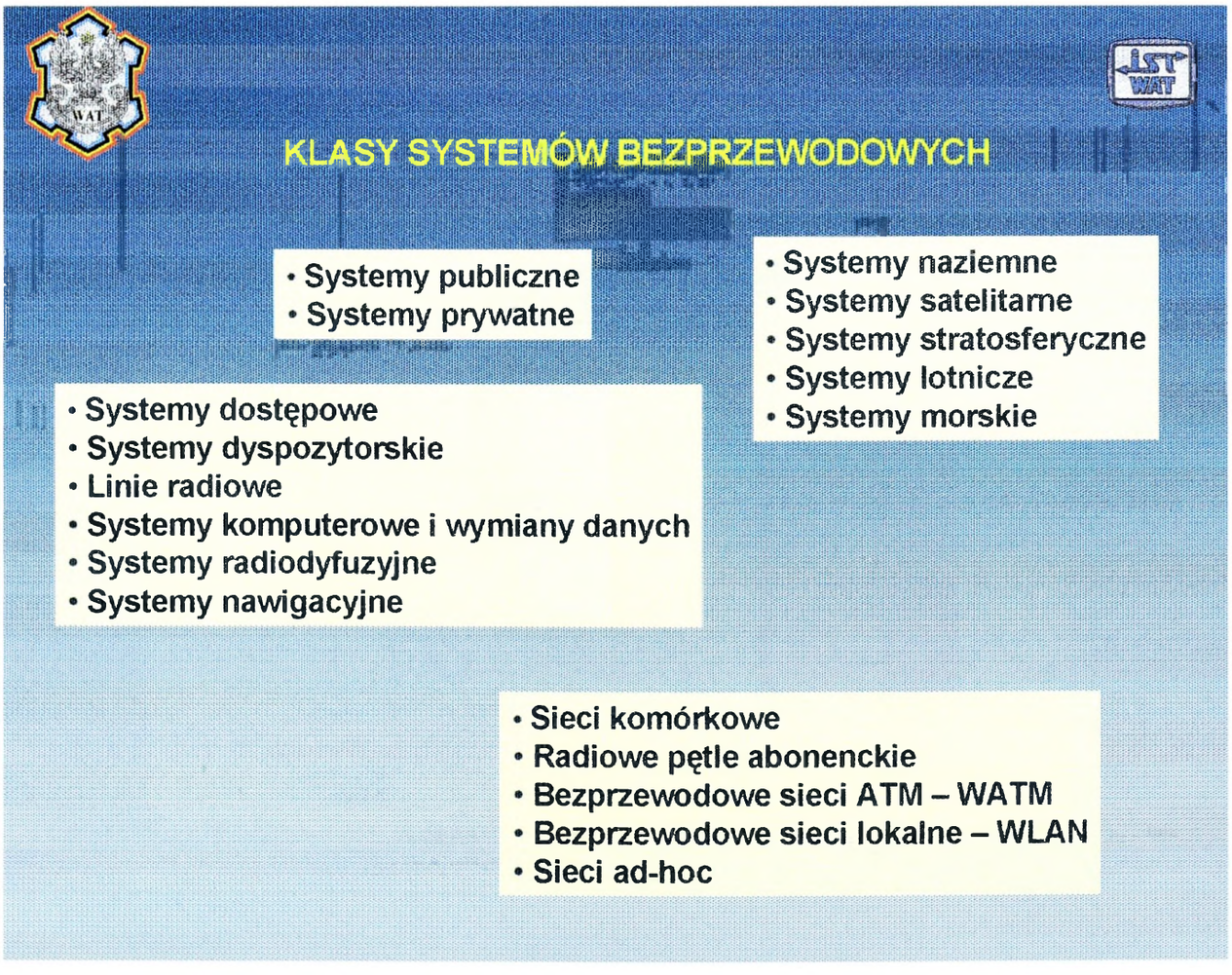
WOJSKOWA
AKADEMIA TECHNICZNA

Piotr GAJEWSKI

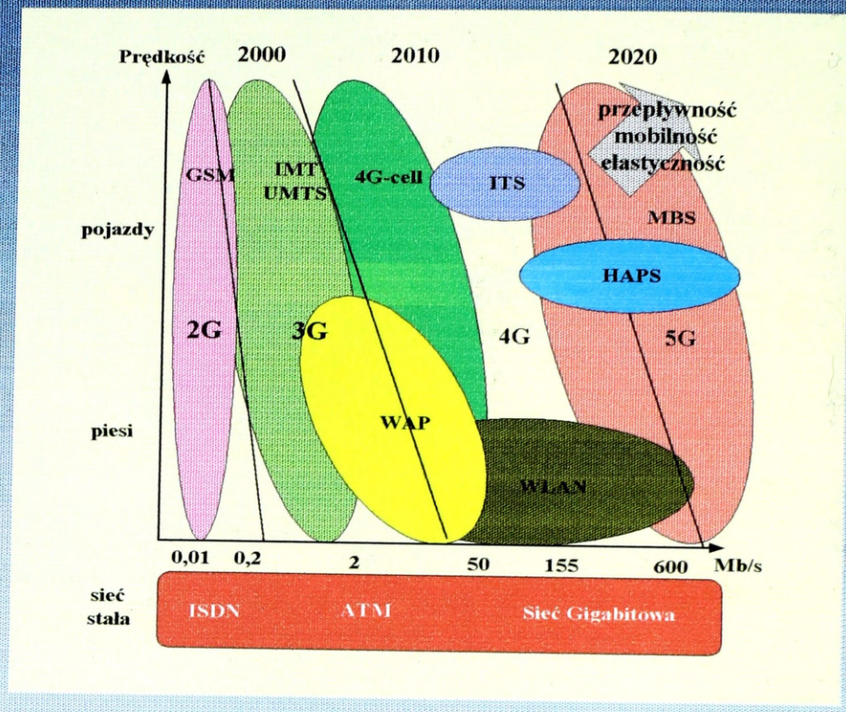
SYSTEMY RADIOKOMUNIKACYJNE NA POTRZEBY SYTUACJI KRYZYSOWYCH

CENTRUM KONFERENCYJNE WP Grudzień 2001

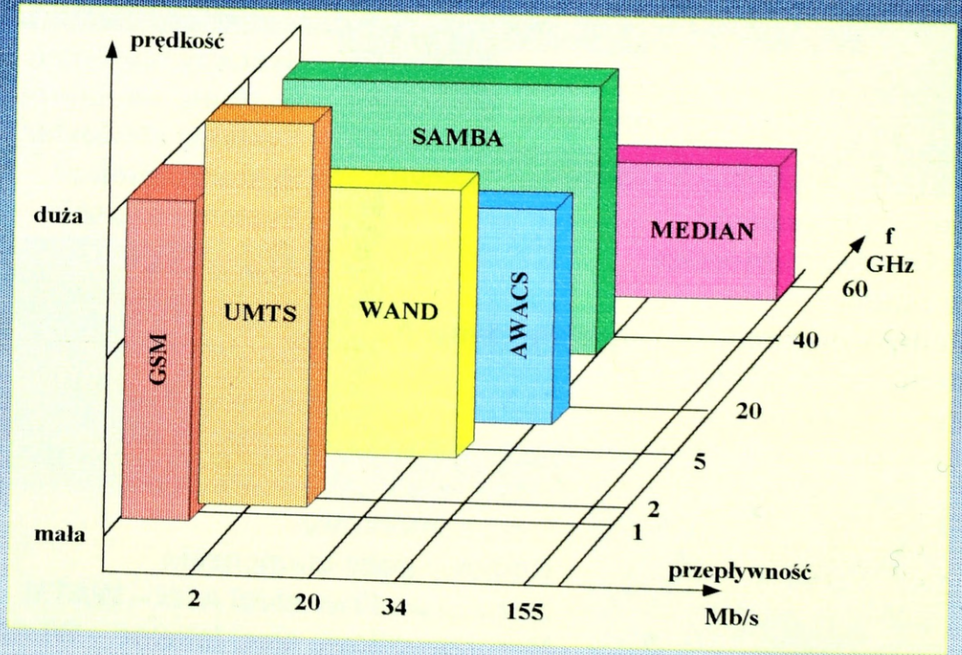

Piotr Gajewski
WSPÓŁCZESNE
SYSTEMY RADIOKOMUNIKACYJNE
Wojskowa Akademia Techniczna
ul. Kaliskiego 2, 00-908 Warszawa
pgajewski@wel.wat.waw.pl


KLASY SYSTEMÓW BEZPRZEWODOWYCH
• Systemy publiczne
• Systemy prywatne
• Systemy naziemne
• Systemy satelitarne
• Systemy stratosferyczne
• Systemy lotnicze
• Systemy morskie
• Systemy dostępowe
• Systemy dyspozytorskie
• Linie radiowe
• Systemy komputerowe i wymiany danych
• Systemy radiodyfuzyjne
• Systemy nawigacyjne
• Sieci komórkowe
• Radiowe pętle abonenckie
• Bezprzewodowe sieci ATM – WATM
• Bezprzewodowe sieci lokalne – WLAN
• Sieci ad-hoc

MOBILNOŚĆ I PRZEPŁYWNOŚĆ



EKSPANSJA CZĘSTOTLIWOŚCI



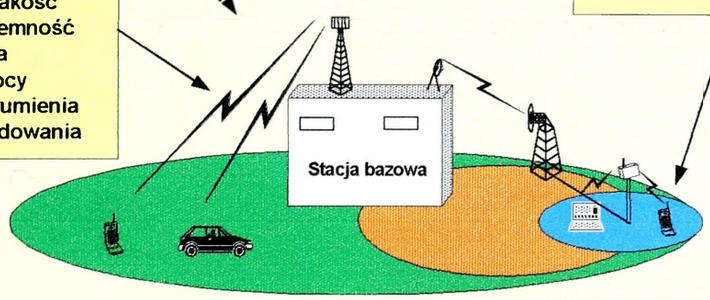
KLUCZOWE TECHNOLOGIE

Propagacja:
- fale milimetrowe
- szerokie pasmo

Anteny adaptacyjne:
- kształtowanie charakterystyki
- tłumienie interferencji
- algorytmy

Modulacja/transmisja
- duża szybkość
- wysoka jakość
- duża pojemność
- adaptacja
  - mocy
  - strumienia
  - kodowania

Technologie radiowe:
- software radio



Bezpieczeństwo i ekologia:
- zabezpieczenie systemu i informacji
- narażenia człowieka
- zewnętrzna EMC

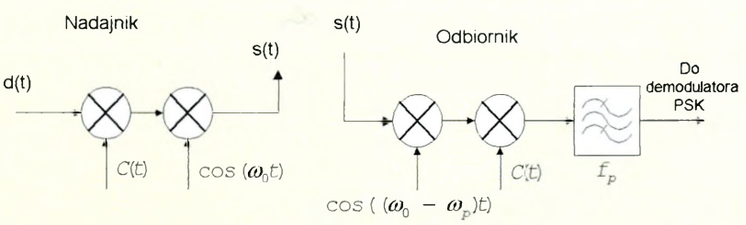
Architektury sieciowe
- sieć pakietowa IP
- bezproblemowe zarządzanie usługami i połączeniami
- efektywne zarządzanie mobilnością
- sterowanie jakością
- struktury piko-, mikro- i makrokomórkowe
- sieci ad-hoc

METODY ROZPRASZANIA WIDMA

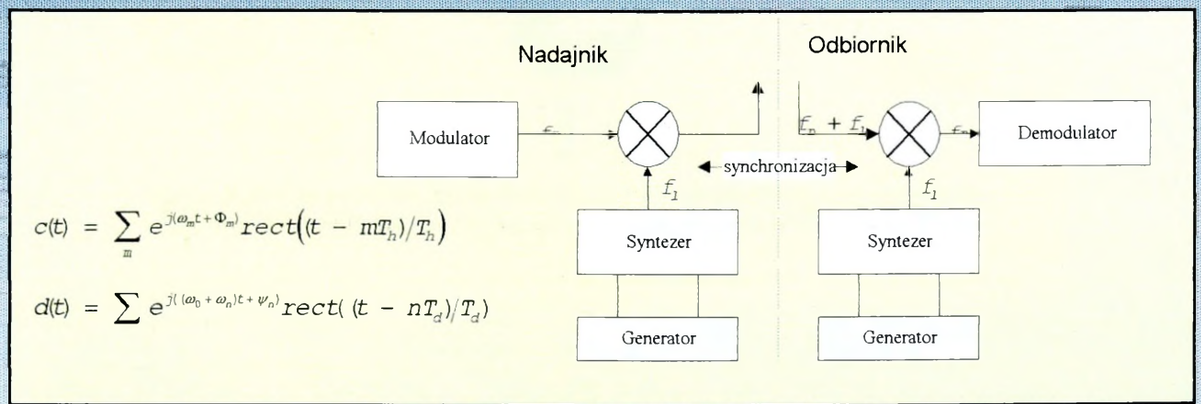
Metoda DS

$$c(t) = \sum_m c_m g_c(t - mT_c)$$

$$d(t) = \sum_n d_n g_d(t - nT_d)$$



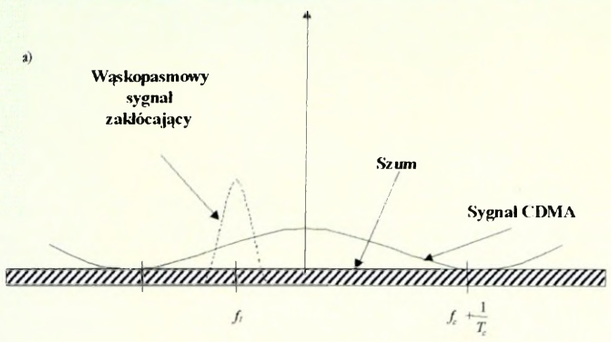
Metoda FH



$$c(t) = \sum_m e^{j(\omega_m t + \Phi_m)} rect\left((t - mT_h)/T_h\right)$$

$$d(t) = \sum e^{j(\omega_0 + \omega_n)t + \psi_n)} rect((t - nT_d)/T_d)$$

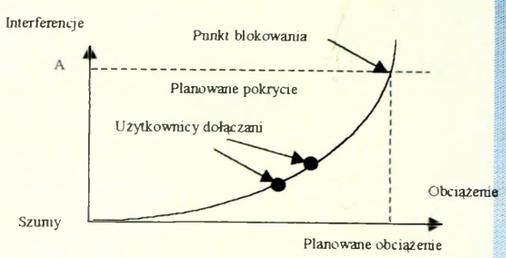
ZALETY SYSTEMU DS-CDMA



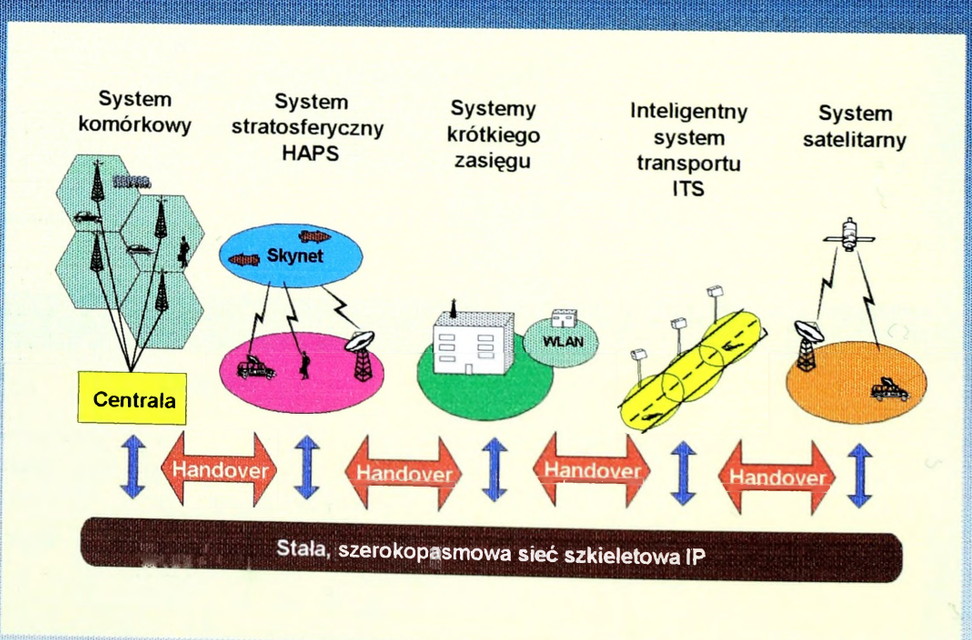
Zysk rozpraszania

$$G_p = \frac{(S/Z)_{wyj}}{(S/Z)_{wej}} \approx \left(\frac{B_{SS}}{B}\right) \approx \frac{T_e}{\tau_i}$$

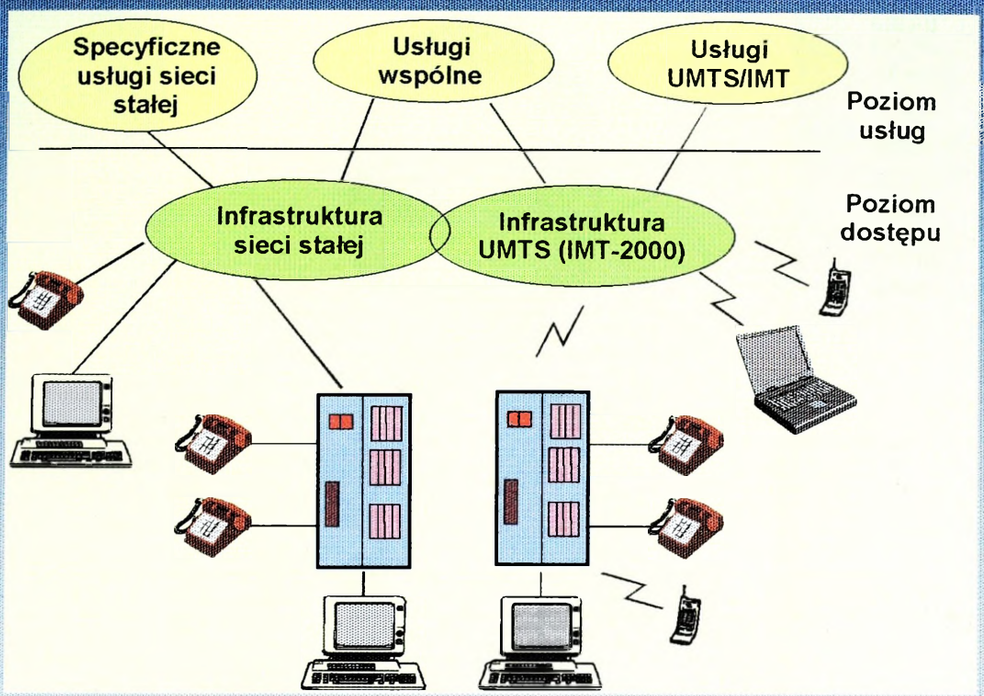
Zależność poziomu zakłóceń Interferencyjnych w stacji bazowej od liczby abonentów



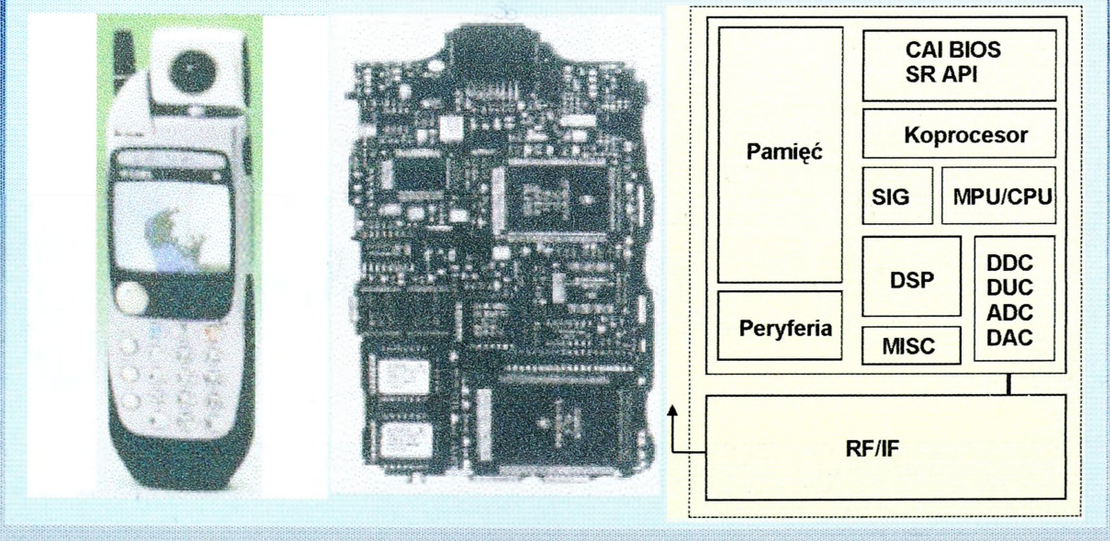
ARCHITEKTURA SYSTEMU 4G, 5G



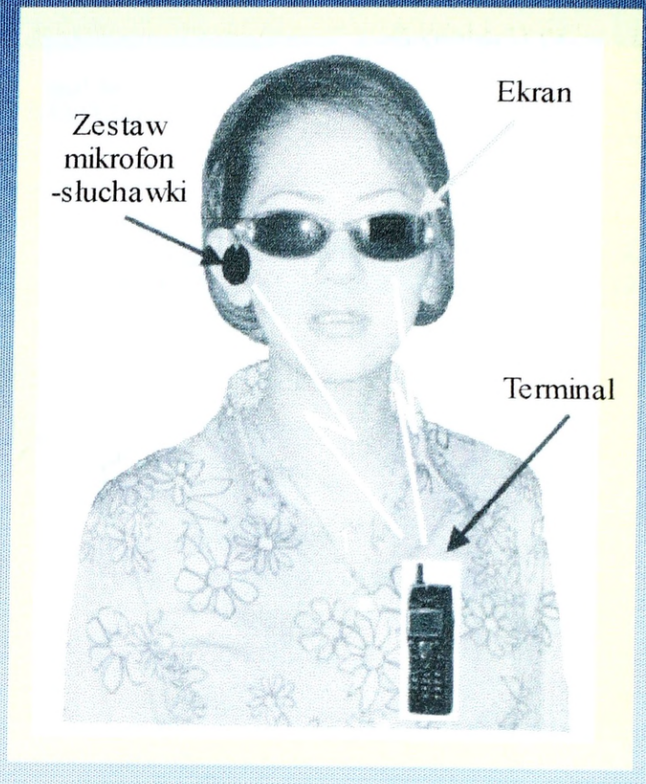
ARCHITEKTURA SYSTEMU UMTS/IMT 2000



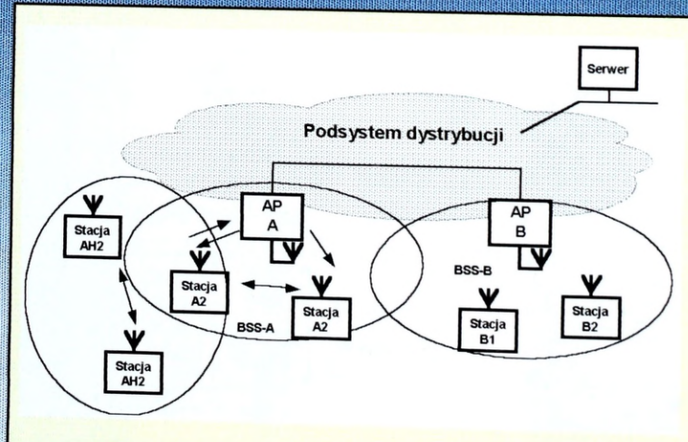
TERMINAL PROGRAMOWALNY



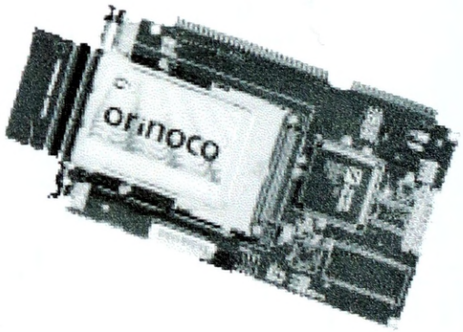
„ MOBILE WALKER" - 2010



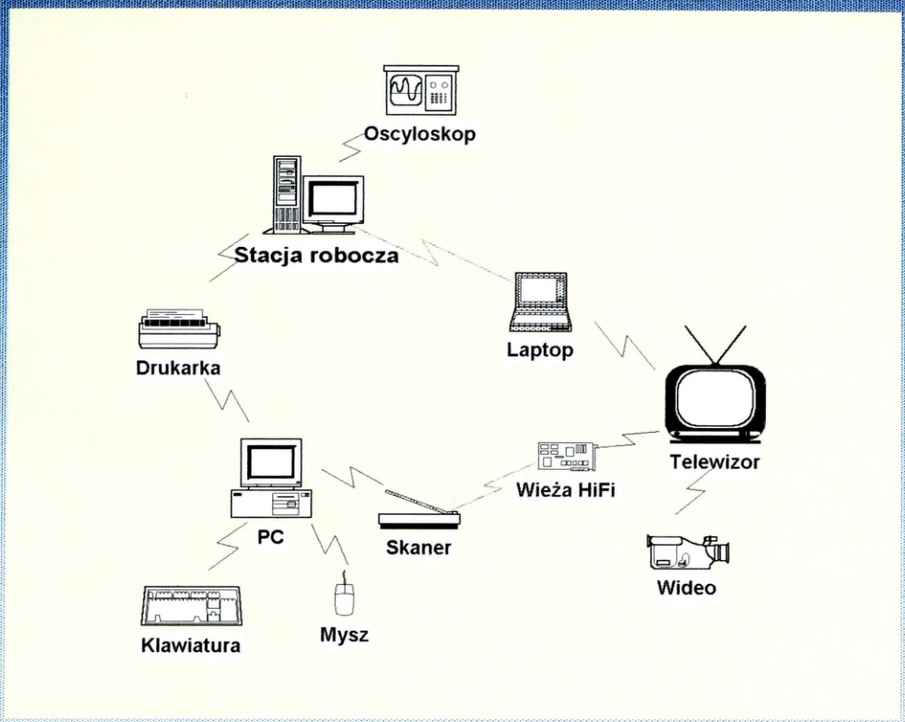
SIECI WLAN



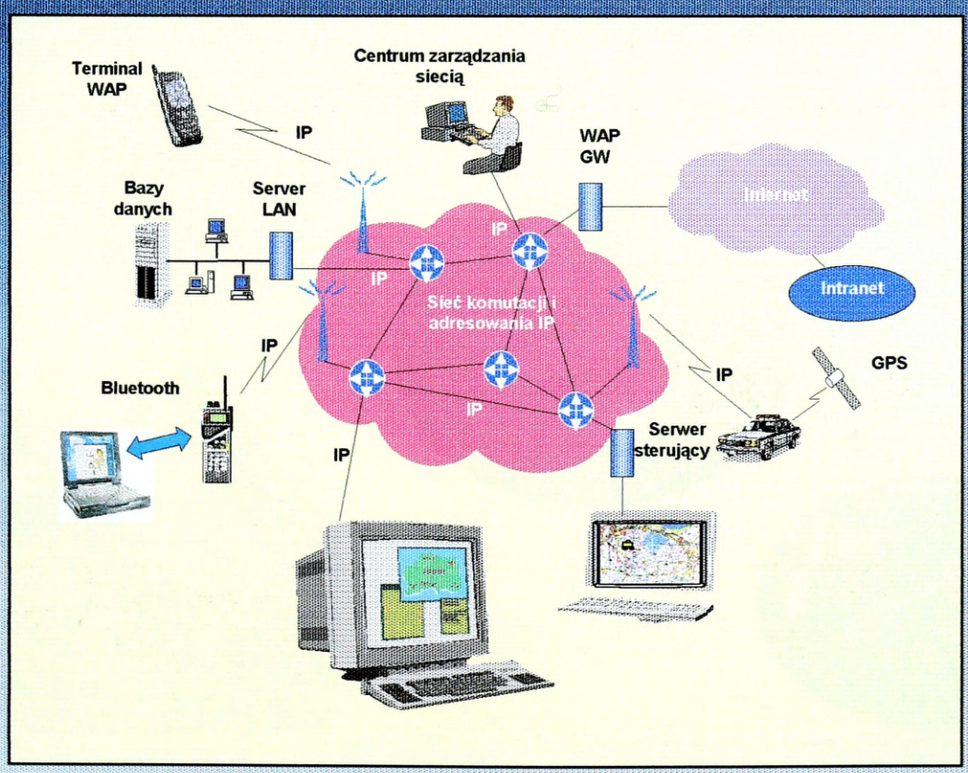
b)



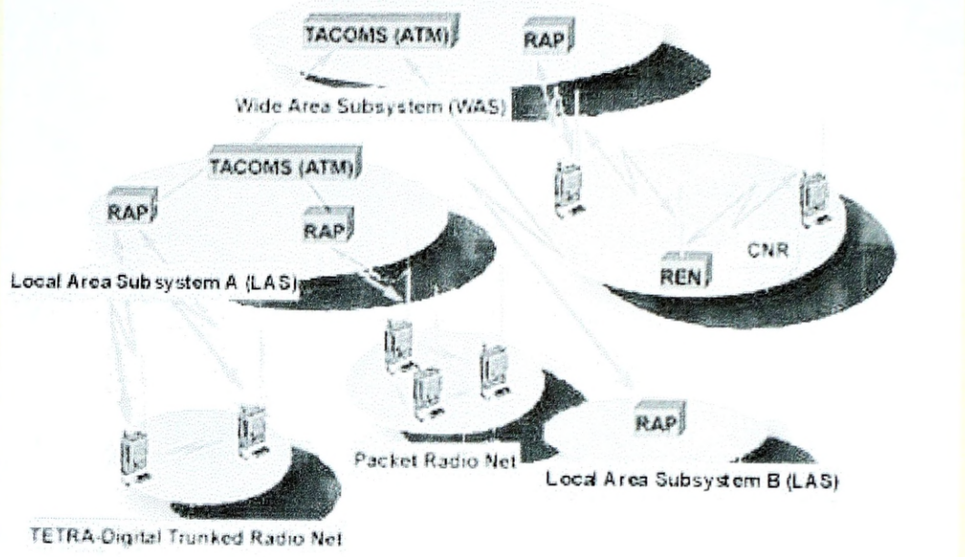
SYSTEMY AD-HOC



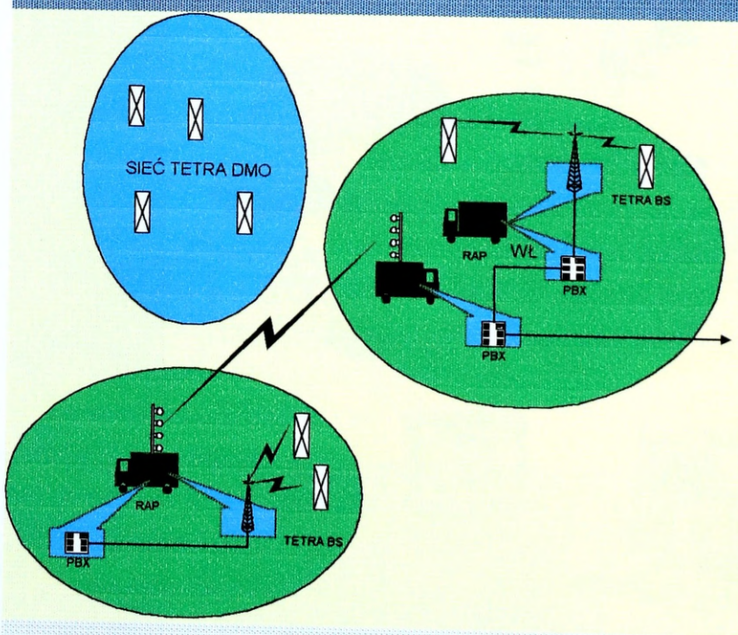
SIEĆ IP - PRZYKŁAD

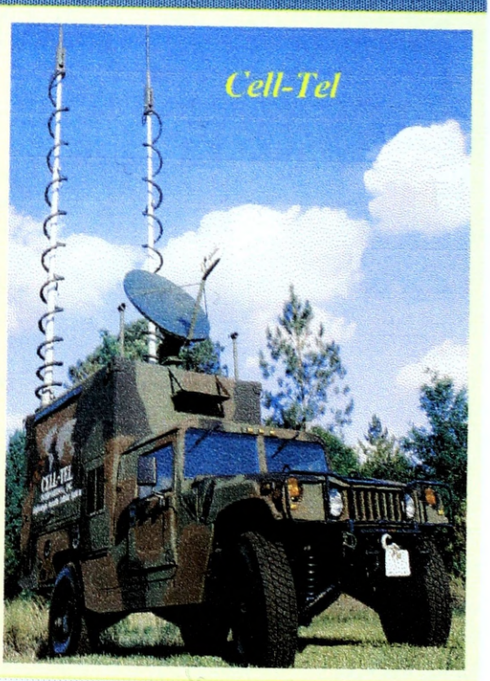


SYSTEMY BEZPRZEWODOWE W OGÓLNEJ ARCHITEKTURZE CIS - przykład

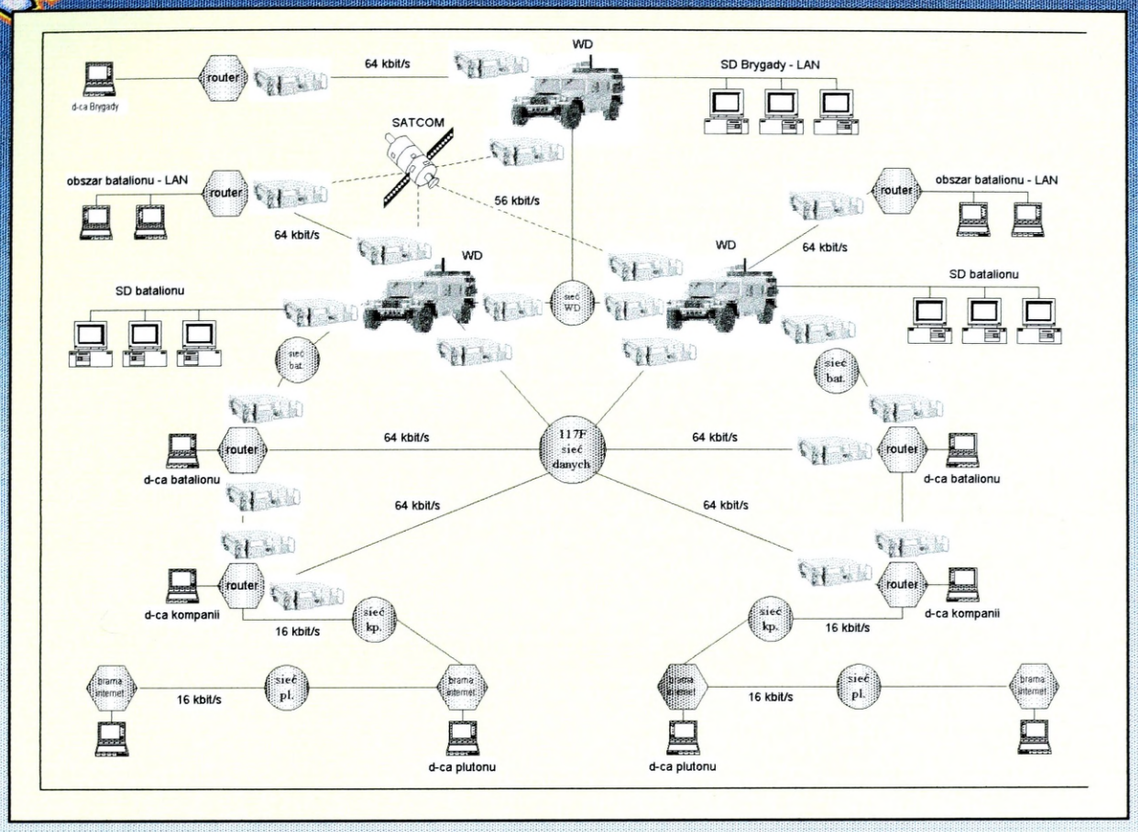


MILITARY TETRA, MILITARY GSM





MULTI-ROLE RADIO



ROZWÓJ SYSTEMÓW BEZPRZEWODOWYCH WYZWANIA

- ***Modernizacja systemów militarnych:***
  - ✓ *Szerokopasmowa sieć szkieletowa IP;*
  - ✓ *Szerokopasmowe sieci dostępowe i lokalne;*
  - ✓ *Zastosowanie bezprzewodowych technologii COTS.*
- ***Organizacja testbedów:***
  - *Symulatory;*
  - *Testy technologii COTS.*
- ***Efektywność widmowa:***
  - ➢ *Optymalizacja projektowania i planowania systemów;*
  - ➢ *Zarządzanie widmem.*

ERA Sp. z o.o.
Warszawa

Krzysztof OLEJNIK

BEZPIECZNA KOMUNIKACJA – ERA BIZNES

CENTRUM KONFERENCYJNE WP Grudzień 2001

Usługi Najnowszej Generacji Sieci ERA

Konferencja naukowa 19-20 grudnia 2001 r.

Sieć Era dzisiaj

- Główna siedziba firmy w Warszawie
  - supernowoczesne Centrum Zarządzania Siecią (NMC).
- Zatrudniamy ponad 3 600 osób.

Sieć Era dzisiaj

- Największy operator telefonii komórkowej w Europie Środkowej od 5 lat.
- Ponad 140 tyś. klientów instytucjonalnych – 65% zarejestrowanych w GUS.
- Ponad 3,6 mln. abonentów - 39% w kraju.
- Największa sieć Doradców Biznesowych wśród firm telekomunikacyjnych, gwarancją doboru najkorzystniejszej oferty:
  - 102, Doradców Biznesowych;
  - 608, Autoryzowanych Doradców Biznesowych.
- Największa sieć sklepów firmowych (70), gwarancją najwyższego poziomu obsługi.
- Biuro Obsługi Abonenta – ISO 2001.

Sieć Era to prestiż
nagrody i wyróżnienia

- **Najlepiej zinformatyzowaną firmą telekomunikacyjną w Polsce.** Ten tytuł przyznawany przez miesięcznik **TELEINFO** otrzymaliśmy już po raz drugi. – **listopad 2001r.**
- **Złota nagroda Quality Summit Award** przyznana przez **Business Inititive Direction**, przyznawana jest m.in. za efektywność, dobre wyniki finansowe oraz wdrażanie nowoczesnych technologii. – **lipiec 2001r.**
- **Złoty Medal** na międzynarodowych **targach Infosystem** w Poznaniu. – **kwiecień 2001r.**
- **Nagroda specjalna „za najlepszą sieć usług ułatwiających prace menedżerom".** W ten sposób oceniono nowy system taryfikacyjny przeznaczony dla abonentów biznesowych - Era Biznes. Nagroda została przyznana przez **Stowarzyszenie Menedżerów w Polsce**. – **grudzień 2000r.**

Era Biznes

Pragnie, wesprzeć działania Administracji Państwowej w kreowaniu strategii gospodarczej i społecznej Polski, najnowocześniejszymi rozwiązaniami informatyczno-telekomunikacyjnymi, które umożliwia sprawne i tańsze zarządzanie Państwem.

5

Zamknięta grupa
usługa „Sieć korporacyjna"

- **Bezpieczne rozmowy w ramach zamkniętej grupy do której mają dostęp tylko jej członkowie.**
- Stosowanie profili użytkownika to możliwość nadawania poszczególnym osobom odpowiednich uprawnień.
- Parametrami Sieci Korporacyjnej w firmie może zarządzać jedynie jej administrator.
- Plan numeracyjny może być opracowany na bazie wskazanej struktury np. podziału regionalnego etc.
- **Taryfikacja za 1 sekundę.***

* pierwsze 30 sek., następne co 1 sek.

6

Efektywne zarządzanie kosztami połączeń

usługa „Podział płatności"

- Instytucja opłaca taryfę biznesową oraz abonament wynikający z usługi podział płatności:
  - ograniczenie wydatków na telefony, wygodny sposób planowania i kontroli kosztów rozmów telefonicznych.
- Pracownik użytkuje telefon i pokrywa koszt rozmów realizowanych poza limit darmowych minut wynikających z taryfy biznesowej:
  - możliwość zaoferowania telefonów większej ilości pracownikom.
- Instytucja i pracownik otrzymują osobne faktury:
  - brak problemu rozliczeń z pracownikami.

7

Praca w zamkniętych grupach

usługa „GSM Pro"

- Tam gdzie istnieje potrzeba komunikacji grupowej:
  - jedno połączenie to rozmowa 16 osób;
  - sms-y, to wygoda i szybkość informacji.
- Tam gdzie istnieje rozbudowana infrastruktura GSM:
  - wydzielony system łączności na bazie GSM.
- GSM dostosowany funkcjonalnie do potrzeb klienta.
- Tendencja do spadku taryf w sieciach GSM.

8

Efektywne zarządzanie zasobami
usługa „Zarządzanie flotą”

- Wyższa efektywność wykorzystania dostępnych środków transportowych i ludzkich:
  - kontrola czasu pracy, przebiegów, tras.
- Zmniejszenie kosztów (np. ograniczenie „pustych przebiegów”):
  - automatyzacja rozliczeń z kierowcami.
- Nowe możliwości zarządzania zasobami:
  - kontrola („wycieki paliwa”, efektywność pracy);
  - stały kontakt z kierowcą i pojazdem;
  - dokumentowanie czasu dojazdu do wypadku, zdarzenia;
  - wdrożenie systemu ostrzegania o awariach, opóźnieniach.

A co za tym idzie:

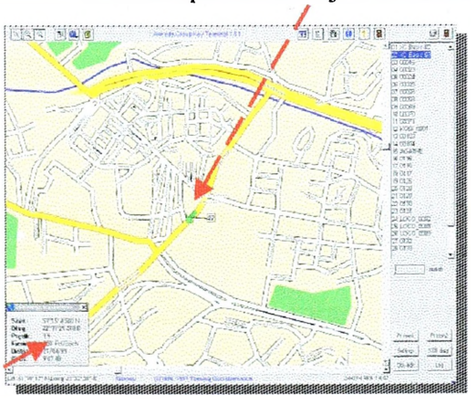
- zwiększa wydajność i obniża koszty ponoszone na użytkowanie taboru.

9

Zasady zarządzania
usługa „Zarządzanie flotą”

Monitorowany pojazd

Zielona strzałka precyzyjne odwzorowuje pozycję pojazdu na ekranie operatora stacji z dokładnością do 5 m



Stacja Monitorowania śledzi i rejestruje dokładną pozycję lub trasę przejazdu i stan czujników

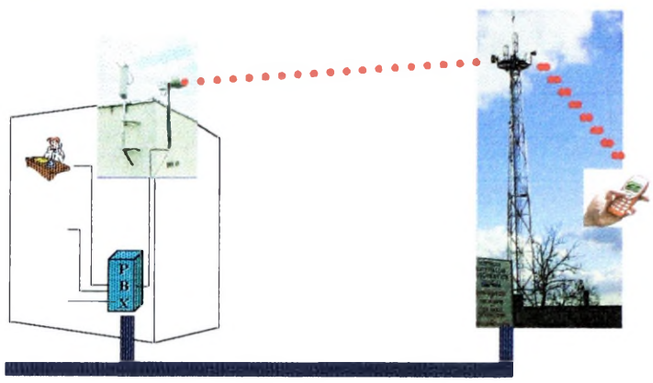
Tu operator Stacji Monitorowania odczytuje prędkość, stan czujników, datę i czas odczytu

W wyniku procedur lub na polecenie Policji operator Stacji może zdalnie zatrzymać pojazd

Redukcja kosztów telekomunikacyjnych

usługi „Bezpośredni dostęp do Sieci Era", „Bramka GSM"

- **Taryfikacja co 1 sekundę;**
- Dzwoniąc z telefonu stacjonarnego poruszamy się wyłącznie w Sieci Era;
- Usługa polega na połączeniu centrali abonenckiej klienta z siecią Era, dzięki czemu można zredukować koszty połączeń.



11

Propozycja dla dużych Instytucji

usługa „Firmowa sieć GSM"

„Firmowa sieć GSM" to wydzielona sieć GSM tworzona na terenie biur klienta, w której zarejestrowani użytkownicy mogą realizować połączenia pomiędzy sobą bezpłatnie.

- Darmowe połączenia lokalnych rozmów pomiędzy telefonami stacjonarnymi i komórkowymi;
- Efektywność komunikacji wewnątrz organizacji;
- Jeden standardowy aparat telefoniczny – aparat GSM;
- Najniższe koszty połączeń wychodzących;
- Profile użytkowników.

12

Szybki i bezpieczny dostęp do danych

usługi „EraInternet", „EraWAP", „dataVPN"

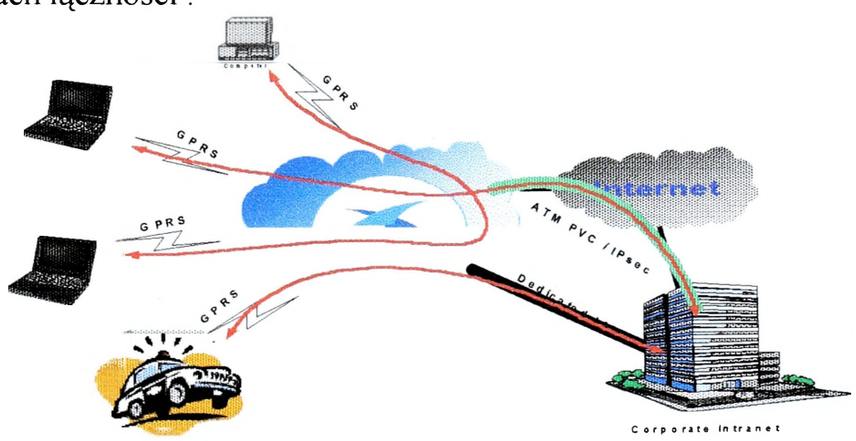
- Bezprzewodowy dostęp do sieci korporacyjnych (intranetów):
  - Transfer plików;
  - Dostęp do baz danych;
  - Synchronizacja danych osobistych;
  - Zdalna praca zespołowa.
- Szybki, bezprzewodowy dostęp do Internetu:
  - WWW, FTP;
  - Usługi WAP.
- Bezprzewodowa poczta elektroniczna;
- Płacimy tylko za faktycznie przesłane informacje.

13

Jak to działa

usługi „EraInternet", „EraWAP", „dataVPN"

Zadaniem systemu transmisji danych jest zapewnienie transmisji informacji pomiedzy komputerami mobilnymi a serwerem firmowym znajdujacym sie w centrach łączności .



14

Ci którzy nam zaufali
Lista wybranych klientów

- **Ministerstwo Spraw Wewnętrznych i Administracji**
- **Ministerstwo Sprawiedliwości**
- **Biuro Bezpieczeństwa Narodowego**
- **Centralny Węzeł Łączności MON**
- **Policja - Komenda Główna**
- **Urząd Ochrony Państwa**
- **Komenda Główna Państwowej Straży Pożarnej**
- **Główny Urząd Ceł i Generalny Urząd Celny**

- **Coca-Cola**
- **Nationale Nederlande**
- **Bank PeKaO S.A.**

15

era

BIZNES

SIEMENS
ZWUT Sp. z o.o.

ZWUT S.A.
& Siemens Company
Warszawa

Mariusz KARBOWSKI

NOWOCZESNE TECHNOLOGIE TELEKOMUNIKACYJNE W SYSTEMIE OBRONNOŚCI PAŃSTWA

CENTRUM KONFERENCYJNE WP Grudzień 2001

SIEMENS

Mariusz Karbowski

NOWOCZESNE TECHNOLOGIE KOMUNIKACYJNE W SYSTEMIE OBRONNOŚCI PAŃSTWA

Siemens Sp z o. o.

SIEMENS

ZWUT i Siemens

- 4 października 2001 – ZWUT Sp. z o.o. i Siemens Sp. z o.o. łączą się w jedną firmę – Siemens Sp. z o.o.
- Nowa struktura światowego koncernu Siemens w Polsce

SIEMENS

Siemens Sp. z o.o. w liczbach :

- Obrót grupy Siemens > 3 mld PLN
- Liczba zatrudnionych > 5 000

- Obrót Siemens I&C > 1,3 mld PLN
  Information&Communication 2000/2001
- Liczba zatrudnionych > 900

SIEMENS

Siemens Sp. z o.o. w liczbach :

Siemens I&C (dawniej ZWUT) jest największym dostawcą rozwiązań telekomunikacyjnych w Polsce

SIEMENS

Siemens – elementy oferty

- Telekomunikacja :
  - Szerokopasmowe systemy transportowe przewodowe i radiowe (TransXpress, WalkAir);
  - Konwergentne systemy komunikacyjne (Surpass, HiPath);
  - Rozwiązania specjalne (m.in. systemy dowodzenia);
- Inne branże (energetyka, medycyna, automatyka, transport, bezpieczeństwo teleinformatyczne, itd.).

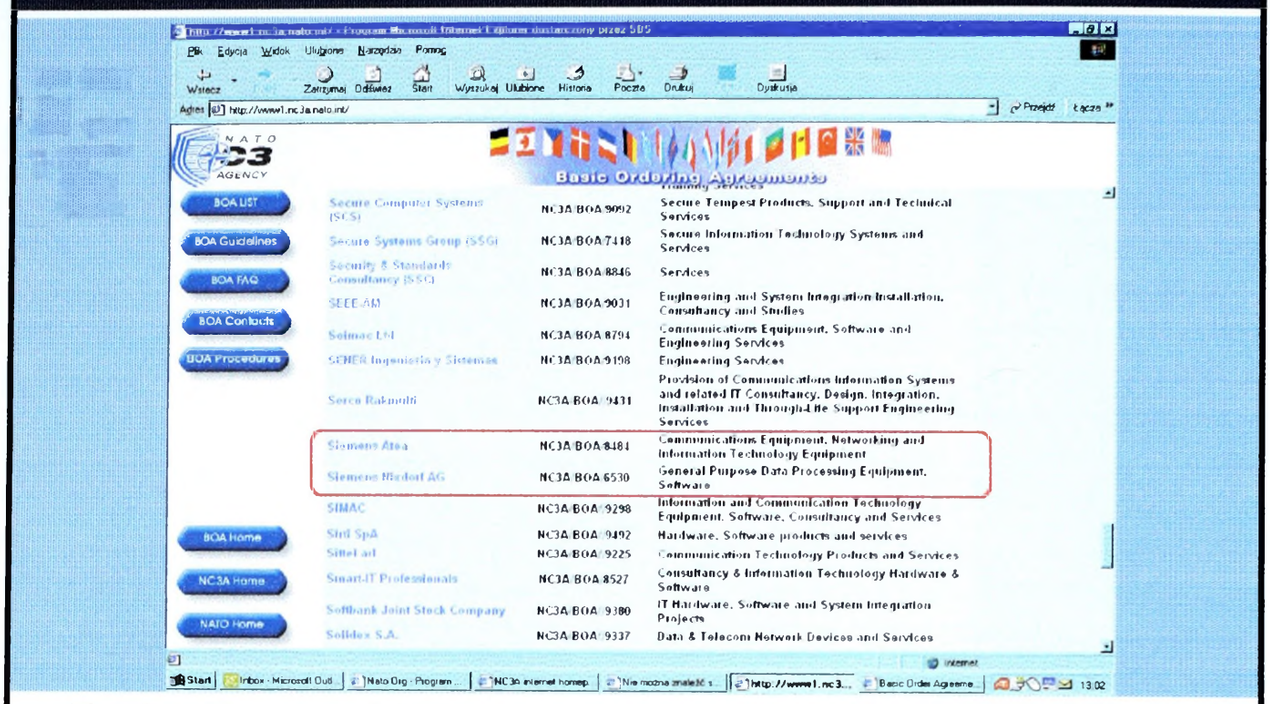
SIEMENS

Siemens – rzeczywistość

- NCN – NATO Core Network (25 węzłów Hicom 300E);
- Autoko 95, IBWW Bonn – Berlin, ...;
- Sieć telekomunikacyjna sił zbrojnych na Węgrzech;
- USAF Europe – system dowodzenia;
- i wiele, wiele innych ...

SIEMENS

Siemens dla NATO



SIEMENS

NOWOCZESNE TECHNOLOGIE KOMUNIKACYJNE

W SYSTEMIE OBRONNOŚCI PAŃSTWA

Siemens Sp. z o.o.

OPTIMUS S.A.
Warszawa

Marek Jan KALA

WSPOMAGANIE KIEROWANIA I DOWODZENIA OGNIWAMI POZAMILITARNYMI W SYSTEMIE OBRONNOŚCI PAŃSTWA

CENTRUM KONFERENCYJNE WP Grudzień 2001

Marek Jan KALA

OPTIMUS
znaczy najlepszy

KOMPUTERY I SERWERY

KONFERENCJA
KIEROWANIE OBRONNOŚCIĄ PAŃSTWA
PODCZAS STANÓW NADZWYCZAJNYCH Z WYKORZYSTANIEM
TECHNICZNYCH ŚRODKÓW NAJNOWSZEJ GENERACJI

Centrum Konferencyjne Wojska Polskiego
Warszawa – Grudzień 2001 r.

OPTIMUS

Strategia produktowa komputerów i serwerów OPTIMUS S.A.

rynek korporacyjny

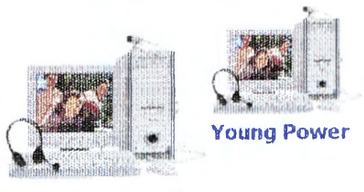
- **Dostarczanie rozwiązań informatycznych zapewniających wysoką jakość i kompleksowość obsługi klienta.**
- **Aktywne definiowanie i zaspakajanie indywidualnych potrzeb klienta:**
  - Oferta dopasowana do indywidualnych potrzeb i oczekiwań odbiorcy;
  - Produkty przygotowane pod specjalne zamówienie.
- **Umożliwianie odbiorcom rynku IT optymalne wykorzystanie zaawansowanych technologicznie rozwiązań:**
  - Wsparcie przedsprzedażne – współpraca przy tworzeniu rozwiązań dla klienta;
  - Instalacja - wdrażanie zaprojektowanych systemów u odbiorcy;
  - Sprzedaż realizowana z wartością dodaną (serwis, support).

OPTIMUS

WYSOKA JAKOŚĆ - NOWOCZESNOŚĆ - INNOWACYJNOŚĆ

Komputery Optimus - roadmapa

cena

Rynek konsumencki	Rynek SMB	Rynek korporacyjny
 Young Power Young Hypermedia  Young First	 Prestige Business Prestige Slim	Prestige VIP
- nowoczesność - bezpieczeństwo - przyjazny w obsłudze - atrakcyjna cena	- ekonomiczność - stabilność - nieprzerwany okres eksploatacji - bogaty zestaw opcji	- wydajność i nowoczesność - najwyższa jakość - zarządzalność - bezpieczeństwo - bogaty pakiet opcji w standardzie

GPTiMUS

NAJWYŻSZA JAKOŚĆ - NOWOCZESNOŚĆ - INNOWACYJNOŚĆ

Rynek korporacyjny

WYDAJNOŚĆ

Ekonomiczność
Długi okres eksploatacji
USB i audio z przodu
Łatwootwieralna obudowa
Możliwosc zamknięcia obudowy
Karta sieciowa w standardzie
2 lata gwarancji + atrakcyjne opcje serwisowe

Prestige Business

Wyjątkowo małe rozmiary (190x355x477)
Możliwość pracy pion/poziom
Wyjścia USB i audio z przodu obudowy
Wysoka stabilność
Niskie koszty eksploatacji
Atrakcyjne wzornictwo
Karta sieciowa w standardzie
2 lata gwarancji z czasem reakcji w opcji

Prestige Slim

Prestige VIP

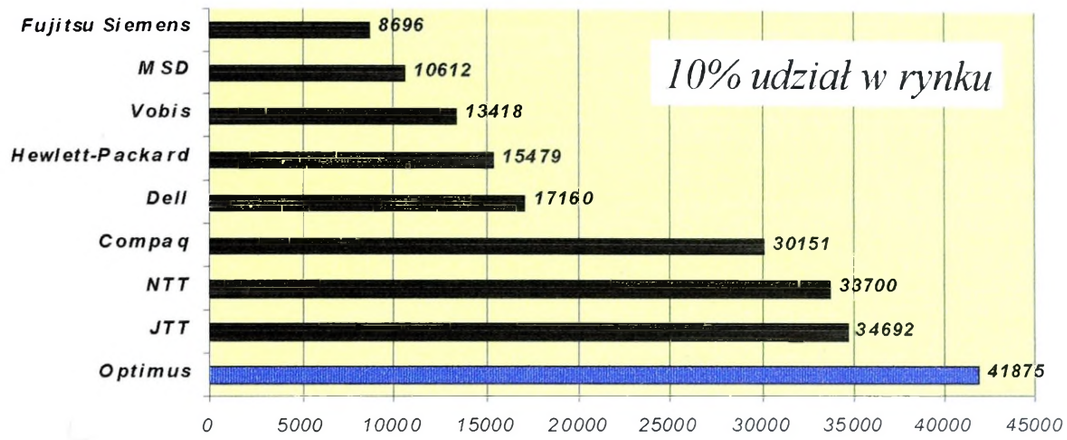
Najbardziej wydajne komputery w swojej klasie
Gwarancja dostępu do najnowszych technologii
USB i audio z przodu
Łatwootwieralna obudowa
Możliwość zamknięcia obudowy
Gwarancja rozbudowy
Najwyższa jakość i stabilność
Niskie koszty eksploatacji
Bogata lista referencji i certyfikatów
Karta sieciowa wysokiej klasy w standardzie
3 lata gwarancji z serwisem na miejscu, w opcji specjalne czasy reakcji
Oprogramowanie do zarządzania

TECHNOLOGIA
ZARZĄDZALNOŚĆ
WYPOSAŻENIE

GPTiMUS

Pozycja rynkowa na rynku PC

Sprzedaż stacjonarnych komputerów PC po 3 kw. 2001 (szt)



Od wielu lat Optimus jest niekwestionowanym liderem na rynku komputerowym w Polsce.

OPTIMUS NSERVER Roadmap

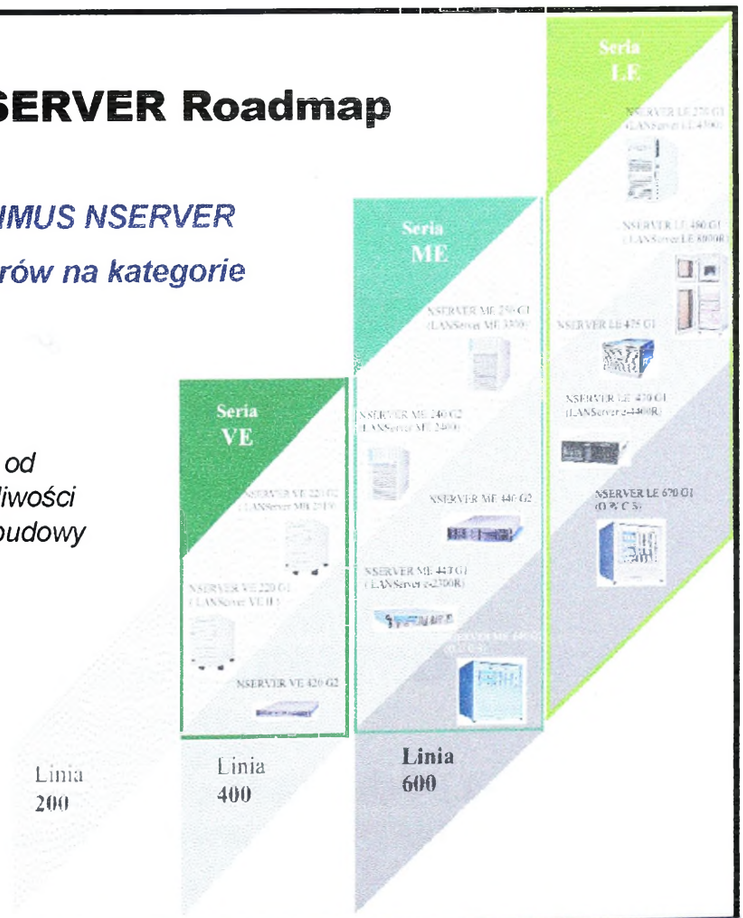
- *Nowa rodzina serwerów OPTIMUS NSERVER*
- *Nowe zasady podziału serwerów na kategorie*

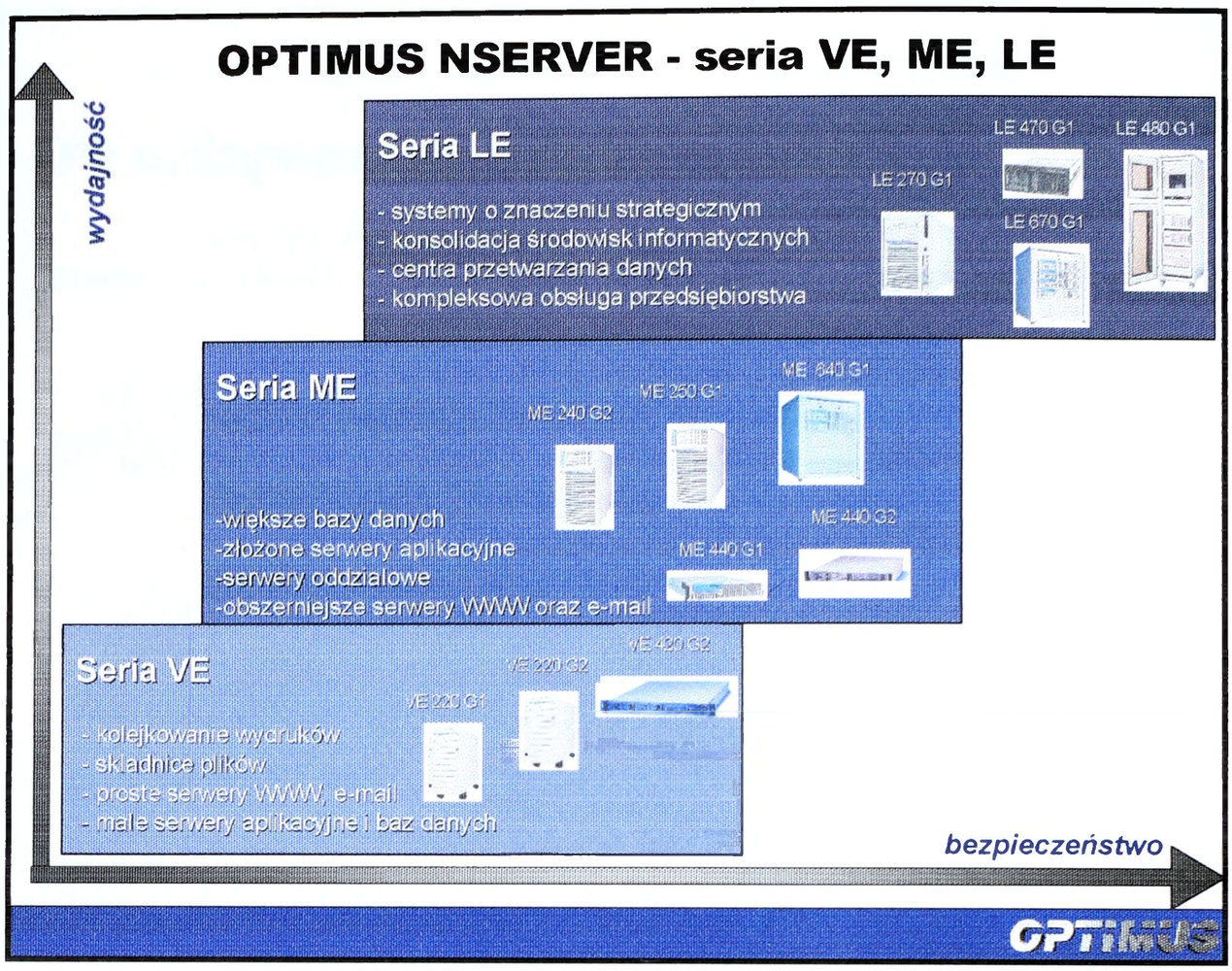
NSERVER serie VE, ME, LE

Przekrój oferty zapewniający wybór odpowiedniego serwera w zależności od zapotrzebowania środowiska na możliwości platformy w zakresie wydajności, rozbudowy jak również bezpieczeństwa.

NSERVER linie 200, 400, 600

Przekrój oferty dający możliwość prawidłowego doboru rozwiązania w zależności od typu zastosowania i rodzaju środowiska.




OPTIMUS NSERVER - seria VE, ME, LE
wydajność
Seria LE
- systemy o znaczeniu strategicznym
- konsolidacja środowisk informatycznych
- centra przetwarzania danych
- kompleksowa obsługa przedsiębiorstwa
LE 270 G1
LE 470 G1
LE 670 G1
LE 480 G1
Seria ME
-większe bazy danych
-złożone serwery aplikacyjne
-serwery oddziałowe
-obszerniejsze serwery WWW oraz e-mail
ME 240 G2
ME 250 G1
ME 640 G1
ME 440 G1
ME 440 G2
Seria VE
- kolejkowanie wydruków
- składnice plików
- proste serwery WWW, e-mail
- małe serwery aplikacyjne i baz danych
VE 220 G1
VE 220 G2
VE 420 G2
bezpieczeństwo
OPTIMUS


OPTIMUS
OPTIMUS Spółka Akcyjna
ul. Nawojowska 118
33-330 Nowy Sącz
tel.: +48 18 444 0 500, fax: +48 18 443 71 85
www.optimus.pl
OPTIMUS

Marek Jan KALA

OPTIMUS

znaczy najlepszy

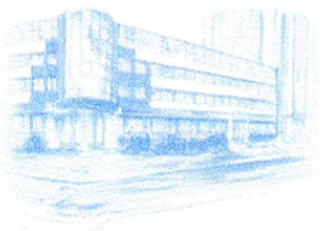
KONFERENCJA
KIEROWANIE OBRONNOŚCIĄ PAŃSTWA
PODCZAS STANÓW NADZWYCZAJNYCH Z WYKORZYSTANIEM
TECHNICZNYCH ŚRODKÓW NAJNOWSZEJ GENERACJI

Centrum Konferencyjne Wojska Polskiego
Warszawa – Grudzień 2001 r.

OPTIMUS ENTERPRISE

OPTIMUS

OPTIMUS



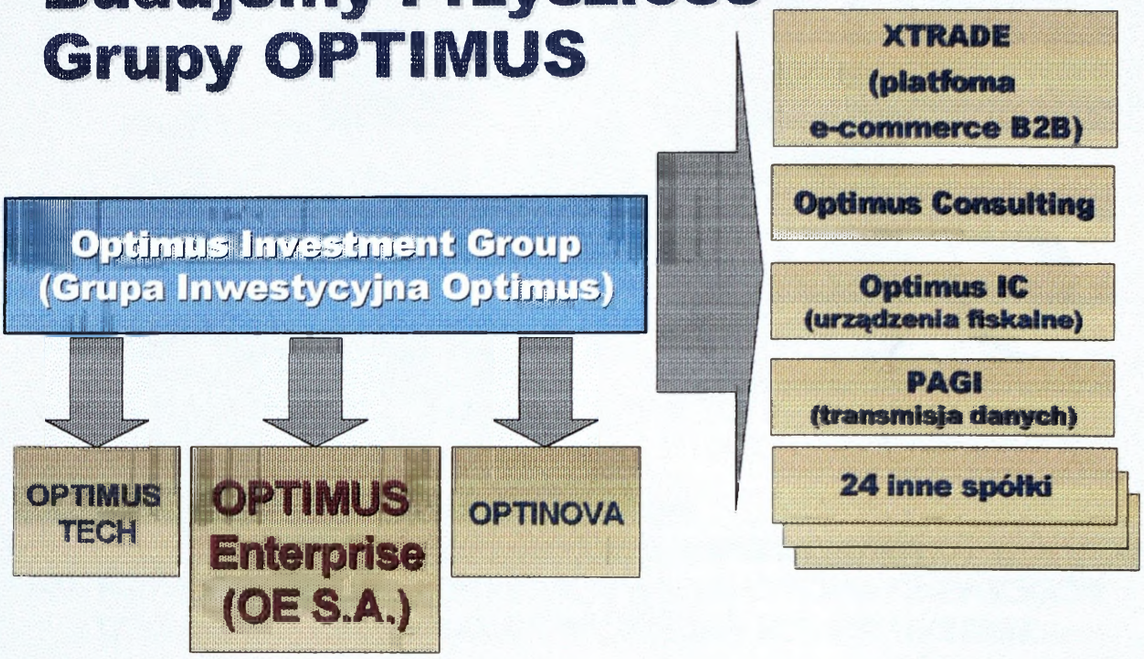
Grupa OPTIMUS

- **Największy producent PC w Europie Środkowo-Wschodniej**
  - prawie 1 mln sprzedanych PC (1988-2001)
- **Pierwsza spółka publiczna w sektorze IT (1994)**
- **Realizacja Projektu SWD dla Komendy Miejskiej Policji w Łodzi**
- **Kompetencje integracyjne skoncentrowane w OPTIMUS Enterprise S.A.**

OPTIMUS ENTERPRISE

OPTIMUS

Budujemy Przyszłość Grupy OPTIMUS



OPTIMUS ENTERPRISE

OPTIMUS

OPTIMUS Enterprise S.A.

Systemy Wspomagania Dowodzenia

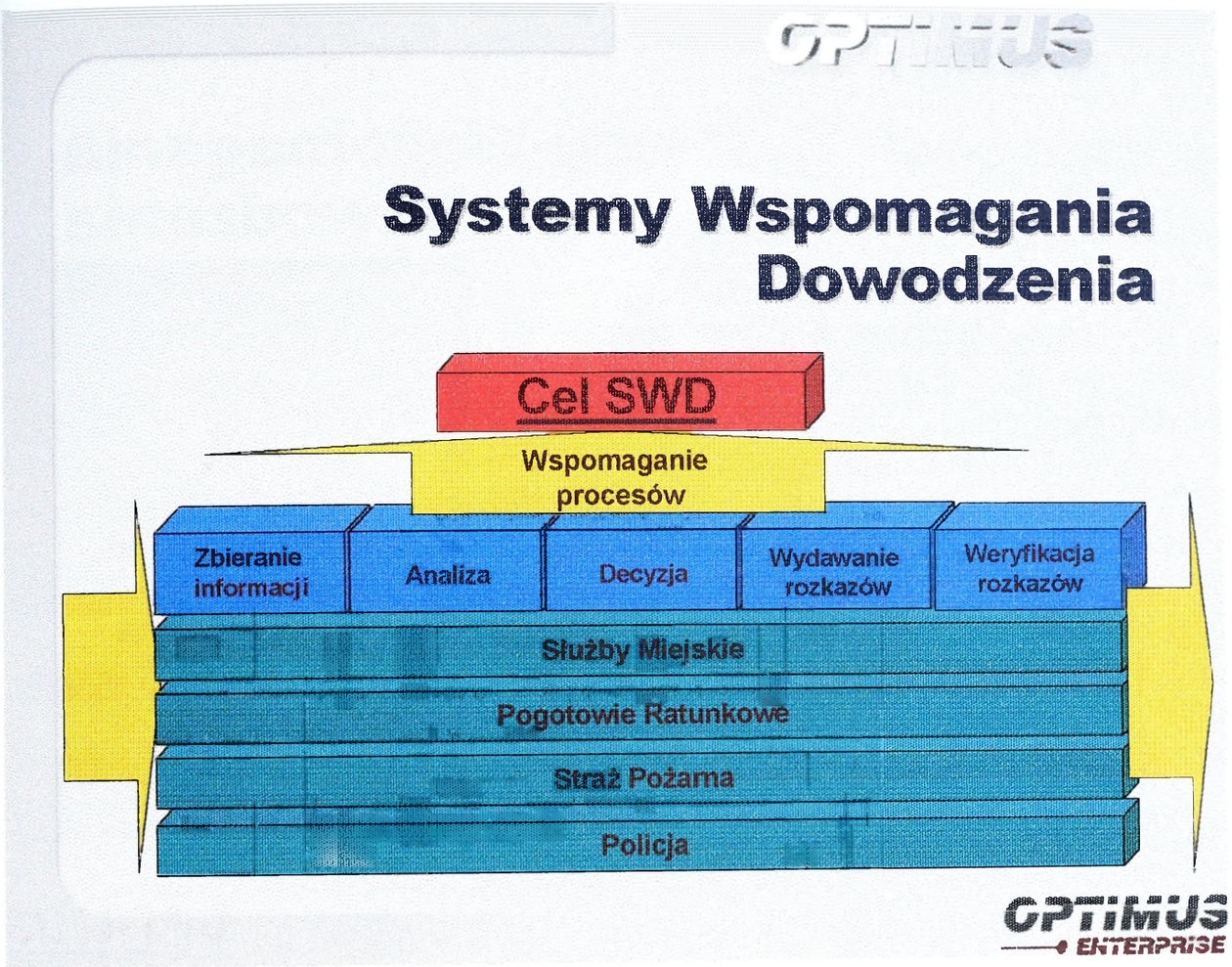
Rodzina Systemów Wspomagania i/lub Zarządzania

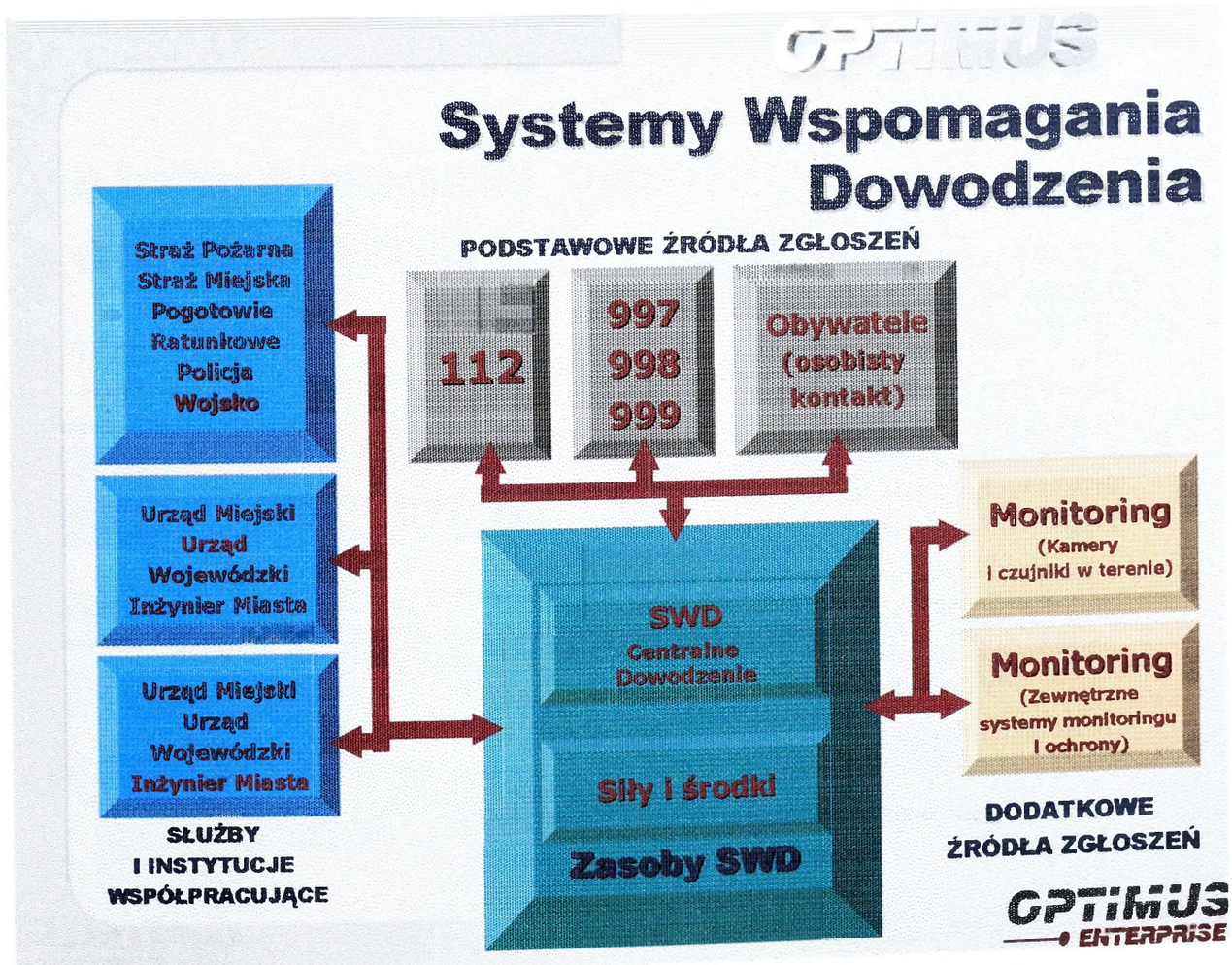
- dowodzenia
  - MSWiA (Policja, Straż pożarna, UOP);
- akcji ratowniczych
  - Centra Powiadamiania Ratunkowego (CPR);
- sytuacjami kryzysowymi
  - powiaty, miasta (ZSK).

oraz elementy SWD

- cyfrowe systemy łączności radiowej;
- śledzenie pojazdów;
- monitoring;
- systemy bezpieczeństwa (dostępowe i inne);
- i inne (np. podsystemy gwarantowanego zasilania).

OPTIMUS ENTERPRISE

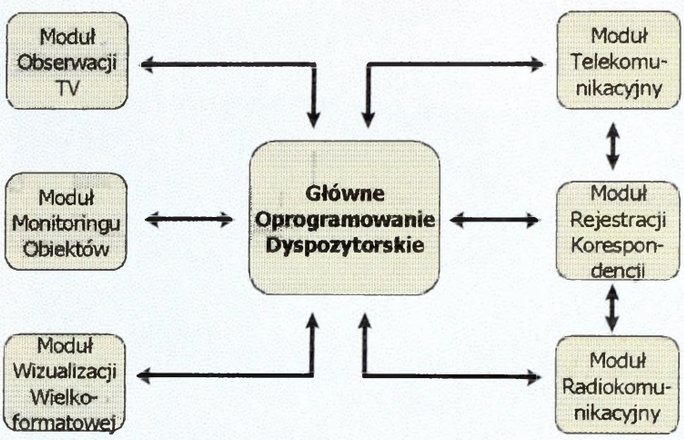

OPTIMUS
Systemy Wspomagania Dowodzenia
Cel SWD
Wspomaganie procesów
Zbieranie informacji
Analiza
Decyzja
Wydawanie rozkazów
Weryfikacja rozkazów
Służby Miejskie
Pogotowie Ratunkowe
Straż Pożarna
Policja
OPTIMUS ENTERPRISE

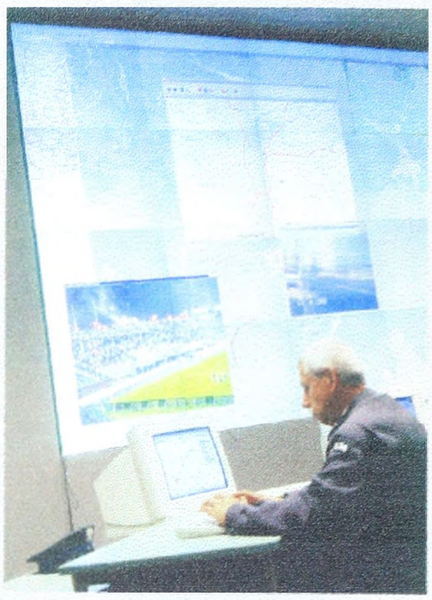

OPTIMUS
Systemy Wspomagania Dowodzenia
PODSTAWOWE ŹRÓDŁA ZGŁOSZEŃ
112
997
998
999
Obywatele (osobisty kontakt)
Straż Pożarna
Straż Miejska
Pogotowie Ratunkowe
Policja
Wojsko
Urząd Miejski
Urząd Wojewódzki
Inżynier Miasta
Urząd Miejski
Urząd Wojewódzki
Inżynier Miasta
SŁUŻBY I INSTYTUCJE WSPÓŁPRACUJĄCE
SWD
Centralne Dowodzenie
Siły i środki
Zasoby SWD
Monitoring (Kamery i czujniki w terenie)
Monitoring (Zewnętrzne systemy monitoringu i ochrony)
DODATKOWE ŹRÓDŁA ZGŁOSZEŃ
OPTIMUS ENTERPRISE

OPTIMUS

Systemy Wspomagania Dowodzenia

Podsystemy SWD
Przykładowa Architektura *





* Wykorzystano zdjęcie realizowanego przez OPTIMUS S.A. SWD dla KWP w Łodzi.

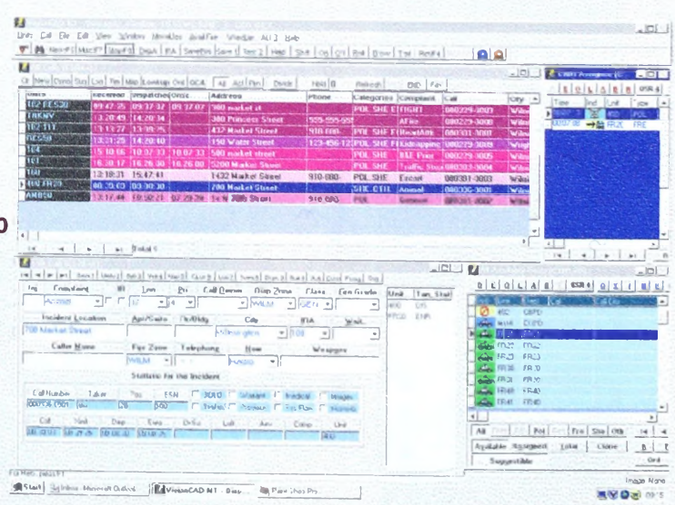
OPTIMUS ENTERPRISE

OPTIMUS

Systemy Wspomagania Dowodzenia

Główne Oprogramowanie Dyspozytorskie

- dostarcza wyselekcjonowane i niezbędne informacje; o zasobach (ludzie, samochody, środki techniczne), ich statusie (czym się zajmują), położeniu, itp
- umożliwia błyskawiczne podjęcie decyzji;
- podpowiada rozwiązania i schematy postępowania;
- dostarcza informacji o zagrożeniach;
- w miarę użytkowania rozszerza swoją wiedzę.



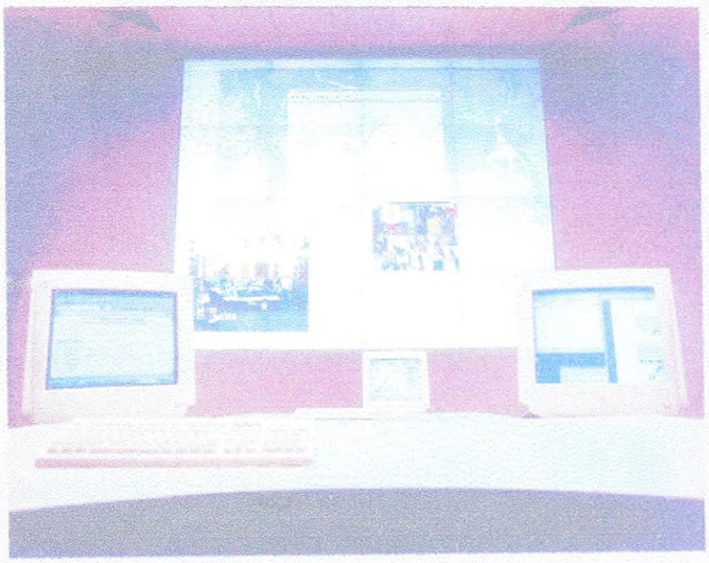
OPTIMUS ENTERPRISE

OPTIMUS

Systemy Wspomagania Dowodzenia

Moduł Wizualizacji Wielkoformatowej*

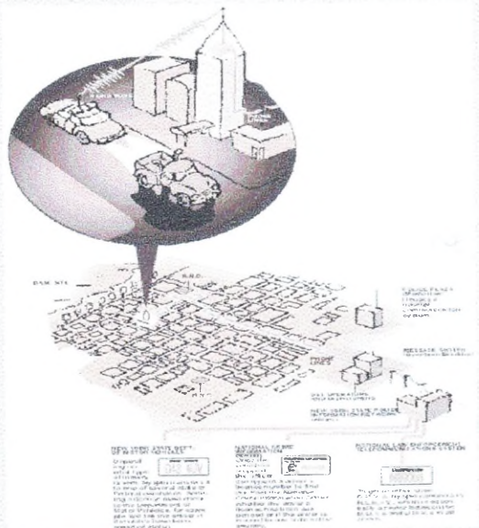
- wizualizacja dostępnych sił i środków w czasie rzeczywistym;
- graficzna informacje o statusie zasobów;
- wizualizacje przekrojowych informacji o infrastrukturze;
- obserwacja miejsca zdarzenia.



* Wykorzystano zdjęcie realizowanego przez OPTIMUS S.A. SWD dla KWP w Łodzi.

OPTIMUS ENTERPRISE

OPTIMUS



Systemy Wspomagania Dowodzenia

Moduł Radiokomunikacyjny

- zapewnia szyfrowaną łączność głosową oraz przesyłanie danych;
- zapewnia komunikację pomiędzy terminalem w terenie (w samochodzie) i Centrum Dowodzenia.

OPTIMUS ENTERPRISE

OPTIMUS

Systemy Wspomagania Dowodzenia

ratują istnienia ludzkie zmniejszają straty majątkowe

- szybsza reakcja na wezwanie (x20);
- zwiększenie efektywności codziennych działań;
- efektywna wymiana informacji;
- lepsza możliwość śledzenia i kierowania rozwojem sytuacji;
- podejmowanie trafniejszych decyzji.

OPTIMUS ENTERPRISE

OPTIMUS

OPTIMUS

OPTIMUS ENTERPRISE
Spółka Akcyjna

OPTIMUS ENTERPRISE

TEL-ENERGO S.A.
Warszawa

Michał SOBOLEWSKI

USŁUGI OGÓLNOPOLSKIEJ SIECI TELEENERGETYCZNEJ NA RZECZ OBRONNOŚCI KRAJU

CENTRUM KONFERENCYJNE WP Grudzień 2001

TEL-ENERGO SA

Możliwości zapewnienia usług w ogólnopolskiej sieci światłowodowej TEL-ENERGO na rzecz obronności państwa

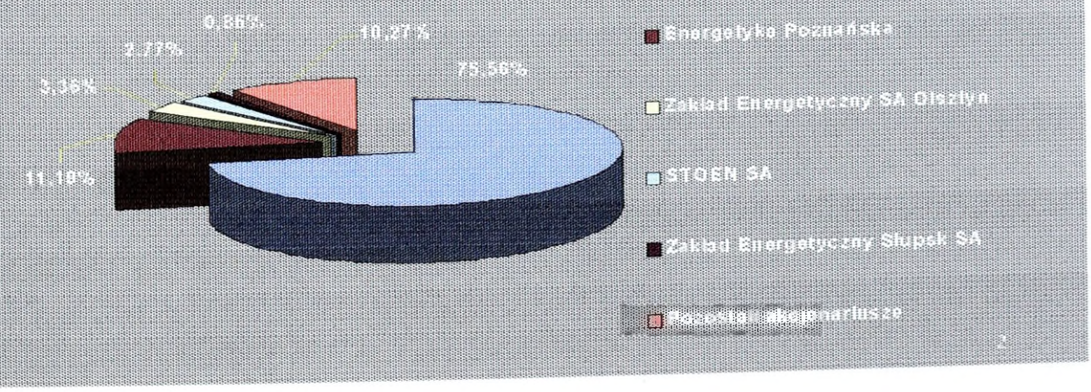
Warszawa, 19 grudnia 2001 r.

TEL-ENERGO SA

TEL-ENERGO SA powstało w 1993 r.
Założycielami są firmy zajmujące się przesyłem i dystrybucją energii elektrycznej i cieplnej - Polskie Sieci Elektroenergetyczne SA, 31 Spółek Dystrybucyjnych oraz Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej.

Jest firma o 100% udziale kapitału polskiego.

Akcjonariusze TEL-ENERGO



TEL-ENERGO SA

TEL-ENERGO dąży do osiągnięcia pozycji telekomunikacyjnego operatora pierwszego wyboru poprzez:

- sprawne zaspokajanie rosnących potrzeb klientów;
- zapewnienie nieograniczonego dostępu do globalnego rynku informacji;
- zapewnienie bezpieczeństwa i niezawodności sieci;
- oferowanie konkurencyjnych rozwiązań;
- rzetelne doradztwo.

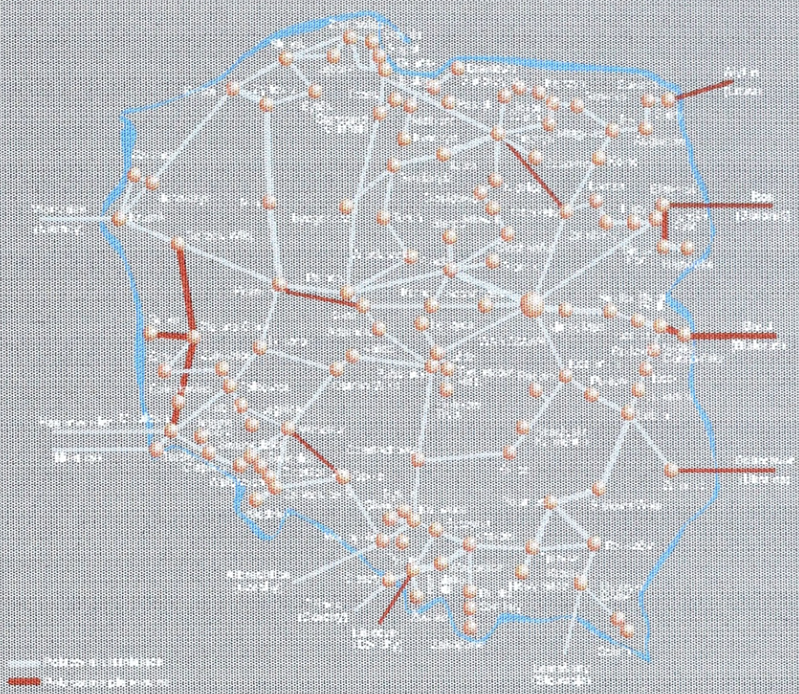
TEL-ENERGO SA

Sieć telekomunikacyjna TEL-ENERGO

- sieć światłowodowa o długości ponad 10 000 km;
- struktura pierścieniowa SDH;
- urządzenia STM-1, STM-4, STM-16;
- technologia DWDM.

TEL-ENERGO SA

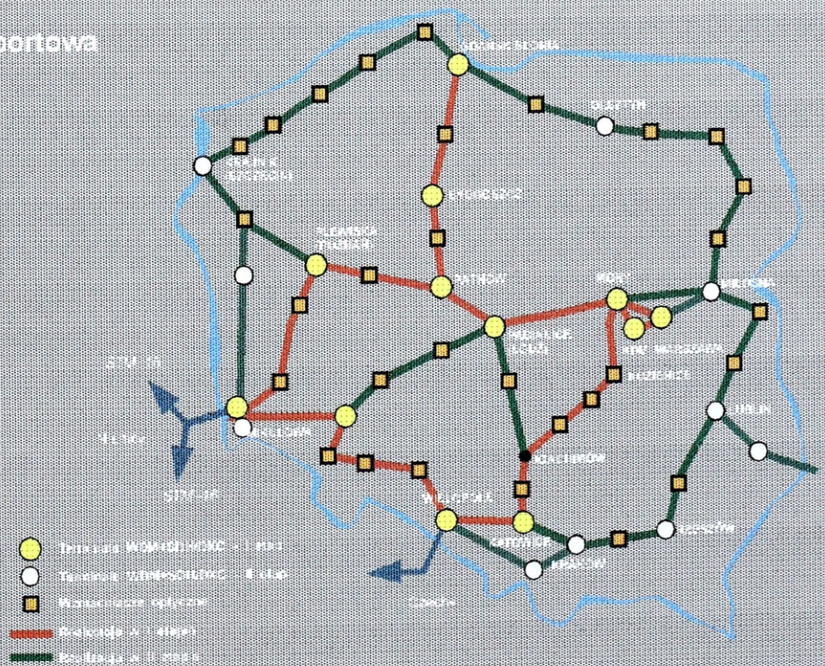
Światłowodowa sieć TEL-ENERGO

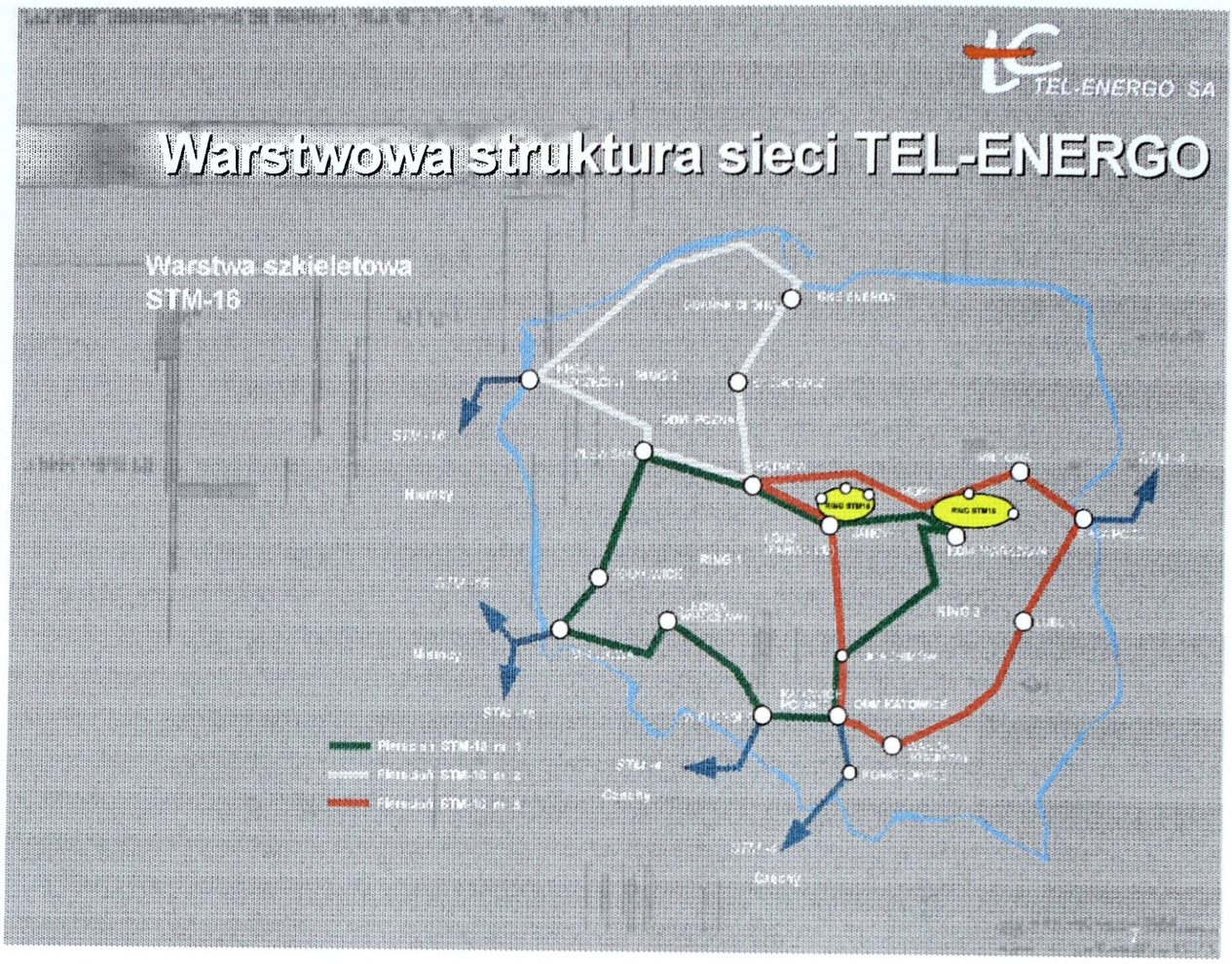


TEL-ENERGO SA

Warstwowa struktura sieci TEL-ENERGO

Warstwa transportowa
DWDM+DXC




TEL-ENERGO SA
Warstwowa struktura sieci TEL-ENERGO
Warstwa szkieletowa
STM-16
RING STM16
RING STM16
RING 1
RING 2
STM-16
STM-4
Katowice
Gliwice
Opole
Wrocław
Poznań
Zielona Góra
Łódź
Włocławek
Gdańsk
Olsztyn
Białystok
Lublin
Rzeszów
Kielce
Warszawa
Płock
Radom
Pierścień STM-16 nr 1
Pierścień STM-16 nr 2
Pierścień STM-16 nr 3


TEL-ENERGO SA
Warstwowa struktura sieci TEL-ENERGO
Warstwa regionalna
STM-4
Katowice
Gliwice
Opole
Wrocław
Poznań
Zielona Góra
Łódź
Włocławek
Gdańsk
Olsztyn
Białystok
Lublin
Rzeszów
Kielce
Warszawa
Płock
Radom

TEL-ENERGO SA

Cechy sieci telekomunikacyjnej TEL-ENERGO

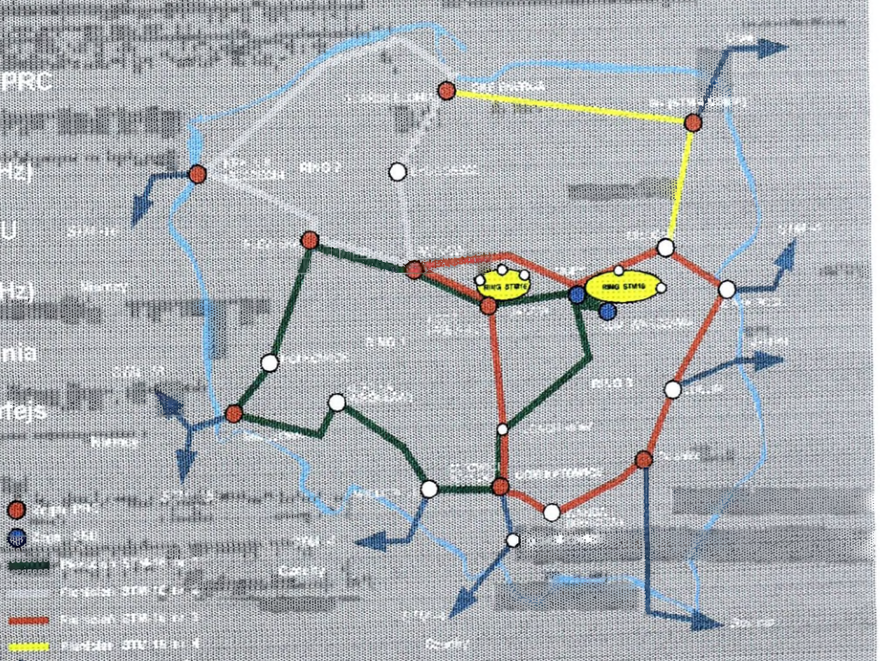
- szybkie zestawianie dróg;
- ciągły nadzór i monitorowanie jakości transmisji;
- szybka rekonfiguracja w przypadku awarii;
- optymalne wykorzystanie przepustowości transmisji;
- możliwość współpracy z różnymi systemami teletransmisyjnymi;
- wysoka niezawodność i bezpieczeństwo przekazywanych informacji;
- zgodność z zaleceniami ITU-T.

TEL-ENERGO SA

Synchronizacja w sieci TEL-ENERGO

Topologia sieci

- 2 główne zegary PRC wyposażone we wzorce cezowe (klasy $1 \cdot 10^{-12}$ Hz/Hz)
- 9 zegarów podrzędnych SSU (SASE) (klasy $1 \cdot 10^{-11}$ Hz/Hz)
- odbiorniki GPS
- system zarządzania SYNC VIEW (dodatkowy interfejs SNMP)



TEL-ENERGO SA

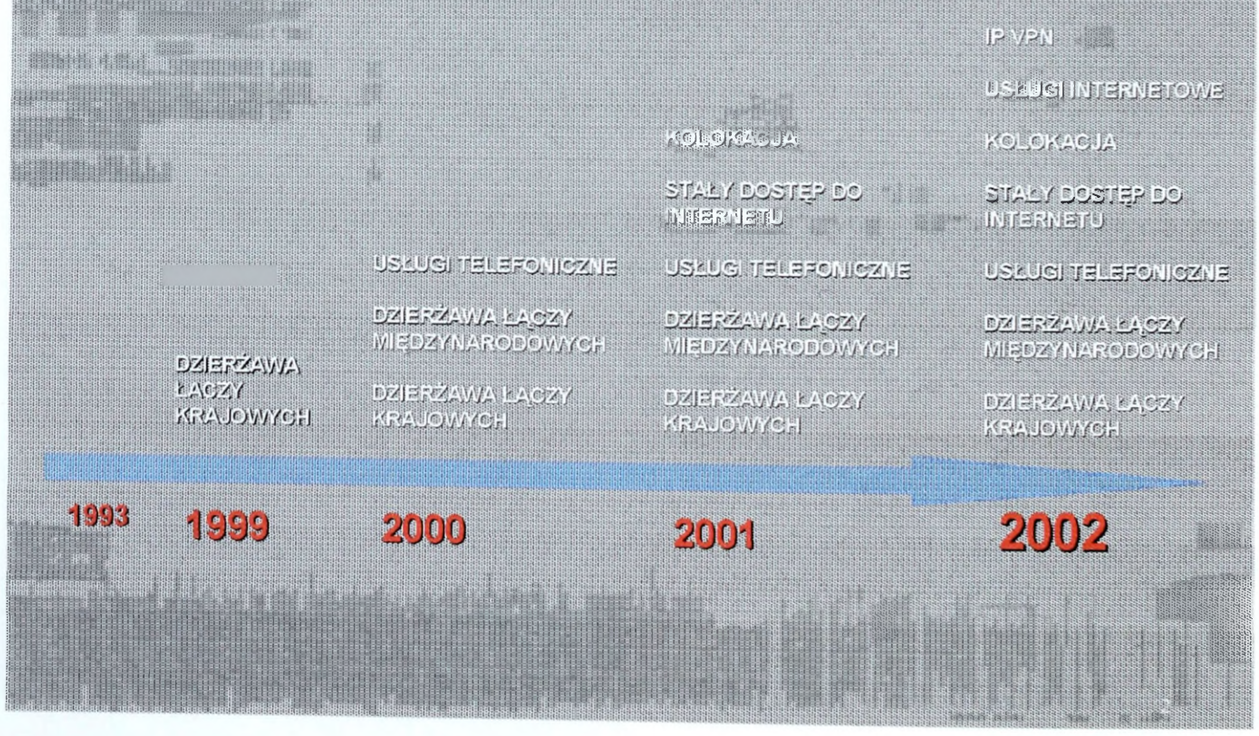
Synchronizacja sieci TEL-ENERGO

Zasady:

- wszystkie źródła wtórne synchronizowane z zegara PRC;
- PRC koordynowany z uniwersalną skalą czasu UTC;
- SSU wyposażone w odbiorniki GPS;
- dystrybucja sygnałów synchronizacyjnych poprzez urządzenia SDH;
- dwie drogi (podstawowa i zapasowa) do każdego węzła;
- współpraca z sieciami innych operatorów na zasadach plezjochronicznych.

TEL-ENERGO SA

Rozwój portfela usług



TEL-ENERGO SA

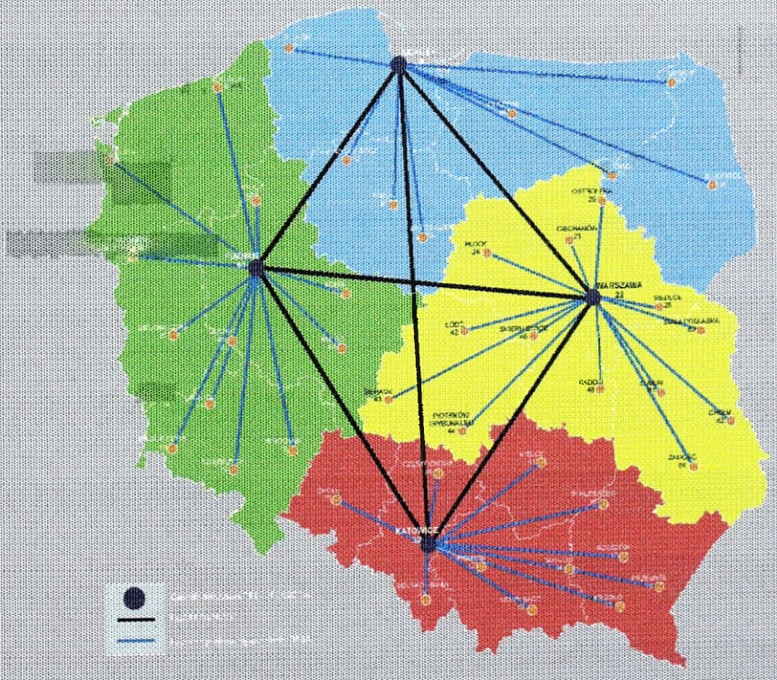
Dzierżawa łączy krajowych i międzynarodowych

Cechy usługi:

- połączenia wewnątrzsieciowe
- kompleksowe rozwiązania do punktu określonego przez klienta lub do punktu dostępu do sieci (PDS);
- instalacja i obsługa urządzeń transmisyjnych do punktów końcowych znajdujących się po stronie użytkownika;
- możliwość wyboru różnych parametrów usługi i dokonywania późniejszych modyfikacji;
- w przypadku awarii drogi podstawowej funkcje sieciowe zapewniają przesyłanie danych drogami zastępczymi eliminując przerwy w komunikacji.

TEL-ENERGO SA

Sieć telefoniczna TEL-ENERGO



TEL-ENERGO SA

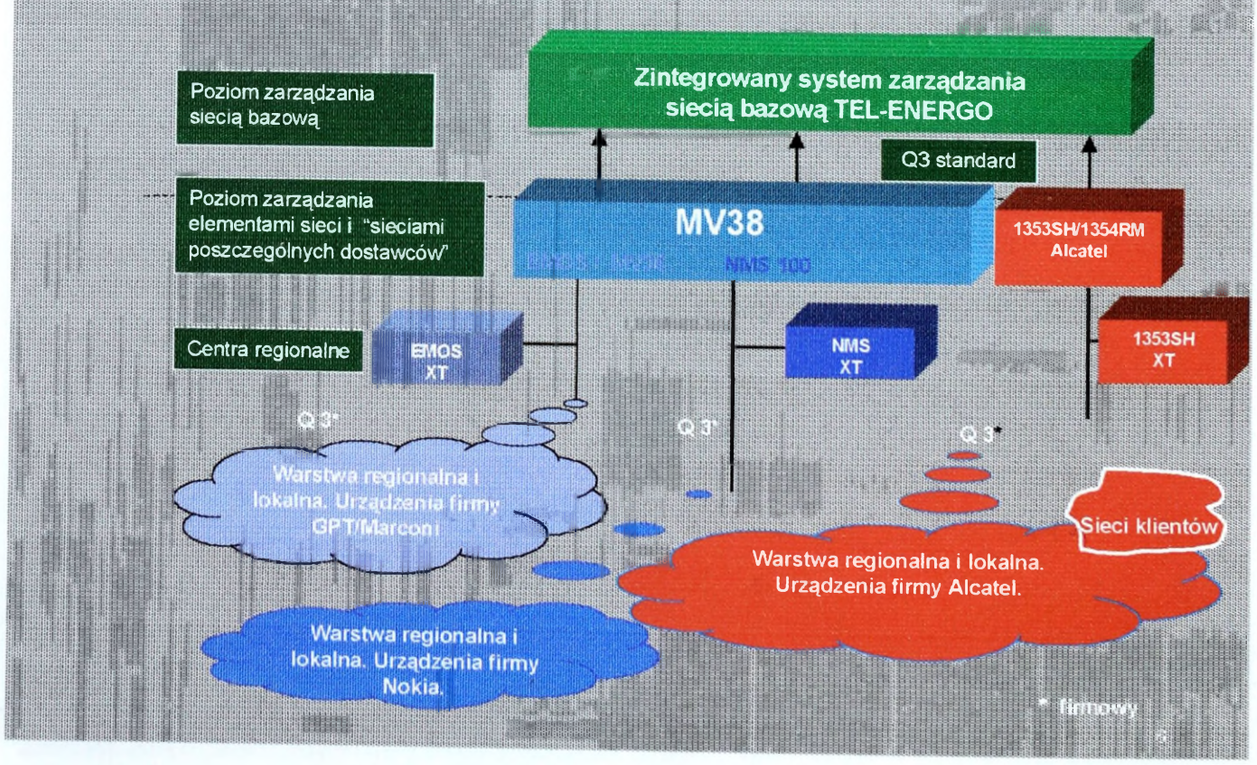
Zarządzanie siecią TEL-ENERGO

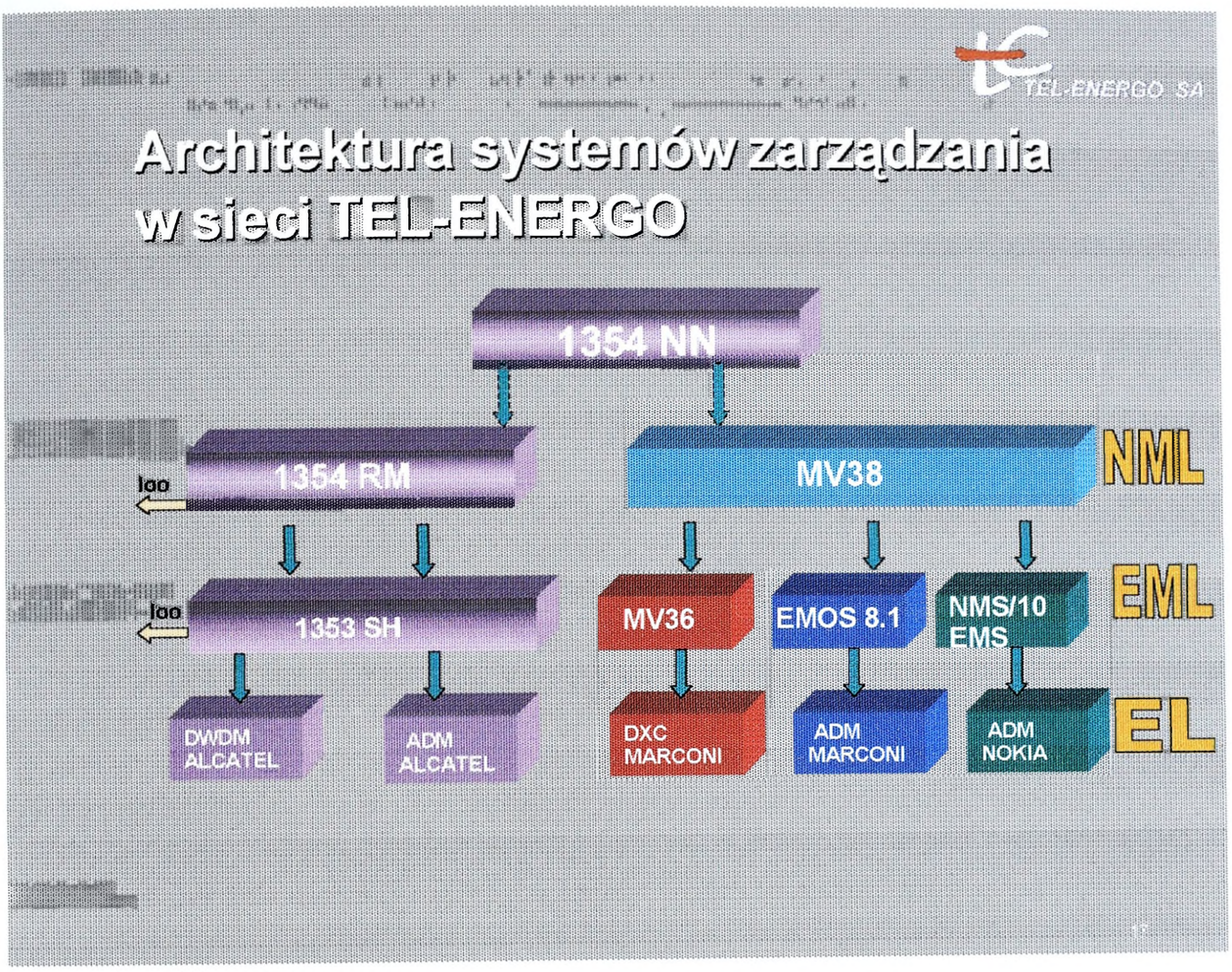
Zarządzanie centralne (CZST Warszawa):

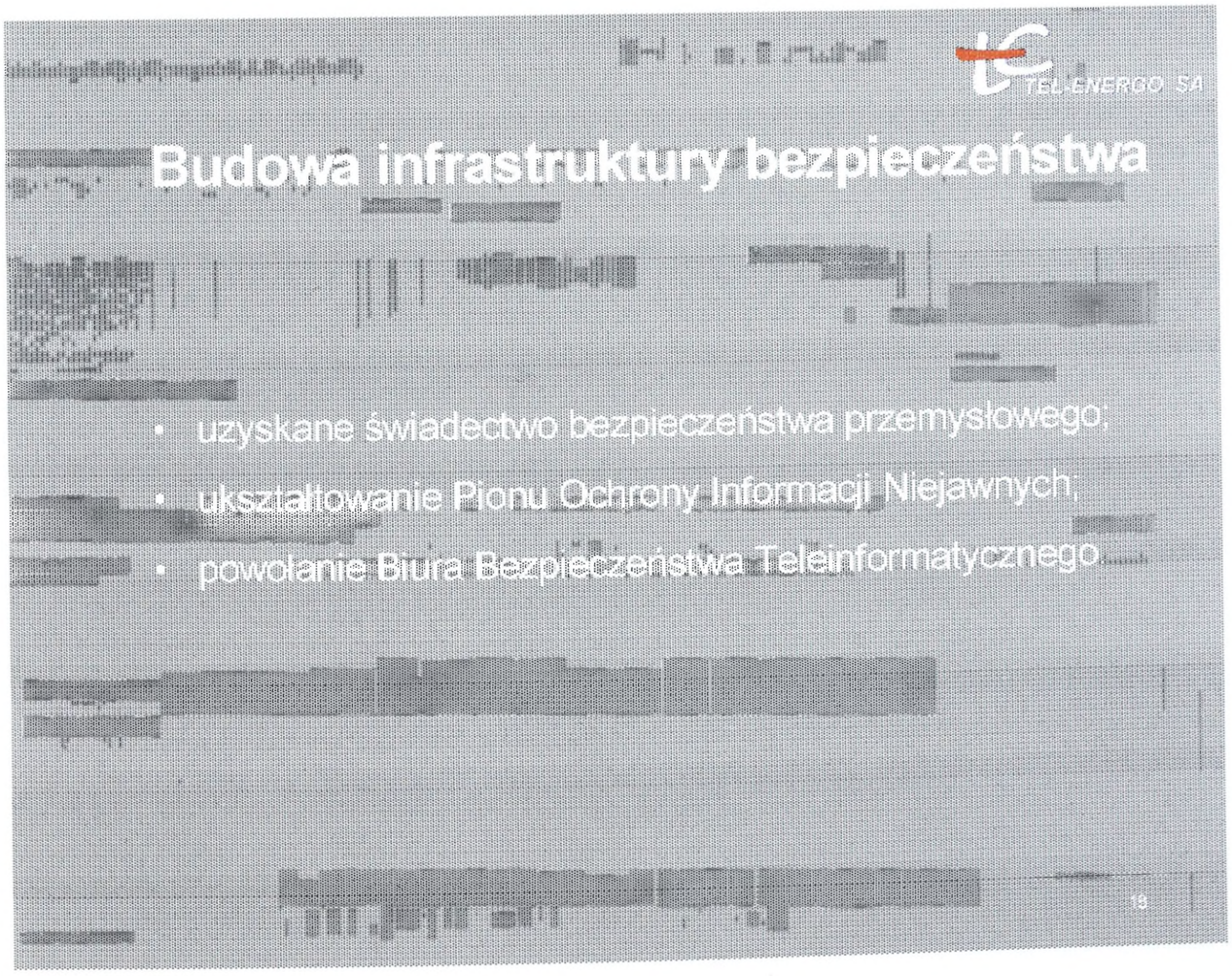
- konfiguracja nowych elementów sieciowych;
- zestawianie i zabezpieczanie ścieżek telekomunikacyjnych;
- graficzna prezentacja topologii sieci bazowej;
- automatyczne znajdowanie ścieżek i dróg zapasowych;
- tworzenie raportów o uszkodzeniach;
- automatyczne przełączanie na drogi rezerwowe;
- kontrola jakości połączeń;
- ograniczenie dostępu przez nadawanie klas uprawnień.

TEL-ENERGO SA

Struktura systemu zarządzania




TEL-ENERGO SA
Architektura systemów zarządzania w sieci TEL-ENERGO
1354 NN
1354 RM
Iao
MV38
NML
Iao
1353 SH
MV36
EMOS 8.1
NMS/10 EMS
EML
DWDM ALCATEL
ADM ALCATEL
DXC MARCONI
ADM MARCONI
ADM NOKIA
EL


TEL-ENERGO SA
Budowa infrastruktury bezpieczeństwa
• uzyskane świadectwo bezpieczeństwa przemysłowego;
• ukształtowanie Pionu Ochrony Informacji Niejawnych;
• powołanie Biura Bezpieczeństwa Teleinformatycznego.

TEL-ENERGO SA

Zadania
Biura Bezpieczeństwa Teleinformatycznego

Zapewnienie właściwego poziomu bezpieczeństwa świadczonych usług w zakresie:

- dzierżawy kanałów telekomunikacyjnych;
- usług telefonicznych w sieci 0-27;
- kolokacji;
- transmisji danych w rozwijanej aktualnie sieci IP (z zastosowaniem kryptografii oraz wykorzystaniem infrastruktury klucza publicznego).

Koordynacja polityki Spółki w zakresie bezpieczeństwa sieci telekomunikacyjnych oraz zapewnienia ciągłości świadczonych usług.

Cd...

TEL-ENERGO SA

Zadania
Biura Bezpieczeństwa Teleinformatycznego wynikające z ustawy Prawo Telekomunikacyjne

- koordynacja polityki Spółki w zakresie zabezpieczenia urządzeń i sieci telekomunikacyjnych oraz zbiorów danych przed ujawnieniem;
- planowanie i koordynacja działań Spółki w sytuacjach szczególnych zagrożeń (art. 64) oraz wykonywanie zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego (art. 40 oraz przepisy odrębne).

TT INVENTEL S.A.
Warszawa

Piotr KUREK

SYSTEMY OCHRONY OBWODOWEJ W SYSTEMIE OBRONNOŚCI RP

CENTRUM KONFERENCYJNE WP Grudzień 2001

Problem ochrony danego terenu towarzyszy ludzkości od początku jej istnienia. Wraz z rozwojem nowych technologii wojskowych powstawały nowe generacje systemów ochrony obwodowej mające zabezpieczać dany teren przed ingerencją obcych osób. W ten sposób możemy obserwować rozwój systemów ochrony obwodowej począwszy od wilczych dołów i zapadni poprzez mury obronne a skończywszy na specjalizowanych konstrukcjach opartych o czujniki pojemnościowe, akustyczne, termiczne, laserowe czy w ostatnich czasach światłowodowe.

Czujniki światłowodowe posiadają wiele zalet w stosunku do czujników tradycyjnych, pozwalają one zastosować czujniki światłowodowe między innymi w takich warunkach, w których czujniki tradycyjne nie mogłyby być zastosowane.

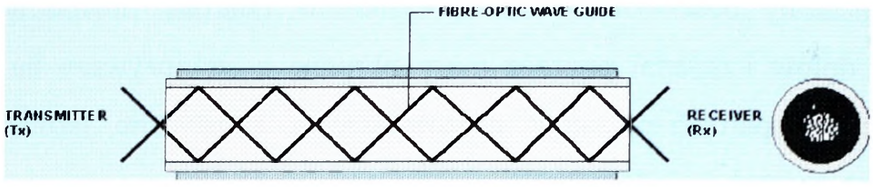
Do najważniejszych zalet czujników światłowodowych w systemach bezpieczeństwa zaliczamy:

1. Możliwość ich prawidłowej pracy przy dużych poziomach zakłóceń elektromagnetycznych i elektrostatycznych, niewrażliwość na trudne warunki meteorologiczne, takie jak deszcz, grad, śnieg, wiatr czy wyładowania atmosferyczne.
2. Posiadanie dużego stopnia bezpieczeństwa związanego z przenoszeniem ładunku elektrycznego – nie występuje zjawisko iskrzenia, można je zatem stosować w strefach niebezpiecznych, np.: składach amunicji, magazynach materiałów wybuchowych oraz w strefach o wysokim prawdopodobieństwie wystąpienia otwartego ognia czy wybuchu.
3. Duża odporność na próby ominięcia przez intruza – niemożliwe jest „mostkowanie" kabla światłowodowego w taki sposób, żeby nie zostać zauważonym przez system.
4. Nieznaczną ilość fałszywych alarmów spowodowanych zwierzętami, ruszającymi się drzewami, przechodniami czy złą pogodą.
5. Możliwość dostosowania geometrii czujnika do różnych wymagań i warunków.

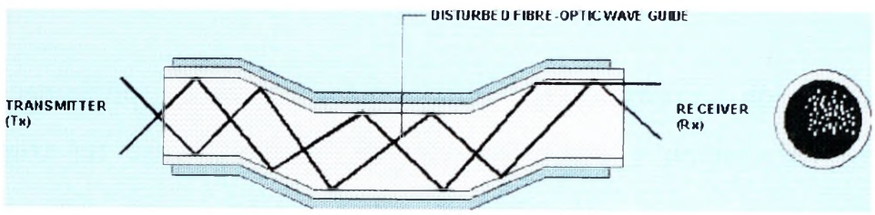
Konstrukcje tego typu czujników światłowodowych najczęściej są tworzone na bazie światłowodów wielomodowych zasilanych diodą elektroluminescencyjną lub laserem.

Wykorzystywane są znane zjawiska fizyczne polegające na wycieku modów rdzeniowych do płaszcza i później na zewnątrz pod wpływem zgięcia światłowodu w przypadku zasilania światłowodu diodą elektroluminescencyjną lub zmiany położenia

obrazu interferencyjnego tworzonego na powierzchni odbiornika (fotodiody) w przypadku zasilania laserem. Zjawiska te są przedstawione na rysunku 1a i 1b.



Rys.1a. Zjawisko wycieku modów rdzeniowych pod wpływem zgięcia światłowodu



Rys. 1b. Zjawisko zmiany obrazu interferencyjnego na powierzchni fotodiody pod wpływem zgięcia światłowodu

Systemy budowane w oparciu o światłowód:

1. Siatka światłowodowa – działa jak detektor wtargnięcia intruza na strzeżony teren, zarówno w razie jej przecięcia jak i próby przejścia nad nią lub pod nią. Alarm jest generowany tylko w przypadku bezpośredniego fizycznego ataku. Charakteryzuje się wysokim stopniem bezpieczeństwa, wolnego od fałszywych alarmów.

2. Krata światłowodowa – działa jak detektor wtargnięcia intruza do strzeżonego obiektu, zarówno w razie jej przecięcia jak i próby jej wyrwania. Jest uproszczoną wersją siatki światłowodowej.

3. Światłowodowy kabel czujnikowy – jest detektorem wtargnięcia intruza na strzeżony teren. Stosowane są wielomodowe kable światłowodowe o specjalnych konstrukcjach, posiadające dodatkowe elementy pokrycia wtórnego wzmacniające efekt zmiany obrazu interferencyjnego na powierzchni odbiornika. Wtórne pokrycie może być wykonane z twardego elastomeru lub nałożonych na włókno światłowodowe odpowiedniego kształtu i długości cylindrów z PCV.

Wymienione wyżej światłowodowe elementy umożliwiają dopasowanie się do istniejących lub stworzenie nowych barier obwodowych, takich jak bramy, drzwi, ściany, ogrodzenia siatkowe, drut kolczasty, ogniwa łańcuchowe, itp. Można je wbudować w dowolną strukturę co umożliwia wykrycie wtargnięcia do chronionego obiektu przez nawiercenie lub zburzenie ściany czy stropu.

Sygnały optyczne odebrane z czujników światłowodowych są przetwarzane na sygnał elektryczny odbierany przez standardowy komputer w centrum nadzoru.

PORÓWNANIE ZEWNĘTRZNYCH SYSTEMÓW WYKRYWANIA WTARGNIĘCIA NA STRZEŻONY TEREN

Właściwości systemu	Światłowodowy system ochrony obwodowej	Detektory drgań i przewody akustyczne	Naprężone kable	Bariery podczerwieni oraz laserowe
Tryb pracy czujnika	Siatka światłowodowa, światłowodowy kabel czujnikowy	Wibracyjny, akustyczny	Naprężone kable	Bariera stworzona przez światło podczerwone lub laserowe w wolnej przestrzeni
Prawdopodobieństwo wykrycia intruza	99,9% prawdopodobieństwo wykrycia wszystkich prób wejścia na teren strzeżony lub przecięcia kabla	Niska skuteczność wykrycia intruza w przypadku zastosowania: a) specjalnych szczypiec do cięcia drutu, b) spawarki, c) wspięcia się na płot po drabinie.	Stosunkowo dobra skuteczność wykrycia próby wejścia na teren strzeżony	Niska skuteczność wykrycia intruza w przypadku zastosowania odpowiedniej konfiguracji luster
Ilość fałszywych alarmów	Nieznaczna ilość fałszywych alarmów, mniej niż jeden fałszywy alarm na 1km rocznie. Alarm jest generowany tylko w przypadku bezpośredniego fizycznego ataku.	Spora ilość fałszywych alarmów spowodowanych złą pogodą, np.: deszczem, burzą gradową, a także warunkami środowiskowymi: fałszywe alarmy powodują przechodnie, duże i małe zwierzęta, ruszające się drzewa, itd.	Mniej niż jeden fałszywy alarm na 1 km miesięcznie. Niska ilość fałszywych alarmów tylko wtedy gdy przewody są dobrze naciągnięte. Zmiany temperatury i ruchy słupków ogrodzenia wpływają na naprężenie przewodów co znacznie wpływa na zwiększenie współczynnika ilości fałszywych alarmów	Spora ilość fałszywych alarmów spowodowanych złą pogodą, np.: mgłą, silnym deszczem, burzą gradową, a także warunkami środowiskowymi: fałszywe alarmy powodują przechodnie, duże i małe zwierzęta, ptaki, itd.
Podatność na ingerencję intruza w system	System całkowicie odporny na próby niezauważonego przekroczenia ogrodzenia, mostkowania przewodów lub ich zwarcia, mechanicznego powstrzymania sygnału czy mechanicznego uszkodzenia	Łatwy do oszukania przez mostkowanie kabla informacyjnego, przez przecięcie z opóźnieniem lub przez przecięcie specjalnymi szczypcami do cięcia drutu	Łatwy do oszukania przez mostkowanie kabla informacyjnego	Stosunkowo łatwy do oszukania w przypadku zastosowania odpowiedniej konfiguracji luster

Zmiany czułości wskutek ciężkich warunków atmosferycznych	System posiada stałą czułość niezależną od warunków atmosferycznych. Nie wymaga dodatkowej rekalibracji.	System redukuje automatycznie swoją czułość zależnie od warunków atmosferycznych. Zdarzają się przypadki, że czułość jest zredukowana do tego stopnia iż nie jest możliwe wykrycie ataku na system.	System posiada stałą czułość. Zależnie od warunków atmosferycznych. wymaga dodatkowej rekalibracji.	System posiada stałą czułość. Zależnie od warunków atmosferycznych. wymaga dodatkowej rekalibracji.
Czujniki	Siatka światłowodowa wykonana jest z kabla ze wzmocnionym pokryciem, odpornego na działanie promieniowania ultrafioletowego, przeznaczonego do pracy w ciężkich warunkach środowiskowych. Światłowodowy kabel czujnikowy przeznaczony do pracy w ciężkich warunkach środowiskowych. Oba elementy systemu spełniają wymagania wojskowe.	Części metalowe czujnika drgań korodują w szkodliwych warunkach środowiska.	Elementy mocujące kabel są wrażliwe na przeciążenia i działanie szkodliwych warunków środowiska.	Elementy optyczne są wrażliwe na działanie szkodliwych warunków środowiska
Instalacja	Bardzo łatwa o krótkim czasie instalacji.	Bardzo łatwa o stosunkowo krótkim czasie instalacji.	Trudna o długim czasie instalacji	Stosunkowo łatwa o krótkim czasie instalacji.
Wpływ ruchów podłoża i wsporników na poprawną pracę systemu	System ignoruje wolne ruchy podłoża i wsporników	System ignoruje wolne ruchy podłoża i wsporników	Wolne ruchy podłoża i wsporników powodują powstawanie fałszywych alarmów	System ignoruje wolne ruchy podłoża i wsporników
Wymagania terenowe na którym instaluje się nowy system	Brak wymagań	Możliwość zamontowania tylko na naprężonych i sztywnych ogrodzeniach, będących w dobrym stanie. Obszar powinien być wolny od drzew, krzewów i falujących obiektów.	Możliwość instalacji tylko na nowym ogrodzeniu, które musi być zbudowane według specjalnych zaleceń.	Obszar powinien być wolny od drzew, krzewów i falujących obiektów.
Konserwacja i niezawodność	Nie wymaga ciągłej konserwacji. Łatwa i stosunkowo tania naprawa uszkodzonego światłowodu.	Wymaga ciągłej konserwacji i strojenia czujników oraz jednostki sterującej.	Wymaga ciągłej konserwacji a zwłaszcza regulacji naprężenia przewodów.	Wymaga okresowej kalibracji oraz justowania elementów optycznych.
Długość życia	Minimum 10 lat. System wykonany z kabli przystosowanych do pracy w ciężkich warunkach zapewniają długoletnią nieprzerwaną pracę.	Stosunkowo krótki czas życia. System wykonany z elementów podlegających korozji.	Stosunkowo krótki czas życia. System wykonany z elementów podlegających korozji.	Średni czas życia, zależny od wpływu warunków środowiska na elementy optyczne systemu.

Piotr KUREK TTI INVENTEL S.A.

t.a.c
talking buildings

T.A.C.
Gdynia

Henryk BUŃKA

ZASTOSOWANIE SYSTEMÓW BEZPIECZEŃSTWA I KONTROLI DOSTĘPU DO OCHRONY OBIEKTÓW SPECJALNYCH

CENTRUM KONFERENCYJNE WP Grudzień 2001

www.tac-global.com

Henryk BUŃKA

t.a.c®

talking buildings

Building IT™

TAC Polska Sp. z o.o.
ul. Batorego 28-32
81-327 Gdynia

t.a.c™

Wieloletnie doświadczenia

1998 t.a.c™

1977 TA TA Control

1962 TA

1925 T.A.

t.a.c™

Dzięki połączonym siłom jesteśmy
swiatowym liderem w zakresie
Otwartych Systemów
Automatyki i Bezpieczeństwa Budynków

t.a.c + CSI Control Systems International

Swiatowy lider pod wzgledem:

- Udzialów na rynku
- Technologii
- Satysfakcji klienta

t.a.c

TAC na swiecie

TAC
w obu Amerykach

Dallas, Texas

TAC
Europa

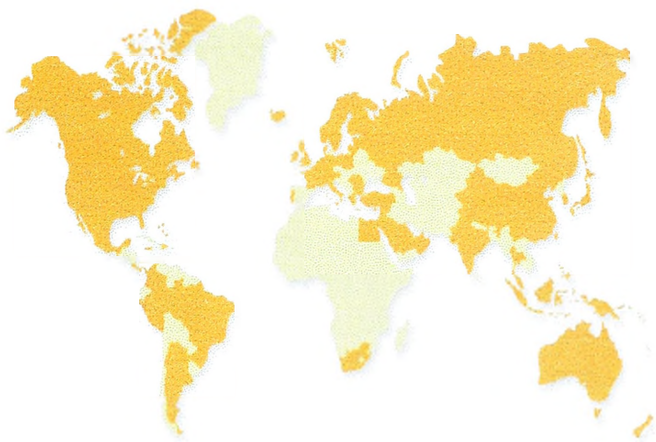
Malmö, Szwecja

TAC
Azja – Pacyfik

Perth, Australia

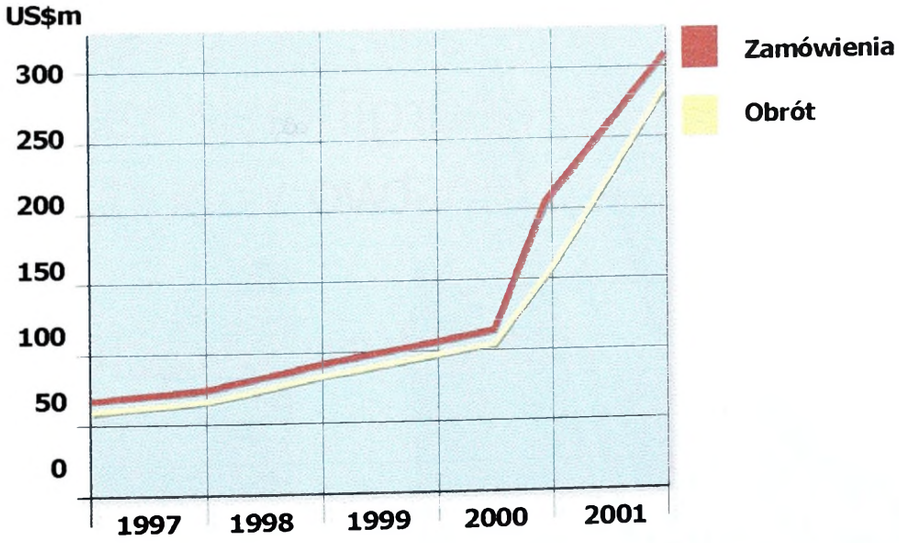
t.a.c

Instalacje TAC pracują w 70 krajach na całym świecie



t.a.c™

Ciągły wzrost



t.a.c™

TAC Polska

- Od roku 1992 na rynku polskim
- 40 pracowników
- Obroty ponad 25 000 000 PLN
- Oddziały:
  - Gdynia – centrala
  - Gdańsk
  - Warszawa
  - Wrocław
  - Kraków
  - Lublin
  - przedstawicielstwo w Poznaniu

t.a.c

t.a.c

Systemy otwarte – nasza wizja

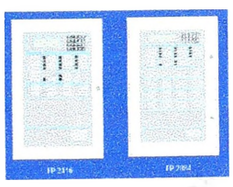
- Ta sama wizja od roku 1992:
  - systemy otwarte gwarantują pewność oraz wolny wybór naszym klientom;
  - TAC stosuje wiodące technologie na rozwijającym się rynku. Do takiego twierdzenia upoważnia nas stosowanie jako bazy technologii LONWORKS® i Internetu.

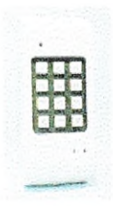
t.a.c ISO 9001 ISO 14001

LONMARK SPONSOR

t.a.c

Systemy bezpieczeństwa w budynkach





- Systemy p. pożarowe
- Systemy kontroli dostępu i czasu pracy
- Sygnalizacja włamania i napadu
- Telewizja przemysłowa
- Systemy nagłaśniające

t.a.c

Systemy bezpieczeństwa spełniające najwyższe wymagania

- Pojedyncze i zintegrowane
  - dla pojedynczych lub 10 000 drzwi
  - dla 20 lub 200 000 użytkowników
  - dla jednego lub 1 000 budynków
- Urządzenia z certyfikatami najwyższej klasy - "S"
- Projektanci o najwyższych uprawnieniach - dla obiektów klasy "SA-4"

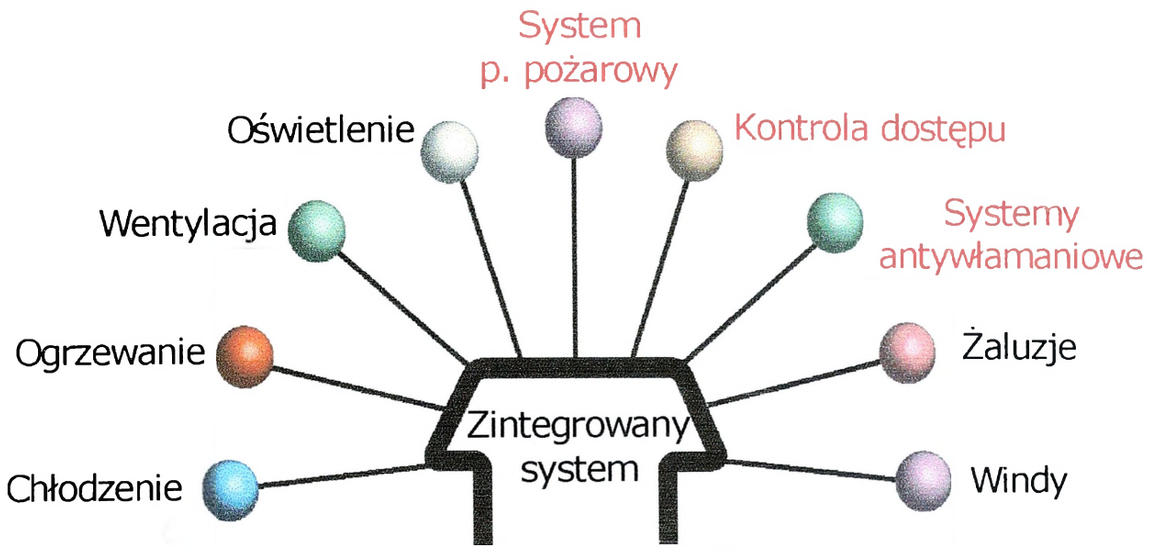
t.a.c

Przykładowe realizacje w kraju

- 3 systemy w Komendzie Głównej Policji
  m.in. przy ul. Puławskiej
- 2 systemy w Komendzie Stołecznej Policji
  m.in. Pałac Mostowskich
- Kompleks budynków Elektrimu w Warszawie
- PTC ERA GSM
- Big Bank Gdański

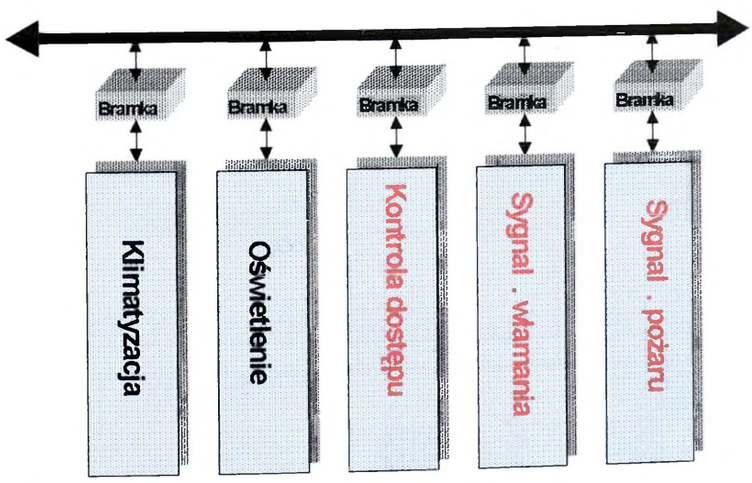
t.a.c

Zintegrowane systemy - przyszłość jest już faktem



t.a.c

Tradycyjne podejście do integracji



- Każdy z podsystemów posiada oddzielne okablowanie
- Wymaga różnych narzędzi do instalacji urządzeń
- Najczęściej potrzeba wielu służb serwisowych
- Dowolna zmiana w protokole podsystemu wymaga przeprogramowania bramki

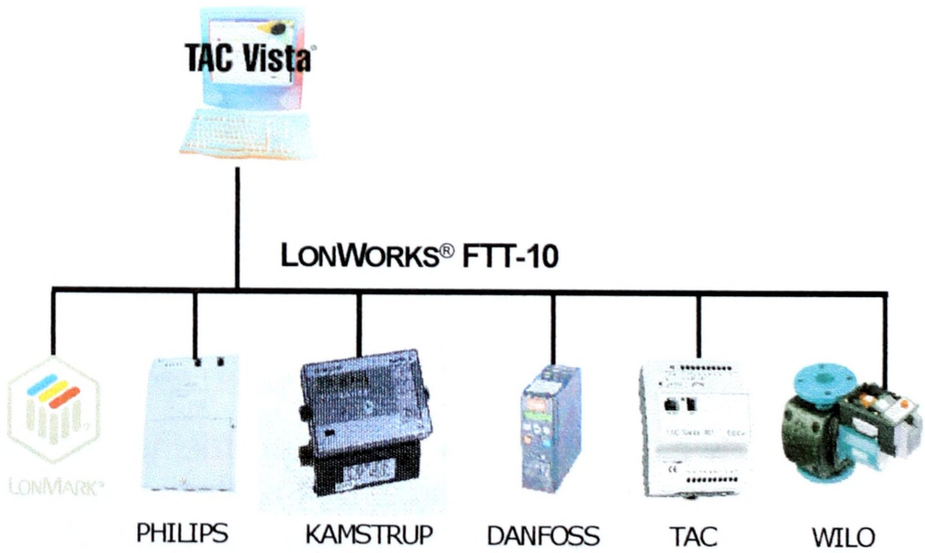
t.a.c

Sieci sterujące LONWORKS®

- Sieci danych a sieci sterujące
- Zorientowane na informacje a nie komendy
- Logika dzialania zawarta tylko w urządzeniach
- Jednopoziomowa architektura

t.a.c

Sieć sterująca LONWORKS®



t.a.c

Komponenty sieci LonWorks®
- media komunikacyjne

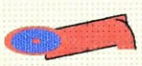
Telefon
< 19.200 kbit/s

Radio
< 20 km
4.8 kbit/s (450MHz)

Światło
Światłowód 78 - 1.25 Mbit/s, < 3 km
Podczerwień 78 kbit/s, 10 - 30 m

Skrętka 2-żyłowa
TP/FT-10 dowolna topologia, 78 kbit/s
TP/XF-1250 magistrala, 1,25 Mbit/s

Sieci zasilające
PL-20 Power Line, 5 kbit/s, General
PL-30 Power Line, 2 kbit/s,



Kable koncentryczne
< 3 km
1,25 Mbit/s

t.a.c

Komponenty tworzące otwarte systemy

Sterowniki
TAC Xenta®

Zarządzanie/Monitoring
TAC Vista®

Narzędzia
TAC Menta®
LonMaker for Windows®

t.a.c

Przykładowe realizacje w kraju

Bank Gdański - Gdańsk

CB Lubicz - Kraków

EUROMARKET 2000 - Kraków

Alfa Plaza - Gdynia

Szpital - Kościerzyna

BRE Bank - Bydgoszcz

Park wodny - Kraków

t.a.c

Inne budynki zrealizowane w kraju

- Szpital w Białogardzie
- Akademia Medyczna w Bydgoszczy
- Biurowiec Land w Warszawie
- Jerozolimskie Bussines Park
- Państwowy Szpital Kliniczny nr 2 w Poznaniu
- Wojewódzki Szpital Chorób Płuc i Gruźlicy w Bydgoszczy
- Wojskowy Szpital Kliniczny w Bydgoszczy
- BFK w Bydgoszczy
- Stomil w Bydgoszczy
- Targówek Ratusz w Warszawie
- Zachęta w Warszawie
- Toyota Centrum w Warszawie
- Biurowiec Intraco 1 w Warszawie
- Stacje Mercedesa w Bydgoszczy, Rzeszowie i Szczecinie
- NBP w Gdańsku
- Zamek Królewski na Wawelu w Krakowie
- Hala ORBITA we Wrocławiu i wiele innych....

t.a.c

Wybrane projekty w ciepłownictwie

- MPEC Kraków – 1995
  - 19 stanowisk operatorów – 8 sieci LAN
  - 130 monitorowanych obiektów
- MPEC Wrocław – 1999
  - 5 stanowisk operatorów – 2 sieci LAN
  - 130 monitorowanych obiektów
- OPEC Gdynia – 2000
  - 26 stanowisk operatorów – 15 sieci LAN
  - 100 monitorowanych obiektów

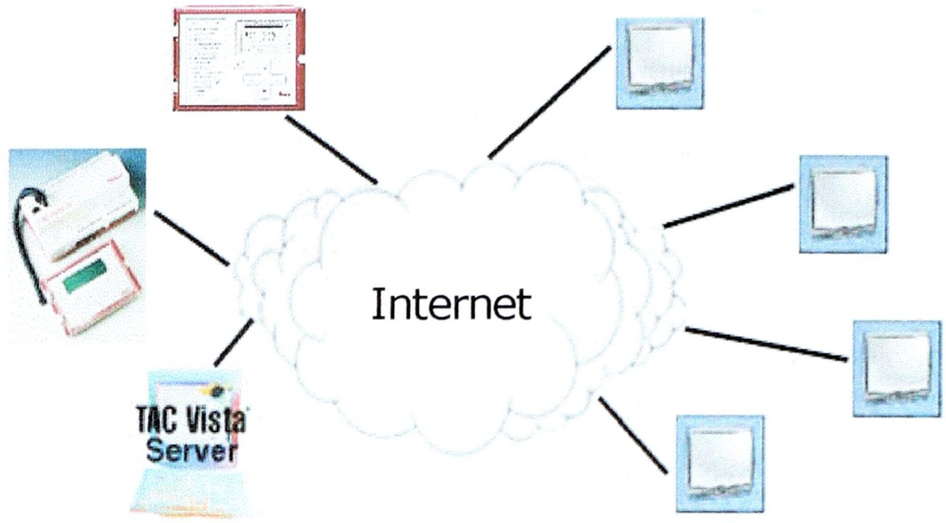
t.a.c

Referencje – funkcjonujące systemy w przedsiębiorstwach ciepłowniczych

- **MPEC Kraków**
- **MPEC Wrocław**
- **OPEC Gdynia**
- **LPEC Lublin**
- **SPEC Warszawa**
- **WPEC Legnica**
- **PEC Kędzierzyn-Koźle**
- **PEC Brzeg**
- **PEC Toruń**
- **PEC Bytom**
- **ECO OPOLE**
- **ZEC Grodków**
- **PEC Namysłów**
- **PEC Prudnik**
- **MPEC Przemyśl**

t.a.c

Zarządzanie z dowolnego miejsca



t.a.c

TAC Xenta® 511 - całkowite sterowanie poprzez Internet

- Nowa generacja efektywnego monitoringu sieci LONWORKS®
- Własności
  - Wbudowany web serwer, dostęp przez zwykłą przeglądarkę Intranetową
  - Kodowanie dostępu z informacją dla wybranych użytkowników
  - Grafiki, alarmy, rejestracje itp.
  - Ethernet 10Base-T z TCP/IP
  - LONWORKS® FTT-10, SNVT

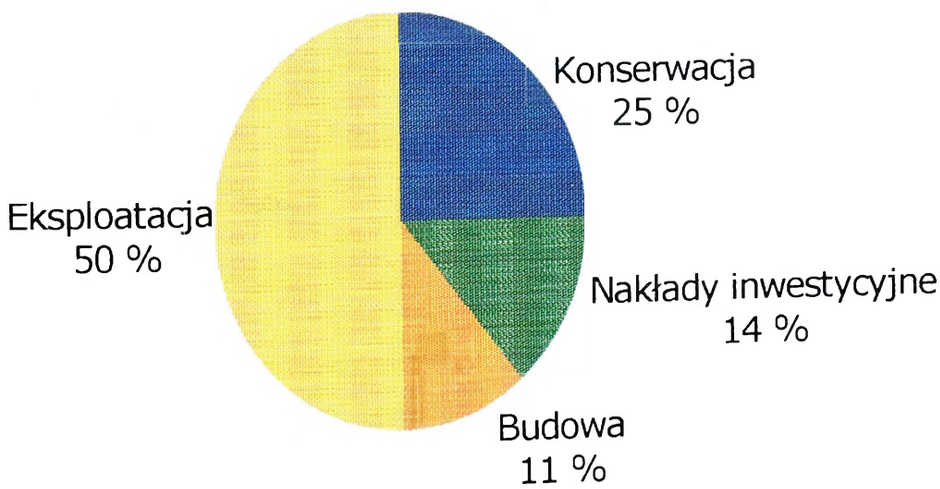
t.a.c

TAC Vista® Wapstation

Zdalny nadzór poprzez Internet
z wykorzystaniem telefonów GSM

t.a.c™

Koszty "życia" budynku

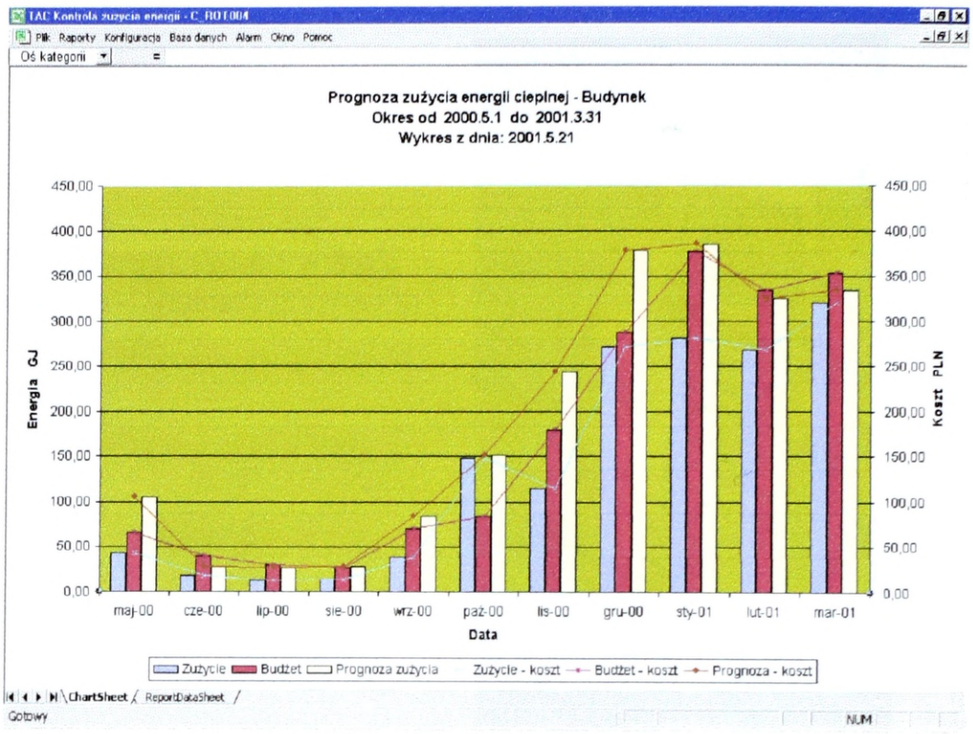


- Kontrola kosztów eksploatacji budynku
- Optymalizacja eksploatacji oraz klimatu wewnętrznego
- Planowanie cykli konserwacji

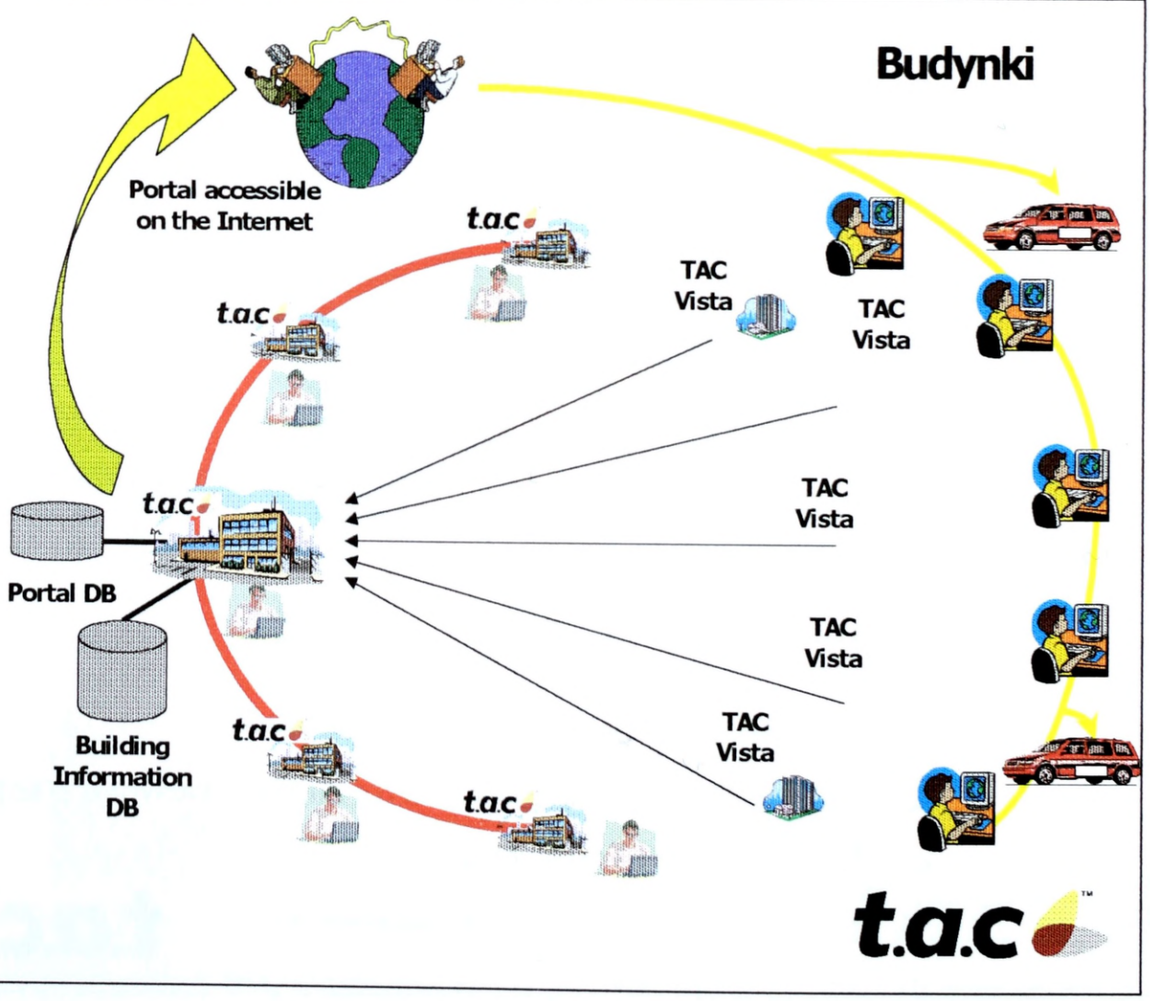
Źródło: Lucent Technologies (Fastighetsutveckling 2/97)

t.a.c™

TAC Signature



t.a.c™



t.a.c™

EPIT & Korporacja Rozwoju Wschód Zachód
Warszawa

Piotr SZMIT

SYSTEM BEZPIECZEŃSTWA I OCHRONA OBIEKTÓW SPECJALNYCH W SYTUACJACH KRYZYSOWYCH NA PRZYKŁADZIE LOTNISKA I PORTU LOTNICZEGO

CENTRUM KONFERENCYJNE WP Grudzień 2001

Dziękuję organizatorom za przekazane do firmy EPIT & KRWZ zaproszenie na tegoroczną konferencję, która jest, inwestorem i developerem projektu *Lotnisko i Strefa Gospodarcza Biała Podlaska*. Jestem przekonany, że udział przedstawicieli Sztabu Generalnego WP, Akademii Obrony Narodowej, Wojskowej Akademii Technicznej w składzie komitetu programowego konferencji wniesie wiele interesujących ocen, opinii i propozycji dalszej współpracy wojskowo-cywilnej ze *Zrzeszeniem Firm Działających na rzecz Obronności RP*.

Przedsięwzięcie w Białej Podlaskiej, jest realizowane na lotnisku, które zostało na stałe udostępnione dla lotnictwa cywilnego, w opcji współużytkowania na podstawie decyzji MON Nr 101 oraz wytycznych dowódcy WLOP Nr 686. Nowy cywilny port lotniczy został utworzony przecież, na czynnym lotnisku wojskowym Biała Podlaska, funkcjonującym w strukturze WSOSP w Dęblinie. Dostosowanie funkcji prawnych i operacyjnych w przedmiocie współużytkowania tego lotniska, nie było zadaniem łatwym oraz możliwym do wykonania w krótkim czasie. Na współużytkowanym lotnisku Biała Podlaska, realizowany jest normatywny program wojskowego szkolenia lotniczego.

Z uwagi na powyższe - działania prawne, organizacyjne i operacyjne, warunkujące pracę nowego cywilnego portu lotniczego, wymagały (poza opracowaniem dokumentacji), również wielostronnego jej uzgodnienia na szczeblu MON, Ministerstwa Skarbu Państwa, MT i GM, WLOP, WSOSP i GILC oraz wdrożenia rozwiązań, które stanowiły podstawę do uzyskania koncesji na prowadzenie cywilnej działalności portowej.

Następnie, dalsze etapy organizacyjne, związane z opracowaniem koncepcji i projektu dostosowania lotniska do wymogów ICAO, aktywnie wspierane przez inwestora zagranicznego, skutkowały zatwierdzeniem docelowego planu modernizacji i przebudowy lotniska przez dowódcę WLOP w sierpniu br. Więcej informacji na temat projektu *Lotnisko i Strefa Gospodarcza Biała Podl*aska, znajdziecie Państwo na stronie internetowej: www.epit-company.com.

Zasadniczym warunkiem w zakresie wdrożenia cywilnej operacyjnej dokumentacji portowej, niezbędnej dla sukcesywnego uruchomienia działalności spółki Port Lotniczy Biała Podlaska, było opracowanie i zatwierdzenie przez odpowiednie służby wojskowe i cywilne:

- programu ochrony portu lotniczego;
- operacyjnego planu ratownictwa lotniskowego.

Z uwagi na przewidziany dla mnie temat referatu, moje wystąpienie podczas dzisiejszej konferencji, powinno więc skupić się głównie na bezpieczeństwie lotnisk

i portów lotniczych. Celowo użyłem określenia „lotnisko'' oraz „port lotniczy'', co ma uzasadnione zastosowanie, z uwagi, na opcję współużytkowania obiektu lotniskowego Biała Podlaska oraz pozostałych wojskowych lotnisk objętych decyzją MON Nr 101. Ponadto, określenie „lotnisko'', ma także zastosowanie w odniesieniu do wielu czynnych lotnisk cywilnych, które nie są jednocześnie portami lotniczymi. Dotyczy to również lotnisk aeroklubowych, prywatnych i fabrycznych oraz wojskowych lotnisk współużytkowanych udostępnionych na stałe i doraźnie dla potrzeb lotnictwa cywilnego. Opcja współużytkowania lotniska, polega na tym, że cywilny port lotniczy, wykorzystuje te elementy infrastruktury lotniskowej, które są niezbędne dla operacyjnej obsługi cywilnych statków powietrznych. Takie rozwiązanie ma uzasadnienie ekonomiczne, zwłaszcza w początkowym okresie uruchamiania cywilnej działalności portowej, kiedy ruch lotniczy jest niewielki i nieregularny. Na tym etapie nie ma uzasadnienia, właśnie z przyczyn związanych ze znacznym ryzykiem ekonomicznym, podejmowanie działań dla utworzenia pełnej struktury cywilnych służb lotniskowych.

Możliwości współpracy z głównym wojskowym użytkownikiem lotniska, na warunkach określonych przez dowódcę WLOP w wytycznych Nr 686, praktycznie zabezpieczają obsługę cywilnych operacji lotniczych w ruchu krajowym, szczególnie dla lotnictwa General Aviation, która wg właściwości dla nadzorowanego ruchu lotniczego, może być zapewniona przez wojskowych kierowników ruchu lotniczego.

Szczegółowe zasady korzystania i warunki częściowego zabezpieczenia cywilnych operacji lotniczych na lotniskach współużytkowanych przez siły i środki wojskowe, określił dowódca WLOP w wytycznych Nr 686, a ich zakres precyzuje szczegółowo umowa zawarta pomiędzy prawnymi współużytkownikami lotniska Biała Podlaska, przy czym nadal głównym użytkownikiem lotniska pozostaje strona wojskowa.

Za wzorcowy i wzorowy przykład współużytkowania lotnisk może posłużyć lotnisko Warszawa – Okęcie, mimo, że cywilno – wojskowe współużytkowanie tego lotniska, ma nieco inny charakter. Wojskowy Port Lotniczy ma swój teren, swoje obiekty, własne służby operacyjne, portowe i techniczne, odpowiedzialne za obsługę specjalnych operacji lotniczych. Natomiast, 36 Specjalny Pułk Lotnictwa Transportowego realizuje przewozy lotnicze dla potrzeb rządowych, a do startów i lądowań wykorzystuje pole manewrowe (drogi startowe i drogi kołowania), międzynarodowego portu lotniczego.

W sytuacjach, które wymagają zastosowania specjalistycznego sprzętu lotniskowego, zostały ustalone zakresy współpracy pomiędzy służbami wojskowymi, a cywilnymi służbami PLL LOT i PP PPL.

Powracając po tym uzupełnieniu do tematu zasadniczego, należy postawić pytanie: Czym jest i jak precyzyjnie zdefiniować bezpieczeństwo portu lotniczego? Nie jest to przecież łatwe zadanie.

Od czasu, gdy człowiek po raz pierwszy wzniósł się w powietrze za pomocą urządzenia cięższego od powietrza, stały postęp techniczny polegający na wprowadzaniu do eksploatacji coraz to nowych konstrukcji lotniczych, nieuchronnie wymusza dostosowanie infrastruktury lotnisk i portów lotniczych oraz procedur operacyjnych bezpośrednio związanych i stanowiących o bezpieczeństwie i zdolności do obsługi operacji lotniczych.

Wiele osób, zwłaszcza starszych, pamięta doskonale początki cywilnego lotnictwa komunikacyjnego i pierwsze loty do i z Warszawy, odbywające się z Pola Mokotowskiego, które miało przecież tylko nawierzchnię trawiastą. Także w przedwojennym lotnictwie wojskowym, nie było praktycznie lotnisk o nawierzchni betonowej, czy asfaltobetonowej. Wraz ze zwiększającym się zasięgiem samolotów oraz wzrostem ich całkowitej masy startowej (MTOW), nastąpiła potrzeba pilnego dostosowania wzajemnych relacji pomiędzy lotniskiem, a statkiem powietrznym. Priorytetem tych prac było oczywiście maksymalne zapewnienie bezpieczeństwa obsługi portowej statków powietrznych i bezpieczeństwa pasażerów i załóg lotniczych.

Na podstawie wielu dostępnych opracowań na temat bezpieczeństwa w lotnictwie cywilnym, własnych kontaktów i praktyki oraz często prowadzonych rozważań na ten temat w środowisku lotniczym, uważam, że w najbardziej przekonywujący sposób, pojęcie bezpieczeństwa w odniesieniu do portu lotniczego, zdefiniował dr inż. Marek Szczelina z Politechniki Wrocławskiej w następujący sposób:

- bezpieczność, to właściwość systemu (obiektu) wyrażająca jego przystosowanie do utrzymania stanu bezpieczeństwa;
- bezpieczeństwo, jako stan systemu, charakteryzujący się brakiem zagrożenia katastrofą.

Tak więc, bez systemowego podejścia do problematyki bezpieczeństwa w ogóle, nie da się rozpatrywać stanu bezpieczeństwa lotniska, bądź portu lotniczego. Nie jest również możliwa ocena stanu i właściwości ochrony lotnictwa cywilnego przed działaniami bezprawnymi, bez uwzględnienia wszystkich elementów tworzących optymalny systemowy i niezawodny układ bezpieczeństwa, właściwy do zastosowania w porcie lotniczym, w linii lotniczej, bądź w innej firmie prowadzącej działalność na rzecz lotnictwa cywilnego.

Podstawowe podsystemy bezpieczeństwa cywilnego portu lotniczego tworzą trzy zasadnicze elementy:

a) personel ochrony, odpowiedzialny za ochronę fizyczną i kontrolę dostępu;
b) urządzenia techniczne wspomagające ochronę fizyczną;
c) środowisko, (uwarunkowania prawne, operacyjne, kategoria lub klasa lotniska), na którym funkcjonuje cywilny port lotniczy.

Ze swojej strony również uważam, że rozszerzenie tematyczne tego zagadnienia będzie niezbędne, jako przynajmniej próba oceny uwarunkowań składających się na jakość systemów i podsystemów bezpieczeństwa stosowanych w portach lotniczych i ogólny stan bezpieczeństwa w lotnictwie cywilnym w RP. Ponadto, z uwagi na wzajemne zależności pomiędzy podmiotami uprawnionymi do współużytkowania lotnisk i zarządzania cywilnymi portami lotniczymi, a użytkownikami statków powietrznych, nie jest możliwe rozważanie zagadnień związanych z bezpieczeństwem lotnisk i portów lotniczych, bez odniesienia się do szerszej oceny i znaczenia tej problematyki dla całego systemu bezpieczeństwa państwa. To, w miarę pełnego zobrazowania znaczenia bezpieczeństwa na lotnisku i w porcie lotniczym, dla systemu bezpieczeństwa państwowego, postaram się odnieść do uwarunkowań, których wykonanie, wynika z uregulowań prawnych w skali międzynarodowej i krajowej.

Nie sposób przy tym pominąć, takich spraw, jak:

1. Struktura cywilnych władz lotniczych w RP.
2. Krajowych i międzynarodowych uwarunkowań prawnych obowiązujących w lotnictwie cywilnym.
3. Powinności i obowiązków, jakie muszą spełnić podmioty uprawnione do zarządzania lotniskami i portami lotniczymi.
4. Powinności i obowiązków, jakie muszą spełnić właściciele i użytkownicy statków powietrznych, (którzy w zależności od profilu prowadzonej działalności lotniczej, są przewoźnikami liniowymi lub operatorami lotniczymi).

Wzajemne relacje w lotnictwie pomiędzy lotniskiem lub portem lotniczym, który w zależności od kategorii, przyjmuje różnego rodzaju statki powietrzne w krajowym i międzynarodowym ruchu lotniczym, a użytkownikami statków powietrznych, nie mogą być traktowane rozdzielnie przy rozpatrywaniu zagadnień odnoszących się do bezpieczeństwa lotniczego.

Wymogi konwencji, których sygnatariuszem jest Rzeczpospolita Polska i międzynarodowych przepisów lotniczych aktualizowanych wraz z rozwojem techniki i komunikacji lotniczej przez ICAO i ECAC, określają normy i procedury w zakresie bezpieczeństwa, obowiązujące, zarówno podmioty zarządzające lotniskami i portami lotniczymi, jak również właścicieli i użytkowników statków powietrznych. Udział w międzynarodowych cywilnych organizacjach lotniczych, nie ogranicza władz lotniczych danego państwa w przedmiocie dostosowania przepisów i norm międzynarodowych, do uwarunkowań, w jakich funkcjonuje lotnictwo cywilne na ich terytorium.

W Polsce odpowiednikiem *Annexów ICAO* (lub dokumentów związanych), jest obowiązujący i na bieżąco aktualizowany zbiór przepisów *PL*. Cywilne władze lotnicze RP, mają również obowiązek wypracowania i stałego doskonalenia zasad współpracy operacyjnej z odpowiednimi strukturami władz wojskowych odpowiedzialnych za kontrolę przestrzeni powietrznej nad terytorium kraju. Podstawowe uregulowania prawne, zarówno w skali międzynarodowej, jak również w odniesieniu do przepisów krajowych, mających zastosowanie w lotnictwie cywilnym, podlegają stałej bieżącej aktualizacji i dostosowaniu do zmieniających się warunków, w których funkcjonuje lotnictwo.

Wobec rozwoju komunikacji lotniczej na świecie, konieczność zapewnienia warunków bezpieczeństwa lotniczego na lotniskach i w portach lotniczych jest pojęciem bardzo obszernym i nie ogranicza się wyłącznie do procedur w zakresie fizycznej i technicznej ochrony obiektów lotniskowych. Specyfika działalności portów lotniczych, wymaga dla spełnienia warunków systemowo pojętego bezpieczeństwa lotniczego, również zastosowania odpowiednich rozwiązań proceduralnych i technicznych w:

a) obszarze zapewniającym optymalne warunki dla bezawaryjnego wykonywania lotów w przestrzeni nadzorowanej i kontrolowanej, lotniska lub portu lotniczego
b) zakresie kontroli, nadzoru i koordynacji naziemnego ruchu statków powietrznych i pojazdów lotniskowych
c) w obszarze związanym z zabezpieczeniem lotnisk i portów lotniczych pod względem ochrony fizycznej i technicznej oraz ratownictwa lotniskowego.

Wymaga to, stałego doskonalenia działań profilaktycznych, których celem jest eliminowanie potencjalnych zagrożeń ze strony działań bezprawnych, jakich wobec lotnictwa cywilnego dopuszczają się różnego rodzaju i charakteru oraz często trudne do zidentyfikowania organizacje terrorystyczne, a także pojedyncze osoby z przyczyn, które mogą wynikać z psychospołecznych zachowań o bardzo zróżnicowanym podłożu.

Dla wykazania wzajemnych zależności i uwarunkowań składających się generalnie na bezpieczeństwo lotnicze, dalszą część swojego wystąpienia podzieliłem na poszczególne zakresy, które łączą najbardziej istotne elementy bezpiecznego funkcjonowania lotnisk i portów lotniczych z systemem bezpieczeństwa państwowego.

Ogólna charakterystyka bezpieczeństwa lotniczego

Stan bezpieczeństwa lotniczego należy rozpatrywać, jako stan faktyczny systemu i jako właściwość systemu bezpośrednio związaną ze zdolnością do dostosowania działań operacyjnych w sytuacji zagrożenia.

1. Bezpieczeństwo lotnicze, jest stanem jakości funkcjonowania systemu procedur i rozwiązań technicznych stosowanych w ochronie lotnisk, portów lotniczych oraz statków powietrznych przed działaniami bezprawnymi.
2. System bezpieczeństwa lotniczego składa się z wzajemnych relacji wszystkich elementów, które tworzą podsystemy oparte na pracy człowieka i urządzeń technicznych.
3. Praktycznie system bezpieczeństwa lotniska lub portu lotniczego, wymaga dostosowania właściwości operacyjnych pomiędzy:
    a) programem ochrony (lotniska lub portu lotniczego);
    b) operacyjnym planem ratownictwa lotniskowego.
4. Programy Ochrony linii lotniczej lub firmy zajmującej się lotniczym przewozem osób i towarów podlegają odrębnym przepisom, (por. podręcznik ICAO Doc 9422 – AN/923).
5. Sprawność systemu bezpieczeństwa lotniczego, lotnisk i portów lotniczych oraz użytkowników statków powietrznych jest najbardziej istotnym czynnikiem decydującym o życiu wielu ludzi.
6. Na podstawie analizy wieloletnich zbiorów danych statystycznych, największe ryzyko podczas operacji lotniczych pod względem wystąpienia przesłanek do zaistnienia tzw. zdarzenia, wypadku lub katastrofy lotniczej związane jest głównie z fazą startu i lądowania statku powietrznego. W tym, około 80 % zdarzeń lotniczych, wypadków i katastrof ma miejsce na lotniskach i w strefie odpowiedzialności zarządzających lotniskami i portami lotniczymi, która obejmuje obszar 8 NM (mil morskich) od granic lotniska lub portu lotniczego.

Zamieszczam poniżej wyciąg z ***Annexu 17 ICAO***, który charakteryzuje podstawowe wymogi w zakresie bezpieczeństwa w transporcie lotniczym.

Za ich przestrzeganie, odpowiadają wg lokalnie przyjętych na lotniskach i w portach lotniczych właściwości organizacyjnych, zarówno podmioty uprawnione do zarządzania lotniskami, jak również przewoźnicy i właściciele statków powietrznych.

Wyciąg z ANNEXU 17 I.C.A.O. AVIATION SECURITY

4.1.1.

Każde umawiające się państwo ustanowi procedury zabezpieczające przed wniesieniem w jakikolwiek sposób przez osoby nie mające uprawnień lub będące o to podejrzane, na pokład statku powietrznego służącego międzynarodowemu lotnictwu cywilnemu: broni, materiałów wybuchowych lub wszelkich innych niebezpiecznych urządzeń, które mogą być użyte do przeprowadzenia aktów bezprawnej ingerencji (terroryzmu). Dla realizacji tego standardu opracowana została lista przedmiotów zakazanych na pokładzie statków powietrznych.

Lista przedmiotów niebezpiecznych obejmuje:

a) broń palną (w tym gazową);
b) broń sieczną i tępą;
c) amunicję do broni palnej (i gazowej);
d) materiały zapalające i zapalniki;
e) granaty ręczne i petardy;
f) związki łatwopalne, gazy bojowe i techniczne w stanie naturalnym oraz pod ciśnieniem;
g) substancje żrące i trujące;
h) wszelkiego rodzaju imitacje broni oraz innych zakazanych przedmiotów od litery ***a*** do litery ***i***;
i) inne przedmioty, których przewóz może być wykorzystany do celów ataku lub obrony, a ponadto siekierki do lodu, ciupagi, brzytwy, spiczaste nożyczki, noże oraz inne przedmioty budzące uzasadnione podejrzenie (odnośnie ich wykorzystania innego, niż pierwotne przeznaczenie) np. sprzęt elektroniczny i elektryczny zasilany bateriami i przewożony w bagażu.

4.2.1.

Każde umawiające się państwo zapewni, iż zostaną przedsięwzięte odpowiednie procedury kontroli pasażerów transferowych i tranzytowych oraz ich bagażu podręcznego

w celu zabezpieczenia się przed wniesieniem zabronionych przedmiotów na pokład statku powietrznego służącego międzynarodowemu lotnictwu cywilnemu.

4.3.1.

Każde umawiające się państwo ustanowi procedury i systemy identyfikacyjne, aby uniemożliwić dostęp osobom i pojazdom nieupoważnionym do:

a) strefy kontrolowanej portu lotniczego świadczącego usługi dla międzynarodowego lotnictwa cywilnego;
b) innych rejonów portu lotniczego ważnych z punktu widzenia jego bezpieczeństwa.

Przestrzeganie tych wymogów jest podstawowym elementem ochrony lotnictwa cywilnego.

Bezpieczeństwo cywilnych lotnisk i portów lotniczych jako istotny element systemu bezpieczeństwa państwowego

Wymogi w zakresie zapewnienia bezpiecznego funkcjonowania oraz eksploatacji lotnisk i portów lotniczych, mają bezpośrednie przełożenie i wpływ na warunki bezpieczeństwa lotniczego użytkowników statków powietrznych (wojskowych i cywilnych), posiadających prawo operowania w polskiej przestrzeni powietrznej (FIR WAW). W przypadku wystąpienia niebezpiecznych zdarzeń, wypadków i katastrof lotniczych na skutek:

a) zaniedbań w eksploatacji lotnisk i portów lotniczych;
b) zaniedbań technicznych podczas użytkowania i eksploatacji statków powietrznych prowadzących do katastrofy lotniczej;
c) braku działań identyfikujących możliwość powstania innych zagrożeń, uwarunkowanych wzajemnymi relacjami pomiędzy lotniskami i portami lotniczymi a użytkownikami statków powietrznych;
d) braku działań profilaktycznych, których celem powinien być stały monitoring potencjalnych zagrożeń oraz eliminacja i minimalizacja skutków spowodowanych przez działania bezprawne wobec lotnictwa i katastrofy lotnicze.

Bardzo często dochodzi do wielu ofiar śmiertelnych, a także olbrzymich strat materialnych w sprzęcie lotniczym, w infrastrukturze lotnisk i terenów przyległych, w tym również możliwość zniszczenia znacznej części miasta, jeżeli samolot uległ katastrofie

podczas wystąpienia takich sytuacji, jakie miały miejsce kilka lat temu na Teneryfie oraz w Amsterdamie i w Krasnojarsku.

Jest oczywiste, że w przypadku wystąpienia katastrofy lotniczej, każde państwo ma obowiązek podjęcia działań w zakresie ratownictwa i poszukiwania zgodnych z międzynarodowymi konwencjami lotniczymi. W zależności od tego, jakiego typu statek powietrzny, z jaką ilością pasażerów lub ładunku na pokładzie uległ katastrofie oraz czy katastrofa miała miejsce na lotnisku, bądź w terenie przylotniskowym, zamieszkałym przez znaczne skupiska ludności lub w terenie trudno dostępnym - zawsze wiąże to olbrzymie środki finansowe i materialne oraz wymaga podjęcia niezwłocznych i niezbędnych działań dla ratowania życia ludzkiego i usunięcia skutków takich katastrof.

Dodatkowym zagrożeniem, może być także poważne skażenie środowiska, jeżeli ulegnie katastrofie samolot przewożący różnego rodzaju materiały niebezpieczne lub jeżeli katastrofa samolotu nastąpi w rejonie, gdzie są zlokalizowane zakłady produkujące materiały niebezpieczne lub magazyny (cywilne lub wojskowe), z takimi środkami.

Z uwagi na powyższe uwarunkowania, ogólna definicja „bezpieczeństwa lotniczego'', obejmuje nierozłącznie wszystkie obszary działalności portowej i lotniczej wiążące się z:

a) utrzymaniem wysokiego stopnia bezawaryjnej eksploatacji statków powietrznych;
b) systemowymi rozwiązaniami w zakresie ochrony lotnisk, portów lotniczych i statków powietrznych przed działaniami bezprawnymi o charakterze terrorystycznym i sabotażowym;
c) utrzymaniem w pełnej gotowości służb państwowych i lokalnych przeszkolonych, wyposażonych i zorganizowanych w odpowiednie struktury oraz środki niezbędne dla natychmiastowego podjęcia akcji antyterrorystycznych lub działań w zakresie poszukiwania i ratownictwa lotniczego.

Kryteria i warunki, niezbędne dla utrzymania wymaganych standardów bezpieczeństwa lotniczego przez użytkowników przestrzeni powietrznej w danym rejonie świata, określają międzynarodowe konwencje lotnicze, przepisy nadzorów lotniczych oraz normy techniczne i eksploatacyjne obowiązujące producentów statków powietrznych i sprzętu lotniczego.

Obowiązek zapewnienia wymaganych warunków bezpieczeństwa lotniczego przez zarządzających lotniskami i portami lotniczymi podlega niemal identycznym normom prawnym, technicznym i operacyjnym, jak w punkcie drugim - powyżej.

W przypadku lotnisk i portów lotniczych, (które w zależności od klasy, bądź kategorii lotniska czy portu lotniczego), muszą bezwzględnie spełniać warunki gwarantujące bezpieczną obsługę statków powietrznych o bardzo zróżnicowanej charakterystyce technicznej, od ultralekkich do transkontynentalnych statków powietrznych.

Zakres niezbędnych działań dla zapewnienia wymaganego poziomu bezpieczeństwa lotniczego, rozpoczyna się już na etapie starań o uzyskanie koncesji na prowadzenie działalności lotniskowej i portowej oraz:

a) wyznacza kierunki prowadzenia prac już w fazie projektowania obiektów, systemów i urządzeń lotniskowych;
b) pod rygorem utraty na stałe lub na czas określony uzyskanych uprawnień, zezwoleń i koncesji w wyniku kontroli prowadzonych przez organa kontroli i nadzoru lotniczego – nakłada obowiązek utrzymania wymaganych kryteriów bezpieczeństwa przez ciągłą aktualizację dokumentacji i doskonalenie procedur i metod w obowiązujących programach ochrony i w operacyjnych planach ratownictwa lotniskowego.

Główne elementy ochrony lotnisk i portów lotniczych

1. Ochrona fizyczna lotniska lub portu lotniczego:
    1. Personel służby ochrony.
    2. Personel nadzoru i kontroli operacyjnej.
    3. Funkcjonariusze Policji.
    4. Funkcjonariusze Straży Granicznej.

2. Dokumentacja:

Podstawowym dokumentem jest program ochrony (lotniska) portu lotniczego, stanowiący część instrukcji operacyjnej, wymagający zatwierdzenia przez zespół ochrony lotnictwa cywilnego – GILC, a w przypadku lotnisk współużytkowanych, również przez WLOP.

Program ochrony (lotniska) portu lotniczego określa szczegółowo:

a) zasady identyfikacji osób i pojazdów oraz uprawnienia w zakresie wstępu, wjazdu i pobytu w danej strefie lotniska lub portu lotniczego przez personel służb lotniskowych, gości i interesantów oraz inne osoby związane z działalnością portową;
b) procedury ochrony strefy ogólnodostępnej;
c) system kontroli parkingów;
d) procedury kontroli dostępu do poszczególnych obiektów i stref lotniska, w tym do stref wymagających specjalnej ochrony;
e) procedury kontroli załóg lotniczych i pasażerów w krajowym i międzynarodowym ruchu lotniczym;
f) procedury kontroli bagażu pod względem bezpieczeństwa;
g) procedury identyfikacji bagażu z pasażerem przylatującym i odlatującym;
h) procedury nadzoru i kontroli osób towarzyszących pasażerom;
i) procedury postępowania z osobami, które naruszyły obowiązujące przepisy;
j) zasady współpracy w zakresie ochrony lotnisk i portów lotniczych ze służbami państwowymi;
k) procedury postępowania z pozostawionymi przedmiotami na terenie lotniska lub portu lotniczego;
l) procedury postępowania w sytuacjach zagrożenia, w tym wykazy telefonów, schematy łączności radiowej, sposób powiadamiania osób odpowiedzialnych za podejmowanie decyzji, wraz z wykazem osób upoważnionych do zastępstwa w przypadku nieobecności.

3. Urządzenia techniczne wspomagające ochronę lotnisk i portów lotniczych:

a) elektroniczne systemy zabezpieczenia pomieszczeń;
b) elektroniczne systemy kontroli i nadzoru:
   - przejść osobowych;
   - bram wjazdowych;
   - ogrodzenia obiektu;
   - stanowisk postoju i parkowania statków powietrznych;
   - urządzenia do prześwietlania bagaży.
c) system kontroli dostępu (przepustek, kart magnetycznych, itd.);
d) telewizja przemysłowa;

e) urządzenia łączności radiowej i telefonicznej, w tym urządzenia do nagrywania rozmów i identyfikacji telefonu rozmówcy;

f) wyposażenie służb ochrony w broń palną lub inne środki przymusu bezpośredniego.

4. Uwarunkowania związane z działalnością prowadzoną na lotnisku lub w porcie lotniczym istotne dla bezpieczeństwa lotniczego:

a) poziom wyszkolenia i utrzymania kwalifikacji personelu ochrony i służb lotniskowych;

b) stan techniczny systemów i urządzeń lotniskowych;

c) natężenie ruchu lotniczego;

d) inne uwarunkowania wynikające z kategorii lotniska lub portu lotniczego, w zależności od tego, czy lotnisko lub port lotniczy obsługuje operacje w nieregularnym lub regularnym ruchu lotniczym, czy port lotniczy jest portem regionalnym, czy międzynarodowym oraz w jakiej fazie organizacyjnej się znajduje, jeżeli sytuacja dotyczy nowych lub modernizowanych, bądź współużytkowanych lotnisk i portów lotniczych.

5. Główne przyczyny powstawania zagrożeń działaniami bezprawnymi wobec lotnictwa cywilnego:

1) Funkcjonowanie portów lotniczych w światowej sieci lotniczych połączeń komunikacyjnych.

2) Możliwość szybkiego przemieszczania się transportem lotniczym, na znaczne odległości.

3) Atrakcyjność czynnika nacisku ze strony grup terrorystycznych dla wymuszenia żądań przez prowadzenie akcji grożącej zniszczeniem i wyłączeniem portów lotniczych z systemu komunikacji lotniczej.

4) Potencjalna możliwość spełnienia żądań stawianych przez terrorystów z pokładu statków powietrznych, pod groźbą pozbawienia życia załóg lotniczych lub pasażerów,

5) Bezwzględne zdecydowanie i desperacja terrorystów stosujących bezpośredni zamach bombowy na terenie lotnisk lub na pokładzie samolotu.

Nietypowe metody działań terrorystycznych na przykładzie zamachu na WTC w Nowym Jorku oraz na Pentagon, jak również ilość ofiar i rozmiary strat, są powszechnie znane. Wymowa tragedii tych zdarzeń, nakazuje się liczyć z dalszymi, trudnymi do określenia w czasie i identyfikacji podobnych zagrożeń, w praktycznie niemożliwym do przewidzenia miejscu na świecie.

Mimo woli nasuwa się pytanie: Czy można było tej tragedii uniknąć? Odpowiedź, niestety musi być przecząca, z uwagi na metody i rodzaj zamachu oraz nigdy dotąd nie notowaną determinację terrorystów. Potoczne opinie oraz „cenne rady'' ze strony „wszystko wiedzących autorytetów'', nie znających specyfiki zagrożeń w lotnictwie, razem z prezentowanymi „gotowymi środkami przeciwdziałania'', w tej konkretnej sytuacji, nie są warte dalszych rozważań.

Żadne państwo – sygnatariusz międzynarodowych konwencji lotniczych, nie miało przecież podstaw do opracowania procedur, na podstawie, których zostały kiedykolwiek (poza stanem wojny), określone okoliczności i uwarunkowania usprawiedliwiające zestrzelenie cywilnego samolotu komunikacyjnego w regularnym, bądź nieregularnym ruchu lotniczym. USA, w dniu 11 września 2001 roku, nie były przecież w stanie wojny z żadnym państwem.

Wystarczy przypomnieć sytuację z początku lat osiemdziesiątych, skalę protestów i oburzenie opinii światowej, gdy radzieckie wówczas siły lotnicze, zestrzeliły w rejonie Sachalinu samolot Boeing 747 Koreańskich Linii Lotniczych z kompletem pasażerów na pokładzie, nie wyczerpując wszystkich procedur postępowania, właściwych do zastosowania wg przepisów międzynarodowych, w sytuacji naruszenia obszaru powietrznego.

Stany Zjednoczone Ameryki Północnej, a wątpię, czy i jakiekolwiek inne państwo na świecie byłoby przygotowane na sytuację, w której potężne liniowe samoloty cywilne zostały kiedykolwiek zastosowane, jako środki rażenia w celu przeprowadzenia ataku na taką skalę. Podjęte środki dla eliminacji podobnych zdarzeń w USA i w skali międzynarodowej, wsparte przez państwa szerokiej koalicji antyterrorystycznej, powinny przywrócić właściwy stan bezpieczeństwa w lotnictwie cywilnym. Pomimo wysokich kosztów niezbędnych dla usunięcia skutków wspomnianych działań terrorystycznych, oraz konieczności dodatkowych nakładów dla zapewnienia bezpieczeństwa i przeciwdziałania podobnym aktom bezprawia, z pewnością nie dojdzie do likwidacji komunikacji lotniczej w skali lokalnej i światowej.

Zakres i charakter międzynarodowych powiązań gospodarczych i stale rosnące potrzeby w zakresie przewozów pasażerskich i towarowych, przy praktycznie jedynej możliwości zapewnienia szybkiego transportu międzynarodowego drogą lotniczą, wykluczają taką ewentualność. Niemniej, w wyniku aktów terroru, jakie wystąpiły w USA, wobec państwa i lotnictwa cywilnego, porty i linie lotnicze na całym świecie poniosły olbrzymie straty, tracąc na jakiś czas, poważny procent pasażerów, szczególnie z grupy tych osób, które dotychczas nigdy nie podróżowały transportem lotniczym, a obecnie będąc pod wrażeniem tragedii, zbyt szybko nie zdecydują się na podróż samolotem.

Trudno jednak nie odnieść się do tych obszarów, w których na skutek niedostatecznego przestrzegania przepisów i procedur określonych w międzynarodowych uregulowaniach prawnych, wielokrotnie i na długo przed wydarzeniami w USA, dochodziło do poważnych zaniedbań w zakresie kontroli pasażerów i ładunków podczas odpraw pasażerskich i towarowych. Duża część tych zaniedbań przypada niestety, na porty lotnicze w USA, co na wniosek organów kontroli i nadzoru lotniczego skutkowało nakładaniem wysokich kar na zarządy portów lotniczych i lotnicze firmy przewozowe. Według źródeł oficjalnych, dostępnych w prasie, w internecie i w biuletynach lotniczych, poważny stopień zaniedbań miał miejsce w porcie lotniczym w Bostonie, z którego zostały uprowadzone dwa samoloty użyte w zamachu na WTC. Można domniemywać, że terroryści nieprzypadkowo wybrali te lotniska, gdzie odprawy pasażerskie nie były zbyt dokładne.

Nie jestem upoważniony i nie czuję się odpowiedzialny za wyciąganie dalszych wniosków w tej sprawie. Czy nie oznacza to jednak, że winni zaniedbań, płacąc wysokie kary, nałożone przez amerykańskie organa kontroli i nadzoru lotniczego, dalej bagatelizowali sprawy bezpieczeństwa i nie czuli się odpowiedzialni za niezwłoczne wdrożenie działań naprawczych.

Czy stwierdzone zaniedbania, można tłumaczyć wyłącznie, jako incydentalne i powstałe w wyniku pracy portów lotniczych w warunkach tzw. stałego deficytu czasowego, gdzie najważniejszy element opłacalność ekonomiczna, jest limitowany utrzymaniem wysokiej zdolności eksploatacyjnej i operacyjnej lotnisk, do obsługi tzw. „strumieni pasażerów'', liczonych w tysiącach osób na godzinę, co z kolei warunkuje zapewnienie terminowego planu połączeń lotniczych.

Ponieważ zamachy terrorystyczne o tak groźnych skutkach miały miejsce w USA, a więc w kraju, który ma największą ilość zarejestrowanych statków powietrznych oraz niezwykle rozwiniętą siatkę lokalnych i międzynarodowych połączeń lotniczych, należy

oczekiwać, iż przy analizie i ocenie sytuacji, weryfikacja procedur bezpieczeństwa została przeprowadzona na wszystkich cywilnych lotniskach amerykańskich. W publikowanych informacjach na temat stanu bezpieczeństwa amerykańskich portów lotniczych, zostały wykazane poważne braki w zakresie wyposażenia lotnisk i portów lotniczych w urządzenia wspomagające ochronę fizyczną oraz umożliwiające pełną kontrolę bagaży, przesyłek i frachtu lotniczego.

W Polsce, również zostały niezwłocznie podjęte działania w zakresie wzmożenia ochrony lotnisk i portów lotniczych oraz kontroli obszaru powietrznego. Zakładam, że zgodnie z wydanymi decyzjami i zaleceniami, każde lotnisko, port i przewoźnik lotniczy wdrożyli procedury przewidziane dla sytuacji szczególnych zagrożeń. Nie wnikam i nie moim zadaniem jest ocena tych działań, ponieważ znaczna część planów i procedur opracowanych dla takich sytuacji wymaga zachowania poufności ze względów oczywistych.

Faktem jest, że po wydarzeniach w USA, w polskiej przestrzeni powietrznej na szczęście nie doszło do zagrożeń o charakterze terrorystycznym i poza utrudnieniami dla pasażerów, nadal nie ma większych zakłóceń w pracy lotnisk i portów lotniczych oraz w komunikacji lotniczej.

Praktycznie oznacza to, że system bezpieczeństwa lotnisk i portów lotniczych w Polsce oraz procedury bezpieczeństwa stosowane przez PLL LOT i innych przewoźników krajowych były na zadowalającym poziomie i w pełnej zdolności do natychmiastowego operacyjnego wdrożenia specjalnych zasad postępowania w sytuacji nadzwyczajnej.

Pamiętam dobrze z okresu mojej pracy w PLL LOT, tematy szkoleń wewnętrznych z zakresu bezpieczeństwa. Te szkolenia z pewnością miały poważny udział w utrzymaniu optymalnego stanu bezpieczeństwa linii lotniczej, a ich zasady obowiązywały od prezesa zarządu do pracownika na ostatnim szczeblu struktury firmy. Nie był to system, który wyłącznie ograniczał się do nakazów i zakazów, lecz inspirował w umiejętny sposób wyobraźnię na każdym stanowisku pracy. W praktyce, skutkowało to niemal natychmiastowym zgłoszeniem każdej wątpliwości wobec nieznanych osób pod względem ich uprawnień w zakresie wstępu na pokład samolotu. Jednocześnie, nikt się nie obrażał, (a wręcz przeciwnie), nawet jeżeli wątpliwości dotyczyły, np. nowego i jeszcze nieznanego personelowi dyrektora. Każdy pracownik, zdawał sobie sprawę, jakie konsekwencje może spowodować pozornie nieistotne zaniedbanie dla linii lotniczej, która

od kilkudziesięciu lat ma swój niekwestionowany udział na światowym rynku usług w transporcie lotniczym.

Potwierdzeniem jakości tego systemu bezpieczeństwa, jest wydanie decyzji władz amerykańskiego nadzoru lotniczego po dokonaniu kontroli w PLL LOT, który po zdarzeniach z 11 września 2001 r., jako drugi europejski przewoźnik lotniczy uzyskał zgodę na wykonywanie operacji lotniczych w obszarze powietrznym USA. Zakładam, że wspomniana zdolność operacyjna będzie podlegała stałej analizie potencjalnych zagrożeń i doskonaleniu metod przeciwdziałania aktom bezprawia i terroru, z którymi należy się nadal liczyć.

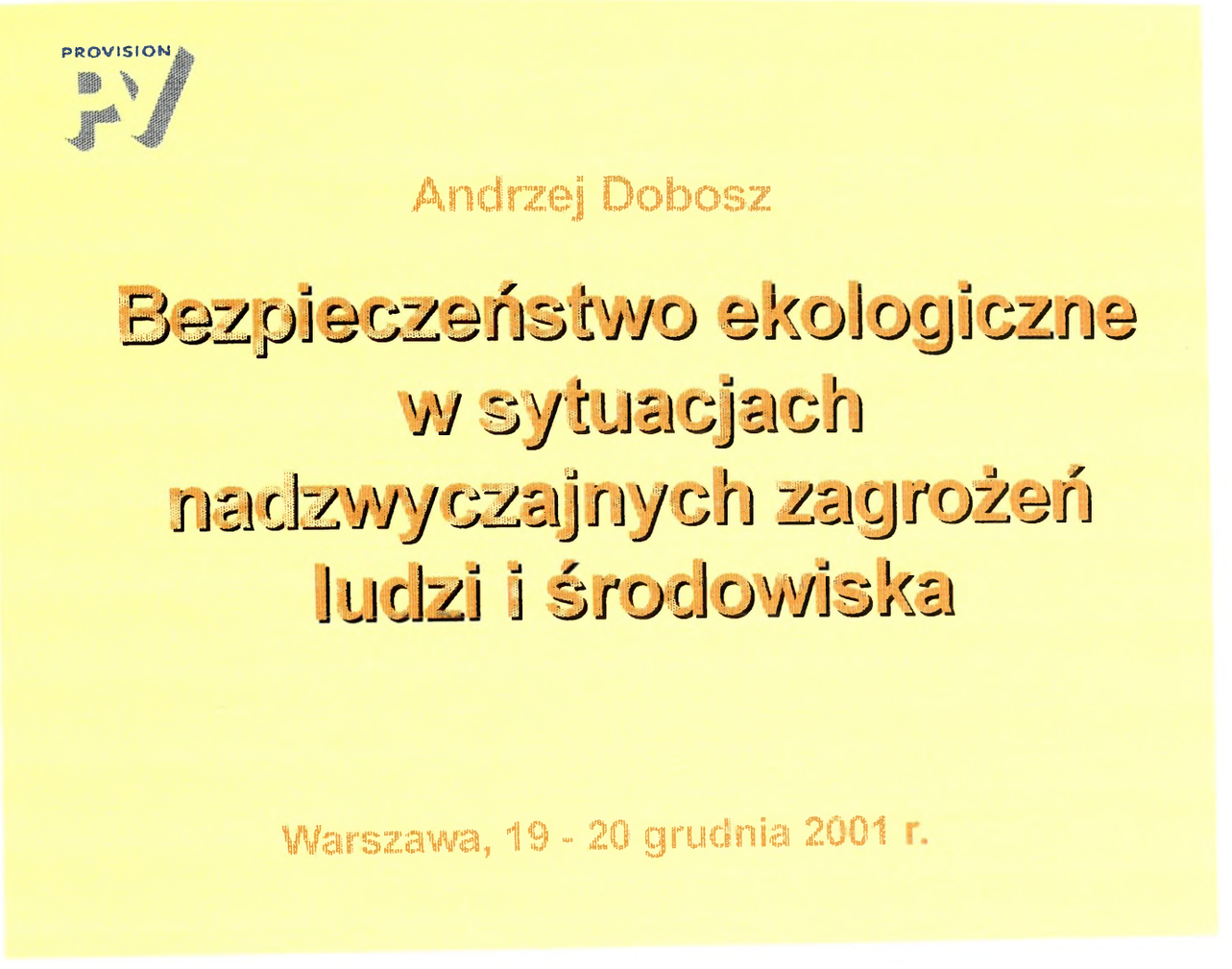
Po zapoznaniu się z osiągnięciami naukowymi, technicznymi i potencjałem zaprezentowanym podczas konferencji przez wojskowe ośrodki naukowe i techniczne oraz firmy uczestniczące, uważam, że wiele rozwiązań, stanowiących dorobek intelektualny i techniczny, powinno znaleźć dalsze praktyczne zastosowanie w gospodarce krajowej, w tym w obszarze stanowiącym o jakości systemów zwiększających bezpieczeństwo lotnisk i portów lotniczych.

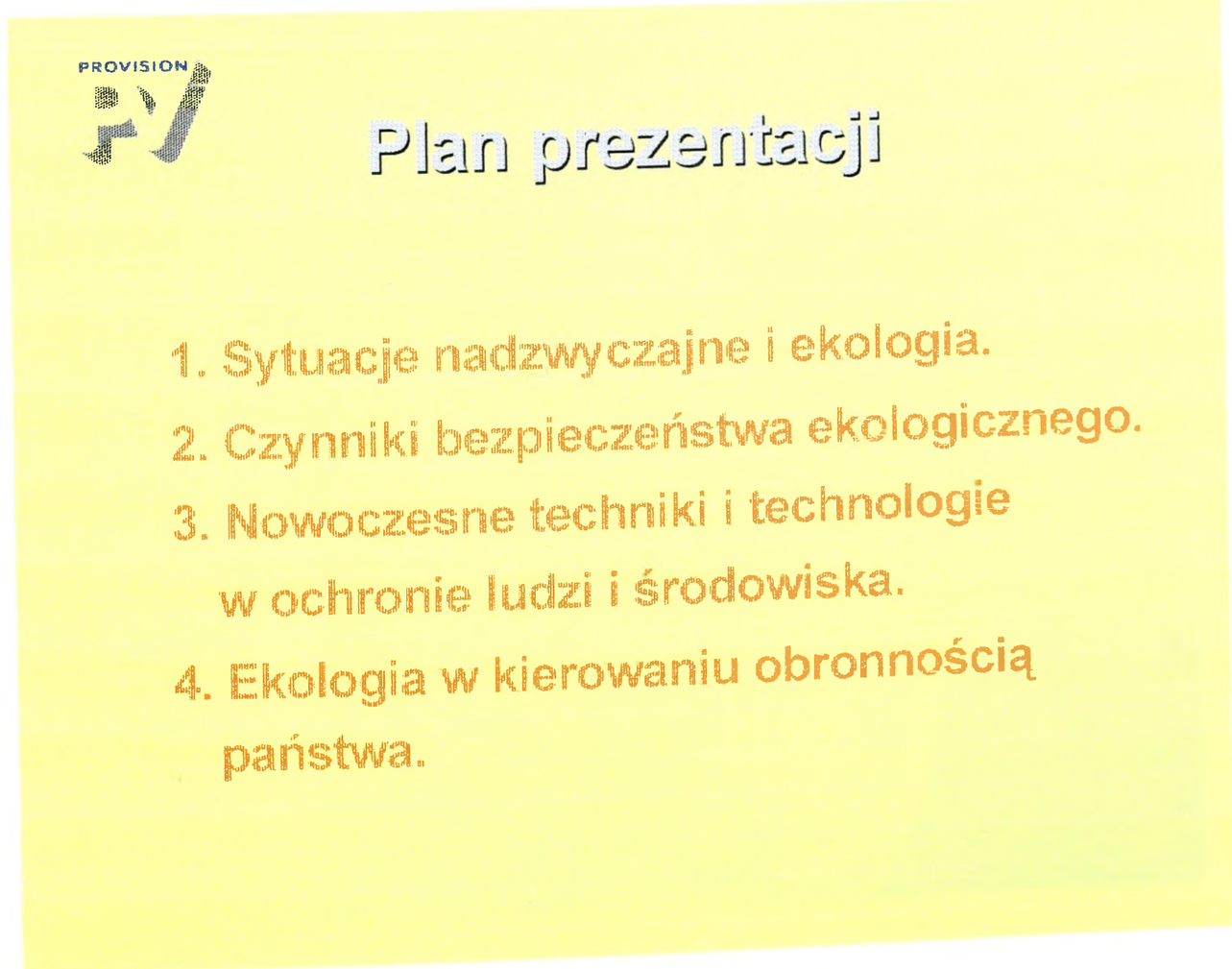
PROVISION Sp. z o.o.
Warszawa

Andrzej DOBOSZ

BEZPIECZEŃSTWO EKOLOGICZNE W SYTUACJACH NADZWYCZAJNYCH ZAGROŻEŃ LUDZI I ŚRODOWISKA

CENTRUM KONFERENCYJNE WP Grudzień 2001


PROVISION
Andrzej Dobosz
Bezpieczeństwo ekologiczne
w sytuacjach
nadzwyczajnych zagrożeń
ludzi i środowiska
Warszawa, 19 - 20 grudnia 2001 r.


PROVISION
Plan prezentacji
1. Sytuacje nadzwyczajne i ekologia.
2. Czynniki bezpieczeństwa ekologicznego.
3. Nowoczesne techniki i technologie
w ochronie ludzi i środowiska.
4. Ekologia w kierowaniu obronnością
państwa.

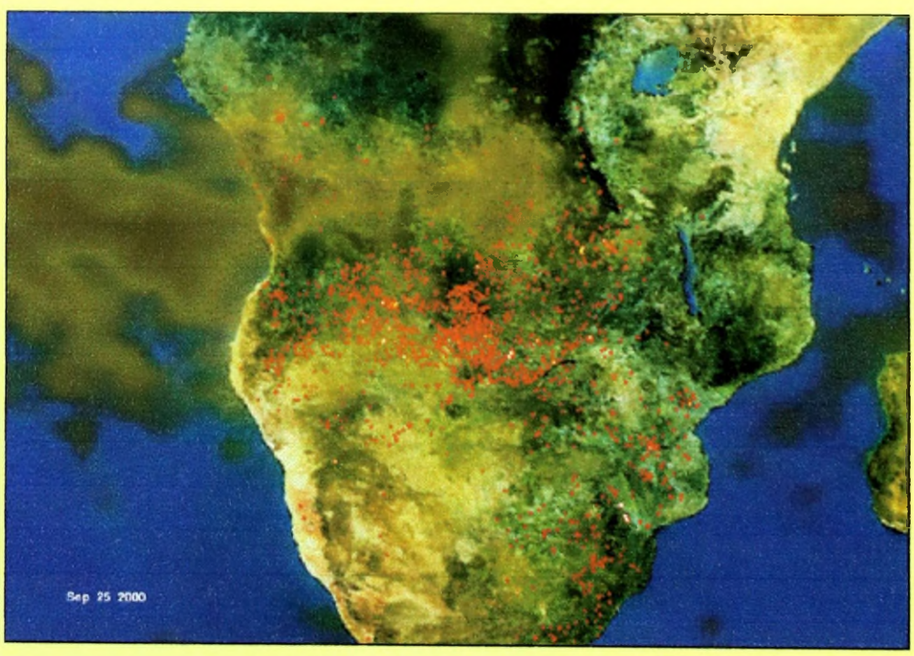
PROVISION

Sytuacje nadzwyczajne i ekologia (1)

1. Klęski żywiołowe, stany wyjątkowe i wojenne.
2. Ograniczenie wolności - ustawa lub rozporządzenie.
3. Aspekty finansowe - wyrównanie strat majątkowych.
4. Procesy zagrożeń - przebieg, działanie, akcja.
5. Planowanie - określenie zagrożeń, ryzyka i skutków.
6. Budowanie systemu zabezpieczeń - ocena stanu bezpieczeństwa.

PROVISION

Sytuacje nadzwyczajne i ekologia



Afryka Południowa
- pożary;
wrzesień 2000 r.

PROVISION

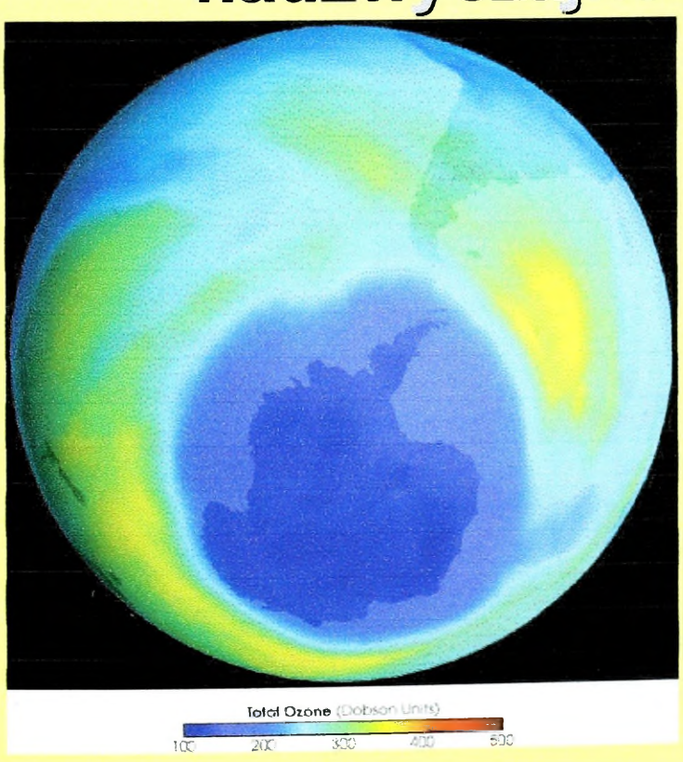
Sytuacje nadzwyczajne i ekologia (2)

Źródła nadzwyczajnych zagrożeń

1. Rozwój cywilizacji - ryzykowne systemy techniczne, efekt cieplarniany, nasilanie się klęsk żywiołowych.
2. Skażenia środowiska (życiodajne zasoby)
   - materiały niebezpieczne, substancje radioaktywne.
3. Pożary, powodzie, trzęsienia na rozległych obszarach.
4. Transport:
   kolejowy, drogowy, lotniczy, wodny (morski), rurociągi.
5. Operowanie zasobami energetycznymi: ropa, gaz, węgiel.

PROVISION

Sytuacje nadzwyczajne i ekologia



Antarktyka
- dziura ozonowa;
sierpień 2001 r.

Sytuacje nadzwyczajne i ekologia (3)

Źródła nadzwyczajnych zagrożeń

6. Epidemiologiczne, epizootyczne.
7. Nowe choroby cywilizacyjne, nierównowaga biologiczna.
8. Systemy masowego niszczenia (NBC).
9. Terroryzm - broń biednych narodów.
10. Działanie wojska w czasie pokoju - katastrofy.

Sytuacje nadzwyczajne i ekologia

Indonezja
- erupcja wulkanu ;
2000 r.

Czynniki bezpieczeństwa ekologicznego (1)

CZŁOWIEK => oddychanie, ciepło, żywność, odpoczynek

ŚRODOWISKO => powietrze, woda, ziemia (flora i fauna)

ODDZIAŁYWANIE => chemiczne, biologiczne, promieniotwórcze, fale elektromagnetyczne

Czynniki bezpieczeństwa ekologicznego (2)

1. Wykrywanie i identyfikacja - system ostrzegania.
2. Informowanie - łączność; systemy komputerowe.
3. Kierowanie ratownictwem - technicznym i medycznym.
4. Unieszkodliwianie - sprzątanie regionu (kraju).
5. Organizacja ochrony - prawo i ekonomika zasoby, personel, procedury.

PEWNOŚĆ OCHRONY- BRAK ZAGROŻENIA FIZYCZNEGO

Nowoczesne techniki i technologie w ochronie ludzi i środowiska (1)

Parametry środowiska - pomiar, wykrywanie i rozpoznanie

1. Sygnalizatory stacjonarne
   - ciągły monitoring, praca w sieci, transmisja danych (PLC).
2. Zdalny pomiar - lidary i termowizja.
3. Nowe podejście do analizy danych.
4. Ochrona indywidualna - mikrotechnologie.
5. Mobilne laboratoria i systemy przenośne.

Nowoczesne techniki i technologie w ochronie ludzi i środowiska (2)

Kierowanie w stanie nadzwyczajnym

1. Informowanie kierownictwa - techniki komputerowe.
2. Informowanie ludności w stanach P i N.
3. Szkolenie - techniki multimedialne.
4. Dowodzenie - agregacja informacji i monitoring.

Nowoczesne techniki i technologie w ochronie ludzi i środowiska (3)

Sztab kryzysowy - kierowanie ratownictwem

1. Współdziałanie - totalna, cyfrowa łączność.
2. Wspomaganie decyzji - systemy okienkowe.
3. Symulacje dynamiczne rozwoju sytuacji.
4. Wczesne ostrzeganie.
5. Przeciwdziałanie, zwalczanie, likwidacja - bazy danych.

Nowoczesne techniki i technologie w ochronie ludzi i środowiska (4)

Likwidacja skutków

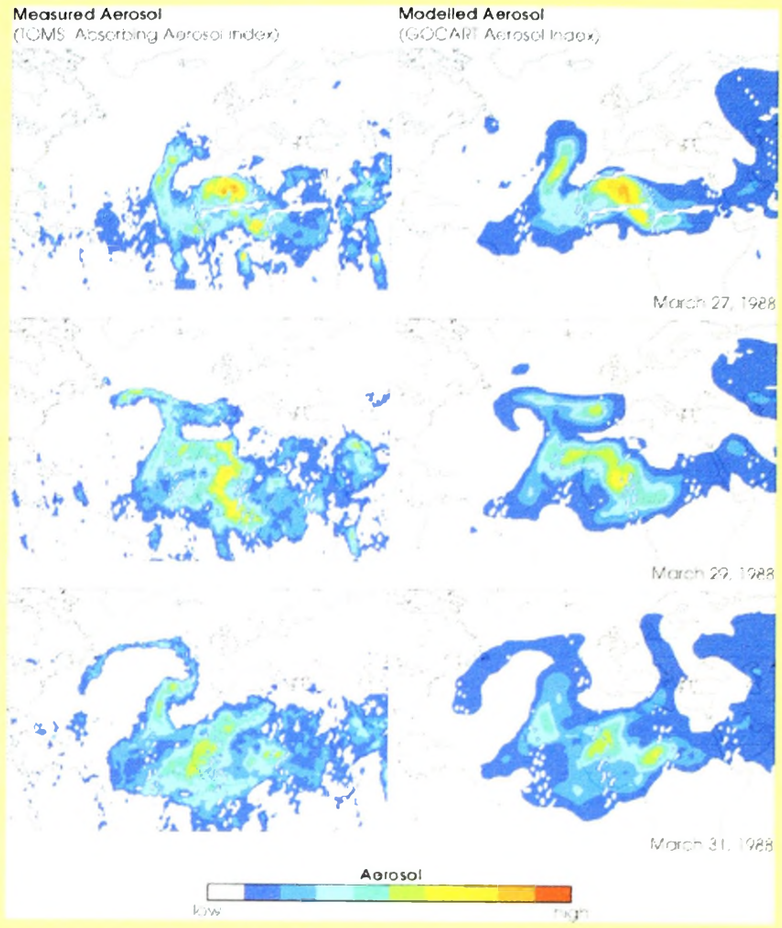
1. Mobilne RCM.
2. Systemy oznakowania terenu.
3. Pomoc medyczna.

Organizacja ochrony

1. Ewidencja i rejestracja (transpondery).
2. Hurtownie danych - dostęp do danych. gminy, powiatu, województwa.
3. Karta tożsamości.
4. Stempel czasu.

PROVISION

Modelowanie przemieszczania się zanieczyszczeń powietrza



PROVISION

Ekologia w kierowaniu obronnością państwa (1)

1. Koncepcja systemu ratowniczo-gaśniczego i bezpieczeństwo ekologiczne.
2. Program i zasady funkcjonowania.
3. Zmiany strukturalne i organizacyjne (urzędy i instytucje odpowiedzialne).
4. Podział zadań, funkcje informacyjne i wykonawcze.
5. Analiza zagrożeń, profilaktyka i likwidowanie.
6. Wiedza naukowa i współpraca międzynarodowa.

PROVISION

Ekologia w kierowaniu obronnością państwa (2)

1. Stan gotowości obronnej i jego weryfikacja.
2. Ustalenie norm i standardów.
3. System odpowiedzialności cywilnej (ubezpieczenia).
4. Równorzędna współpraca z krajami Unii Europejskiej.
5. Świadomość ekologiczna społeczeństwa.

Koncepcja strategiczna NATO (listopad 1991) - postrzeganie bezpieczeństwa ekologicznego

PROVISION

Andrzej Dobosz

ProVision Sp. z o.o.
ul. Goworowska 4
03-363 Warszawa

tel. (22) 811 27 16
tel. kom 0602 - 65 84 60
e-mail: prov001@pol.pl

ADVICE Sp z oo
COMMUNICATION

Advice Communication Sp. z o.o.
Warszawa

Eugeniusz PIEDZIUK

BEZPIECZEŃSTWO INFORMACJI W SIECIACH TELEINFORMATYCZNYCH

CENTRUM KONFERENCYJNE WP Grudzień 2001

W ostatnich latach nastąpił w Polsce gwałtowny rozwój infrastruktury teleinformatycznej. Sytuacja ta umożliwiła szerokie wykorzystywanie w procesach zarządzania i kierowania nowoczesnych technik przekazu i przetwarzania informacji. Znaczenie obiegu informacji[77] w instytucji państwowej, przedsiębiorstwie, organizacji militarnej, czy też koncernie działającym w sieci globalnej, porównać można do znaczenia krwioobiegu w organizmie ludzkim. Każda organizacja dysponująca informacjami, wykorzystuje do ich przechowywania, przetwarzania i przesyłania systemy teleinformatyczne.[78] Przesyłane informacje wykorzystywane przez użytkowników systemów mogą być chronione i niepodlegające ochronie. Informacje chronione to takie, które są nakazane przez obowiązujące przepisy prawne lub wskazywane przez kompetentne organy użytkowników. Ochrona informacji jest zagadnieniem bardzo szerokim, zasadniczo jest związana z bezpieczeństwem teleinformatycznym i obejmuje wszystkie formy wymiany informacji za pomocą szerokiej gamy technicznych środków łączności. Kompleksowa ochrona informacji w sieciach teleinformatycznych obejmuje aspekt prawny, zabezpieczenia fizyczne i techniczne oraz organizacyjne, ochronę przed emisją ujawniającą, a także ochronę kryptograficzną.

Bezpieczeństwo teleinformatyczne określa ochronę informacji przetwarzanej, przechowywanej i przesyłanej za pomocą systemów teleinformatycznych, przed niepożądanym ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania.

Podstawowe parametry informacji związane z jej bezpieczeństwem:

- tajność;
- dostępność;
- integralność.

Przez tajność należy rozumieć, że dostęp do określonych informacji i danych posiadają wyłącznie uprawnione osoby. Dostępność odnosi się do systemu teleinformatycznego i oznacza dostęp do danych, procesów i aplikacji zgodnie z potrzebami i wymaganiami użytkowników. Integralność oznacza, że informacje oraz dane są poprawne i nie zostały naruszone.

---

[77]Informacja - jakakolwiek wiedza, która może być przechowywana, przetwarzana lub przesyłana. Informacja niejawna - informacja, która wymaga ochrony przed nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem, oznaczona odpowiednią klauzulą tajności.

[78]Systemy teleinformatyczne - urządzenia, narzędzia, metody postępowania, procedury oraz personel zorganizowany w taki sposób, aby zapewnić funkcje przechowywania, przetwarzania i przesyłania informacji.

Ochrona systemu teleinformatycznego polega na niedopuszczeniu do korzystania z niego nieupoważnionym użytkownikom oraz na niedopuszczeniu do stanu, w którym system byłby niezdolny do realizacji swojej funkcji lub realizował je w sposób niezgodny z wymaganiami użytkowników. Schemat ochrony informacji w sieci teleinformatycznej przedstawiono na rys.1.

Rys.1. Schemat ochrony informacji w sieci teleinformatycznej

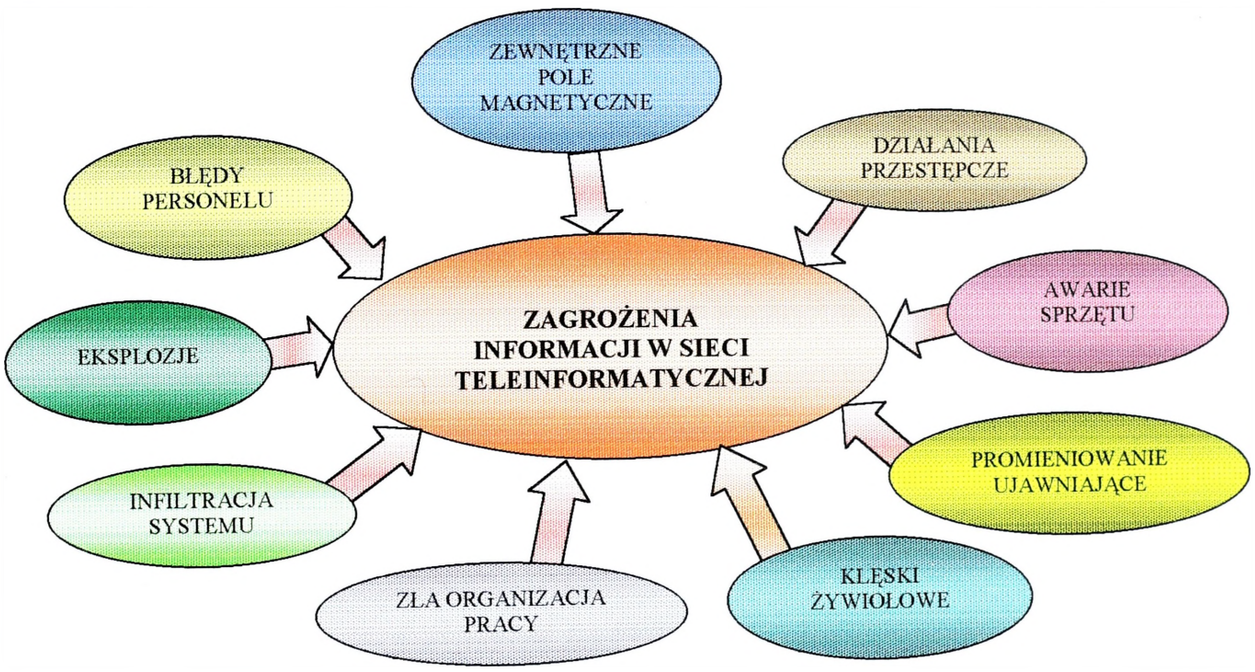
Specyfika eksploatacji sieci teleinformatycznej powoduje występowanie szeregu czynników sprzyjających powstawaniu zagrożeń bezpieczeństwa informacji. Klęski żywiołowe, działania przestępcze, potencjalne możliwości nieuprawnionego działania w sieci teleinformatycznej jej użytkowników lub osób nie będących jej użytkownikami i inne, ogólnie nazywane są zagrożeniami. Poznanie ich pozwala prawidłowo projektować strukturę systemu, oraz konstrukcję i funkcje urządzeń. Na podstawie danych statystycznych pozyskanych z firm można stwierdzić, że największe zagrożenie dla systemu teleinformatycznego stanowią czynniki związane z fizycznym uszkodzeniem lub awarią sprzętu, niż działania przestępcze związane z kradzieżą bądź manipulacją informacji, które są zwykle uważane za największe zagrożenie.

Ogólnie zagrożenia dla bezpieczeństwa informacji można podzielić na:

- klęski żywiołowe, np.: pożar, powódź, zalanie wodą, trzęsienie ziemi, agresywne gazy i środki chemiczne;
- działania przestępcze, np.: kradzież sprzętu i oprogramowania;
- promieniowanie ujawniające, zewnętrzne pole magnetyczne;
- infiltracja systemu bierna i czynna;

- zła organizacja pracy, np.: nieprzestrzganie lub brak odpowiednich przepisów
- błędy personelu obsługującego system;
- awarie sprzętu i wady oprogramowania.

Ogólne zagrożenia bezpieczeństwa informacji przedstawiono schematycznie na rysunku 2.



Rys. 2. Ogólne zagrożenia bezpieczeństwa informacji

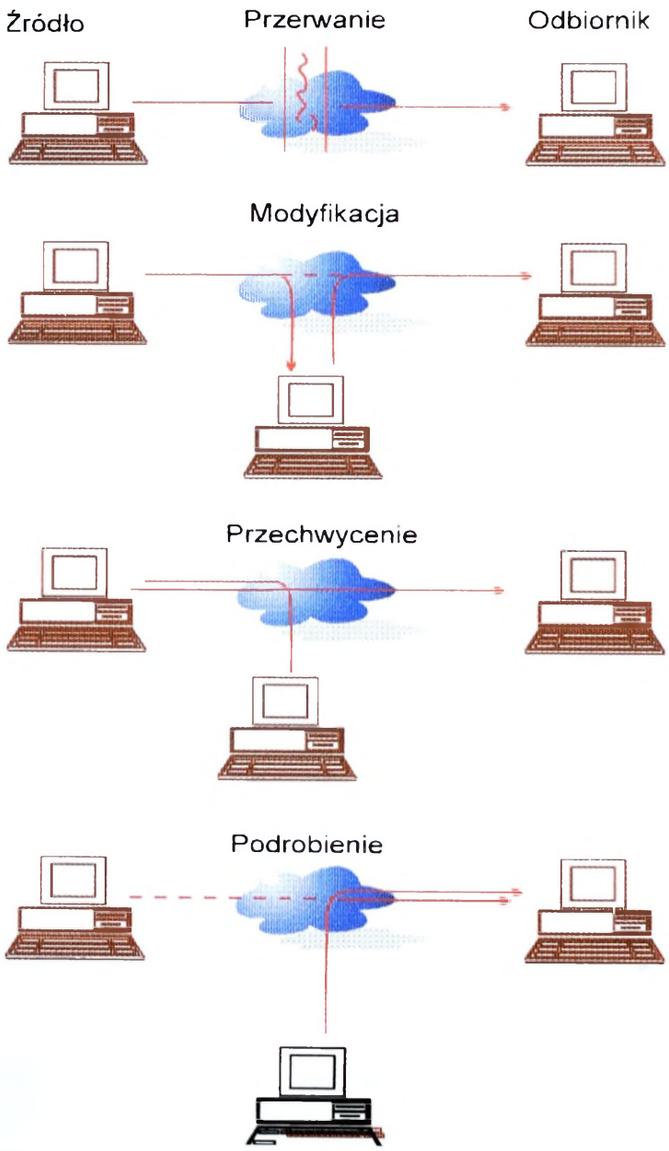
Do czynników sprzyjających powstawaniu zagrożeń bezpieczeństwa informacji zaliczyć należy:

- rozproszenie zasobów informatycznych na dużym terenie;
- eksploatowanie niewłaściwego sprzętu komputerowego i „pirackiego" oprogramowania (systemowego lub użytkowego);
- stosowanie do ochrony informacji nieetatowych środków ochrony (mechanizmów programowych i urządzeń technicznych);
- stosowanie sprzętu i oprogramowania nie sprawdzonego na obecność tzw. „pluskiew" programowych i sprzętowych;
- niechęć użytkowników i projektantów do stosowania środków ochrony informacji;
- niedocenianie zagrożeń bezpieczeństwa informacji przez użytkowników.

Ponadto zagrożeniami bezpieczeństwa informacji mogą być następujące elementy:

- ujawniająca emisja elektromagnetyczna komputerów, terminali i aparatury kanałowej oraz wrażliwość tych elementów na zakłócenie elektromagnetyczne;
- możliwość zdalnej penetracji zasobów informatycznych systemu;
- dołączanie podsłuchowych urządzeń rejestrujących;
- dołączanie niesankcjonowanych terminali;
- nielegalne wykorzystanie terminali użytkowników;
- stosowanie nielegalnego oprogramowania;
- czynniki losowe: pożary, powodzie, zakłócenia w komutacji i transmisji;
- awarie urządzeń, zaniki napięcia;
- niesolidność personelu - niedoszkolenie, bezmyślność lub szantaż.

Zagrożenia bezpieczeństwa informacji w sieci przedstawiono na rysunku 3.



Rys. 3. Zagrożenia bezpieczeństwa informacji w sieci teleinformatycznej

Zagrożenia mogą występować przypadkowo lub być skutkiem przestępczego działania celowego związanego z atakiem na informację w celu naruszenia przede wszystkim jej tajności, integralności i dostępności. Natomiast celowe działania przestępcze związane z atakiem na system, mogą być realizowane bez aktywnego oddziaływania (atak pasywny) lub z oddziaływaniem na system (atak aktywny). Atak pasywny polega na podsłuchiwaniu (szeroko pojętym) i monitorowaniu przesyłanych informacji. Celem ataku pasywnego może być dążenie do ujawnienia treści wiadomości lub uzyskanie informacji o samym ruchu informacji. Atak pasywny to szeroko rozumiany podsłuch lub podgląd w celu zdobycia informacji niejawnej i/lub analiza ruchu w sieci dla zlokalizowania ważnych obiektów i stanowisk kierowania. Jest on najczęściej etapem przygotowawczym do wykonania ataku aktywnego na system. Atak aktywny dąży do modyfikowania strumienia informacji lub tworzenia fałszywych informacji. W działaniach tych mieszczą się: podszywanie się pod osobę uprawnioną i blokowanie działania. Rezultatem skutecznego ataku na system może być zmiana jego stanu i sposobu działania.

Istnieją różne metody zablokowania systemu teleinformatycznego. Jedną z najprostszych do przeprowadzenia metod jest atak polegający na tak silnym przeciążeniu działania systemu wówczas praca w nim okazuje się niemożliwa. Ten rodzaj sabotażu może sparaliżować pracę organizacji w takim stopniu, że nie będzie ona mogła normalnie funkcjonować. Napastnik zaleje system falą komunikatów, listów elektronicznych, połączeń modemowych i żądań usług sieciowych w tak dużym stopniu, że system nie będzie praktycznie robił nic poza próbami wykonania tych wszystkich zleceń. Bardziej wyrafinowane ataki polegają na przekierowywaniu żądań usług systemu w inne, zupełnie niewłaściwe miejsca. Znany jest przykład takiego przeprogramowania połączeń modemowych, że każde połączenie było kierowane na przypadkowy błędny numer. Szczególną bolączką jest fakt, że ochrona przed blokadą usług systemu jest bardzo trudna, w praktyce wiąże się z izolowaniem systemu od otoczenia sieciowego.

Zagrożenia atakiem występują, gdy istnieją możliwości:

1. Nieuprawnionego dostępu do przechowywanych, przetwarzanych lub przesyłanych informacji niejawnych.
2. Nieuprawnionego oddziaływania na system.

Wykorzystanie nieuprawnionego oddziaływania na system, może powodować:

- zmiany w funkcjonowaniu sieci teleinformatycznej, w tym przerwanie lub czasowe zablokowanie usług realizowanych przez sieć;
- dostęp do przesyłanych, przetwarzanych lub przechowywanych informacji;

- dezinformację;
- zniszczenie informacji lub innych zasobów;
- fałszowanie lub nieuprawnioną modyfikację informacji.

Przyszli użytkownicy systemów, urządzeń czy też oprogramowania, które mają służyć do przechowywania, przetwarzania i przesyłania informacji o charakterze niejawnym, muszą mieć pewność, że wyrób który zamierzają kupić spełnia wymagania bezpieczeństwa teleinformatycznego. Wiara w werbalne zapewnienia producentów czy dealerów o bezpieczeństwie teleinformatycznym tej kategorii wyrobów jest niewystarczająca. Użytkownik powinien polegać na wynikach formalnej i bezstronnej oceny, dokonanej przez uprawniony do tego organ. Ocena wyrobu wymaga dobrze zdefiniowanego kryterium oceny zabezpieczenia oraz istnienia jednostki certyfikującej, uprawnionej do wydania potwierdzenia, że oceny dokonane przez laboratorium badawcze zostały przeprowadzone właściwie. Ocena możliwości zabezpieczających systemu może być rozpatrywana jako część większej formalnej procedury przyjęcia systemu teleinformacyjnego do stosowania w konkretnym środowisku.

Znane dzisiaj metody ochrony informacji nie gwarantują absolutnego bezpieczeństwa i dalekie są od ideału, a zjawiska włamań do sieci nie dają się wyeliminować. Włamania do systemów teleinformatycznych przynoszą znaczne straty finansowe i często utratę zaufania do instytucji, której powierzono poufne informacje. Środki ochrony, zmniejszające ryzyko uzyskania dostępu do danych przez osoby nieupoważnione, można ogólnie podzielić na dwie kategorie:

1. Ograniczenie dostępu do zasobów systemu zgodnie z ustaloną polityką ochronną organizacji.
2. Kodowanie informacji (utajnianie) za pomocą metod kryptograficznych.

Ochrona kryptograficzna, chociaż ma zasadnicze znaczenie, sama nie gwarantuje pełnego bezpieczeństwa informacji. Jeśli informacja jest szyfrowana, ale nie ma fizycznych ograniczeń w dostępie do systemu lub brak jest zabezpieczeń przed emisją ujawniającą, to szyfrowanie nie zapewni wysokiego poziomu bezpieczeństwa. Celem kryptograficznej ochrony informacji w systemie teleinformatycznym jest:

- wyeliminowanie dostępu do zasobów podsystemu osobom nieuprawnionym;
- zapewnienie dostępu do zasobów użytkownikom w ramach ich uprawnień;
- zapewnienie poufności informacjom niejawnym na dyskach;

- zapewnienie poufności, integralności i uwierzytelniania informacjom niejawnym.

Kryptograficzne metody ochrony są ważnym elementem bezpieczeństwa informacji w sieciach teleinformatycznych. Odpowiednio zaprojektowane i wdrożone szyfry zdecydowanie ograniczają możliwości działania nawet wyrafinowanego przeciwnika. Brak kryptograficznej ochrony informacji w sieci może powodować, że bezcelowe są inne działania np. ochrona przed emisją ujawniającą. Istnieje szereg różnych metod i środków ochrony informacji. Do podstawowych metod i środków można zaliczyć:

1. Metody organizacyjno - administracyjne:
   - ograniczenie dostępu do informacji niejawnych;
   - ograniczenie uprawnień osób funkcyjnych w systemie zarządzania;
2. Metody i środki programowe:
   - hasła dostępu do zbiorów;
   - uprawnienia;
   - uwierzytelnienie i identyfikacja;
   - zamknięte grupy użytkowników;
3. Środki techniczne:
   - osłony ekranujące;
   - kabiny ekranujące;
   - ekranowanie pomieszczeń;
   - urządzenia o obniżonym poziomie ujawniającej emisji elektromagnetycznej;
   - światłowody;
   - środki ochrony przed nieuprawnionym dostępem do sprzętu;
   - środki ochrony przed nieuprawnionym dostępem do programów;
4. Szyfrowanie informacji:
   - szyfrowanie kanałowe;
   - szyfrowanie baz danych;
   - uwierzytelnianie użytkownika.

Usługi ochrony danych zapewniają uzyskanie pewnych gwarancji w zakresie wiarygodności systemu teleinformatycznego:

- poufność - ochrona przed atakiem pasywnym;
- uwierzytelnienie - zapewnienie autentyczności informacji i osób: zagwarantowanie, że informacja pochodzi z takiego źródła, które jest przy niej wymieniane lub też osoba jest tą, za którą się podaje;

- nienaruszalność - zapewnienie integralności komunikacji, tzn. tego, że informacja jest odbierana w takiej postaci, w jakiej została wysłana;
- niezaprzeczalność - niemożliwość zaprzeczenia faktowi wysłania lub odebrania informacji;
- kontrola dostępu - możliwość kontrolowania dostępu do informacji (systemów) drogą identyfikacji i uwierzytelniania;
- dyspozycyjność - ograniczanie skutków ataku w sferze dostępności informacji.

Mechanizmy zabezpieczające wiarygodność informacji obejmują działania:

- szyfrowanie;
- uwierzytelnianie (podpisy cyfrowe);
- ochrona antywirusowa;
- identyfikacja osób uprawnionych.

W specjalistycznej literaturze spotyka się często pojęcie, że urządzenia elektroniczne wytwarzają promieniowanie elektromagnetyczne, które może być związane z przetwarzaną informacją, jednak to stwierdzenie jest truizmem. Ta konstatacja spowodowała, że w Stanach Zjednoczonych pod koniec lat 50-tych zapoczątkowano specjalny program badawczy pod kryptonimem TEMPEST[79].

Bezpieczeństwo emisji związane jest ściśle z normami dotyczącymi tego zagadnienia (zazwyczaj są to normy niejawne). Należy jednakże podkreślić, że poszczególne kraje członkowskie NATO niezależnie od zobowiązań, stosują swoje narodowe normy, które stworzyły swoje wymagania nie udostępniane innym krajom, nawet sojusznikom.

Zabezpieczenie komputerów oraz sieci przed emisją ujawniającą w wielu instytucjach i urzędach centralnych z przedstawionych powyżej przyczyn nie jest najlepsze, a szczególnie w instytucjach placówkach naukowych. Można mieć nadzieję, że w najbliższych latach, konieczność tworzenia społeczeństwa informacyjnego, a przede wszystkim obecności państwa w strukturach NATO i UE pozwoli na nadrobienie zaistniałych zaległości i stworzenia skutecznych systemów zabezpieczeń i ochrony informacji w systemach teleinformatycznych jak i w samych komputerach.

---

[79]TEMPEST jest oficjalnym akronimem dla „Telecommunications Electronics Material Protected from Emanating Spurious Transmissions" i zawiera techniczne środki bezpieczeństwa, standardy i oprzyrządowanie, które zapobiegają (ewentualnie minimalizują) wykorzystaniu słabych punktów bezpiecznych systemów.

Ocena zagrożeń jest pierwszym etapem pracy przy analizie bezpieczeństwa sieci oraz systemów teleinformatycznych.

Analiza bezpieczeństwa informacji w sieciach i systemach teleinformatycznych obejmuje.

a) identyfikację słabych punktów systemu;
b) analizę prawdopodobieństwa występowania zagrożeń z uwzględnieniem słabych punktów systemu;
c) ocenę konsekwencji wykorzystania każdego zagrożenia indywidualnie oraz w powiązaniu z innymi zagrożeniami;
d) oszacowanie kosztów każdego ataku (w tym ocenę na ile udany atak ułatwia następne);
e) oszacowanie kosztów potencjalnych środków przeciwdziałania, w tym również ewentualnego pogorszenia parametrów funkcjonalnych systemu.

Następnym etapem realizacji ochrony informacji powinno być zrealizowanie przedsięwzięć organizacyjno-administracyjnych z uwzględnieniem następujących zasad:

1. Informacja powinna być przekazana, udostępniona lub przedstawiona do oceny tylko tym użytkownikom, którzy są do tego odpowiednio uprawnieni.
2. Użytkownicy powinni mieć dostęp do zasobów tylko w zakresie swojego uprawnienia.
3. Każda próba nieuprawnionego działania w systemie powinna być wykrywana, rejestrowana i sygnalizowana służbom nadzoru.
4. Działania użytkowników systemu łączności, powinny być rejestrowane w dzienniku kontrolnym z podaniem danych identyfikujących użytkownika, rodzaju i terminu wykonywanej operacji.
5. O prowadzeniu dziennika użytkownicy powinni być poinformowani, ale nie powinni mieć do niego dostępu. Dostęp do dziennika powinien być zagwarantowany dla służb nadzoru.

Kolejnym etapem powinien być więc wybór odpowiednich urządzeń utajniających, w których powinny być zainstalowane następujące niezbędne elementy:

- ściśle sprecyzowane algorytmy obsługi, uwzględniające wprowadzenie hasła;
- konieczność pracy z identyfikatorem osobistym, wykorzystywanym m.in. do tworzenia grup użytkowników;
- segmenty realizujące funkcje archiwizacji podstawowych zdarzeń;
- segmenty realizujące procedury zdalnej dystrybucji;

- procedury transmisyjne;
- algorytmy zabezpieczające dane kluczowe przechowywane w urządzeniach.

Bezpieczeństwo sieci teleinformatycznej to nie tylko środki techniczne i programowe systemów ochrony. Bezpieczeństwo to, zarówno problem środków ochrony, jak i zarządzania zasobami danych oraz informacją. Jest ono w rzeczy samej pochodną dobrej organizacji i właściwej polityki ochrony wprowadzanej na wszystkich szczeblach organizacyjnych.

Problem ochrony sieci teleinformatycznej instytucji bądź firmy należy rozpatrywać na wszystkich szczeblach struktury organizacyjnej. Polityka ochrony musi być jednoznaczna i przejrzysta, a każdy pracownik instytucji czy też firmy powinien być z nią zaznajomiony. Sama technologia nie może zapewnić pełnego bezpieczeństwa sieci teleinformatycznej. Ochrona przekazywanych informacji w sieciach teleinformatycznych to przede wszystkim właściwe zarządzanie i organizacja.

Bibliografia:

1. Jańczak J.; *Zakłócanie informacyjne*, AON, Warszawa 2001.
2. Jemioło T.; *Globalizacja szanse i zagrożenia*; AON, Warszawa 2000.
3. Kaeo M.; *Tworzenie bezpiecznych sieci*, Mikom, Warszawa 2000.
4. Kwećka R.; *Informacja w walce zbrojnej*, AON, Warszawa 2001.
5. Liderman K.; *Bezpieczeństwo informacji w sieciach komputerowych*, WAT 1999.
6. Materiały z konferencji; *Bezpieczeństwo – być na bieżąco*, Forum Secure 2000, Warszawa 2000.
7. Praca studyjna; *Kierowanie obronnościa państwa. Bezpieczeństwo systemów telekomunikacyjnych*, AON Warszawa 2000.
8. Sportack M.; *Sieci komputerowe. Księga eksperta*, Helion, Gliwice 1999.
9. Zięba R.; *Nowa instytucjonalizacja bezpieczeństwa europejskiego*, AON, Warszawa 1998.

Wojskowy Instytut Łączności
Zakład Doświadczalny

Ryszard FLORYŃSKI
Mieczysław OLSZÓWKA

ELEKTROMAGNETYCZNA OCHRONA INFORMACJI NIEJAWNYCH W SYSTEMACH TELEINFORMATYCZNYCH

CENTRUM KONFERENCYJNE WP Grudzień 2001

Ochrona informacji jest we współczesnym świecie traktowana jako jeden z najistotniejszych warunków bezpieczeństwa interesów społeczności narodowych, finansowych, przemysłowych a nawet przestępczych. W większości państw ochrona informacji, stanowiących tajemnice państwowe lub służbowe istotne dla bezpieczeństwa narodowego, jest unormowana prawnie. Również w naszym kraju już od dwóch lat obowiązuje ustawa z dnia 22 stycznia 1999 r. „O ochronie informacji niejawnych". Jednocześnie prawodawstwa zdecydowanej większości państw umożliwiają służbom czuwającym nad bezpieczeństwem narodowym jak najdalej idącą kontrolę nad wszystkimi aspektami przetwarzania, przechowywania i przesyłania informacji.

Już na wstępie należy zaznaczyć, że współczesna ochrona informacji stanowi zespół bardzo poważnych problemów organizacyjno-technicznych i wymaga stosowania bardzo zaawansowanych technik i mechanizmów. Wynika to z konieczności konstrukcji i eksploatacji kompleksowego systemu ochrony informacji, które w różnym czasie podlegają przetwarzaniu, przechowywaniu i przesyłaniu w systemach teleinformatycznych współczesnej generacji.

Jeszcze do niedawna w kraju naszym problematyka ochrony informacji przed przenikaniem elektromagnetycznym była znana tylko w stosunkowo wąskim kręgu specjalistów pracujących głównie na potrzeby instytucji wojskowych lub służb ochrony państwa. Jednakże sytuacja zmieniała się z chwilą wejścia w życie ustawy z dnia 22 stycznia 1999 roku (o ochronie informacji niejawnych). Ustawa ta w sposób obligatoryjny nakłada na instytucje finansowane ze środków publicznych obowiązek stosowania do przetwarzania informacji niejawnych stanowiących tajemnicę państwową lub służbową urządzeń teleinformatycznych w specjalny sposób zabezpieczonych pod względem ochrony informacji przed przenikaniem elektromagnetycznym. Ponadto większość instytucji z własnej inicjatywy pragnie zapewnić ochronę przetwarzanych przez siebie informacji.

Termin ochrona informacji przed przenikaniem elektromagnetycznym lub (równoważne mu sformułowanie) bezpieczeństwo emisji są dość popularne, jednakże nie zawsze poprawnie interpretowane. Dlatego też właściwym wydaje się na samym początku określić przedmiot naszego zainteresowania. Pod pojęciem ochrony informacji przed przenikaniem elektromagnetycznym rozumieć będziemy zespół przedsięwzięć organizacyjnych i technicznych mających na celu zapewnienie takiego stanu zabezpieczenia obiektu lub urządzenia, w którym niemożliwe jest prowadzenie infiltracji elektromagnetycznej. Infiltracja elektromagnetyczna to wszelkie (wykorzystujące zjawisko

przenikania elektromagnetycznego) działania zmierzające do odtworzenia informacji przesyłanej, przetwarzanej lub przechowywanej w systemach łączności i informatyki. Zjawisko elektromagnetyczne przenikania informacji związane jest z istnieniem emisji ujawniającej czyli niepożądanej emisji sygnałów, których pewne cechy związane są z informacją użyteczną. Sygnały takie, mające charakter emisji promieniowanych lub przewodzonych, w przypadku ich odebrania i poddawania stosownej obróbce umożliwić mogą odtworzenie związanej z nimi informacji.

Na przestrzeni bez mała czterdziestu lat powstało szereg dokumentów, szczegółowych instrukcji i procedur dotyczących ochrony elektromagnetycznej sprzętu przeznaczonego do przetwarzania informacji niejawnych. Dokumenty związane z programem TEMPEST w większości mają charakter niejawny, udostępniane są tylko osobom upoważnionym zgodnie z zasadą „need-to-know".

Organizacja Paktu Północno-Atlantyckiego (NATO) na potrzeby swojego funkcjonowania posiada własne wymagania dotyczące ochrony informacji przed przenikaniem elektromagnetycznym. Wymagania te zostały zdefiniowane w roku 1982 i zawarte zostały w dokumencie AMSG 720B noszącym tytuł „Compromising Emanations Laboratory Tests Standard". Wymagania tego dokumentu zbieżne są z wymaganiami pierwszego poziomu dokumentu NSTISSAM TEMPEST/1-92. Mniej restrykcyjne wymagania zawierają dokumenty AMSG 788A i 784, które odpowiadają odpowiednio wymaganiom NSTISSAM TEMPEST/1-92-Level II oraz NSTISSAM TEMPEST/1-92-Level III. Poszczególne kraje członkowskie NATO posiadają oczywiście również własne wymagania i pracujące na potrzeby swoich rządów instytucje zajmujące się ochroną informacji przed przenikaniem elektromagnetycznym.

Ustawa o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (Dz. U. Nr 11, poz. 95) zastąpiła obowiązującą wcześniej ustawę z dnia 14 grudnia 1982 r. o ochronie tajemnicy państwowej i służbowej. Rozdział 10 obowiązującej obecnie ustawy poświęcony został bezpieczeństwu systemów i sieci teleinformatycznych. W rozdziale tym mówi się o konieczności określenia podstawowych wymagań w zakresie między innymi ochrony elektromagnetycznej i bezpieczeństwa transmisji w sieciach lub systemach teleinformatycznych służących do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych.

Uzupełnieniem powyższego wymagania jest rozporządzenie prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. z 1999 r. Nr 18, poz. 162).

Rozporządzenie owo stwierdza, że:

„ochronę elektromagnetyczną systemu lub sieci teleinformatycznej zapewnia się przez umieszczenie urządzeń, połączeń i linii w strefach bezpieczeństwa gwarantujących spełnienie wymogów zabezpieczenia elektromagnetycznego lub zastosowanie urządzeń, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie i filtrowanie zewnętrznych linii zasilających i sygnałowych".

ZD WIŁ jest jedynym w kraju zakładem specjalizującym się w opracowaniu i produkcji urządzeń utajniających i urządzeń ochrony informacji. Główne kierunki opracowań i działalności produkcyjnej to:

- urządzenia dla ochrony informacji i zabezpieczenia kompatybilności elektromagnetycznej (kabiny ekranujące KE-100 i bezpieczne stanowiska komputerowe BSK);
- cyfrowe urządzenia utajniające (kryptograficzne) – grupowe i indywidualne;
- urządzenia elektroniczne dla cyfrowych sieci telekomunikacyjnych;
- urządzenia i elementy światłowodowe polowych węzłów łączności;
- systemy i elementy zasilania polowych i stacjonarnych urządzeń łączności.

Wyżej wymienione urządzenia produkowane są dla MON od sześciu lat z serwisem gwarancyjnym i pogwarancyjnym. Zakład Doświadczalny WIŁ posiada pełne zabezpieczenie do produkcji urządzeń specjalnych, a wszystkie urządzenia dla elektromagnetycznej ochrony informacji podlegają odbiorowi wojskowemu (96 RPW) i każde z nich posiada certyfikat jakości. W chwili obecnej ZD WIŁ specjalizuje się w osłonach zabezpieczających urządzenia technicznej obróbki informacji (komputery, drukarki, plotery, faxy, swiche, rutery, huby) przed ulotem elektromagnetycznym, jak również i przed oddziaływaniami zewnętrznymi.

Wszystkie urządzenia opracowane i produkowane w ZD WIŁ posiadają indywidualne certyfikaty zgodności z odpowiednią normą. Urządzenia te dzielą się na:

- urządzenia uniwersalne – dla grupy urządzeń – spełniające wymagania norm krajowych i zagranicznych tj. NO-06-A201, NSA 65-6, AMSG 719F;
- indywidualne – na poszczególne urządzenia spełniające wymagania warunków technicznych oraz norm: AMSG-720B, AMSG-784B, AMSG-788B.

Do urządzeń indywidualnych zaliczamy między innymi:

- kabiny ekranujące do zastosowań specjalnych typu KE-100;
- pomieszczenia ekranowane metodą materiałów elastycznych;

- kontenery samochodowe.

Do urządzeń indywidualnych zaliczamy urządzenia wykonane pod określony rodzaj technicznych urządzeń do przetwarzania informacji niejawnej i spełniających wymagania na skuteczność ekranowania dla tych urządzeń. Zakład nasz opracował i produkuje osłony (obudowy) na następujące urządzenia:

- specjalne urządzenia wojskowe opracowane i produkowane w zakładzie wykonywane są w technice „TEMPESTOWEJ" tzn. są szczelne elektromagnetyczne na odpowiednim poziomie;
- stanowiska komputerowe typu PC wraz z drukarkami (typu BSK);
- urządzenia faxowe różnych typów (OKI OF-38, ILLEX, CANON typu OF-1);
- specjalizowane terminale komputerowe (np. SILICON typu BSK);
- bierne i czynne elementy sieci komputerowej (np. SWICH, RUTER, HUB lub EPD-SK);
- małe serwery PC (EPD-SK).

Przykładami obecnie produkowanych urządzeń indywidualnych są:

- zestawy komputerowych obudów ekranujących typu BSK;
- ekranowane punkty dystrybucyjne typu EPS-SK: 42-1, 42-2, 24-1, 15-1;
- obudowy ekranujące fax np.
  - typu OF-1 na urządzenie faxowe OF-38;
  - typu OED/F na urządzenia faxowe CANON.

Zabezpieczenie elektromagnetyczne indywidualnych stanowisk pracy realizowane jest poprzez stosowanie obudów ekranujących redukujących niepożądaną emisję elektromagnetyczną. Przykładem tego typu stanowisk opracowanych i produkowanych przez ZD WIŁ jest rodzina urządzeń typu BSK (BSK1, BSK2).

Indywidualne, elektromagnetycznie bezpieczne stanowiska komputerowe (BSK) przeznaczone są do tłumienia niepożądanej emisji przewodzonej i promieniowanej, której źródłem jest standardowy zestaw komputerowy (jednostka centralna, monitor, drukarka, klawiatura, mysz). W skład zestawu BSK wchodzą:

- obudowa ekranująca komputer;
- obudowa ekranująca drukarkę;
- elektromagnetycznie bezpieczna klawiatura;
- mysz;
- transformator separujący.

Połączenie transmisyjne obudów komputera i drukarki realizowane jest w oparciu o elementy techniki światłowodowej z zastosowaniem modułów światłowodowych serii MS-16C-C/DCE-C. Dodatkowym elementem wyposażenia może być moduł MS-16B-DTE zapewniający współpracę, poprzez moduł MK-16A, stanowiska BSK z cyfrowym systemem łączności STORCZYK.

Innym przykładem obudowy ekranującej produkowanym przez ZD WIŁ jest szafa EPD-SK. Szafa EPD-SK jest elementem bezpiecznych sieci komputerowych. Służy ona do ochrony przed elektromagnetycznym przenikaniem informacji oraz przed oddziaływaniem zewnętrznych narażeń elektromagnetycznych montowanych w niej urządzeń np. serwerów, ruterów, komputerów, drukarek, tablic krosowych, zasilaczy oraz kaset o szerokości 19".

Zabezpieczenie elektromagnetyczne pomieszczeń wykonywane jest w oparciu o kabiny ekranujące typu KE-100 lub w oparciu o technologię elastycznych materiałów przewodzących. Kabiny ekranujące KE-100 charakteryzują się konstrukcją modułową tzn. montowane są z poszczególnych paneli skręcanych ze sobą, które tworzą ściany, podłogę i sufit. Panele wykonane są z ocynkowanej blachy stalowej o grubości 2mm. Do uszczelniania elektromagnetycznego połączeń międzypanelowych stosowane są specjalne uszczelki objętościowe oraz system osłon spinkowych.

Zabezpieczenie elektromagnetyczne pomieszczeń w oparciu o technologię elastycznych materiałów przewodzących realizowane jest w oparciu o materiał metalizowany typu FLECTRON, którym wyklejane są od strony wewnętrznej wszystkie elementy pomieszczenia – ściany, sufit i podłoga. Uzyskanie wymaganej skuteczności ekranowania takiego pomieszczenia wymaga bardzo starannego i specjalnego przygotowania pomieszczenia pod kątem zastosowania elastycznego materiału przewodzącego. ZD WIŁ jako jedyny wykonawca w kraju uzyskał certyfikat zgodności wydany przez UOP na zabezpieczenie pomieszczeń z zastosowaniem materiału typu FLECTRON.

ZESTAW KOMPUTEROWYCH OBUDÓW EKRANUJĄCYCH BSK-2

CHARAKTERYSTYKA

Bezpieczne stanowisko komputerowe jest przeznaczone do obróbki informacji o charakterze niejawnym. Charakteryzuje się nowoczesnym rozwiązaniem zapewniającym dużą skuteczność ekranowania sygnałów ubocznych generowanych przez komputer. Konstrukcja modułowa oraz małe gabaryty preferują do stosowania w pomieszczeniu pracy.

PODSTAWOWE PARAMETRY

- zasięg przenikania informacji wg uzgodnionych WT;
- brak emisji ujawniającej w obwodzie zasilania;
- klawiatura zapewnia bezpieczne wprowadzanie danych i sterowanie przetwarzaniem informacji.

ZASTOSOWANIE

W obiektach specjalnych (wojskowych, rządowych, bankowych), w których jest przetwarzana informacja szczególnie chroniona.

BEZPIECZNE STANOWISKO KOMPUTEROWE BSK-3

CHARAKTERYSTYKA

Bezpieczne stanowisko komputerowe jest przeznaczone do obróbki informacji o charakterze niejawnym. Charakteryzuje się nowoczesnym rozwiązaniem zapewniającym dużą skuteczność ekranowania sygnałów ubocznych generowanych przez komputer. Konstrukcja modułowa oraz małe gabaryty preferują do stosowania w pomieszczeniu pracy.

PODSTAWOWE PARAMETRY

- zasięg przenikania informacji wg uzgodnionych WT;
- brak emisji ujawniającej w obwodzie zasilania;
- klawiatura zapewnia bezpieczne wprowadzanie danych i sterowanie przetwarzaniem informacji.

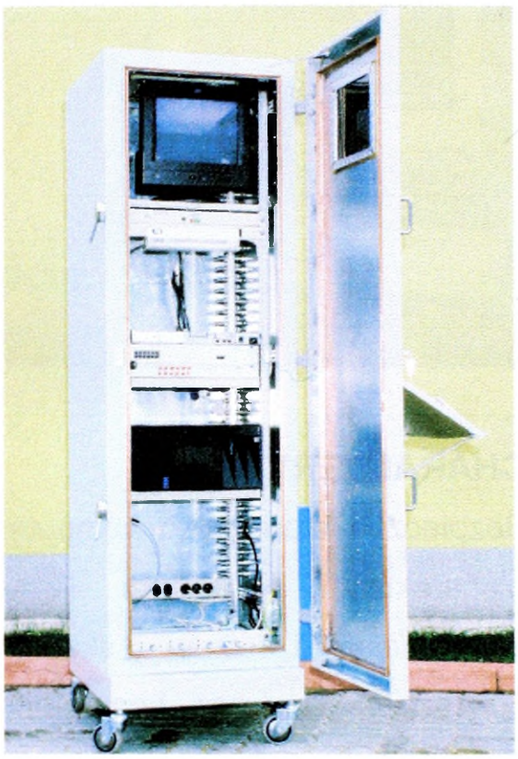
ZASTOSOWANIE

W obiektach specjalnych (wojskowych, rządowych, bankowych), w których jest przetwarzana informacja szczególnie chroniona do poziomu „ŚCIŚLE TAJNE".

SZAFA EPD-LAN-42/ZD

CHARAKTERYSTYKA

Szafa EPD-LAN-42/ZD jest urządzeniem technicznym przeznaczonym do instalacji w lokalnych sieciach komputerowych, chroniącym przed elektromagnetycznym przenikaniem informacji oraz przed oddziaływaniem narażeń elektromagnetycznych.



PODSTAWOWE PARAMETRY

- wymiary: szerokość – 740 mm, głębokość – 840 mm, wysokość – 2221 mm prześwit montażowy – 495x1870 mm;
- zasilanie urządzeń 220V 50Hz 1500VA;
- skuteczność ekranowania szafy w częstotliwości 1 MHz-1 GHz na poziomie zgodnie z WT Nr W-100.00.00.00.
-

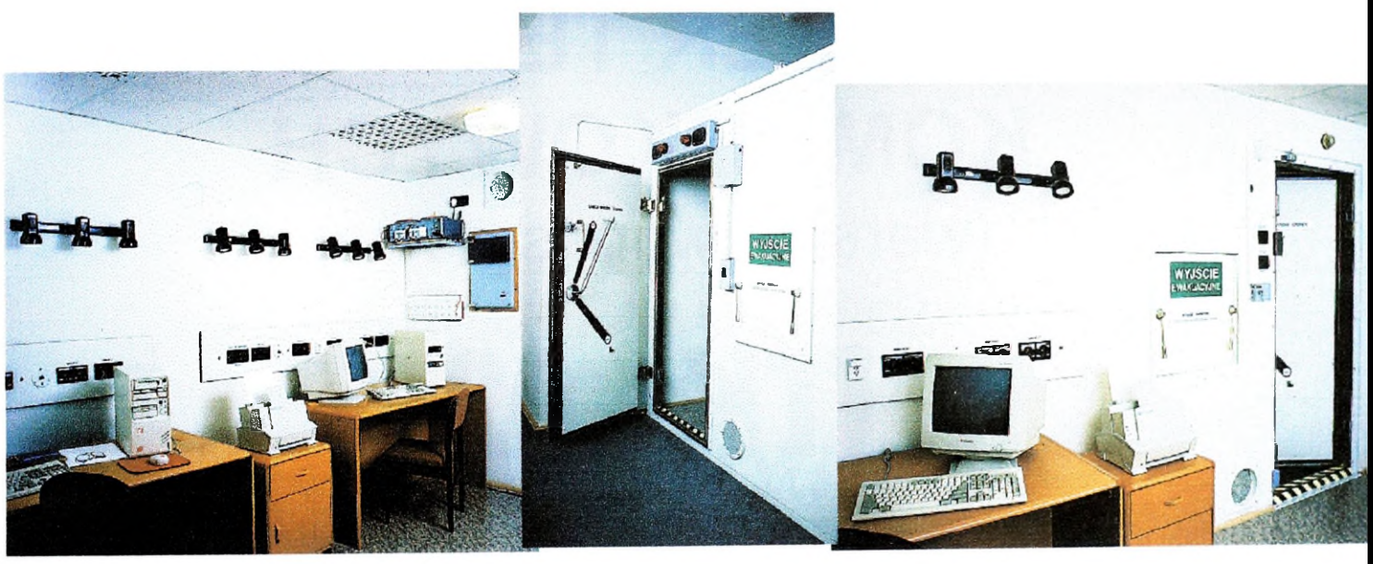
ZASTOSOWANIE

Szafa służy do montażu w niej typowych urządzeń, aktywnych i pasywnych, sieci komputerowych, m.in. komputerów, drukarek, monitorów, tablic krosowych, zasilaczy oraz kaset o szerokości 19".

KABINY I POMIESZCZENIA EKRANOWANE

CHARAKTERYSTYKA

Kabiny i pomieszczenia ekranowane są przeznaczone do tłumienia emisji niepożądanych urządzeń elektronicznych oraz do ich ochrony przed oddziaływaniem silnych zakłóceń zewnętrznych. Charakteryzują się nowoczesnym rozwiązaniem zapewniającym dużą skuteczność ekranowania.



PODSTAWOWE PARAMETRY

- konstrukcja modułowa umożliwia montaż o powierzchni do 70 m^2 i wysokości kabin do 3,5 m;
- specjalne drzwi, falowodowe filtry wentylacyjne oraz filtry sieciowe i transformatory ekranowane separujące zapewniają skuteczność ekranowania nie mniejszą niż 100 dB w zakresie częstotliwości 150 kHz÷1 GHz.

ZASTOSOWANIE

- w obiektach specjalnych (przemysłowych, wojskowych, rządowych), w których jest przetwarzana informacja szczególnie chroniona, np. w specjalnych ośrodkach;
- komputerowych;
- w laboratoriach kompatybilności elektromagnetycznej;
- w przemysłowych zakładach elektronicznych i telekomunikacyjnych;
- w szpitalach dla elektromagnetycznej ochrony czułych urządzeń elektromagnetycznych.

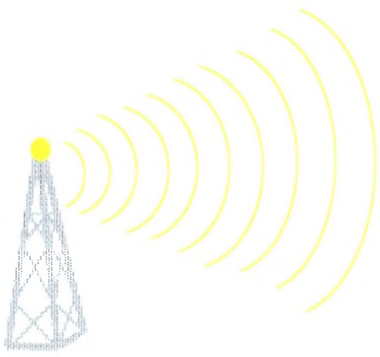
OCHRONA INFORMACJI

pozyskiwanych z telefonów komórkowych
poprzez

IMMOBILIZER TELEFONÓW KOMÓRKOWYCH

(wersja dwupasmowa)

ITK - 02P



ZAKŁAD DOŚWIADCZALNY
WOJSKOWEGO INSTYTUTU ŁĄCZNOŚCI
05-130 ZEGRZE
tel./fax 782 25 32; tel. 782 21 34
e-mail: zdwil@zdwil.com.pl

EBS
04-555 WARSZAWA
ul. B. CZECHA 59
tel.: 81 20 505

Centralny Węzeł Łączności WLOP

Jan SOŁYGA
Grzegorz NAZAREWICZ

BEZPIECZEŃSTWO SIECI KOMPUTEROWEJ A SWIADOMOŚĆ JEJ UŻYTKOWNIKÓW

CENTRUM KONFERENCYJNE WP Grudzień 2001

Podstawą przygotowania wystąpienia były obserwacje poczynione w ciągu ostatnich kilku lat w zakresie opracowywania i wdrażania procedur bezpieczeństwa teleinformatycznego, zarówno w resorcie Ministerstwa Obrony Narodowej, jak i instytucjach cywilnych.

Dla podkreślenia wielkiego znaczenia bezpieczeństwa informacji należy zacytować fragment raportu skierowanego kilka lat temu do prezydenta i Kongresu Stanów Zjednoczonych Ameryki Północnej. Raport ten przygotował w 1997r. dyrektor NSA - generał porucznik Kenneth A. Miniham – i napisał w nim:

„Okres po Zimnej Wojnie charakteryzuje się rozproszeniem sił, niepewnością geopolityczną i zmianami technologicznymi. Rewolucja informacyjna ogarnia cały świat, powodując zmiany tak radykalne, jak te spowodowane opracowaniem bomby atomowej. Tak jak panowanie nad technologiami przemysłowymi stanowiło klucz do potęgi ekonomicznej i militarnej przez dwa ostatnie wieki, tak panowanie nad bezpieczeństwem technologii informacyjnych będzie kluczem do potęgi w XXI wieku."

Na dzień dzisiejszy istnieje wiele zagrożeń, na które narażona jest informacja przechowywana i przetwarzana w systemach informatycznych. Proste pogrupowanie i wyliczenie zagrożeń jest ważnym elementem wspomagającym edukację personelu oraz kadry kierowniczej. Zagrożenia te można podzielić na:

1. Zagrożenia losowe zewnętrzne – uwzględniają takie czynniki jak temperaturę, wilgotność, zanieczyszczenia powietrza, zakłócenia w zasilaniu, zakłócenia w komunikacji, wyładowania atmosferyczne, klęski żywiołowe, itp.
2. Zagrożenia losowe wewnętrzne - to niezamierzone błędy ludzi, błędy i pomyłki operatorów, administratorów (konfiguracja sprzętu i oprogramowania), zaniedbania użytkowników oraz defekty sprzętu i oprogramowania.
3. Zagrożenia zamierzone – wynikają przede wszystkim z działania własnych pracowników powodowanych chciwością, chęcią rewanżu, itd.

W tej grupie zagrożeń są także działania użytkowników wykraczające poza ich obowiązki, działania przestępców komputerowych podejmowane z chęci zysku, działania przedstawicieli prasy i innych mediów szukających dostępu do informacji, szpiegostwo gospodarcze i wojskowe, wandalizm i terroryzm.

Inny bardzo uogólniony podział zagrożeń można przeprowadzić ze względu na miejsce wystąpienia źródła niebezpieczeństwa:

- zagrożenia wewnętrzne – inicjowane wewnątrz organizacji;

- zagrożenia zewnętrzne – inicjowane na zewnątrz;

Statystycznie przyjmuje się, że około 80% ataków na zasoby sieci informatycznych odbywa się z wewnątrz tych sieci. Obecnie możemy wyodrębnić różne narzędzia umożliwiające przeprowadzenie mniej lub bardziej skutecznych ataków na sieci informatyczne, a co za tym idzie pozyskanie zawartych w nich informacji lub zablokowanie udostępnianych usług.

Najbardziej znanymi i najczęściej praktykowanymi technikami ataku na systemy komputerowe są:

- zgadywanie hasła dostępu – wykorzystuje się tutaj z reguły fakt, że większość użytkowników jako hasła dostępu do konta przyjmuje łatwe do zapamiętania słowa (np. imiona, nazwy miejscowości, itp.), które w łatwy sposób mogą być odgadnięte przez cierpliwego włamywacza;
- atak słownikowy (brutalny) – wykorzystywany w systemach, w których nie istnieją żadne restrykcje co do ilości błędnych logowań. Specjalny program w sposób automatyczny dokonuje kolejnych logowań, wykorzystując wyrazy zawarte w specjalnie przygotowanym pliku tekstowym – słowniku.
- „sniffing" /podsłuch sieciowy/ - technika ta polega na przechwytywaniu informacji przesyłanych za pośrednictwem sieci komputerowej. Wykorzystuje się w tym celu wyspecjalizowane urządzenia /programy/ selektywnie przechwytujące pakiety danych i dekodujące ich zawartość.
- wirusy, konie trojańskie i inne groźne aplikacje;
- „backdoors" / furtki/ - nieudokumentowane wejścia do legalnych programów /często tworzone przez ich autorów/, których odnalezienie umożliwia przejęcie kontroli nad daną aplikacją;
- „ping of death" – wykorzystanie usługi o nazwie „ping" do blokowania /załamywania/ serwerów lub zapór ogniowych;
- „spoofing" – technika polegająca na oszukiwaniu systemów poprzez przekazywanie im fałszywych informacji np. IP spoofing, czyli fałszowanie adresu źródłowego pakietów;
- SYN flood – polega na blokowaniu określonych usług serwera poprzez inicjowanie dużej liczby połączeń sieciowych w taki sposób, aby pełna komunikacja sieciowa nie została do końca nawiązana, a serwer przebywał w stanie ciągłego oczekiwania;

- zagrożenia płynące z mechanizmów funkcjonowania poczty elektronicznej i serwisów WWW;
- „Eksploits" – programy wykorzystujące błędy w systemach operacyjnych i oprogramowaniu użytkowym;
- wykorzystywanie nieudokumentowanych portów TCP/IP / portów nie chronionych przez system/;
- kryptoanaliza zaszyfrowanych informacji;
- „connection hijacking" – przechwytywanie otwartych połączeń sieciowych;
- rejestrowanie promieniowania elektromagnetycznego.

Mnogość technik włamań oraz ciągła ewolucja systemów /oprogramowania/ powoduje, że nie jest możliwym wykonanie zabezpieczeń dających stu procentową gwarancję. Możemy jedynie zmniejszać ryzyko włamania do zasobów chronionych w naszych sieciach poprzez inwestowanie w coraz to nowsze technologie zabezpieczeń.

Łatwość pozyskania różnych narzędzi do przeprowadzania ataków nie powinna być na dzień dzisiejszy najważniejszym czynnikiem potęgującym nasze obawy o bezpieczeństwo systemów informatycznych. Największego zagrożenia należy doszukiwać się w najsłabszych ogniwach tych systemów tzn. użytkownikach /ich ignorancji, niechęci oraz niedbalstwie/. To właśnie oni zwykle nie są świadomi konsekwencji związanych z naruszeniem bezpieczeństwa sieci. Wykorzystują sieci oraz narzędzia w nich udostępniane do bardziej efektywnej pracy, często traktując środki bezpieczeństwa jako utrudnienie, a nie pomoc.

Dlatego też dla każdej firmy niezmiernie ważne jest zapewnienie pracownikom właściwego treningu, mającego na celu uświadomienie im wielu problemów oraz aspektów związanych z bezpieczeństwem. Szkolenie dotyczące bezpieczeństwa powinno zostać zapewnione wszystkim pracownikom projektującym, implementującym oraz obsługującym systemy sieciowe. Szkolenie powinno obejmować informacje dotyczące typów zabezpieczeń oraz technik wewnętrznej kontroli, które powinny zostać uwzględnione podczas tworzenia, działania i konserwacji systemów sieciowych.

Osoby odpowiedzialne za bezpieczeństwo sieci powinny zostać dogłębnie przeszkolone z następujących tematów:

- zagrożenia systemów i techniki włamań;
- techniki zabezpieczające;
- metodologie oceniania zagrożeń oraz słabych punktów;

- kryteria wyboru oraz implementacja nadzoru;
- określanie wagi zasobów oraz szacowanie ewentualnych strat, w przypadku zaniechania utrzymywania zabezpieczeń.

Dla personelu odpowiedzialnego za zarządzanie hasłami również niezbędne jest szkolenie. Według CERT (Computer Emergency Response Team) ok. 80% problemów bezpieczeństwa sieci jest związanych ze złym stosowaniem haseł dostępu.

W związku z powyższym należy wymuszać na personelu technicznym przestrzegania następujących reguł:

- nigdy nie pozostawiaj w systemie haseł skonfigurowanych domyślnie;
- wymuszaj na użytkownikach w systemie częstą zmianę haseł;
- naucz użytkowników jak wybierać mocne hasła:
  - długość co najmniej 7 znaków;
  - mieszanka cyfr oraz liter wielkich i małych;
  - pseudo-losowy zbiór liter i cyfr;.
- wymagaj stosowania haseł przy każdym koncie;
- staraj się nie zapisywać haseł i nie przechowuj ich w plikach elektronicznych (np. w przesyłkach e-mail);
- cykliczne uruchamiać programy typu crack (NTCrack) w celu sprawdzenia siły haseł stosowanych w twojej sieci.

Kluczową rolę w rozpowszechnianiu informacji dotyczących działań, mających wpływ na bezpieczeństwo sieci lokalnych powinni pełnić właśnie ich administratorzy. Ponadto to oni powinni przede wszystkim dbać o przestrzeganie pewnych zasad zanim podłączą swoją sieć lokalną do sieci rozległej:

Do przykładowych zasad należy:

- zapewnienie należytej dokumentacji infrastruktury sieci;
- zapewnienie kontroli ściąganego oprogramowania;
- zapewnienie adekwatnego szkolenia użytkowników.

Podczas informowania użytkowników sieci zwrócić uwagę na metody pozyskiwania informacji przy wykorzystaniu socjotechnik. Wielu intruzów odnosi większe sukcesy stosując socjotechnikę, niż gdyby stosowali najwymyślniejsze sztuczki techniczne. Najważniejszym punktem szkolenia powinno być podkreślenie, że pracownicy i użytkownicy nie mogą wierzyć każdemu, kto np. do nich telefonuje prosząc o coś, co

mogłoby naruszyć bezpieczeństwo. Przed ujawnieniem wszelkich poufnych informacji, należy zidentyfikować osobę, z którą się rozmawia.

Następnym bardzo poważnym zagadnieniem jest stosowanie ochrony antywirusowej w postaci wyspecjalizowanych aplikacji mających na celu zlokalizowanie i neutralizację złośliwych kodów programowych. Oprócz reakcji na ewentualne realne zagrożenia niezbędna jest również profilaktyka, czyli ciągłe uświadamianie użytkowników o konieczności przestrzegania pewnych reguł dotyczących utrzymania należytego poziomu bezpieczeństwa w procesie eksploatacji sieci informatycznych np. nie wprowadzamy do sieci oprogramowania nieznanego pochodzenia, które nie przeszło kontroli antywirusowej. Chodzi tutaj przede wszystkim o możliwość wgrywania oprogramowania shareware i freeware, które w bardzo wielu przypadkach jest idealnym nośnikiem kodów wirusów. Takie praktyki prowadzą często do zarażenia całej sieci dzięki mechanizmom replikowania się stosowanym przez wirusy, co w konsekwencji może spowodować zniszczenie cennych zasobów informacyjnych.

Zagadnień dotyczących bezpieczeństwa systemów jest wiele. Można je rozważać w aspekcie zagrożeń oraz technik służących ich przeciwdziałaniu. Jednak jak już wspomniałem najważniejszym problemem staje się dzisiaj edukacja /uświadamianie/ użytkowników w zakresie proporcjonalnym do ich kompetencji. I tutaj należy zwrócić szczególną uwagę na następujące grupy:

- kadrę kierowniczą;
- obsługę techniczną;
- użytkowników końcowych.

Stopień uświadomienia o istniejących zagrożeniach na jakie narażona jest informacja w sieci, jest najsłabszy wśród kadry kierowniczej i użytkowników końcowych. Paradoksalnym staje się fakt, że to właśnie kadra kierownicza decyduje o nakładach finansowych na techniczne zabezpieczenia implementowane w sieciach. Jednak bardzo często zapomina się o specjalistycznych szkoleniach dla personelu technicznego, które z drugiej strony nie są znowu takie tanie.

Proces szkolenia może być dosyć kosztowny, a w przypadku konieczności przygotowania pełnej obsady IT pracującej w systemie dyżurowym, całkowity koszt szkolenia mógłby zamknąć się w sumie nawet kilkuset tysięcy złotych. Dlatego też wiele instytucji i firm nie posiadając odpowiednich środków finansowych w swoich budżetach rezygnuje ze szkoleń. Istnieje również obawa, że osoby przeszkolone /posiadające już

w ręku certyfikat ukończenia kursu/ mogą w najbliższym okresie zmienić miejsce pracy w poszukiwaniu lepszego wynagrodzenia. Natomiast bardzo złym przykładem jest sytuacja, w której środki finansowe istnieją, natomiast nie widzi się potrzeb ochrony własnych zasobów. W efekcie końcowym tzw. „oszczędności" prowadzą do utraty ciągłości pracy systemu lub utraty danych, czego następstwem może być nawet zagrożenie misji instytucji / firmy/.

Reasumując, chciałem zwrócić uwagę na zwiększenie nakładów celem szkolenia podległego personelu technicznego, zwiększenie wysiłku w zakresie samokształcenia oraz przestrzegania zasad dotyczących bezpieczeństwa i nie traktowanie procedur bezpieczeństwa jako elementu utrudniającego życie.

Bibliografia:

1. Ahuja V. *Bezpieczeństwo w sieciach*, Mikom, Warszawa 1997.
2. Klander L.; *Hacker proof – czyli jak bronić się przed intruzami*, Mikom, Warszawa 1998.
3. Materiały seminarium technicznego.; *Bezpieczeństwo i pomiary w sieciach teleinformatycznych*, NetWorld, Warszawa 2001.
4. Stawowski M.; *Badanie zabezpieczeń sieci komputerowych*, ArsKom, Warszawa 1999.
5. Strebe M. Perkins Ch.; *Firewalls*, *Mikom*, Warszawa 2000.
6. Zienkiewicz A.; *Bezpieczeństwo informacji i sieci telekomunikacyjnych a wirtualna rzeczywistość*, Materiały seminarium - Miedzeszyn 97, Warszawa 1997.


Zagrożenia zewnętrzne sieci
Internet
Router
Zapora ogniowa + proxy server
STOP
Chroniona sieć LAN
Użytkownicy
dial up
Internet
Intruz


Metody zabezpieczenia sieci
Kontrola antywirusowa
Zapora ogniowa + proxy server
Internet
Router
STOP
Chroniona sieć LAN
Użytkownicy
Intruz
IDS /system detekcji intruzów/

SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

obejmuje:

Zarządzanie bezpieczeństwem teleinformatycznym

Polityka bezpieczeństwa teleinformatycznego

Bezpieczeństwo logiczne w sieciach komputerowych

Bezpieczeństwo sieci w e-biznesie i środowisku internetowym

SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA I ADMINISTROWANIA MS WINDOWS NT4.0

obejmuje:

Bezpieczeństwo systemu MS Windows NT

Securing Windows NT Server

Administrowanie systemem Microsoft Windows NT 4.0

Supporting Microsoft Windows NT 4.0 Core Technologies

Instaling and Configuring Microsoft Windows NT Server 4.0

Procedury awaryjne w Microsoft Windows NT

Internetworking Microsoft TCP/IP on Microsoft WIndows NT 4.0

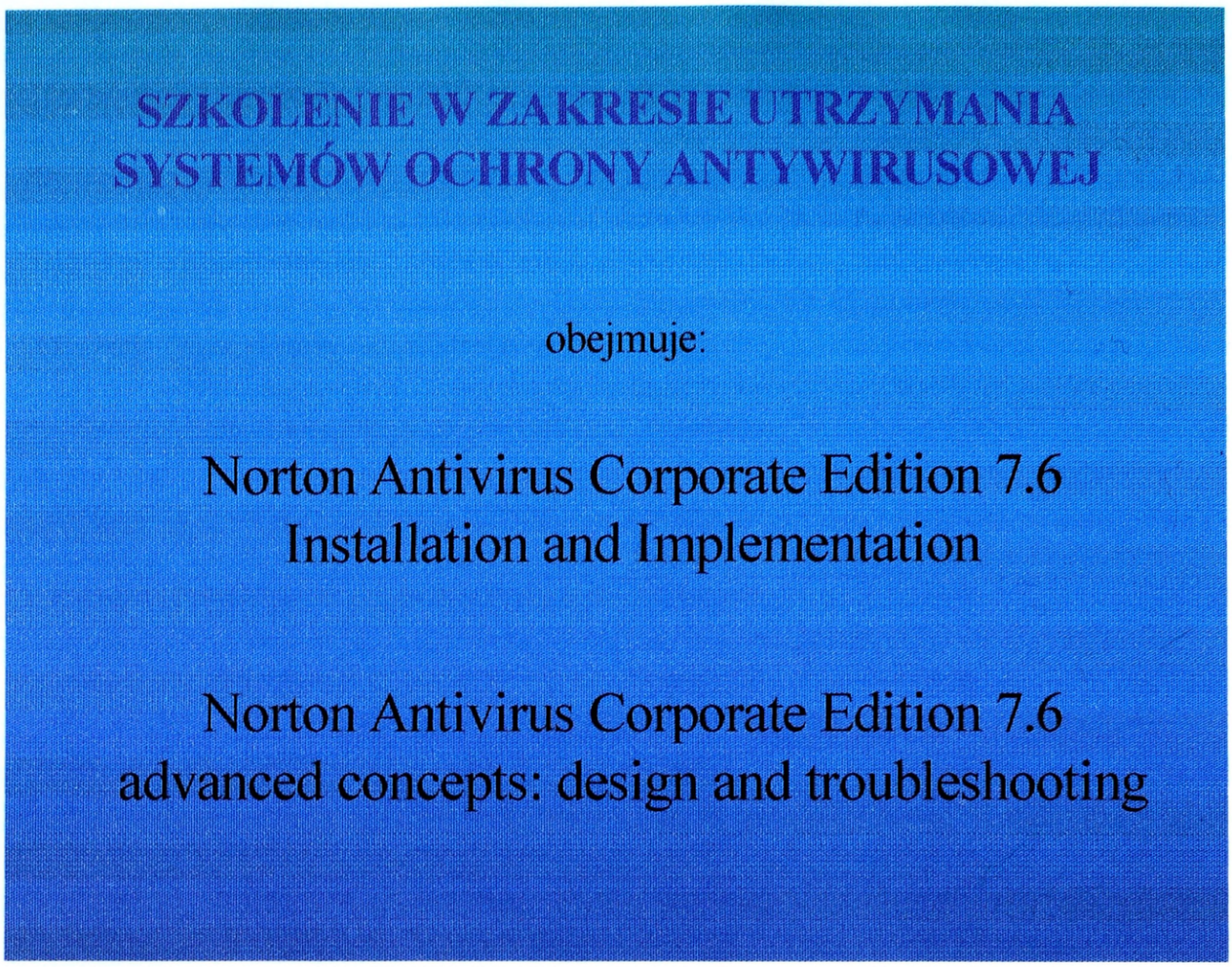
SZKOLENIE W ZAKRESIE UTRZYMANIA ZAPORY OGNIOWEJ I SYSTEMU IDS

obejmuje:

Symantec Enterprise Firewall/VelociRaptor 6.5 Administration

Symantec Enterprise Firewall/VelociRaptor 6.5 Advanced Administration

Intruder Alert


SZKOLENIE W ZAKRESIE UTRZYMANIA SYSTEMÓW OCHRONY ANTYWIRUSOWEJ
obejmuje:
Norton Antivirus Corporate Edition 7.6 Installation and Implementation
Norton Antivirus Corporate Edition 7.6 advanced concepts: design and troubleshooting

URZĄD REGULACJI
TELEKOMUNIKACJI

Zbigniew TADEUSIAK

REALIZACJA ZADAŃ OBRONNYCH PRZEZ OPERATORÓW TELEKOMUNIKACYJNYCH PODCZAS SYTUACJI KRYZYSOWYCH W ŚWIETLE AKTÓW PRAWNYCH

CENTRUM KONFERENCYJNE WP Grudzień 2001

URZĄD REGULACJI TELEKOMUNIKACJI

Ograniczenia działalności telekomunikacyjnej ze względu na obronność i bezpieczeństwo państwa

Zbigniew TADEUSIAK

URZĄD REGULACJI TELEKOMUNIKACJI

Ograniczenia działalności telekomunikacyjnej

Na etapie

- uzyskiwania zgody na świadczenie usług telekomunikacyjnych
- świadczenia usług telekomunikacyjnych

na rzecz:

- organów powołanych do niesienia pomocy;
- rządowych jednostek organizacyjnych (Art.4);
- bezpieczeństwa państwa;
- obronności państwa.

URZĄD REGULACJI TELEKOMUNIKACJI

Rozdział 2
Zezwolenie telekomunikacyjne - Art. 8

1. Prezes URT wydaje zezwolenie...operatorowi... jeżeli... nie zachodzą:
2) uzasadnione okoliczności prowadzące do:
a) zagrożenia obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego;

2. Odmowa wydania zezwolenia z powodu okoliczności, o których mowa w ust. 1 pkt 2 lit. a), następuje po zasięgnięciu opinii ministra Obrony Narodowej lub szefa Urzędu Ochrony Państwa, w zakresie ich właściwości. Opinia Ministra Obrony Narodowej lub szefa Urzędu Ochrony Państwa stwierdzająca, że zachodzą okoliczności prowadzące do zagrożenia obronności lub bezpieczeństwa państwa, nie wymaga uzasadnienia.

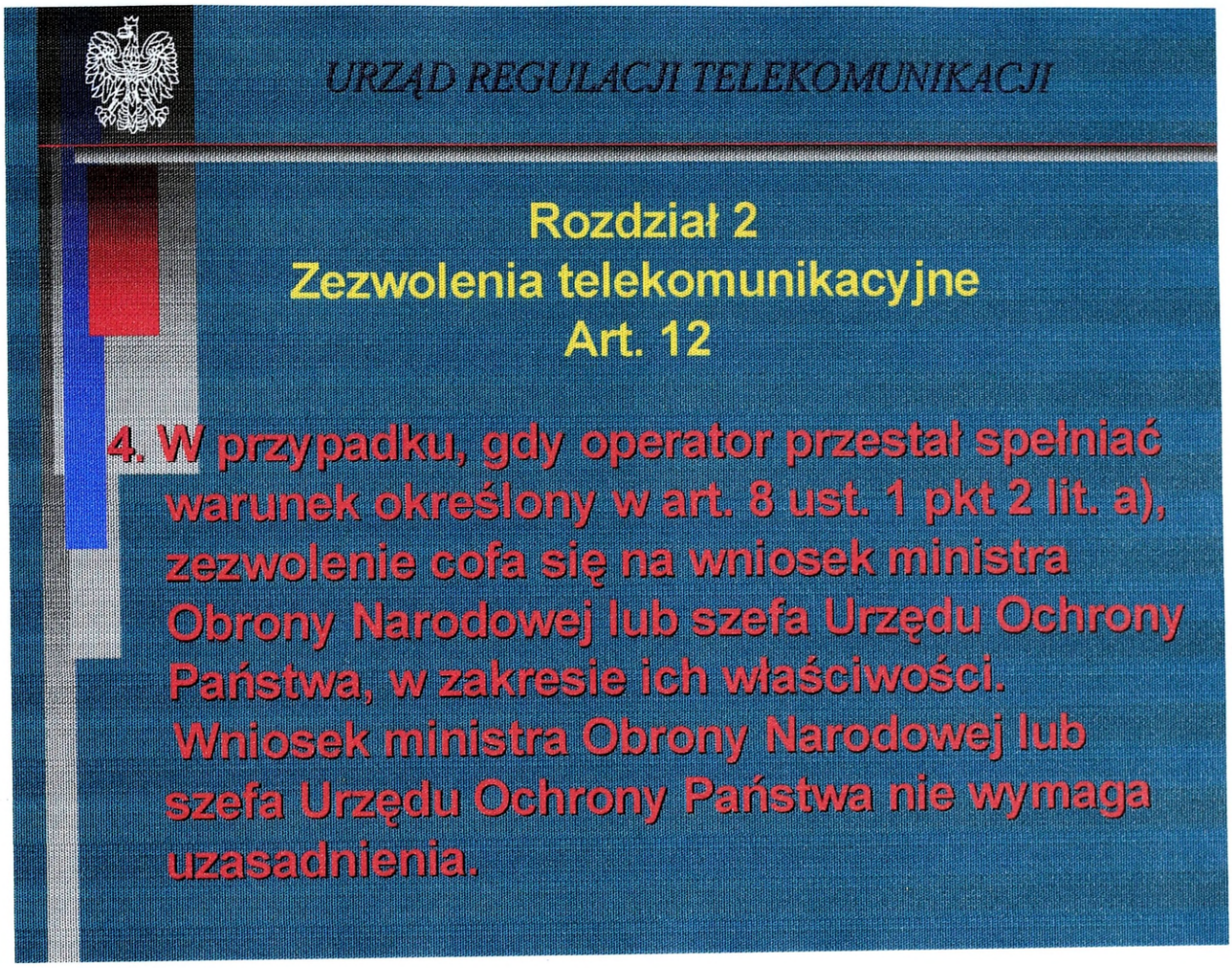
URZĄD REGULACJI TELEKOMUNIKACJI

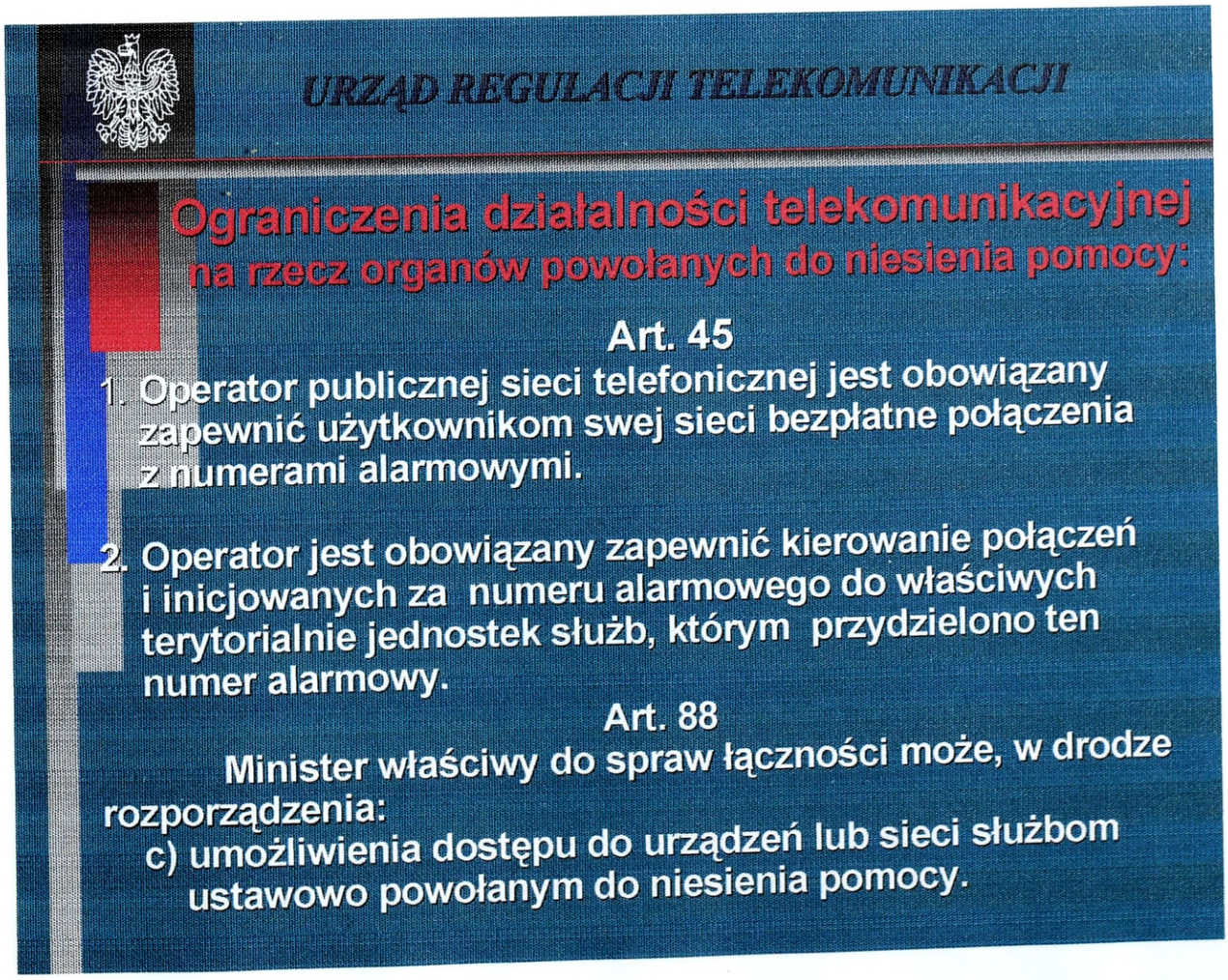
Rozdział 4
Pozwolenia radiowe
Art. 18

1. Pozwolenie wydaje się..... jeżeli...
- Nie zachodzą okoliczności o których mowa w art.8 ust. 1 pkt 2.

Rozdział 5
Rezerwacja częstotliwości
Art. 22

6. Do odmowy rezerwacji stosuje się odpowiednio przepisy w art. 8 ust. 2.


URZĄD REGULACJI TELEKOMUNIKACJI
Rozdział 2
Zezwolenia telekomunikacyjne
Art. 12
4. W przypadku, gdy operator przestał spełniać warunek określony w art. 8 ust. 1 pkt 2 lit. a), zezwolenie cofa się na wniosek ministra Obrony Narodowej lub szefa Urzędu Ochrony Państwa, w zakresie ich właściwości.
Wniosek ministra Obrony Narodowej lub szefa Urzędu Ochrony Państwa nie wymaga uzasadnienia.


URZĄD REGULACJI TELEKOMUNIKACJI
Ograniczenia działalności telekomunikacyjnej
na rzecz organów powołanych do niesienia pomocy:
Art. 45
1. Operator publicznej sieci telefonicznej jest obowiązany zapewnić użytkownikom swej sieci bezpłatne połączenia z numerami alarmowymi.
2. Operator jest obowiązany zapewnić kierowanie połączeń i inicjowanych za numeru alarmowego do właściwych terytorialnie jednostek służb, którym przydzielono ten numer alarmowy.
Art. 88
Minister właściwy do spraw łączności może, w drodze rozporządzenia:
c) umożliwienia dostępu do urządzeń lub sieci służbom ustawowo powołanym do niesienia pomocy.

URZĄD REGULACJI TELEKOMUNIKACJI

Ograniczenia działalności telekomunikacyjnej w sytuacja szczególnych zagrożeń

Art. 45

1. Operatorzy są obowiązani uwzględniać przy planowaniu, budowie, rozbudowie, eksploatacji lub łączeniu sieci telekomunikacyjnych możliwość wystąpienia sytuacji szczególnych zagrożeń, a w szczególności wprowadzenia stanu wojennego, stanu wyjątkowego lub stanu klęski żywiołowej.

2. Operatorzy publiczni są obowiązani posiadać aktualny plan działań w sytuacjach szczególnych zagrożeń.

URZĄD REGULACJI TELEKOMUNIKACJI

Plan działan w sytuacjach szczególnych zagrożeń

1. Wzajemnej współpracy operatorów z organami koordynującymi działania ratownicze, służbami ustawowo powołanymi do niesienia pomocy oraz Siłami Zbrojnymi.
2. Zabezpieczania sieci telekomunikacyjnych i urządzeń telekomunikacyjnych przed skutkami zagrożenia.
3. Zachowania ciągłości świadczenia usług telekomunikacyjnych, zwłaszcza dla służb ratowniczych.
4. Sposobu wykonywania przez operatorów sieci telekomunikacyjnych i osoby eksploatujące urządzenia telekomunikacyjne świadczeń rzeczowych przewidzianych w ustawie.
5. Ewidencji i gromadzenia rezerw.

URZĄD REGULACJI TELEKOMUNIKACJI

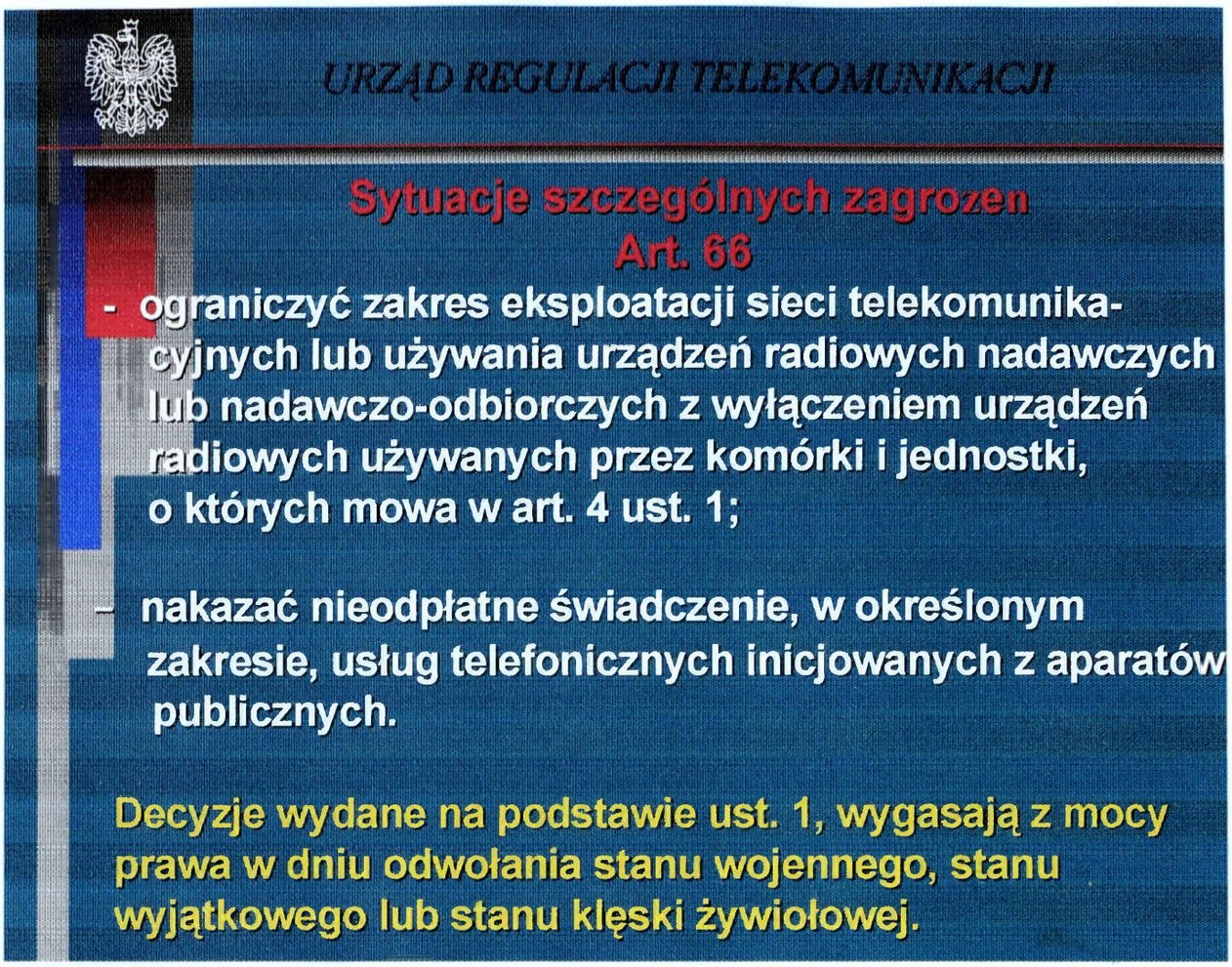
Sytuacje szczególnych zagrozen Art. 65

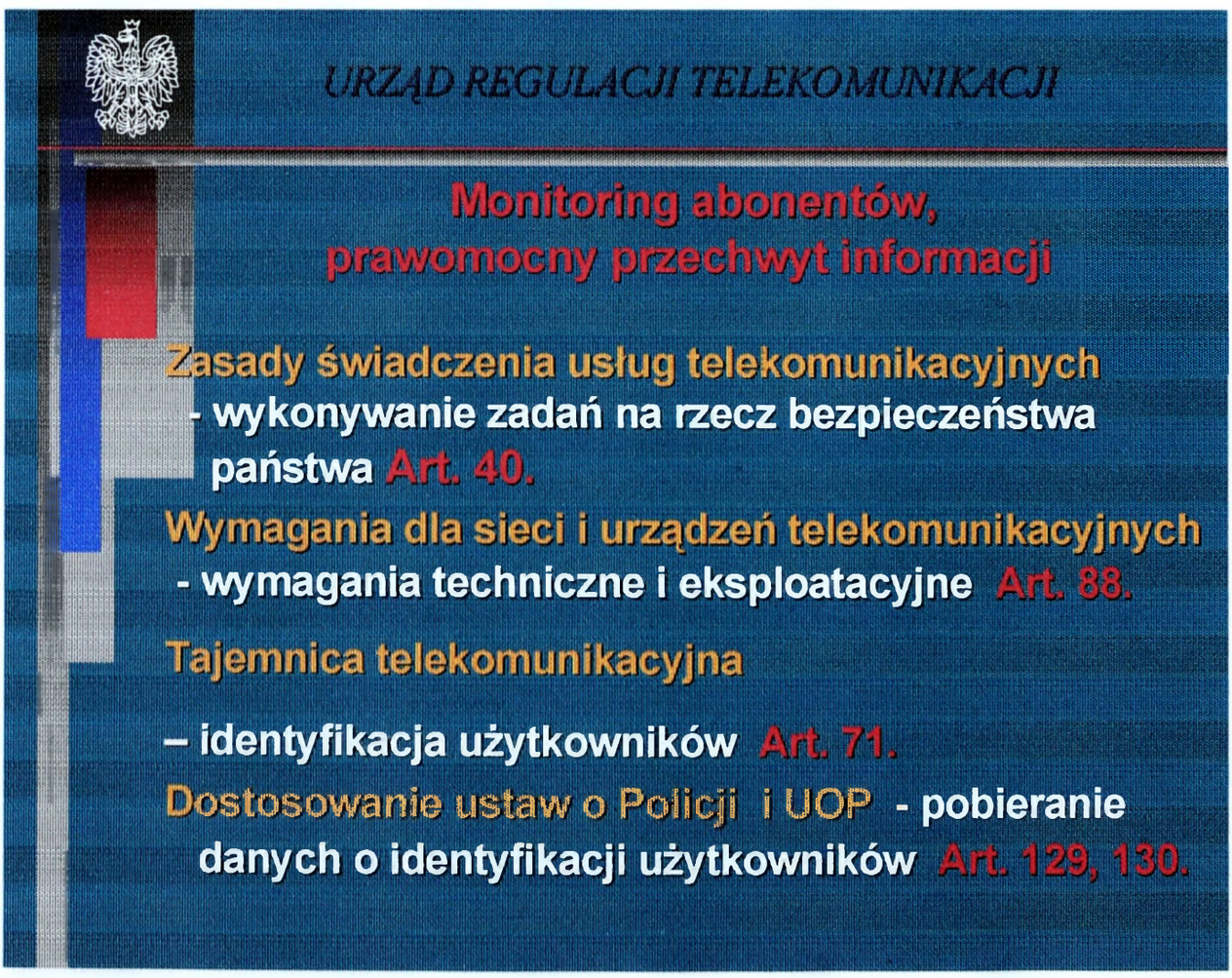
1. W sytuacji szczególnego zagrożenia, operatorzy publiczni podejmują...działania określone w planie,.. utrzymując świadczenie usług telekomunikacyjnych w pierwszej kolejności służbom powołanym do ratowania życia ludzkiego, a następnie organom administracji rządowej lub samorządu terytorialnego, Policji, Siłom Zbrojnym, obronie cywilnej, Służbie Więziennej oraz pozostałym użytkownikom, ...
2. Przepisy ust. 1 stosuje się odpowiednio wobec osób używających urządzenia radiowe nadawcze i nadawczo- odbiorcze, wykorzystywane w służbach radiokomunikacyjnych.

URZĄD REGULACJI TELEKOMUNIKACJI

Sytuacje szczególnych zagrozen Art. 66

1. W przypadku wprowadzenia stanu wojennego, stanu wyjątkowego lub stanu klęski żywiołowej minister właściwy do spraw łączności może, w drodze decyzji:
   - nałożyć na operatorów publicznych określone obowiązki dotyczące utrzymania ciągłości świadczenia usług telekomunikacyjnych;
   - określić numery alarmowe dla określonych służb lub podmiotów;
   - ograniczyć publiczną dostępność niektórych usług telekomunikacyjnych.


URZĄD REGULACJI TELEKOMUNIKACJI
Sytuacje szczególnych zagrozen
Art. 66
- ograniczyć zakres eksploatacji sieci telekomunikacyjnych lub używania urządzeń radiowych nadawczych lub nadawczo-odbiorczych z wyłączeniem urządzeń radiowych używanych przez komórki i jednostki, o których mowa w art. 4 ust. 1;
– nakazać nieodpłatne świadczenie, w określonym zakresie, usług telefonicznych inicjowanych z aparatów publicznych.
Decyzje wydane na podstawie ust. 1, wygasają z mocy prawa w dniu odwołania stanu wojennego, stanu wyjątkowego lub stanu klęski żywiołowej.


URZĄD REGULACJI TELEKOMUNIKACJI
Monitoring abonentów,
prawomocny przechwyt informacji
Zasady świadczenia usług telekomunikacyjnych
- wykonywanie zadań na rzecz bezpieczeństwa państwa Art. 40.
Wymagania dla sieci i urządzeń telekomunikacyjnych
- wymagania techniczne i eksploatacyjne Art. 88.
Tajemnica telekomunikacyjna
– identyfikacja użytkowników Art. 71.
Dostosowanie ustaw o Policji i UOP - pobieranie danych o identyfikacji użytkowników Art. 129, 130.

URZĄD REGULACJI TELEKOMUNIKACJI

Wykonywanie zadań na rzecz bezpieczeństwa państwa Art. 40 - monitoring abonentów

Operatorzy są obowiązani do wykonywania zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Obowiązek ... dotyczy zapewnienia, na koszt operatora, technicznych i organizacyjnych możliwości wykonywania w sieci telekomunikacyjnej eksploatowanej przez operatora zadań na rzecz prokuratury, sądów, ... jednostek organizacyjnych podporządkowanych ministrowi Obrony Narodowej, właściwemu do spraw wewnętrznych, ministrowi finansów publicznych oraz szefowi Urzędu Ochrony Państwa, ... kierując się zasadą osiągania celu przy najniższych nakładach.

URZĄD REGULACJI TELEKOMUNIKACJI

Zapewnienia.... technicznych i organizacyjnych możliwości - Art. 88 - wymagania dla sieci.

Minister, ... określi, ... , szczegółowe wymagania techniczne i eksploatacyjne dla sieci ..(i). urządzeń telekomunikacyjnych, dotyczące ich przystosowania do wypełniania przez operatorów obowiązku, o którym mowa w art. 40..oraz danych określonych w art. 67 ust. 1 ... kierując się wymaganiami europejskich organizacji normalizacyjnych, a w przypadku braku takich wymagań - wymaganiami innych międzynarodowych organizacji normalizacyjnych, których Rzeczpospolita Polska jest członkiem.

URZĄD REGULACJI TELEKOMUNIKACJI

Monitoring abonentów, prawomocny przechwyt informacji

Art. 71

Dane identyfikujące użytkowników wywołujących, są rejestrowane przez operatora na żądanie .. organów Operator, ... udostępnia dane, organom państwa wykonującym zadania na rzecz bezpieczeństwa i porządku publicznego w zakresie i na warunkach określonych w odrębnych przepisach.

URZĄD REGULACJI TELEKOMUNIKACJI

Łączenie sieci telekomunikacyjnych

Art. 87

Prezes Rady Ministrów określi, w drodze rozporządzenia, szczegółowe warunki współpracy komórek organizacyjnych i jednostek organizacyjnych określonych w art. 4 ust.1 z operatorami sieci publicznych, związanej z łączeniem sieci ...uwzględniając specyfikę działalności prowadzonej przez te jednostki.

TELZAS Sp. z o.o.
Szczecinek

Franciszek KALATA

SYSTEMY GWARANTOWANEGO ZASILANIA NA RZECZ OBRONNOŚCI PAŃSTWA

CENTRUM KONFERENCYJNE WP Grudzień 2001

Współczesne urządzenia i systemy informatyczne, układy zabezpieczeń, systemy alarmowe, centrale telefoniczne łączności przewodowej i bezprzewodowej będące na wyposażeniu współczesnej armii, wojskowe systemy dyspozytorskie wymagają bezprzerwowego lub gwarantowanego zasilania. Prawie w każdym z wymienionych, przypadków brak zasilania, po stronie DC lub po stronie AC, może okazać się bardzo przykry w skutkach a nawet może stwarzać zagrożenie dla życia ludzkiego. Jest więc bardzo istotne, aby zasilanie nie było tutaj ogniwem krytycznym w niezawodności działania określonego systemu. Najbardziej znaczące firmy projektujące oraz wytwarzające systemy zasilające tworzą urządzenia bardziej niezawodne, sprawne i mniejsze. Realizowanie tych zadań możliwe jest dzięki stosowaniu różnych metod.

Firma ***TELZAS*** od ponad dwudziestu pięciu lat skutecznie rozwiązuje problemy związane z bezprzerwowym zasilaniem zarówno prądem przemiennym, jak i prądem stałym odbiorników energii elektrycznej.

Burzliwy rozwój w elektronice, energoelektronice, a w szczególności w informatyce przyczynił się do ogromnego postępu również w zakresie urządzeń zasilających. Porównując wyroby produkowane na przełomie lat 70/80 z wyrobami produkowanymi dzisiaj, można zauważyć zmiany w parametrach ogólnych systemów zasilających:

- gabaryty zewnętrzne uległy zmniejszeniu ok. 3-4 krotnie;
- przeciętna sprawność wzrosła o ok.15-20%;
- masa urządzeń uległa zmniejszeniu ok. 3-4 krotnie.

Osiąganie odpowiednich parametrów technicznych oraz wysoki poziom ogólny tych wyrobów jest możliwy dzięki:

- nowoczesnym rozwiązaniom konstrukcyjnym;
- zachowaniu odpowiedniej technologii;
- odpowiednim rozwiązaniom układowym;
- unifikacji podzespołów oraz seryjności produkcji;
- dużej niezawodności urządzeń;
- stosowaniu odpowiednich elementów;
- kwalifikacjom i doświadczeniom kadry technicznej;
- wysokiej estetyce wyrobów;
- zapewnieniu jakości potwierdzonej np. certyfikatem ISO 9001, AQAP 110.

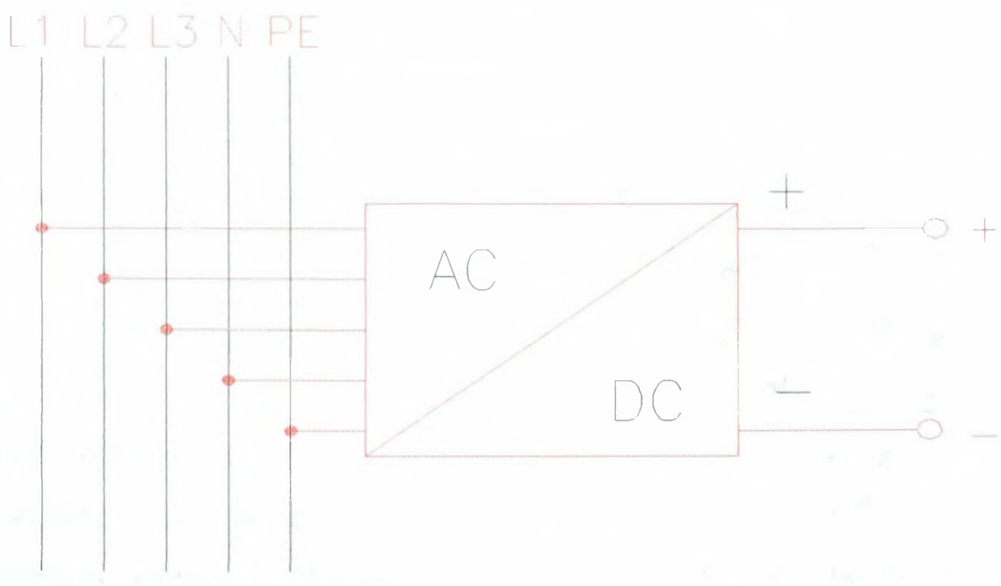
Podstawowymi elementami systemów zasilających są przekształtniki. W zależności od wykonywanej funkcji mogą to być np.: prostowniki, inwertery, przetwornice DC/DC

i inne. Współczesnym urządzeniom zasilającym stawia się bardzo wysokie wymagania. Do podstawowych wymagań można zaliczyć:

- wysoką stabilizację napięcia wyjściowego przy zmieniających się warunkach zewnętrznych (szeroki zakres zmian temperatur otoczenia, napięcia zasilania, natężenia prądu obciążenia);
- minimalne tętnienia na wyjściu;
- odporność na zwarcia obwodów wyjściowych;
- niewprowadzanie zakłóceń radioelektrycznych oraz odkształceń do sieci elektroenergetycznej;
- odporność na zakłócenia zewnętrzne;
- bardzo krótkie czasy regulowania oraz przełączania;
- praca urządzeń przy minimalnym poborze mocy biernej z sieci (stosowanie w prostownikach aktywnych kompensatorów mocy biernej);
- możliwie duża sprawność urządzeń;
- funkcjonalność i uniwersalność.

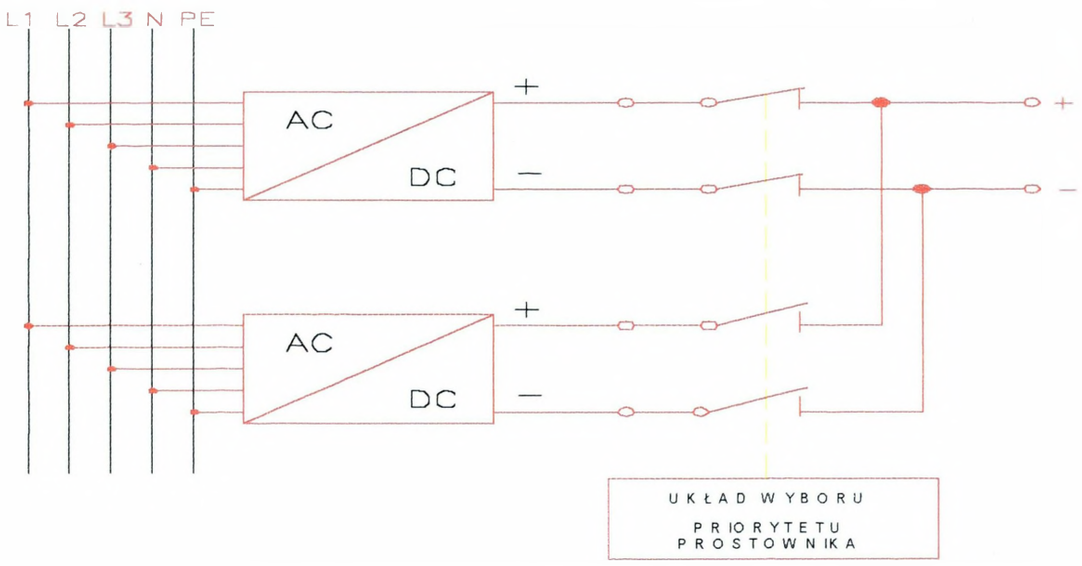
Wielomodułowość

Najogólniej system gwarantowanego zasilania można zbudować w oparciu o urządzenia monomodułowe lub wielomodułowe. Wybór systemu opartego o urządzenia monomodułowe czy wielomodułowe zależy od przeznaczenia. W sytuacji, gdy ciągłość zasilania nie ma decydującego znaczenia można zastosować systemy monomodułowe, pracujące samodzielnie (rys.1).



Rys.1. System monomodułowy pracujący samodzielnie

W przypadku awarii, system zmuszony będzie pracować wyłącznie na baterii akumulatorów do chwili usunięcia usterki lub wymiany urządzenia. W jednostkach o większej mocy wymiana urządzenia może stwarzać wiele problemów, gdyż posiadają one zwykle dość znaczne gabaryty i dość znaczną masę własną. Tak więc w celu uniknięcia tych problemów należałoby zastosować tutaj dodatkowy np. prostownik, który stanowiłby rezerwę (rys. 2).



Rys.2. System monomodułowy z prostownikami rezerwującymi się wzajemnie

W chwili uszkodzenia się prostownika podstawowego w sposób automatyczny załączony zostanie prostownik rezerwujący. Rozwiązanie takie jest dość drogie, gdyż obciążenie jakie może być dołączone stanowi tylko 50% możliwości całego systemu. Dodatkowo oba prostowniki nie starzeją się w jednakowym stopniu. Aby problem ten rozwiązać należy w sposób automatyczny lub ręczny zmieniać priorytet prostownika. Tak więc z punktu widzenia serwisowego oraz ekonomicznego systemy monomodułowe są stosunkowo mało atrakcyjne. Podstawą wielomodułowego systemu zasilającego są pracujące równolegle tranzystorowe prostowniki, inwertery, przetwornice DC/DC lub inne urządzenia. Charakteryzują się one wysoką niezawodnością, dużą sprawnością, bardzo dobrymi własnościami dynamicznymi oraz niewielkimi rozmiarami i masą.

Koncepcja systemów wielomodułowych umożliwia indywidualne dopasowanie zasilania do odpowiednich żądań użytkownika oraz daje możliwość dalszej rozbudowy systemu i tworzenia jego różnej konfiguracji. Elastyczność systemu jest bardzo istotnym elementem, ponieważ nie wymusza na projektancie precyzyjnego określenia ewentualnych

późniejszych różnych wariantów rozbudowy obiektu. Systemy te umożliwiają współpracę z odbiornikami w zakresie od kilku do kilku tysięcy amperów. Ich wielomodułowa budowa umożliwia, przy stosunkowo niskim koszcie, zabezpieczyć odpowiedni zapas mocy (mała moc prostownika rezerwowego).

Przykład

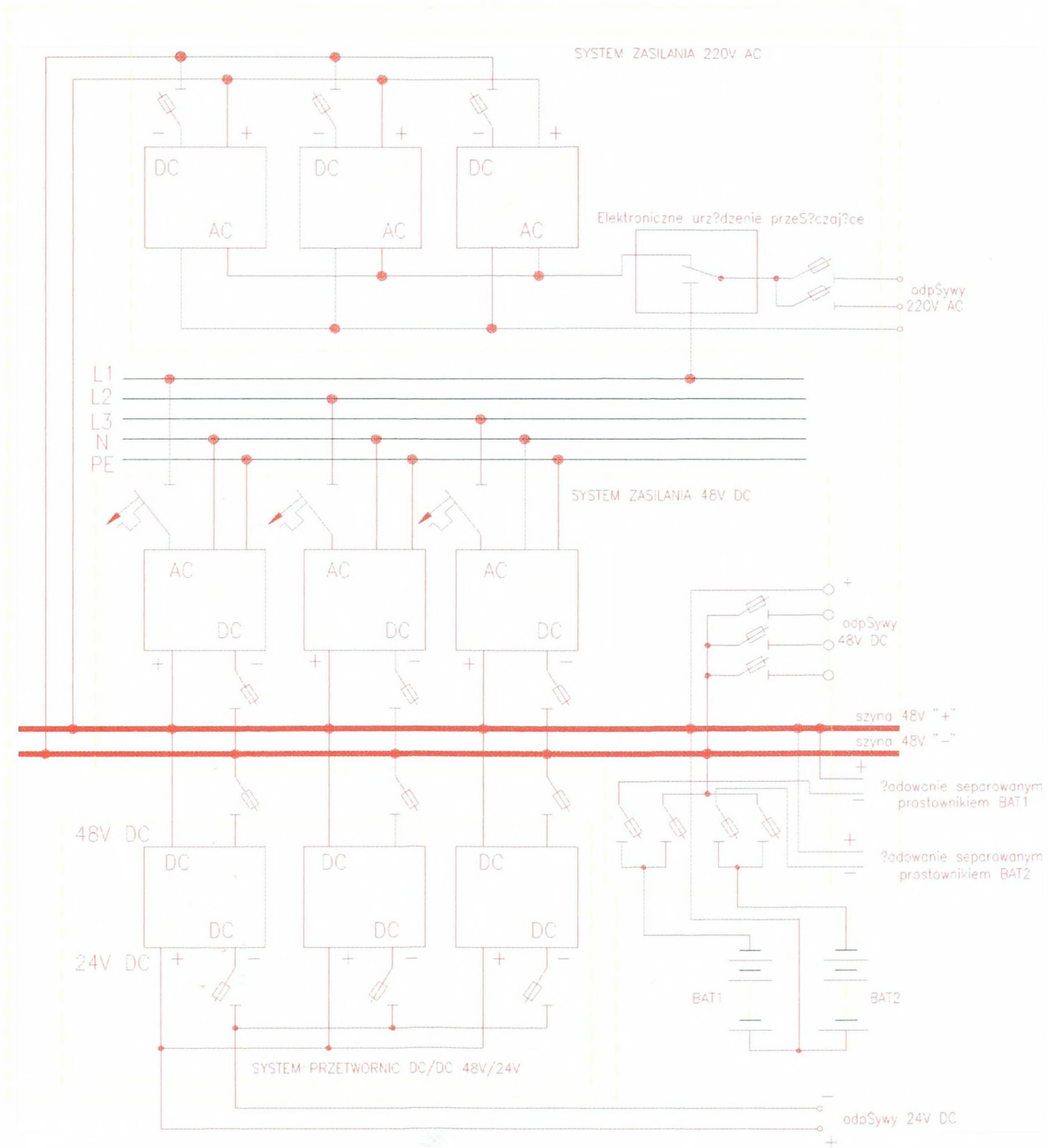
Porównajmy systemy o prądzie wyjściowym równym 50A.

W celu zagwarantowania poprawnej pracy urządzeń napięcia stałego należy zabezpieczyć system dodatkowym modułem. W przypadku urządzeń monomodułowych należy podłączyć dodatkowy prostownik o parametrach takich samych jak prostownik podstawowy. Tak więc cena całego systemu w zasadzie się podwaja. W przypadku urządzeń wielomodułowych dla systemu składającego się z prostowników 10A należy dołączyć dodatkowo jeden prostownik o prądzie znmionowym 10A. W przypadku uszkodzenia się jednego z pracujących równolegle prostowników, moduł uszkodzony odłącza się. System natomiast działa poprawnie i wysyła alarm zewnętrzny wskazujący rodzaj awarii.

Przykład ten dowodzi, że zapas mocy całego systemu, a zatem i koszt tego zapasu jest znacznie mniejszy w systemie opartym o urządzenie wielomodułowe.Urządzenia wielomodułowe sąrównieżwygodniejszepod względem serwisowym. W przypadku uszkodzenia jednego modułu, w prosty sposób, można go zamienić na sprawny moduł zapasowy. Prostownik uszkodzony można wysłać do producenta, a system cały czas jest w pełni sprawny. Służby obsługujące kilka obiektów opartych na tych samych modułach (przy różnych mocach systemu!) mogą posiadać w swoim podręcznym magazynie np. jeden taki prostownik, który może być wykorzystany w opisanym przypadku.

Wielomodułowość systemów gwarantowanego zasilania umożliwia również tworzenie systemów wielofunkcyjnych umieszczonych np. w jednej obudowie. Rys.3. przedstawia właśnie taki system oparty na rzeczywistych urządzeniach, w skład którego wchodzą:

- system zasilania napięciem 48VDC (1-8 prostowników każdy po 30A , pole odpływów 48VDC, pole bateryjne 48VDC, kontroler nadzorujący poprawną pracą prostowników);
- przetwornice 48VDC/24VDC (1-3 przetwornic o napięciu wyjściowym 24V każda po 12A);
- inwerter 230VAC wraz z elektronicznym urządzeniem przełączającym (max. moc wyjściowa 1-3,3kVA).



Rys. 3. Wielofunkcyjny system urządzeń wielomodułowych

System ten jest połączony z dwiema bateriami akumulatorów 48V (np. zamkniętych). Współpraca baterii akumulatorów wraz z prostownikami i odbiorami możliwa jest dzięki połączeniu tzw. "buforowemu na wprost" (dla odbiorów 48VDC o wąskim zakresie zasilania możliwa jest również współpraca przez kilkustopniowy

reduktor napięcia lub przetwornicę dodawczą). Specjalna charakterystyka prostowników umożliwia współpracę z baterią akumulatorów zamkniętych. Charakterystyka ta jest ściśle związana z temperaturą otoczenia baterii. Napięcie wyjściowe na prostownikach, co jest równoznaczne napięciu na baterii akumulatorów, zmienia się wraz ze zmianami temperatury otoczenia baterii. Wraz ze wzrostem temperatury otoczenia baterii maleje napięcie wyjściowe prostownika i odwrotnie. Zmiany te zależą od typu baterii akumulatorów i wynoszą -2÷8mV/K/ogn. Zależnie od potrzeb temperaturowy współczynnik korekcji napięcia można ustawiać dowolnie, w zakresie -2÷8mV/K/ogn.

Dołączone do wspólnej baterii akumulatorów 48V przetwornice DC/DC, umożliwiają zasilanie odbiorów wymagających bardzo wąskiego zakresu zasilania stabilnym napięciem np. 24VDC (±1%). Przetwornice te połączone są równolegle i zapewniają galwaniczną izolację między obwodami wejścia i wyjścia. Ilość przetwornic zależy od zapotrzebowania mocy odbiorów i zachowana jest zasada redundancji (n+1).

Do tej samej baterii akumulatorów 48V dołączone jest wejście inwertera 220VAC. Wyjście inwertera połączone jest z elektronicznym urządzeniem przełączającym. Dzięki temu układowi możliwa jest praca z priorytetem sieci elektroenergetycznej (sieć jest podstawowym źródłem zasilania, inwerter natomiast stanowi rezerwę) lub priorytetem inwertera (inwerter jako podstawowe źródło zasilania, sieć elektroenergetyczna stanowi rezerwę). Czas przełączania w obu przypadkach jest nie dłuższy jak 2ms. i nie jest "wyczuwalny" przez urządzenia 220VAC 50Hz.

Konfiguracja taka oraz umieszczenie w jednej obudowie o wymiarach 2000X600X600 mm jest bardzo wygodna pod względem eksploatacyjnym. Zbudowanie takiego systemu jest możliwe dzięki wielomodułowej budowie poszczególnych urządzeń składowych.

Na obiektach, gdzie występują odbiory wymagające różnych napięć zasilania opisane rozwiązanie jest optymalne. Wydaje się tu bezcelowe stosowanie baterii akumulatorów o różnych napięciach (np. 24VDC, 48VDC). Stosowanie jednej baterii akumulatorów sprawia, że generalnie system bezprzerwowego zasilania odbiorników wymagających różnych napięć zasilania jest korzystny.

Z powyższych rozważań wynika jak bardzo istotny jest prawidłowy wybór odpowiedniego systemu bezprzerwowego zasilania. Celem optymalnej konfiguracji systemu jest maximum niezawodności przy minimum kosztów. Systemy oparte o urządzenia wielomodułowe zalety te posiadają.

Monitoring

Współczesnym systemom bezprzerwowego zasilania stawia się coraz większe wymagania. Podstawowym wymaganiem jest niezawodność. Aby temu wymaganiu sprostać systemy zasilające, oprócz niezawodnej pracy, powinny mieć możliwość łatwej kontroli poprawności działania oraz w miarę potrzeby, podejmowania odpowiednio szybko decyzji i korygowanie ewentualnych nieprawidłowości. Bardzo intensywny w ostatnim okresie postęp w informatyce, umożliwił wykorzystanie tej dziedziny do tych właśnie celów.

Zadaniem komputerowego systemu nadzoru jest ciągła kontrola systemów zasilających a w przypadku wystąpienia alarmu przekazanie sygnału do centrum. Obecnie wszystkie siłownie produkowane przez ***TELZAS*** przystosowane są do takich systemów.

Dzięki istnieniu komputerowych systemów nadzoru otwierają się całkowicie nowe perspektywy w zakresie optymalizacji alokacji personelu do prac związanych z utrzymaniem sprzętu i podczas jego nieprawidłowej pracy.

System nadzoru posiada swoje centrum - Centrum Nadzoru - gdzie zbierane są informacje na temat pracy wszystkich urządzeń przyłączonych do systemu. Obiekty, w których zainstalowane są nadzorowane urządzenia mogą być rozmieszczone na dużym obszarze, komunikacja między Centrum Nadzoru i obiektami odbywa się za pomocą linii transmisyjnych. Przeważnie są to linie telefoniczne lub sieci logiczne.

Podsumowanie

Bardzo duża paleta, produkowanych przez ***TELZAS,*** rodzajów i typów urządzeń zasilających zarówno napięcia przemiennego 230VAC (od 1kVA do kilkudziesięciu kVA), jak również napięcia stałego (12V, 24V, 48V, 60V, 110V, 220V), opartych na tranzystorowych równolegle pracujących prostownikach 6A, 15A, 30A, 70A, 160A, umożliwia konfigurowanie systemów bezprzerwowego zasilania praktycznie w dowolnych zakresach mocy. Możliwość uaktywniania różnych charakterystyk ładowania (ładowanie buforowe, ładowanie samoczynne, ładowanie dozorowane) oraz możliwość korekcji napięcia wyjściowego w funkcji temperatury pozwala utrzymywać baterię akumulatorów w optymalnych warunkach. Dodatkowo stosowanie urządzeń takich jak: przetwornice wyrównujące, przetwornice dodawcze, reduktory napięcia, przetwornice DC/DC, inwertery DC/AC oraz komputerowy system nadzoru pozwalają zaprojektować bardzo nowoczesny system gwarantowanego zasilania urządzeń telekomunikacyjnych, informatycznych, automatyki, zabezpieczeń i inne.

Oferta ***TELZASU*** obejmuje kompleksową obsługę obiektów w zakresie bezprzerwowego zasilania prądem stałym i przemiennym. Oferujemy następujący sprzęt:

- siłownie prądu stałego i przemiennego;
- przetwornice DC/DC;
- tablice prądu stałego i przemiennego;
- UPS;
- baterie akumulatorów;
- generatory prądotwórcze;
- komputerowe systemy nadzoru;
- klimatyzację;
- sprzęt pomocniczy (tablice prądowe, zabezpieczenia skrzynki rozdzielczej).

Długoletnia współpraca z Ministerstwem Obrony Narodowej dowodzi jak ważne jest dalsze pogłębianie współpracy w zakresie techniki na polu cywilno-wojskowym celem osiągania optymalnych wyników oraz wdrażania nowoczesnych urządzeń zasilających w Wojsku Polskim.

PODSUMOWANIE

PODSUMOWANIE

Podstawowym celem polityki naszego państwa jest zapewnienie mu szeroko rozumianego bezpieczeństwa, co stanowi warunek wstępny harmonijnego rozwoju w wymiarze społecznym i gospodarczym. W praktyce polityka ta wyrażana jest w dążeniu do utrzymania suwerenności i nienaruszalności granic RP oraz w rozwijaniu jego potencjału obronnego zdolnego do przeciwdziałania niebezpieczeństwu ewentualnej agresji. Zapewnienie bezpieczeństwa i obronności państwa uzyskuje się poprzez stosowanie prawnie usankcjonowanych środków i metod, adekwatnych do zaistniałej sytuacji zewnętrznej i wewnętrznej.

Stosunki międzynarodowe mogą cechować się wzajemnym zrozumieniem, partnerską współpracą i wolą poszukiwania consensusu. Stwarza to możliwość pokojowego i bezpiecznego rozwoju narodu. Brak dobrej woli do negocjacji i określenia warunków porozumienia może doprowadzić do zaostrzenia różnych form wzajemnych oskarżeń, których skutkiem może być stan zagrożenia bezpieczeństwa państwa, a w krańcowych przypadkach - agresja zbrojna. Zagrożeniem dla bezpieczeństwa państwa, jest więc ograniczenie lub utrata warunków jego bytu i rozwoju, bądź naruszenie lub utrata jego suwerenności i integralności terytorialnej. Zagrożenia te mogą mieć charakter militarny i pozamilitarny.

W przypadku wystąpienia kryzysów w bezpośrednim otoczeniu, Polska może być narażona, zarówno na oddziaływania militarne, jak i pozamilitarne. Istotnym problemem jest to, że kryzysy mają zwykle duży zasięg i obejmują różne dziedziny funkcjonowania państwa, czyli mają charakter wszechogarniający. Rozprzestrzeniają się, pokonując wszelkie granice, zwłaszcza polityczne, geograficzne, organizacyjne czy socjologiczne. Oznacza to, że wiarygodne uporządkowane (opracowane) informacje dotyczące zaistniałego kryzysu muszą szybko trafić do wszystkich zainteresowanych stron, reprezentujących różne poziomy kierowania i zarządzania, a więc lokalny, wojewódzki i krajowy, funkcjonujące zarówno w sektorze publicznym, jak i prywatnym. Istnieje ponadto potrzeba zintegrowania informacji pomiędzy wieloma dziedzinami, organizacjami i regionami geograficznymi.

Zagrożenia militarne mogą przejawiać się w postaci: prowokacji, incydentów granicznych, przypadków naruszania granicy przez ugrupowania zbrojne, naruszania polskiej przestrzeni powietrznej i polskich wód terytorialnych, prowadzenia w bliskości polskiej granicy działań zbrojnych, przenikania lub działania na polskim terytorium grup

terrorystycznych lub sabotażowo-dywersyjnych. Oddziaływania pozamilitarne w takiej sytuacji mogą mieć charakter: rozszerzenia się przestępczości zorganizowanej, niekontrolowanych masowych migracji ludności, skażeń promieniotwórczych, chemicznych lub zakażeń biologicznych, epidemii, itp. W odniesieniu do zagrożeń wojennych ocenia się, że obecnie zdecydowanie zmniejszyła się groźba wybuchu wojny globalnej i konfliktu ogólnoeuropejskiego. Nie można jednak wykluczyć pojawienia się takiej ewentualności w bardziej odległej perspektywie czasowej.

W rezultacie zrealizowanych porozumień rozbrojeniowych, istniejący poziom uzbrojenia konwencjonalnego w otoczeniu Polski uniemożliwia przeprowadzenie z zaskoczenia agresji na dużą skalę. Zagrożenie takie mogłoby zostać wykryte ze znacznym wyprzedzeniem. Dlatego ewentualna agresja z zaskoczenia może mieć głównie wymiar lokalny. Odnosi się to także do groźby agresji na któregokolwiek naszego sojusznika z NATO. Jest zatem mało prawdopodobne, aby Polska mogła być w niezbyt odległym czasie obiektem agresji militarnej na dużą skalę, zagrażającej jej suwerenności oraz integralności terytorialnej, a także wymagającej mobilizacji i zaangażowania całego potencjału obronnego państwa. Nie można jednak wykluczyć wystąpienia tego typu zagrożenia wojennego w dalszej perspektywie. Większe natomiast staje się prawdopodobieństwo niespodziewanego wystąpienia zagrożenia o małej skali, lokalnego naruszenia terytorium Rzeczypospolitej Polskiej lub wręcz przypadkowego incydentu granicznego, do którego mogłoby dojść w razie niebezpiecznego rozwoju sytuacji w bezpośrednim otoczeniu strategicznym Polski. Agresja zbrojna zależnie od jej skali może przybrać formy:

- kampanii zaczepnej na pełną skalę prowadzonej, w wymiarze lądowym, powietrznym i morskim lub ograniczonej operacji na jednym kierunku;
- uderzeń rozproszonych (na kilku kierunkach) o ograniczonym rozmachu;
- działań grup terrorystycznych i dywersyjno-rozpoznawczych na wybranych kierunkach lub celach;
- rajdów grup zbrojnych o różnym składzie i wyposażeniu, aktów terroryzmu, dywersji i innych niekonwencjonalnych działań bojowych.

Wojnę określa się jako stan walki orężnej między państwami, albo jako przeciwstawienie stanu pokoju. Określenia te, które w przeszłości stanowiły podstawę podziału prawa międzynarodowego na dwie dziedziny - prawo wojny i pokoju - nie odpowiadają jednak współczesnym tendencjom zmierzającym do objęcia przepisami prawa działań o charakterze zbrojnym, także wówczas, gdy państwa z różnych przyczyn

nie uważają tych działań za wojenne. Dlatego coraz częściej ma zastosowanie szersze określenie „konflikt zbrojny". Istotne znaczenie ma podział konfliktów zbrojnych na konflikty międzynarodowe i konflikty nie mające charakteru międzynarodowego. Zakres zobowiązań w odniesieniu do pierwszej kategorii konfliktów, jest znacznie szerszy aniżeli w odniesieniu do kategorii drugiej.

Należy jednak pamiętać, że w świetle doświadczeń naszej epoki linie podziału na konflikty międzynarodowe i nie mające charakteru międzynarodowego nie są wyraźne, często bowiem konflikt początkowo jak najbardziej wewnętrzny, na skutek interwencji z zewnątrz nie zawsze zresztą w formie wyłącznie oddziałów ekspedycyjnych, ale przez pomoc ekspertów i dostawy broni, nabiera charakteru międzynarodowego. Pojęciem o zasięgu szerszym niż wojna i konflikt zbrojny jest „użycie siły". Obejmuje ono bowiem nie tylko przypadki, w których ma miejsce starcie sił zbrojnych dwóch lub więcej przeciwników, ale także akcje zbrojne, które nie napotykają zorganizowanego oporu, jak to ma często miejsce przy interwencjach zbrojnych, demonstracjach o charakterze wojennym.

Jak wspomniano wcześniej, w otoczeniu Polski, istnieje większe prawdopodobieństwo wystąpienia konfliktu lokalnego bądź regionalnego. Może on być wynikiem trudności w transformacji systemowej w niektórych państwach naszego regionu. Zagrożeniem dla Polski, nawet gdyby znalazła się poza bezpośrednią strefą konfliktu, byłoby przeniesienie działań militarnych lub ich skutków na nasze terytorium. Konflikty tego rodzaju charakteryzować się mogą stosunkowo krótkim czasem przygotowania oraz zmienną intensywnością od pierwszych dni działań zbrojnych. Pozbawione kontroli i ograniczeń politycznych konflikty lokalne mogą prowadzić do eskalacji, angażowania w nie innych państw oraz do przekształcenia się w konflikt regionalny. Celem starć zbrojnych zwaśnionych stron może być opanowanie spornego terytorium lub wymuszenie ustępstw na płaszczyźnie politycznej czy też ekonomicznej. W razie objęcia Polski takim konfliktem należy się liczyć z możliwością dysponowania selektywnych uderzeń lotniczych i rakietowych oraz aktów terroru na całym terytorium państwa, a nawet zajęcia jego części.

Niebezpieczeństwo konfliktów regionalnych i lokalnych potęgują zagrożenia pozamilitarne. Ich znaczenie, zasięg oraz możliwe rodzaje wykazują tendencję wzrostową przybierając rozmiar regionalny, a nawet kontynentalny. Narastającym objawom degradacji społecznej w niektórych państwach objętych transformacją ustrojową towarzyszą zjawiska patologii, tworzenia sprzyjających warunków do rozwoju

międzynarodowej przestępczości zorganizowanej, obejmującej swoim zasięgiem całe regiony. Najbardziej niebezpieczną formą zagrożenia wynikającą z międzynarodowej aktywności przestępczej staje się terroryzm przybierający różne oblicza i zakładający różne cele. Następstwem działań przestępczości międzynarodowej jest także zorganizowany przemyt, korupcja struktur władzy, handel narkotykami oraz potencjalne zagrożenie skażeniem środowiska mogące wystąpić na skutek nielegalnego obrotu materiałami rozszczepianymi, chemicznymi lub biologicznymi.

Polska w coraz większym stopniu narażona będzie na skutki wynikające z rozprzestrzeniania technologii podwójnego zastosowania, broni masowego rażenia i środków jej przenoszenia. Problemy te będą występować, zarówno w okresie pokoju, ze względu na położenie geograficzne kraju, który stanowi obszar tranzytowy przy nielegalnym obrocie technologiami i materiałami służącymi do produkcji broni masowego rażenia, jak też w okresie kryzysu i wojny. Wtedy broń masowego rażenia może być użyta przez potencjalnego agresora na wybrane obiekty rozmieszczone w dowolnym miejscu na obszarze państwa.

W świetle zagrożeń występujących aktualnie i mogących mieć miejsce w bliższej i dalszej przyszłości, ogromnego znaczenia nabiera sprawa kierowania systemem obronności państwa. Kierowanie to uznano powszechnie za szczególną formę zarządzania, stanowiącą zespół czynności związanych z racjonalnym wykorzystaniem potencjału ludzkiego, gospodarczego i środków walki na potrzeby obrony kraju przed agresją zbrojną.

Kierowanie systemem obronności, a także przygotowaniami do obrony państwa odbywa się w układzie organizacyjno - funkcjonalnym obejmującym: organa władzy, administrację rządową i samorządową z ich ustawowymi kompetencjami, jak również infrastrukturę gospodarczą. Najbardziej newralgicznym okresem w kierowaniu państwem jest przechodzenie z pokojowego systemu kierowania na system wojenny. Dlatego też przyjmuje się zasadę dokonywania jak najmniejszych zmian w kierowaniu państwem w stosunku do zasad i rozwiązań obowiązujących w czasie pokoju.

W celu zapewnienia sprawnego funkcjonowania najwyższych organów władzy, administracji państwa i sił zbrojnych w czasie przechodzenia ze stanu pokojowego na wojenny, już w czasie pokoju tworzy się odpowiednie struktury organizacyjne. Ich zadaniem jest zapewnienie utrzymania ciągłości kierowania oraz sprawnego przejścia gospodarki i sił zbrojnych ze struktury pokojowej na wojenną. W wielu krajach o rozwiniętych demokracjach struktury te są takie same lub zbliżone. System kierowania obronnością państwa, obok podsystemu militarnego i pozamilitarnego jest jednym

z zasadniczych elementów systemu obronności. Jego rola polega na informacyjnym sprzężeniu poszczególnych elementów systemu obronności w jednolitą i sprawnie funkcjonującą całość. O jego efektywności decyduje nie tylko właściwy dobór kadr na kierownicze stanowiska i funkcje, ale i jego struktura gospodarcza, a przede wszystkim infrastruktura telekomunikacyjna i informatyczna. Kierowanie obronnością państwa jest procesem bardzo złożonym, wymagającym posiadania odpowiednio przygotowanego systemu kierowania, funkcjonującego nieprzerwanie w okresie pokoju, kryzysu i wojny. Dotychczasowy system kierowania obronnością funkcjonował opierając się na niezbyt aktualnych dokumentach normatywnych.

Przyjęcie Konstytucji RP zapoczątkowało okres budowy nowego systemu kierowania, dostosowanego do zaistniałych zmian polityczno-militarnych. Jednak wiele zapisów konstytucyjnych, bez uszczegółowienia w ustawach i aktach wykonawczych, może spowodować ich niejednoznaczną interpretację, szczególnie w zakresie kompetencji poszczególnych organów kierowania. Dlatego też niezbędne jest przygotowanie ustaw szczegółowo regulujących sprawy obronności państwa, a zwłaszcza problematykę dotyczącą systemu kierowania obronnością. Ustawy te powinny w sposób jednoznaczny określić miejsce i rolę poszczególnych organów kierowania oraz ich zadania i kompetencje w systemie kierowania państwem w najbardziej krytycznych sytuacjach - w czasie zagrożenia militarnego i wojny.

Sytuacje kryzysowe wymagają podjęcia skutecznych działań w celu zapewnienia ciągłości świadczenia usług telekomunikacyjnych dla ludności oraz utrzymania dzierżawionych usług międzynarodowych. Szczególnie duże znaczenie ma zapewnienie łączności dyplomatycznej pomiędzy państwami członkowskimi NATO oraz łączności ważnej dla członków sojuszu w ramach struktur, a także pomiędzy sojuszem i innymi państwami. Łączność ta powinna umożliwić skuteczne działania na rzecz uniknięcia kryzysu, a jeśli działania te okażą się nieskuteczne, powinna umożliwić podejmowanie wysiłków na rzecz osiągnięcia pokoju. W czasie kryzysów i wojny konieczne jest zastosowanie odpowiednich środków kontroli, po to zwłaszcza aby umożliwić podjęcie odpowiednich działań w zakresie zestawiania łączy bezpośrednich i obejściowych pomiędzy członkami sojuszu i innymi państwami.

W tym kontekście „środki kontroli" oznaczają zarządzanie łączami i ruchem obsługiwanym przez te łącza. Na żądanie właściwych władz krajowych operatorzy telekomunikacyjni powinni stosować odpowiednie środki kontroli w odniesieniu do usług publicznych i dzierżawionych usług międzynarodowych. Rozwiązania tego rodzaju mogą

doprowadzić do poszerzenia zwykłych funkcji zarządzania siecią sprawowanych w czasie pokoju. W celu zagwarantowania skutecznego kontrolowania międzynarodowych usług telekomunikacyjnych, zarówno publicznych, jak i dzierżawionych, ważne jest, aby wszystkie kraje członkowskie NATO wprowadziły uzgodnione środki kontroli jednocześnie respektując przy tym odpowiednie rozporządzenia NATO. W celu zapewnienia wysokiego poziomu usług telekomunikacyjnych możliwe jest budowanie sieci specjalnych, wydzielonych z sieci publicznych na potrzeby władz krajowych w sytuacjach szczególnych zagrożeń, kryzysów międzynarodowych lub wojny. Krajowe sieci specjalne mają z reguły ograniczoną pojemność i możliwości obsługi ruchu telekomunikacyjnego. W czasie pokoju lub we wczesnej fazie kryzysu korzystne jest łączenie poszczególnych krajowych sieci specjalnych ze sobą w celu zapewnienia łączności właściwym abonentom specjalnym. Wykonywanie tego rodzaju czynności zależne jest od skali wdrożenia odpowiednich systemów sygnalizacji umożliwiających współpracę sieci międzynarodowych i w efekcie wysoką jakość transmisji. W niektórych sytuacjach konieczna może się okazać rozbudowa tych sieci pod kątem obsługi ruchu dodatkowego, generowanego przez abonentów specjalnych. W celu zagwarantowania użyteczności sieci specjalnych i ich łączy na potrzeby zestawiania połączeń w warunkach wojennych, systemy i łącza tych sieci muszą być maksymalnie uodpornione, by prawdopodobieństwo bezprzerwowej łączności było możliwie wysokie. Wymaga to zaimplementowania różnych tras przesyłania ruchu oraz zastosowania wielu dróg łączy obejściowych. Biorąc pod uwagę ograniczoną pojemność krajowych sieci specjalnych, kraje członkowskie NATO mogą wprowadzić kontrolę połączeń zewnętrznych przychodzących do sieci.

W krajach Europy Zachodniej, zwłaszcza takich jak Francja, Niemcy, powszechnie wykorzystywane są szerokie możliwości systemów cyfrowych. W krajach tych na potrzeby obronności stworzono jednolite cyfrowe systemy łączności w postaci krajowych sieci specjalnych. Sieci te łączą sferę pozamilitarną kierowania obronnością kraju tzn. Policję, Straż Graniczną, Straż Pożarną, ośrodki kierowania administracją państwową, itp. jak również sferę militarną tzn. stanowiska kierowania obroną. Elementy, o których mowa wyżej, tworzą spójny system kierowania obronnością racjonalnie wykorzystujący infrastrukturę teletechniczną kraju umożliwiając przez to tworzenie spójnych systemów kierowania obronnością i obroną. Systemy takie, z uwagi na jednorodność sprzętową, umożliwiają wykorzystywanie przez kierujących obroną wspólnych systemów informatycznych zwiększając tym samym szybkość obiegu informacji, co wpływa

korzystnie na ich efektywność. Zaspokojenie ciągle rosnących potrzeb użytkowników systemów łączności w zakresie usług teleinformatycznych, będzie możliwe poprzez wykorzystanie nowych szerokopasmowych technik telekomunikacyjnych. Technologie te zapewnią organom kierującym sytuacjami kryzysowymi niespotykane dotychczas możliwości usługowe dotyczące: zwłaszcza szybkiej wymiany danych, transferu dużych zbiorów informacji, rozproszonego przetwarzania danych, wymiany danych w czasie rzeczywistym, przekazywania obrazów ruchomych, itp.

Podobne systemy, budowane w krajach będących członkami NATO, charakteryzują się wykorzystywaniem technik szerokopasmowych - ATM, ISDN, IP oraz komercyjnych systemów trankingowych. Niezależnie od stosowania nowych technologii, każdy kraj w swoich projektach budowy nowych systemów, uwzględnia istniejącą infrastrukturę telekomunikacyjną. Dla bezkolizyjnej współpracy tych systemów dąży się do stosowania urządzeń wykonanych wg standardów ITU. Do współpracy z innymi systemami np. militarnym, wykonanymi wg standaryzacji STANAG i EUROCOM, powinny być stosowane specjalne interfejsy (gatway'e) międzysystemowe. Nowe technologie teleinformatyczne umożliwiają tworzenie wydzielonych sieci dla zamkniętych grup użytkowników ze specjalizowanymi usługami, co jest istotne dla tego typu zastosowań.

Charakterystyka mobilnych systemów radiotelefonicznych wskazuje na możliwości łatwego i wygodnego ich zastosowania w różnych uwarunkowaniach operacyjnych. Podyktowane to jest głównie zgodnością standaryzacyjną z innymi systemami, elastycznością wyboru pasma częstotliwości (dla systemów trankingowych) oraz łatwością zastosowania w koniecznych miejscach funkcjonowania systemu. Urządzenia wykonane w nowych technologiach teleinformatycznych są podatne na zarządzanie, co sprawia, że można dokonywać rekonfiguracji systemu dopasowując go do określonych wymagań i potrzeb stanów nadzwyczajnych.

Stowarzyszenie Polski z Unią Europejską oraz potrzeba utrzymania ścisłej współpracy z NATO wymuszają konieczność posiadania systemu specjalnego, kompatybilnego z ich systemami. Wynika stąd konieczność prowadzenia konsultacji i dokonywania wymiany doświadczeń w dziedzinie organizacji i zabezpieczenia funkcjonowania systemu łączności specjalnej z przedstawicielami państw Europy Zachodniej. Systemy specjalne państw UE posiadają następujące cechy:

a) są cyfrowe o kanale podstawowym 16 kbit/s i hierarchii zwielokrotnienia od 3 kanałów (48 kbit/s) do 120 kanałów (2048 kbit/s);

b) dysponują typowymi strumieniami traktowymi: 128, 256, 512, 1024 i 2048 kbit/s (USA wykorzystują także 4096 kbit/s),

c) wykorzystują w węzłach sieci automatyczne łącznice kanałów podstawowych 16 kbit/s o pojemnościach 120, 240 i 480 kanałów,

d) eksploatują jako media teletransmisyjne cyfrowe i analogowe zasoby sieci stacjonarnych, głównie dzierżawione od operatorów państwowych (również od prywatnych).

e) dzierżawią z zasobów cyfrowych głównie:
   - podstawowe grupy cyfrowe 2048 kbit/s PCM (łącznice tworzą na ich bazie strumienie 120 kanałowe),
   - kanały 64 kbit/s PCM (łącznice tworzą na ich bazie strumienie 4 kanałowe),

f) wykorzystują niezależnie od zasobów stacjonarnych, także okresowo rozwijane polowe środki radioliniowe o przepływnościach 128...2048 kbit/s,

g) wykorzystują uniwersalnie do rozmów telefonicznych (przy użyciu modulacji delta) oraz do rozmaitych transmisji danych z szybkościami do 16 kbit/s. kanały podstawowe 16 kbit/s doprowadzane do abonenta.

h) wykorzystują rządowe informatyczne i zautomatyzowane systemy kierowania,

i) charakteryzują się dwoma poziomami zabezpieczeń (utajniania) sieci:
   - bezpośrednio u abonenta za pomocą indywidualnych urządzeń utajniających kanału 16 kbit/s. Kanał ten jest odtajniany dopiero u adresata (zasada ciągłości utajniania),
   - pośrednio, poprzez utajnianie wszystkich traktów grupowych (międzycentralowych) za pomocą grupowych urządzeń utajniających.
   - wykorzystuje się dodatkowe utajnianie programowe (w komputerach osobistych abonentów).

W ramach aktualnych tendencji rozwojowych zautomatyzowanych stanowisk kierowania i dowodzenia, wymienia się trzy grupy wymagań stawianych przed systemami łączności:

- trwałości - a więc zapewnienia odporności na zakłócenia, dużej niezawodności i żywotności, co wiąże się z budową sieci o strukturze siatkowej;
- skrytości - zapewnienia utajniania z wymaganą mocą kryptograficzną;
- mobilności – tzn. zachowania ciągłości łączności w czasie przemieszczania się stanowisk kierowania i dowodzenia.

System łączności (teleinformatyczny) powinien umożliwiać przesyłanie informacji do korespondentów w sposób bezpieczny. Reorganizacja systemu obronności państwa pociągać będzie za sobą jego przebudowę, polegającą na dynamicznej zmianie funkcji i aktywności poszczególnych stanowisk, dokonywana w celu dostosowania struktury kierowania obronnością państwa do aktualnej sytuacji stanu nadzwyczajnego, możliwości realizacyjnych i potrzeb, spowoduje potrzebę rekonfiguracji systemu łączności.

System łączności powinien nadążać za dynamicznymi zmianami struktury organizacyjnej stanowisk kierowania i dowodzenia. Realizacja zadań stawianych nowoczesnemu systemowi kierowania obronnością państwa będzie integralnie związana z permanentną dynamiczną rekonfiguracją jego struktury. Rekonfiguracja ta polegać będzie głównie na zmianie funkcji poszczególnych stanowisk kierowania spowodowanej aktualną sytuacją. System łączności budowany na potrzeby systemu kierowania obronnością, przy zapewnieniu wysokiej niezawodności działania, powinien zapewnić ciągłość łączności oraz umożliwić wymianę informacji między poszczególnymi stanowiskami w postaci różnego typu wiadomości i baz danych. Spełnienie tych wymagań możliwe jest jedynie w nowoczesnych systemach organizacji łączności, w których wszystkie ogniwa (węzły komutacyjne) połączone ze sobą na zasadzie równorzędności tworzą strukturę niehierarchiczną. Stosowanie dynamicznego poszukiwania abonenta w sieci czyni taki system łączności odpornym na zniszczenia i podatnym na dynamiczną rekonfigurację całej sieci. Docelowo system łączności na potrzeby zapewnienia bezpieczeństwa i kierowania obronnością państwa, według przyjętych założeń, powinien stanowić zintegrowany pod względem organizacyjnym i technicznym zespół węzłów, traktów i linii łączności (stałych i budowanych środkami polowymi), urządzeń komutacyjnych oraz końcowych, zapewniających korzystanie z niezbędnych usług telekomunikacyjnych wszystkim organom kierowania i dowodzenia funkcjonującym w ramach tego systemu. Wymagania najwyższych organów władzy, administracji państwowej i sił zbrojnych wobec telekomunikacji są szczególne. Zaliczyć do nich należy:

- utrzymanie wyprzedzającej gotowości systemu w każdej sytuacji, a przede wszystkim w stanach nadzwyczajnych;
- zapewnienie bezpieczeństwa przekazywanych informacji i ochrony systemu;
- zapewnienie adaptacyjności i mobilności systemu;
- zintegrowanie rozwiązań technicznych w celu zapewnienia współdziałania wszystkich elementów systemu teleinformatycznego;
- uzyskanie efektywności ekonomicznej rozwiązań systemowych.

Realizacji przedstawionych wymagań i zadań powinny sprzyjać:

- jednoznacznie sformułowane i skoordynowane potrzeby organów władzy i administracji w zakresie usług teleinformatycznych;
- wyraźnie określone założenia techniczne i organizacyjne dotyczące wszystkich elementów systemu;
- możliwość wyboru najkorzystniejszych rozwiązań spełniających powyższe wymagania ogólne integrujące potrzeby użytkowników z uwzględnieniem ich specyfiki, np. sił zbrojnych, policji, straży pożarnej, urzędów ochrony państwa, celnego, itp.

Podstawową cechą określającą stopień przydatności danego systemu telekomunikacyjnego na potrzeby najwyższych organów władzy i administracji państwa jest możliwość hermetyzacji czyli zapewnienia najważniejszym abonentom priorytetowego dostępu do świadczonych usług. Cechą sieci hermetycznych jest to, iż tworzą zamknięte systemy całkowicie niedostępne dla innych abonentów. Sieci takie, poprzez powszechne stosowanie urządzeń kryptograficznych, umożliwiają użytkownikom prowadzenie niejawnej korespondencji. Zaspokojenie ciągle rosnących potrzeb użytkowników, systemów łączności w zakresie usług teleinformatycznych, będzie możliwe poprzez wykorzystanie nowych technik i technologii telekomunikacyjnych. Technologie te zapewnią organom kierującym sytuacjami kryzysowymi niespotykane dotychczas możliwości usługowe dotyczące: szybkiej wymiany danych, transferu dużych zbiorów informacji, rozproszonego przetwarzania danych, wymiany danych w czasie rzeczywistym, przekazywania obrazów ruchomych, itp.

Społeczeństwo staje się społeczeństwem informacyjnym, gdy osiąga stopień rozwoju oraz wysoki poziom skomplikowania procesów społecznych i gospodarczych wymagający zastosowania nowych technik gromadzenia, przetwarzania, przekazywania i użytkowania olbrzymiej masy informacji generowanych przez owe procesy. W takim społeczeństwie informacja i wynikająca z niej wiedza oraz stosowane technologie są podstawowym czynnikiem wytwórczym, natomiast wszechstronnym czynnikiem rozwoju jest wykorzystywanie teleinformatyki. Szybsze docieranie do pełniejszych, bardziej wiarygodnych informacji ułatwia podejmowanie optymalnych decyzji, co jest szczególnie ważne w okresie stanów nadzwyczajnych oraz umożliwia szybsze zaspokajanie potrzeb społecznych i obsługę niezbędnych podmiotów gospodarczych.

W sytuacji teoretycznie idealnej, polityka decydowałaby o wymaganiach technicznych. Wymagania techniczne przesądziłyby o projekcie systemu, a ten z kolei

wymagałby doboru i zakupu komponentów technicznych odpowiednich dla wdrożenia właściwych procedur. W takiej sytuacji zostałaby sformułowana polityka adekwatna do wszystkich przewidywanych sytuacji i możliwe byłoby uniknięcie marnowania czasu i środków na zakupienie lub stosowanie systemów, które nie odpowiadają ich docelowemu przeznaczeniu. W takiej sytuacji „wzorcowej", w której czas i środki byłyby nieograniczone, celowe byłoby zdefiniowanie i wdrożenie krajowej polityki antykryzysowej przed rozwinięciem jakiegokolwiek potencjału operacyjnego.

Społeczeństwo informacyjne tworzy warunki do uzyskania wysokiej sprawności administracji publicznej, obniżenia z czasem jej kosztów, zintegrowania różnych jej części we współpracujący system, za pośrednictwem technik przetwarzania i przekazywania informacji. Tworzone są nowe formy demokracji dzięki zwiększonemu dostępowi obywateli do informacji oraz zwielokrotnionym możliwościom wyrażania i badania opinii publicznej, powstawaniu kanałów poziomej komunikacji społecznej oraz łatwości organizowania się, uczestnictwa jednostek i grup w społecznym obiegu informacji. Pełne wykorzystanie potencjału demokratycznego państwa i nowych technik informacyjno-komunikacyjnych wymaga zagwarantowania prawa dostępu do informacji, w tym tworzonej i przechowywanej przez administrację publiczną. Szybki postęp telekomunikacji, w dziedzinie transmisji, głównie zaś szerokie wykorzystanie techniki cyfrowej i światłowodowej umożliwia stworzenie jednolitych systemów teleinformatycznych opartych w całości o cyfrowe kanały łączności.

Technologicznym fundamentem społeczeństwa informacyjnego jest proces konwergencji telekomunikacji i informatyki z radiem i telewizją, powstawanie nowoczesnej infrastruktury telekomunikacyjnej, szerokopasmowych sieci multimedialnych opartych w znacznym stopniu na instalacjach światłowodowych o ogromnej przepustowości (autostrad informacyjnych lub infostrad) oraz przenikanie nowoczesnych technik informacyjno - komunikacyjnych do wszystkich dziedzin życia. Towarzyszy temu kapitałowa i gospodarcza integracja tych dziedzin w obrębie korporacji multimedialnych, w ramach których różne dziedziny działalności wspierają i uzupełniają się nawzajem.

W systemach telekomunikacyjnych większości państw zachodnich zachodzą istotne zmiany. W kraju również, zdecydowanie przyspieszono proces cyfryzacji sieci telekomunikacyjnej i budowę elektronicznych central telefonicznych. Wykorzystanie infrastruktury telekomunikacyjnej to także problem oceny efektywności działania systemu łączności - teleinformatycznego w nowych warunkach.

System teleinformatyczny rozwijany w stanach nadzwyczajnych, będzie skuteczny jeśli dysponując określonym potencjałem, osiąga w danych warunkach i pożądanym stopniu zamierzony cel główny. Oznacza to, że system będzie posiadać możliwości do należytego wykorzystania jego cech podczas wykonywania zadań. Sieć telekomunikacyjna państwa w okresie stanów nadzwyczajnych powinna być rozwinięta na bazie węzłów stacjonarnych jak i polowych. W zależności od potrzeb węzły stacjonarne i polowe będą pełnić różne funkcje np. węzły sieci bazowej lub pomocnicze. Sieć bazowa (podstawowa) powinna być powiązana z innymi systemami tworzącymi otoczenie systemowe, w tym:

- z systemem łączności przełożonego , którym może być system łączności ND SZ RP;
- z systemem łączności rodzajów sił zbrojnych;
- z systemem łączności dowództwa subregionalnego NATO;
- z systemem łączności Wielonarodowych Połączonych Sił Zbrojnych uczestniczących w misji pokojowej.

Sieć łączności – teleinformatyczna powinna być dowiązana do systemu łączności przełożonego co najmniej dwoma niezależnymi przestrzennie liniami łączności, do co najmniej dwóch, niezależnych przestrzennie węzłów (stacjonarnych lub polowych) systemu łączności przełożonego. Przepływność linii dowiązania do systemu łączności przełożonego powinna zapewnić terminową wymianę pełnej ilości (objętości) wymaganej informacji w obydwu relacjach, tj. : „przełożony-podwładny" i „podwładny - przełożony". Należy przyjąć, że przepływność linii dowiązania do systemu przełożonego powinna wynosić nie mniej niż 2 Mbit/s lub więcej – w przypadku wykorzystywania kanałów o niższej jakości. Natomiast do podległych systemów powinna mieścić się w przedziale 2048 kbit/s – 8 Mbit/s, z systemami łączności współdziałających (sąsiednich) oraz systemami łączności rodzajów SZ (MW, WLOP), gdzie zakłada się możliwość współpracy z systemami wykonanymi w różnych technologiach. Podczas wykorzystywania kanałów o niższej jakości, powinny być stosowane urządzenia wstępnej korekcji błędów, z systemami łączności podległych punktów kierowania.

Zakłada się przy tym, że systemy współpracujące i podległe mogą być wykonane w różnych technologiach np.:

- zgodnych z technologiami wykorzystanymi np. ISDN, ATM, TCP/IP;
- w technologii cyfrowej z modulacją „delta" (modulacją CVSD);
- w technice cyfrowej z modulacją PCM oraz usługami IDN;
- w technice analogowej z systemem telekomunikacyjnym państwa.

W materiałach konferencyjnych instytucji i firm zaprezentowane zostały:

- wymagania systemu obronności państwa i dowodzenia siłami zbrojnymi oraz koncepcja systemu kierowania obronnością w stanach nadzwyczajnych;
- systemy teleinformatyczne mogące być wykorzystane w systemie obronności państwa;
- przykłady zastosowania urządzeń teleinformatycznych nowej generacji na potrzeby kierowania obronnością państwa,
- aspekty bezpieczeństwa i ochrony obiektów oraz informacji w systemie teleinformatycznym.

Do realizacji ogólnej wizji systemu teleinformatycznego na potrzeby kierowania obronnością państwa w stanach nadzwyczajnych koniecznym będzie:

- opracowanie szczegółowej koncepcji systemu teleinformatycznego w stanach nadzwyczajnych uwzględniającego potrzeby organów kierowniczych i administracji państwa,
- poddanie koncepcji opiniowaniu odpowiednim jednostkom organizacyjnym organów kierowniczych i administracji państwa, zajmującym się zbieżnymi projektami,
- opracowanie założeń techniczno-operacyjnych i taktycznych z uwzględnieniem opinii i oceny reprezentatywnych ekspertów i komórek naukowych;
- opracowanie projektu wstępnego systemu i zbudowanie sieci eksperymentalnej (pilotowej);
- weryfikacja przyjętych założeń i koncepcji systemu teleinformatycznego;
- opracowanie projektu technicznego i budowa określonego modułu systemu teleinformatycznego,
- przeprowadzenie badań wstępnych i końcowych modułu systemu teleinformatycznego,

Ocena zakresu prac i możliwości ich wykonania wskazuje, iż realizacja systemu na potrzeby organów kierowniczych i administracji państwa w stanach nadzwyczajnych może mieć miejsce w okresie około 3 - 4 lat. Szczególny nacisk powinien być położony na realizację projektu wstępnego, dotyczącego budowy sieci pilotowej. Należy podkreślić, że w kraju jednocześnie są prowadzone prace nad nową generacją, zarówno sieci strategiczno-operacyjnej, jak i sieci taktycznej. Powyższe wskazuje, iż jest niezbędna

koordynacja tych prac prowadząca w konsekwencji do unifikacji infrastruktury teleinformatycznej wykorzystywanej w stanach nadzwyczajnych. Szczególnie urządzenia kryptograficznej ochrony informacji oraz urządzenia szkieletowej infrastruktury teleinformatycznej (systemy komutacyjne, urządzenia dostępowe) powinny być, w miarę możliwości, na tyle uniwersalne, aby mogły spełniać wymagania stawiane przed systemami, w których zostaną zainstalowane. Dlatego też, wyraźne określenie roli organów administracji państwowej i ich kompetencji w budowie zintegrowanego systemu teleinformatycznego na potrzeby obronności państwa, a szczególnie stanów nadzwyczajnych staje się pilną koniecznością. Przedstawiciele z różnych sektorów organów kierowniczych i administracji państwa, powinni zatem uczestniczyć w projektowaniu i integrowaniu sieci teleinformatycznej do przekazywania informacji w stanach nadzwyczajnych. Wybór docelowej struktury narodowego (krajowego) systemu łączności - teleinformatycznego musi być poprzedzony wnikliwą analizą oraz pracami koncepcyjnymi i badawczymi.

Wydaje się, że zaproponowany sposób realizacji systemu teleinformatycznego na potrzeby stanów nadzwyczajnych zminimalizuje ryzyko jego opracowania. Współdziałanie z systemem telekomunikacyjnym państwa warunkuje zapewnienie łączności z osobami funkcyjnymi jednostek administracji państwowej funkcjonujących na obszarze objętym działaniami kryzysowymi. Należy przyjąć, że abonenci najwyższych organów władzy i administracji państwa będą w najbliższej przyszłości abonentami krajowej sieci specjalnej, która będzie posiadać dużą zgodność techniczną i technologiczną z siecią telekomunikacyjną państwa.

W związku z członkostwem w NATO i bliską perspektywą wejścia w struktury UE, istnieje pilna potrzeba, a wręcz konieczność kontynuacji tych prac i rozbudowy systemu teleinformatycznego w stanach nadzwyczajnych.