AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ ZARZĄDZANIA I DOWODZENIA

ZARZĄDZANIE INFORMACJĄ W ŚRODOWISKU SIECIOCENTRYCZNYM – KONCEPCJA DOMEN INFORMACYJNYCH „DOMENY"

Praca naukowo-badawcza

WARSZAWA

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ ZARZĄDZANIA I DOWODZENIA

Zarządzanie informacją w środowisku sieciocentrycznym – koncepcja domen informacyjnych „Domeny”

Praca naukowo-badawcza

Warszawa **2009**

Recenzja: płk dr hab. inż. Jarosław Wołejszo

	1	2	3	

4

Tytuł.: Zarządzanie informacją w środowisku sieciocentrycznym – koncepcja domen informacyjnych

5	6	7
Rozpoczęto: 1.06.2009 Zakończono: 15.11.2009	kart: 142	

8	9

Opracował zespół autorski:

płk dr inż. Piotr Dela: **redakcja naukowa, wstęp, rozdział 1, rozdział 2, rozdział 4, zakończenie**

mjr mgr inż. Bartosz Biernacik: **rozdział 3**

Spis treści

WSTĘP

Rozwój technologii informatycznych spowodował lawinowe narastanie nowych, nieznanych dotychczas możliwości komunikowania się oraz gwałtownie poszerzył obszary ich zastosowania. Technologie transmisji danych (technologie wykorzystywane głównie w sieci Internet) dostosowane do potrzeb użytkowników cywilnych dały także nowe możliwości systemom wykorzystywanym w wojsku. To pozwoliło na zwiększenie możliwości wojskowym systemom łączności i informatyki w zakresie przekazywania, przetwarzania i analizy danych. Liczne tego typu rozwiązania zostały już wprowadzone na wyposażenie wiodących armii świata, kolejne są w trakcie badań, opracowywania lub wdrażania. Dalsze perspektywy rozwoju w tym zakresie, stwarzając jednocześnie nowe wymagania i możliwości, umożliwią wdrożenie w życie koncepcji działań sieciocentrycznych (ang. *network centric warfare* – NCW).

W koncepcji sieciocentrycznej podkreślana jest nowa jakość, jaką stanowi środowisko w którym będzie prowadzona walka informacyjna. Rosnące znaczenie operacji innych niż wojna, ogromny postęp technologiczny oraz asymetryczne formy działań zbrojnych doprowadziły do konieczności odchodzenia od identyfikowania „pola walki" na rzecz postrzegania środowiska prowadzenia walki sieciocentrycznej jako „przestrzeni walki". W przestrzeni tej nie występuje granica oddzielająca walczących od ludności cywilnej. Zmieniać się może także charakter przeciwnika oraz obszar konfliktu. Walka sieciocentryczna będzie wszechobecna, wszechogarniająca i wieloaspektowa.

Zasadniczy cel koncepcji walki sieciocentrycznej polega na zaprojektowaniu takiego zestawu wzajemnie połączonych elementów przestrzeni walki, które będą wykorzystywać zwiększoną ilość dostępnych informacji. Zostanie ona przekształcona w niezbędne zasoby wiedzy i w konsekwencji pozwoli uzyskać wzrost zdolności bojowej. Do zapewnienia powodzenia i efektywności działań prowadzonych zgodnie z założeniami walki sieciocentrycznej, niezbędne jest zapewnienie wysokiego poziomu wymiany informacji pomiędzy poszczególnymi jej komponentami oraz odpowiedni poziom ich wykorzystania, niezbędny do prawidłowego współdziałania.

Funkcjonowanie w środowisku NCW daje wprawdzie nowe możliwości związane z przetwarzaniem, przesyłaniem i przechowywaniem informacji ale nastręcza też nowe trudności związane z organizacją obiegu informacji, a tym samym z jej właściwym zarządzaniem. Klasyczne rozwiązania przyjęte w tym zakresie nie zdają egzaminu, co powoduje niejednokrotnie niespójność danych posiadanych przez poszczególne zespoły funkcjonale stanowisk

dowodzenia. Występowanie takich sytuacji potwierdzają obserwacje przeprowadzone w trakcie wielu ćwiczeń dowódczo-sztabowych. Z tego też względu istnieje pilna potrzeba określenia w jaki sposób zarządzać informacją w środowisku sieci teleinformatycznych aby zapewnić możliwość jej współdzielenia na potrzeby wspólnej świadomości operacyjno-taktycznej, zgodnej z koncepcją NCW.

Stan wiedzy w przedstawionym obszarze wytworzył sytuację problemową, której rozwiązania podjęli się autorzy, rozpoczynając w ten sposób pierwszy etap badań naukowych.

Wyniki badań wstępnych oraz posiadana wiedza pozwoliła autorom zdefiniować następujący **cel główny pracy:**

identyfikacja stanu obecnego i wskazanie możliwości oraz sposobów zarządzania informacją w środowisku sieciocentrycznym w działaniach wojsk lądowych, a w konsekwencji opracowanie koncepcji zarządzania informację w sieciach teleinformatycznych umożliwiającą współdzielenie informacji wszystkim uprawnionym uczestnikom operacji.

Osiągnięcie celu głównego wymagało zdefiniowania następujących **celów cząstkowych**:

1. ***Zidentyfikowanie istoty oraz charakterystyki działań w środowisku sieciocentrycznym;***
2. ***Określenie roli i znaczenia informacji w procesie decyzyjnym oraz jej uwarunkowań organizacyjnych w wojskach lądowych;***
3. ***Określenie technologii informatycznych możliwych do wykorzystania na potrzeby zarządzania informacją w środowisku sieciocentrycznym;***
4. ***Opracowanie koncepcji zarządzania informacją w sieciach teleinformatycznych na potrzeby współdzielenia informacji.***

Podczas dalszych badań, dążąc do osiągnięcia opisanych uprzednio celów, autorzy sformułowali **główny problem badawczy** w postaci następującego pytania:

W jaki sposób i w jakim zakresie należy dokonać zmian w obszarze zarządzania informacją w sieciach teleinformatycznych, aby sprostać wymaganiom współdzielenia informacji w środowisku sieciocentrycznym?

Kolejny etap badań oznaczał dla autorów przeprowadzenie szeregu analiz, porównań i analogii oraz dalsze studiowanie dostępnej literatury przedmiotu. W konsekwencji autorzy utwierdzili się w poglądzie, iż istnieje konieczność dokonania podziału problemu głównego na szereg problemów szczegółowych. Tą drogą wyodrębniono następujące **problemy szczegółowe**:

1. ***Jak jest istota i główne założenia koncepcji działań w środowisku sieciocentrycznym?***
2. ***Jaka jest istota i charakter informacji wykorzystywanej w procesie dowodzenia realizowanym w wojskach lądowych oraz jakie są jej uwarunkowania organizacyjne?***
3. ***Jakie technologie zarządzania sieciami są możliwe do wykorzystania na potrzeby współdzielenia informacji w środowisku sieciocentrycznym?***
4. ***W jaki sposób zorganizować zarządzanie informacją w środowisku sieciocentrycznym, aby uwzględniona została struktura dowodzenia i specyfika realizowanych przez wojska lądowe zadań?***

Sprecyzowanie problemów szczegółowych powodowało wyodrębnienie kolejnych faktów naukowych. Te zaś z kolei pozwoliły na sprecyzowanie hipotezy badawczej w postaci przypuszczenia:

Zmiany technologiczne zachodzące we współczesnym świecie odzwierciedlają się m. in. w szerokim wykorzystaniu zdobyczy współczesnej łączności i informatyki. Dotyczy to także wojsk lądowych, w których coraz większego znaczenia nabierają sieci teleinformatyczne, a w głównej mierze ich możliwości świadczenia usług teleinformatycznych oraz możliwość współdzielenia informacji w ramach tworzenia wspólnej świadomości operacyjno-taktycznej. Należy przypuszczać, że zgodnie z podejściem COTS, polegającym na wykorzystaniu teleinformatycznych technologii cywilnych w siłach zbrojnych, istnieją technologie umożliwiające zapewnienie współdzielenia informacji w globalnej sieci teleinformatycznej.

Zarządzanie informacją na potrzeby prowadzenia działań powinno obywać się w dwóch głównych obszarach, a mianowicie w obszarze globalnym – globalnej sieci informacyjnej oraz w obszarze lokalnym – w ramach stanowiska dowodzenia.

Na potrzeby tworzenia wspólnej świadomości informacyjnej w globalnej sieci informacyjnej powinien zostać stworzony odpowiedni system domen informacyjnych, odzwierciedlający strukturę organizacyjną sił zbrojnych, w których przechowywana jest informacja. Zarządzanie informacją odbywać się będzie poprzez wyodrębnienie domen specjalistycznych, zadaniowych i obszarowych i przydzielanie praw dostępu do danych na poziomie domen. Dodatkowo na potrzeby zarządzania informacją na stanowisku dowodzenia należy zorganizować administratora informacji odpowiadającego za zachowanie spójności danych w ramach danego stanowiska. W ramach organizacji pracy stanowiska dowodzenia, na potrzeby zachowania spójności danych, należy wyróżnić dodatkowo następujące stany pracy stanowiska dowodzenia: praca ciągłą w miejscu stałej dyslokacji, praca w warunkach bojowych na stanowisku dowodzenia, praca wydzielonej grupy (zespołu) poza stanowi-

skiem dowodzenia, praca w trakcie zmiany stanowiska dowodzenia, praca bez stanowisk dowodzenia.

Autorzy zastosowali szereg metod badawczych zmierzających do rozwiązania zidentyfikowanych uprzednio problemów szczegółowych. Specyfika tych problemów rzutowała bezpośrednio na fakt, iż wśród użytych metod znalazły się głównie metody teoretyczne. Ponadto, w ramach metod empirycznych, w celu uzyskania szerszego materiału badawczego, posłużono się metodą obserwacji bezpośredniej i pośredniej, uczestniczącej i zewnętrznej. Metoda ta pozwoliła na praktyczne zweryfikowanie otrzymanych w toku badań teoretycznych wyników. Obserwowane były ćwiczenia organizowane przez wojska lądowe, a także ćwiczenia dowódczo-sztabowe organizowane w Akademii Obrony Narodowej.

Struktura pracy obejmuje wstęp, cztery rozdziały merytoryczne oraz zakończenie.

We wstępie zaprezentowano metodologiczne aspekty badań oraz konstrukcję opracowania pisarskiego pracy badawczej. Uzasadniono w nim także wybór tematu i przedstawiono przyjętą procedurę badań. Rozdział pierwszy obejmuje wyniki badań dotyczących identyfikacji koncepcji NCW. W rozdziale drugim zawarto rezultaty badań dotyczące istoty i charakteru informacji wytwarzanej i wykorzystywanej w procesie dowodzenia realizowanym w wojskach lądowych oraz uwarunkowań organizacyjnych mających wpływ na kierunki przesyłu informacji. Rozdział trzeci stanowi podsumowanie procesu badawczego dotyczącego technologii informatycznych możliwych do wykorzystania na potrzeby zarządzania informacją w środowisku NCWW rozdziale czwartym przedstawiono wyniki badań związane z koncepcją zarządzania informacją poprzez stworzenie domen informacyjnych w globalnej sieci informacyjnej i lokalnych administratorów informacji na stanowiskach dowodzenia. Pracę wieńczy zakończenie w którym podsumowano wyniki przeprowadzonych badań.

1. Idea działań sieciocentrycznych

Rozwój technologii teleinformatycznych zainicjował szybkie narastanie nowych, nieznanych dotychczas możliwości komunikowania się między ludźmi. Technologie transmisji danych dostosowane do potrzeb użytku cywilnego dały także nowe możliwości systemom wykorzystywanym w wojsku, co pozwoliło zwiększyć możliwości w zakresie przekazywania, przetwarzania i analizy informacji.

Znaczenie informacji w prowadzeniu wojen było docenione już w starożytności. Według klasyka sztuki wojennej Sun Tzu *„kto zna przeciwnika i kto zna swoje siły będzie zwycięzcą w stu bitwach. Kto nie zna przeciwnika, ale zna własne siły, raz wygra, a raz przegra. Kto zna przeciwnika, ale nie zna własnych sił, będzie w niebezpieczeństwie w każdej bitwie."*[1] Teoria wykorzystania informacji w wojnie została rozwinięta przez znakomitego niemieckiego teoretyka Karla von Clausewitza w pracy *O wojnie*, który rozdział VI księgi I poświęcił roli i znaczeniu informacji w wojnie. Z kolei w rozdziale VII von Clausewitz wprowadził pojęcie „mgły wojny", czyli niepewności wynikającej z braku informacji i związanego z tym ryzyka. Tezy zawarte w pracach obu znamienitych teoretyków sztuki wojenej pozostały do dziś aktualne.

Pełne korzystanie z informacji umożliwiło dopiero zastosowanie technologii teleinformatycznych przełomu XX i XXI wieku. W celu pełnego wykorzystania najnowszych możliwości technologii teleinformatycznych na potrzeby militarne w krajach NATO powołano liczne komórki zadaniowe oraz podpisano umowy z firmami cywilnymi specjalizującymi się w dostawach sprzętu wojskowego w celu równoległego wypracowania koncepcji funkcjonowania tzw. sieci centrycznych (sieci zdolnych do współdzielenia informacji).

Zakrojone na szeroką skale badania naukowe zaowocowały stworzeniem koncepcji sieci centrycznych umożliwiających uzyskanie przewagi informacyjnej nad przeciwnikiem i prowadzeniem efektywnych działań przy minimalizacji kosztów. Nierozerwalnie związanym z sieciami centrycznymi jest od pojęcie **przewagi informacyjnej,**[2] które należy rozumieć jako: *zdolność do zbierania, gromadzenia, przetwarzania, analizowania i dystrybucji informacji oraz utrzymania nieprzerwanego strumienia ich przepływu oraz pełnego jej wykorzystania, przy jednoczesnej zdolności do uniemożliwienia przeciwnikowi prowadzenia podobnej działalności informacyjnej.*

---

[1] Sun Tzu: *Sztuka wojowania*, cytat z wersji pracy dostępnej na stronie: www.sonshi.com/sun3.html
[2] Joint Pub 3-13, DoD USA

Możliwość zastosowania nowych technologii pozwoliło na wyodrębnienie się nowych koncepcji prowadzenia walki. W literaturze przedmiotu pojawiło się pojęcie **walka sieciocentryczna,** zaprezentowane po raz pierwszy w 1998 roku, w artykule *Network Centric Warfare - Its Origins and Future* na łamach Proce-edings.[3] Przedstawiono w nim nowy sposób prowadzenia działań militarnych w erze społeczeństw informacyjnych. Od chwili ukazania się cytowanej publikacji pojawiło się mnóstwo artykułów, opracowań, książek dotyczących walki sieciocentrycznej.

Walka sieciocentryczna, według Davida Albertsa, Johna Garstki, i Frederica Steina to *„ ... zachowania ludzkie i organizacyjne. Bazuje ona na nowym sposobie myślenia - myśleniu sieciocentrycznym - i na zaadaptowaniu go do operacji militarnych. Skupia się ona na sile, która może być wygenerowana poprzez efektywne połączenie (sieciowanie) elementów ugrupowania bojowego. Charakteryzuje ją zdolność rozproszonych geograficznie sił (elementów ugrupowania) do wykreowania jednolitej sytuacji taktycznej, poznanie której może być wykorzystane poprzez samo synchronizowanie i inne działania sieciocentryczne, aby zrealizować zamiar dowódcy. Walka sieciocentryczna przyczynia się do zwiększenia tempa dowodzenia oraz do konwersji przewagi informacyjnej na uzyskanie przewagi w działaniach bojowych. Walka sieciocentryczna nie zależy od rodzaju misji, wielkości sił i uwarunkowań geograficznych. Dodatkowo walka sieciocentryczna spaja taktyczny, operacyjny i strategiczny poziom działań bojowych. W skrócie - walka sieciocentryczna to nie tylko technologia, ale w szerokim rozumieniu, odpowiedź sił zbrojnych na wyzwania ery informacyjnej".* [4] Rosnące znaczenie operacji innych niż wojna, szybki postęp techniczny i technologiczny oraz asymetryczne formy prowadzenia działań zbrojnych wymusiły konieczności odchodzenia od identyfikowania „pola walki" na rzecz postrzegania środowiska prowadzenia walki sieciocentrycznej jako „przestrzeni realizacji zadań" (*ang. Mission Space*). W przestrzeni tej nie istnieje wyraźna granica oddzielająca walczących od ludności cywilnej. Zmieniać się może charakter potencjalnego przeciwnika oraz obszar konfliktu. Walka sieciocentryczna będzie wszechobecna, wszechogarniająca i wieloaspektowa.

Według założeń amerykańskich walka sieciocentryczna będzie takim sposobem prowadzenia działań, w którym siły zbrojne, spięte w sieć teleinformatyczną, będą wykorzystywać przewagę informacyjną i pełną świadomość sytuacji do prowadzenia szybkich i skutecznych działań. Wykorzystywane technologie i rozwiązania organizacyjno-funkcjonalne po-

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

[4] D. Alberts, J. Garstka, F. Stein, *Nełwork Centric Warfare,* DoD C4ISR Cooperative Research Program, 2000, s. 88.

zwolą na pokonanie przeciwnika w sposób szybki i efektywny przy jednoczesnym minimalizowaniu wysiłku wojsk własnych.

W literaturze przedmiotu widoczna jest polaryzacja poglądów na temat stopnia sieciocentryczności możliwego do osiągnięcia przez wojska. Stopień rozwoju założeń koncepcyjnych walki sieciocentrycznej, wyposażenia oraz wyszkolenia wojsk, w opinii wielu teoretyków sztuki wojennej plasuje współczesne siły zbrojne na poziomie nie pozwalającym na prowadzenie działań sieciocentrycznych. Doświadczenia z Afganistanu i Iraku wskazują, że w pełnym zakresie działania sieciocentryczne były możliwe tylko w wymiarze taktycznym. W perspektywie najbliższych lat możliwe będzie zintegrowanie w ramach wspólnej sieci systemów w skali rodzaju sił zbrojnych, a dopiero około 2020 r. osiągnięcie pełnej implementacji standardów zapewniających prowadzenie operacji sieciocentrycznych.

Także w polskiej myśli wojskowej widoczne są próby definiowania walki sieciocentrycznej. Jedna z nich została przedstawiona przez Ryszarda Szpakowicza. Według niego walka sieciocentryczna jest „*...definiowana jako opierająca się na przewadze informacyjnej koncepcja prowadzenia operacji, według której wzrost siły bojowej jest generowany poprzez połączenie w sieć informacyjną sensorów, decydentów i systemów walki w celu osiągnięcia wspólnej świadomości, zwiększenia szybkości dowodzenia oraz tempa operacji, zwiększenia skuteczności uzbrojenia, wzrostu odporności na uderzenia przeciwnika oraz zwiększenia stopnia synchronizacji działań. NCW przekłada, zatem przewagę informacyjną na zdolności bojowe poprzez efektywne łączenie na polu walki różnego typu jednostek organizacyjnych i wykorzystanie ich wiedzy".*[5]

Definicje walki sieciocentrycznej są różnorodne i nie precyzują tego pojęcia jednoznacznie. Z tego też względu w ramach ekspertyzy „Wykonanie Studium Wykonalności Projektu Network Enabled Capabilities" przeprowadzonej w siłach zbrojnych RP w 2006 roku podjęto próbę określenia narodowej interpretacji zdolności sieciocentrycznej. Poniżej przedstawiono przyjęte definicje.

Walka Sieciocentryczna (*ang. Network Centric Warfare - NCW*), to rozwijająca się teoria działań wojennych, wyrażona poprzez zbiór zasad i reguł, które mogą być wykorzystane do opracowania nowych sposobów prowadzenia walki.

Teoria ta opiera się na zasadach:

- połączone niezawodną siecią siły usprawniają współdzielenie informacji;
- współdzielenie informacji poprawia jakość informacji i wspólną świadomość sytuacyjną;

[5] R. Szpakowicz, *Wojna w Iraku a koncepcja wojny sieciocentrycznej,* Przegląd Sił Powietrznych 11/2003, s. 8.

- wspólna świadomość sytuacyjna pozwala na współpracę, osiągnięcie samo synchronizacji, usprawnia ciągłość i szybkość dowodzenia.

Zdolność sieciocentryczna (*ang. Network Enabled Capability - NEC*) to zdolność szybkiego i precyzyjnego osiągnięcia zamierzonego efektu operacyjnego poprzez wykorzystanie infrastruktury informacyjnej wiążącej sensory, decydentów i środki walki. Uzależniona jest ona od możliwości pozyskania, integracji i analizy informacji w czasie zbliżonym do rzeczywistego, pozwalającej na szybkie podejmowanie decyzji oraz osiągnięcie pożądanego efektu.

Sieciocentryczność to podejście do tworzenia koncepcji lub zdolności, w której sieć (lub sieci) pełni zasadniczą rolę.

Przewaga informacyjna w wymiarze militarnym może być zdefiniowana jako zdolność do zbierania, gromadzenia, przetwarzania, analizowania i dystrybucji informacji oraz utrzymania nieprzerwanego strumienia ich przepływu i pełnego ich wykorzystania, przy jednoczesnej zdolności do uniemożliwienia przeciwnikowi prowadzenia podobnej działalności informacyjne".

Dane są pojedynczymi faktami, pomiarami lub obserwacjami, które mogą być wykorzystane do wypracowania konkretnej, szczegółowej decyzji.

Informacja powstaje w wyniku gromadzenia danych, ich weryfikacji i integracji oraz interpretacji w kontekście operacyjnym.

Wiedza stanowi osobisty stan poznania człowieka w wyniku oddziaływania na niego obiektywnej rzeczywistości. Wypływa ona ze zdolności użycia informacji do zbudowania, a następnie wykorzystywania modelu pojęciowego, bazuje na zrozumieniu sytuacji lub zjawiska. Taki model umożliwia prognozowanie przyszłych stanów, przewidywanie rezultatów działań, tym samym zwiększa zdolność do kontrolowania sytuacji.

Świadomość sytuacyjna w ogólnym znaczeniu określa postrzeganie i rozumienie rzeczywistej sytuacji przez człowieka. W kontekście ZSC oznacza zdolność posiadania:

- dokładnej i aktualnej informacji o położeniu sił i środków własnych, przeciwnika oraz niezaangażowanych i cywilnych;
- wspólnego (dostępnego, powszechnego) obrazu pola walki w skali odpowiadającej aktualnym, specyficznym potrzebom i zainteresowaniom.

Zasadniczy cel koncepcji walki sieciocentrycznej polega na zaprojektowaniu takiego układu wzajemnie połączonych elementów przestrzeni walki, które będą zdolne do wykorzystania zwiększonej ilość informacji. Zostanie ona przekształcona w niezbędne zasoby wiedzy i w konsekwencji pozwoli uzyskać wzrost zdolności bojowej.

Do zapewnienia powodzenia i efektywności działań prowadzonych zgodnie z założeniami walki sieciocentrycznej, niezbędne jest zapewnienie wysokiego stopnia wymiany informacji pomiędzy poszczególnymi jej komponentami oraz odpowiedniego poziomu ich wykorzystania, niezbędnego do prawidłowego współdziałania. Warunkiem zapewniającym prowadzenie walki sieciocentrycznej jest stworzenie **interoperacyjności informacyjnej** rozumianej jako: „... *zdolność poszczególnych elementów (komponentów) do zapewnienia wzajemnej wymiany zrozumiałej dla nich informacji niezbędnej do odpowiedniej współpracy. W szerszym rozumieniu interoperacyjność informacyjna oznacza też zrozumienie zjawisk i wydarzeń zachodzących w środowisku, opisywanych tymi informacjami*".[6]

Interoperacyjność informacyjna powinna zachodzić na trzech następujących poziomach[7]:

- technicznym,
- syntaktycznym,
- semantycznym.

Poziom techniczny jest podstawowym poziomem dla interoperacyjności informacyjnej zapewniającym odbieranie i przetwarzanie informacji na poziomie sygnałów. Poziom syntaktyczny to nic innego jak zdolność do pośredniego przetwarzania otrzymanych informacji pod względem językowym oraz formatu ich zakodowania. Poziom semantyczny interoperacyjności informacyjnej to zdolność odbiorcy informacji do prawidłowego zrozumienia otrzymanej informacji. Kluczową sprawą dla zapewnienia interoperacyjności informacyjnej stanowią kwestie techniczne, jednakże istotne znaczenie ma także poziom semantyczny. Ujednolicenie procedur działania i wykorzystywanej terminologii umożliwia właściwe zrozumienie intencji nadawcy informacji i ułatwia komunikowanie się.

Podsumowując celem tworzenia koncepcji wojny sieciocentrycznej jest wzrost zdolności bojowych sił zbrojnych przez:

- lepsze synchronizowanie działań na polu walki,
- skrócenie cyklu dowodzenia,
- zwiększenie skuteczności rażenia, zdolności przetrwania i zdolności do reagowania.

---

[6] S. Munk, *Walka sieciocentryczną a interoperacyjność informacyjna*, Myśl Wojskowa nr 6/2004, s. 50.

1.1. Przestrzeń walki

W celu lepszego zrozumienia i poznania środowiska działań sieciocentrycznych, należy uwzględniać zmiany, jakie zaszły w podstawach i uwarunkowaniach prowadzenia działań podczas operacji innych niż wojna. Zakończenie zimnej wojny oraz koniec istnienia dwubiegunowego układu sił na świecie niesłychanie skomplikowały sytuacje bezpieczeństwa na świecie i to zarówno w skali globalnej jak i lokalnej. Pojawiło się wiele nieznanych wcześniej zagrożeń, a przeciwdziałanie im wymaga niekonwencjonalnych podejść do kierowania operacją militarną oraz niestandardowym użyciu sił i środków. Wymusiło to całkowicie nowe podejście do planowania, dowodzenia, kierowania, współdziałania wewnątrz sił zbrojnych zarówno w układzie narodowym, jak i koalicyjnym oraz we współdziałaniu z innymi organizacjami rzędowymi i cywilnymi.

Prowadzenie działań militarnych w konflikcie asymetrycznym wymaga często odejścia od ustalonych kanonów sztuki wojennej. W konfliktach tego rodzaju atak, oprócz postaci fizycznej, przybiera też inną formę, np. formę ataku cybernetycznego na sieci teleinformatyczne lub działalności propagandowo-informacyjnej.

Jednocześnie era informacyjna wiąże się z gwałtownym rozwojem mediów i środków masowego przekazu: dzienników, czasopism, radia, telewizji i mediów elektronicznych w tym Internetu. Spowodowało to rewolucję w dziedzinie masowego informowania społeczeństw, w tym o aktualnym przebiegu działań bojowych nawet w odległych zakątkach świata. Procesy decyzyjne na najwyższych poziomach dowodzenia są pilnie obserwowane przez wszystkie media. Pozwala to opinii publicznej na aktywne włączenie się w proces oceny działalności sił zbrojnych, a w państwach demokratycznych na wywieranie ogromnego wpływu na podejmowanie decyzji. Dowódcy muszą więc liczyć się z tym, że ich bieżąca działalność jest stale oceniana przez własną oraz światową opinię publiczną. Opinia ta wpływa pośrednio na polityków decydujących o operacjach militarnych.

W tradycyjnym rozumieniu pole walki było zamkniętym geograficznie obszarem, na którym prowadzono działania bojowe, a samo pojęcie zawierało w sobie wszystkie uwarunkowania związane z prowadzeniem tych działań. W większości przypadków pole walki wiązało się z wydzielonym i zamkniętym obszarem geograficznym. Obecne uwarunkowania wywierające wpływ na działania bojowe, nawet na najniższym szczeblu taktycznym, w znacznym stopniu znajdują się poza obszarem geograficznym, tradycyjnie rozumianym jako pole walki. Są to działania propagandowo-informacyjne związane z aktualnymi działaniami taktycznymi, mające na

[7] Tamże

celu utrzymanie poparcia opinii publicznej. Mogą to być również działania sensorów o zasięgu globalnym (rozpoznanie satelitarne, system nawigacji GPS), działania środków ogniowych o zasięgu globalnym (np. bombowce strategiczne, rakiety dalekiego zasięgu), ale wykonujących zadania taktyczne itd. Istotne jest także zwiększenie roli sił specjalnych operujących na całym terytorium przeciwnika oraz roli lotnictwa, bazującego często daleko od obiektów działania.

W związku z powyższym Amerykanie zaproponowali zastąpienie pojęcia **pole walki** *(ang. battlefield)* nowym pojęciem - **przestrzeń walki** *(ang. battlespace),* obejmującym wszystkie uwarunkowania związane z prowadzeniem działań bojowych na wszystkich szczeblach dowodzenia (strategicznym, operacyjnym, przede wszystkim - taktycznym), niezależnie od ich geograficznej dyslokacji.[8]

O trafności pojęcia **przestrzeń walki** może świadczyć fakt, że działania nawet na szczeblu taktycznym są uwarunkowane olbrzymią ilością czynników, których znaczna część jest poza obszarem geograficznym, na którym są fizycznie prowadzone działania bojowe. W tradycyjnie zorganizowanych siłach zbrojnych dowódca taktyczny nie jest zdolny do prowadzenia skutecznych działań z powodu braku możliwości monitorowania i oceny sytuacji. Nie może on uwzględnić w swoich decyzjach tych czynników, które są poza zasięgiem jego obserwacji i bezpośredniej łączności. Problem ten rozwiązuje zastosowanie sieciocentrycznego podejścia do działań bojowych. Stworzenie sieci centrycznej zapewniającej terminowy przepływ dowolnej informacji, której źródło znajduje się w dowolnym punkcie globu, do odpowiedniego użytkownika pozwala na monitorowanie, analizę i uwzględnienie w podejmowaniu decyzji wszystkich czynników, nawet tych które znajdują się poza zasięgiem obserwacji dowódcy i jego systemu łączności.

O geograficznie pojmowanym polu walki trudno też mówić w przypadku działań antyterrorystycznych. W reakcji na ataki terrorystyczne na terytorium danego państwa, mogą zostać przeprowadzone kontrakcje, które co prawda mają miejsce na terytorium innego państwa, ale de facto nie są wymierzone przeciwko niemu lecz przeciwko terrorystom.

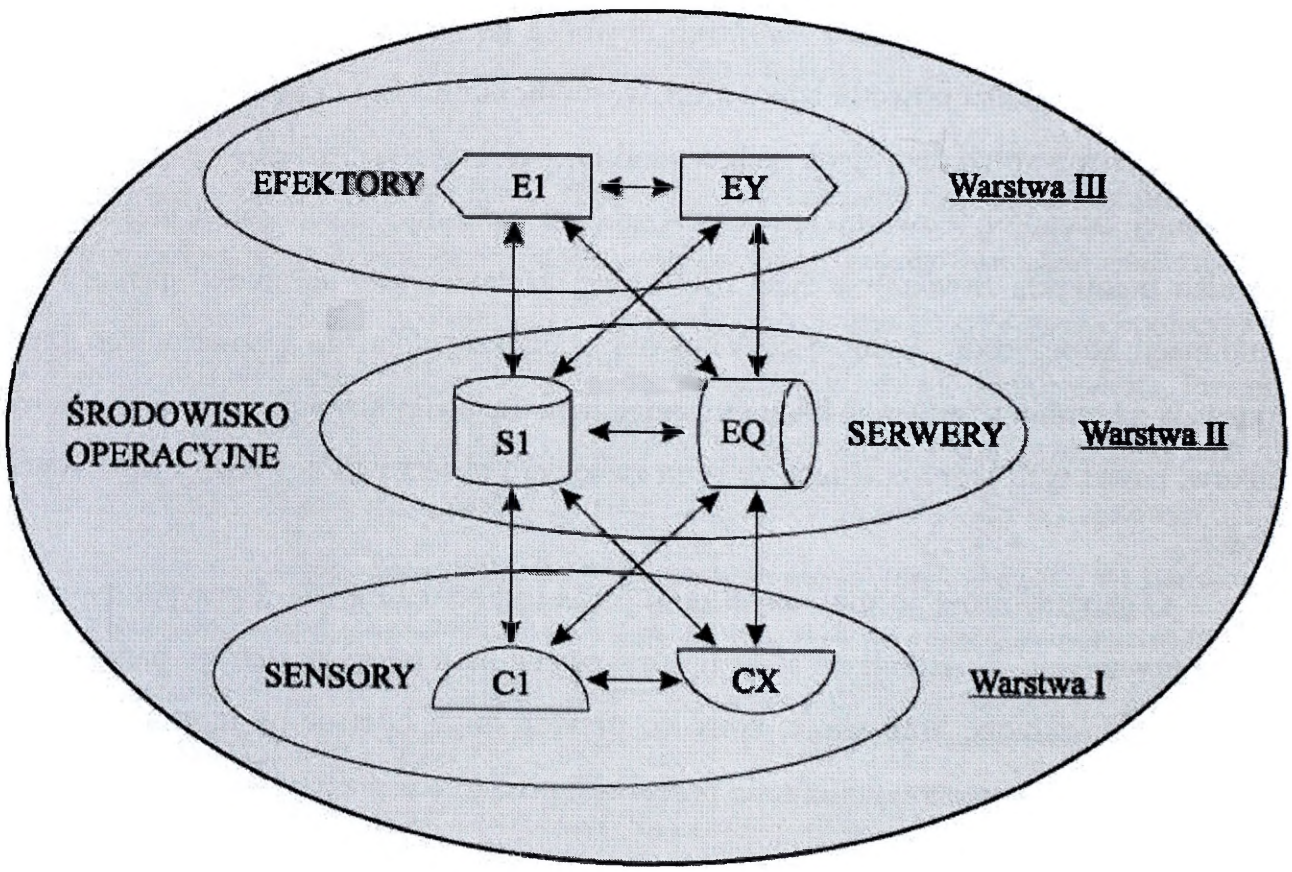
---

[8] *Concept forFuture Joint Operations,* Joint Chiefs of Staff, 1997, s. 83

1.2. Globalna sieć informacyjna

W aspekcie technologicznym systemy sieciocentryczne, zwane w literaturze angielskojęzycznej systemami NCW - *Network Centric Warfare*, są oparte na trójwarstwowej strukturze rozproszonej sieci telekomunikacyjnej obejmującej warstwy:[9]

- warstwa sensorów, zawierająca źródła informacji oraz wszelkiego rodzaju receptory i czujniki zdolne do zbierania i przekazywania informacji z określonego środowiska operacyjnego;
- warstwa serwerów, odbierająca informacje z warstwy sensorów i przetwarzająca je na informację użyteczną dla elementów wykonawczych utożsamianych przez efektory;
- warstwa efektorów która zawiera systemy oddziaływania materialnego i niematerialnego na przeciwnika (w tym systemu fizycznego niszczenia).



Rys. 1.1. Model struktury sieciocentrycznej
Źródło: *K. Ficoń, Inteligentny pył podstawą funkcjonowania systemów network centric warfare, Myśl wojskowa 6/2005, str. 57-72*

[9] K. Ficoń, *Inteligentny pył podstawą funkcjonowania systemów network centric warfare,* Myśl wojskowa 6/2005, str. 57-72

Zebrane i dostarczone przez sensory dane umożliwiają analizę, syntezę i uogólnienie zebranej informacji co zapewnia zbudowanie w warstwie serwerów informacyjnego obrazu środowiska operacyjnego, będącego wirtualną mapą przestrzeni walki. Warstwa serwerów to przede wszystkim komputerowe systemy baz danych, w których są przechowywane i przetwarzane informacje pochodzące od sensorów oraz od innych źródeł informacji. Pozyskane informacje źródłowe są przetwarzane za pomocą odpowiednich procedur na prawdopodobne warianty działania, które w końcowym etapie są zamieniane na decyzje.

Akceptowane przez operatorów decyzje są przesyłane kanałami dystrybucji do wykonawczej warstwy efektorów, w której z reguły w sposób automatyczny uruchamiane są odpowiednie systemy uzbrojenia. Są to zazwyczaj inteligentne systemy broni, działające najczęściej w reżimie „odpal i zapomnij" (*ang. fire and forget*). Efektorami są środki ogniowe, bierne i czynne urządzenia walki radioelektronicznej, mobilne systemy sterujące ruchem obiektów, zmianą ich położenia, a nawet funkcji. Efektory wykonują głównie aktywne zadanie energetyczne (kienatyczne).

Zasadniczym zadaniem tak zorganizowanej trójwarstwowej struktury jest wypracowanie jednolitego obrazu sytuacji. Polega to na zbudowaniu możliwie wiernego obrazu przestrzeni walki, w celu racjonalnego sterowania przebiegającymi na nim działaniami sił własnych. Dysponowanie pełnym obrazem sytuacji w czasie rzeczywistym to zasadniczy problem współczesnych systemów dowodzenia. Informacja zawsze była, jest i nadal będzie czynnikiem preferującym daną stronę i krytycznym zasobem przestrzeni walki. Panowanie w sferze informacyjnej stymuluje przewagę w wymiarze operacyjnym. Natychmiastowy dostęp do informacji, czyli dysponowanie kompleksowym obrazem taktycznym, jest warunkiem niezbędnym podejmowania wszystkich decyzji. Systemy sieciocentryczne zwiększają sprawność i efektywność dowodzenia, podnoszą skuteczność użycia różnorodnych środków walki i systemów uzbrojenia, przyczyniają się do synchronizacji działań zarówno w czasie jak i przestrzeni. Prowadzi to do minimalizacji strat własnych i maksymalnego rażenia potencjalnych celów.

W odniesieniu do struktur militarnych bazę materialno-funkcjonalną systemów sieciocentrycznych stanowi **globalna sieć informacyjna** tzw. *Global Information Grid* (GIG), rozumiana jako pewna struktura sieciowa, której elementami węzłowymi są następujące sieci warstwowe[10]:

- G1 - sieć sensorów jako zbiór technicznych (inteligentnych) środków rozpoznania i zbierania informacji *(ang. Sensor Grid);*

[10] Tamże

- G2 - sieć serwerów rozumiana jako zorganizowany system stanowisk dowodzenia i centrów decyzyjnych *(ang. Command and Control Grid);*
- G3 - sieć efektorów utożsamianych głównie z zaawansowanymi systemami uzbrojenia i aktywnymi środkami walki *(ang. Shooter Grid).*

Sieć informacyjna reprezentuje strukturę nadrzędną i stanowi szkielet budowanego obrazu informacyjnego przestrzeni walki, zwanego wspólnym obrazem sytuacji *(ang. Common Operational Picture - COP*). Wspólny, jednolity obraz przestrzeni walki można utożsamiać z pojęciem środowiska operacyjnego, w którym są umieszczone trzy współzależne sieci warstwowe: G1, G2, G3.

Warstwa sensorów jest umieszczona fizycznie w przestrzeni operacyjnej i pozyskuje stamtąd niezbędne informacje o monitorowanych obiektach oraz stanach parametrów środowiskowych. Głównymi elementami funkcjonalnymi tej warstwy są sensory, receptory i wszelkiego rodzaju urządzenia pozwalające na zdobywanie informacji źródłowej.

Koncepcje sieciocentryczne bazują na idei która zakłada, że współużytkowanie informacji jest źródłem wartości. W operacjach wojskowych wartość ta może być oceniana pod względem podstawowych atrybutów zdolności bojowej, mianowicie[11]:

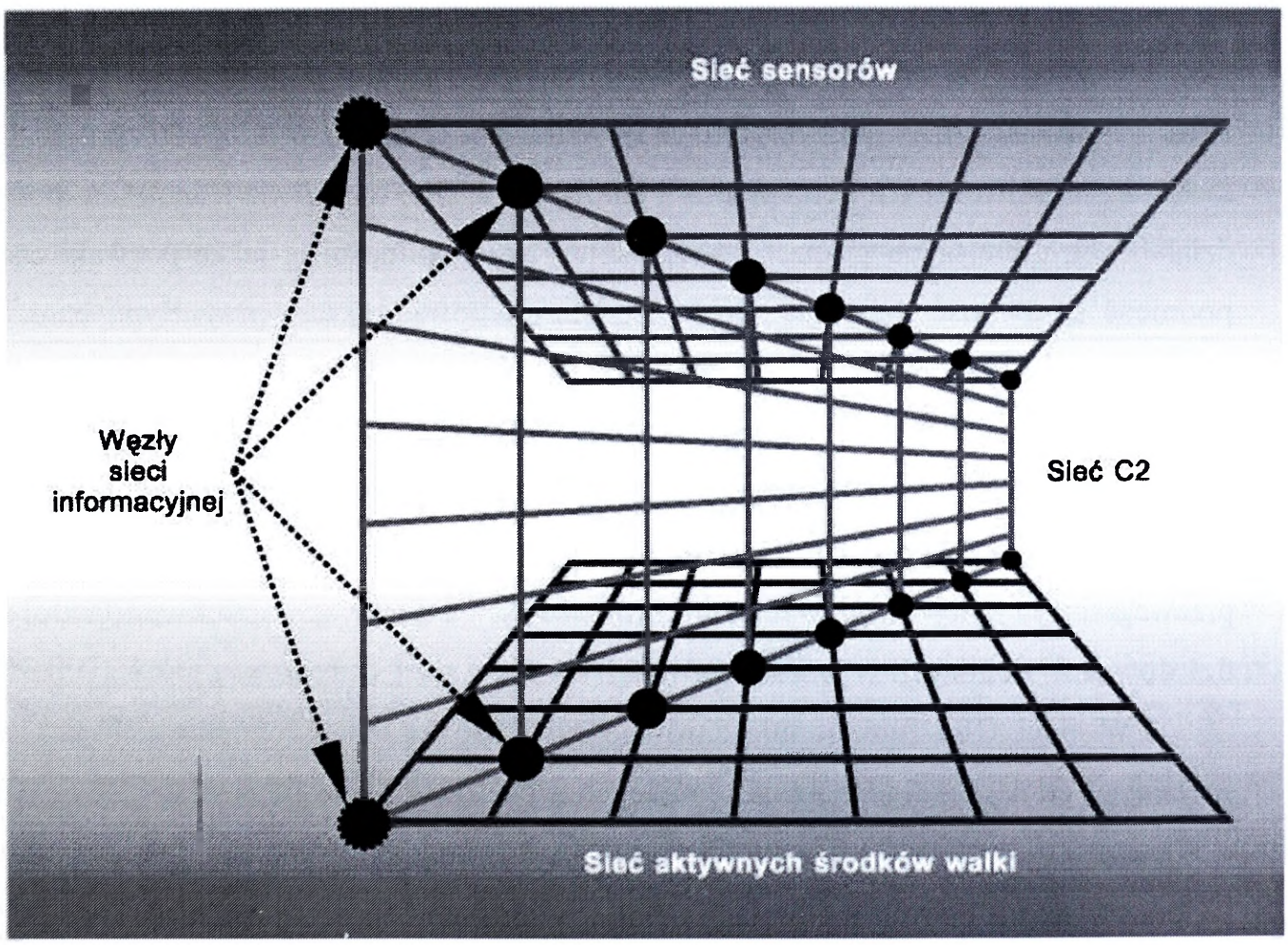
- zdolność do przetrwania,
- skuteczność rażenia,
- szybkość,
- dostępność,
- zdolność do reagowania.

Określenie zakresu, w jakim stosowanie technologii sieciowej w siłach zbrojnych może przyczynić się do zwiększenia ich zdolności bojowych jest złozone. Podkreślić należy, że nowa taktyka i procedury postępowania, których stosowanie jest możliwe dzięki radykalnemu zwiększeniu zdolności do współużytkowania informacji, w ogromny sposób wpływają na zwiększenie zdolności bojowych. Zwiększone zostają możliwości dowódców poprzez przekazywanie swoich zamiarów i decyzji szybciej, wierniej i dokładniej. Zdolność do ciągłego monitorowania wykonywania zadań pozwala na zmianę decyzji stosownie do rozwoju sytuacji. Istotną zaletą współużytkowania informacji jest możliwość nowego podejścia do dowodzenia, a mianowicie wykorzystywania wspólnej świadomości przestrzeni walki do osiągnięcia w wysokim stopniu samosynchronizacji działań i jednocześnie zachowania zdolności do natychmiastowego dostosowania się do zmian sytuacji operacyjnej.

---

[11] Tamże

Bazą funkcjonowania wojny sieciocentrycznej jest sieć przedstawiona na rysunku 1.2. Przez połączenie sieci środków rozpoznania (*ang. Sensor Grid*), sieci systemu dowodzenia (*ang. C2 Grid*) oraz sieci systemów uzbrojenia - aktywnych środków walki (*ang. Shooter Grid*), można osiągnąć efektywność i sprawność w prowadzeniu operacji militarnych. Jest to możliwe dzięki efektowi zespolenia, będącego skutkiem współużytkowania informacji we wspólnym środowisku operacyjnym. Co więcej, takie połączenie pozwoli na opracowanie nowych koncepcji prowadzenia działań bojowych[12].



Rys. 1.2. Sieć GIG

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

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

NCW to nie tylko koncepcja operacyjna, lecz także koncepcja systemu stanowiącego konglomerat systemów powiązanych ze sobą w jednolitą i spójną sieć.

Jak wspomniano wcześniej, idea wojny sieciocentrycznej może zostać zrealizowana tylko wtedy, gdy zostanie zbudowana odpowiednia infrastruktura sieciowa - tzw. Globalna Sieć Informacyjna[13]. Główne zadanie GIG będzie polegało na dostarczeniu i udostępnianiu infrastruktury technicznej w celu połączenia sił zbrojnych w jedną sieć. GIG zapewnia usługi w dziedzinie łączności, bezpieczeństwa, przetwarzania, zarządzania i dystrybucji informacji. Umożliwia połączenia typu „każdy z każdym" oraz interoperacyjność poszczególnych komponentów sił zbrojnych.

GIG umożliwia prowadzenie operacji sieciocentrycznych (*ang. Network Operations - NetOps*) dzięki możliwościom współdzielenia świadomości przestrzeni walki. Infrastruktura GIG umożliwia poszczególnym dowództwom działanie w dużym rozproszeniu oraz zwiększa możliwości ich percepcyjne i analityczne. GIG umożliwia jednostkom podległym działanie w mniejszych grupach, zwiększenie ich mobilności, a także pozwala znacznie podnieść sprawność działania. Sieć ta dostarcza infrastrukturę przyszłym, bardziej zaawansowanym systemom i aplikacjom dowodzenia, które pozwolą na elastyczną i adaptacyjną koordynację sił i systemów rozpoznania.

Rolą GIG[14] jest w głównej mierze umożliwienie prowadzenia wojny sieciocentrycznej a przez to uzyskanie przewagi informacyjnej (*ang. Information Superiority - IS*) i przewagi decyzyjnej (*ang. Decision Superiority - DS*) co w konsekwencji doprowadzi do pełnej dominacji w przestrzeni walki.

W sieci GIG funkcjonują zarówno systemy, sprzęt, oprogramowanie jak i usługi spełniające co najmniej jedno z następujących kryteriów[15]:

- umożliwiają transmisję danych i informacji w kierunku od źródła do odbiorcy i odwrotnie oraz wymianę danych i informacji pomiędzy sprzętem, oprogramowaniem i usługami sieci,
- umożliwiają utrzymanie, organizowanie, wizualizację i zabezpieczenie informacji a także wiedzy wymienianej z innym komponentami systemu (w tym sprzętem, oprogramowaniem lub usługami),

---

[13] The Joint Staff, C4 Systems Directorate, Information Superiority Division (J6Q): *Enabling the Joint Yision.* May 2000
[14] R. Szpakowicz, R. Hoffmann, *Koncepcja wojny sieciocentrycznej jako odpowiedź ...*
[15] Tamże

- umożliwiają przetwarzanie informacji lub danych w celu użycia ich przez inny sprzęt, oprogramowanie lub usługi.

1.3. Koncepcja NATO NEC[16]

Doświadczenia ostatnich konfliktów zbrojnych, w szczególności z operacji *Iraqi Freedom*[17], wykazały, że współdzielenie informacji pomiędzy różnymi systemami dowodzenia, wykrywania i śledzenia zwiększa efektywność sił zbrojnych. Aby jednak w pełni sprostać nowym wyzwaniom stojącym przed siłami zbrojnymi, istnieje pilna potrzeba głębokiej ich transformacji nie tylko poprzez inwestycje w sieć teleinformatyczną, systemy dowodzenia, wykrywania i śledzenia, ale w głównej mierze w sferze organizacji dowodzenia. Rozwój technologii teleinformatycznych zmienił diametralnie sytuację na współczesnym polu walki umożliwiając zwiększenie szybkości podejmowania decyzji, a przez to także tempa prowadzenia operacji. Z tego względu istnieje potrzeba przeprowadzenia głębokich zmian w sposobie planowania i prowadzenia walki.

Podczas szczytu NATO w Pradze w listopadzie 2002 roku ustalono, że w obliczu nowych zagrożeń niezbędna jest transformacja sił Sojuszu. Podjęto zobowiązania znane jako *Prague Capabilities Commitments*, identyfikując ponad czterysta obszarów, w których konieczne są zmiany. Czołowe miejsca zajęły dziedziny związane z dowodzeniem, łącznością i informatyką oraz rozpoznaniem. Rozważano ideę NATO Network Enabled Capability (NNEC), którą postrzegano jako jedną z kluczowych koncepcji mających decydujący wpływ na transformację sił zbrojnych NATO.

W odpowiedzi na decyzje podjęte w Pradze, dowództwo strategiczne Sojuszu opracowało w roku 2004 r. dokument *Bi-SC Strategic Vision: The Military Challenge*, w którym wyznaczone zostały:

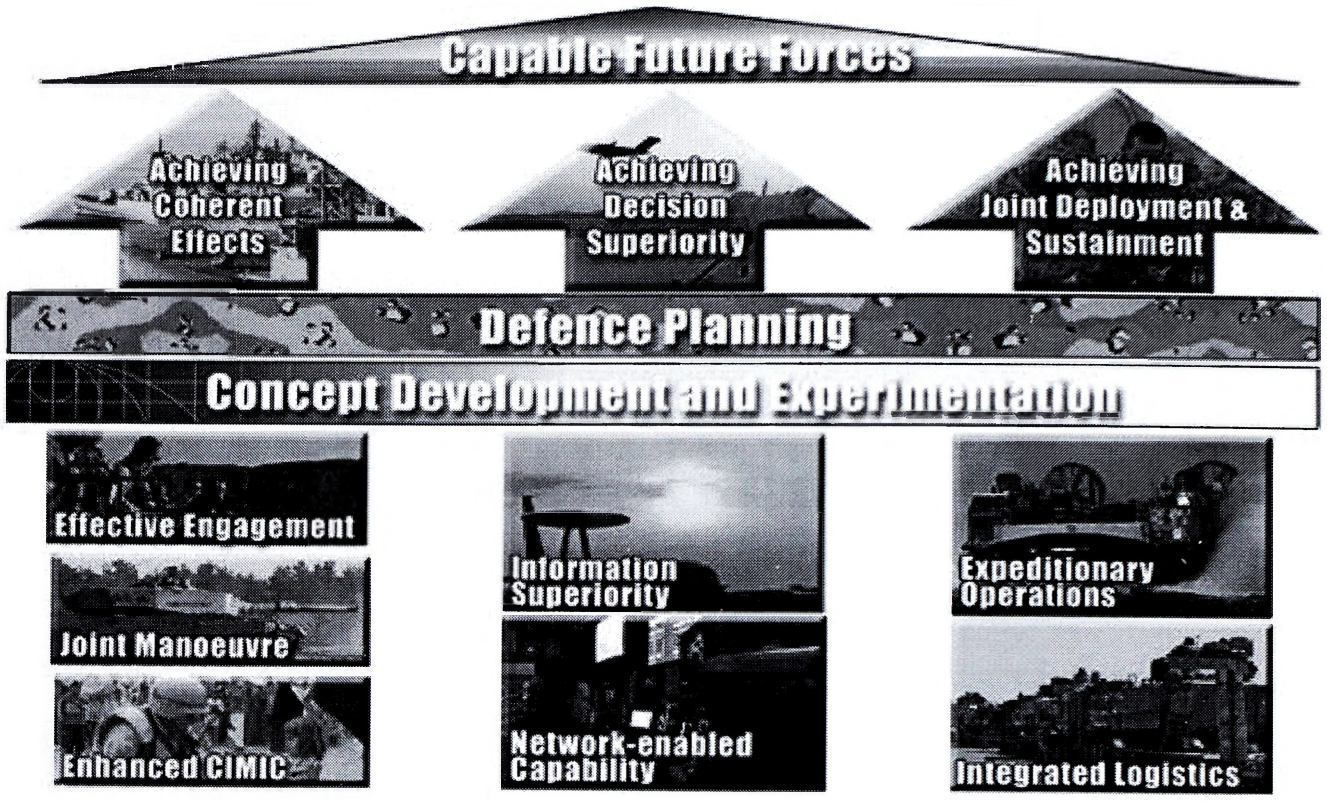
- cele i obszary przekształceń (transformacji),
- wizją prowadzenia przez Sojusz przyszłościowych operacji,
- zdolności, które powinien osiągnąć Sojusz,
- ramowe zasady prowadzenia procesu przekształceń (transformacji).

---

[16] Patrz *Wykonanie Studium Wykonalności Projektu Network Enabled Capabilities, Zegrze 2006*

[17] *Operation Iraqi Freedom C⁴ISR Lessons Learned*, http://defense-update.com/features/du-1-05/feature-oif-c4-1.htm

Sojusz określił 3 cele główne oraz 7 obszarów transformacji, wśród których kluczowymi wyznacznikami osiągnięcia wymaganej efektywności operacyjnej są dominacja informacyjna oraz **NATO Network Enabled Capability** .



Rys. 1.3. Cele i obszary transformacji NATO
Źródło: Wykonanie Studium Wykonalności Projektu Network Enabled Capabilities, Zegrze 2006

Zgodnie z przyjętą definicją, Network Enabled Capability rozumiane jest jako osiągnięcie zdolności integracji wszystkich elementów zaangażowanych w prowadzone operacje, począwszy od szczebla strategicznego a na szczeblu taktycznym kończąc. Założono, że integracja umożliwi osiągnięcie przewagi informacyjnej a w konsekwencji przewagi decyzyjnej, która pozwoli na uzyskanie zamierzonego efektu operacyjnego w krótszym czasie, przy efektywnym wykorzystaniu potencjału militarnego.

Komitet Wojskowy NATO w dokumencie (*MCM-0038-2005*) zdefiniował NATO NEC jako zdolność Sojuszu do integracji różnorodnych komponentów środowiska operacyjnego począwszy od poziomu strategicznego (włączając w to dowództwa NATO), na poziomie taktycznym kończąc, poprzez heterogeniczną sieć teleinformatyczną.

Należy przy tym zwrócić uwagę na przyjęte następujące wyróżniki NEC[18]:

- NEC jest ogólną koncepcją osiągania nowych jakościowo możliwości efektywnego i sprawnego wykorzystania potencjału militarnego, nie zaś konkretnym rozwiązaniem tech-

[18] *Wykonanie Studium Wykonalności Projektu Network Enabled Capabilities...*

nicznym będącym przedmiotem zakupu, ani też nie jest dojrzałym i spójnym rozwiązaniem gotowym do bezpośredniej implementacji;

- sieć teleinformatyczna jest niezbędnym atrybutem NEC. Jest warunkiem koniecznym, lecz dalece niewystarczającym do osiągnięcia oczekiwanych i pełnych zdolności;
- ważnym atrybutem NEC jest zdolność do współdzielenia informacji pomiędzy wszystkimi uczestnikami walki, która umożliwi tworzenie współdzielonego obrazu przestrzeni walki, dostarczająca niezbędnych danych dla zrozumienia zamiaru dowódcy;
- NEC, poprzez zmiany w doktrynie i sposobach walki oraz zachowaniach dowódców stworzy warunki do osiągnięcia samo synchronizacji walczących sił, zwiększenia szybkości procesu dowodzenia a tym samym istotnego zwiększenia siły bojowej;
- efektywne wykorzystanie osiągnięć współczesnej technologii i techniki teleinformatycznej stanowi niezbędny warunek osiągnięcia celów NEC;
- NEC stanowi wyzwanie dla sił zbrojnych państw członków NATO, wymagające przyjęcia odpowiedniej doktryny, zidentyfikowanych i wydajnych procesów oraz technologii, a także rozwiązania szeregu zasadniczych problemów, w tym związanych z osiągnięciem interoperacyjności oraz bezpieczeństwa, zarówno w wymiarze informacyjnym, technicznym, organizacyjnym, jak i socjologicznym.

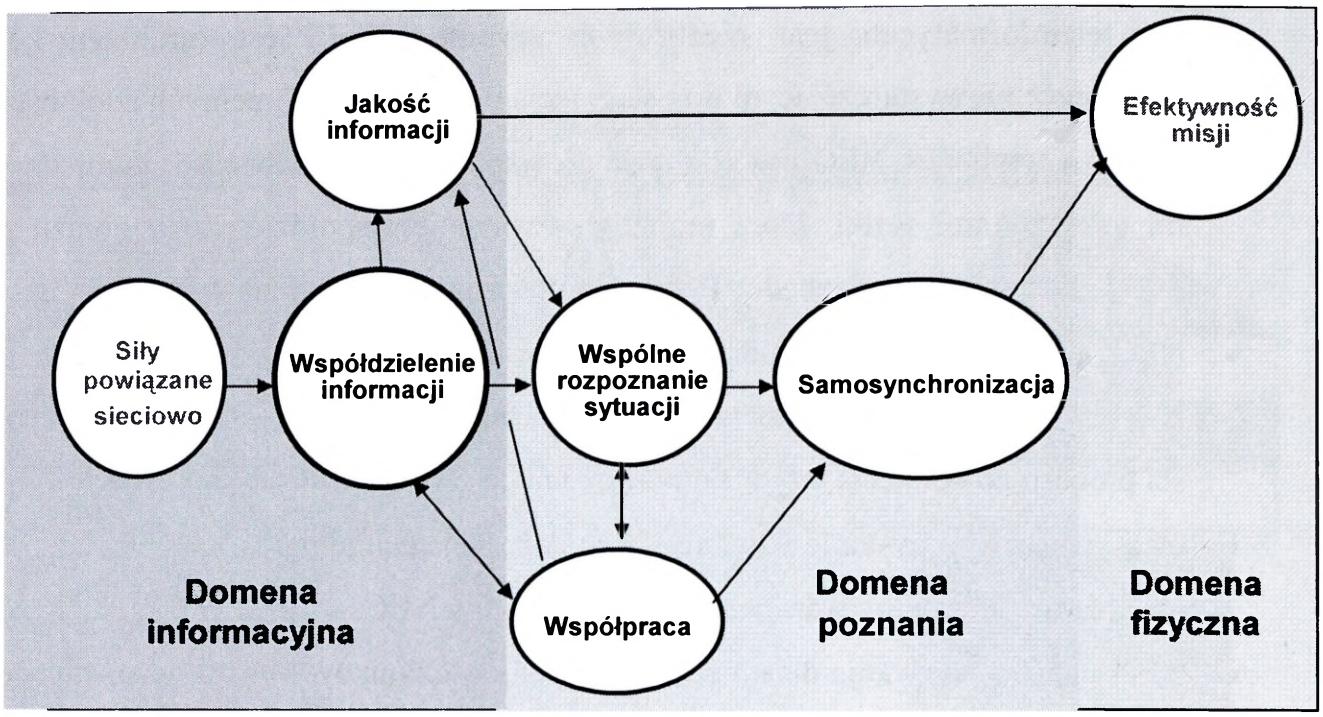
Zasady sieciocentryczności, przedstawione na rys. 1.4. można ująć następująco[19]:

- powiązanie walczących sił niezawodną i elastyczną strukturą sieciową znacząco polepsza zdolność współdzielenia (współposiadania) informacji;
- współdzielenie informacji oraz współdziałanie sił zaangażowanych w operację poprawia jakość zarówno informacji, jak i rozpoznania przestrzeni walki;
- współdzielenie rozpoznania stwarza dogodniejsze warunki do współdziałania, umożliwia osiągnięcie samo synchronizacji walczących sił bez konieczności koordynacji dowódców wyższych szczebli dowodzenia. Poprawia zdolność utrzymania powodzenia w walce i wysokiego tempa operacji.

Rozwój i implementacja koncepcji sieciocentrycznej, jako jednego z zasadniczych obszarów transformacji, postrzegany jest jako najefektywniejszy sposób wykorzystania inwestowanych środków w celu sprostania wymaganiom przyszłych operacji. W opinii większości członków Sojuszu wdrożenie koncepcji NCW jest celowe. Z tego też względu państwa NATO oraz Unii Europejskiej przeprowadziły niezależne oceny własnych możliwości transformacji i określiły drogi rozwoju w tym obszarze.

---

[19] Tamże



Rys. 1.4. Zasady sieciocentryczności
Źródło: Wykonanie Studium Wykonalności Projektu Network Enabled Capabilities, Zegrze 2006

W czerwcu 2005 roku Komitet Wojskowy NATO wydał dokument *Development of a NATO Network Enabled Capability*, który zawierał wstępną strategię rozwoju i wdrażania koncepcji NNEC. Dowództwo ACT powołało interdyscyplinarny zespół zadaniowy ds. NNEC – ACT NNEC IPT (*ang. ACT NNEC Integrated Project Team*), którego zadanie polega na opracowaniu dokumentów wchodzących w skład tzw. *NNEC Strategic Framework* (Ramowego Programu NNEC). Przyjęto, że dokumenty programu ramowego będą obejmowały[20]:

- wizję i koncepcję NATO NEC;
- rekomendowane struktury operacyjne i architektury systemowe;
- mapę drogową (*ang. NNEC Roadmap*) i plan przedsięwzięć (*ang. NNEC Business Case*);
- harmonogram wdrażania NNEC ze szczególnym uwzględnieniem kolejnej fazy prac nad rozwojem zdolności sieciocentrycznej.

W wyniku realizacji powyższych zadań, w styczniu 2006r. dowództwo ACT przyjęło pierwszy z dokumentów *NNEC Vision & Koncept*. Bazując na podstawowych dokumentach NATO sprecyzowano rolę NNEC w procesie transformacji militarnej Sojuszu wskazując kluczowe elementy koncepcji warunkujące osiągnięcie założonych celów. Przedstawiono

[20] Tamże

koncepcję osiągania zdolności sieciocentrycznej przez NATO, przede wszystkim w sferze poznawczej i technicznej oraz sformułowano zalecenia implementacyjne i kierunki dalszych działań.

Wizją NNEC jest poprawa efektywności operacyjnej poprzez tworzenie zdolności wynikających z powiązania siecią dostępnych zasobów informacyjnych. NNEC jest jednym z priorytetowych obszarów transformacji umożliwiającym maksymalizację zdolności NATO do osiągnięcia dominacji informacyjnej. Przyjęto, że rozwój NNEC powinien być realizowany poprzez powiązanie i doskonalenie istniejących już systemów, tworzących tzw. **federację sieci, usług i procesów**, nie zaś poprzez wymianę aktualnie wykorzystywanych systemów. Rozwój ten powinien przebiegać w sposób stopniowy, wspierany przez poszczególne państwa Sojuszu tak, aby zaspokoić potrzeby Dowództwa Operacyjnego (ACO).

Przyjęto, że realizacja NNEC przyczyni się do istotnej poprawy funkcjonowania sił zbrojnych NATO w zakresie[21]:

- uzyskania przewagi informacyjnej i decyzyjnej, w tym poprzez:
  - dostęp do szerszego zbioru źródeł informacji;
  - dostarczenie w odpowiednim czasie informacji w celu wsparcia procesu podejmowania decyzji;
  - konsolidację sensorów, uczestników działań i platform oraz wsparcie zdolności operacyjnych;
  - optymalizację procesów wsparcia decyzyjnego i planowania;
  - zwiększenie powiązań informacyjnych z organizacjami pozamilitarnymi umożliwiającymi ich pełne zaangażowanie, a także ich zdolność do pełniejszego rozumienia środowiska operacyjnego;
  - odpowiednie wsparcie grup zainteresowań w celu zapewnienia im pełnej świadomości sytuacyjnej i zdolności do skutecznego wspólnego działania;
- zwiększonych zdolności sił NATO - wspólne powiązania informacyjne pozwolą poprawić koordynację i synchronizację działań, zapewniając bardziej precyzyjne ich efekty.

Osiągnięcie przewagi informacyjnej oraz decyzyjnej nad przeciwnikiem możliwe będzie dzięki współdzieleniu informacji, współpracy, wspólnej ocenie sytuacji, pozyskiwaniu oraz integrowaniu informacji, a także tworzeniu na ich podstawie zasobów wiedzy dostosowanych do indywidualnych potrzeb użytkownika.

---

[21] Tamże

Należy zauważyć, że tworzenie i utrzymanie standardowych, współdzielonych zestawów usług w środowisku federacji sieci, usług i procesów będzie wymagać stworzenia odpowiednich mechanizmów zarządzania, działających pomiędzy systemami narodowymi oraz obszarami funkcjonalnymi.

Współdzielenie informacji oraz jej udostępnienie uprawnionym użytkownikom w odpowiednim czasie jest uwarunkowane także wykorzystaniem zaawansowanych mechanizmów ochrony informacji. Zwiększenie efektywności misji poprzez osiąganie przewagi informacyjnej jest ściśle związane z zaufaniem do źródła informacji oraz wysokim poziomem bezpieczeństwa posiadanej infrastruktury teleinformatycznej. Z tego względu niezbędne jest zapewnienie odpowiednich mechanizmów szyfrowania i zarządzania kluczami, etykietowania obiektów i ich szyfrowania na podstawie zawartości informacyjnej, zwiększonej ochrony przed niepowołanym dostępem do informacji oraz nieuprawnionymi działaniami. Współdzielenie informacji musi być także wsparte narodowymi procedurami umożliwiającymi wzajemne korzystanie z zasobów informacyjnych, a także skutecznymi mechanizmami dynamicznej analizy i oceny ryzyka.

Konieczne zmiany w obszarze poznawczym i technicznym tworzą wyzwania, których przezwyciężenie umożliwi uzyskanie oczekiwanego efektu. Niezbędne jest odpowiednie kształtowanie zachowań ludzkich, dostosowanie zasad i metod dowodzenia do nowych uwarunkowań i możliwości technicznych.

Wprowadzenie zmian systemowych i wdrożenie rozwiązań zgodnych z koncepcją wojny sieciocentrycznej powinno pozwolić na uzyskanie przez siły zbrojne nowych zdolności, które przełożą się na szereg korzyści przedstawionych na rysunku 1.5.

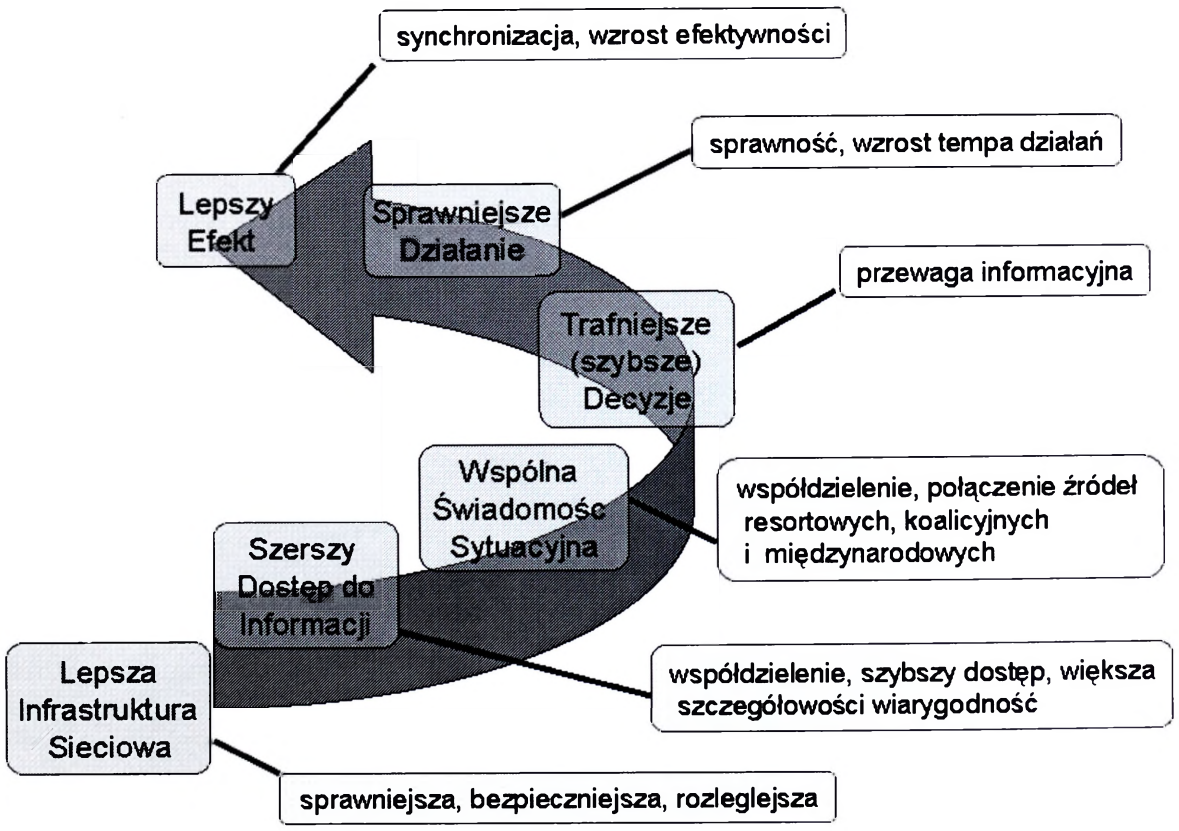
Dane uzyskiwane od sensorów umożliwiają stworzenie ciągłego pola informacyjnego to znaczy jednolitego obrazu sytuacji, który może być wykorzystywany przez każdy system walki znajdujący się w zasięgu tego pola. Pozwala to na uzyskanie następujących efektów[22]:

- zapewnienie szybszego i ciągłego przepływu informacji pomiędzy różnymi szczeblami dowodzenia, umożliwiającego zwiększenie tempa prowadzonych operacji;
- utworzenie sprawnych, elastycznych, zdolnych do szybkiego reagowania struktur dowodzenia i wojsk;
- zwiększenie skuteczności dowodzenia i efektywności pracy sztabów dzięki dostępowi do wspólnego obrazu sytuacyjnego;

[22] Tamże

- zwiększenie możliwości tworzenia i wykorzystania wspólnej świadomości sytuacyjnej przez dowódców niższych szczebli dowodzenia, a tym samym stworzenie warunków dla wystąpienia efektu samosynchronizacji;
- zwiększenie skuteczności ostrzegania przed atakiem przeciwnika;
- zwiększenie efektywności broni precyzyjnego rażenia;
- lepsze wykorzystanie rozproszonych geograficznie sił;
- umożliwienie oferowanie poszczególnym siłom narodowym specjalistycznych usług, wykorzystanie efektu synergii i skalowalności w środowisku typu „dołącz się i działaj" (ang. *plug&play*).

Osiągnięcie zdolności sieciocentrycznej umożliwia przewagę decyzyjną poprzez terminowe dostarczanie i efektywne wykorzystanie informacji z różnych źródeł.



Rys. 1.5. Łańcuch korzyści wynikających z osiągnięcia zdolności sieciocentrycznej
Źródło: Wykonanie Studium Wykonalności Projektu Network Enabled Capabilities, Zegrze 2006

Uogólniając, można stwierdzić, że sieciocentryczność[23]:

- obejmuje integrację wielu komponentów środowiska operacyjnego, od szczebla strategicznego do taktycznego za pomocą wydajnych sieci połączeń;
- wykorzystuje przewagę decyzyjną do zwiększenia efektywności procesu decyzyjnego drogą terminowego dostarczania właściwej informacji wszystkim uczestnikom działań;
- wspiera proces planowania operacyjnego, rozwijania, wykorzystania i zabezpieczania wojsk oraz zapewnia dostarczanie dokładnej, pewnej i właściwej informacji, która powoduje wzrost zdolności bojowej i efektywności działania;
- wspiera prowadzenie operacji ukierunkowanych na efekt poprzez zapewnienie wykorzystania wsparcia informacyjnego, tj. zapewnia zdolność wykorzystania zasobów informacyjnych i możliwości różnych rządowych agend, ośrodków naukowych, przemysłowych czy akademickich oraz służb publicznych do wsparcia prowadzonych działań (operacji);
- wspiera logistykę poprzez dostarczanie niezbędnych informacji dla prognozowania potrzeb, planowania procesu zabezpieczenia działań oraz kierowania logistyką w dynamice działań;
- przyśpiesza proces ustalania i stosowania wspólnych standardów oraz wymusza zacieśnienie współpracy z instytutami naukowymi i przemysłem obronnym;
- umożliwia rozwój oraz wspiera proces implementacji nowych, efektywniejszych struktur i procedur dowodzenia i zarządzania w szeroko rozumianym systemie obrony państwa.

Sieciocentryczność ma trzy zasadnicze, zazębiające się i zależne od siebie wymiary[24]:

- ludzi,
- infosferę,
- sieć powiązań.

Ludzie są najważniejszym aktywem każdych sił zbrojnych. Szczególnie w erze informacyjnej, zwiększenie efektywności działania SZ w głównej mierze zależy od ich zdolności do pozyskania odpowiednich kandydatów i powszechnego oraz efektywnego szkolenia personelu. Osiągnięcie niezbędnego poziomu przewagi decyzyjnej zależy przede wszystkim od zdolności poszczególnych osób funkcyjnych do wykorzystania możliwości, jakie niosą nowoczesne technologie. Personel powinien posiadać umiejętności wykorzystania wiedzy i doświadczenia do szukania i współużytkowania informacji z wielu różnorodnych sensorów i użycia jej w procesie decyzyjnym. Wymiar ludzki obejmuje aspekty[25]:

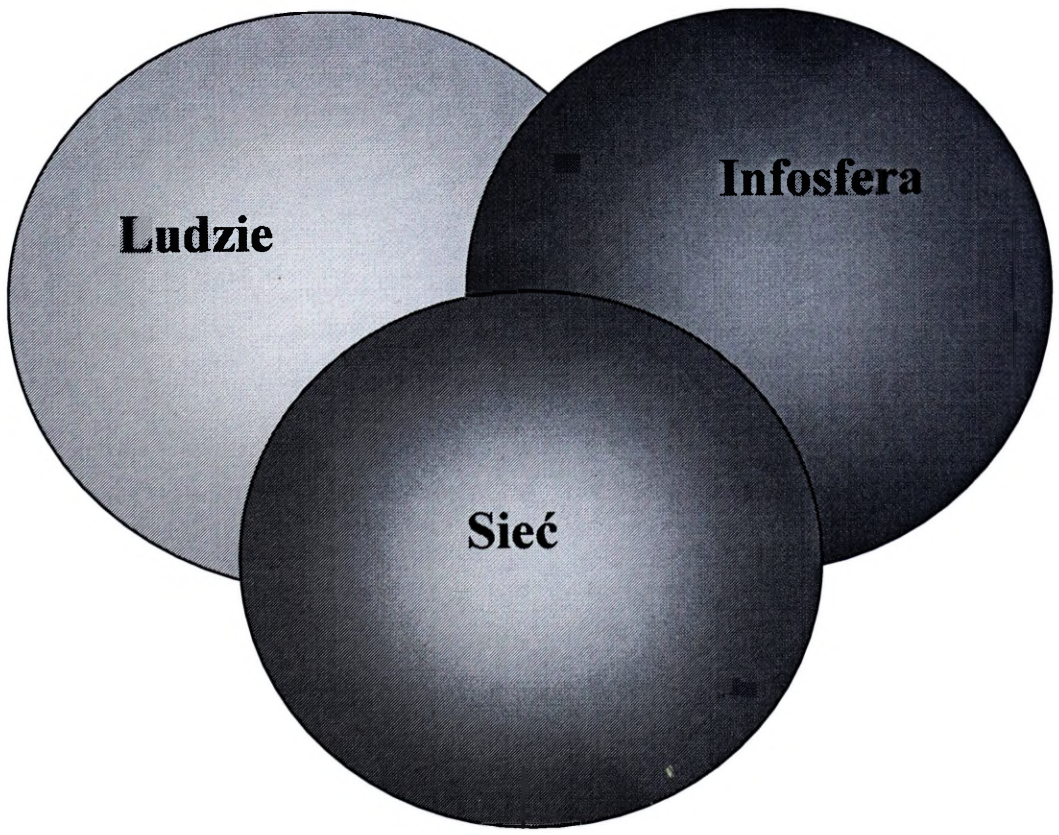
---

[23] Tamże
[24] Tamże
[25] Tamże

- personalny: rekrutacja, selekcja, rozwój, kompetencje, przywództwo, kształcenie i szkolenie;
- organizacyjny: struktury, odpowiedzialność, rola i zakres obowiązków;
- kulturowy: bariery kulturowe, zaufanie, różnice w percepcji i rozumieniu (ocenie) zjawisk;
- realizacji programu: procedury, polityczne i prawne uwarunkowania oraz doktryna.

Informacyjny wymiar sieciocentryczności obejmuje wszystkie aspekty zarządzania informacją, w tym[26]:

- udostępnienie raz pozyskanej informacji wielu użytkownikom bazując na zasadzie „need-to-know" i „right to know";
- informowanie o posiadanych zasobach informacji w celu zapewnienia dostępu za pośrednictwem bazowego zestawu usług;
- interpretacja i translacja danych do wspólnego formatu;
- prezentacja i fuzja informacji;
- tworzenie grup użytkowników informacji;
- uzyskiwanie właściwej informacji we właściwym czasie;
- bezpieczeństwo informacyjne.



Rys. 1.6. Wymiary koncepcji sieciocentrycznej
Źródło: Wykonanie Studium Wykonalności Projektu Network Enabled Capabilities, Zegrze 2006

Sieć powiązań to środowisko różnorodnych sieci teleinformatycznych i telekomunikacyjnych umożliwiających współużytkowanie informacji. Istotne znaczenie mają następujące cechy środowiska[27]:

- skalowalność;
- rozległość oraz zasięg sieci, jej przepustowość spełniająca wymogi sił zbrojnych w całym zakresie przewidywanych działań;
- mobilność, zdolność do szybkiej rekonfiguracji i natychmiastowego przemieszczenia się do rejonów działań;
- jakość usług i adaptowalność;
- odporność i bezpieczeństwo.

Wnioski

Wyniki badań przedstawione w niniejszym rozdziale pozwalają na stwierdzenie, że początki teorii walki sieciocentrycznej są rezultatem rozwoju technologii teleinformatycznych i ich szerokiego komercyjnego wykorzystania. Rozwiązania stosowane na rynku cywilnym (komercyjnym) szybko zostały zaadoptowane do działań militarnych.

Badania wykazały, że istnieje wiele różnorodnych definicji walki sieciocentrycznej. Ich analiza udowodniła, że walka sieciocentryczna jest sposobem prowadzenia działań w którym siły zbrojne, spięte siecią teleinformatyczną, uzyskują przewagę informacyjną na wszystkich poziomach prowadzenia działań. Umożliwia to prowadzenie szybkich i skutecznych działań militarnych przy możliwie najefektywniejszym i ekonomiczniejszym wykorzystaniu sił i środków.

Współczesne wyposażenie i wyszkolenie sił zbrojnych państw NATO pozwala na prowadzenie walki sieciocentrycznej jedynie na poziomie taktycznym, co potwierdziły doświadczenia z operacji prowadzonych w Afganistanie i Iraku. W perspektywie najbliższych kilku lat przewidywane jest prowadzenie działań sieciocentrycznych w skali rodzajów sił zbrojnych, a dopiero prawdopodobnie około 2020 roku możliwe będzie osiągnięcie pełnej implementacji standardów w tym zakresie.

Główną zasadą prowadzenia działań w sieciocentrycznej przestrzeni walki jest dążenie do uzyskania przewagi informacyjnej, co oznacza zapewnienie własnym wojskom terminowej, dokładnej i odpowiedniej do aktualnej sytuacji informacji w stosunku do tego co może uzyskać przeciwnik.

---

[26] Tamże
[27] Tamże

Stworzenie sieci współdziałających użytkowników, w której dostępne będą systematycznie uaktualniane informacje o przeciwniku i siłach własnych oraz ich możliwościach zapewni osiągnięcie i utrzymanie adekwatnej do potrzeb zbiorowej świadomości sytuacyjnej. Szybkość dowodzenia i skuteczność podejmowanych decyzji w działaniach sieciocentrycznych pozwoli na szybkie użycie niezbędnych sił.

W działaniach sieciocentrycznych znacząca będzie także zasada samo synchronizacji. Opiera się ona na założeniu, że na najniższych szczeblach dowodzenia możliwe będzie, w oparciu o zamiar dowódcy wyższego szczebla oraz zbiorową świadomość sytuacyjną, oddolne zmienianie zakresu i sposobu realizacji otrzymanych zadań przez działające niemal autonomicznie zgrupowania taktyczne. Zwiększanie możliwości przejawiania inicjatywy przez podwładnych osiągnięte będzie poprzez zwiększenie tempa działań oraz poprawę zdolności sił zaangażowanych w walce. Zasada samo synchronizacji wymaga odpowiedniego poziomu wyszkolenia sił wojskowych na wszystkich szczeblach dowodzenia.

Przeprowadzone badania wskazały, że rozproszenie sił w przestrzeni walki w działaniach sieciocentrycznych wpływa na zmianę sposobu osiągania przewagi. Pozostawienie sił w rozproszeniu zwiększa ich zdolność do przeżycia i powoduje, iż wejście w kontakt z przeciwnikiem realizowane jest wtedy, gdy wymagają tego realizowane zadania.

W walce sieciocentrycznej kluczową rolę odgrywać będą kompatybilne systemy rozpoznania, łączności i dowodzenia, które zapewnią odpowiednią architekturę informacyjną. Siły i środki połączone będą siecią składającą się z trzech elementów: sieci informacyjnej, sieci czujników i sieci dowodzenia.

2. Rola i znaczenie informacji

Abstrakcyjny i wieloaspektowy charakter informacji powoduje, iż może być ona postrzegana w różny sposób, w różnej postaci oraz za pomocą wielorakich kodów. Jednocześnie powszechność stosowania terminu informacja wyraża się tym, iż trudno wskazać dziedzinę nauk, w której nie mamy do czynienia z pozyskiwaniem, przetwarzaniem oraz przekazywaniem informacji.

2.1. Definicje informacji

Współcześnie istnieje szereg różnorodnych definicji oraz ujęć terminu informacja. Przez wielu teoretyków zajmujących się definiowaniem pojęcia informacji, jest ona uważana jest za pojęcie pierwotne, nie dające się zdefiniować. Funkcjonowanie informacji w różnorodnym środowisku spowodowało, iż do tej pory nie doczekała się ona jednoznacznej definicji wyrażającej jej istotę. Część autorów rezygnuje z jej definiowania, poprzestając na intuicyjnym i potocznym jej rozumieniu.

Słowo informacja wywodzi się z łacińskiego słowa *informatio* co oznacza wyobrażenie, wyjaśnienie, zawiadomienie. Interesujący zbiór definicji terminu informacja przedstawia w jednej ze swoich publikacji W. Flakiewicz[1]. Przytacza on najpopularniejsze definicje tego pojęcia:

- *Informacja to komunikacja, łączność, w wyniku której likwiduje się nieokreśloność* (C. Shannon).
- *Informacja jest nazwą treści zaczerpniętej ze świata zewnętrznego, nie jest więc ani materią, ani energią* (N. Wiener).
- *Informacja jest to czynnik sterujący strumieniami zasileń, wykorzystywany w organizmach żywych lub maszynach do bardziej sprawnego, efektywnego i celowego działania* (E. Kowalczyk).
- *Informacja jest to treść przekazywanych od nadawcy do odbiorcy wiadomość, będąca opisem, poleceniem, zakazem, nakazem lub zleceniem* (J. Gościński).
- *Jest to przekazywanie wiedzy do odbiorcy informacji, ze względu na jej wartość, umożliwiające zmniejszenie niepewności działania odbiorcy informacji* (R. Ackoff).

---

[1] W. Flakiewicz, *Podejmowanie decyzji kierowniczych*, Warszawa 1973, s. 38.

- *Informacja jest to wiedza przekazywana przez innych ludzi bądź uzyskiwana przez studia, obserwacje, badania* (A. Webster).

Analiza powyższych definicji zaowocowała przedstawieniem przez Flakiewicza własnej definicji informacji jako ... *czynnika, który zwiększa naszą wiedzę o otaczającej nas rzeczywistości*. Ujęcie to uzupełnia koncepcja profesora Mariana Mazura, największego polskiego cybernetyka, który w odniesieniu do psychologicznej teorii odbicia stwierdza, że informacja to *związek zachodzący pomiędzy oryginałem a obrazem tego oryginału*.

Definicję, stanowiącą niejako podsumowanie prezentowanych powyżej poglądów przedstawił profesor Piotr Sienkiewicz, który ujął informację jako *„zbiór faktów, zdarzeń, cech, obiektów ujęty w takiej formie, że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne"*[2].

Przedstawione definicje uprawniają do stwierdzenia, że informacja jest czymś więcej niż tylko wiadomością, znakiem lub inną formą komunikowania. W swojej istocie jest ona zarówno opisem rzeczywistości, jak i odzwierciedleniem stanu systemu oraz jego elementu, który może podlegać procesom pozyskiwania, przetwarzania, gromadzenia lub dystrybucji.

Pojęciem nierozerwalnie związanym z informacją jest pojęcie systemu informacyjnego. Jest to zintegrowany zespół ludzi, środków i metod zbierania, kodowania, dekodowania, przechowywania, przetwarzania, odnajdywania i komunikowania a także aktualizacji i użytkowania niezbędnych danych dla potrzeb kadry kierowniczej w celu podjęcia prawidłowych decyzji.[3] System taki jest w pewnym stopniu odzwierciedlony poprzez strukturę organizacyjną wskazującą główne drogi przepływu danych, uwidaczniając jednocześnie hierarchię potrzebnych informacji na poszczególnych szczeblach organizacyjnych i ich wzajemne relacje.

Przed systemem informacyjnym organizacji są stawiane z góry ustalone wymagania[4]:

- dostarczanie kompleksowych i aktualnych informacji, zapewnianie selektywnego i skutecznego wykorzystania informacji oraz właściwej wymiany informacji pomiędzy komórkami organizacyjnymi, przełożonymi i podwładnymi w obydwu kierunkach,
- prostotę w użytkowaniu i zapewnieniu stałej, automatycznej metody pozyskiwania informacji z ustalonych źródeł,
- umożliwienie natychmiastowego pozyskania danych, nawet z najniższego szczebla zarządzania, wyszukiwanie i kojarzenie informacji z różnych źródeł, przedstawienie danych i wyników ich analiz w różnych układach sprawozdawczych,

---

[2] P. Sienkiewicz, *Systemy kierowania,* Warszawa 1989, s. 128.
[3] S. Pietrzak, *Informacyjny system zarządzania przedsiębiorstwem*, Ekonomika i Organizacja Przedsiębiorstwa, nr 6/1998, s. 7
[4] Tamże, s. 7-8

- przepływu informacji opartego na sprzężeniach zwrotnych.

Należy zauważyć, że w miarę zwiększania potrzeb i możliwości system informacyjny ulega przemianom w celu zabezpieczenia prawidłowego przetwarzania, gromadzenia i przesyłania informacji. Na przemiany te ma wpływ zarówno zarządzanie informacją, którego realizacja sprawia, że pojawiają się nowe potrzeby informacyjne a tym samym konieczność określenia nowych powiązań komunikacyjnych jak i nowe metody przetwarzania, gromadzonych i przesyłania informacji.

Wykorzystanie samej technologii nie zagwarantuje skutecznego działania. Jej zastosowanie daje efekty, tylko wtedy, gdy jest ona zastosowana właściwie.[5] W tym celu organizacja musi dysponować odpowiednio wyszkolonym personelem, zdolnym do wykorzystania nowych technologii informacyjnych. Posiadanie takich umiejętności staje się obligatoryjne i jest warunkiem sprawnego zarządzania informacją. Warunkiem rzeczywistego stosowania tych narzędzi jest przekonanie pracowników, zarówno decydentów jak i operatorów, że są one im niezbędne podczas realizacji procesu decyzyjnego. Niezbędne jest także wykorzystanie wiedzy i doświadczenia personelu (operatorów), nowoczesnych metod archiwizowania informacji i sprawnej komunikacji pomiędzy uczestnikami danego procesu z wykorzystaniem systemów wspomagających procesy decyzyjne.

W literaturze przedmiotu można spotkać także pojęcie „zarządzania wiedzą" co oznacza kształtowanie odpowiednich czynników motywujących pracowników do tworzenia wiedzy i wykorzystania jej w wyznaczonym kierunku. Istotne znaczenie ma racjonalizacja zasobów wiedzy ze względu na potrzeby organizacji i możliwości twórcze operatorów. Inna definicja tego pojęcia mówi, że jest to świadoma strategia dostarczania potrzebnej wiedzy odpowiednim ludziom we właściwym czasie i pomaganie im w dzieleniu się nią i wykorzystywaniu w działaniu.[6] Z powyższego wynika, że celem zarządzania wiedzą jest wypracowanie odpowiednich metod i technik umożliwiających efektywny przebieg procesów tworzenia, gromadzenia i wykorzystania wiedzy.

Przeprowadzone analizy wykazały, że w procesie przetwarzania informacji mamy do czynienia z tzw. wiedzę cichą i formalną. Źródłem powstawania wiedzy cichej jest doświadczenie personelu - co czasami skutkuje brakiem możliwości jej sformułowania, a przez to przekazania innym osobom. Sposobem na jej wydobycie są w głównej mierze obserwacja i

---

[5] E. Kolbusz, *Informacja jako przedmiot zarządzania, Informatyka w zarządzaniu*, Zeszyt IIwZ, Studia Informatica 13/1999, s. 15

[6] J. Brzóska, K. Palucha, *Zarządzanie wiedzą jako czynnik sukcesu restrukturyzowanego przedsiębiorstwa, Źródła sukcesów i porażek przedsiębiorstw. Aspekt strategiczny*, Zeszyty naukowe Akademii Ekonomicznej we Wrocławiu, 870/2000, s. 364

naśladownictwo oraz nieformalne przekazywanie spostrzeżeń. Wiedza formalna jest wyrażona za pomocą słów, znaków, czy symboli. Wiedzę taką definiuje się jako zbiór informacji świadomych, które człowiek aktualizuje w swojej pamięci i na których może koncentrować uwagę, a także potrafi je przekazać na zewnątrz.[7] Powstanie dodatkowej wiedzy ma miejsce w wyniku interakcji pomiędzy tymi dwoma jej rodzajami. Należy pamiętać, że przetwarzanie wiedzy jest działalnością ludzką, a tym samym działalnością nieograniczoną, stale podlegającą rozwojowi. Można pokusić się o stwierdzenie, że zarządzanie wiedzą nigdy się nie kończy, ponieważ wiedza, tak jak informacje, poprzez ich wykorzystanie stale zwiększa swoją wartość.

2.2. Klasyfikacja i elementy składowe informacji

Po tak przedstawionych definicjach kolejnym krokiem identyfikacji informacji jest określenie elementów składowych, które są przydatne do sklasyfikowania informacji. Według profesora Zbigniewa Ścibiorka struktura każdej informacji składa się z czterech następujących elementów[8]:

- treści informacji;
- nośnika treści;
- symboli, za pomocą których jest utrwalona;
- sposobu przenoszenia informacji.

Powiązanie powyższych elementów tworzy informację, która determinuje warunki jej przetwarzania, dystrybucji i wykorzystania, a więc warunki jakie występują w procesie dowodzenia.

Treścią informacji jest to, co dana osoba chce przekazać innym. Do treści można zaliczyć: wiedzę, opis, odczucia lub inne wrażenia odnoszące się do danego przedmiotu, zjawiska lub stanu określone przyjętymi symbolami. W procesie dowodzenia treścią informacji jest treść dokumentu dowodzenia przesyłanego pomiędzy uczestnikami wymiany informacji.

Nośnik treści informacji jest elementem fizycznym, na którym informacja została utrwalona. Może to być odpowiednio: papier, taśma magnetofonowa, klisza filmowa, dyskietka, płyta, pamięć komputera, obrazy, tablice oraz wszystkie inne elementy, na których możemy zapisać treść informacji. Dobór nośnika informacji odbywa się najczęściej w odnie-

---

[7] B. Stefanowicz, *Wybrane zagadnienia infologicznej analizy danych*, Zeszyty Naukowe Szkoły Wyższej im. P. Włodkowica, 12/1999, s. 27

[8] Z. Ścibiorek, *Podejmowanie decyzji,* Warszawa 2003, s. 73.

sieniu do procedur oraz możliwości technicznych danej organizacji. Nośnikiem informacji mogą być odpowiednie bazy danych, zdolne do przechowywania treści informacji.

Następny element składowy wiadomości - symbole treści informacji - są umownymi znakami za pomocą których została zapisana informacja. W odniesieniu do najpopularniejszego narzędzia komunikowania interpersonalnego jakim jest język symboli, są to odpowiednio: litery, cyfry, rysunki, znaki, dźwięki, sygnały świetlne itp. Stosowanie poszczególnych rodzajów symboli ma sens tylko wtedy, jeśli wszyscy uczestnicy procesu wymiany informacji posługują się tymi samymi symbolami. Wszędzie tam, gdzie użytkownik chce ukryć przed innymi treść informacji stosuje symbole stanowiące określony kod. Dobierając symbole do zapisu informacji należy pamiętać o zasadzie takiego ich doboru, aby jak najwierniej oddać istotę treści informacji. Język jest w tej sytuacji jest uniwersalnym narzędziem, którego poszczególne elementy – wyrazy i zdania, mogą być dobierane w różnorodny sposób. Symbole mogą być także dobierane odpowiednio do możliwości percepcji odbiorcy, jak również środków za pomocą, których przekazywana będzie informacja.

W organizacji jaka są siły zbrojne szybka i bezbłędna wymiana informacji ma znaczenie fundamentalne. W celu wyeliminowania pomyłek błędnej interpretacji tekstu stworzono własny język wymiany informacji opublikowany jako ADatP-3 (Allied Data Publication Nr 3) [9]. Informacja zapisana w tym języku jest *spójna, dokładna, zaktualizowana i czytelna.* W standardzie tym zakres pojęciowy opisany jest wyłącznie za pomocą słów (z uwzględnieniem skrótów i kodów), których znaczenie zostało w sposób jednoznaczny zdefiniowane przez wszystkich zainteresowanych (kraje członkowskie). W tak stworzonym sztucznym języku opracowano strukturę umożliwiającą przekazanie jak najwięcej informacji przez samo położenie słów w ramach zdefiniowanych formatów. Struktura ta, znana pod pojęciem FORMETS (*ang. NATO MESSAGE TEXT FORMATTING SYSTEM*), określa zasady, składnie i słownictwo dla FORMATÓW TEKSTU WIADOMOŚCI.

Ostatnim elementem struktury informacji jest sposób przenoszenia informacji. Najczęściej jest on wynikiem wymienionych już aspektów technicznych lub przyjętych w organizacji rozwiązań. Przekaz informacji odbywać się może w bezpośrednich relacjach interpersonalnych lub za pomocą różnego rodzaju urządzeń lub organizacji specjalizujących się w przesyłaniu informacji. Współczesny, dynamiczny rozwój techniczny powoduje, iż oprócz tradycyjnego przekazu informacji za pomocą poczty, prasy, telewizji, radia i telefonów szerokie

[9] Koncepcja systemu opisana została w normie STANAG 5500

zastosowanie ma przekaz pocztą elektroniczną, prądem elektrycznym lub impulsem elektromagnetycznym.

Różnorodność nośników oraz sposobów ich przekazywania generuje podział informacji, którego istota odnosi się do kryterium formy przedstawienia, wyróżniamy więc informacje:[10]

- ustne;
- pisemne;
- audiowizualne;
- graficzne;
- dźwiękowe;
- sygnałowe;
- inne.

Istotnym kryterium jest także znaczenie informacji w procesie decyzyjnym. Według niego wyróżniamy informacje:[11]

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

Z punktu widzenia wpływu informacji na podejmowane decyzje, wyróżniamy informacje:[12]

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

---

[10] *Zarządzanie informacjami w procesie dowodzenia na szczeblach taktycznych wojsk lądowych z wykorzystaniem sieci teleinformatycznych, praca naukowo-badawcza*, AON, Warszawa 2006, s. 70
[11] Tamże,
[12] Tamże, s. 71

- koordynacyjne, regulujące działania i procesy zachodzące pomiędzy poszczególnymi elementami organizacji;
- podające do wiadomości wyniki działania (kontrolne).

W procesie dowodzenia realizowanym na szczeblach taktycznych informację można podzielić także uwzględniając pilności i ważności przekazu, na:[13]

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

Informacja z kategorią „*błyskawiczna*" przeznaczona jest dla początkowego kontaktu z przeciwnikiem lub dla komunikatów bojowych o najwyższym stopniu pilności. Z tego też względu forma informacji powinna być jak najkrótsza, co umożliwi jej szybką transmisję poprzez sieci teleinformatyczne. Zazwyczaj jest ona przekazywana w formie (postaci) z góry ustalonych kodów (sygnałów).

Kategoria „*natychmiastowa*" zarezerwowana jest dla ważnych wiadomości odnoszących się do sytuacji, które mają istotne znaczenie dla bezpieczeństwa wojsk własnych. Informacja ta, podobnie jak błyskawiczna, także jest przekazywana w postaci ustalonych wcześniej sygnałów.

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

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

Każda informacja zwiększa wiedzę odbiorcy o otaczającym świecie. Niesie ona ze sobą pewną wartość poznawczą. Wartość, która jest pojęciem samym w sobie i może ewentualnie stanowić treść rozważań filozoficznych. Niemniej jednak, z punktu widzenia każdej organizacji „konkretną wartość", jaką niesie informacja należy zamienić na pojęcie „użyteczności informacji". Inaczej mówiąc, w informacji ważne jest to w jakim stopniu jest ona przydatna i użyteczna dla adresata.

Wartość informacji zależy od czterech głównych czynników, a mianowicie:[14] jej jakości, aktualności, ilości oraz powiązania z zadaniami możliwymi do podjęcia przez kierownictwo (dowództwo).

---

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

Oceniając pierwszy z czynników - **jakość informacji** – należy porównać informację z rzeczywistością. Im informacja jest dokładniejsza (precyzyjniejsza), tym wyższa jest jej jakość i tym pewniej decydenci mogą na niej polegać przy podejmowaniu decyzji. Z punktu widzenia ekonomii, koszt pozyskania informacji rośnie wraz z jej jakością. Dla przykładu podwójne i potrójne sprawdzanie świeżo uzyskanej informacji z innymi danymi pozwala na weryfikację jej wiarygodność, lecz dodatkowy czas na to potrzebny i wykorzystane siły i środki podwyższają koszty. Potrzebny stopień dokładności będzie różny w zależności od sytuacji. W procesie dowodzenia głównym wyznacznikiem kosztu będzie czas potrzebny na zweryfikowanie informacji.

Informacja jest swoistego rodzaju „towarem", który ma swój koszt oraz odpowiednią wartość. W wyniku poniesionych nakładów otrzymujemy informację, która ma dla jej adresata określoną przydatność. Teoretycznie przydatność informacji powinna być większa niż nakład użyty dla jej uzyskania. Z tego też względu należy bardzo szczegółowo ustalić które informacje są newralgiczne w procesie dowodzenia i których koszt może być wysoki.

Wraz ze wzrostem ilości informacji rośnie także koszt ich uzyskania. Jednocześnie należy być świadomym luki informacyjnej, która powoduje podejmowanie decyzji nieoptymalnych, w warunkach ryzyka, co również związane jest z określonym kosztem. W przypadku procesu dowodzenia kosztem tym będzie niemożność osiągnięcia zamierzonego celu działania i w konsekwencji duże straty.

Następnym czynnikiem informacji, który bardzo silnie oddziałuje na jej wartość jest **aktualność informacji.** Wszelkie działania korygujące należy podejmować, zanim wystąpi znaczne odchylenie od zamierzonego planu. Informacja zatem musi być dostarczana przez system informacyjny w czasie umożliwiającym podjęcie efektywnego działania. W tym miejscu należy zwrócić uwagę na aspekt ochrony posiadanej informacji która musi być w odpowiedni sposób zabezpieczona zarówno przez jej utajnienie jak i właściwą dystrybucję.

Ilość informacji jest czynnikiem pozwalającym decydentowi podjąć sprawną decyzję. W praktyce dowódca jest często zasypywany nieistotnymi i bezużytecznymi informacjami. Z olbrzymiej ilości otrzymywanych informacji pierwotnych muszą zostać wybrane informacje użyteczne w danym czasie i danej sytuacji. Z tego też powodu w odniesieniu do każdego stanowiska dowodzenia nieodzowne jest stosowanie zasady selekcji informacji, określonej również mianem „zasada 20-80" lub zasada Pareto. Okazuje się, że tylko 20% informacji docierających do dowództwa (kierownictwa) dotyczy spraw kluczowych i w 80% przesądza o

---

[14] *Zarządzanie informacjami w procesie dowodzenia na szczeblach taktycznych wojsk lądowych z wykorzystaniem sieci teleinformatycznych...* , s. 72

wynikach działalności. Określenie puli informacji o newralgicznym znaczeniu stanowi zasadę redukcji w odniesieniu do pracy z informacjami. Redukcja informacji polega na odpowiednim określeniu wagi gatunkowej każdej informacji dla danego rodzaju decyzji oraz na rezygnowaniu z informacji nieistotnych. Redukcja polega nie tylko na odrzuceniu nieprzydatnych informacji pierwotnych, lecz także na ich scalaniu, łączeniu i uogólnianiu cząstkowych informacji użytecznych.

Ostatni czynnik - **związek informacji z zadaniami** - wynika z celowości podejmowanego działania, opartego na właściwym rodzaju i typie informacji odznaczającej się wysoką użytecznością. Informacje otrzymywane przez decydentów (dowódców) powinny być powiązane z ich obowiązkami i zadaniami. Dowódcy batalionu nie są potrzebne wszystkie informacje dowódcy dywizji i na odwrót.

Dostarczany decydentowi zbiór informacji podstawowych musi być uporządkowany według ściśle określonych kryteriów warunkujących jej przydatność. Dostarczenie decydentowi (dowódcy) szczegółowych i rzetelnych, lecz bardzo licznych i oderwanych od siebie informacji, nie pozwala na pełne ich wykorzystanie, a wręcz może uniemożliwić wykorzystanie informacji newralgicznych. Informacje muszą być tak uporządkowane, aby w pełni opisywały konkretną sytuację. Na ich podstawie decydenci mogą ustalić, co należy w zaistniałej sytuacji zrobić i jakie decyzje należy podejąć, aby osiągnąć zamierzone cele.

Informacje gromadzone w organizacji powinny być odpowiedniej jakości, tzn. obiektywne, istotne dla sprawy, dostępne w odpowiednim czasie, porównywalne, pełne, zwięzłe i cenne. Cenność informacji nie jest związana z ich liczbą ani też z pojemnością informacyjną wiadomości, lecz z jej znaczeniem dla sytuacji decyzyjnej i wagą podejmowanych dzięki nim decyzji. Cenność zależy od posiadanego przez daną organizację potencjału informacyjnego. O cenności informacji decyduje również układ odniesienia, którym jest zawsze określona sytuacja decyzyjna, a także koszt jej uzyskania.

Zawsze należy także pamiętać o tym, że informacje ulegają szybko starzeniu. Czym starsza informacja tym prawdopodobnie mniejsza jej wartość dla organizacji. Trzeba zawsze brać pod uwagę to, że w praktyce podejmowania decyzji nie uzyskuje się najczęściej pełnej i wyczerpującej, tj. kompletnej informacji. Zawsze istnieć będzie luka informacyjna, stanowiąca różnicę między informacją pełną a dostępną.

Proces decyzyjny realizowany w siłach zbrojnych rozłożony jest na wiele faz i etapów. Skuteczność tego procesu, trafność podejmowanych decyzji, będzie zależała min. od jakości

zarządzania posiadaną informacją. Zespoły realizujące proces zarządzania informacją powinny zapewnić:[15]

- dostępność informacji;
- wiarygodność informacji;
- bezpieczeństwo informacji;
- spójność informacji;
- trwałość informacji;
- aktualność informacji.

Dostępność informacji wyraża się możliwością pozyskania odpowiedniej, będącej w posiadaniu informacji przez wszystkie organa biorące udział w procesie dowodzenia w celu prawidłowej realizacji cyklu decyzyjnego. Informacja ta powinna być dostarczana tylko tym organom, które są nią zainteresowane ze względu na swoje miejsce w procesie decyzyjnym.

Wiarygodność informacji powinna być zapewniona poprzez jej odpowiednią weryfikację, zarówno przez uprawnione organa uczestniczące w procesie dowodzenia jak również przez zespół zajmujący się zarządzaniem informacją.

Bezpieczeństwo informacji polega w głównej mierze na jej odpowiednim zabezpieczeniu różnego rodzaju systemami utajniającymi, ale także poprzez odpowiedni system obiegu informacji. Konkretna informacja powinna trafiać tylko i wyłącznie do organów które jej potrzebują.

Niezmiernie istotnym wyznacznikiem jest spójność informacji. Jej zapewnienie polega na jednolitej świadomości informacyjnej wszystkich organów dowodzenia, co wyraża się potrzebą dostarczania tej samej informacji do wszystkich zainteresowanych. Należy unikać sytuacji, w której jeden z organów procesu dowodzenia posiada najnowsze informacje na konkretny temat, natomiast inne organy bazują na informacji przestarzałej.

Trwałość informacji wyraża się potrzebą jej zachowania w niezmienionej postaci przez dłuższy okres czasu. Jest to uwarunkowane nie tylko potrzebami procesu decyzyjnego ale także odpowiednimi przepisami prawnymi. Z tego względu struktura organizacyjna zespołu zarządzającego informacjami powinna uwzględniać potrzebą przechowywania posiadanej informacji w kilku miejscach, co powinno uchronić ją przed całkowitą utratą.

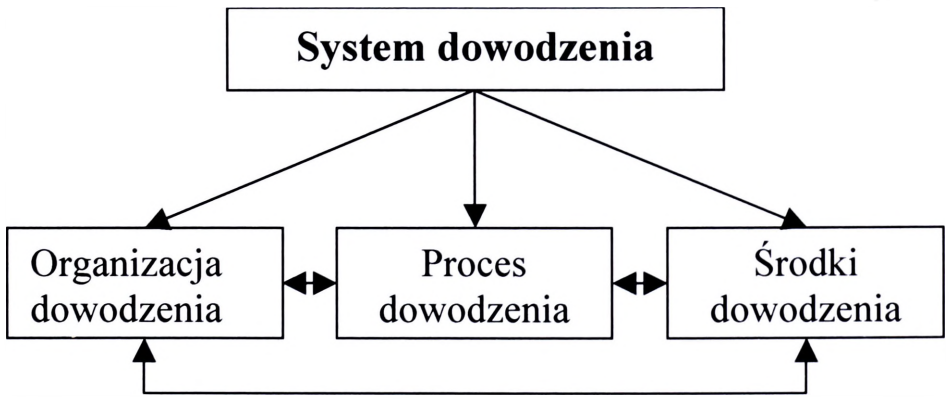
---

[15] P. Dela, *Wybrane uwarunkowania funkcjonowania sieci teleinformatycznych*, referat na Konferencji Automatyzacja Dowodzenia, Serock 2008

Aktualność informacji polega na stałym uaktualnianiu posiadanej bazy danych z informacjami i dostarczaniu odpowiednim organom dowodzenia tylko i wyłącznie najświeższej informacji.

2.3. Organizacyjne uwarunkowania informacji

Przeprowadzone badania wykazały, że ilość, postać oraz rodzaj informacji jest nierozerwalnie związana z systemem dowodzenie stworzonym na potrzeby realizowanych zadań. W literaturze przedmiotu[16] dowodzenie postrzegane jest jako złożony proces informacyjno-zasileniowy, w którym dowódca narzuca swoją wolę i zamiary podwładnym oraz w ramach którego wspomagany przez swój sztab planuje, organizuje, koordynuje i ukierunkowuje działania podległych mu wojsk przez użycie standardowych procedur działania i wszelkich dostępnych środków przekazywania informacji. Aby proces ten mógł sprawnie przebiegać, jego poszczególne elementy personalne, techniczne i organizacyjne wzajemnie zależne, powinny być odpowiednio zaprojektowane i zorganizowane w system dowodzenia, w którym celowe i skoordynowane działanie tych elementów umożliwia skuteczne dowodzenie. W systemie dowodzenia wyszczególnione powyżej elementy najczęściej grupuje się w trzy wzajemnie wpływające na siebie zasadnicze grupy, które zostały przedstawione na rysunku 2.1.



Rys.2.1. Podstawowe elementy systemu dowodzenia
Źródło: *J. Kręcikij, J. Wołejszo, Podstawy dowodzenia, Warszawa, AON 2007, s. 61*

Badania wykazały, że zarówno organizacja dowodzenia, proces dowodzenia jak i środki dowodzenia są ze sobą połączone sprzężeniami zwrotnymi. Oznacza to, że zmiany zachodzące w którymkolwiek z elementów systemu wywierają wpływ na pozostałe elementy systemu dowodzenia. Efektem takiego powiązania jest np. teoria walki w środowisku sieciocentrycznym jako reakcja na wzrost możliwości i znaczenia sieci teleinformatycznych i tech-

[16] J. Kręcikij, J. Wołejszo i inni, *Podstawy Dowodzenia*, AON, Warszawa 2007

nologii przetwarzania danych. Nowe środki dowodzenia implikują nową organizację dowodzenia i wymuszają zmiany w procesie dowodzenia. Z drugiej strony rozwój teorii organizacji wymusza często poszukiwania nowych rozwiązań techniczno-technologicznych i organizacyjnych możliwych do wykorzystania w praktyce.

Analizując pierwszy z elementów systemu dowodzenia - **organizacja dowodzenia** – można zauważyć, że składa się z następujących elementów:

1. Ogólnych zasad działania (doktryna).
2. Sposobu zorganizowania dowództw.
3. Uprawnień i odpowiedzialności dowództw.
4. Podziału struktury funkcjonalnej dowództw na stanowiskach dowodzenia.
5. Relacji pomiędzy dowództwami.

Pod względem organizacyjnym system dowodzenia, tak jak każdy system kierowania, stanowi zbiór określonych relacji sprzężonych ze sobą informacyjnie lub technicznie, niezależnie od hierarchicznego poziomu (szczebla) dowodzenia. Jest więc on zbiorem określonych **środków dowodzenia**[17] oraz zabezpieczających (obsługujących) ich ludzi powiązanych ze sobą, odpowiednio do struktury organizacyjnej oraz decyzji dowódcy podejmowanych w ramach wykonywania funkcji dowodzenia.

Ważnym elementem w systemie dowodzenia są stanowiska dowodzenia, które stanowią centra kierowania działaniami. Są one powiązane ze sobą funkcjonalnie i informacyjnie w określonym układzie poziomym i pionowym.

Analizując[18] istniejące w literaturze przedmiotu i dokumentach normatywnych zapisy dotyczące stanowisk dowodzenia należy stwierdzić, że są one zróżnicowane. Dlatego na potrzeby dalszych rozważań autor przyjął następującą definicję określającą stanowisko dowodzenia jako „*powiązane organizacyjnie i funkcjonalnie elementy koncepcyjne (organa dowodzenia) i zabezpieczające (oddziały i pododdziały dowodzenia) rozmieszczone w określonych miejscach (obiektach) w celu zapewnienia sprawnego dowodzenia*".[19]

---

[17] Środki dowodzenia to zasoby techniczne i materiałowe wydzielone do działania w systemie dowodzenia zorganizowane jako: stanowiska dowodzenia; sieci teleinformatyczne, pocztowe, sygnalizacyjne, itp.

[18] J. Michniak, *Dowodzenie w teorii i praktyce wojsk*, AON, Warszawa 2003; J. Michniak, *Dowodzenie i łączność,* AON, Warszawa 2005, s. 53; J. Kręcikij, J. Wołejszo i inni, *Podstawy dowodzenia*, AON, Warszawa 2007, s. 214; J. Kręcikij, J. Wołejszo i inni, *Podręcznik dowódcy batalionu*, AON, Warszawa 2007, s. 51; *Regulamin działań wojsk lądowych*, DWLąd 115/2008, s. 281.

[19] N. Prusiński, M. Strzoda, *System dowodzenia. Terminologia*, AON, Warszawa 2001, s. 87.

Podobna różnorodność występuje w stosunku do klasyfikacji stanowisk dowodzenia występujących w wojskach lądowych. Jednym z kryteriów klasyfikacji jest kryterium czasu pracy SD wg, którego powinno się organizować następujące rodzaje stanowisk dowodzenia[20]:

- *stale funkcjonujące*: główne stanowiska dowodzenia (GSD), zapasowe stanowiska dowodzenia (ZSD), tyłowe stanowiska dowodzenia (TSD),
- *doraźnie funkcjonujące*: wysunięte stanowiska dowodzenia (WSD), punkty dowódczo-obserwacyjnych (PDO) i powietrzne punkty dowodzenia (PPD) – wydzielane z GSD.

Ilość, rodzaj i struktura wewnętrzna stanowisk dowodzenia uzależniona jest od zadania, składu sił, czy też poziomu dowodzenia na którym jest ono rozwijane. Zdaniem profesora Józefa Michniaka na szczeblu komponentu lądowego powinny być organizowane następujące rodzaje stanowisk dowodzenia[21]:

- Główne stanowisko dowodzenia (GSD);
- Tyłowe stanowisko dowodzenia (TSD);
- Zapasowe stanowisko dowodzenia (ZSD);
- Wysunięte stanowisko dowodzenia (WSD);
- Powietrzny punkt dowodzenia (PPD) – element składowy GSD.

Główne stanowiska dowodzenia[22] (GSD) na wszystkich szczeblach dowodzenia wojsk lądowych przeznaczone są do planowania działań taktycznych oraz do bezpośredniego dowodzenia wojskami. Stanowią one miejsca pracy dowódcy i sztabu. Praca na nich prowadzona jest w systemie dwuzmianowym. GSD powinno zapewniać:

- łączność dowodzenia ze wszystkimi elementami ugrupowania taktycznego oraz z wy suniętym stanowiskiem dowodzenia i powietrznym punktem dowodzenia;
- łączność z przełożonym i sąsiadami;
- ciągłe przygotowywanie informacji potrzebnych dowódcy do oceny sytuacji i podejmowania decyzji;
- przygotowywanie planów i rozkazów;
- koordynację prowadzenia rozpoznania i analizę informacji rozpoznawczych ze wszelkich dostępnych źródeł;
- koordynację wsparcia ogniowego;
- koordynację potrzeb zabezpieczenia logistycznego;

---

[20] J. Kręcikij, J. Wołejszo i inni, *Podstawy dowodzenia* ..., s. 215.
[21] J.W. Michniak, *Stanowiska dowodzenia w wojskach lądowych,* AON Warszawa 2003, s. 18-19; J. Michniak, *Zarządzanie w sztabach wojskowych*, AON, Warszawa 2008, s. 105
[22] J. Kręcikij, J. Wołejszo i inni, *Podstawy dowodzenia* ..., s. 215; J. Michniak, *Dowodzenie i łączność*..., s. 69; J. Michniak, *Zarządzanie w sztabie wojskowym* ... , s. 105.

- przygotowywanie i przesyłanie meldunków do przełożonego;
- dowodzenie wojskami i sterowanie środkami rażenia w toku działań (walki, operacji);
- kontrolę nad realizacją zadań;
- planowanie kolejnych (przyszłych) działań taktycznych.

Zapasowe stanowiska dowodzenia (ZSD)[23] organizowane są w celu zapewnienia ciągłości i trwałości dowodzenia wojskami oraz przejęcia dowodzenia w wypadku obezwładnienia głównego stanowiska dowodzenia (GSD). Zapasowe stanowiska dowodzenia pozostają w ukryciu (nie realizują zadań) gdy dowodzenie odbywa się z GSD. Zajmują się głównie kontrolowaniem rozwoju sytuacji i uaktualnianiem informacji przetwarzanej na głównym stanowisku dowodzenia (GSD). Struktura organizacyjna ZSD nie jest określona, ale powinna zapewnić realizację powyższych zadań. O wielkości obsady operacyjnej decyduje dowódca danego szczebla dowodzenia.

Tyłowe stanowiska dowodzenia (TSD)[24] organizowane są w celu zapewnienia realizacji funkcji dowodzenia w obszarze tyłowym oraz w sytuacji, gdy nie jest organizowane ZSD w celu podtrzymania zasadniczych funkcji dowodzenia w wypadku obezwładnienia głównego stanowiska dowodzenia (GSD). Zajmują się one głównie koordynacją wsparcia personalnego i zabezpieczenia logistycznego, kontrolowaniem rozwoju sytuacji w obszarze sił głównych, pozyskiwaniem dokumentów dowodzenia opracowywanych na głównym stanowisku dowodzenia (GSD) oraz realizacją planu działania w obszarze tyłowym. Struktura organizacyjna tyłowego stanowiska dowodzenia (TSD) powinna umożliwić realizację powyższych zadań.

Wysunięte stanowiska dowodzenia (WSD)[25] rozwijane są czasowo, stosownie do istniejących potrzeb, w celu zapewnienia dowódcy bezpośredniego wglądu w aktualną sytuację i skrócenia do minimum czasu reakcji w relacjach dowodzenia z podległymi wojskami w decydujących fazach operacji (walki). Obsada operacyjna tych stanowisk wydzielana jest z GSD w zależności od potrzeb dowodzenia i decyzji dowódcy. Powinny one zapewnić:

- kontrolę nad prowadzonymi działaniami bojowymi,
- kontrolę i koordynację manewru i wsparcia ogniowego,
- koordynację wsparcia powietrznego i obrony przeciwlotniczej,
- przekazywanie potrzeb zabezpieczenia logistycznego do głównego SD,

---

[23] J. Kręcikij, J. Wołejszo i inni, *Podstawy dowodzenia* ..., s. 216; J. Michniak, *Dowodzenie i łączność*..., s. 73; J. Michniak, *Zarządzanie w sztabie wojskowym*..., s. 113

[24] J. Kręcikij, J. Wołejszo i inni, *Podstawy dowodzenia*..., s. 216; J. Michniak, *Dowodzenie i łączność*..., s. 74; J. Michniak, *Zarządzanie w sztabie wojskowym*..., s. 114.

[25] J. Kręcikij, J. Wołejszo i inni, *Podstawy dowodzenia*..., s. 216; J. Michniak, *Dowodzenie i łączność*..., s. 76; J. Michniak, *Zarządzanie w sztabie wojskowym* ..., s. 112

– możliwość szybkiej zmiany rejonu rozmieszczenia stanowiska,
– ciągłą łączność z podległymi wojskami, głównym, zapasowym i tyłowym SD oraz z przełożonym i sąsiadami.

Punkt dowódczo-obserwacyjny (PDO)[26] organizuje się na szczeblu brygady, pułku, batalionu (dywizjonu) w celu zapewnienia dowódcy bezpośredniego wglądu w sytuację oraz skrócenia czasu reakcji w relacjach dowodzenia podległymi pododdziałami (elementami ugrupowania).

Powietrzne punkty dowodzenia (PPD)[27] stanowią element składowy głównego stanowiska dowodzenia i wykorzystywane są do zapewnienia dowodzenia w czasie przemieszczania się dowódcy, przegrupowania związków operacyjnych i taktycznych, wyprowadzania wojsk z rejonów zmasowanych uderzeń przeciwnika itp.

Przeprowadzone analizy[28] literatury uprawniają do stwierdzenia, że w wojskach lądowych przyjmuje się tworzenie i funkcjonowanie następujących typów stanowisk dowodzenia:

– *stacjonarne,*
– *stacjonarno-mobilne,*
– *mobilno-stacjonarne,*
– *mobilne (aeromobilne).*

Stacjonarne stanowisko dowodzenia jest rozmieszczane w wybranych i przygotowanych obiektach, a infrastruktura stacjonarna zabezpiecza miejsca pracy dla całej obsady operacyjnej stanowiska dowodzenia i w pełni zaspokaja potrzeby dowodzenia, współdziałania oraz powiadamiania w zakresie wymiany informacji.

Stacjonarno-mobilne stanowisko dowodzenia jest rozmieszczane w wybranych i przygotowanych obiektach, które zabezpieczają miejsca pracy dla jednej zmiany obsady operacyjnej a mobilne środki dowodzenia uzupełniają tylko doraźne potrzeby.

Mobilno-stacjonarne stanowiska dowodzenia mogą być rozmieszczane w obiektach, które nie pokrywają potrzeb w zakresie sieci teleinformatycznych, a mobilne środki teleinformatyczne stanowią główną bazę w zakresie zaspokojenia potrzeb dowodzenia na usługi teleinformatyczne.

---

[26] J. Kręcikij, J. Wołejszo i inni, *Podstawy dowodzenia*..., s. 215; J. Michniak, *Dowodzenie i łączność*..., s. 69; J. Michniak, *Zarządzanie w sztabie wojskowym*..., s. 113.
[27] J. Kręcikij, J. Wołejszo i inni, *Podstawy dowodzenia*..., s. 217; J. Michniak, *Dowodzenie i łączność*..., s. 73; J. Michniak, *Zarządzanie w sztabie wojskowym*..., s. 113.
[28] J.W. Michniak, *Stanowiska dowodzenia w wojskach lądowych*...; J. Kręcikij, J. Wołejszo i inni, *Podstawy dowodzenia*...; J. Michniak, *Zarządzanie w sztabie wojskowym*..., s. 113

Mobilne (aeromobilne) stanowiska dowodzenia są z kolei przygotowane do rozmieszczenia w każdych warunkach i rejonach, a praca operatorów na SD prowadzona byłaby na środkach mobilnych lub aeromobilnych, autonomicznych pod względem usług teleinformatycznych.

Inny podział i klasyfikację stanowisk dowodzenia zastosowano w najnowszym *Regulaminie działań wojsk lądowych*, gdzie wyróżniono[29]:

- Stanowiska dowodzenia – SD;
- Alternatywne stanowiska dowodzenia – Alter. SD;
- Wysunięte stanowiska dowodzenia – WSD;
- Punkty dowódczo-obserwacyjne;
- Powietrzne elementy dowodzenia.

Według obowiązujących regulaminów stanowisko dowodzenia (SD) powinno zapewnić realizację funkcji dowodzenia na wszystkich poziomach dowodzenia oraz umożliwić dowodzenie wojskami. Stanowi ono zasadnicze miejsce pracy dla dowództwa danego poziomu dowodzenia.

Alternatywne stanowisko dowodzenia jest organizowane w celu zapewnienia ciągłości i trwałości dowodzenia wojskami oraz przejęcia dowodzenia w przypadku obezwładnienia stanowiska dowodzenia (SD). Stanowisko to zajmuje się głównie monitorowaniem rozwoju sytuacji oraz pozyskiwaniem, gromadzeniem, analizowaniem i przechowywaniem dokumentów dowodzenia opracowanych na SD. Struktura organizacyjna Alter. SD jest taka sama jak SD, a o jego obsadzie personalnej decyduje dowódca.

Wysunięte Stanowisko Dowodzenia (WSD) jest rozwijane czasowo, w zależności od potrzeb, celem zapewnienia dowódcy dowodzenia podległymi wojskami w decydujących fazach walki. Obsada operacyjna WSD wydzielana jest doraźnie ze składu SD.

Punkt Dowódczo-Obserwacyjny (PD-O) to element organizowany doraźnie w jednostkach poziomu taktycznego, w celu zapewnienia dowódcy możliwości bezpośredniego wglądu w teren i dowodzenie na kierunkach, gdzie realizowane są najważniejsze zadania bojowe. PD-O wydziela się ze składu SD.

Ostatnim elementem wymienionym w *Regulaminie działań wojsk lądowych* jest powietrzny element dowodzenia, organizowany doraźnie, w przypadku posiadania odpowiednich sił i środków, w celu zapewnienia dowodzenia w czasie przemieszczania się dowódcy,

---

[29] *Regulamin działań wojsk lądowych*, DWLąd 115/2008, s. 281.

przegrupowania (przemieszczania) wojsk oraz wyprowadzania wojsk z rejonów zmasowanych uderzeń przeciwnika, itp.

Dodatkowo w *Regulaminie* wymieniono cztery rodzaje stanowisk dowodzenia[30], uwzględniające ich stopień mobilności, a mianowicie: stacjonarne, stacjonarno-mobilne, mobilno-stacjonarne i mobilne.

Według najnowszej instrukcji organizacji i funkcjonowania Wojennego Systemu Dowodzenia w Wojskach Lądowych organizowane są stanowiska dowodzenia przedstawione w tabeli 2.1.

Tabela 2.1.

System stanowisk dowodzenia w Siłach Zbrojnych RP

Szczebel dowodzenia	**Rodzaje stanowisk dowodzenia**			
	SD	**Alter.SD**	**WSD**	**PD-O**
Dywizja	X	X	X	X
Brygada	X	X		X
Pułk	X			X
Batalion	X			X
Kompania				X

Źródło: Opracowano na podstawie *Instrukcja organizacji i funkcjonowania wojennego systemu dowodzenia Siłami Zbrojnymi RP*, Sztab Generalny WP, Warszawa 2008

Analizując strukturę wewnętrzna stanowiska dowodzenia należy zauważyć, że występują tam określone komponenty takie jak[31]:

- Organa dowodzenia –zespoły funkcjonalne odpowiadające odpowiednim obszarom problemowym dowodzenia. W zależności od szczebla i przeznaczenia stanowiska dowodzenia jego strukturę wewnętrzną tworzą elementy funkcjonalne wydzielane z jednej lub kilku komórek organizacyjnych dowództwa;
- Węzeł telekomunikacyjny i siły poczty polowej – zapewniający przepływ informacji w ramach wewnętrznych i zewnętrznych więzi informacyjnych [32];

[30] *Regulamin działań wojsk lądowych*, DWLąd 115/2008, s. 283.
[31] J. Wołejszo, *Więzi informacyjne stanowisk dowodzenia szczebla taktycznego wojsk lądowych*, materiały z konferencji *Sieci teleinformatyczne stanowisk dowodzenia szczebla taktycznego wojsk lądowych*, AON, Warszawa 2006, s. 150; J. Kręcikij, J. Wołejszo i inni, *Podstawy dowodzenia*…., s. 220; J. Michniak, *Dowodzenie i łączność*…, s. 65.
[32] W *Regulaminie działań wojsk lądowych* zamiast węzła telekomunikacyjnego wymieniono węzeł łączności stanowiska dowodzenia – *Regulamin działań wojsk lądowych*, DWLąd 115/2008, s. 283

- Grupa zabezpieczenia – organizowana w celu zabezpieczenia bojowego i logistycznego SD;
- Lądowisko dla śmigłowców.

Liczba komórek organizacyjnych stanowisk dowodzenia oraz wielkość obsady personalnej są uzależnione od wielu czynników, m. in.:[33]

- zadań, jakie ma realizować dany zespół stanowiska dowodzenia,
- stopnia przygotowania personelu i wyposażenia w techniczne środki dowodzenia,
- wymagań wynikających z organizacji rozmieszczenia i pracy stanowisk dowodzenia,
- potrzeby zapewnienia ciągłości pracy podczas 24 godzin z uwzględnieniem systemu dwuzmianowego,
- wytycznych dowódcy i szefa sztabu.

W zależności od poziomu dowodzenia i przeznaczenia stanowiska dowodzenia jego strukturę wewnętrzną (*części operacyjnej)* tworzą elementy funkcjonalne, które są wydzielane z jednej lub kilku komórek organizacyjnych dowództwa połączone odpowiednio w: centra, zespoły, sekcje i grupy. Analiza literatury dowiodła dużej rozbieżności poglądów, na temat zasadniczych komponentów tych części stanowiska dowodzenia.

Z uwagi na przeznaczenie stanowiska dowodzenia, jego część operacyjną stanowią najczęściej elementy funkcjonalne wydzielane z jednej lub kilku komórek organizacyjnych dowództwa. Tworzą one cztery zespoły funkcjonalne będące zasadniczymi komponentami części operacyjnej stanowiska dowodzenia, to jest odpowiednio:[34]

- zespół dowodzenia;
- zespół wsparcia dowodzenia;
- zespół wsparcia działań;
- zespól zabezpieczenia działań.

Zespół dowodzenia – pełni funkcję planistyczną w zakresie prowadzonych działań. Koordynuje działania powstałych komponentów SD, określa potrzeby informacyjne lub dane niezbędne do powzięcia decyzji przez dowódcę;

Zespół wsparcia dowodzenia –pełni funkcję wsparcia procesu dowodzenia w różnych relacjach i obszarach. Organizuje, zabezpiecza i nadzoruje przepływ i bezpieczeństwo

---

[33] Porównaj: J. Wołejszo, *Więzi informacyjne stanowisk dowodzenia szczebla taktycznego wojsk lądowych*, materiały z konferencji *Sieci teleinformatyczne stanowisk dowodzenia szczebla taktycznego wojsk lądowych…*

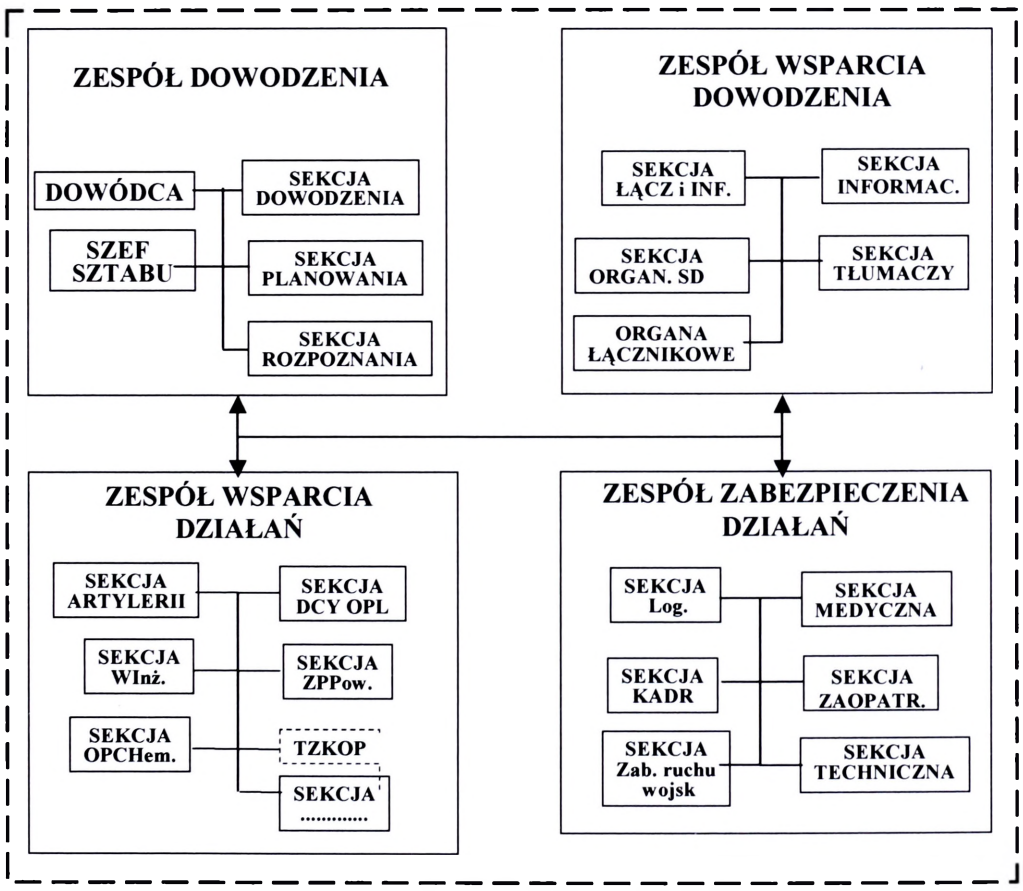
[34] W dokumentach normatywnych często podkreśla się, że szczegółowe struktury organizacyjno-funkcjonalne stanowisk dowodzenia każdorazowo określają dowódcy danego szczebla

informacji pomiędzy poszczególnymi elementami SD oraz pomiędzy innymi SD i elementami ugrupowania bojowego.

Zespół wsparcia działań – pełni funkcję koordynatora wsparcia ogniowego i lotniczego na potrzeby wojsk zmechanizowanych i pancernych. Planuje użycie sił lotnictwa wojsk lądowych i innych specjalistycznych zgrupowań w wymiarze lądowo-powietrznym. Koordynuje działanie innych rodzajów wojsk na rzecz sił głównych.

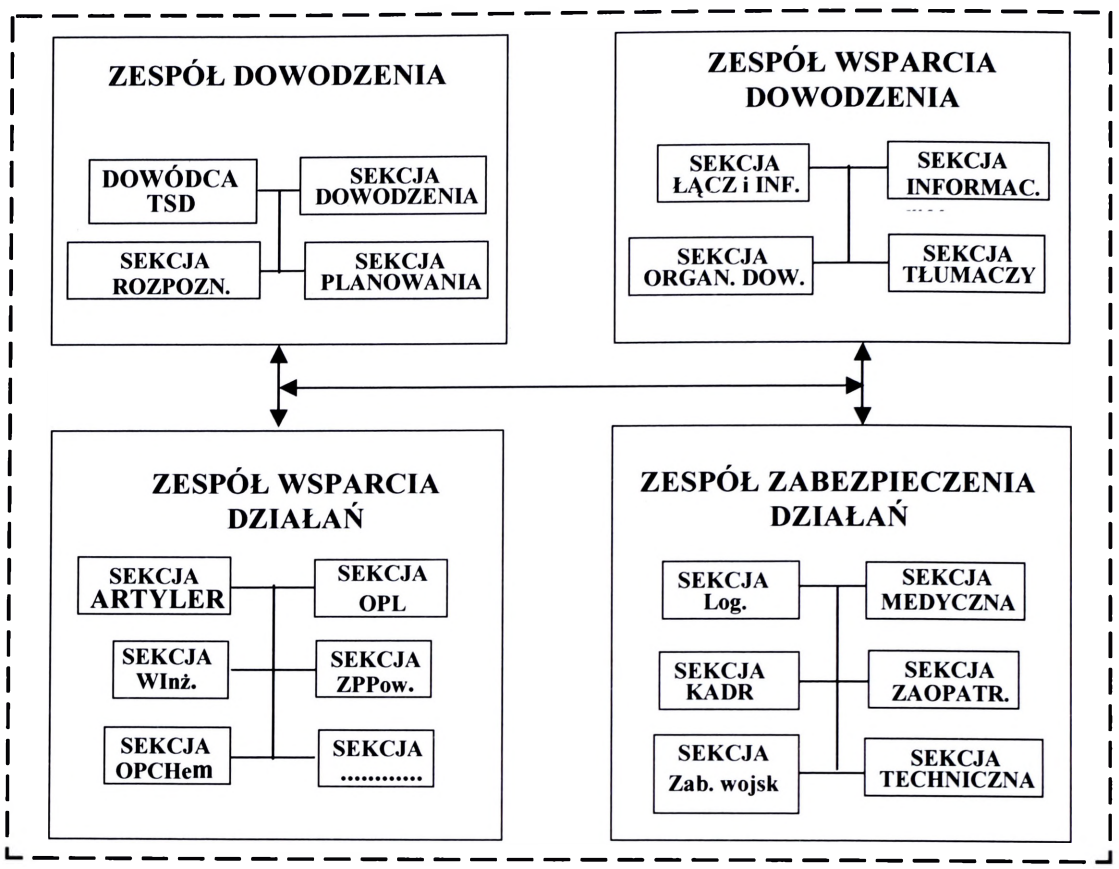
Zespół zabezpieczenia działań – realizuje funkcje planistyczno-koordynujące zabezpieczenia logistycznego wojsk lądowych oraz administratora zasobów działalności personalnej i wsparcia dowodzenia wewnętrznego.

Przedstawione rozwiązanie (patrz rysunek 2.2. i 2.3.), przyjmowane są z reguły jako modelowe – w którym struktura części operacyjnej stanowiska dowodzenia (GSD) i tyłowego stanowiska dowodzenia (TSD) składa się z czterech podstawowych zespołów oraz wchodzących w ich skład sekcji.



Rys. 2.2. Część operacyjna GSD związku taktycznego (oddziału) - w*ariant*

Źródło: J. Wołejszo, Więzi informacyjne stanowisk dowodzenia szczebla taktycznego wojsk lądowych, materiały z konferencji Sieci teleinformatyczne stanowisk dowodzenia szczebla taktycznego wojsk lądowych, AON, Warszawa 2006



Rys. 2.3. Część operacyjna TSD związku taktycznego (oddziału) - w*ariant*

Źródło: J. Wołejszo, Więzi informacyjne stanowisk dowodzenia szczebla taktycznego wojsk lądowych, materiały z konferencji Sieci teleinformatyczne stanowisk dowodzenia szczebla taktycznego wojsk lądowych, AON, Warszawa 2006

Analiza wyników badań naukowych realizowanych w AON w zakresie doskonalenia struktur stanowisk dowodzenia wykazała, że zostały wyodrębnione dwa warianty struktury części operacyjnej stanowiska dowodzenia.[35]

W **wariancie pierwszym** różnica w strukturze dotyczy rozmieszczenia zespołów wsparcia i zabezpieczenia działań, które nie występują w strukturze GSD. Przedstawiciele tych zespołów znajdują się w sekcji planowania i dowodzenia zespołu dowodzenia na TSD. Struktura części operacyjnej TSD składa się z 2 zespołów funkcjonalnych, dowódcy TSD oraz zespołu kontroli rejonu tyłowego, ze specjalistami z S/G 3/2 dowództwa oraz sekcja łączności i sekcję informacyjną.

W **wariancie drugim** struktura części operacyjnej stanowiska dowodzenia (GSD) i tyłowego stanowiska dowodzenia (TSD) składa się z dwóch podstawowych zespołów funkcjonalnych (dowodzenia i planowania) oraz wchodzących w ich skład sekcji, uzupełnionych odpowiednio poszczególnymi specjalistami. Struktura części operacyjnej TSD podobna do wariantu pierwszego.

---

[35] Porównaj: J. Wołejszo, *Więzi informacyjne stanowisk dowodzenia szczebla taktycznego wojsk lądowych*, materiały z konferencji *Sieci teleinformatyczne stanowisk dowodzenia szczebla taktycznego wojsk lądowych*...; J. Michniak, *Zarządzanie w sztabie wojskowym*..., s. 103

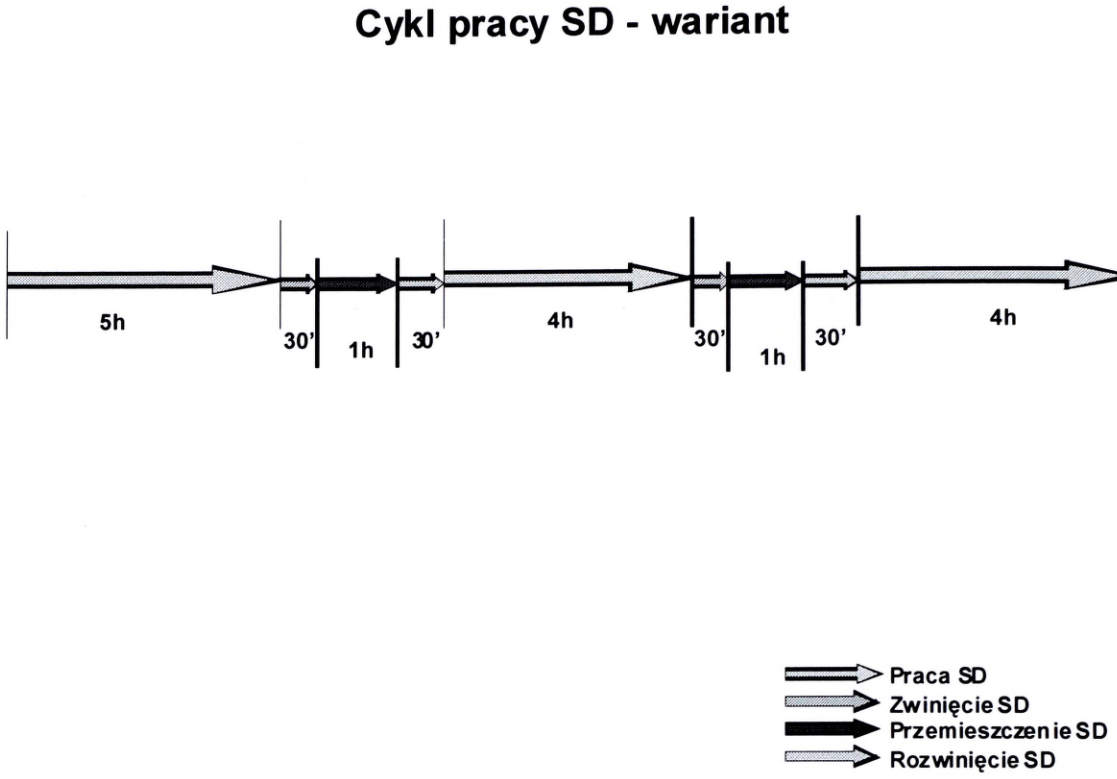
Nowa instrukcja WSyD wprowadza na poziomie taktycznym podział komórek organizacyjnych stanowiska dowodzenia na : zespoły, grupy i sekcje. Organ dowodzenia składa się z następujących zespołów:

- zespół planowania;
- zespół dowodzenia;
- zespół rozpoznania;
- zespół wsparcia.

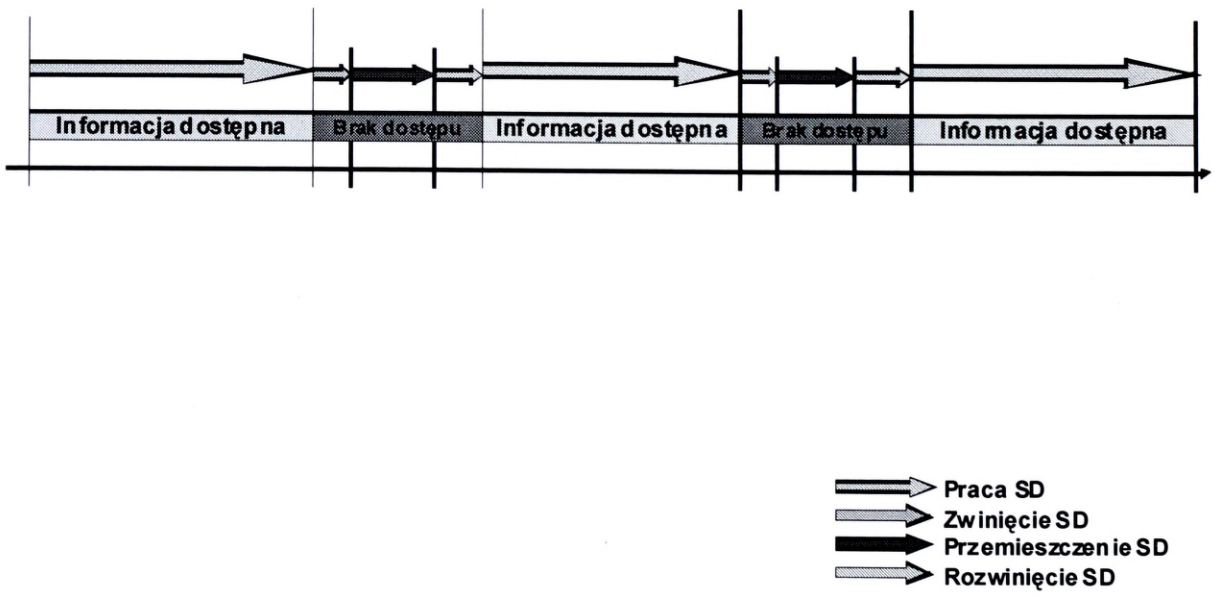
Szczegółową strukturę organizacyjną stanowisk dowodzenia, zadania i skład poszczególnych zespołów (na podstawie instrukcji WSyD) określa dowódca, uwzględniając specyfikę działań, sytuację operacyjno-taktyczną i możliwości współdziałania w systemie sojuszniczym.

Stanowiska dowodzenia powinny być rozwijane w miejscach umożliwiających niezawodną wymianę informacji pomiędzy dowództwem a podległymi wojskami przy wykorzystaniu posiadanych środków łączności. Z drugiej jednak strony zasada zachowania żywotności wymusza potrzebę dyslokacji stanowisk dowodzenia, tak aby zminimalizować możliwość porażenia przez przeciwnika. Wraz ze wzrostem czasu w jakim jest rozwinięte stanowisko dowodzenia rośnie prawdopodobieństwo jego wykrycia przeciwnika. Dyslokacja stanowisk dowodzenia podyktowana jest także zmieniającą się sytuacją operacyjno-taktyczną i potrzebą zachowania ciągłości dowodzenia.

Istotnym uwarunkowaniem wpływającym na dostęp do informacji na stanowisku dowodzenia jest to, w jakim stopniu stanowisko dowodzenia zostało rozwinięte. Na rysunku 2.4. przedstawiono wariant pracy stanowiska dowodzenia wojsk lądowych na szczeblu taktycznym. Informacja przechowywana na głównym stanowisku dowodzenia w ramach systemów wspomagających dowodzenia nie będzie dostępna przez cały czas ale tylko wtedy, gdy nastąpi pełne rozwinięcie stanowiska dowodzenia (rysunek 2.5).



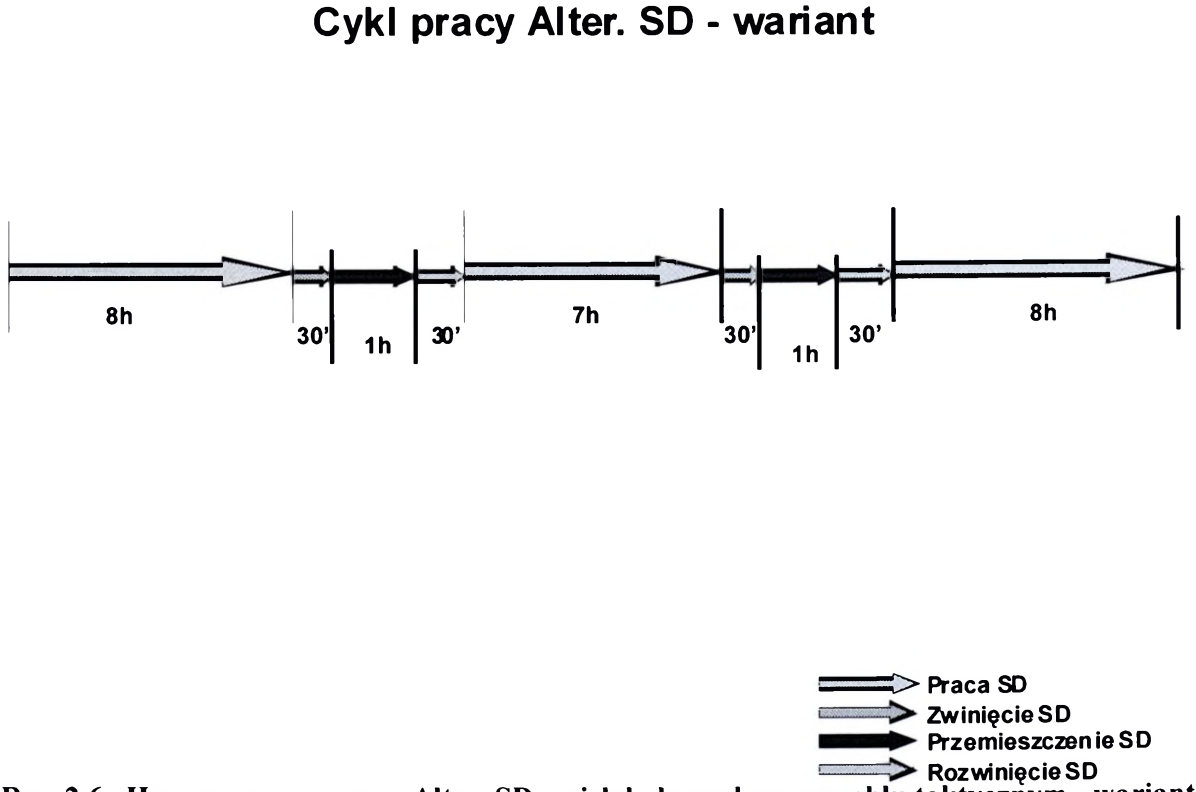
Rys. 2.4. Harmonogram pracy SD wojsk lądowych na szczeblu taktycznym - wariant
Źródło: P. Dela, Domeny informacyjne – nowe podejście do zarządzania informacją, referat na konferencji Wsparcie teleinformatyczne dowództw w działaniach wojsk lądowych, AON, Warszawa 2008



Rys. 2.5. Dostęp do informacji na SD wojsk lądowych - wariant
Źródło: P. Dela, Domeny informacyjne – nowe podejście do zarządzania informacją, referat na konferencji Wsparcie teleinformatyczne dowództw w działaniach wojsk lądowych, AON, Warszawa 2008

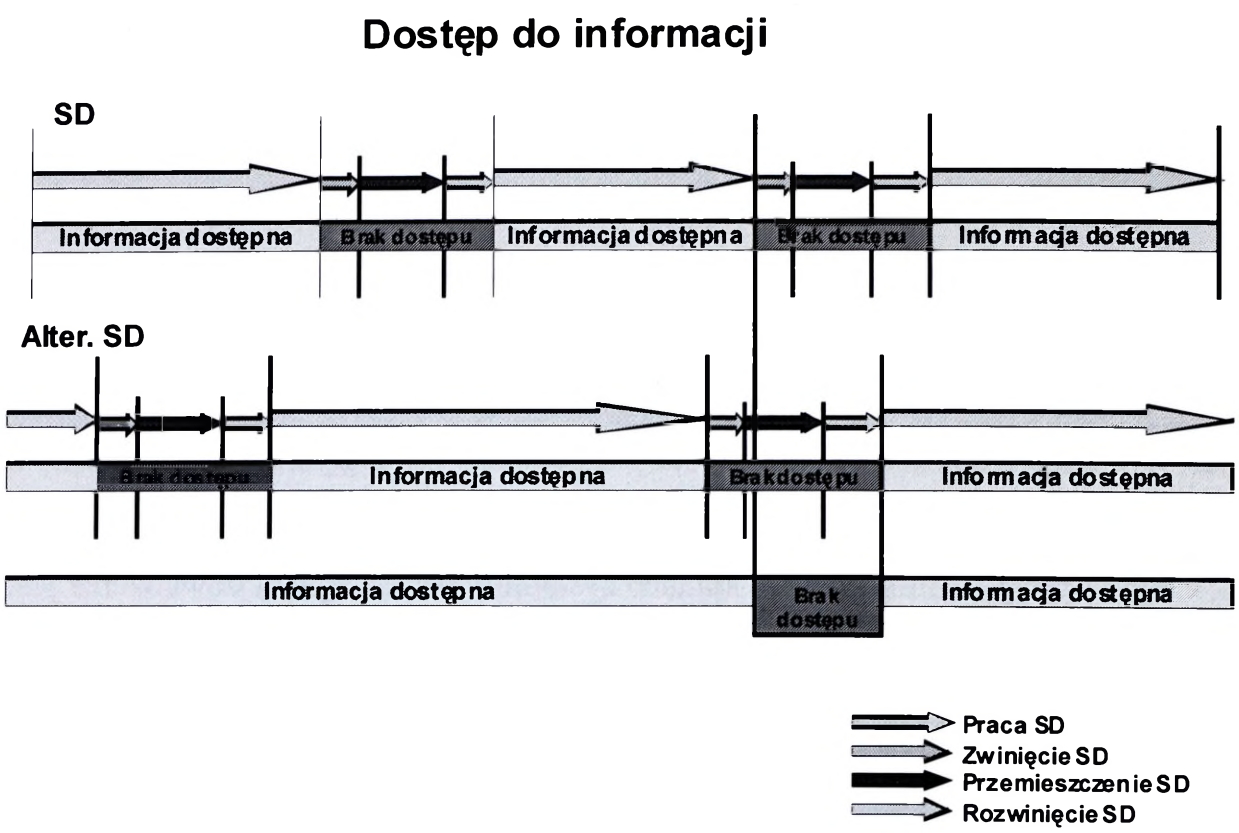
Przyjęty w Wojsku Polskim system dowodzenia przewiduje organizowanie alternatywnych stanowisk dowodzenia. Stanowiska te powinny być zdolne do przejęcia roli SD w przypadku jego porażenia. Z tego względu na Alter. SD powinna znajdować się taka sama informacja jak na SD. Rola i znaczenie Alter. SD wymusza potrzebą zmiany jego dyslokacja w miarę zmieniającej się sytuacji taktyczno-operacyjnej. Dyslokacja Alter. SD powinna sprzyjać wymianie informacji pomiędzy dowództwem a podległymi wojskami oraz zapewniać jego żywotność. Na rysunku 2.6. przedstawiono wariant pracy Alter. SD.

Ciągły dostęp do informacji w ramach systemów wspomagania dowodzenia jest możliwy tylko wtedy, gdy stanowiska dowodzenia SD i Alter. SD będą przemieszczane na zmianę, tak aby w danym czasie jedno z nich posiadało pełną funkcjonalność. Istnieje jednak prawdopodobieństwo, że oba stanowiska dowodzenia nie będą w pełni rozwinięte a tym samym dostęp do informacji zostanie zakłócony. Na rysunku 2.7. przedstawiono hipotetyczną możliwość braku dostępu do informacji na danym szczeblu dowodzenia.



Rys. 2.6. Harmonogram pracy Alter. SD wojsk lądowych na szczeblu taktycznym - wariant

Źródło: P. Dela, Domeny informacyjne – nowe podejście do zarządzania informacją, referat na konferencji Wsparcie teleinformatyczne dowództw w działaniach wojsk lądowych, AON, Warszawa 2008



Rys.2.7. Dostęp do informacji na SD i Alter. SD wojsk lądowych na szczeblu taktycznym w ramach systemów wspomagania dowodzenia - wariant

Źródło: P. Dela, Domeny informacyjne – nowe podejście do zarządzania informacją, referat na konferencji Wsparcie teleinformatyczne dowództw w działaniach wojsk lądowych, AON, Warszawa 2008

Pomimo możliwości wystąpienie problemów z dostępem do informacji na stanowiskach dowodzenia należy pamiętać o tym, że przez cały czas dyslokacji stanowisk dowodzenia funkcjonują sieci radiowe. Zapewniają one dowódcy ciągłość dowodzenia, jednakże z powodu ograniczonych możliwości transmisji danych w ramach sieci radiowych, dowodzenie będzie odbywało się głównie „fonem". W tym przypadku uaktualnienie sytuacji będzie się odbywało się z dużym opóźnieniem, co wpłynie na szybkość przetwarzania posiadanych informacji.

Następny element systemu dowodzenia - **proces dowodzenia**[36] - postrzegany jest jako proces informacyjno-decyzyjny realizowany przez dowództwa. Polega na cyklicznym zbieraniu i opracowywaniu informacji oraz przetwarzaniu ich w decyzje, które w postaci zadania doprowadza się do wykonawców. Z kolei wykonawczy składają meldunki o sposobach i terminach wykonania tych decyzji. W procesie dowodzenia odbywa się ciągła wymiana informacji. Istotną rolę w procesie dowodzenia odgrywają więc więzi informacyjne.

Zasadniczym uwarunkowaniem powodzenia w działaniach taktycznych wojsk lądowych jest koordynacja i synchronizacja działalności dowództw, która charakteryzuje się

[36] J. Kręcikij, J. Wołejszo i inni, *Podstawy dowodzenia...*, s. 87

szybką wymianą informacji (w czasie zbliżonym do rzeczywistego). Warunek ten może być spełniony tylko w przypadku, kiedy struktura poszczególnych szczebli dowodzenia, tzn. dowództw dostosowana jest do roli, jaką one mają spełniać w walce.

W ujęciu czynnościowym proces dowodzenia obejmuje więc kompleks przedsięwzięć związanych z dowodzeniem, realizowanych przez komórki organizacyjne i osoby funkcyjne na stanowiskach dowodzenia w ramach systemu dowodzenia.

Z operacyjno-taktycznego punktu widzenia proces dowodzenia, przedstawia się jako cykl decyzyjny jednakowy na wszystkich szczeblach dowodzenia, składający się z cyklicznie powtarzających się faz, etapów i czynności. Do czterech tworzących go faz zalicza się: ustalanie położenia, planowanie, stawianie zadań, kontrolę.

W klasycznym ujęciu proces dowodzenia jest oparty na przesyłaniu różnego rodzaju zadań i meldunków (dokumentów normatywnych). Takie podejście ogranicza wykorzystanie nowoczesnych technologii informacyjnych w zakresie stworzenia środowiska sieciocentrycznego ukierunkowanego na współdzielenie informacji. Wytworzona informacja nie powinna być przesyłana w postaci meldunków lub innych dokumentów normatywnych. Powinna być umieszczana w przestrzeni sieciocentrycznej, a dostęp do niej byłby zarządzany przez administratorów sieci.

Proces wymiany informacji odbywa się pomiędzy osobami funkcyjnymi i zespołami funkcjonalnymi systemu dowodzenia, pomiędzy którymi istnieje „więź informacyjna" – formalna lub nieformalna droga przekazywania informacji.

Biorąc za podstawę rozważań kryterium struktury organizacyjnej[37] (służbowej) w systemie informacyjnym związków taktycznych, oddziałów i pododdziałów wojsk lądowych można wyróżnić następujące rodzaje więzi informacyjnych:

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

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

---

[37] J. Michniak, J. Wołejszo, *Determinanty skutecznego organizowania struktur dowództw Cz. III, Transformacja dowództwa szczebla operacyjnego na stanowiska dowodzenia*, AON, Warszawa 2002, s. 38.

– współdziałania – związane z wymianą informacji pomiędzy poszczególnymi stanowiskami dowodzenia nie mających zależności służbowych, a wynikających bezpośrednio z wykonywanego zadania.

Więzi organizacyjne wyrażające stosunki między poszczególnymi osobami funkcyjnymi a komórkami organizacyjnymi, w których te zasoby zostały zlokalizowane, klasyfikowane są najczęściej ze względu na rodzaj powiązań. Z tego punktu widzenia więzi organizacyjne podzielono na[38]:

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

– funkcjonalne – zachodzące na tle zróżnicowania kompetencji zawodowych,

– informowania – zachodzące na tle wymiany informacji.

Więzi służbowe dotyczą relacji dowódcy ze wszystkimi elementami dowództwa szczebla taktycznego. Służą one do przekazywania poleceń i informacji z góry. Charakteryzują się uprawnieniami danego dowódcy do decydowania o zakresie, rodzaju, czasie oraz strukturze pracy podwładnego. Przełożony jest uprawniony do stawiania zadań, które podwładni muszą wykonać, a w razie konieczności może decydować także o sposobach i kolejności ich realizacji. Tak szerokie uprawnienia mogą być również ograniczone przez szczególne rozwiązania organizacyjne.

Więzi funkcjonalne powstają w wyniku wyodrębnienia się najpierw stanowisk pracy, następnie komórek organizacyjnych wspomagających merytorycznie kierowników zespołów (sekcji) poszczególnych centrów głównego stanowiska dowodzenia. Więź ta występuje między komórkami niezależnymi od siebie służbowo.

Więzi informowania pokrywają się na ogół z innymi więziami: podporządkowania, funkcjonalną, bezpośredniego zasilania i koordynacyjną. Mogą jednak przebiegać także niezależnie od nich.

Przyjmując kryterium kierunku przepływu informacji[39] na stanowisku dowodzenia – można wyróżnić trzy rodzaje więzi informacyjnych:

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

---

[38] B. R. Kuc, *Zarządzanie doskonałe*, Oskar-Master of Biznes, Warszawa 1999, s.136.
[39] Tamże, s.39.

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

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

Obieg informacji w ramach zewnętrznych więzi informacyjnych odbywa się pomiędzy stanowiskami dowodzenia rozwijanymi na potrzeby poszczególnych dowództw, zgodnie z obowiązującymi procedurami w sytuacji zagrożenia i kryzysu militarnego w wymiarze narodowym[40] lub międzynarodowym.

Funkcjonowanie zewnętrznych więzi informacyjnych związane jest ze zbieraniem informacji i dotyczą szeroko pojętego otoczenia. Biorąc pod uwagę kierunki dystrybucji informacji oraz przyjęte kryteria można dokonać podziału zewnętrznych więzi informacyjnych na:

– więzi informacyjne w systemie dowodzenia przełożonego (płaszczyzna pozioma dystrybucji informacji);

– więzi informacyjne w relacjach współdziałania[41] (płaszczyzna pozioma dystrybucji informacji);

– więzi informacyjne w systemie dowodzenia do podległych elementów ugrupowania bojowego (płaszczyzna pionowa dystrybucji informacji);

– więzi informacyjne w relacjach specjalistycznych (płaszczyzna pionowa dystrybucji informacji).

W pierwszych dwóch wymienionych relacjach wymiany informacji źródłami informacji sytuacyjnych i dyrektywnych są stanowiska dowodzenia przełożonego, sąsiadów w ugrupowaniu operacyjnym (bojowym) oraz związków taktycznych (oddziałów i pododdziałów) wojsk lądowych. Wymiana informacji odbywa się w relacjach dowodzenia przełożonego, a w wypadku współdziałania zgodnie z zasadami określonymi w dokumentach normatywnych[42]. Zewnętrzne więzi informacyjne na przykładzie związku taktycznego w systemie dowodzenia przełożonego oraz w relacji współdziałania przedstawiono na rysunku 2.8.

W procesie wymiany informacji ważną role odgrywają także zewnętrzne więzi informacyjne organizowane na potrzeby specjalistyczne różnych rodzajów wojsk i służb, w których istnieje konieczność przekazywania informacji w wielu relacjach. Więzi te mogą się

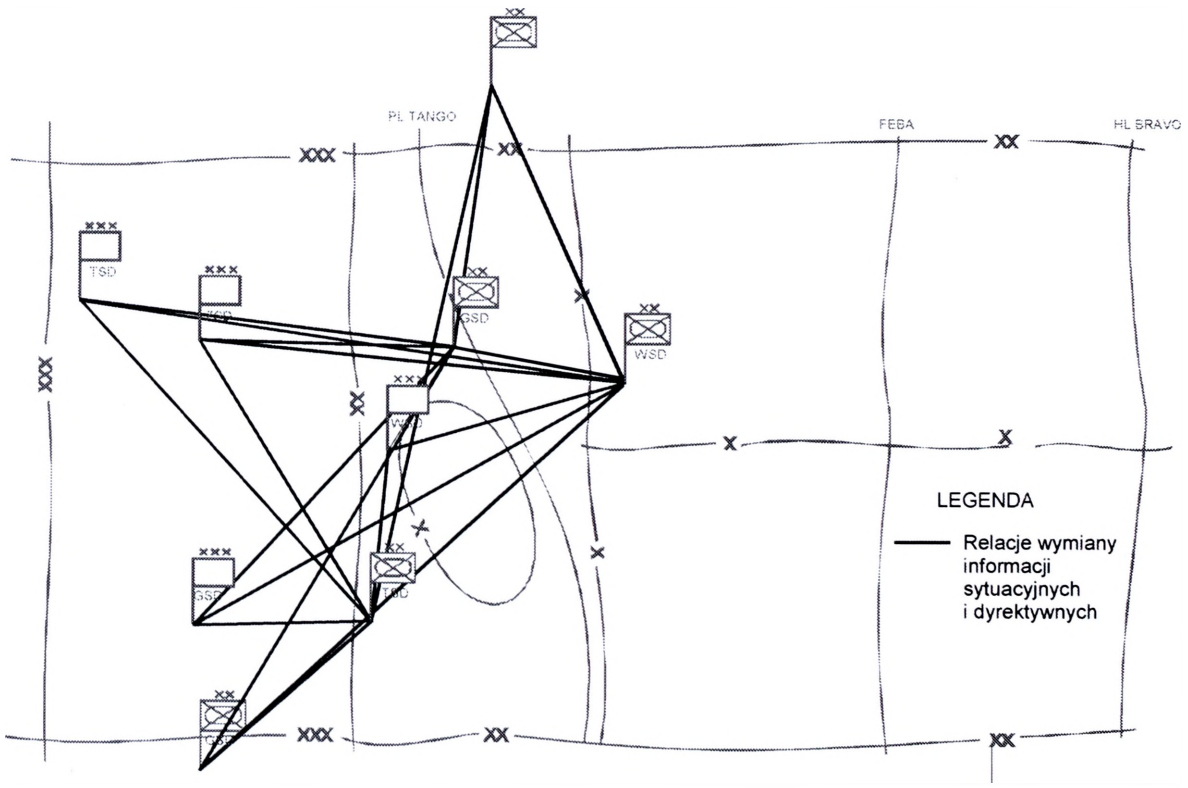
---

[40] Zawarte są w Instrukcji Wojennego Systemu Dowodzenia, wyd. Szt. Gen. WP, Warszawa 1998

[41] Więzi współdziałania występują w trakcie realizacji wspólnych zadań, bez udziału przełożonego. Występują także więzi synchronizacji, które organizuje dowódca danego szczebla w stosunku do podwładnych.

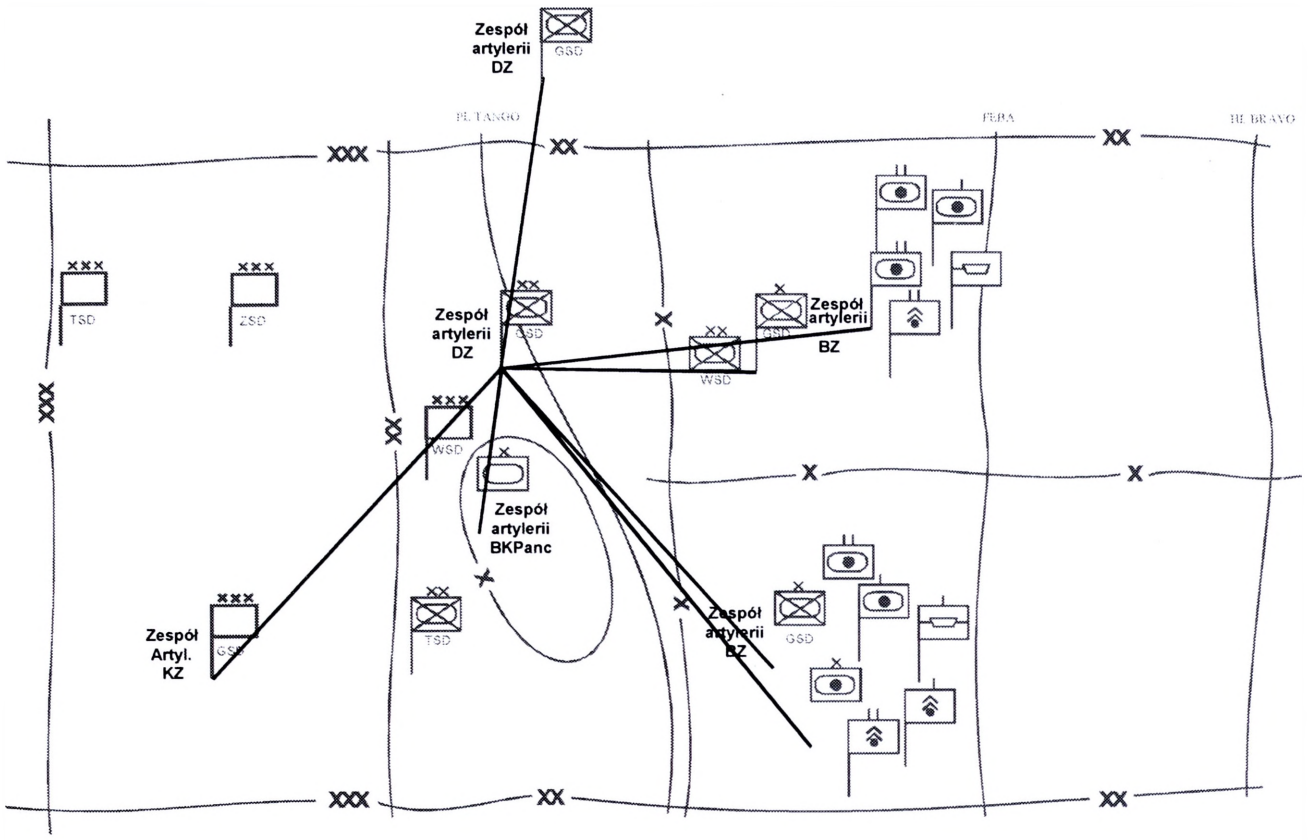
[42] *Zasady organizacji łączności współdziałania w operacjach wielonarodowych*, wyd. MON, Warszawa 1999.

pokrywać z relacjami dowodzenia danego rodzaju wojsk lub służb. Relacje te mogą wynikać z konieczności wymiany informacji, niezbędnych dla prawidłowego działania danego rodzaju wojsk, pomiędzy organami nie powiązanymi zależnościami służbowymi. W relacjach tych mogą występować zespoły funkcjonalne stanowisk dowodzenia szczebla taktycznego wojsk lądowych (ogólnowojskowe) i organa dowodzenia oddziałów lub pododdziałów specjalistycznych. Analizując więzi informacyjne w relacjach specjalistycznych należy także uwzględniać podsystemy sterowania środkami walki oraz podsystem zbierania i przetwarzania informacji w ramach rozpoznania. Przykład więzi informacyjnej, w ramach wybranych specjalności (rodzajów wojsk) na szczeblach taktycznych wojsk lądowych przedstawiono graficznie na rysunku 2.9.



Rys. 2.8. Zewnętrzne więzi informacyjne na przykładzie związku taktycznego w systemie dowodzenia przełożonego oraz w relacji współdziałania - wariant

Źródło: Fiołna Zb. i inni, Podstawowe relacje dowodzenia oddziału, związku taktycznego i związku operacyjnego w działaniach wojsk lądowych, część II - album schematów, wyd. AON, Warszawa 2001



Legenda: zewnętrze więzi specjalistyczne ————————

Rys. 2.9. Zewnętrzne więzi informacyjne w systemie dowodzenia dywizji na potrzeby artylerii - wariant
Źródło: Fiołna Zb. i inni, Podstawowe relacje dowodzenia oddziału, związku taktycznego i związku operacyjnego w działaniach wojsk lądowych, część II - album schematów, wyd. AON, Warszawa 2001

WNIOSKI

Z wyników przeprowadzonych badań, zaprezentowanych w rozdziale drugim można sformułować następujące wnioski:

1. Przed systemem informacyjnym organizacji są stawiane z góry ustalone wymagania, a mianowicie:

- dostarczanie kompleksowych i aktualnych informacji, zapewnianie selektywnego i skutecznego wykorzystania informacji oraz właściwej wymiany informacji pomiędzy komórkami organizacyjnymi, przełożonymi i podwładnymi w obydwu kierunkach,
- prostotę w użytkowaniu i zapewnieniu stałej, automatycznej metody pozyskiwania informacji z ustalonych źródeł,
- umożliwienie natychmiastowego pozyskania danych, nawet z najniższego szczebla zarządzania, wyszukiwanie i kojarzenie informacji z różnych źródeł, przedstawienie danych i wyników ich analiz w różnych układach sprawozdawczych,
- przepływu informacji opartego na sprzężeniach zwrotnych.

2. W specyficznym środowisku jaki jest proces dowodzenia realizowany na szczeblach taktycznych informację dzieli się ze względu na pilności i ważności przekazu na następujące kategorie:

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

3. W organizacji jaką są wojska lądowe proces decyzyjny rozłożony jest na wiele faz i etapów, realizowanych na różnych szczeblach dowodzenia. Skuteczność tego procesu, trafność podejmowanych decyzji, będzie zależała min. od jakości zarządzania posiadaną informacją. Z tego też względu zespoły realizujące proces zarządzania informacjami powinny zapewnić:

- dostępność informacji;
- wiarygodność informacji;
- bezpieczeństwo informacji;
- spójność informacji;
- trwałość informacji;
- aktualność informacji.

4. Istotnym kryterium jest znaczenie informacji w procesie decyzyjnym, co warunkuje jej zarządzanie. Według tego kryterium wyróżniamy informacje:

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

5. We wszystkich rodzajach sił zbrojnych dowodzenie wojskami jest realizowane przez dowódców z wykorzystaniem stanu osobowego dowództw w okresie pokoju lub obsady stanowisk dowodzenia w okresie zagrożenia lub wojny. Struktura organizacyjna dowództw traktowana jest jako podział dowództwa na komórki organizacyjne wraz z określeniem ich zadań, uprawnień i odpowiedzialności oraz uwzględnieniem powiązań informacyjnych między tymi komórkami. Stanowiska dowodzenia umożliwiają dowódcy dowodzenie w każdym rodzaju działań. Są one powiązane ze sobą funkcjonalnie i informacyjnie w określonym układzie po-

ziomym i pionowym, i stanowią jeden z najważniejszych elementów całego systemu dowodzenia.

6. Proces wymiany informacji odbywa się pomiędzy osobami funkcyjnymi i zespołami funkcjonalnymi systemu dowodzenia, pomiędzy którymi istnieje „więź informacyjna" – formalna lub nieformalna droga przekazywania informacji. Są to utrwalone drogi przepływu informacji między elementami danego dowództwa bądź między danym dowództwem a systemem wyższego przełożonego i otoczeniem, niezbędne do integrowania i koordynowania prowadzonej działalności.

3. Technologie informatyczne wykorzystywane do zarządzania informacja w sieci teleinformatycznej

W niniejszym rozdziale przedstawiono analizą najpopularniejszych, a zarazem najważniejszych technologii umożliwiających zarządzanie informacją w sieci teleinformatycznej. Do technologii tych zaliczono rozwiązanie Active Directory oraz DNS. Z uwagi na charakter pracy, analizie poddano stronę techniczną powyższych technologii.

3.1. Możliwości i przeznaczenie technologii Active Directory

Active Directory jest jednym z podstawowych narzędzi w rodzinie systemów Windows do zarządzania obiektami jak również relacjami, które tworzą środowisko sieciowe. Jest to bardzo popularne rozwiązanie stosowane powszechnie w wielu korporacjach, które uzyskują w ten sposób znaczną redukcję tzw. całkowitych kosztów posiadania TCO (*ang. Total Cost of Ownership*) i obsługi wykorzystywanego oprogramowania. Oferowane przez AD usługi spowodowały, że jest to narzędzie wykorzystywane również w NATO.

AD jest usługą katalogową – hierarchiczną bazą danych, której podstawowym protokołem jest LDAP (ang. Lightweight Directory Access Protocol). Active Directory jest rdzeniem bezpieczeństwa w środowisku sieciowym platformy Microsoft Windows Server. Jest odpowiedzialna m.in. za autentykacje użytkowników i komputerów w domenie organizacji, zarządzanie i wdrażanie zasad grup, funkcjonowanie polityk bezpieczeństwa (dotyczących np. zasad tworzenia haseł) oraz kontrolę dostępu do zasobów sieciowych.

Używając innej definicji, Active Directory to usługa katalogowa, dzięki której możliwe jest zarządzanie domeną[1]. Pierwszy raz pojawiła się ona w systemie Windows NT 4. (jednakże dopiero od wersji Windows 2000 otrzymało hierarchiczną strukturę) i od tej pory była stale rozbudowywana i aktualizowana. Wraz z rozwojem systemów firmy Microsoft, również i AC ewoluowało, było obecne w systemie Windows Server 2003, jest również dostępne w najnowszej wersji, zintegrowane z Windows Server 2008[2].

---

[1] Domena - to grupa komputerów połączonych w sieć, składająca się z serwera pełniącego rolę kontrolera domeny oraz stacji roboczych - klientów. Różni się ona od grupy roboczej sposobem przechowywania informacji o użytkownikach i ich uprawnieniach. O ile w klasycznych workgroup'ach każdy komputer w sieci posiada swoją własną bazę użytkowników, tak w domenie jest ona przechowywana tylko na serwerze. Dzięki temu zarządzanie taką siecią jest znacznie prostsze. Źródło: http://infojama.pl/150,artykul.aspx

[2] Definicja: opracowanie własne na podstawie: http://infojama.pl/150,artykul.aspx

3.1.1. Protokół LDAP

LDAP (*ang. Lightweight Directory Access Protocol*) – to protokół zapewniający dostęp do usług katalogowych. Protokół oparty jest na usługach katalogowych X.500. Wykorzystywany praktycznie w adresacji sieci Internet/Intranet w celu zapewnienia niezawodności, skalowalności i bezpieczeństwa danych. W odróżnieniu od X.500 nie potrzebuje ani szerokiego pasma ani dużej mocy obliczeniowej. LDAP pracuje w oparciu o protokół TCP/IP lub inne połączeniowe usługi transportu. Dane grupowane są w strukturze przypominającej drzewo katalogów. Każdy obiekt jest jednoznacznie identyfikowany poprzez swoje położenie w drzewie - tzw. DN (ang. distinguished name). Słowo "katalog" oznacza raczej kartotekę, niż znany "folder", dlatego myślenie o LDAP w kategoriach kartoteki znacznie ułatwia zrozumienie czym jest LDAP. Jest to serwis katalogowy pozwalający na wymianę informacji ponad protokołem TCP/IP. LDAP, w wielu sytuacjach, uznawane jest za rozwiązanie lepsze od innych usług katalogowych, ponieważ korzystając z TCP/IP (które działa tylko w warstwie transportowej modelu OSI) daje niezwykle szybkie odpowiedzi na żądania zgłaszane przez klienta. Słowo "katalog" oznacza raczej kartotekę, niż znany "folder", dlatego myślenie o LDAP w kategoriach kartoteki znacznie ułatwia zrozumienie czym jest LDAP.[3] W tabeli 3.1. przedstawiono podstawowe operacje realizowane przez ten protokół.

Informacje w katalogu są przechowywane w postaci wpisów (Entries). Każdy wpis jest obiektem jednej lub wielu klas. Klasy mogą być dziedziczone. Każda klasa składa się z jednego lub wielu atrybutów, które mogą być opcjonalne lub obowiązkowe. Tabela 3.2. przedstawia atrybutów dostępne w LDAP. Istnieje wiele podstawowych typów atrybutów. Atrybuty mogą mieć więcej niż jedną wartość. Można tworzyć swoje klasy i atrybuty. Wpisy są identyfikowane jednoznacznie przez DN (ang. Distinguished Name). Mogą być również identyfikowane względem nadrzędnego wpisu (kontekstu) poprzez RDN (ang. Relational Distinguished Name). Dostęp do wpisu chroniony jest poprzez listy kontroli dostępu ACL (ang. Access Control List). Można tworzyć uprawnienia dla kontekstów, wpisów oraz poszczególnych atrybutów. Wpisy mogą być eksportowane / importowane do / z plików tekstowych w specjalnym formacie LDIF (ang. LDAP Data Interchange Format). Format LDIF jest to format wymiany danych protokołu LDAP. W tych plikach znajdują się instrukcje manipulujące informacjami katalogowymi.

[3] http://infojama.pl/150,artykul.aspx

Tabela 3.1.

Podstawowe operacje realizowane przez protokół LDAP

Lp.	Nazwa operacji	Opis operacji
1.	**bind**	Uwierzytelnienie użytkownika – powiązanie jego tożsamości (oraz obiektu LDAP) z połączeniem sieciowym i sesją LDAP. Pozwala ona na uwierzytelnienie klienta wobec serwera. Wymaga potwierdzenia odbioru od serwera, w którym znajduje status żądania klienta. W wersji 2 protokołu LDAP musiała być ona pierwszą operacją w ramach sesji, w wersji 3 zniesiono to ograniczenie. Operacja bind może też przestawić sesję w stan "anonimowy" jeśli podany zostanie pusty DN (ang. Distinguished Name) i hasło. W ramach sesji LDAP można wielokrotnie dokonywać operacji bind zmieniając w ten sposób kontekst uwierzytelniania tej sesji.
2.	**unbind**	Funkcją operacji jest zakończenie sesji i połączenia sieciowego LDAP. Operacja unbind nie wymaga potwierdzenia.
3.	**search**	Umożliwia użytkownikowi zgłoszenia żądania poszukiwanego zasobu, które będzie realizowane przez serwer. W ten sposób klient może pobierać oraz wyszukiwać informacje.
4.	**add**	Pozwala użytkownikowi zgłoszenia żądać od serwera możliwości dodania wpisów do katalogu, zmiany istniejącego wpisu oraz zmiany nazwy wpisu.
5.	**modify**	Zezwala użytkownikowi na modyfikowanie, wprowadzanie nowych pozycji oraz ich usuwanie z bazy danych znajdującej się na serwerze.
6.	**delete**	Operacja delete zezwala użytkownikowi na żądanie od serwera usunięcia wpisów do katalogu.

Źródło: opracowanie własne na podstawie: http://www.technet.microsoft.com

Wszystkie wpisy zorganizowane są w postaci struktury drzewa katalogowego, najczęściej bazującego na politycznej, geograficznej lub organizacyjnej strukturze (struktura hierarchiczna).

W protokole LDAP uwierzytelnianie jest realizowane na kilka sposobów:

- anonimowe – klient ma prawa wbudowanego użytkownika (guest);
- poprzez hasło – użytkownik loguje się poprzez DN/hasło;
- protokół SSL – następuje wymiana certyfikatów;
- PROXY – wykorzystywane przez aplikację, która uwierzytelnia się na hasło użytkownika PROXY, a następnie działa w imieniu zadanego użytkownika. Takie uwierzytelnienie stosuje serwis AD LDS (Active Directory Lightweight Directory Services).

Bardzo ważną cechą LDAP jest to, że autoryzacja wykonywana jest podczas wykonywania operacji, a nie po uwierzytelnieniu.

Tabela 3.2.

Atrybuty dostępne w LDAP (występujące w pliku schematów core.schema):

Lp.	Nazwa atrybutu	Opis atrybutu
1.	**UID (ang. User IDentifier)**	Identyfikator użytkownika
2.	**RID (ang. Realtive IDentifier)**	Liczba reprezentująca względny identyfikator użytkownika
3.	**CN (ang. Common Name)**	Nazwa
4.	**SN (ang. Surname)**	Nazwisko
5.	**OU (ang. Organizational Unit Name)**	Nazwa jednostki organizacyjnej
6.	**O (ang. Organization Name)**	Nazwa organizacji
7.	**DC (ang. Domain Component)**	Składnik nazwy domenowej
8.	**C (ang. Country)**	Państwo
9.	**L (ang. Locality Name)**	Nazwa lokalna
10.	**ST (ang. State Or Province Name)**	Nazwa stanu lub województwo
11.	**STREET**	Ulica

Źródło: opracowanie własne na podstawie: http://www.technet.microsoft.com oraz http://msdn.microsoft.com/en-us/library/aa366101(VS.85).aspx

System Windows 2003 Server posiada rozbudowane mechanizmy LDAP[4]. Przykładem są tzw. wirtualne listy elementów. Jeżeli klient chce odczytać duży zestaw obiektów, to może utworzyć taką listę po stronie serwera, po czym dalej przeglądać kolejno informacje, ściągając je małymi porcjami.

3.1.2. Protokół LDAPS

LDAPS (ang. LDAP over SSL) to niestandardowe rozszerzenie protokołu LDAP wykorzystujące protokół SSL do szyfrowania komunikacji między serwerem, a klientem. Serwery udostępniają połączenie LDAPS na oddzielnym porcie TCP - domyślnie jest to port 636.

[4] Jest to rozszerzenie LDAP opracowane przez IETF

Aby uruchomić ten protokół, wystarczy zainstalować parę kluczy/certyfikatów na kontrolerze domeny.

Od trzeciej wersji protokołu LDAP zdefiniowany jest standardowy tryb szyfrowania oparty o funkcję StartTLS, zgodnie z dokumentem RFC 2830 (nie wymagający osobnego portu). Można też wykorzystywać autoryzację typu „diggest", jak to opisuje dokument RFC 2829, co powoduje, że LDAPS utracił rację bytu.

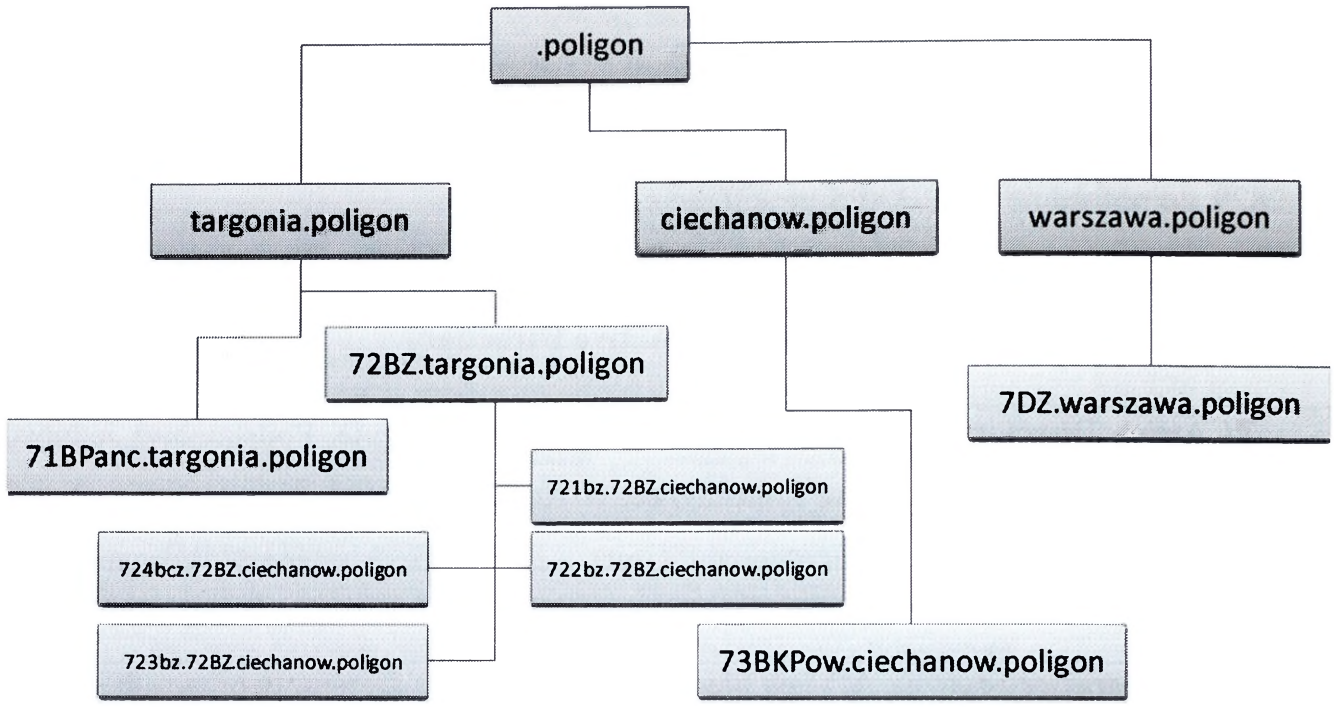
3.1.3. Struktura Active Directiory

W Active Directory informacje grupowane są hierarchicznie. Podstawową jednostką jest tzw. **liść**, który położony jest w **kontenerze,** w Active Directory nazywanym jednostką organizacyjną OU (ang. Organizational Unit). Liście i kontenery zorganizowane są w domeny.

Cechą charakterystyczną AD jest hierarchiczna struktura domen, tworzących strukturę **drzewa**, które posiada zawsze przynajmniej jedną domenę najważniejszą. Jest to domena najwyższego poziomu, nazywaną **korzeniem** lub czasem korzeniem drzewa (ang. root). Wszystkie pozostałe domeny umieszcza się jako domeny podrzędne. W ten sposób budowane jest drzewo domen. Każda podległa domena również może się rozgałęziać.

Tak jak w naturze tak i w przypadku AD drzewo zazwyczaj umieszczane jest w lesie. (ang. forest). Każdy **las** składa się z przynajmniej jednego drzewa. Domena nie może istnieć samodzielnie, musi być w jakimś drzewie i lesie. W sytuacji, gdy jest to domena najwyższego poziomu lub jest to pierwsza z domen, to tworzy pierwsze drzewo (staje się jego korzeniem) oraz pierwszy las. Wówczas las otrzymuje nazwę od nazwy tej domeny.

Domeny zorganizowane w drzewo współdzielą jedną przestrzeń adresową DNS, tzn. domeny kolejnych poziomów mają wspólny korzeń (dla domeny najwyższego poziomu) nazewniczy, np. polska.pl, a wszystkie domeny niższych poziomów posiadają nazwy powstałe przez dodanie nazwy domeny do domeny najwyższego poziomu, np. warszawa.polska.pl, pogoda.polska.pl, historia.polski.pl. Inny przykład został przedstawiony na rysunku 3.1., gdzie domeną- korzeniem jest .poligon, domenami drugiego poziomu są trzy domeny: Targonia, ciechanow, warszawa. Domenami trzeciego poziomu są: - dla domeny warszawa – domena 7DZ; - dla domeny ciechanow – domena 73BKPow; – dla domeny targonia – 71BPanc, 72BZ. Ostatnim, czwartym poziomem doemn podrzędnych są domeny podległe pod domenę 72BZ – 721bz, 722bz, 723bz, 724bcz.



Rys.3.1. Przykładowy las domen w Active Directory
Źródło: Opracowanie własne

3.1.3.1. Relacje zaufania

Zasadniczą zaletą Active Directory jest autoryzacja użytkowników, którzy otrzymują zdefiniowane i przypisane przez administratora prawo lub (jego brak) dostępu do zasobów Active Directory np. kontenera lub obiektu użytkownika, jak również zasobów dyskowych, sieciowych, czy też aplikacji. Dostęp do innych usług AD lub zasobów korzystających z tej innej usługi (np. zasobu sieciowego), w sposób automatyczny (automatyczna autoryzacja), użytkownik uzyskuje poprzez **relacje zaufania** pomiędzy domenami AD. Domeny połączone relacją zaufania "ufają sobie", o ile jest to relacja zaufania dwustronna, lub tylko jedna ufa drugiej, jeżeli jest to relacja jednostronna. Domeny w obrębie jednego lasu (w tym w obrębie tego samego drzewa) ufają sobie.

W systemach Windows 2000 i Windows Server 2003 istnieją trzy typy relacji zaufania, z których każdy pełni odpowiednią funkcję w strukturze domeny[5]. Relacje zaufania do-

[5] Więcej można znaleźć pod adresem: http://support.microsoft.com/kb/310996/PL

stępne w domenach systemów Windows 2000 i Windows Server 2003 zostały opisane w tabeli 3.3.

Zmniejszenie liczby relacji zaufania, którymi trzeba zarządzać, stanowi bardzo istotne ulepszenie w systemach Windows 2000 i Windows Server 2003. Bardzo potrzebne było także inne ulepszenie, związane z granicami administracyjnymi. W systemie Microsoft Windows NT 4.0 administratorzy, którzy potrzebowali możliwości administrowania podzbiorami użytkowników lub grup w danej domenie systemu Windows NT, musieli mieć pełne uprawnienia administracyjne w całej domenie. Nawet jeśli byłoby lepiej, aby ich prawa administracyjne nie obejmowały całej domeny, potrzebne im prawa wymagały przyznania im tak ogromnych uprawnień. Tę sytuację zmieniło wprowadzenie jednostek organizacyjnych w systemie Windows 2000 i Windows Server 2003.

3.1.3.2. Jednostki organizacyjne (kontenery)

Innym pojęciem związanym z AD są **jednostki organizacyjne**. Ich zadaniem jest tworzenie granic administracyjnych w ramach domeny. Dzięki nim istnieje możliwość delegacji zadań administracyjnych (przez administratorów domeny) podległym im administratorom, nie przydzielając im całkowitych uprawnień administracyjnych w całej domenie.

W ramach jednej domeny może funkcjonować więcej niż jedna jednostka organizacyjna. Jednostkę organizacyjną można porównać, w przypadku Akademii Obrony Narodowej do podziału Instytutu (np. Instytutu Wojsk Lądowych) na zakłady. Obiekty zawarte w jednostkach organizacyjnych muszą należeć do tej samej domeny, co jednostka. Dodatkowym atutem wykorzystywania jednostek organizacyjnych jest możliwość przypisywania tzw. zasad grupy (praw do zasobów AC), dla małych zbiorów zasobów. Pozwala to oszczędzić pracy administratorom, gdyż nie muszą dzięki temu zmieniać zasad dla całej domeny. Przez to, że jednostki organizacyjne pomagają w uporządkowaniu obiektów zgodnie z ich funkcjonalnością, ułatwiają zarządzanie zasobami. Jednostki organizacyjne przedstawione są jako foldery w konsoli Użytkownicy i komputery usługi Active Directory.

Tabela 3.3.

Relacje zaufania Active Directory w systemach Windows 2000 oraz Windows Server 2003.

Lp.	Nazwa relacji zaufania	Opis relacji zaufania
1.	**przechodnie**	Ustanawiają relację zaufania między dwiema domenami, która może przechodzić na inne domeny (np. jeśli domena A ufa domenie B, a domena B ufa domenie C, to domena A automatycznie ufa domenie C i na odwrót. Między domenami różnych poziomów są ustanawiane automatycznie w momencie utworzenia nowych domen w drzewie domeny. Są natomiast ograniczone do domen systemu Windows 2000 lub Windows Server 2003 oraz do domen w ramach tego samego drzewa domeny lub lasu, nie można utworzyć przechodniej relacji zaufania z domenami niższego poziomu (system Windows NT 4.0). Nie można także utworzyć zaufania przechodniego między dwiema domenami systemu Windows 2000 lub dwiema domenami systemu Windows Server 2003 znajdującymi się w różnych lasach.
2.	**jednokierunkowe**	Definiują relację zaufania tylko między dwiema domenami. Można utworzyć dwie oddzielne jednokierunkowe relacje zaufania (po jednej w każdym kierunku), aby utworzyć dwukierunkową relację zaufania. Takie symetryczne zaufania jednokierunkowe nie są równoważne zaufaniu przechodniemu. Relacje tego typu są nieprzechodnie, czyli zaufania jednokierunkowe w systemach Windows 2000 i Windows Server 2003 są takie same, jak zaufania jednokierunkowe w systemie Windows NT 4.0 i są wykorzystywane w kilku sytuacjach w systemach Windows 2000 lub Windows Server 2003. W pierwszym przypadku, zaufania jednokierunkowe są często wykorzystywane wtedy, gdy nowe relacje zaufania należy ustanowić między domenami niższego poziomu, takimi jak domeny systemu Windows NT 4.0 Ponieważ domeny niższego poziomu nie mogą wchodzić w skład środowiska zaufania przechodniego systemów Windows 2000 i Windows Server 2003 (takich jak drzewa lub lasy), należy ustanowić zaufania jednokierunkowe, aby umożliwić relacje zaufania między domeną systemu Windows 2000 lub Windows Server 2003 a domeną niższego poziomu systemu Windows NT. W drugim, przypadku, wykorzystuje się je, gdy trzeba ustanowić relację zaufania między domenami znajdującymi się w różnych lasach systemów Windows 2000 lub Windows Server 2003. Można użyć jednokierunkowych relacji zaufania między domenami w różnych lasach systemu Windows 2000 lub Windows Server 2003, aby wyodrębnić relację zaufania z domeną, w której utworzono i obsługuje się tę relację, zamiast tworzyć relację zaufania dotyczącą całego lasu. W obu przypadkach można utworzyć zaufanie dwukierunkowe przy użyciu dwóch pojedynczych jednokierunkowych relacji zaufania
3.	**skrzyżowane**	Służą do zwiększania wydajności. Powstaje wówczas wirtualny most weryfikacji zaufania w ramach hierarchii drzewa lub lasu umożliwiający przyspieszenie potwierdzania (lub odmawiania) relacji zaufania. Aby dowiedzieć się więcej o tej relacji zaufania skrzyżowane, niezbędne jest zrozumienie sposobu obsługi uwierzytelnienia między domenami w systemach Windows 2000 i Windows Server 2003.

Źródło: opracowanie własne na podstawie: Active Directory Services for Microsoft Windows 2000 Technical Reference, Microsoft Press.

Inny przykład pochodzący z tego samego opracowania, Active Directory Services for Microsoft Windows 2000 Technical Reference pomoże wyjaśnić, dlaczego jednostki organizacyjne są przydatne. „Powiedzmy, że dział sprzedaży w danej organizacji ma własnych administratorów sieci i takie zasoby, jak drukarki i serwery, które opłaca z własnego budżetu. Administratorzy sieci z działu sprzedaży chcą więc kontrolować zasoby, zasady i inne elementy administracyjne w grupie działu sprzedaży. Dział sprzedaży jest jednak częścią domeny firmy. W przypadku sieci systemu Windows NT 4 administratorów z działu sprzedaży należałoby dodać do grupy Administratorzy domeny, aby udzielić im uprawnień administracyjnych potrzebnych do administrowania jednostką działu sprzedaży. Członkostwo w grupie Administratorzy domeny dałoby administratorom działu sprzedaży kontrolę administracyjną nad domeną całej firmy (a nie tylko nad jednostką działu sprzedaży). Przekazanie całkowitej kontroli administracyjnej nie byłoby właściwe, ale tylko dzięki temu administratorzy działu sprzedaży mogliby mieć kontrolę administracyjną nad zasobami i zasadami działu sprzedaży. Ta sytuacja uległa diametralnej zmianie w systemie Windows 2000 i Windows Server 2003, w których wprowadzono jednostki organizacyjne. W sieci systemów Windows 2000 lub Windows Server 2003 nadzorujący administratorzy sieciowi mogą utworzyć jednostki organizacyjne, w tym jednostkę działu sprzedaży, w ramach struktury domeny i w ten sposób ustanowić nowe, bardziej ograniczone granice administracyjne. Rozwiązanie mogłoby wyglądać następująco: utworzono by jednostkę organizacyjną obejmującą dział sprzedaży i przyznano administratorom działu sprzedaży pełne uprawnienia administracyjne wyłącznie do jednostki organizacyjnej działu sprzedaży, a nie do jakichkolwiek innych obszarów firmowej domeny. Po utworzeniu jednostek organizacyjnych członkostwo w grupie Administratorzy domeny (które daje uprawnienia administracyjne do całej domeny, w tym do jednostek organizacyjnych) może zostać ograniczone tylko do tych administratorów, których obowiązki administracyjne dotyczą całej domeny. W ten sposób powstaje bezpieczniejsza i lepiej obsługiwana sieć."

Ważną informacją dotyczącą jednostek organizacyjnych jest możliwość ich zagnieżdżania. Jest to możliwe do 15 poziomów zagnieżdżenia, ponieważ powyżej tej liczby wydajność staje się niezadowalająca. Potrzeba taka może się pojawić, gdy w firmie potrzebne są jednostki organizacyjne działające w ramach innych jednostek organizacyjnych.

3.1.3.3. Granica administracyjna

Domena systemu Windows 2000 lub Windows Server 2003 jest tzw. **granicą administracyjną.** Jest to bardzo ważna cecha AD, ponieważ prawa administracyjne nie przechodzą przez granice domen ani nie przebiegają w dół drzewa domeny systemu Windows 2000 lub Windows Server 2003. Cytując za Active □ekord□□y Services for Microsoft Windows 2000 Technical Reference „jeśli istnieje drzewo domeny z domenami A, B i C, gdzie A jest domeną nadrzędną nad B, a B jest domeną nadrzędną nad C, użytkownicy mający prawa administracyjne w domenie A nie mają praw administracyjnych w domenie B, a użytkownicy mający prawa administracyjne w domenie B nie mają praw administracyjnych w domenie C". Warunkiem niezbędnym do uzyskania przez użytkownika praw administratora w danej domenie, muszą być mu przyznane wyższe uprawnienia. Nie jest to jednoznaczne z tym, że istnieją ograniczenia na nadawanie uprawnień administratora w wielu domenach; oznacza to tylko, że wszystkie prawa trzeba wyraźnie definiować.

Informacje zawarte w jednej domenie mogą być potrzebne użytkownikom, którzy nie są jej członkami. Ujawnia się w tym momencie kolejne połączenie AD z usługą DNS, ponieważ Active □ekord□□y używa wyszukiwania i kwerend DNS do realizacji kwerend, tak jak w Internecie. Usługi Active □ekord□□y i systemy Windows 2000 oraz Windows Server 2003 korzystają z systemu DNS, jak z usługi wyszukiwania. Korzystają przy tym z wpisu w rekordach zasobów RRs (ang. □ekord□ Records)[6], specjalnej usługi SRV (ang. SRV □ecord lub □ekord□ □ekord) [7], który oznacza dany wpis DNS jako kontrolera domeny. Kontrolery domen określają natomiast, czy mogą wykonać kwerendę (byłoby to możliwe, gdyby kwerenda dotyczyła obiektu znajdującego się w ich domenie lokalnej). Jeśli nie mogą, żądanie jest przekazywane do kontrolera domeny, który albo może sam zrealizować żądanie, albo skierować kontroler domeny do następnego serwera logicznego, do którego należy złożyć żądanie. W końcu znajdowany jest kontroler domeny, który może zrealizować żądanie (lub okazuje się, że takiego kontrolera nie ma), a klient jest odsyłany do serwera, na którym proces realizacji kwerendy jest kontynuowany.[8]

---

[6] RRs (ang. Resource Records) są częścią DNS (ang. Domain Name System). Dokładne informacje dotyczące formatu oraz informacji w nich przechowywanych można znaleźć w dokumencie: RFC 1035(§3.2.1.) pod adresem: http://freesoft.org/CIE/RFC/1035/13.htm

[7] SRV (ang. SRV record lub Service record) wchodzi w skład w DNS (ang. Domain Name System) i jest odpowiedzialny za przekazywanie informacji o dostępności usług (serwisów). Dokładną definicję można znaleźć w dokumencie RFC 2782. Źródło: http://en.wikipedia.org/wiki/SRV_record

[8] Na podstawie: http://support.microsoft.com/kb/310996/PL

3.1.3.4. Katalog

Katalog, który został już częściowo opisany w podrozdziale dotyczącym protokołu LDAP (patrz podrozdział 3.1.1.) jest często określany jako magazyn danych i zawiera informacje dotyczące obiektów takich jak użytkownicy, grupy, komputery, domeny, jednostki organizacyjne (OU) oraz zasady zabezpieczeń. Publikowane informacje tego typu mogą być wykorzystane przez użytkowników i administratorów. Katalog jest przechowywany na serwerach zwanych kontrolerami domeny i jest udostępniany aplikacjom lub usługom sieciowym. W domenie może znajdować się jeden lub kilka kontrolerów. Każdy kontroler domeny dysponuje kopią katalogu przystosowaną do modyfikacji i przeznaczoną dla domeny, w której znajduje się dany kontroler. Zmiany wprowadzone w katalogu są replikowane ze źródłowego kontrolera domeny do innych kontrolerów w danej domenie, drzewie domen lub lesie. Możliwość replikacji katalogu i modyfikacji kopii katalogu dostępnych na poszczególnych kontrolerach domeny gwarantuje wysoki poziom dostępności katalogu dla użytkowników i administratorów w domenie. Dane katalogu są przechowywane w pliku Ntds.dit na kontrolerze domeny. Zalecane jest przechowywanie tego pliku na partycji systemu plików NTFS. Niektóre dane są przechowywane w pliku bazy danych katalogu, a pewne informacje, takie jak skrypty logowania i zasady grupy, są przechowywane w replikowanym systemie plików[9].

Bardzo istotne dla poprawnego funkcjonowania usługi Active Directory jest **rozpowszechnianie katalogu**. W systemach Windows 2000 i Windows Server 2003 kontroler domeny w przechowuje kopię partycji katalogu własnej domeny. Umożliwia to realizowanie lokalnie kwerend dotyczące informacji o obiektach w domenie, do której należy.

Takie podejście jest sensowne, ponieważ w wielu wypadkach użytkownicy (lub inne jednostki korzystające z usług Active Directory) częściej wykorzystują zasoby sieciowe domeny lokalnej niż zasoby znajdujące się w domenie zdalnej. Rozpowszechnienie kopii partycji domeny na każdym kontrolerze domeny w domenie oraz udostępnienie każdej kopii do odczytu i zapisu umożliwia uzyskanie następujących usprawnień i udoskonaleń[10]:

- Zwiększenie wydajności, ponieważ każdy kontroler domeny może wykonywać lokalne wyszukiwanie obiektów znajdujących się w jego domenie.
- Zwiększenie skalowalności, gdyż każdy kontroler domeny zawiera wzorcową kopię partycji wykazu katalogu, przeznaczoną do odczytu i zapisu.

---

[9] Active Directory – omówienie techniczne, materiały firmy Microsoft.
[10] Tamże.

- Zwiększenie skalowalności spowodowane tym, że żaden pojedynczy komputer nie jest obciążony obowiązkiem wykonywania aktualizacji katalogu.

Jest to szczególnie przydatne, kiedy lokacje zdalne lub oddziały filii stanowią część topologii sieci. Po umieszczeniu kontrolera domeny (który z definicji zawiera kopię partycji wykazu katalogu) w lokacji zdalnej kwerendy użytkownika mogą być wykonywane lokalnie. Oznacza to, że zmniejsza się wykorzystanie prawdopodobnie kosztownych lub ograniczonych zasobów sieci rozległej (WAN). Korzyści płynące z umieszczenia kontrolera domeny w lokacji zdalnej lub kompleksie biurowym filii nie sprowadzają się tylko do oszczędniejszego wykorzystania zasobów sieci rozległej, ponieważ wzrasta wydajność kwerend, gdy kontroler domeny (i jego partycja wykazu katalogu) jest dostępny w sieci lokalnej (LAN) lokacji zdalnej[11].

Innym zagadnieniem jest **replikacja katalogu**. Każdy kontroler domeny zawiera przeznaczoną do zapisu wzorcową kopię partycji usługi Active Directory dla swojej domeny, więc zmiany w partycji domeny można wprowadzić na każdym dostępnym kontrolerze domeny. W takim przypadku musi istnieć sposób powielania aktualizacji na innych kontrolerach domen po wprowadzeniu zmian na jednym kontrolerze domeny. Proces rozpowszechniania zaktualizowanych informacji na właściwe kontrolery domen nosi nazwę replikacji. Kategorie danych katalogu replikowane między kontrolerami domeny zawarto w tabeli 3.4. W systemach Windows 2000 i Windows Server 2003 jednostką replikacji jest partycja domeny. Na inne kontrolery domen są jednak replikowane tylko zmiany na poziomie atrybutów danego obiektu; nie są replikowane całe obiekty (zakres informacji przechowywanych i replikowanych na kontrolerze domeny przedstawiono w tabeli 3.5.) Prowadzi to do znacznych oszczędności w natężeniu ruchu związanego z replikacją. Priorytet aktualizacji jest określany za pomocą numerów sekwencji aktualizacji USN (ang. Update Sequence Number). Zamiast porównywać wartości atrybutów obiektów, usługi Active Directory używają bieżącego numeru USN do określania, czy replikacja jest potrzebna i - jeśli odpowiedź jest twierdząca - które wartości atrybutu obiektu muszą być transmitowane. Implementacja numerów USN to kolejna zaleta domeny jako jednostki podziału na partycje; dzięki niej ruch związany z replikacją (który i tak jest ograniczony do zmian atrybutów) odbywa się tylko w granicach domeny, w której zaszły zmiany[12].

---

[11] Tamże.
[12] Tamże.

Tabela 3.4.

Kategorie danych katalogu replikowane między kontrolerami domeny

Lp.	Nazwa kategorii	Opis kategorii
1.	**Dane domeny**	Zawierają informacje dotyczące obiektów znajdujących się w domenie. Są to informacje, które są zazwyczaj uwzględniane w katalogu, takie jak kontakty e-mail, atrybuty kont użytkowników i komputerów oraz publikowane zasoby istotne z perspektywy administratorów i użytkowników.
2.	**Dane konfiguracji**	Dane konfiguracji opisują topologię katalogu. Przykładem może być lista wszystkich domen, drzew i lasów oraz lokalizacje kontrolerów domeny i katalogów globalnych.
3.	**Dane schematu**	Schemat jest formalną definicją wszystkich danych dotyczących obiektów i atrybutów, które mogą być przechowywane w katalogu. W systemie Windows Server 2003 uwzględniono domyślny schemat definiujący wiele typów obiektów, takich jak konta użytkowników i komputerów, grupy, domeny, jednostki organizacyjne i zasady zabezpieczeń. Administratorzy i programiści mogą rozszerzać schemat, definiując nowe typy i atrybuty obiektów lub dodając nowe atrybuty do istniejących obiektów. Obiekty schematu są chronione przy użyciu list kontroli dostępu (ACL), które akceptują wyłącznie modyfikacje schematu wprowadzone przez autoryzowanych użytkowników.

Źródło: opracowanie własne na podstawie: Active Directory – omówienie techniczne, materiały firmy Microsoft

Tabela 3.5.

Zakres informacji przechowywanych i replikowanych na kontrolerze domeny

Lp.	Nazwa informacji	Opis informacji
1.	**Informacje o schemacie**	Definiują obiekty i atrybuty obiektów, które mogą być tworzone w katalogu. Są one wspólne dla wszystkich domen w lesie. Replikuje się je do wszystkich kontrolerów domeny w lesie.
2.	**Informacje o konfiguracji**	Opisują logiczną strukturę rozmieszczenia oprogramowania i danych, np. o strukturze domeny lub topologii replikacji. Te informacje również są wspólne dla wszystkich domen w lesie oraz replikowane do wszystkich kontrolerów domeny w lesie.
3.	**Informacje o domenie**	Opisują wszystkie obiekty w domenie. Są one specyficzne dla domeny i nie są dystrybuowane do innych domen. Dla celów związanych z wyszukiwaniem informacji w drzewie domen lub lesie podzestaw właściwości wszystkich obiektów we wszystkich domenach jest przechowywany w wykazie globalnym. Dane domeny są replikowane do wszystkich kontrolerów w danej domenie.
4.	**Informacje o aplikacji**	Informacje przechowywane w partycji katalogu aplikacji są używane wówczas, gdy konieczna jest lokalna replikacja danych, a nie replikacja na skalę globalną. Dane aplikacji mogą być jawnie przekierowane do kontrolerów domeny w lesie, określonych przez administratora, w celu eliminacji zbędnego ruchu sieciowego związanego z replikacją, lub skonfigurowane do replikacji do wszystkich kontrolerów domeny w domenie.

Źródło: opracowanie własne na podstawie: Active Directory – omówienie techniczne, materiały firmy Microsoft

3.1.3.5. Katalog globalny

Usługą odpowiadającą za skrócenie czasu oczekiwania na odpowiedź kwerendy użytkownika, który potrzebuje informacji wykraczającej poza granice jednej domeny i dotyczy np. całej organizacji jest **katalog globalny** zwany również **wykazem globalnym**. Składa się on z wybranych atrybutów każdego obiektu w organizacji. Oznacza to , że atrybuty te dotyczące każdego obiektu w lesie są dostępne dla kwerend domeny lokalnej.

Ponadto, przechowuje najczęściej wyszukiwane atrybuty poszczególnych obiektów. Przechowywana jest w nim pełna kopia wszystkich obiektów w katalogu związanym z domeną macierzystą i częściowa kopia wszystkich obiektów dla pozostałych domen w lesie.

Takie rozwiązanie gwarantuje efektywne wyszukiwanie bez zbędnych odwołań do kontrolerów domeny. Jest on tworzony automatycznie na początkowym kontrolerze domeny w lesie. Istnieje możliwość dodania funkcji wykazu globalnego do innych kontrolerów domeny lub zmiany jego domyślnej lokalizacji poprzez wskazanie innego kontrolera domeny.

Natychmiast po utworzeniu przez firmę Microsoft domyślnego zestawu obiektów w schemacie, domyślne atrybuty każdego obiektu schematu są znakowane jako włączane do wykazu globalnego. (Być może nigdy nie trzeba będzie ich modyfikować, ale taka możliwość istnieje). Większość obiektów ma około 15 atrybutów, a mniej więcej siedem z tych atrybutów znakuje się jako włączane do wykazu globalnego. Wykaz globalny znajduje się, jak wspomniany powyżej, na wybranych kontrolerach domen w każdej domenie i obsługuje kwerendy wymagające wyszukiwania globalnego. Kiedy użytkownik prześle globalną kwerendę opartą na atrybucie obiektu, który jest oznakowany jako włączony do wykazu globalnego, kwerendę może zrealizować kontroler domeny w domenie lokalnej mający konfigurację powodującą przechowywanie kopii wykazu globalnego. Ponieważ w każdej domenie jest przynajmniej jeden kontroler domeny zawierający wykaz globalny, kwerendy polegające na wyszukiwaniach globalnych mogą być szybko wykonywane i realizowane. Atrybuty włączane do wykazu globalnego zostały domyślnie wybrane, gdyż nie zmieniają się zbyt często. Użycie informacji statycznych w wykazie globalnym minimalizuje ruch związany z replikacją; zmiana atrybutu obiektu oznakowanego jako włączany do wykazu globalnego musi być bowiem replikowana do wszystkich kontrolerów domeny z wykazem globalnym. Informacje statyczne nie tylko minimalizują ruch, są także właściwszym przedmiotem wyszukiwania globalnego.[13]

W tabeli 3.6. przedstawiono zadania realizowane przez katalog globalny.

[13] Na podstawie: http://support.microsoft.com/kb/310996/PL

Tabela 3.6.

Zadania realizowane przez katalog globalny

Lp.	Nazwa zadania	Opis zadania
1.	**Odnajdywanie obiektów**	Użytkownik ma możliwość wyszukiwania we wszystkich domenach w lesie, niezależnie od lokalizacji, w której są one przechowywane. W lesie wykonuje się je z maksymalną szybkością i przy generowaniu minimalnego ruchu w sieci. W przypadku wyszukiwania osób lub drukarek przy użyciu menu Start lub opcji Cały katalog w kwerendzie w rzeczywistości przeszukiwany jest wykaz globalny. Wprowadzone żądanie dotyczące wyszukiwania jest kierowane do domyślnego portu wykazu globalnego, tzn. portu 3268, i wysyłane do wykazu globalnego w celu rozpoznania obiektów.
2.	**Uwierzytelnianie głównych nazw użytkowników**	Główne nazwy użytkowników są rozpoznawany przez katalog globalny wówczas, gdy uwierzytelniający kontroler domeny nie dysponuje informacjami dotyczącymi określonego konta. Na przykład, jeżeli użytkownik korzystający z konta znajdującego się w domenie przykład1.microsoft.com używa głównej nazwy użytkownika użytkownik1@przykład1.microsoft.com podczas logowania z komputera znajdującego się w domenie przykład2.microsoft.com, kontroler domeny przykład2.microsoft.com nie będzie mógł odnaleźć konta użytkownika, dlatego skontaktuje się z serwerem wykazu globalnego w celu kontynuacji procesu logowania.
3.	**Dostarczanie informacji dotyczących członkostwa grup uniwersalnych w środowisku wielu domen**	W przeciwieństwie do informacji dotyczących członkostw grup globalnych, które są przechowywane w każdej domenie, członkostwa grup uniwersalnych są przechowywane tylko w wykazie globalnym. Na przykład, jeżeli użytkownik należący do grupy uniwersalnej loguje się w domenie ustawionej na poziomie funkcjonalnym domeny trybu macierzystego systemu Windows 2000 lub wyższym, wykaz globalny dostarcza informacje dotyczące członkostwa grup uniwersalnych dla danego konta użytkownika. Jeżeli wykaz globalny nie jest dostępny podczas logowania użytkownika w domenie uruchomionej na poziomie trybu macierzystego systemu Windows 2000 lub wyższym, komputer wykorzystuje buforowane poświadczenia do logowania użytkownika, który logował się już wcześniej w danej domenie. Użytkownik, który nie logował się jeszcze w danej domenie, może zalogować się wyłącznie na komputerze lokalnym.[14]

Źródło: Active Directory – omówienie techniczne, materiały firmy Microsoft

Wyszukiwanie informacji w katalogu dla użytkowników oraz administratorów jest bardzo proste, ponieważ dostępne jest w menu start i użycia polecenia Wyszukaj. Programy klienckie uzyskują dostęp do informacji przechowywanych w usłudze Active Directory przy użyciu interfejsów usługi ADSI (ang. Active Directory Service Interfaces).

[14] Członkowie grupy Administratorzy domeny mogą logować się w sieci nawet wówczas, gdy wykaz globalny nie jest dostępny.

3.1.4. Narzędzia do administrowania Active Directory

Do wykorzystywania (konfigurowania) tak wielu usług oferowanych przez Active Directory administrator musi mieć do wyboru wiele zaawansowanych narzędzi. Można je podzielić na trzy grupy: **narzędzia graficzne, narzędzia wiersza poleceń oraz narzędzia wsparcia**.

Pierwsza grupa to **narzędzia graficzne** - przystawki do konsoli MMC. (przystawki te możemy w dowolnej kolejności dołączyć do własnej konsoli roboczej)[15]:

- Użytkownicy i komputery Active Directory – pozwala zarządzać komputerami, użytkownikami i grupami;
- Domeny i relacje zaufania Active Directory - umożliwia pracę z domenami, drzewami domen i lasami domen - struktura logiczna sieci;
- Lokacje i usługi Active Directory - zarządza lokacjami i podsieciami, - struktura fizyczna sieci;
- Wynikowy zestaw zasad - umożliwia planowanie zmian i przeglądanie zasad dla użytkowników.

Druga grupa to **narzędzia wiersza poleceń**. Najczęściej wykorzystywanymi programami są[16]:

- adprep - wykonuje wstępne przygotowanie domeny Windows 2000 do zainstalowania domeny Windows Serwer 2003;
- dsadd - dodaje do katalogów obiekty komputerów, kontaktów, grup i użytkowników oraz jednostek organizacyjnych;
- dsget - wyświetla właściwości obiektu podanego w parametrze wywołania;
- dsmod - zmienia właściwości obiektów istniejących w katalogu;
- dsmove - przenosi obiekt w obrębie jednej domeny lub zmienia mu nazwę;
- dsrm - usuwa obiekt z katalogu;
- dsquery - wyszukuje obiekty różnego rodzaju według podanych kryteriów;
- ntdsuti - umożliwia przeglądanie informacji o lokacjach, domenach i serwerach oraz wykonywanie konserwacji bazy danych Active Directory.

Trzecia grupa narzędzi – narzędzia wsparcia zawarte są w Support Tool. Przykładami mogą być[17]:

- adsiedit.msc - umożliwia edycję interfejsu Active Directory dla kontenerów domen;

---

[15] Źródło: http://infojama.pl/177,artykul.aspx - 10.2009r.
[16] Źródło: http://infojama.pl/177,artykul.aspx - 10.2009r.
[17] Źródło: http://infojama.pl/177,artykul.aspx - 10.2009r.

- replmon.exe - umożliwia śledzenie przebiegu replikacji w interfejsie graficznym;
- dsacls.exe - pozwala zarządzać listami kontroli dostępu dla obiektów w katalogu Active Directory;
- dnscmd.exe - pozwala na zarządzanie rekordami stref serwera DNS;
- movetree.exe - przenosi obiekty z jednej domeny do drugiej;
- repadmin - pozwala na monitorowanie replikacji i zarządzanie w trybie wiersza poleceń;
- sdcheck.exe - sprawdza replikacje i poprawność dziedziczenia list kontroli dostępu;
- sidwalker.exe - ustanawia listy kontroli dostępu dla obiektów, uprzednio należących do kont, które zostały usunięte lub wydziedziczone;
- netdom.exe - pozwala na zarządzanie relacjami zaufania i domenami z wiersza poleceń.

3.1.5. Zabezpieczenia Active Directory

Dostęp do jakichkolwiek zasobów Active Directory odbywa się po autoryzacji użytkownika. Funkcje uwierzytelniania logowania i autoryzacji użytkowników są dostępne domyślnie i zapewniają bezpośrednią ochronę dostępu do sieci i zasobów sieciowych. Niespełnienie tego wymogu powoduje brak dostępu do sieci.

Uwierzytelnianie ma podstawowe znaczenie dla komunikacji zabezpieczonej. Użytkownicy muszą mieć możliwość dowiedzenia swojej tożsamości przed osobami, z którymi się komunikują, oraz sprawdzenia tożsamości innych osób. Uwierzytelnianie tożsamości w sieci jest procesem złożonym, ponieważ komunikujące się strony nie spotykają się fizycznie. Nieuczciwej osobie daje to możliwość przechwycenia wiadomości albo podszycia się pod inną osobę lub organizację. Certyfikat cyfrowy jest typowym poświadczeniem, które pozwala sprawdzić tożsamość. W związku z problemem braku fizycznego kontaktu między komunikującymi się stronami, certyfikaty korzystają z technik kryptograficznych. Korzystanie z tych technik ogranicza możliwość przechwycenia, zmiany lub sfałszowania wiadomości przez nieuczciwą osobę. Techniki kryptograficzne utrudniają modyfikowanie certyfikatów. Dzięki temu trudno jest podszyć się pod inną osobę. Dane zawarte w certyfikacie obejmują publiczny klucz kryptograficzny, jeden z pary kluczy - klucza publicznego i prywatnego - podmiotu certyfikatu. Wiadomość podpisana przy użyciu klucza prywatnego jej nadawcy może być zweryfikowana jako autentyczna przez adresata wiadomości przy użyciu klucza publicznego nadawcy. Ten klucz znajduje się w kopii certyfikatu nadawcy. Zweryfikowanie podpisu przy

użyciu klucza publicznego dowodzi, że podpis został utworzony przy użyciu klucza prywatnego podmiotu certyfikatu. Jeśli nadawca był ostrożny i utrzymywał w tajemnicy swój klucz prywatny, adresat może ufać, że tożsamość nadawcy wiadomości jest prawdziwa[18].

Aby uzyskać dostęp do sieci, wystarczy jeden raz zarejestrować się w domenie (lub domenach zaufanych). Gdy usługa Active Directory potwierdzi tożsamość użytkownika, urząd LSA na uwierzytelniającym kontrolerze domeny generuje token dostępu, który określa poziom dostępu użytkownika do zasobów sieciowych. Usługa Active Directory obsługuje wiele bezpiecznych protokołów i mechanizmów uwierzytelniania będących standardami internetowymi używanymi do potwierdzania tożsamości w czasie logowania, w tym Kerberos V5, certyfikaty X.509 v3, karty inteligentne, infrastruktura kluczy publicznych (PKI), opiany w podrozdziale 1.1.1. protokół LDAP (Lightweight Directory Access Protocol) w systemie Windows Server 2003 i wyższym.

Proces uwierzytelniania może dotyczyć nie tylko pojedynczych użytkowników, ale również domen. Zapewniają to opisane w podrozdziale 1.2.1 relacje zaufania. Pozwala to na uwierzytelnianie użytkowników jednej domeny przez kontroler domeny innej domeny.

Logowanie się do sieci użytkowników to nie jedyne zabezpieczenie w Active Directory. Po uwierzytelnieniu użytkownika przez usługę Active Directory, na podstawie praw, które zostały mu przypisane za pomocą grup zabezpieczeń, oraz uprawnień, które zostały przypisane zasobowi udostępnionemu, Active Directory ustalona, do których zasobów użytkownik może uzyskać dostęp. Ten proces autoryzacji chroni zasoby udostępnione przed nieupoważnionym dostępem, zezwalając na dostęp tylko autoryzowanym użytkownikom i grupom.

3.1.6. Zgodność wersji Active Directory

Jak wspomniano na wstępie istnieje wiele wersji Active Directory, które były oferowane wraz z kolejnymi wersjami systemów operacyjnych dedykowanych dla serwerów sieciowych. Przykładem są Windows 2000, Windows Server 2003, czy najnowsza wersja Windows Server 2008.

Rozwój Active Directory powoduje, że dostępne są coraz nowsze i bardziej zaawansowane rozwiązania. Należy jednak pamiętać, że wiele organizacji wykorzystuje wcześniejsze wersje Active Directory i niekoniecznie chce inwestować niemałe środki finansowe w zmianę posiadanego oprogramowania. Dlatego też firma Microsoft, aby zapewnić obsługę (współpra-

[18] http://technet.microsoft.com/pl-pl/library/cc776927(WS.10).aspx – 10.2009r.

cę z) starszych wersji systemów stworzyła cztery poziomy funkcjonalności (w systemie Windows Server 2003), które zostały przedstawione w tabeli 3.7.

Tabela 3.7.

Poziomy funkcjonalności Active Directory

Lp.	Nazwa poziomu funcjonalności	Opis poziomu funkcjonalności
1.	**Windows 2000 mieszany**	1. Obsługuje domeny: – Windows NT, Windows 2000, Windows Serwer 2003. 2. W tym trybie domeny nie mogą korzystać z wielu nowych funkcji oferowanych przez Active Directory, jak np.: grup uniwersalnych, konwersji typów grup, prostego przemianowywania kontrolerów domen, centrum dystrybucji kluczy Kerberos. 3. Kontroler domeny Windows Serwer 2003 pracujący w tym trybie, skonfigurowany jest jako emulator głównego kontrolera domeny i obsługuje dwa protokoły uwierzytelniające: Kerberos (podstawowy mechanizm uwierzytelniania w Windows Serwer 2003) i NTLM[19] (wykorzystywany do uwierzytelnienia komputerów w domenach Windows NT).
2.	**Windows 2000 macierzysty**	1. Obsługuje domeny Windows 2000 i Windows Serwer 2003. 2. Udostępnia większość funkcji Active □irektory za wyjątkiem: – prostego przemianowywania kontrolerów domen; – centrum dystrybucji kluczy Kerberos; – oraz aktualizacji czasu logowania. 3. Nie jest możliwe obniżenie poziomu do trybu mieszanego, mechanizm replikacji NTLM nie jest już obsługiwany. Nie można też przyłączyć żadnego kontrolera domeny Windows NT.
3.	**Windows Server 2003 tymczasowy**	1. Obsługuje domeny: – Windows NT; – Windows Serwer 2003. 2. Ma te same ograniczenia, co tryb Windows 2000 mieszany. 3. Pozwala na aktualizacje domen z Windows NT do Windows Server 2003 z pominięciem szczebla Windows 2000. Aktualizacje należy rozpocząć od głównego kontrolera domeny, a na końcu aktualizować kontrolery zapasowe. Po udanej aktualizacji wszystkich kontrolerów można podnieś poziom funkcjonalności do najwyższego.
4.	**Windows Server 2003**	1. Daje pełny dostęp do funkcji Active □irektory które nie były dostępne na pozostałych poziomach. 2. Nie obsługuje też domen Windows 2000 i Windows NT. Na tym poziomie nie ma możliwości obniżenia poziomu funkcjonalności na niższy. Ten tryb pozwala zmieniać nazwy domen zarządzanych przez Windows Serwer 2003, tworzyć rozszerzone dwukierunkowe relacji zaufania pomiędzy lasami domen, umieszczać domeny na innym poziomie hierarchii.

Źródło: Opracowanie własne na podstawie: http://technet.microsoft.com/pl-pl/library/

[19] NTLM (ang. *NT LAN Manager*) – kryptograficzny protokół sieciowy opracowany przez firmę Microsoft. Źródło: http://pl.wikipedia.org/wiki/NTLM - 10.2009r.

3.1.7. Nowe usługi Active Directory dostępne z Windows Server 2003

Poza wspomnianymi poziomami funkcjonalności zapewniającymi współpracę z wcześniejszymi domenami działającymi na bazie starszych systemów operacyjnych Active Directory dostępny z Windows Server 2003 posiada również zupełnie nowe funkcje usługi Active Directory, przedstawione w poniższej tabeli 3.8.

Na następującej liście podsumowano wybrane funkcje usługi Active Directory, które są dostępne domyślnie na każdym kontrolerze domeny z systemem Windows Server 2003.

Tabela 3.8.

Wybrane nowe usługi Active Directory dostępne z Windows Server 2003.

Lp.	Nazwa usługi	Opis usługi
1.	**Wybieranie wielu obiektów typu użytkownik**	Istnieje możliwość jednoczesnego modyfikowania wspólnych atrybutów wielu obiektów typu użytkownik.
2.	**Funkcja przeciągania i upuszczania**	Obiekty usługi Active Directory można przenosić między kontenerami przez przeciąganie i upuszczanie jednego lub kilku obiektów do żądanej lokalizacji w hierarchii domen. Obiekty można również dodawać do list członkostwa grup, przeciągając i upuszczając jeden lub kilka obiektów (w tym obiektów typu grupa) na grupę docelową.
3.	**Wydajniejsze możliwości wyszukiwania**	Funkcja wyszukiwania jest zorientowana obiektowo i zapewnia wydajniejsze wyszukiwanie, które minimalizuje ruch sieciowy związany z przeglądaniem obiektów.
4.	**Narzędzia wiersza polecenia usługi Active Directory**	Dostępne są nowe polecenia usługi katalogowej do użycia w scenariuszach administracyjnych.
5.	**Partycje katalogu aplikacji**	Istnieje możliwość skonfigurowania zakresu replikacji danych właściwych dla aplikacji między kontrolerami domeny. Można na przykład kontrolować zakres replikacji danych strefy DNS (Domain Name System) w usłudze Active Directory, tak aby w replikacji strefy DNS uczestniczyły tylko określone kontrolery domeny w lesie.
6.	**Zabezpieczony ruch sieciowy LDAP**	Narzędzia administracyjne usługi Active Directory domyślnie podpisują i szyfrują cały ruch sieciowy LDAP. Podpisywanie ruchu sieciowego LDAP gwarantuje, że spakowane dane pochodzą ze znanego źródła i nie zostały po drodze zmienione przez osoby niepowołane. Usługa ta została opisana wcześniej.
7.	**Buforowanie członkostwa grup uniwersalnych**	Buforowanie informacji o członkostwie grup uniwersalnych na uwierzytelniającym kontrolerze domeny eliminuje konieczność lokalizowania wykazu globalnego za pośrednictwem sieci WAN podczas logowania użytkowników.

8.	**Możliwość dodania dodatkowych kontrolerów domeny przy użyciu nośnika kopii zapasowej**	Używając nośnika kopii zapasowej, można skrócić czas dodawania kolejnego kontrolera domeny do istniejącej domeny.
9.	**Przydziały usługi Active Directory**	W usłudze Active Directory można określać przydziały liczby obiektów na danej partycji katalogu, których właścicielem może być użytkownik, grupa lub komputer. Członkowie grup Administratorzy domeny i Administratorzy przedsiębiorstwa są wyłączeni z przydziałów.
10.	**Narzędzie do zmiany nazwy kontrolera domeny**	Nazwy kontrolerów domeny można zmieniać bez konieczności uprzedniego obniżania ich roli.
11.	**Zmienianie nazw domen**	Istnieje możliwość zmiany nazwy dowolnej domeny systemu Windows Server 2003. Możliwość zmiany nazwy dotyczy nazwy NetBIOS lub nazwy DNS dowolnej domeny podrzędnej, domeny nadrzędnej, drzewa domen lub domeny katalogu głównego lasu.
12.	**Inna opcja lokalizacji kont użytkowników i komputerów**	Obecnie istnieje możliwość przekierowania domyślnych lokalizacji kont użytkowników i komputerów utworzonych przez następujące interfejsy programowania aplikacji (API): NetUserAdd, NetGroupAdd i NetJoinDomain. Można przekierowywać lokalizacje kont z kontenerów Użytkownicy i komputery do jednostek organizacyjnych, gdzie mogą być zastosowane ustawienia zasad grupy.
13.	**Kontrola dostępu użytkowników do zasobów między domenami i lasami**	Istnieje możliwość zablokowania dostępu użytkowników w domenie lub lesie do zasobów w innej domenie lub lesie, a następnie selektywnego udzielania dostępu przez ustawienie dla określonych zasobów lokalnych wpisu kontroli dostępu (ACE) zezwalającego na uwierzytelnienie określonych obiektów typu użytkownik lub grupa.
14.	**Zaufanie lasu**	Utworzenie relacji zaufania między lasami pozwala na rozszerzenie zakresu przechodniości dwukierunkowej z jednego lasu na inny.
15.	**Restrukturyzacja lasu**	Istniejące domeny można przenosić do innych lokalizacji w hierarchii domen.
16.	**Dezaktywacja obiektów schematu**	Niepotrzebne klasy i atrybuty można dezaktywować w schemacie.
17.	**Dynamiczne klasy pomocnicze**	Ta funkcja zapewnia obsługę dynamicznego łączenia klas pomocniczych z poszczególnymi obiektami, a nie wyłącznie z całymi klasami obiektów. Ponadto klasy pomocnicze, które zostały dołączone do danego wystąpienia obiektu, mogą być następnie usunięte z tego wystąpienia.
18.	**Usprawnienia replikacji**	Replikacja wartości połączonych umożliwia replikowanie w sieci poszczególnych członków grupy zamiast traktowania całego członkostwa grupy jako jednego obiektu replikacji. Aby uzyskać więcej informacji o replikacji wartości połączonych, zobacz Jak działa replikacja. Ponadto nowe algorytmy rozszerzania drzewa zwiększają wydajność i skalowalność replikacji, rozszerzając jej zakres na większą liczbę domen i lokacji zarówno w lesie systemu Windows 2000, jak i Windows Server 2003.
19.	**Usprawnienia replikacji wykazu globalnego**	Stan synchronizacji wykazu globalnego jest zachowywany, nawet jeśli jakaś czynność administracyjna prowadzi do rozszerzenia częściowego zestawu atrybutów. Minimalizuje to ruch sieciowy replikacji wynikający z rozszerzenia częściowego zestawu atrybutów, ponieważ przesyłane są tylko te atrybuty, które zostały dodane.

Źródło: Opracowanie własne na podstawie: http://technet.microsoft.com/pl-pl/library/

3.2. DNS (*ang. Domain Name System*)

Podobne znaczenie dla sprawnego korzystania z sieci ma rozwiązanie DNS. Najprostszym wytłumaczeniem działania DNS jest tłumaczenie nazwy hosta na adres IP, który ma przypisany w sieci. Dzięki temu nie trzeba znać adresu IP hosta, z którym chcemy się połączyć. Wystarczy znać jego nazwę. Przykładem może być codzienne wykorzystanie Internetu – chcąc połączyć się z portalem informacyjnym, np. Wirtualną Polską, Interią, wystarczy wpisać nazwę strony tej witryny – www.wp.pl. www.interia.pl. Gdyby nie było usługi DNS, aby uzyskać połączenie użytkownik zmuszony byłby do wpisania adresu IP tych serwerów portali. Byłoby to znaczące utrudnienie korzystania z sieci. Inną definicję DNS można przytoczyć za „Vademecum Teleinformatyka" cz.3: „ DNS (ang. Domain Name Server[20]) jest serwerem (oprogramowaniem) pracującym w sieciach standardu TCP/IP, który świadczy zgłaszającym się do niego klientom konkretną usługę: dołącza adres IP do nazwy stanowiska pracy podanego przez klienta. Użytkownik korzystający z usług Internetu nie musi więc znać adresów IP (co jest bardzo kłopotliwe, ponieważ adresy IP składają się z" czterech oktetów – w zapisie dziesiętnym są to liczby z zakresu 0-255), „a może stosować wyłącznie nazwy komputerów, drukarek, oraz wszystkich urządzeń pracujących w Internecie."[21]

DNS został zaprezentowany publicznie w 1984 roku, choć historia tego rozwiązania zaczyna się znacznie wcześniej. Tak jak w większości przypadków, tak i tu, rozwiązanie to stworzono na zlecenie Departamentu Obrony Stanów Zjednoczonych. Początkowo polegało to na tym, że nazwy komputerów podłączonych do sieci były przechowywane w pliku Hosts, który znajdował się w centralnym serwerze. Każdy użytkownik sieci, który chciał rozwinąć nazwę innego użytkownika pobierał ten plik z tego głównego serwera. To rozwiązanie funkcjonowało dobrze do czasu, gdy sieć była mała, a liczba użytkowników nie była zbyt duża. Rozwój sieci spowodował, że obciążenie sieci spowodowane ściąganiem tego pliku jak również jego rozmiar wzrósł do tego stopnia, że twórcy musieli pomyśleć nad modernizacją rozwiązania. Kolejnym krokiem w rozwoju DNS było utworzenie bazy danych, w której przechowywane były nazwy hostów w sieci. Dane te były przechowywane na wielu serwerach, które były rozmieszczone w sieci w sposób hierarchiczny, co pozwoliło na zmniejszenie obciążenia sieci spowodowanego pobieraniem pliku Hosts.

---

[20] W literaturze można spotkać sie z dwoma rozwinięciami skrótu DNS -Domain Name Server oraz Domain Name System. Autor uważa, że obie nazwy można traktować jako równorzędne i obowiązujące.
[21] Vademecum teleinformatyka, cz.3, IDG Poland S.A. 2004r., s.17.

Obecnie DNS opiera się na hierarchicznej, rozproszonej bazie danych, przechowującej dane różnego typu, w tym nazwy hostów oraz nawy domen. Nazwy przechowywane w bazie danych DNS to tekst oddzielony kropką, np. www.wp.pl, czy www.aon.edu.pl. Końcówka nazwy każdego z hostów nie jest przypadkowa i podlega ścisłym regułom. Dzięki nim możliwe jest określenie dokładnej lokalizacji hosta w całej sieci. Dla przykładu, w przytoczonym adresie Akademii Obrony Narodowej: www.aon.edu.pl aon oznacza domenę funkcjonalną należącą do uczelni, edu domenę organizacji, a pl polską domenę w sieci. Najważniejsza domena (najwyższego poziomu) zawsze zapisywana jest w nazwie jako ostatnia. W przypadku powyższego przykładu widać, że domena .pl jest ważniejsza od domeny .edu, która z kolei jest wyżej w hierarchii domen DNS od domeny .aon. W ten sposób możliwe jest budowanie hierarchii nazw, które porządkują Internet.

3.2.1. Struktura domen DNS

DNS składa się z kilku poziomów domen, uporządkowanych w sposób hierarchiczny. Nazwy domen najwyższego poziomu zostały zdefiniowane w zgodzie z dokumentem International Standard 3166 (IS 3166). W tabeli poniżej przedstawiono nazwy najwyższego poziomu, przypisane organizacjom oraz państwom.

Tabela 3.9.

Wybrane najważniejsze nazwy domen zawartych w IS 3166

Lp.	Nazwa domeny DNS	Organizacje wykorzystujące domenę
1.	**.com**	Organizacje komercyjne (ang. commercial organizations)
2.	**.org**	Organizacje nie przynoszące zysków (ang. Non-profit organizations)
3.	**.gov**	Pozawojskowe organizacje rządowe (ang. Non-military government organizations)
4.	**.edu**	Instytucje dydaktyczno-naukowe (ang. Educational institutions)
5.	**.net**	Organizacje sieciowe (ang. Networks – the backbone of the Internet)
6.	**.mil**	Organizacje wojskowe (ang. Military government organizations)
7.	**.xx**[22]	Dwuliterowy kod państwa (ang. Two letter country code), np. .pl – Polska, .dk – Dania, .fr – Francja, itd.

Źródło: opracowanie własne na podstawie: http://www.iana.org/domains/root/db/ oraz http://technet.microsoft.com/pl-pl/library/bb742582(en-us).aspx

[22] Pełna lista kodów państw jest dostępna na stronie: http://www.iana.org/domains/root/db/

Więcej na temat nazw domen najwyższego poziomu oraz najnowszych rozwiązań tym zakresie dostępne jest na oficjalnej stronie organizacji: http://www.icann.org/.

Za nadzór nad domenami odpowiadają organizacje do tego celu wyznaczone. Na najwyższym poziomie działają dwie instytucje – IANA[23] i ICANN[24]. Nadzorują one ogólne zasady przyznawania nazw domen i adresów IP. Ich zadanie nie polega jednak na kontaktowaniu się z poszczególnymi chętnymi do uzyskania nazwy domeny, tylko na rozdzielaniu domeny najwyższego poziomu (takich jak .pl, .gov, .com, .eu) pomiędzy kraje lub wybrane organizacje jak również przekazaniu im praw do zarządzania tymi domenami. Wyznaczone organizacje mają możliwość dobierać partnerów, czyli inne organizacje wspomagające, którym delegowane jest prawo do nadzoru nad całością bądź częścią swoich domen. Dla przykładu w Polsce organizacją odpowiedzialną za nadzór nad domeną .pl jest wyznaczone przez Rząd Rzeczypospolitej Polskiej Naukowa i Akademicka Sieć Komputerowa (NASK), która rozdziela poddomeny w obrębie domeny .pl pomiędzy zainteresowanych, jak również przekazuje nadzór nad częścią domen swoim partnerom. Ci z kolei mogą rozdzielać te domeny pomiędzy poszczególne komputery, lub dalej swoim klientom. W obrębie domeny można tworzyć poddomeny. I tak w domenie .pl można stworzyć poddomenę .rembertow (pełna nazwa .rembertow.pl).

W wielu krajach domena internetowa przyznana przez system DNS staje się własnością tego, kto pierwszy ją kupi. W Polsce jest ona tylko wynajmowana na określony czas.

---

[23] IANA (ang. *Internet Assigned Numbers Authority*) to organizacja, która odpowiedzialna jest za uporządkowanie nazewnictwa stosowanego w nazwach domen i adresach IP komputerów przyłączonych do Internetu. Początkowo IANA była jedną z grup roboczych IETF, zajmującej się stworzeniem standardów przyznawania numerów IP. Z czasem powstała konieczność powstania instytucji, która będzie na co dzień zarządzała zasadami przyznawania numerów IP i nazw domen kolejnym użytkownikom. To zadanie spełniała długi czas właśnie IANA, która mimo że nie była od strony prawnej sformalizowana, dostała od rządu USA uprawnienia do zarządzania domenami, ponieważ nie było wówczas innej instytucji, która mogła tego dokonać. Na podstawie umowy z rządem USA większość codziennej pracy przy przyznawaniu numerów IP oraz zarządzaniu domenami najwyższego poziomu została ostatecznie przekazana organizacji ICANN, której autonomiczną częścią jest właśnie IANA. Do zadań IANA należy obecnie tylko zarządzanie domenami najwyższego poziomu oraz ogólny nadzór nad działaniem mechanizmu DNS – źródło: Opracowanie własne na podstawie: http://pl.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority

[24] ICANN - Internetowa Korporacja ds. Nadawania Nazw i Numerów (ang. *The Internet Corporation for Assigned Names and Numbers*) to instytucja odpowiedzialna obecnie za przyznawanie nazw domen internetowych, ustalanie ich struktury oraz za ogólny nadzór nad działaniem serwerów DNS na całym świecie. Powstała 18.09.1998 r. w celu przejęcia od rządu USA funkcji nadzorowania technicznych aspektów Internetu. Formalnie ICANN jest prywatną organizacją non-profit, o statusie firmy zarejestrowanej w stanie Kalifornia, której rząd USA przekazał czasowo prawo nadzoru nad systemem DNS, przydziałem puli adresów IPv4 oraz IPv6 dla tzw. Regional Internet Registries RIR oraz rejestracją numerów portów. W ramach ICANN prowadzi się też dyskusje na temat tworzenia nowych domen najwyższego poziomu (TLD, ang. *Top Level Domains*), czyli np: .gov, .edu, itp. Do zadań ICANN należy m.in.: administrowanie adresami IP zarządzanie domenami i serwerami DNS najwyższego poziomu (root) przyznawanie parametrów protokołom internetowym – źródło: Opracowanie własne na podstawie: http://pl.wikipedia.org/wiki/ICANN

Jeżeli ktoś zrezygnuje ze swojej domeny i zwróci ją administratorowi DNS, może ona trafić w inne ręce[25].

Organizacje odpowiedzialne za domeny DNS na świecie przedstawiono w poniższej tabeli 3.10., natomiast tabela 3.11. przedstawia przykładowe organizacje odpowiedzialne za domeny DNS w Polsce.

Tabela 3.10.

Przykładowe organizacje odpowiedzialne za domeny DNS na świecie

Lp.	Nazwa organizacji	Nadzór nad domeną:
1.	ICANN-IANA	nadzór ogólny nad nazewnictwem i strukturą domen najwyższego poziomu (TLD – ang. *Top Level Domains*), np.: .no, .gov, .com, itp.
2.	VERISIGN GLOBAL REGISTRY SERVICES	rejestracja i nadzór nad domenami: .net, .org,
3.	NEULEVEL	rejestracja i nadzór nad domeną – .biz
4.	IEEE	rejestracja i nadzór nad domeną – .aero
5.	AFILIAS LIMITED	rejestracja i nadzór nad domeną – .info
6.	Global Name Registry	rejestracja i nadzór nad domeną – .name
7.	EurID	rejestracja i nadzór nad domeną – .eu

Źródło: opracowanie własne na podstawie: http://pl.wikipedia.org/wiki/DNS.

[25] Patrz: **http://www.dmoz.org/World/Polski/Komputery/Internet/Domeny/**

Tabela 3.11.

Przykładowe organizacje odpowiedzialne za domeny DNS w Polsce

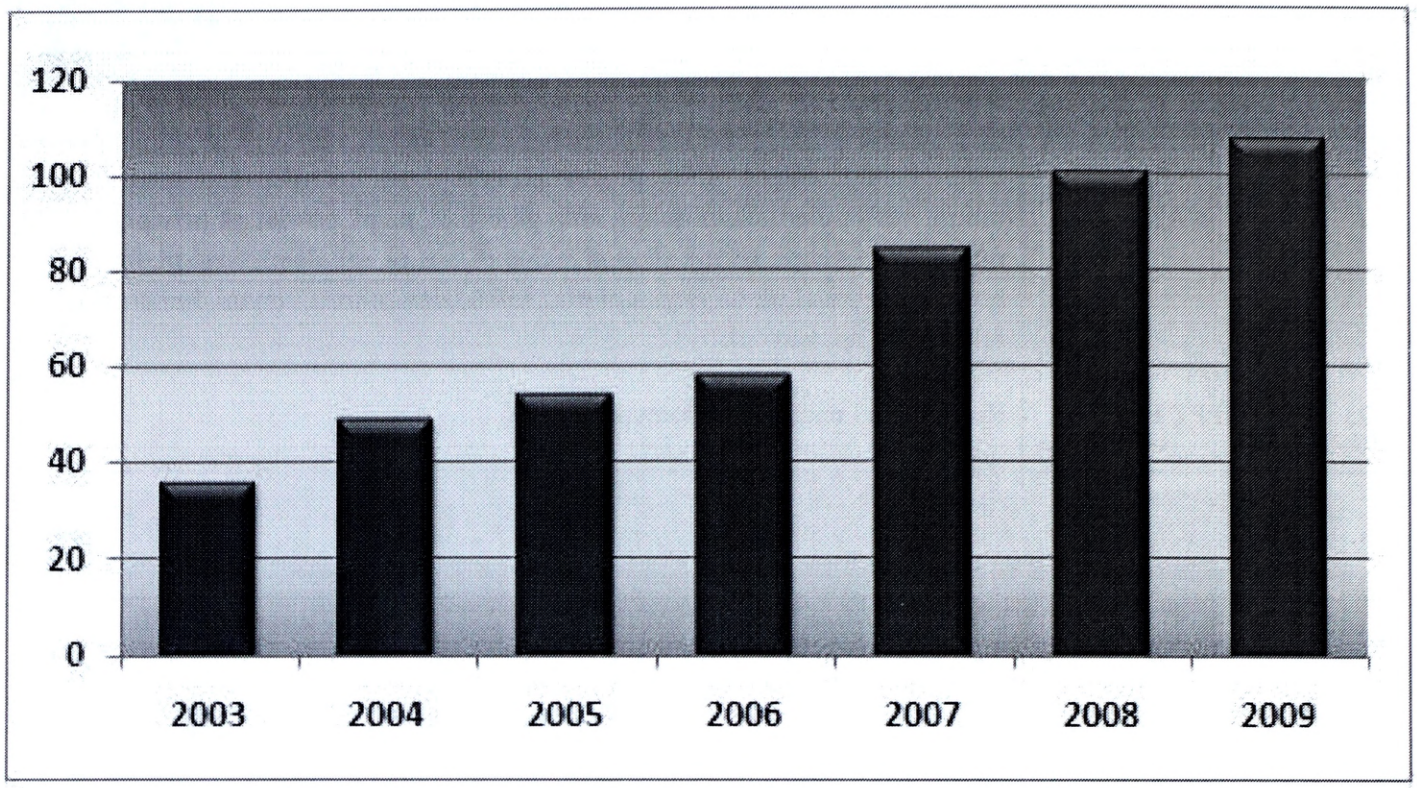
Lp.	Nazwa organizacji	Nadzór nad domeną:
1.	NASK	Nadzór nad domeną .pl jako całością, obsługa rejestrowania domen drugiego poziomu – domen funkcjonalnych, m.inn.: aid.pl, agro.pl, atm.pl auto.pl, biz.pl, com.pl, edu.pl, gmina.pl ,gsm.pl, info.pl, mail.pl, miasta.pl, media.pl, mil.pl, net.pl, nieruchomosci.pl, nom.pl, org.pl, pc.pl, powiat.pl, priv.pl, realestate.pl, rel.pl, sex.pl, shop.pl, sklep.pl, sos.pl, szkola.pl, targi.pl, tm.pl, tourism.pl, travel.pl, turystyka.pl oraz kilkudziesięcioma innymi domenami lokalnymi, np. waw.pl.
2.	IPPT PAN	Rejestracja i nadzór nad domeną .gov.pl;
3.	ICM	Rejestracja i nadzór nad domenami: .art.pl, .mbone.pl;
4.	Stowarzyszenie Klon/Jawor	Rejestracja i nadzór nad domeną –.ngo.pl; .aero
5.	TASK	Rejestracja i nadzór nad domenami: . med.pl, .gda.pl, .gdansk.pl, .gdańsk.pl, .sopot.pl, .gdynia.pl;
6.	SGH	Rejestracja i nadzór nad domeną – .irc.pl
7.	Politechnika Wrocławska	Rejestracja i nadzór nad domeną – .usenet.pl.

Źródło: opracowanie własne na podstawie: http://www.dns.pl/rejestracja-domen.html#1 oraz http://pl.wikipedia.org/wiki/DNS.

Poza wymienionymi organizacjami nadzorującymi domeny DNS w Polsce wiele domen typu nazwa-firmy.pl zostały wykupione od NASK przez rozmaite firmy, które w imieniu NASK zarządzają tymi domenami we własnym zakresie.

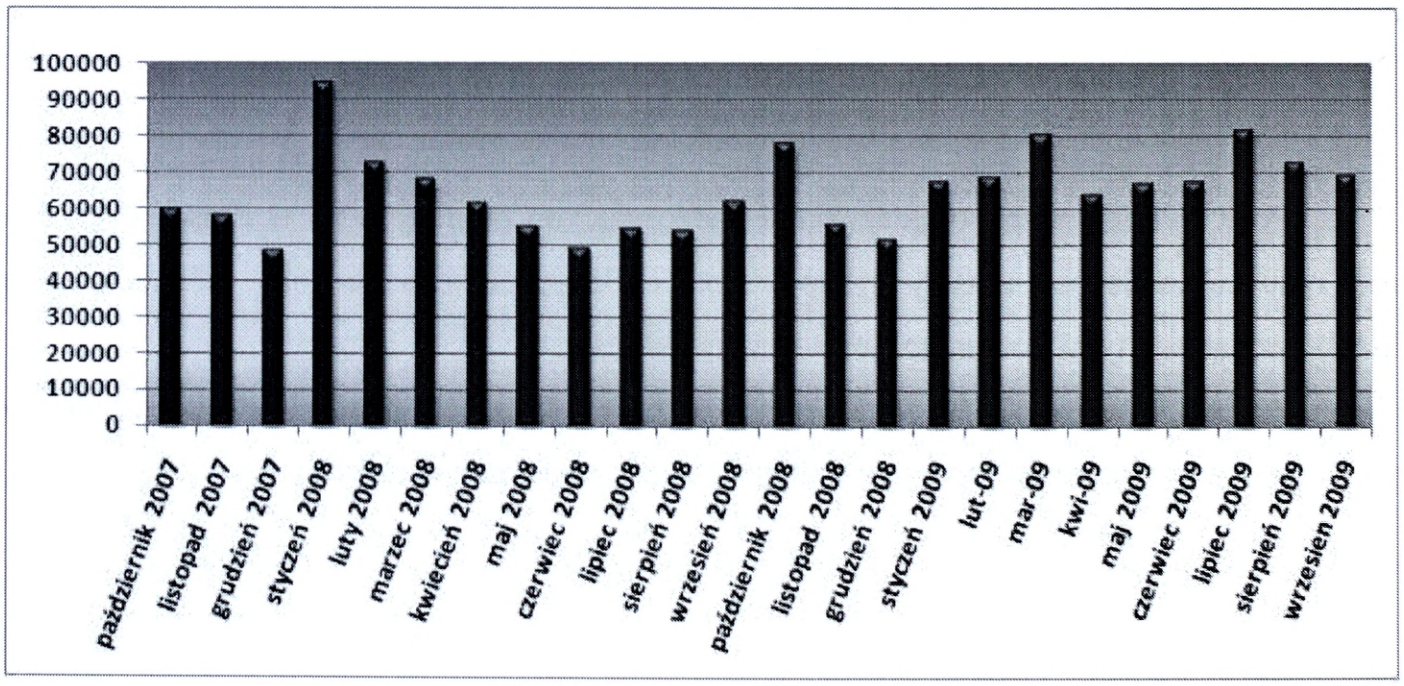
Poniżej, na rys. 3.2. przedstawiono liczbę partnerów NASK administrujących domenami w Polsce, natomiast rys. 3.3. przedstawia liczbę rejestrowanych domen.

Liczba akredytowanych partnerów NASK (rocznie)



Rys.3.2. Liczba akredytowanych partnerów NASK.
Źródło: http://www.dns.pl/essentials_pl.html

Liczba nowych rejestracji nazw domen .pl (miesięcznie)



Rys.3.3. Liczba nowych rejestracji nazw domen .pl w NASK
Źródło: http://www.dns.pl/essentials_pl.html

Lista partnerów NASK znajduje się na stronie: http://dns.pl/porozumienie/partner.html natomiast dokładne informacje o rejestracji domen .pl można znaleźć pod adresem: http://dns.pl/index.html

3.2.2. Nazewnictwo domen DNS

Stosowanie narodowych znaków diakrytycznych w nazwach domen było do niedawna całkowicie zabronione. Jednakże wraz z pojawieniem się uaktualnienia IDN (ang. Internationalized Domain Name)[26] Ograniczeniem tego rozwiązania jest możliwość korzystania w nazwie domeny jedynie z jednego zestawu znaków narodowych, co oznacza, że nie można zastosować w nazwie jednej domeny znaków narodowych polskich i np. greckich.

Tabela 3.12.

Zasady rejestrowania w Polsce nazw zawierających narodowe znaki diakrytyczne, zgodne z IDN (ang. Internationalized Domain Name) w NASK

Lp.	Znaki narodowe w nazwach domen w NASK
1.	Od dnia 11.09.2003 dopuszcza się rejestrowanie domen z prefiksem "xn--" w strefie .pl, a dnia 18.09.2003 w pozostałych strefach obsługiwanych przez NASK.
2.	Przesłana nazwa domenowa zaczynająca się ciągiem znaków "xn--" musi być przygotowana zgodnie z dokumentami organizacji IETF (www.IETF.org) oznaczonych jako RFC 3490, RFC 3491, RFC 3492.
3.	Przesłana do rejestracji nazwa domenowa zaczynająca się ciągiem znaków "xn--", po przekodowaniu za pomocą operacji ToUnicode (zgodnie z RFC 3490) może jedynie zawierać znaki pochodzące tylko i wyłącznie z jednego z zestawów zdefiniowanych w dokumencie znaki_narodowe_-_zestawy.pdf. Mieszanie znaków pochodzących z różnych zestawów jest niedozwolone.
4.	Nazwa domeny w kodzie ASCII z prefiksem "xn--" jest rejestrowana zgodnie ze standardem IDNA (RFC 3490). NASK nie odpowiada za skutki przyjęcia, za powszechnie obowiązujący na świecie, innego standardu niż stosowany w dniu zarejestrowania danej nazwy domeny. Rejestrując nazwę domeny w kodzie ASCII z prefiksem "xn--" zgadzasz się na korzystanie z usługi oferowanej przez NASK z zastrzeżeniem, o którym mowa w zdaniu poprzedzającym

Źródło: opracowanie własne na podstawie: http://dns.pl/IDN/info.html

[26] IDN – (ang. Internationalized Domain Name) nazwy domen zawierające znaki spoza ASCII, m.in. narodowe znaki diakrytyczne (np. używane w języku polskim ą, ę, ó, ś, ł, ż, ź, ć, ń). W związku z tym, że system nazw domenowych opiera się na siedmiobitowych znakach standardu ASCII, wielojęzyczne nazwy domen internetowych są przekształcane z formy zapisanej w Unikodzie do znaków siedmiobitowych opierając się na sposobie zapisu zwanym Punycode, opisanym w RFC 3490 – źródło: http://pl.wikipedia.org/wiki/ Internationalized_Domain_Name . W przypadku zastosowania narodowych znaków diakrytycznych w nazwie domeny, np. Rembertów, jego tłumaczenie na nazwę domeny zgodnej z kodami ASCII przyjmuje postać: xn--rembertw-13a.

Standard IDN jest obsługiwany przez następujące programy[27]:

- Dla systemów operacyjnych z rodziny Windows:
  - Firefox 0.6 lub wyższa;
  - Internet Explorer 5.0 lub wyższa + i-NavTM plug-in;
  - Internet Explorer 7;
  - Mozilla 1.4 lub wyższa;
  - Netscape Navigator 7.1 lub wyższa;
  - Opera 7.11 lub wyższa;
  - Microsoft Outlook and Outlook Express + VeriSign i-NavTM plug-in.
- Dla systemów operacyjnych Mac OS X:
  - Camino Version: 0.7 lub wyższa
  - Firefox 0.6 lub wyższa
  - Mozilla 1.4 lub wyższa
  - Netscape Navigator 7.1 lub wyższa
  - Opera 7.11 lub wyższa
  - Safari 1.2 lub wyższa
- Dla systemów LINUX:
  - Epiphany 1.2.2 lub wyższa (Gnome)
  - Firefox 0.6 lub wyższa
  - Galeon 1.3.14 lub wyższa (Gnome)
  - Konqueror 3.2 lub wyższa (KDE)
  - Mozilla 1.4 lub wyższa
  - Netscape Navigator 7.1 lub wyższa
  - Opera 7.11 lub wyższa
  - Mutt 1.4.1 lub wyższa

Pomimo możliwości używania w nazwach domen znaków narodowych w praktyce nie spotyka się ich w Internecie. Nazewnictwo domen ogranicza się najczęściej do znaków ASCII, czyli w przypadku nazwy domeny .rembertów.pl najczęściej nadano by nazwę .rembertow.pl z pominięciem polskiego znaku diatrytycznego.

[27] Źródło: http://dns.pl/IDN/programy.html

3.2.3. Techniczna organizacja DNS

Podstawą technicznego systemu DNS jest ogólnoświatowa sieć serwerów przechowujących informacje na temat adresów domen. Każdy wpis zawiera nazwę oraz odpowiadającą jej wartość, najczęściej adres IP. System DNS jest podstawą działania Internetu[28].

DNS to również protokół komunikacyjny opisujący sposób łączenia się klientów z serwerami DNS. Częścią specyfikacji protokołu jest również zestaw zaleceń, jak aktualizować wpisy w bazach domen internetowych. Na świecie jest wiele serwerów DNS, które odpowiadają za obsługę poszczególnych domen internetowych. Domeny mają strukturę drzewiastą, na szczycie znajduje się 13 głównych serwerów[29] (root servers) obsługujących domeny najwyższego poziomu (TLD – top level domains), których listę z ich adresami IP można pobrać z ftp://ftp.rs.internic.net/domain/named.root. Posiadają one nazwy od a.root-servers.net do m.root-servers.net. Nie może być ich więcej, ograniczenie wynika z tego, że pojedynczy pakiet UDP o standardowej wielkości 1500 bajtów mieści właśnie informacje o maksymalnie 13 serwerach. Ponieważ główne serwery DNS są podstawą działania Internetu i otrzymują ogromne ilości zapytań, zostały one skopiowane. Kopie głównych serwerów umieszczone są w różnych częściach świata (posiadają te same adresy IP co serwery główne). Użytkownicy z reguły łączą się z najbliższym im serwerem. Przykładowo serwer k.root-servers.net zarządzany przez organizację RIPE NCC umieszczony jest w Amsterdamie, Londynie, Tokio, Delhi oraz Miami[30].

Serwery najwyższego poziomu z reguły posiadają tylko odwołania do odpowiednich serwerów DNS odpowiedzialnych za domeny niższego rzędu, np. serwery główne (obsługujące między innymi TLD .com) „wiedzą", które serwery DNS odpowiedzialne są za domenę example.com. Serwery DNS zwracają nazwę serwerów odpowiedzialnych za domeny niższego rzędu. Możliwa jest sytuacja, że serwer główny odpowiada, że dane o domenie example.com posiada serwer dns.example.com. W celu uniknięcia zapętlenia w takiej sytuacji serwer główny do odpowiedzi dołącza specjalny rekord (tak zwany glue record) zawierający także adres IP serwera niższego rzędu (w tym przypadku dns.example.com)[31].

Rozproszona baza informacji DNS ma strukturę odwróconego drzewa. Każda nazwa domenowa jest konstruowana w trakcie podróży przez węzły po ścieżce drzewa w stronę jego korzenia. Każdy węzeł posiada etykietę tekstową o długości maksymalnie 63 znaków; wyjąt-

---

[28] Źródło, patrz: http://pl.wikipedia.org/wiki/DNS
[29] Mapa rozmieszczenia serwerów DNS oraz szczegółowy opis serwerów głównych można znaleźć również na stronie: http://www.root-servers.org/
[30] Źródło, patrz: http://pl.wikipedia.org/wiki/DNS
[31] Tamże.

kiem jest węzeł główny identyfikowany pustą etykietą. Poszczególne nazwy na ścieżce oddziela się kropkami. Domena jest poddrzewem w przestrzeni nazw domenowych, a jej nazwę stanowi nazwa węzła znajdującego się u szczytu poddrzewa. Nazwy domenowe będące liśćmi drzewa DNS reprezentują zwykle hosty, jak również informacje na temat hosta oraz o trasowaniu poczty. Nazwy w głębi drzewa identyfikują dodatkowo domenę[32]. W tabeli 3.13., przedstawione zostały wybrane cechy techniczne DNS.

Decentralizacja DNS została osiągnięta dzięki delegowaniu domen. Delegowanie polega na przekazaniu zwierzchności nad całością bądź częścią danej domeny innej organizacji. Proces ten może być powtarzany wielokrotnie, zatem organizacja obsługująca oddelegowaną domenę może dalej oddelegować jej część. Domeny najwyższych poziomów podzielone są z reguły na strefy. Strefa to w istocie mniejsza jednostka stanowiąca fragment domeny[33].

Serwer nazw to program pracujący na hoście internetowym, który umożliwia dostęp do informacji DNS zawartej w plikach danych strefowych. Standard DNS definiuje dwa rodzaje serwerów nazw. Podstawowy serwer (ang. Primary Name Server - PNS) ładuje dane strefowe z plików znajdującego się w jego hoście. Serwer wtórny (ang. Secondary Name Server - SNS) pobiera dane strefowe z serwera autorytatywnego dla danej strefy, zwykle podstawowego, ale równie dobrze może być to inny autorytatywny serwer wtórny[34].

[32] Źródło: https://www.dns.pl/dnssec/theory_intro.html
[33] Źródło: https://www.dns.pl/dnssec/theory_intro.html.
[34] Źródło: https://www.dns.pl/dnssec/theory_intro.html.

Tabela 3.13.

Wybrane, główne cechy techniczne DNS

Lp.	Cechy DNS
1.	Nie ma jednej centralnej bazy danych adresów IP i nazw. Podstawą DNS jest 13 głównych serwerów rozrzuconych na różnych kontynentach, odpowiedzialnych za domeny najwyższego poziomu.
2.	Informacja przechowywana na serwerach DNS ogranicza się tylko do wybranych domen.
3.	Stosuje się nadmiarowość, tzn. każda domena powinna mieć co najmniej 2 serwery DNS obsługujące ją, po to, aby nastąpiła awaria jednego z serwerów, to drugi będzie może przejąć jego zadanie.
4.	Każda domena posiada jeden główny dla niej serwer DNS (tzw. master), który przechowuje konfigurację tej domeny, wszystkie inne serwery obsługujące tą domenę są typu slave i dane dotyczące tej domeny pobierają automatycznie z jej serwera głównego. Podobnie się dzieje po każdej zmianie zawartości domeny.
5.	Serwery DNS mogą przechowywać przez pewien czas odpowiedzi z innych serwerów (ang. caching), a więc proces zamiany nazw na adresy IP jest często krótszy niż w podanym przykładzie.
6.	Rozwiązaniem pozwalającym na przyspieszenie odpowiedzi na zapytanie o rozwinięcie nazwy jest przechowywanie przez nie (serwery DNS)przez pewien określony czas odpowiedzi z innych serwerów (ang. caching).
7.	Na dany adres IP może wskazywać wiele różnych nazw. Na przykład na jeden adres IP mogą wskazywać nazwy http://www.microsoft.com/pl/PL/default.aspx oraz http://www.microsoft.com/en/us/default.aspx. różnica w tym wypadku będzie polegała na języku, w jakim zostanie zaprezentowana treść strony.
8.	Możliwa jest również sytuacja odwrotna, tj. czasami pod jedną nazwą może kryć się więcej niż 1 adres IP po to, aby jeśli jeden z nich zawiedzie, inny mógł spełnić jego rolę.
9.	Kolejnym ułatwieniem dla administratorów poszczególnych serwerów jest możliwość dokonania w serwerze DNS obsługującym domenę poprawki poprzez zmianę wpisu, w przypadku, gdy z jakichś powodów musimy przenieść serwer WWW na inny szybszy komputer, z lepszym łączem, ale z innym adresem IP.
10.	Protokół DNS posługuje się do komunikacji serwer-klient głównie protokołem UDP[35], serwer pracuje na porcie numer 53, przesyłanie domeny pomiędzy serwerami master i slave odbywa się protokołem TCP[36] na porcie 53

Źródło: opracowanie własne na podstawie: http://pl.wikipedia.org/wiki/DNS

---

[35] UDP (ang. *User Datagram Protocol* – Datagramowy Protokół Użytkownika) – jeden z podstawowych protokołów internetowych. Umieszcza się go w warstwie czwartej (transportu) modelu OSI. Jest to protokół bezpołączeniowy, więc nie ma narzutu na nawiązywanie połączenia i śledzenie sesji (w przeciwieństwie do TCP). Nie ma też mechanizmów kontroli przepływu i retransmisji. Korzyścią płynącą z takiego uproszczenia budowy jest większa szybkość transmisji danych i brak dodatkowych zadań, którymi musi zajmować się host posługujący się tym protokołem. Z tych względów UDP jest często używany w takich zastosowaniach jak wideokonferencje, strumienie dźwięku w Internecie i gry sieciowe, gdzie dane muszą być przesyłane możliwie szybko, a poprawianiem błędów zajmują się inne warstwy modelu OSI. Przykładem może być VoIP lub protokół DNS. UDP udostępnia mechanizm identyfikacji różnych punktów końcowych (np. pracujących aplikacji, usług czy serwisów) na jednym hoście dzięki *portom* (porównaj: gniazdo). UDP zajmuje się dostarczaniem pojedynczych pakietów, udostępnionych przez IP, na którym się opiera. Kolejną cechą odróżniającą UDP od TCP jest możliwość transmisji do kilku adresów docelowych na raz (tzw. multicast). Pakiety UDP (zwane też *datagramami*) zawierają oprócz nagłówków niższego poziomu nagłówek UDP. Składa się on z pól zawierających sumę kontrolną, długość pakietu oraz porty: źródłowy i docelowy. Podobnie jak w TCP, porty UDP zapisywane są na dwóch bajtach (szesnastu bitach), więc każdy adres IP może mieć przypisanych 65536 różnych zakończeń. Z przyczyn historycznych, porty 0-1023 zarezerwowane są dla dobrze znanych usług sieciowych – dla aplikacji użytkownika przydziela się porty od 1024. Źródło: http://pl.wikipedia.org/wiki/UDP

[36] TCP (ang. Transmission Control Protocol – protokół kontroli transmisji) – strumieniowy protokół komunikacji między dwoma komputerami. Został stworzony przez Vintona Cerfa i Roberta Kahna.
Jest on częścią większej całości określanej jako stos TCP/IP. W modelu OSI TCP odpowiada warstwie transportowej. TCP jest protokołem działającym w trybie klient-serwer. Serwer oczekuje na nawiązanie połączenia na określonym porcie. Klient inicjuje połączenie do serwera. W przeciwieństwie do UDP, TCP gwarantuje wyższym warstwom komunikacyjnym dostarczenie wszystkich pakietów w całości, z zachowaniem kolejności i bez duplikatów. Zapewnia to wiarygodne połączenie kosztem większego narzutu w postaci nagłówka i większej liczby przesyłanych pakietów. Chociaż protokół definiuje pakiet TCP, to z punktu widzenia wyższej warstwy oprogramowania, dane płynące połączeniem TCP należy traktować jako ciąg oktetów. W szczególności – jednemu wywołaniu funkcji API (np. send()) nie musi odpowiadać wysłanie jednego pakietu. Dane z jednego wywołania mogą zostać podzielone na kilka pakietów lub odwrotnie – dane z kilku wywołań mogą zostać połączone i wysłane jako jeden pakiet (dzięki użyciu algorytmu Nagle'a). Również funkcje odbierające dane (recv()) w praktyce odbierają nie konkretne pakiety, ale zawartość bufora stosu TCP/IP, wypełnianego sukcesywnie danymi z przychodzących pakietów. Źródło: http://pl.wikipedia.org/wiki/TCP_(protok%C3%B3%C5%82)

3.2.4. Budowa i sposób działania protokołu DNS

Protokół DNS opiera się na zapytaniach i odpowiedziach, które przesyłane są w pakietach UDP. Warunkiem jest spełnienie warunku, że zapytanie lub odpowiedź, zwane komunikatami DNS, mieszczą się w całości w jednym pakiecie UDP, czyli standardowo 512 oktetów, jednakowoż wielkość tę można zmieniać pamiętając również o ustawieniu takiej samej wielkości w MTU (ang. Maximum Transmission Unit). W innym przypadku komunikat DNS przesyłany jest protokołem TCP i poprzedzony dwubajtową wartością określającą długość zapytania i długość odpowiedzi (bez wliczania tych dwóch bajtów). Format komunikatu DNS został zdefiniowany w RFC 1035.

Poniżej zostaną zaprezentowane rodzaje zapytań (patrz tabela 3.14.) oraz odpowiedzi (patrz tabela 3.15.), wykorzystywanych w protokole DNS.

Tabela 3.14.

Rodzaje zapytań stosowanych w protokole DNS

Lp.	Nazwa zapytania	Opis zapytania:
1.	Rekurencyjne	Powodują, że serwer poszukuje zadanej w zapytaniu wymaganej informacji lub zwrócenia wiadomości o błędzie. Zapytania rekurencyjne realizowane są przez resolvera (programu, który wysyła zapytania do serwerów DNS), czyli program resolver oczekuje podania przez serwer adresu IP poszukiwanego hosta lub informacji o błędzie. Wykonywanie zapytań rekurencyjnych pozwala wszystkim uczestniczącym serwerom zapamiętać odwzorowanie (ang. DNS caching), co podnosi efektywność systemu.
2.	Iteracyjne	Ograniczają się do oczekiwania od serwera jedynie podania najlepszej dostępnej mu w danej chwili odpowiedzi, przy czym nie wymaga to od serwera, który otrzymał zapytanie łączenia się jeszcze z innymi serwerami. Zapytania wysyłane pomiędzy serwerami są iteracyjne, przykładowo wiarygodny serwer domeny org nie musi znać adresu IP komputera www.pl.wikipedia.org, podaje więc najlepszą znaną mu w tej chwili odpowiedź, czyli adresy serwerów autorytarnych dla domeny wikipedia.org.

Źródło: opracowanie własne na podstawie: http://pl.wikipedia.org/wiki/DNS

Tabela 3.15.

Rodzaje odpowiedzi stosowanych w protokole DNS

Lp.	Nazwa odpowiedzi	Opis odpowiedzi:
1.	Autorytatywne	Dotyczą domeny w strefie, nad którą dany serwer ma zarząd. Pochodzą bezpośrednio z bazy danych serwera; jest to pozytywna odpowiedź zwracana do klienta, która w komunikacie DNS zawiera ustawiony bit uwierzytelniania (ang. AA – Authoritative Answer) wskazujący, że odpowiedź została uzyskana z serwera dokonującego bezpośredniego uwierzytelnienia poszukiwanej nazwy.
2.	Nieautorytatywne	Dane które zwraca serwer pochodzą spoza zarządzanej przez niego strefy. Odpowiedzi nieautorytatywne są buforowane przez serwer przez czas TTL, wyspecyfikowany w odpowiedzi, później są usuwane.

Źródło: opracowanie własne na podstawie: http://pl.wikipedia.org/wiki/DNS

W protokole DNS format komunikatu jest następujący:

- Nagłówek (ang. Header);
- Zapytanie (ang. Question) – zapytanie kierowane do serwera DNS;
- Odpowiedź (ang. Answer) – odpowiedź zwrotna od serwera DNS;
- Zwierzchność (ang. Authority) – zawiera informację o serwerach nadrzędnych dla danej domeny;
- Dodatkowe – (ang. Additional) – zawiera dodatkowe informacje.

Nagłówek komunikatu DNS ma następującą postać, przedstawioną na rys. 3.4.

Nr bitu	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	ID															
	RCODE				Z			RA	RD	TC	AA	OPCODE				QR
	QDCOUNT															
	ANCOUNT															
	NSCOUNT															
	ARCOUNT															

Rys.3.4. Nagłówek komunikatu protokołu DNS

Źródło: opracowanie własne na podstawie: http://pl.wikipedia.org/wiki/DNS

Objaśnienia:

- ID (16 bitów) – (ang. IDentifier) – identyfikator, który jest tworzony przez program (wspomniany wcześniej resolver) wysyłający zapytanie; serwer przepisuje ten identyfikator do swojej odpowiedzi. Pozwala to na powiązanie zapytania z odpowiedzią;
- QR (1 bit) – (ang. Query or Response) – definiuje, czy komunikat jest zapytaniem (0), czy odpowiedzią (1);
- OPCODE (4 bity) – odpowiada za określenie rodzaju zapytania wysyłanego od klienta, jest przypisywany przez serwer do odpowiedzi. Możliwe są następujące wartości:
    - Wartość bitów: 0000 (dziesiętnie: 0) – QUERY – standardowe zapytanie;
    - Wartość bitów: 0001 (dziesiętnie: 1) – IQUERY – zapytanie zwrotne;
    - Wartość bitów: 0010 (dziesiętnie: 2) – STATUS – pytanie o stan serwera;
    - Wartość bitów: 0011 – 1111 (dziesiętnie: 3-15) – zarezerwowane do przyszłego użytku.
- AA (1 bit) – (ang. Authoritative Answer) – odpowiada, czy odpowiedź jest autorytatywna;
- TC (1 bit) – (ang. TrunCation) – oznacza, że odpowiedź nie zmieściła się w jednym pakiecie UDP i została obcięta;
- RD (1 bit) – (ang. Recursion Desired) – oznacza, że klient wymaga rekurencji – wówczas pole to jest kopiowane do odpowiedzi;
- RA (1 bit) – (ang. Recursion Available) – bit oznacza, że serwer obsługuje zapytania rekurencyjne;
- Z (3 bity) – zarezerwowane do przyszłego wykorzystania. Bity powinny mieć wartość zero;
- RCODE (4 bity) – (ang. Response CODE) – kod odpowiedzi. Możliwe są następujące wartości:
    - Wartość bitów: 0000 (dziesiętnie: 0) – brak błędu;
    - Wartość bitów: 0001 (dziesiętnie: 1) – błąd formatu – serwer nie potrafił zinterpretować zapytania;
    - Wartość bitów: 0010 (dziesiętnie: 2) – błąd serwera – wewnętrzny błąd serwera;

  - Wartość bitów: 0011 (dziesiętnie: 3) – błąd nazwy – nazwa domenowa podana w zapytaniu nie istnieje;
  - Wartość bitów: 0100 (dziesiętnie: 4) – nie zaimplementowano – serwer nie obsługuje typu otrzymanego zapytania;
  - Wartość bitów: 0101 (dziesiętnie: 5) – odrzucono – serwer odmawia wykonania określonej operacji, np. transferu strefy;
  - Wartość bitów: 0110 - 1111 (dziesiętnie: 6-15) – zarezerwowane do przyszłego użytku.
- QDCOUNT (16 bitów) – określa liczbę wpisów w sekcji zapytania;
- ANCOUNT (16 bitów) – określa liczbę rekordów zasobów w sekcji odpowiedzi;
- NSCOUNT (16 bitów) – określa liczbę rekordów serwera w sekcji zwierzchności;
- ARCOUNT (16 bitów) – określa liczbę rekordów zasobów w sekcji dodatkowej.

W komunikacie DNS sekcja nagłówka występuje zawsze. W sekcji zapytania zawsze znajduje się jedno zapytanie zawierające nazwę domenową, żądany typ danych i klasę (IN). Sekcja odpowiedzi zawiera rekordy zasobów stanowiące odpowiedź na pytanie.

Najważniejsze typy rekordów DNS, oraz ich znaczenie[37]:

1. Rekord A lub rekord adresu (ang. Address Record) kieruje nazwę domeny DNS na jej numer IP. Przykład - domena.pl A 82.132.23.44;
2. Rekord CNAME (ang. Canonical Name Record) ustala alias nazwy domeny na inną nazwę. Przykład - ftp.domena.pl CNAME domena.pl;
3. Rekord MX lub rekord wymiany poczty (ang. Mail Exchange Record) wskazuje nazwę domeny DNS na nazwę serwera poczty. Przykład - poczta.domena.pl MX 5 domena.pl;
4. Rekord NS lub rekord serwera nazw (ang. Name Server Record) wskazuje nazwę domenową na serwer DNS dla tej domeny. Przykład – domena.cz NS ns.forspi.cz.

3.2.5. Bezpieczeństwo w DNS

Korzystanie z DNS odbywa się najczęściej przy wykorzystaniu usługi DHCP[38] (ang. Dynamic Host Configuration Protocol – protokół dynamicznego konfigurowania węzłów) – protokół komunikacyjny umożliwiający komputerom uzyskanie od serwera danych

[37] Patrz: http://kb.forpsi.pl/article.php?id=130
[38] DHCP został opublikowany jako standard w roku 1993. W kolejnej generacji protokołu IP, czyli IPv6, jako integralną część dodano nową wersję DHCP, czyli DHCPv6. Jego specyfikacja została opisana w RFC 3315.

konfiguracyjnych, np. adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS, maski podsieci. Protokół DHCP jest zdefiniowany w RFC 2131 i jest następcą BOOTP.

Jest to oczywiście duże ułatwienie dla użytkowników, ponieważ nie wymaga żadnych dodatkowych czynności konfiguracyjnych. Niesie to jednak ze sobą duże niebezpieczeństwo, polegające na możliwości wprowadzenia użytkownika w błąd. Dzieje się tak dlatego, że protokół DHCP jest tak skonstruowany, że komputery chcące pobrać dynamiczny adres IP wysyła zapytanie do sieci z prośbą o przesłanie konfiguracji. Na takie zapytanie może odpowiedzieć każdy komputer, odpowiadając na zapytanie informacją, jakiego serwera DNS pytający komputer ma używać. Nie ma zatem gwarancji, że informacje, które otrzymuje komputer podłączający się do sieci, będą informacjami prawdziwymi.

Należy przypomnieć, że DNS korzysta z bezpołączeniowego protokołu UDP, nie zawierający żadnych mechanizmów autoryzujących. Pierwsza cecha może być używana w atakach DDoS[39] (ang. Distributed Denial of Service) – komputer atakujący może wysyłać zapytania DNS do różnych serwerów na świecie ze sfałszowanym adresem źródłowym, przedstawiając się jako komputer ofiara. Serwery te odpowiadają na zapytania, wysyłając odpowiedzi do komputera ofiary, bo tak wskazuje adres źródłowy pakietu. Konstrukcja protokołu DNS powoduje, że jedno małe zapytanie mieszczące się w pakiecie o wielkości poniżej 100 bajtów, może wygenerować odpowiedź o wielkości ponad dziesięciokrotnie większej. Atakujący komputer wysyłając strumień 1 Mbps takich zapytań może spowodować ponad 10 Mbps odpowiedzi przychodzących do komputera ofiary, zakłócając w ten sposób pracę jego łącza[40].

Jednym z zastosowanych zabezpieczeń jest certyfikat SSL, który informuje użytkownika o przekierowaniu ruchu. Dzieje się tak jednak tylko w przypadku witryn z prefiksem https. Nie działa to natomiast w przypadku stron nie zabezpieczonych tym certyfikatem. Wówczas możliwa jest sytuacja, gdy chcąc połączyć się z pocztą elektroniczną użytkownik zostanie przekierowany na serwer cyberprzestępców, którzy będą w stanie w ten sposób uzyskać dane niezbędne do włamania się do poczty, tj. login oraz hasło.

---

[39] DDoS - atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów (np. zombie). Atak DDoS jest odmianą ataku DoS polegającą na jednoczesnym atakowaniu ofiary z wielu miejsc. Służą do tego najczęściej komputery, nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania (różnego rodzaju tzw. boty i trojany). Na dany sygnał komputery zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług, jakie oferuje. Dla każdego takiego wywołania atakowany komputer musi przydzielić pewne zasoby (pamięć, czas procesora, pasmo sieciowe), co przy bardzo dużej ilości żądań prowadzi do wyczerpania dostępnych zasobów, a w efekcie do przerwy w działaniu lub nawet zawieszenia systemu.

[40] Źródło: http://pl.wikipedia.org/wiki/DNS.

Innym problemem, z jakim mogą mieć do czynienia użytkownicy korzystający z usługi DHCP jest atak tzw. „odmowa usługi" (ang. Deny of Service – DoS) prostsza wersja opisanego powyżej ataku DDoS na serwer DNS, polegającego na „zapchaniu" serwera DNS zapytaniami, a w efekcie spowolnienie lub całkowite zablokowanie usługi DNS. Dzieje się tak wówczas, gdy serwer DHCP jest równocześnie skonfigurowany jako serwer proxy DNS.

Innym zabezpieczeniem pozwalającym podnieść poziom bezpieczeństwa użytkowników jest zastosowanie autoryzacji serwerów DHCP. Jest to możliwe przy wykorzystaniu serwerów DHCP z systemami: Windows 2000, Windows Server 2003 lub nowszym. Wówczas serwer DHCP sprawdza, czy jest autoryzowany w usłudze Active Directory (więcej – patrz następny rozdział). Jeżeli nie jest, natychmiast przestaje świadczyć usługi klientom DHCP. „Dzięki tej funkcji autoryzacji, jeśli złośliwy lub niekompetentny użytkownik zainstaluje w sieci organizacji nieautoryzowany serwer DHCP z systemem Windows 2000 lub Windows Server 2003, serwer ten nie może przypisywać dzierżaw niepoprawnych lub powodujących konflikt, konfigurować klientów DHCP przy użyciu niewłaściwych opcji ani zakłócać działania innych usług sieciowych. Oprogramowanie serwera DHCP firmy innej niż Microsoft nie obejmuje funkcji autoryzacji dostępnej dla serwerów DHCP z systemem Windows 2000 lub Windows Server 2003. Ponieważ klienci DHCP emitują komunikaty odnajdywania DHCP do najbliższego serwera DHCP, jeśli złośliwy użytkownik zainstaluje w sieci organizacji nieautoryzowany serwer DHCP firmy innej niż Microsoft, najbliżsi klienci DHCP będą uzyskiwać niepoprawne dzierżawy, które mogą być w konflikcie z innymi adresami IP, przypisanymi innym klientom DHCP w sieci. Ponadto klienci DHCP uzyskujący dzierżawy od serwera DHCP firmy innej niż Microsoft mogą być konfigurowani przez ten serwer przy użyciu niewłaściwych opcji. Może to prowadzić do ponownego przekierowania ruchu w sieci i jej niepoprawnego działania"[41]. Więcej informacji na temat interakcji DHCP/DNS można znaleźć na stronie: http://technet.microsoft.com/pl-pl/library/cc787034(WS.10).aspx

DNS łatwo też poddaje się atakom typu „man in the middle"[42], co pozwala na przysyłanie fałszywych odpowiedzi do komputera ofiary, zmuszając go do połączenia się z innym serwerem, co pozwala na przykład na kradzież haseł. Istnieje wiele innych możliwości ataków na infrastrukturę DNS, łącznie nawet z uruchamianiem fałszywych serwerów głównych. O słabościach protokołu DNS zdano sobie sprawę wcześnie i stworzono jego roz-

[41] Źródło: http://technet.microsoft.com/pl-pl/library/cc780347(WS.10).aspx

[42] Man in the middle (z ang. człowiek pośrodku) – atak kryptologiczny polegający na podsłuchu i modyfikacji wiadomości przesyłanych pomiędzy dwiema stronami bez ich wiedzy. Przykładem takiego ataku jest podsunięcie nadawcy własnego klucza przy transmisji chronionej szyfrem asymetrycznym. Źródło: http://pl.wikipedia.org/wiki/Atak_man_in_the_middle

szerzenie oparte o podpisy cyfrowe nazwane DNSSEC (ang. DNS Security Extensions, więcej patrz podrozdział 2.7.1.), jednakże system ten nie został całkowicie zaakceptowany przez Internet, nie jest wspierany przez wiele narzędzi, w związku z czym w Internecie praktycznie nie jest używany[43].

3.2.6. Odmiany DNS

3.2.6.1. DNSSEC (DNS Security Extensions)

Jedną z odmian DNS jest wspomniany wcześniej DNSSEC (ang. DNS Security Extensions). Jest to rozszerzenie systemu DNS mające na celu zwiększenie jego bezpieczeństwa. DNSSEC zapewnia autoryzację źródeł danych (serwerów DNS) za pomocą kryptografii asymetrycznej oraz podpisów cyfrowych.

DNSSEC jest protokołem opartym o cyfrowe podpisy, który wykorzystuje mechanizmy kryptograficzne bazujące na kluczach publicznych, co potencjalnie stwarza możliwość zabezpieczenia całej drzewiastej struktury systemu DNS. Protokół zabezpiecza informacje DNS przed sfałszowaniem i modyfikacją, oferując dodatkowo możliwość wykorzystania go jako infrastruktury do dystrybucji kluczy publicznych.

Protokół DNSSEC umożliwia zapewnienie integralności i możliwość weryfikacji autentyczności pozyskanych danych. Klient systemu może mieć pewność, że otrzymane przez niego dane są wiarygodne i nie zostały zmienione w trakcie transportu ze źródła. Protokół definiuje zabezpieczanie strefy a nie serwera, dzięki czemu nawet w przypadku złamania zabezpieczeń jednego z serwerów autorytatywnych dla danej strefy, bezpieczeństwo systemu jako całości zostaje zachowane. Klucze prywatne wykorzystywane są tylko w momencie podpisywania rekordów strefy i nie muszą być dostępne on-line, co dodatkowo wzmacnia bezpieczeństwo systemu. Sytuację komplikują nieco dynamiczne update'y, które wymuszają dostępność kluczy prywatnych w serwerze je obsługującym[44].

DNSSEC wprowadza do DNSu pięć nowych rekordów związanych z usługami bezpieczeństwa:

- DNSKEY - klucz publiczny do weryfikacji podpisów,
- RRSIG - podpis grupy rekordów,
- DS - wskazanie na klucz podpisujący klucz strefy u potomka,

[43] Źródło: http://pl.wikipedia.org/wiki/DNS.
[44] Źródło: https://www.dns.pl/dnssec/theory_intro.html

– NSEC - zapewnienie spójności danych strefy i umożliwienie weryfikacji informacji o nieistnieniu rekordu lub o braku zabezpieczeń (wersja opt-in).

DNSSEC definiuje trzy nowe bity nagłówka komunikatu DNS, dotychczas niewykorzystywane (porównaj z rys.3.5.).

Dodatkowe bity nagłówka[45]:

– DO - 1 bit - (DNSSEC OK) — resolver obsługuje DNSSEC;
– AD - 1 bit - (ang. Authenticated Data) – dane autentyczne – wskazuje, iż dane otrzymane w sekcji odpowiedzi i zwierzchności zostały zweryfikowane przez serwer stosownie do wykorzystywanych przez niego procedur;
– CD – 1 bit - (ang. Checking Disabled) - sprawdzanie wyłączone – informuje odpytywany serwer, że także nie zweryfikowane informacje będą zaakceptowane przez resolver.

Nr bitu	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	ID															
	RCODE				**Z**			RA	RD	TC	AA	OPCODE				QR
	QDCOUNT															
	ANCOUNT															
	NSCOUNT															
	ARCOUNT															

Rys.3.5. Nagłówek komunikatu protokołu DDNS. Czerwonym kolorem zaznaczono miejsce, w którym umieszczono bity nagłówka: DO, AD oraz CD.

Źródło: opracowanie własne na podstawie: https://www.dns.pl/dnssec/theory_intro.html oraz http://pl.wikipedia.org/wiki/DNS

Nr bitu	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	ID															
	RCODE				DO	AD	CD	RA	RD	TC	AA	OPCODE				QR
	QDCOUNT															
	ANCOUNT															
	NSCOUNT															
	ARCOUNT															

Rys.3.6. Nagłówek komunikatu protokołu DDNS wraz z prawdopodobnym rozmieszczeniem bitów: DO, AD oraz CD.

Źródło: opracowanie własne na podstawie: https://www.dns.pl/dnssec/theory_intro.html oraz http://pl.wikipedia.org/wiki/DNS

[45] Źródło: https://www.dns.pl/dnssec/theory_intro.html

Wprowadzenie mechanizmów DNSSEC nie pociąga za sobą żadnych znaczących zmian w protokole DNS. Istniejące serwery cache'ujące oraz resolvery powinny poprawnie działać o ile wspierają one dodane rekordy zasobów. Wyjątkowo, odwołania CNAME w zabezpieczonej strefie nie mogą być autoryzowane, jeżeli dotyczą serwerów nie wspierających mechanizmów bezpieczeństwa[46].

Pakiety UDP DNS są ograniczone do 512 bajtów, co stanowi istotne ograniczenie dla komunikatów DNSSEC. Większa objętość odpowiedzi zwiększa prawdopodobieństwo jej obcięcia, którego rezultatem może być ponowienie zapytania przez resolwer, wykorzystując tym razem protokół TCP. Obsługa zapytań TCP jest bardziej czasochłonna, głównie z powodu konieczności zestawiania i zrywania dedykowanego połączenia. Z tego względu DNSSEC wymusza wsparcie dla EDNS0. Najbardziej znaczący bit pola Z nagłówka OPT, tak zwany bit DO (DNSSEC OK), informuje o możliwości zaakceptowania przez klienta odpowiedzi DNSSEC[47].

3.2.6.2. DDNS (ang. Dynamic Domain Name System)

Inną odmianą DNS jest rozwiązanie DDNS (ang. Dynamic Domain Name System), dynamiczny system nazw domenowych, umożliwiający urządzeniom sieciowym, takim jak router bądź komputer, korzystający z adresacji IP, zakomunikować w czasie rzeczywistym serwerowi nazw zmianę obecnej konfiguracji DNS w postaci skonfigurowanych domen, adresów oraz innych danych zamieszczonych w rekordach DNS.

Popularnym zastosowaniem DDNS jest umożliwienie bramce internetowej ze zmiennym adresem IP uzyskania stałej nazwy hosta, która jest rozwiązywana przez standardowe zapytania DNS aplikacji działających w sieci Internet.

Dostawcy DDNS udostępniają oprogramowanie klienckie, które automatyzuje proces wykrywania i rejestracji publicznego IP klienta. Oprogramowanie to jest uruchamiane na komputerze bądź urządzeniu znajdującym się w sieci prywatnej. Łączy się ono z systemem dostawcy i powoduje połączenie wykrytego publicznego adresu IP sieci domowej z odpowiednią nazwą hosta w systemie DNS. W zależności od dostawcy, nazwa hosta zostaje zarejestrowana w domenie będącej własnością dostawcy, bądź we własnej domenie będącej własnością klienta. Zwykle oprogramowanie to wykorzystuje protokół HTTP ponieważ jest on z reguły wspierany nawet w najbardziej restrykcyjnych środowiskach. Ta grupa usług jest

[46] Źródło: https://www.dns.pl/dnssec/theory_intro.html
[47] Źródło: https://www.dns.pl/dnssec/theory_intro.html

najczęściej kojarzona z terminem Dynamic DNS, aczkolwiek nie wykorzystuje się tu standardowej metody DNS Update. Jednakże metoda ta może być wykorzystywana w systemach dostawców.

Przykładem zastosowania może być użytkownik domowy, który chciałby korzystać ze swojej domowej sieci podczas podróży. Użytkownik ten może mieć przyznany adres IP, który ulega zmianie za każdym razem kiedy jest ustanawiane nowe połączenie. Nie ma zatem stałego adresu z którym mógłby się on połączyć. Jeśli usługa DDNS zostaje wykorzystana do przydzielenia stałego adresu do urządzenia sieciowego to użytkownik będzie w stanie, przykładowo, nawiązać sieć VPN[48] do swojej sieci za pomocą stałego adresu. Konkretnym przykładem może być adres IP, który jednego dnia wynosi 123.234.111.112, a drugiego zaś 123.124.45.16, podczas gdy adres DDNS będzie zawsze, na przykład, mojdom.ddns.org. Program służący do zdalnego dostępu, taki jak serwer VNC[49] (ang. Virtual Network Computing) – system przekazywania obrazu – może być uruchamiany na takim komputerze w sieci; użytkownik może wtedy połączyć się z nią za pomocą zastrzeżonego hasłem połączenia VPN do mojdom.ddns.org, a następnie połączyć się z komputerem za pomocą klienta VNC.

W sieciach Microsoft Windows, DDNS jest integralną częścią Active Directory ponieważ kontroler domeny rejestruje swój rekord SRV w DNS, aby inne komputery w domenie (lub lesie) mogły się z nimi połączyć.

---

[48] VPN (ang. *Virtual Private Network*, Wirtualna Sieć Prywatna), można opisać jako tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. Taki kanał może opcjonalnie kompresować lub szyfrować w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa przesyłanych danych. Określenie "Wirtualna" oznacza, że sieć ta istnieje jedynie jako struktura logiczna działająca w rzeczywistości w ramach sieci publicznej, w odróżnieniu od sieci prywatnej, która powstaje na bazie specjalnie dzierżawionych w tym celu łącz. Pomimo takiego mechanizmu działania stacje końcowe mogą korzystać z VPN dokładnie tak, jak gdyby istniało pomiędzy nimi fizyczne łącze prywatne. Rozwiązania oparte na VPN powinny być stosowane np. w sieciach korporacyjnych firm, których zdalni użytkownicy dosyć często pracują ze swoich domów na niezabezpieczonych łączach. Wirtualne Sieci Prywatne charakteryzują się dość dużą efektywnością, nawet na słabych łączach (dzięki kompresji danych) oraz wysokim poziomem bezpieczeństwa (ze względu na szyfrowanie). Źródło: http://pl.wikipedia.org/wiki/VPN

[49] VNC (ang. Virtual Network Computing) – system przekazywania obrazu z wirtualnego, bądź fizycznego środowiska graficznego. Prosty pakiet serwer+klient jest dostępny pod najpopularniejsze systemy operacyjne z trybem graficznym, jak: Linux, Windows, BSD, MacOS, OS/2, Solaris, AmigaOS, SCO i wiele innych. Klienci VNC są dostępni nawet dla urządzeń typu PDA i niektórych telefonów komórkowych. Jego wielką zaletą jest użycie licencji GPL, dzięki czemu VNC jest darmowe, bardzo rozwinięte i dostosowane do różnych potrzeb. Jego poważnym konkurentem staje się system NX, który działa z większą wydajnością. Domyślnie VNC korzysta z portów TCP 5900 – 5906, gdzie każdy z portów oznacza odrębną sesję (od 0 do 6), lecz zarówno klient jak i serwer mogą zostać przekonfigurowane do pracy na dowolnych innych portach. Źródło: http://pl.wikipedia.org/wiki/VNC

3.2.6.3. Open DNS (ang. Dynamic Domain Name System)

OpenDns jest alternatywą dla rozwiązania DNS, ponieważ oferuje swoje za darmo. OpenDNS jest organizacją, która powstała w 2006 roku. Jej założycielem jest David Ulevitch. Jedynym wymogiem, który musi zostać spełniony przez użytkownika Internetu to rejestracja. Można jej dokonać na stronie projektu www.opendns.com. Należy również skonfigurować domyślne serwery DNS w swoim systemie operacyjnym. Są to serwery o adresach IP: 208.67.222.222 oraz 208.67.220.220.

Jedynym utrudnieniem korzystania z tej usługi jest fakt, że jest to organizacja działająca w Stanach Zjednoczonych, a co za tym idzie praktycznie wszystkie serwery są zlokalizowane w USA. Na szczęście są już serwery w Wielkiej Brytanii (w Londynie), a w najbliższym czasie powinien zostać uruchomiony serwer w Holandii (w Amsterdamie).

W rozwiązaniu tym stosowana jest technologia Anycast[50], pozwalająca, w razie problemów z odpowiedzią na zapytanie DNS, automatycznie przekierować do następnego najbliższego serwera i otrzymać od niego odpowiedź. W tabeli 3.16. przedstawiono podstawowe, główne cechy odróżniające OpenDNS od rozwiązania DNS.

Tabela 3.16.

Podstawowe, główne cechy odróżniające OpenDNS od DNS.

Lp.	Nazwa cechy	Opis cechy:
1.	**Obrona przez phishingiem (ang. Phishing protection)**	Jest to możliwe dzięki współpracy OpenDNS z innym projektem PhishTank.com.
2.	**Filtrowanie zawartości (ang. Content filtering)**	OpenDNS oferuje możliwość blokowania zawierających niechcianą przez użytkowników zawartość stron www. Usługa ta pozwala na nadanie stronie jednej z ponad 30 kategorii, takich jak: pornografia, narkotyki, P2P, gry, itp. Jest to wykonywane przez użytkowników.
3.	**Lista domen zaufanych (ang. Domain Whitelist)**	Użytkownik ma możliwość zdefiniowania tzw. białej listy domen zaufanych, co do zawartości których nie ma on żadnych wątpliwości.

[50] **Anycast** - rodzaj transmisji sieciowej, w której dane wysyłane są do najbliższego lub najlepszego węzła. Komunikacja następuje od jednego nadawcy do (potencjalnie) wielu odbiorców, przy czym jednocześnie dane są odbierane przez jednego z nich. Najlepiej do tego rodzaju transmisji nadają się protokoły bezpołączeniowe (np. UDP). Anycast może być wykorzystywany m.in. do implementowania serwerów DNS, jak również do przeprowadzania ataków DoS. Źródło:http://pl.wikipedia.org/wiki/Anycast"

4.	**Blokowanie domen (ang. Domain Blocking – Blacklist)**	Każdy z użytkowników OpenDNS ma możliwość blokowania dostępu do dowolnych domen, gdy uzna, że ich zawartość może być szkodliwa np. dla dzieci. Tworzona jest wówczas tzw. czarna lista domen.
5.	**Blokowanie stron www dla dorosłych (ang. Adult Site Blocking)**	Opcja o działaniu analogicznym do blokowania domen, cechy OpenDNS opisanej powyżej.
6.	**Skróty (ang. Shortcuts)**	Użytkownik ma możliwość zdefiniowania skrótów odpowiadających adresom stron www. Pozwala to uzyskać znaczne przyspieszenie w dostępie do najczęściej odwiedzanych portali www.
7.	**Korekta literówek / Type Corrections**	Usługa ta polega na tym, że system automatycznie przekierowuje użytkownika na właściwą stronę www w przypadku, gdy użytkownik omyłkowo błędnie wpisze jej nazwę.
8.	**Dostęp do narzędzi administratora**	Użytkownik otrzymuje możliwość korzystania z narzedzi administratora. Są one dostępne w panelu administracyjnym.
9.	**Dynamiczne IP (ang. Setup Dynamic IP)**	Umożliwia to dokonywanie konfiguracji komputerów korzystających z dynamicznego przypisywania adresów IP. Jest to możliwe dla wielu użytkowników.

Źródło: opracowanie własne na podstawie: http://iname.pl/2008/03/open-dns-ciekawa-alternatywa/

3.2.6.4. BIND (ang. Berkeley Internet Name Domain)

BIND (*ang. Berkeley Internet Name Domain, poprzednio używana nazwa to: Berkeley Internet Name Daemon*) jest rozwiązaniem popularnym. Powstało w 1988 roku, jego twórcą był Paul Vixie. BIND jest serwerem (demonem) DNS. Choć to może być zaskakujące, BIND jest jednym z najpopularniejszych serwerów DNS wykorzystywanym w systemach Linux i Unix. Stanowi niezmiernie ważny składnik zapewniający poprawne działanie systemu nazw w Internecie. Wielu użytkowników globalnej sieci bezwiednie korzysta z serwera BIND, kiedy ich przeglądarka WWW odpytuje go o adres IP komputera udostępniającego interesującą ich stronę.

Istnieje wiele wersji serwera BIND. Ostatnia wersja BIND 9, w celu uniknięcia popełnionych w poprzednich wersjach błędów, została napisana od początku.

Wersja BIND 9 zapewnia m. in.:

- obsługę rozszerzeń bezpieczeństwa (ang. DNS Security Extensions);

- powiadomienia DNS;
- obsługę rekordów TSIG (uwierzytelnianie kryptograficzne opisane w dokumencie RFC 2845);
- nsupdate (ułatwiona aktualizacja rekordów DNS);
- obsługę protokołu IPv6;
- czyszczenie rekordów rndc (ang. rndc flush);
- widoki;
- pracę wieloprocesorową;
- poprawiony (ulepszony) poziom przenośności kodu między różnymi platformami.

Historia tego rozwiązania sięga lat 80-tych, w ramach projektów DARPA, a więc niemalże równolegle z rozwiązaniem DNS. W połowie dekady pracę nad serwerem przejęła korporacja DEC. Jednym z jej pracowników biorących udział w projektowaniu BIND (wspomniany wcześniej jego twórca, Paul Vixie), kontynuował swoją pracę po opuszczeniu tej firmy. Był on jednym z założycieli ISC (ang. Internet Software Consorcium), organizacji zarządzającej standardami Internetu, która przejęła prace nad dalszym rozwojem BIND-a.

Wersja 9 BIND powstała jako efekt realizacji kilku komercyjnych oraz wojskowych projektów. Firmy wykorzystujące Uniksa chciały zapewnić, aby BIND był ciągle konkurencyjny względem serwerów DNS sprzedawanych przez ich konkurencję, firmę Microsoft.

Podobnie, jak w przypadku DNS, tak i historia powstania rozwiązania BIND sięga czasów, kiedy bezpieczeństwem pracy w sieci nie zajmowano się zbyt poważnie. Powodem podstawowym był ograniczony zasięg jego wykorzystania do ośrodków naukowych, przez co użytkownikami sieci były osoby „świadome", którym nie zależało specjalnie na działaniu na szkodę Internetu. Wraz z rosnącą ilością użytkowników twórcy BIND-a stanęli przed koniecznością modyfikacji rozwiązania o zabezpieczenia. Szybko bowiem okazało się, że wielu użytkowników sieci wykorzystywało luki twgo rozwiązania do różnego rodzaju ataków. Wówczas zaczęto tworzyć kolejne wersje BIND. Niestety, architektura pierwszego BIND, która w następnych wersjach nie była zmieniana (dokonywano jedynie łatania znalezionych luk) spowodowała, że wersja 9 BIND-a została stworzona „od nowa". Jednak zmiany architektury powodują zwykle pewne utrudnienia w ich administrowaniu przez administratorów, którzy używali wcześniejszych wersji. Duży zasób dostępnych funkcji może spowodować, że

administratorzy będą mieli kłopoty w ich poprawnym skonfigurowaniu, co powodując możliwość powstania zagrożeń bezpieczeństwa[51].

Poniżej, w tabeli 3.17. przedstawiono serwisy online oferowane przez BIND 9.

Tabela 3.17.

Serwisy online, oferowane przez BIND 9

Lp.	Nazwa serwisu	Opis serwisu:
1.	**SNS@ISC (ang. Secondary Name Service)**	Korzystanie z usługi SNS@ISC pozwala dostarczać nazwy serwerów zastępczych (slave servers), zawierających nazwy domen, obsługiwanych przez użytkownika. Jest ona dostępna w dwóch wersjach – płatnej, typowo komercyjnej (SNS@ISC) oraz bezpłatnej, tzw. no-cost dla organizacji publicznych.
2.	**SIE (ang. Security Information Exchange)**	Usługa polega na połączeniu informacji o stanie bezpieczeństwa z wielu sensorów umieszczonych w różnych sieciach, dzięki czemu możliwa jest szybsza reakcja na pojawiające się w sieci incydenty.
3.	**DLV (ang. DNS Lookaside Validation registry)**	Umożliwia korzystanie z rozwiązania DNSSec zanim strefa sieci wyższego poziomu zostanie podpisana.
4.	**Domain Survey**	Raz na kwartał dokonywania jest inwentaryzacja domen przypisanym poszczególnym adresom IP. Dane, w postaci statystyk są dostępne (płatne) dla zainteresowanych użytkowników.
5.	**DNS-OARC**	Jest to usługa operacyjna DNS, tzw. Research center, zajmujące się m.in. analizowaniem tego, co się dzieje w podległych sieciach komputerowych.

Źródło: opracowanie własne na podstawie: https://www.isc.org/solutions

WNIOSKI

Przeprowadzone analizy wykazały, że zarówno rozwiązanie Active Directory jak i DNS są technologiami, które można wykorzystać do zarządzania informacją w sieci teleinformatycznej.

Active Directory jest usługą katalogową – hierarchiczną bazą danych, której podstawowym protokołem jest protokół LDAP (ang. Lightweight Directory Access Protocol). Technologia ta jest rdzeniem bezpieczeństwa w środowisku sieciowym platformy Microsoft Windows Server. Odpowiada m.in. za identyfikowanie użytkowników i komputerów w domenie organizacji, zarządzanie i wdrażanie zasad grup, funkcjonowanie polityk bezpieczeństwa oraz

[51] Opracowano na podstawie: http://pl.wikipedia.org/wiki/BIND

kontrolę dostępu do zasobów sieciowych. Jest to usługa dzięki której możliwe jest zarządzanie domeną informacyjną.

Z kolei DNS jest rozwiązaniem stworzonym na zlecenie Departamentu Obrony Stanów Zjednoczonych, opierającym się na hierarchicznej, rozproszonej bazie danych, przechowującej dane różnego typu, w tym nazwy hostów oraz nawy domen.

Podstawą technicznego systemu DNS jest ogólnoświatowa sieć serwerów przechowujących informacje na temat adresów domen. Każdy wpis zawiera nazwę oraz odpowiadającą jej wartość, najczęściej adres IP. DNS to także protokół komunikacyjny opisujący sposób łączenia się klientów z serwerami DNS. Częścią specyfikacji protokołu jest zestaw zaleceń, jak aktualizować wpisy w bazach domen internetowych. Domeny mają strukturę drzewiastą, na szczycie której znajduje się 13 głównych serwerów obsługujących domeny najwyższego poziomu.

Przeprowadzone badania wykazały, że zarówno technologia proponowana przez Active Directory jak i DNS umożliwiają zarządzanie informacje w środowisku sieci teleinformatycznych na potrzeby NCW. Niemniej jednak rozwiązanie DNS jest rozwiązaniem lepszym z uwagi na jego powszechny charakter i niezależność od konkretnego producenta. Gro rozwiązań DNS ma charakter Open Source co ma niebagatelne znaczenie dla bezpieczeństwa całego systemu zarządzania informacją.

4. Koncepcja zarządzania informacją

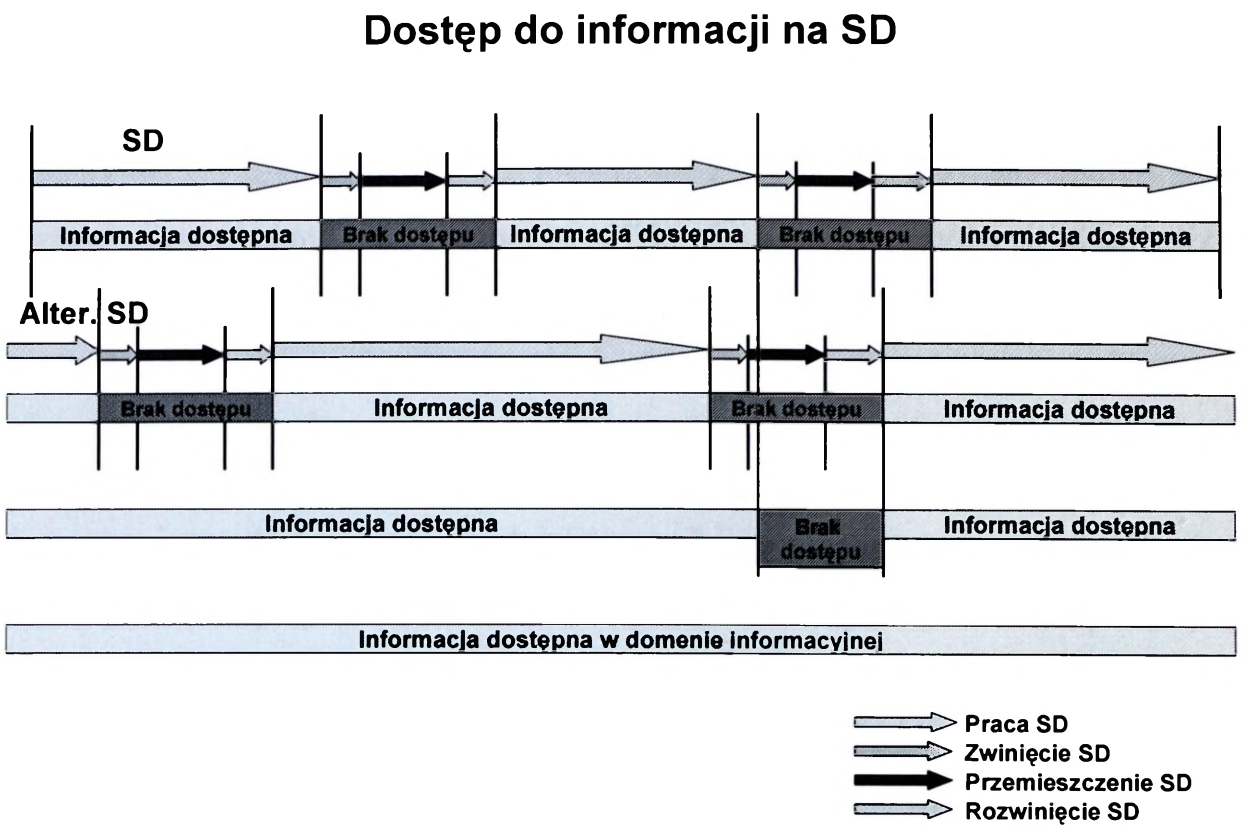
W niniejszym rozdziale przedstawiono koncepcję tworzenia wspólnej świadomości operacyjnej na bazie „domen informacyjnych" oraz sposób zarządzania informacją w sieciach teleinformatycznych stanowisk dowodzenia w celu zachowania jej spójności.

4.1. Domeny informacyjne

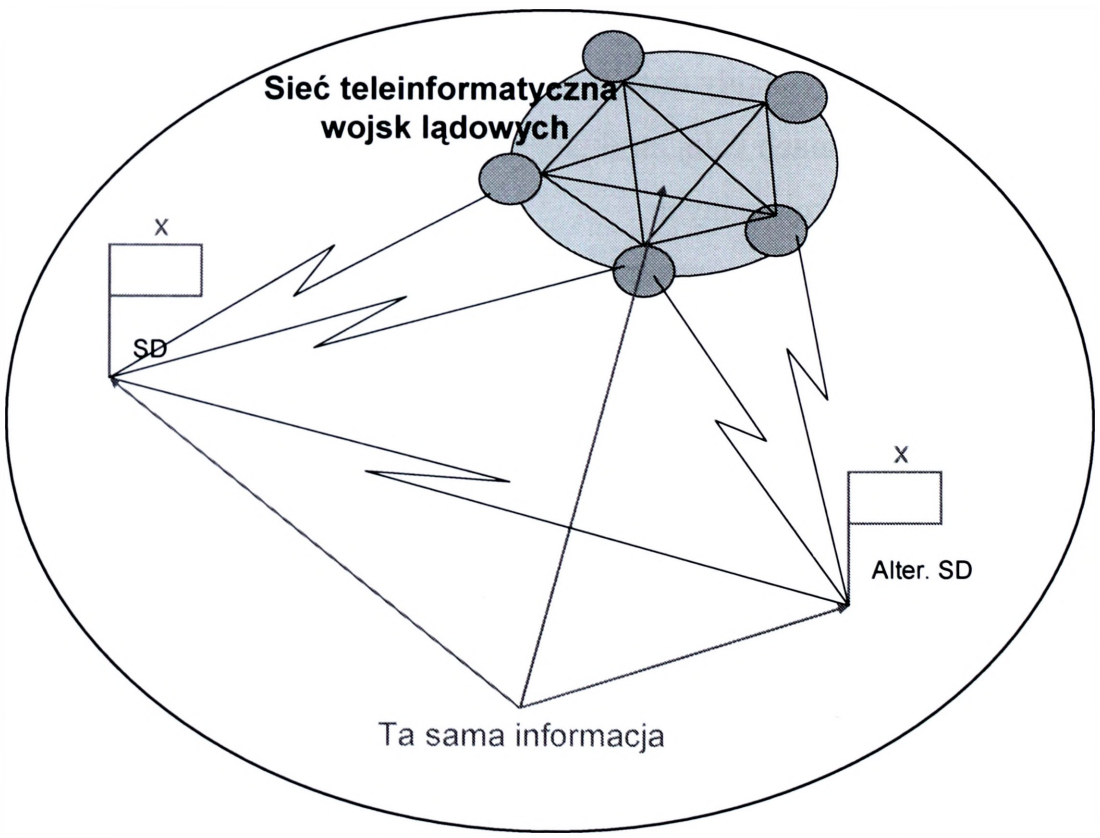
W przedstawionym na rysunku 2.7 (w rozdziale drugim) hipotetycznej sytuacji baraku dostępu do danych znajdujących się zarówno na serwerach SD jak i Alter. SD należy stwierdzić, że stanowi to potencjalne zagrożenie utraty spójności posiadanych danych i skutkować może podjęciem nieoptymalnych decyzji.

Przeprowadzone badania uprawniają do stwierdzenia, że dobrym i skutecznym rozwiązaniem powyższego problemu będzie przechowywanie informacji nie tylko na stanowiskach dowodzenia lecz także w sieci teleinformatycznej. Istniejące technologie teleinformatyczne, rozwijane komercyjnie i wdrażane do sił zbrojnych w ramach podejścia COTS, pozwalają na stworzenie odpowiedniej struktury logicznej domen informacyjnych, które umożliwią zarządzanie informacją w sposób spójny na poziomie całych wojsk lądowych (sił zbrojnych). Domeny zapewniałyby ciągły dostęp do informacji nie tylko w ramach danego organu dowodzenia, ale także w ramach całej struktury dowodzenia zarówno w relacjach dowodzenia, współdziałania jak i funkcjonalnych.

Przyjęta koncepcja przechowywania informacji w Globalnej Sieci Informacyjnej wywodzi się z powszechnie znanej i stosowanej w sieciach komputerowych technologii DNS (*ang. Domain Name System*), zaprezentowanej w rozdziale trzecim. Jej główne zalety, takie jak łatwość konfiguracji i modyfikacji, duża niezawodność i prosty sposób zarządzania uprawniają do stwierdzenia, że zastosowanie tej technologii do zarządzania informacją w znaczny sposób przyczyni się do szybkiego osiągnięcia zdolności sieciocentrycznych. Dodatkowo stworzenie na bazie technologii DNS odpowiednich domen informacyjnych wprowadzi nową jakość w proces dowodzenia i wymusi jego modyfikację uwzględniającą posiadane środki dowodzenia.



Rys. 4.1. Dostęp do informacji z poziomu domen informacyjnych – wariant
Źródło: P. Dela, Domeny informacyjne – nowe podejście do zarządzania informacją, referat na konferencji Wsparcie teleinformatyczne dowództw w działaniach wojsk lądowych, AON, Warszawa 2008



Rys. 4.2. Miejsca przechowywania informacji na danym szczeblu dowodzenia – wariant
Źródło: P. Dela, Domeny informacyjne – nowe podejście do zarządzania informacją, referat na konferencji Wsparcie teleinformatyczne dowództw w działaniach wojsk lądowych, AON, Warszawa 2008

Idea domen informacyjnych[1] polega na założeniu, że informacja wytwarzana przez organ decyzyjny jest przechowywana zarówno na jego stanowisku dowodzenia jak i w domenie informacyjnej (Rysunek 4.1. i 4.2.). Domena znajdująca się w sieci poprzez swoje właściwości zapewni podstawowe wymagania nakładane na informację a mianowicie: dostępność, wiarygodność, bezpieczeństwo, spójność, trwałość i aktualność informacji. Jednocześnie system domen informacyjnych będzie systemem rozproszonym posiadającym następujące możliwości: współdzielenia zasobów, otwartości, współbieżności, skalowalności, przeźroczystości i tolerowania uszkodzeń.

System domen informacyjnych powinien być postrzegany poprzez strukturę zarówno fizyczną jak i logiczną. Struktura fizyczna to zbiór serwerów umieszczonych m. in. w węzłach sieciowych GIG. Serwery te będą odpowiadały za przechowywanie informacji w bazach danych oraz za prawidłowe funkcjonowanie struktury logicznej domen informacyjnych. Dlatego należy wyróżnić trzy zasadnicze grupy serwerów, a mianowicie:

- serwery adresowe domen – odpowiadające za strukturę logiczną domen informacyjnych;
- serwery bezpieczeństwa sieci (domen) – odpowiadające za bezpieczeństwo sieci i przestrzeganie praw dostępu do danych;
- serwery przechowujące informację – posiadające systemy baz danych z informacją wytworzoną przez organy dowodzenia.

Struktura logiczna domen informacyjnych to sposób konfiguracji poszczególnych domen w postaci struktury hierarchicznej odzwierciedlającej aktualną strukturą sił zbrojnych oraz tworzenia na jej bazie struktur domen wynikających z bieżących potrzeb.

Informacja wytworzona przez organ dowodzenia na stanowisku dowodzenia umieszczana będzie dodatkowo w domenie informacyjnej przypisanej danemu organowi dowodzenia, a dostęp do niej będzie się odbywał na podstawie odpowiednich praw dostępu skonfigurowanych przez administratora systemu domen. Fizyczne usytuowanie informacji będzie nieznane i nieistotne dla użytkowników sieci, a dostęp do danych będzie się odbywał poprzez strukturę logiczną domen informacyjnych, co umożliwi wymianę informacji we wszystkich relacjach (więziach) informacyjnych zarówno dowodzenia, współdziałania, synchronizacji, koordynacji jak i funkcjonalnych.

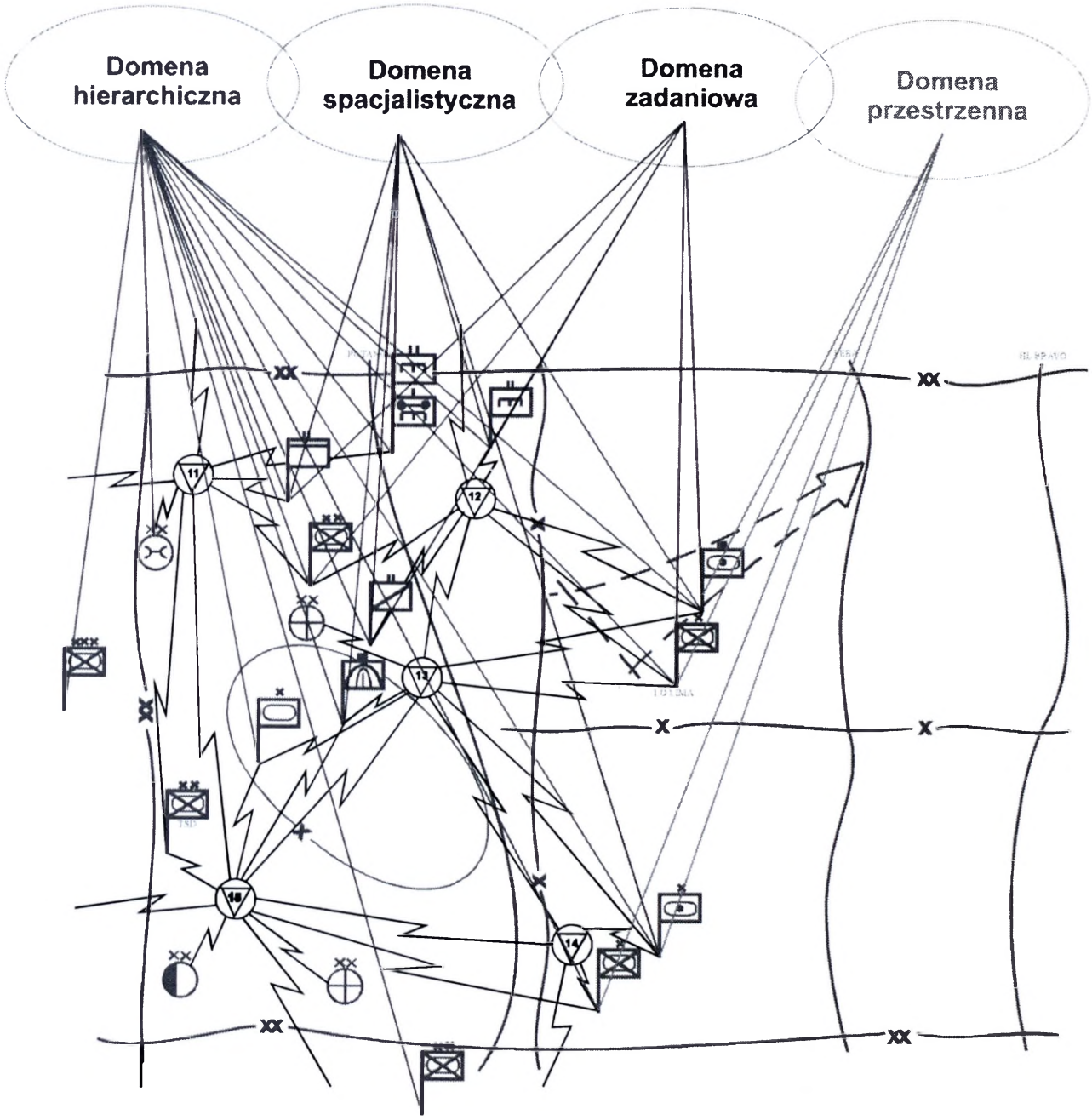
---

[1] Porównaj: P. Dela, *Domeny informacyjne – nowe podejście do zarządzania informacją, referat na konferencji Wsparcie teleinformatyczne dowództw w działaniach wojsk lądowych,* AON, Warszawa 2008; P. Dela, *Domeny informacyjne a zarządzanie informacją w środowisku sieciocentrycznym*, PWLąd 2/2009.

Przeprowadzone badania wykazały, że z uwagi na specyfiką sił zbrojnych, charakterystykę wykonywanych zadań i wynikające z tego potrzeby informacyjne należy wyróżnić cztery podstawowe rodzaje domen informacyjnych a mianowicie:

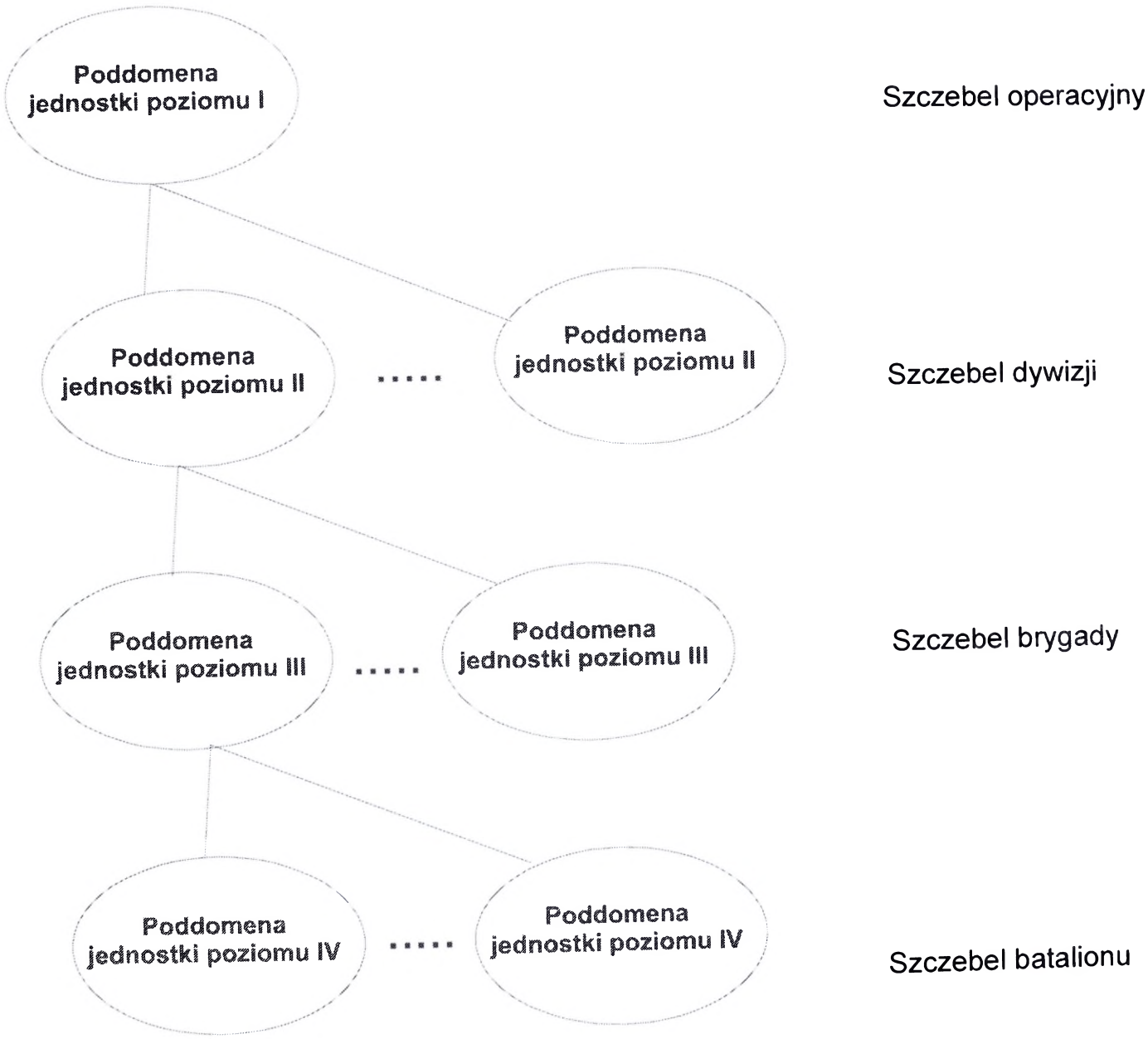
- domeny hierarchiczne;
- domeny specjalistyczne;
- domeny zadaniowe;
- domeny przestrzenne.

Usytuowanie wyżej wymienionych domen w zależności od realizowanych zdań i przyjętej organizacji dowodzenia zobrazowano na rysunku 4.3.



Rys. 4.3. Przykład struktury domen informacyjnych
Źródło: P. Dela, Domeny informacyjne – nowe podejście do zarządzania informacją, referat na konferencji Wsparcie teleinformatyczne dowództw w działaniach wojsk lądowych, AON, Warszawa 2008

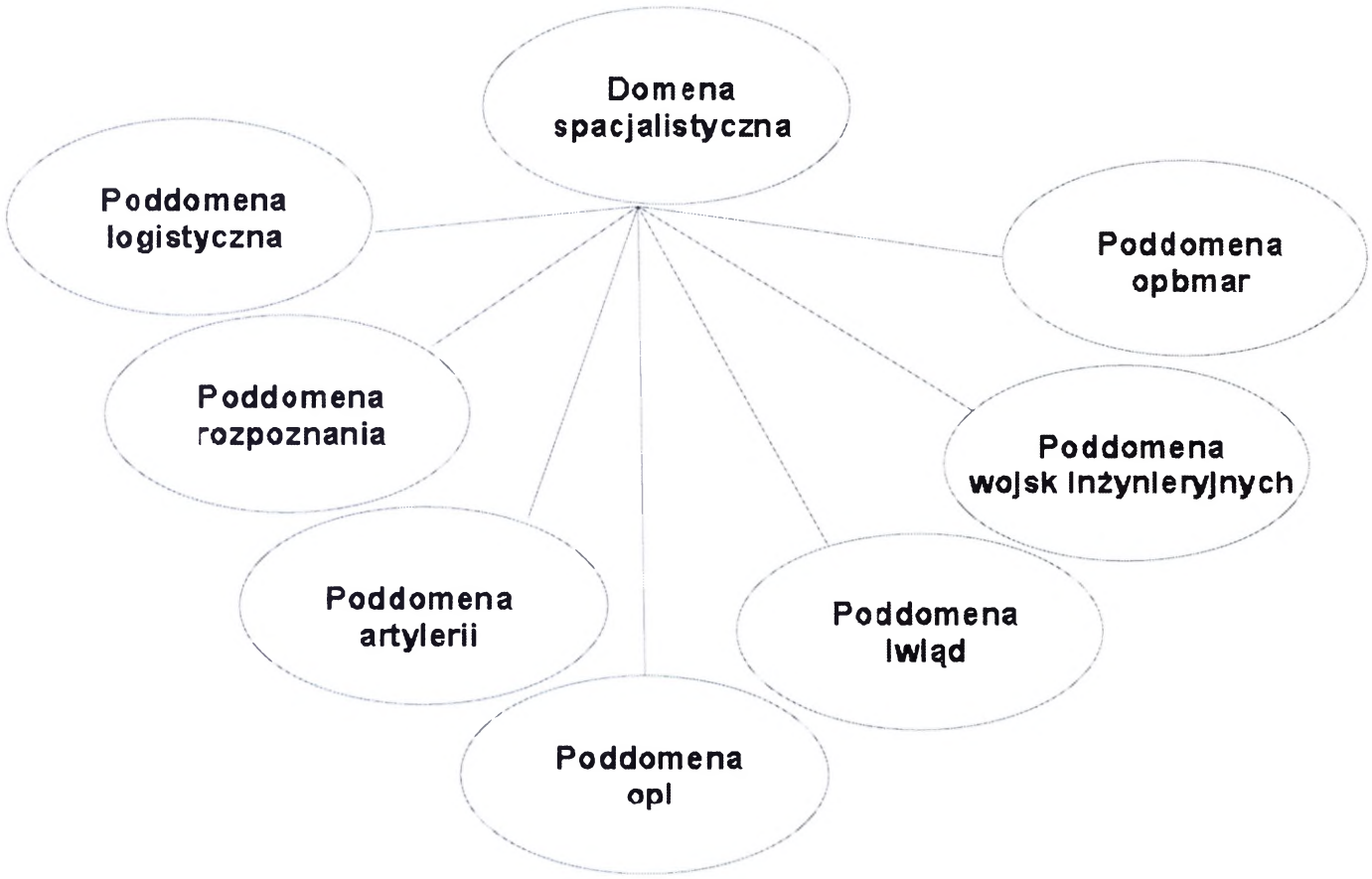
Domeny hierarchiczne będą podstawowym rodzajem domen informacyjnych których struktura zgodna będzie z przyjętą strukturą sił zbrojnych. Każda jednostka posiadająca odpowiedni personel zdolny do przetwarzania informacji powinna posiadać swoją domenę informacyjną. Z tego też względu należy przyjąć, że najniższym poziomem domen informacyjnych w wojskach lądowych powinien być poziom batalionu/dywizjonu. Domeny hierarchiczne będą domenami pierwotnymi w których przechowywana będzie informacja wytworzona przez jej właściciela. Pozostałe domeny będą tworzone z domen hierarchicznych poprzez rekonfigurację systemu domen. Rekonfiguracja powinna uwzględniać bieżące zadania realizowane przez siły zbrojne, zmiany w podporządkowaniu itp.



Rys. 4.4. Przykład hierarchicznych domen informacyjnych – wariant struktury domen informacyjnych wojsk lądowych

Źródło: P. Dela, Domeny informacyjne – nowe podejście do zarządzania informacją, referat na konferencji Wsparcie teleinformatyczne dowództw w działaniach wojsk lądowych, AON, Warszawa 2008

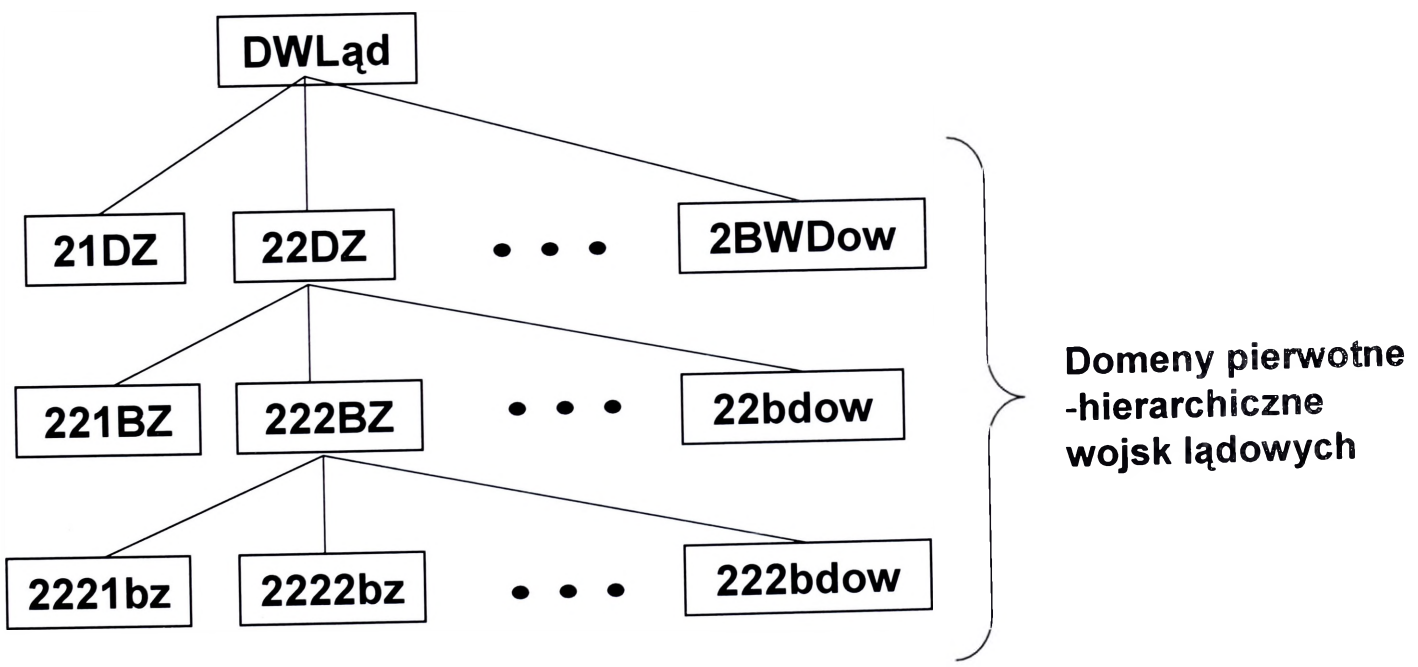
Następny rodzaj domen - domeny specjalistyczne - będą odpowiadały za dostęp do informacji w ramach poszczególnych rodzajów wojsk z jednoczesnych uwzględnieniem przyjętej hierarchii dowodzenia i potrzeb współdziałania. Na rysunku 4.5. przedstawiono przykład uproszczonej struktury domen specjalistycznych. Domeny specjalistyczne będą tworzone na bazie domen hierarchicznych poprzez odpowiednią konfiguracją systemu domen. Takie podejście będzie odzwierciedlało więzi funkcjonalne i przyczyni się do zwiększenia poziomu wspólnej świadomości operacyjnej w ramach poszczególnych rodzajów wojsk.



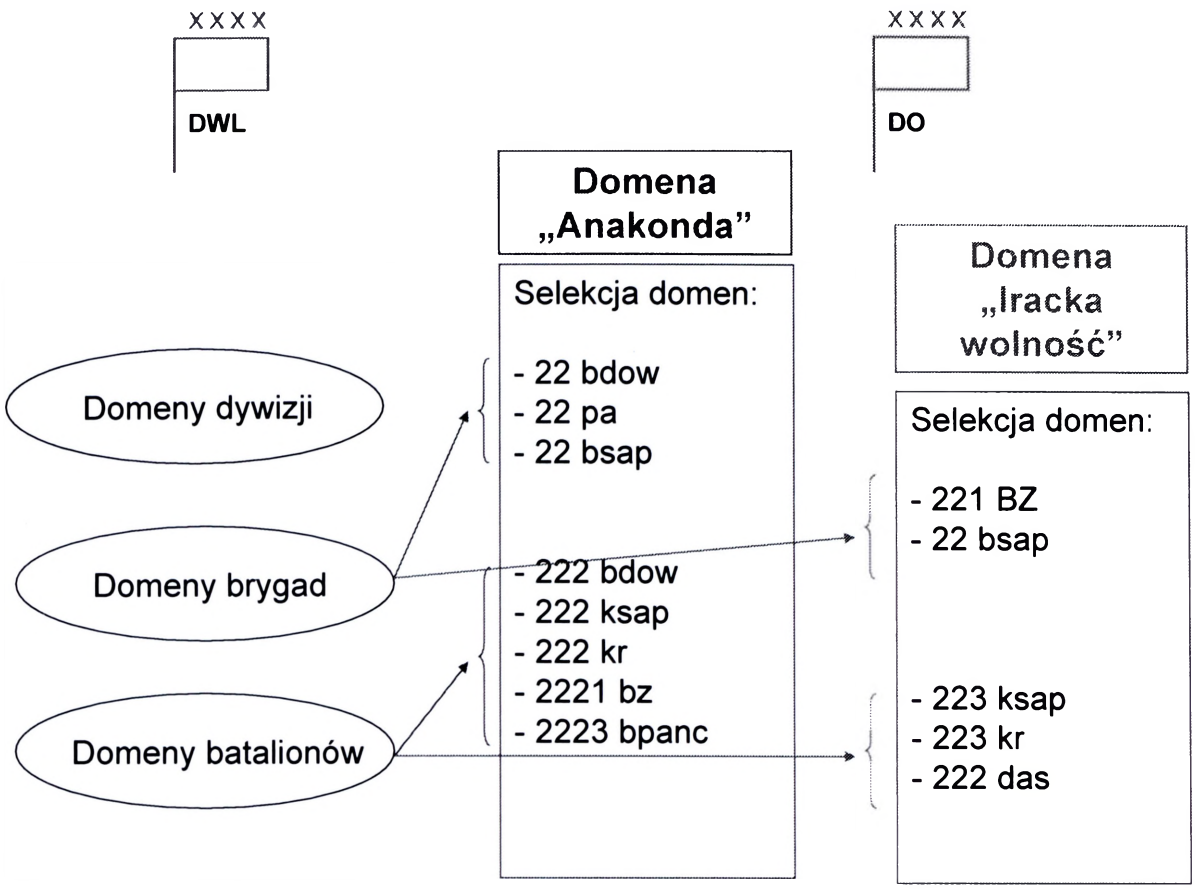
Rys. 4.5. Przykład specjalistycznych domen informacyjnych wojsk lądowych
Źródło: P. Dela, Domeny informacyjne – nowe podejście do zarządzania informacją, referat na konferencji Wsparcie teleinformatyczne dowództw w działaniach wojsk lądowych, AON, Warszawa 2008

Specyfika realizowanych zadań i potrzeba zachowania wcześniej wymienionych właściwości informacji wymusza wprowadzenie dodatkowo domen zadaniowych jak i przestrzennych. Domeny zadaniowe będą grupowały informacje wytwarzane przez jednostki biorące udział w realizacji konkretnego zadania natomiast domeny przestrzenne będą zapewniały dostęp do informacji z jednostek znajdujących się na wybranym obszarze. Domeny te będą tworzone poprzez odpowiednią rekonfiguracja systemu domen. Informacja w nich zawarta będzie informacją pierwotną zawartą w domenach hierarchicznych.

Na rysunkach 4.6. - 4.8. przedstawiono uproszczony sposób wyboru domen hierarchicznych w celu stworzenia domen zadaniowych i specjalistycznych na potrzeby dowództwa operacyjnego. Należy jeszcze raz podkreślić, że informacja będzie fizycznie umieszczona w swojej domenie hierarchicznej, a dostęp do niej będzie zapewniony poprzez logiczną strukturę domen informacyjnych. Struktura logiczna stanowić będzie element organizacji dowodzenia i powinna być określona w fazie planowania działań. Uprawnienia dostępu do informacji powinny odpowiadać więziom informacyjnym i uwzględniać potrzeby tworzenia wspólnej świadomości operacyjnej dla określonej grupy użytkowników systemu (organów dowodzenia).

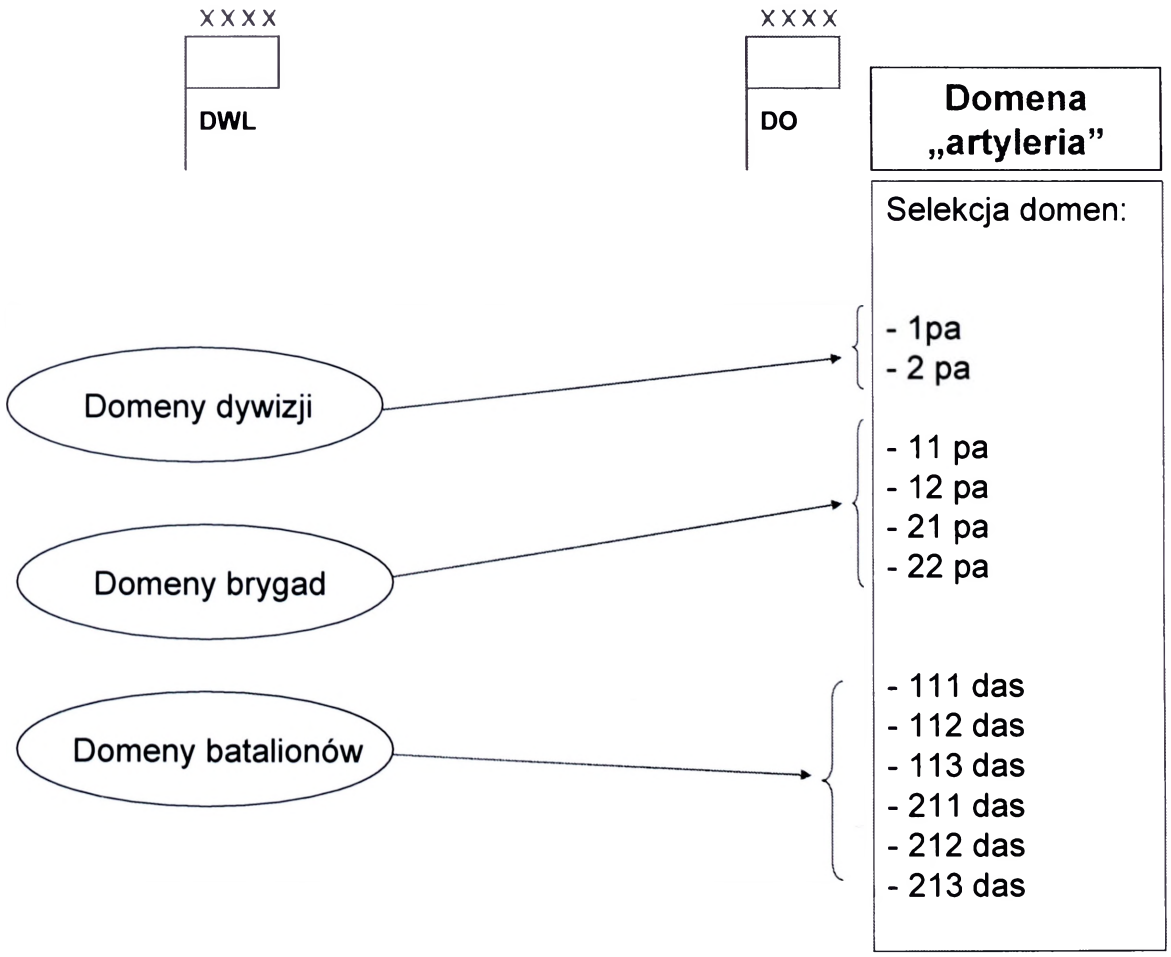


Rys. 4.6. Struktura domen hierarchicznych wojsk lądowych
Źródło: P. Dela, Domeny informacyjne – nowe podejście do zarządzania informacją, referat na konferencji Wsparcie teleinformatyczne dowództw w działaniach wojsk lądowych, AON, Warszawa 2008



Rys. 4.7. Przykład selekcji i tworzenia domen zadaniowych

Źródło: P. Dela, Domeny informacyjne – nowe podejście do zarządzania informacją, referat na konferencji Wsparcie teleinformatyczne dowództw w działaniach wojsk lądowych, AON, Warszawa 2008



Rys. 4.8. Przykład selekcji i tworzenia domen specjalistycznych

Źródło: P. Dela, Domeny informacyjne – nowe podejście do zarządzania informacją, referat na konferencji Wsparcie teleinformatyczne dowództw w działaniach wojsk lądowych, AON, Warszawa 2008

4.2. Zarządzanie informacją w sieci teleinformatycznej stanowiska dowodzenia

Rozpatrując zarządzanie informacją w sieci teleinformatycznej stanowiska dowodzenia należy stwierdzić, że głównym zdaniem stawianym przed zespołem zarządzającym informacją będzie zachowanie spójności informacji pomiędzy systemem wspomagania dowodzenia wykorzystywanym na stanowisku dowodzenia a jego otoczeniem, zarówno w ramach samego SD jak i poza nim.

Przeprowadzone badania pozwoliły wyodrębnić, w ramach funkcjonowania sieci teleinformatycznych na stanowisku dowodzenia, dwa zasadnicze środowiska pracy a mianowicie: środowisko kompatybilne i środowisko niekompatybilne.

Pierwsze z nich – środowisko kompatybilne – to środowisko w którym spójność informacji zachowana jest poprzez mechanizmy systemu wspomagania dowodzenia wykorzystywanego na stanowisku dowodzenia. Wszystko co przetwarzane jest w systemie wspomagania dowodzenia jest dostępne dla jego użytkowników na stanowisku dowodzenia. System zapewnia wszystkie wymagania stawiane w stosunku do informacji.

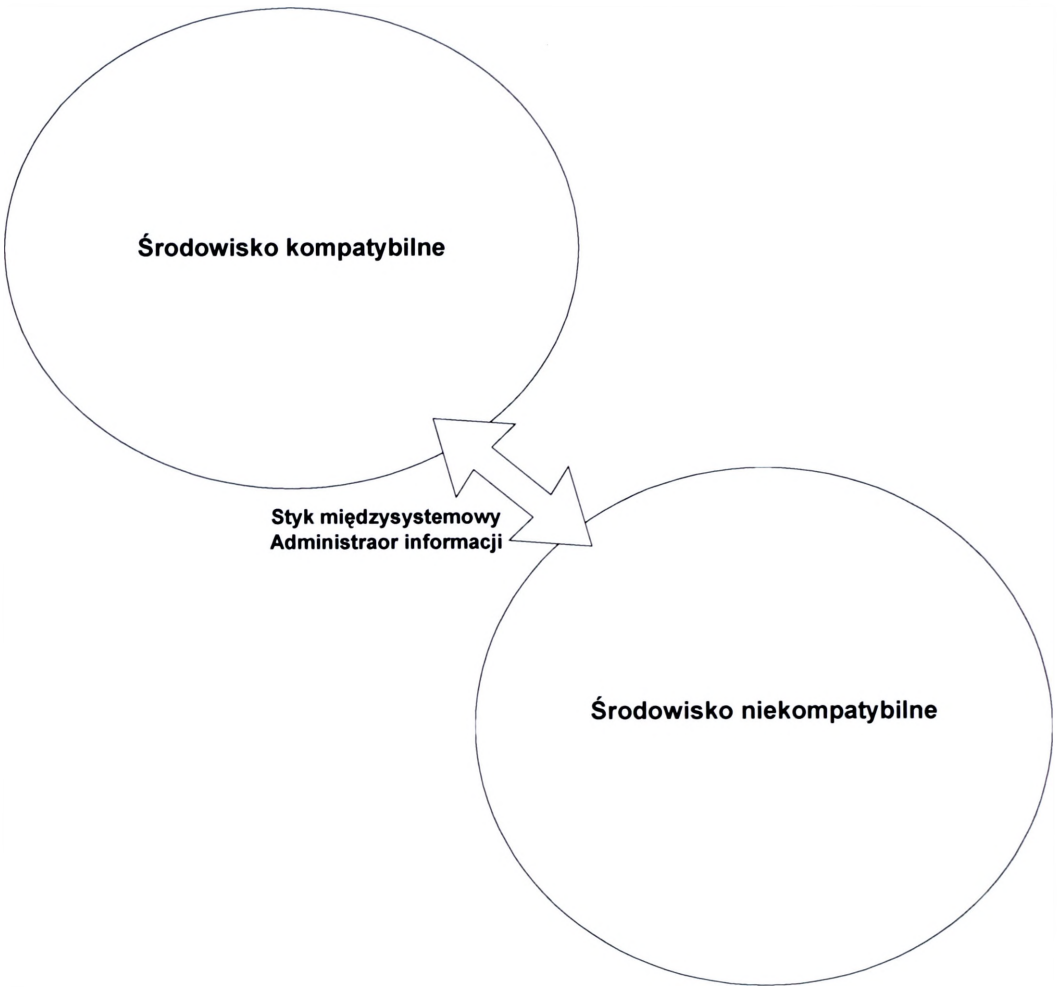
Środowisko niekompatybilne - to środowisku w którym informacja nie może być przetworzona automatycznie w systemie wspomagania dowodzenia, a organa dowodzenia posiadają różne zasoby informacyjne, często niespójne o różnej postaci. Typowym środowiskiem niekompatybilnym jest środowisko fizyczne (otoczenie SD) i środowisko sieci radiowych UKF i KF. Większość przekazywanej informacji w tym środowisku posiada postać foniczną, niesformalizowaną. Jej przetworzenie i umieszczenie w środowisku kompatybilnym wymaga odpowiedniego przetworzenia, zarządzania i procedur postępowania. Z tego też względu niezbędnym jest posiadanie organu (administratora informacji) odpowiedzialnego za wyrównywanie informacji pomiędzy środowiskiem kompatybilnym i niekompatybilnym, co zobrazowano na rysunku 4.9.

Analizując potrzeby zachowania spójności danych pomiędzy środowiskiem kompatybilnym i niekompatybilnym należy zastanowić się w jakich stanach będzie pracował system wspomagania dowodzenia i w jaki sposób będą pracowali jego użytkownicy[2]. Dokonane analizy pozwalają na wyodrębnienie pięciu zasadniczych trybów pracy systemów wspomagania dowodzenia:

- praca ciągłą w miejscu stałej dyslokacji,

[2] Użytkownik systemu występuje często pod pojęciem „klient" dla którego definiowane są odpowiednie uprawnienia i któremu systemu musi zapewnić żądane usługi.

- praca w warunkach bojowych na stanowisku dowodzenia,
- praca wydzielonej grupy (zespołu) poza stanowiskiem dowodzenia,
- praca w trakcie zmiany stanowiska dowodzenia,
- praca bez stanowisk dowodzenia.



Rys. 4.9. Środowisko kompatybilne i niekompatybilne sieci teleinformatycznych
Źródło: P. opracowanie własne

Dla potrzeb zachowania spójności danych, we wszystkich trybach, został wyróżniony **administrator informacji**[3] w systemie. Zespół ten powinien posiadać odpowiednią strukturę i odpowiednie środki techniczne umożliwiające sprawne zarządzanie informacją. Należy przyjąć, że administrator informacji powinien dysponować co najmniej następującymi urządzeniami:

- serwerem administratora informacji (zapasowym serwerem systemu wspomagania dowodzenia),

[3] Przez administratora informacji należy rozumieć odpowiedni zespół organizacyjno-funkcjonalny sztabu, stanowiska dowodzenia lub węzła teleinformatycznego stanowiska dowodzenia zdolny do zarządzania informacją zarówno w systemie wspomagania dowodzenia jak i w jego otoczeniu zewnętrznym

- wozem dowodzenia wyposażonym w środki radiowe umożliwiające pracę w sieciach radiowych: dowodzenia przełożonego, dowodzenia dowódcy i współdziałania,
- urządzeniami do rejestrowania informacji przekazywanej w sieciach dowodzenia dowódcy i współdziałania.

Głównymi zdaniami „administratora informacji" powinny być odpowiednio:

- informowanie wszystkich uprawnionych abonentów sieci radiowej o bieżącej sytuacji,
- synchronizacja informacji pomiędzy systemem wspomagania dowodzenia a otoczeniem systemu na danym szczeblu dowodzenia[4],
- rejestrowanie przekazu informacji w sieciach radiowych dowodzenia i współdziałania,
- przejęcie roli jądra systemu wspomagania dowodzenia w momencie awarii głównego serwera systemu wspomagania dowodzenia lub jego dyslokacji na nowe SD.

W pierwszym trybie (rys. 4.10.) system będzie pracował w sposób ciągły, wykorzystując do komunikacji z użytkownikami i innymi systemami stacjonarną infrastrukturę teleinformatyczną. Głównym zadaniem systemu powinna być obsługa bieżącej działalności jednostki oraz uaktualnianie baz danych systemu niezbędnych do realizacji zadań w czasie kryzysu i wojny. Jądrem systemu będzie serwer na którym znajdują się bazy danych zawierające bieżącą sytuację. Serwer ten zarządza także wymianą informacji pomiędzy użytkownikami systemu, zarówno w ramach danego sztabu jak i pomiędzy innymi sztabami oraz systemem domen informacyjnych stworzonym na bazie stacjonarnej sieci teleinformatycznej.

Drugi tryb pracy (rys. 4.11.) w praktyce nie różni się niczym od pracy w miejscu stałej dyslokacji. Użytkownicy systemu mają zapewniony ciągły dostęp do baz danych zawartych zarówno na serwerach systemu jak i w domenach informacyjnych. Mogą oni w pełnym zakresie współdzielić posiadaną informację. Jedyna różnica polega na częstych zmianach dyslokacji stanowisk dowodzenia, a tym samym potrzebą przemieszczania elementów systemu. Użytkownicy systemu na SD mogą wymieniać informację z innymi użytkownikami systemu w ramach więzi wewnętrznych SD[5], oraz pomiędzy użytkownikami znajdującymi się na różnych stanowiskach dowodzenia w ramach istniejących zewnętrznych więzi funkcjonalnych, synchronizacji i koordynacji[6]. Administrator informacji będzie odpowiadał za wymianę da-

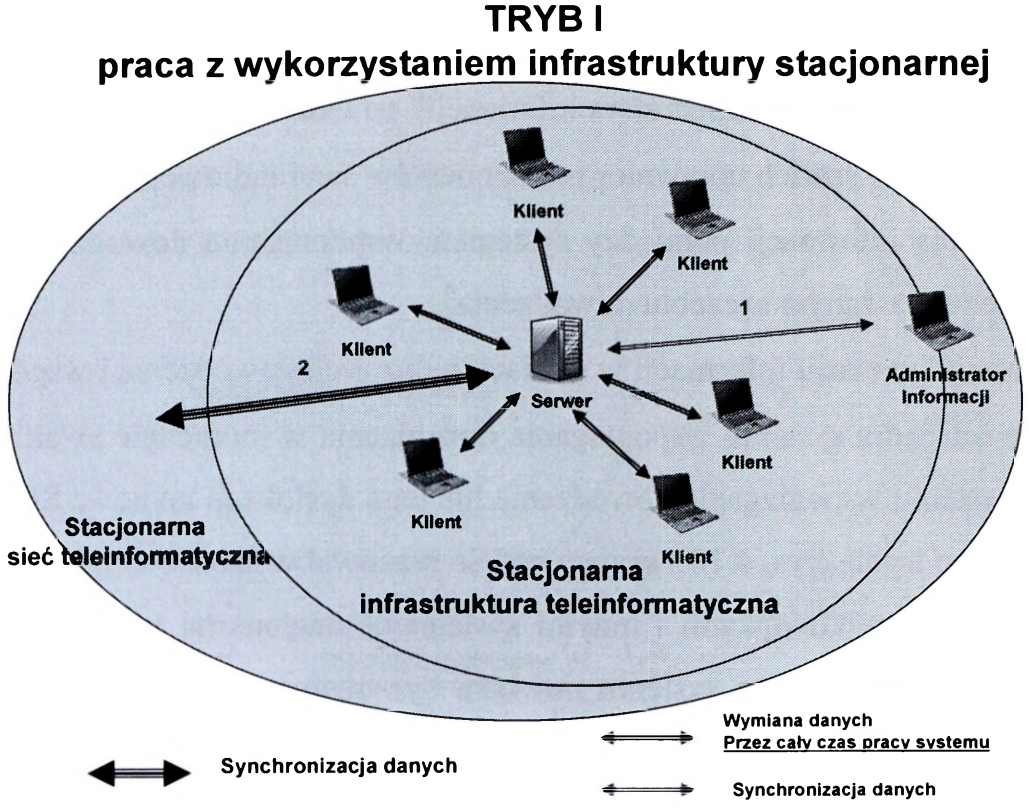
---

[4] Otoczenie systemu na danym szczeblu dowodzenia to przede wszystkim sieci radiowe dowodzenia i współdziałania nie sprzężone informacyjnie z systemem. To także informacja spływająca na stanowisko dowodzenia w postaci tradycyjnej (papierowej, ustnej).

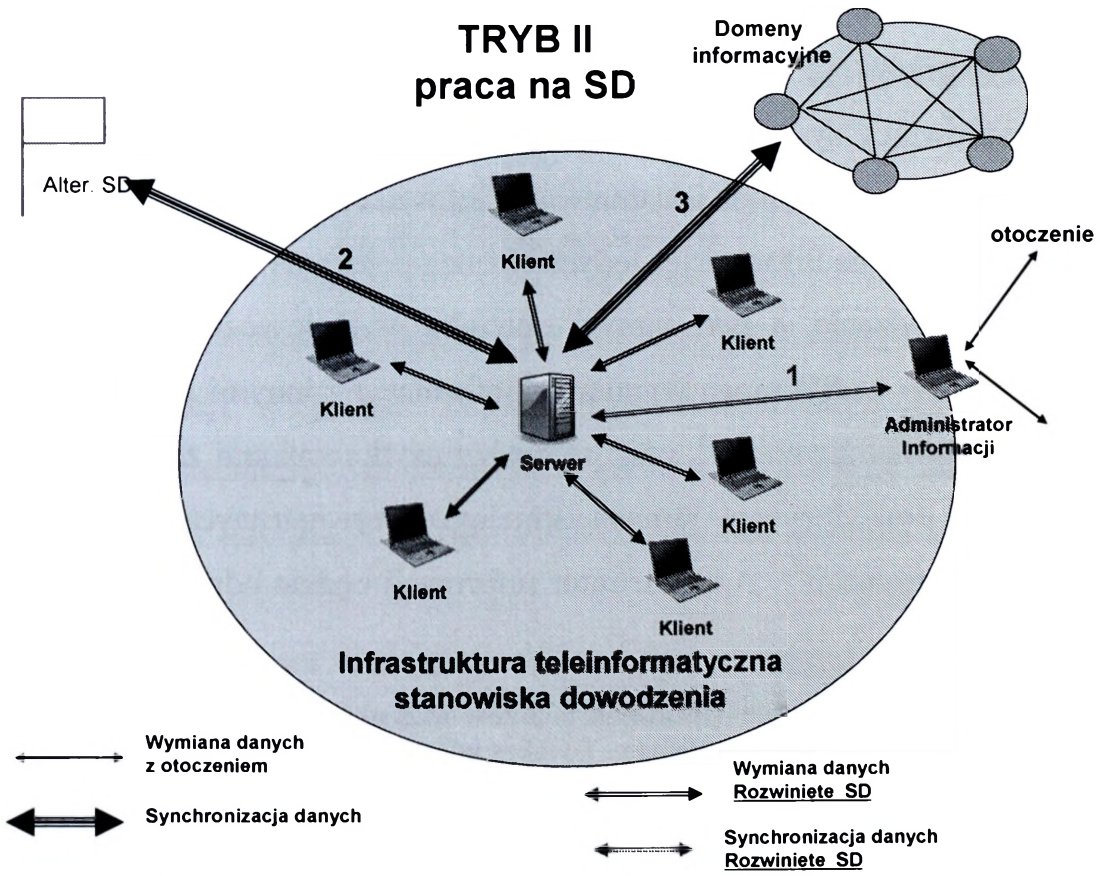
[5] Więzi wewnętrzne SD zapewnione są przez odpowiednią konfiguracją systemu wspomagania dowodzenia

[6] Zewnętrzne więzi funkcjonale, synchronizacji i koordynacji będą realizowane zarówno w ramach systemu wspomagania dowodzenia z wykorzystaniem sieci teleinformatycznych jak również poprzez sieci radiowe i pocztę polową.

nych w ramach więzi dowodzenia i współdziałania z otoczeniem zewnętrznym SD i zapewnia jej ciągłą synchronizacją z jądrem systemu. Dodatkowo wykonywana jest synchronizacja danych z serwerem znajdującym się na Alter. SD i systemem domen informacyjnych.



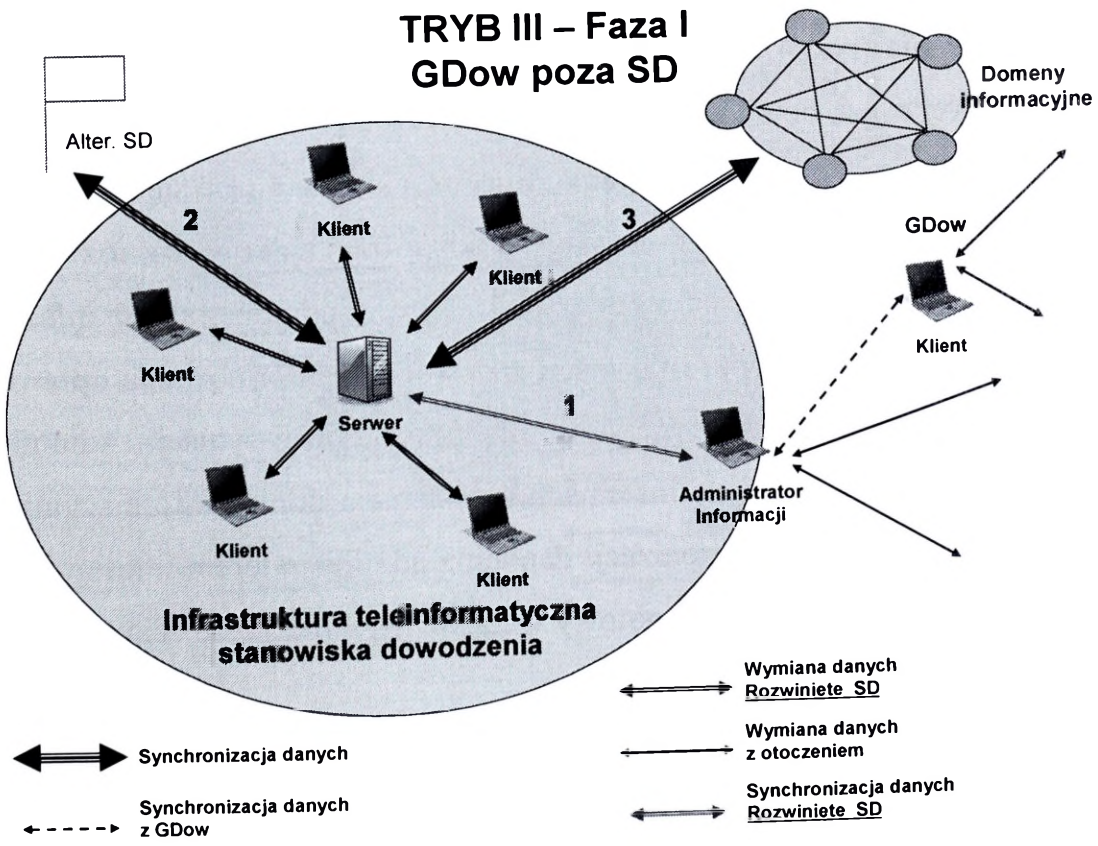
Rys. 4.10. Praca systemu wspomagania dowodzenia z wykorzystaniem infrastruktury stacjonarnej
Źródło: opracowanie własne



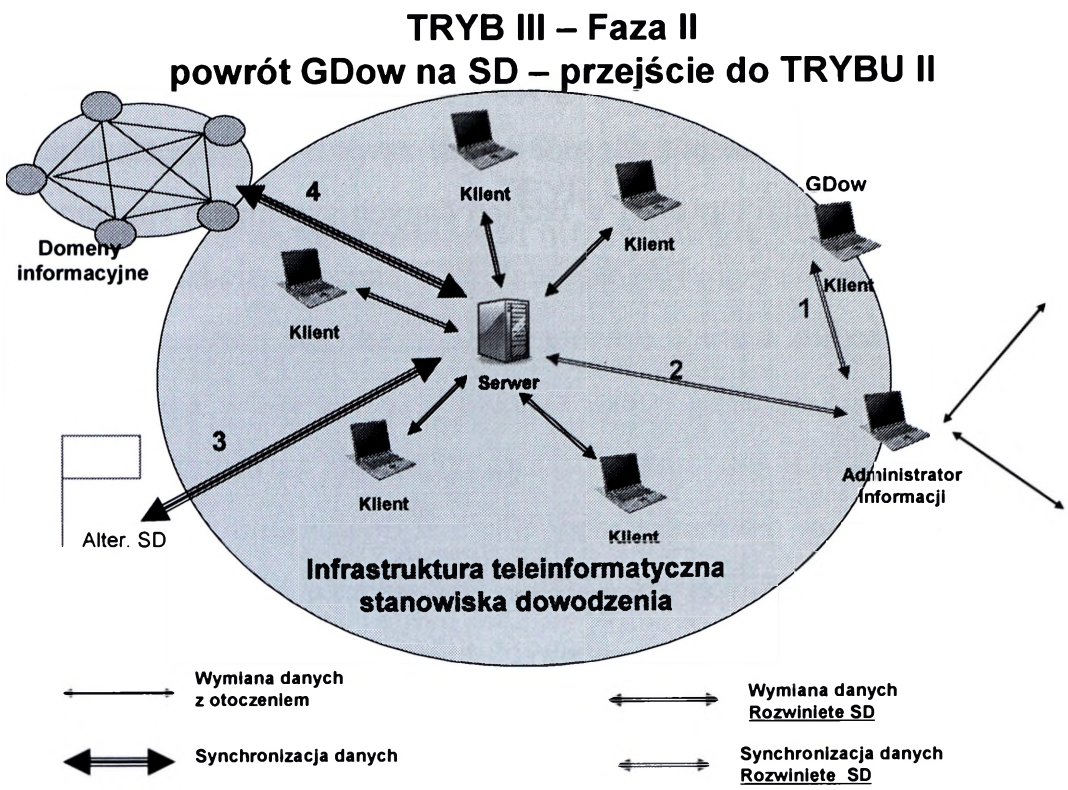
Rys. 4.11. Praca systemu wspomagania dowodzenia na SD
Źródło: opracowanie własne

Trzeci tryb pracy (rys. 4.12.) - praca wydzielonej grupy (zespołu) poza stanowiskiem dowodzenia – ma miejsce w przypadku gdy grupa dowódcy (inny zespół stanowiska dowodzenia) opuści stanowisko dowodzenia. Zespół ten nie zawsze będzie posiadał bezpośredni i niezawodny dostęp do informacji zawartej w bazach danych systemu. Tym samym może zaistnieć zjawisko niespójności danych. Różnica w ilości i jakości posiadanej informacji pomiędzy stanowiskiem dowodzenia a grupą dowódcy znajdującej się poza stanowiskiem dowodzenia może doprowadzić do błędnej oceny sytuacji przez dowódcę i podjęcia nieefektywnych decyzji. Głównym zadaniem administratora informacji powinno być wyrównywanie różnic w posiadanej informacji pomiędzy stanowiskiem dowodzenia a grupą dowódcy znajdująca się poza stanowiskiem dowodzenia. Pełne wyrównanie informacji i zapewnienie jej spójności dla wszystkich zespołów funkcjonalnych SD nastąpi po powrocie grupy dowódcy na stanowisko dowodzenia (rys. 4.13.). W pierwszej kolejności powinna zostać zsynchronizowana informacja pomiędzy grupą dowódcy a administratorem informacji, następnie pomiędzy administratorem informacji a jądrem systemu i na koniec pomiędzy SD a Alter. SD.

Opuszczenie stanowiska dowodzenia przez grupą dowódcy powoduje, że klienci (operatorzy) systemu znajdujący się w tej grupie nie będą posiadali bezpośredniego połączenia z serwerami systemu wspomagania dowodzenia, co wymusza potrzebę samodzielnej pracy aplikacji klienta systemu bez potrzeby nawiązywania połączenia z serwerami systemu.

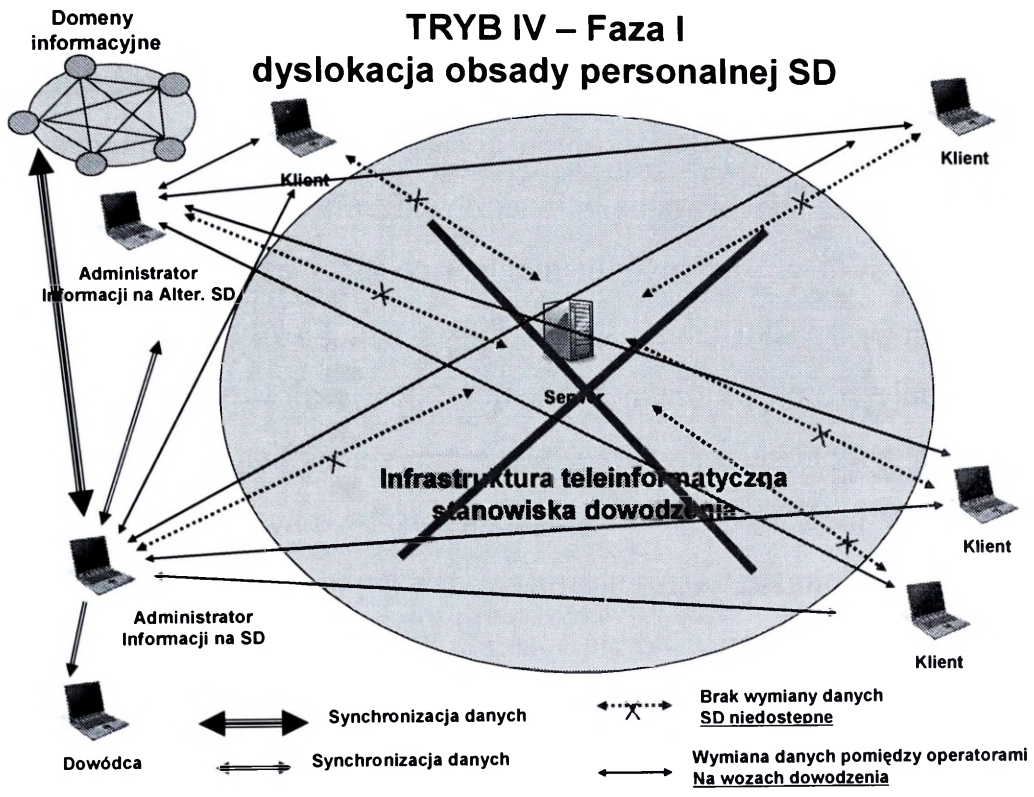


Rys. 4.12. Praca systemu wspomagania dowodzenia w trybie III – faza I
Źródło: opracowanie własne

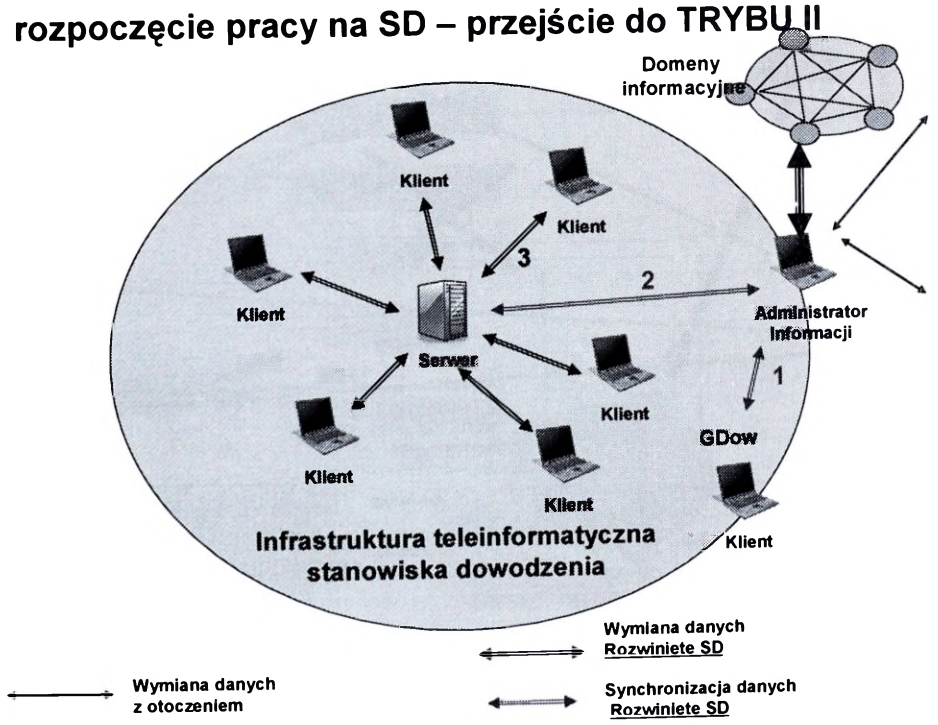


Rys4.13. Praca systemu wspomagania dowodzenia w trybie III – faza II
Źródło: opracowanie własne

Czwarty tryb pracy systemu wspomagania dowodzenia - praca w trakcie zmiany stanowiska dowodzenia (rys. 4.14.) - powoduje istotne ograniczenia w dostępie do danych zawartych na serwerach systemu wspomagania dowodzenia. W trakcie dyslokacji stanowiska dowodzenia serwery systemu wspomagania dowodzenia znajdujące się na stanowisku są wyłączone. Ich pełna funkcjonalność jest osiągana dopiero po całkowitym rozwinięciu stanowiska dowodzenia w nowym miejscu pracy (rys. 4.15.). Na administratorze informacji spoczywa zadanie wyrównania poziomu informacji z dowódcą i informowania uprawnionych abonentów sieci radiowych, znajdujących się w ruchu, o bieżącej sytuacji. Administrator informacji opowiada także za wymianę informacji z systemem domen informacyjnych. Istotnego znaczenia nabiera potrzeba synchronizacji danych z administratorem informacji znajdującym się na Alter. SD, który powinien być gotowy w każdej chwili do przejęcia roli SD.

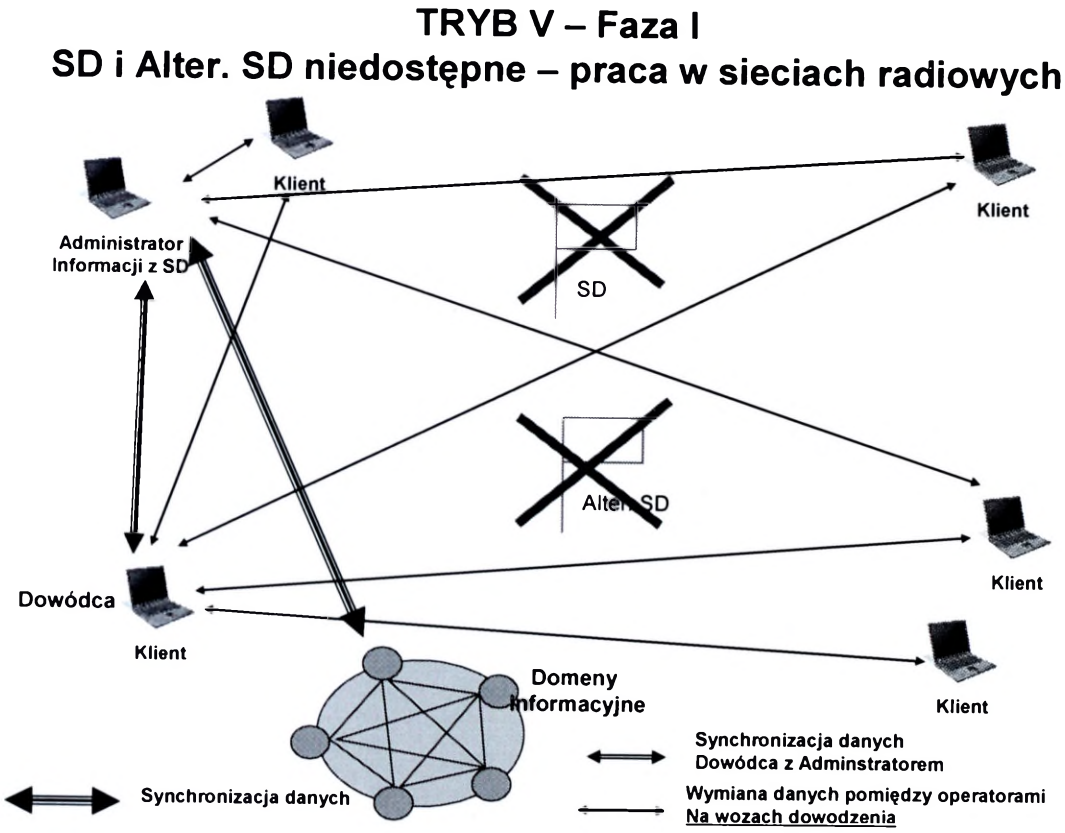


Rys. 4.14. Praca systemu wspomagania dowodzenia w trybie IV – faza I
Źródło: opracowanie własne



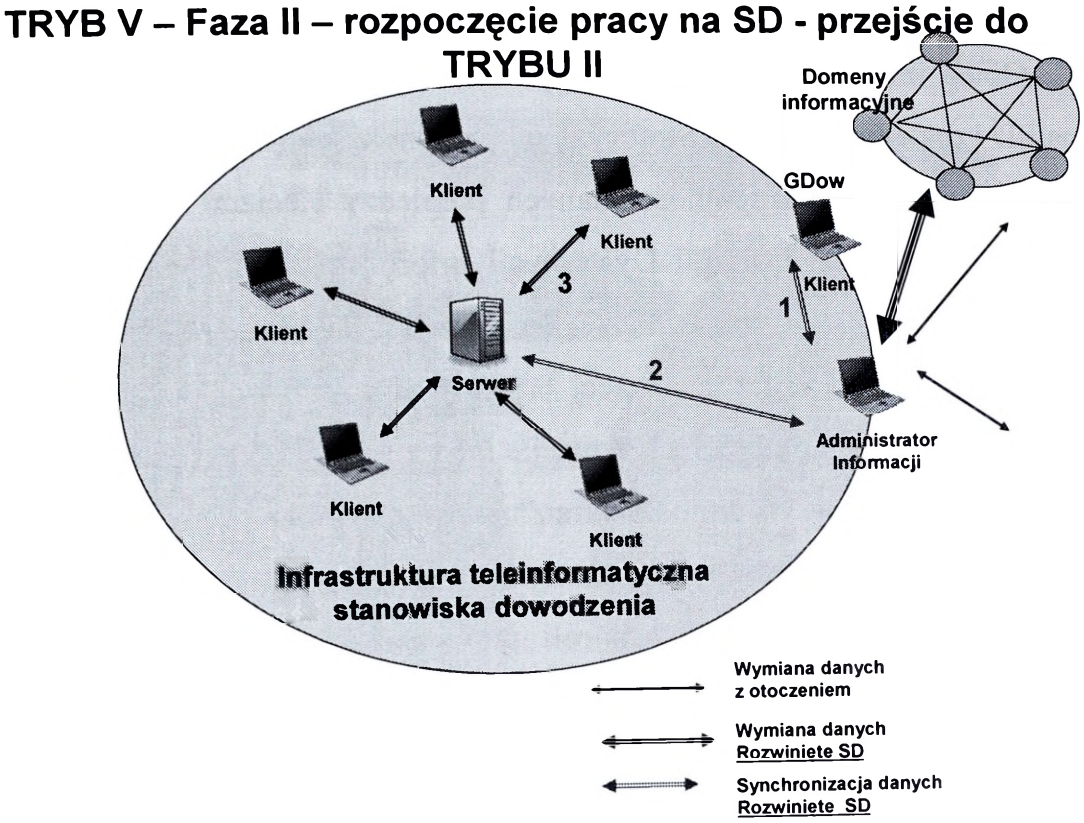
Rys. 4.15. Praca systemu wspomagania dowodzenia w trybie IV – faza II
Źródło: opracowanie własne

Ostatni tryb pracy – praca bez SD (rys. 4.16.) – może zaistnieć w momencie porażenia Alter. SD przy jednoczesnym przemieszczaniu SD. Klienci systemu będą zmuszeni do funkcjonowania, przez dłuższy czas, bez dostępu do jądra systemu wspomagania dowodzenia. Taka sytuacja jest bardzo niekorzystna z punktu widzenia spójności informacji posiadanej przez użytkowników systemu. Jedynym elementem posiadającym dostęp do baz danych systemu będzie w tym przypadku administrator informacji, który synchronizuje informację z dowódcą i udostępnia ją uprawnionym abonentom sieci radiowej. Przejście do normalnego trybu pracy nastąpi w momencie rozwinięcia jednego ze stanowisk dowodzenia (rys. 4.17.). Po rozpoczęciu pracy na SD w pierwszej kolejności powinny być zsynchronizowane dane pomiędzy dowódcą a administratorem informacji, a następnie z jądrem system na SD. Dopiero po zakończeniu synchronizacji z jądrem systemu dostęp do danych mogą uzyskać operatorzy.

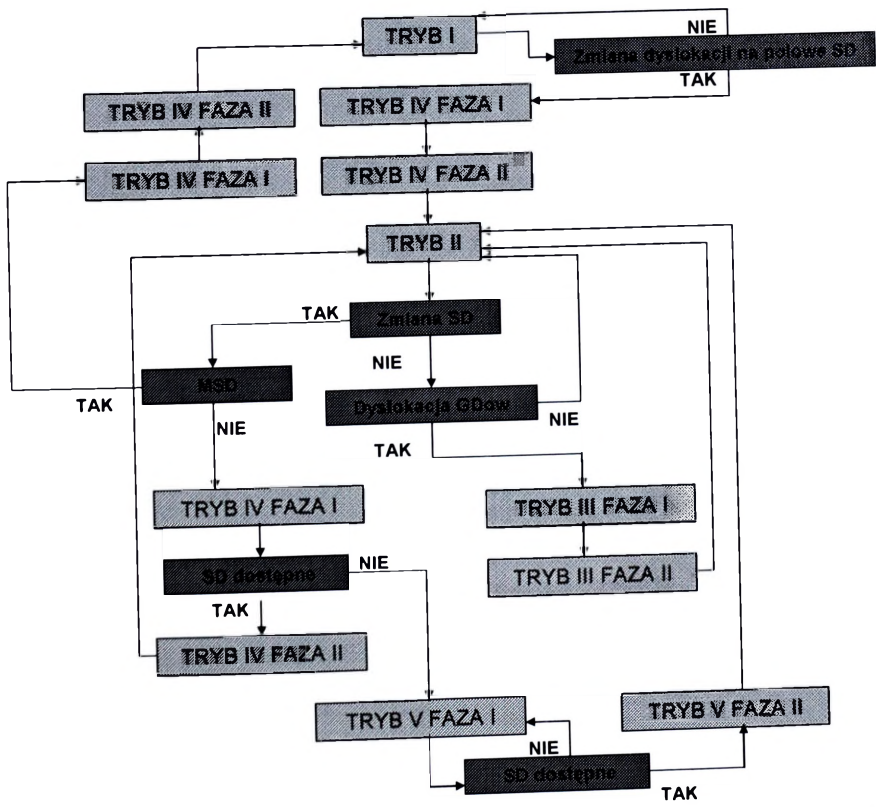


Rys. 4.16. Praca systemu wspomagania dowodzenia w trybie V – faza I
Źródło: opracowanie własne

Na rysunku 4.18. przedstawiono algorytm funkcjonowania systemu wspomagania dowodzenia z uwzględnieniem przedstawionych wcześniej trybów pracy. Przejście pomiędzy poszczególnymi trybami pracy systemu (bloki zielone) następuje w momencie zaistnienia odpowiedniego zjawiska (bloki czerwone). Algorytm ten uwzględnia ciągłą pracę systemu wspomagania dowodzenie zarówno w czasie P, K jak i W.



Rys. 4.17. Praca systemu wspomagania dowodzenia w trybie V – faza II
Źródło: opracowanie własne

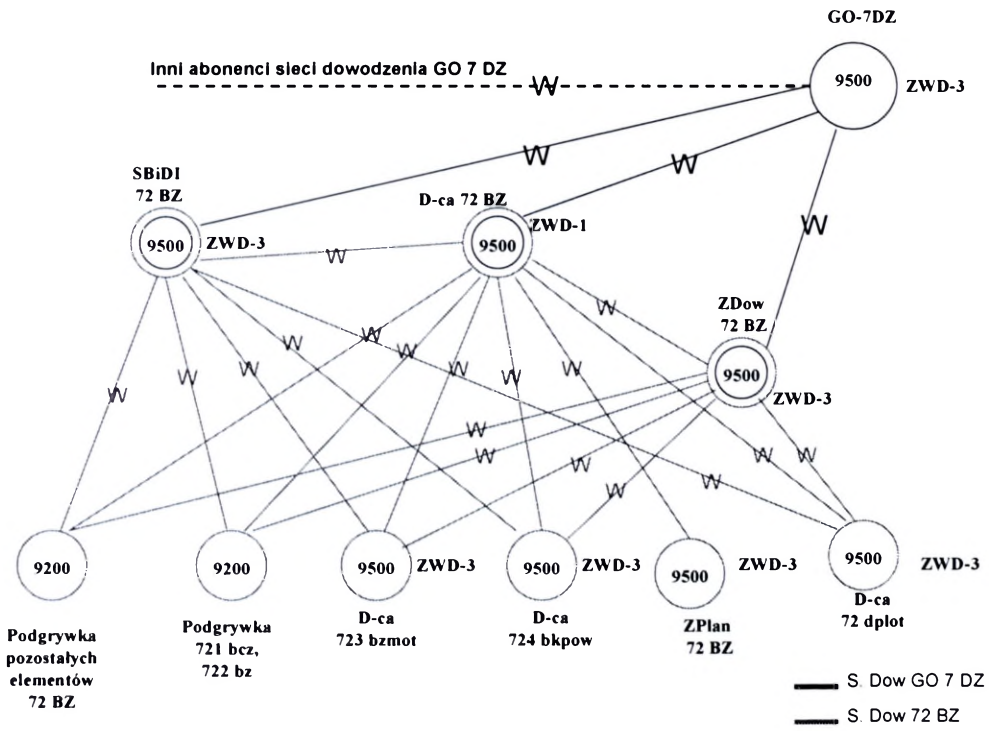


Rys. 4.18. Algorytm pracy systemu wspomagania dowodzenia
Źródło: opracowanie własne

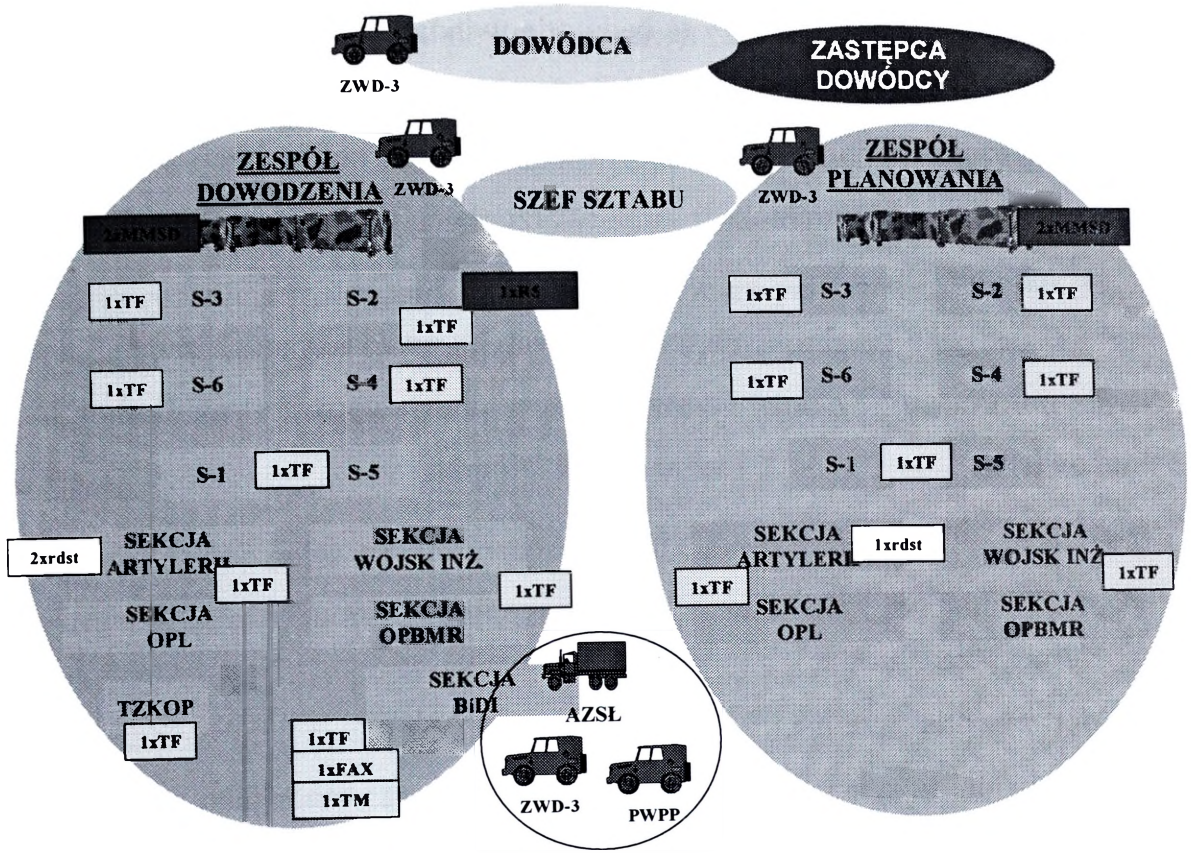
Próba stworzenia „administratora informacji" w systemie wspomagania dowodzenia została podjęta przez autora w trakcie ćwiczenia dowódczo-sztabowego „Pierścień 08" w

Akademii Obrony Narodowej. W ćwiczeniu tym na szeroką skalę został wykorzystany system „Szafran". Obieg informacji realizowany był zarówno w systemie „Szafran" poprzez sieci lokalne na SD i rozległe systemu „Storczyk" jak i poprzez sieci radiowe.

W celu zapewnienia spójności danych pomiędzy sieciami radiowymi a systemem „Szafran" Sekcja Bezpieczeństwa i Dystrybucji Informacji (SBiDI) została wyposażona w wóz dowodzenia ZWD-3 i aparatownię AZSŁ. Sekcja była abonentem sieci radiowej dowodzenia przełożonego i dowódcy ćwiczącej brygady uprawnionym do informowania innych abonentów sieci radiowej o aktualnej sytuacji. Informacje przekazywane w sieciach dowodzenia były uaktualniane w systemie „Szafran" na bieżąco przez personel SBiDI pracujący na ZWD-3. W AZSŁ umieszczony był zapasowy serwer systemu „Szafran" (ZPD – zapasowy punkt dystrybucyjny) zdolny do przejęcia roli głównego serwera (CPD – centralnego punktu dystrybucyjnego). Dodatkowym zadaniem personelu pracującego w AZSŁ było uaktualnianie w systemie „Szafran" informacji otrzymywanej pocztą polową. Na rysunku nr 4.19. przedstawiono strukturę sieci radiowej dowodzenia ćwiczącej brygady, natomiast na rysunku 4.20. zobrazowano abonentów sieci teleinformatycznej stanowiska dowodzenia ćwiczącej brygady.



Rys. 4.19. Sieć radiowa dowodzenia dowódcy ćwiczącej brygady na ćwiczeniu „Pierścień 08"
Źródło: opracowanie własne



Rys. 4.20. Abonenci sieci teleinformatycznej stanowiska dowodzenia ćwiczącej brygady na ćwiczeniu „Pierścień 08"
Źródło: opracowanie własne

Abonentami sieci teleinformatycznej stanowiska dowodzenia były zarówno wszystkie sekcje w zespole dowodzenia i zespole planowania (na MMSD) jak również wszystkie wozy dowodzenia ZWD-3 i AZSŁ pracujące na SD.

Wnioski

Wyniki badań przedstawione w niniejszym rozdziale, dotyczące zarządzania informacją uprawniają do sformułowania następujących wniosków:

1. Informacja wytworzona w procesie dowodzenia powinna być przechowywana nie tylko na stanowiskach dowodzenia ale także w globalnej sieci informacyjnej. Istniejące technologie teleinformatyczne pozwalają na stworzenie odpowiedniej struktury logicznej domen informacyjnych, które umożliwią zarządzanie informacją w sposób spójny na poziomie całych wojsk lądowych (sił zbrojnych). Domeny informacyjne zapewnią ciągły dostęp do informacji nie tylko w ramach danego organu dowodzenia, ale także w ramach całej struktury dowodzenia zarówno w relacjach dowodzenia, współdziałania jak i funkcjonalnych.

2. System domen informacyjnych powinien być postrzegany poprzez strukturę zarówno fizyczną jak i logiczną. Struktura fizyczna to zbiór serwerów umieszczonych w węzłach sieciowych sieci informacyjnej. Serwery te będą odpowiadały za przechowywanie informacji w bazach danych oraz za prawidłowe funkcjonowanie struktury logicznej domen informacyjnych. Struktura logiczna domen informacyjnych to sposób konfiguracji poszczególnych domen w postaci struktury hierarchicznej oraz tworzenia na jej bazie struktur domen wynikających z bieżących potrzeb.

3. Z uwagi na specyfiką sił zbrojnych, charakterystykę wykonywanych zadań i wynikające z tego potrzeby informacyjne należy wyróżnić cztery podstawowe rodzaje domen informacyjnych a mianowicie:

- domeny hierarchiczne;
- domeny specjalistyczne;
- domeny zadaniowe;
- domeny przestrzenne.

4. W ramach funkcjonowania sieci teleinformatycznych na stanowisku dowodzenia można wyróżnić dwa zasadnicze środowiska pracy a mianowicie: środowisko kompatybilne i środowisko niekompatybilne. Pierwsze z nich – środowisko kompatybilne – to środowisko w którym spójność informacji zachowana jest poprzez mechanizmy systemu wspomagania dowodzenia wykorzystywanego na stanowisku dowodzenia. System zapewnia wszystkie wymagania stawiane w stosunku do przetwarzanej (posiadanej) informacji. Środowisko niekompatybilne - to środowisko w którym informacja nie może być przetworzona automatycznie w systemie wspomagania dowodzenia, a organa dowodzenia posiadają różne zasoby informacyjne, często niespójne o różnej postaci. Z tego też względu niezbędnym jest posiadanie organu (administratora informacji) odpowiedzialnego za wyrównywanie informacji pomiędzy środowiskiem kompatybilnym i niekompatybilnym.

6. Należy wyodrębnienie pięciu zasadniczych trybów pracy systemów wspomagania dowodzenia:

- praca ciągłą w miejscu stałej dyslokacji,
- praca w warunkach bojowych na stanowisku dowodzenia,
- praca wydzielonej grupy (zespołu) poza stanowiskiem dowodzenia,
- praca w trakcie zmiany stanowiska dowodzenia,
- praca bez stanowisk dowodzenia.

Dla potrzeb zachowania spójności danych, we wszystkich trybach, powinien występować zespół administratora informacji w systemie, który posiada odpowiednią strukturę organizacyjno-funkcjonalną i odpowiednie środki techniczne umożliwiające sprawne zarządzanie informacją. Głównymi zdaniami „administratora informacji" powinny być odpowiednio:

- informowanie wszystkich uprawnionych abonentów sieci radiowej o bieżącej sytuacji,
- synchronizacja informacji pomiędzy systemem wspomagania dowodzenia a otoczeniem zewnętrznym systemu na danym szczeblu dowodzenia,
- rejestrowanie przekazu informacji w sieciach radiowych dowodzenia i współdziałania,
- przejęcie roli jądra systemu wspomagania dowodzenia w momencie awarii głównego serwera systemu wspomagania dowodzenia lub jego dyslokacji na nowe SD.

ZAKOŃCZENIE

Wyniki badań przedstawione w niniejszej pracy naukowo-badawczej pozwalają na stwierdzenie, że początki teorii walki sieciocentrycznej są rezultatem rozwoju technologii informatycznych i ich szerokiego komercyjnego wykorzystania. Walka sieciocentryczna jest sposobem prowadzenia działań w którym siły zbrojne, spięte sieciami teleinformatycznymi, uzyskują przewagę informacyjną na wszystkich poziomach prowadzenia działań, co pozwala na prowadzenie szybkich i skutecznych działań militarnych przy możliwie najefektywniejszym i ekonomiczniejszym wykorzystaniu własnych sił.

Idea zarządzania informacją z wykorzystaniem domen informacyjnych polega na przyjęciu założenia, że informacja wytwarzana przez organ decyzyjny (dowództwo danego szczebla) jest przechowywana zarówno na jego stanowisku dowodzenia jak i w domenie informacyjnej. Domena znajdująca się w globalnej sieci informacyjnej poprzez swoje właściwości zapewnia podstawowe wymagania nakładane na informację a mianowicie: dostępność, wiarygodność, bezpieczeństwo, spójność, trwałość i aktualność informacji. Jednocześnie system domen informacyjnych stanowi system rozproszony co implikuje możliwość zapewnienia odpowiednio: współdzielenia zasobów, otwartości, współbieżności, skalowalności, przeźroczystości i tolerowania uszkodzeń.

Należy zauważyć, że system domen informacyjnych będzie postrzegany w dwojaki sposób, zarówno poprzez strukturę fizyczną jak i poprzez strukturę logiczną. Struktura fizyczna stanowił zbiór odpowiednich serwerów umieszczonych w przestrzeni sieciocentrycznej (sieciach teleinformatycznych). Serwery te będą odpowiadały za przechowywanie informacji oraz za prawidłowe funkcjonowanie domen informacyjnych. Z tego też względu należy wyróżnić trzy zasadnicze grupy serwerów a mianowicie:

- serwery adresowe domen;
- serwery zarządzające bezpieczeństwem sieci (domen);
- serwery przechowujące informację.

Z uwagi na specyfiką sił zbrojnych, charakterystykę wykonywanych zadań i wynikające z tego potrzeby informacyjne należy wyróżnić cztery podstawowe rodzaje domen informacyjnych a mianowicie:

- domeny hierarchiczne;
- domeny specjalistyczne;

- domeny zadaniowe;
- domeny przestrzenne.

Dostęp do informacji na poziomie domen pozwoliłby na rezygnacją z dotychczasowego systemu meldunkowo na rzecz współdzielenia informacji.

Innym aspektem związanym z zarządzaniem informacją jest organizacja pracy na stanowisku dowodzenia. W ramach funkcjonowania sieci teleinformatycznych na stanowisku dowodzenia należy wyróżnić dwa zasadnicze środowiska pracy a mianowicie: środowisko kompatybilne i środowisko niekompatybilne. Pierwsze z nich – środowisko kompatybilne – to środowisko w którym spójność informacji zachowana jest poprzez mechanizmy systemu wspomagania dowodzenia wykorzystywanego na stanowisku dowodzenia. Środowisko niekompatybilne - to środowisko w którym informacja nie może być przetworzona automatycznie w systemie wspomagania dowodzenia, a organa dowodzenia posiadają różne zasoby informacyjne, często niespójne o różnej postaci. Niezbędnym rozwiązaniem organizacyjnym jest stworzenie organu (administratora informacji) odpowiedzialnego za wyrównywanie informacji pomiędzy środowiskiem kompatybilnym i niekompatybilnym.

Pozytywna weryfikacja przyjętej hipotezy roboczej oraz udzielenie w rozdziałach merytorycznych odpowiedzi na przyjęte we wstępie pytania problemowe, są podstawą, zdaniem autorów, do stwierdzania, że cel pracy naukowo-badawczej został osiągnięty.

W opinii autorów praca stanowi istotny wkład w rozwiązanie przyjętych problemów. Zawiera wyniki badań, które mają wymierne walory zarówno poznawcze jak i utylitarne. Przedstawione poglądy i rozwiązania mogą stanowić asumpt do podejmowania dalszych działań tym obszarze. Konieczność ta wynika zarówno z charakteru głównego problemu badawczego, który jest problemem otwartym, jak też z istnienia w jego otoczeniu wielu nie opracowanych naukowo problemów.

Bibliografia

1. Active Directory Services for Microsoft Windows 2000 Technical Reference, Microsoft Press.
2. Antczak S. Informacja w dowodzeniu siłami powietrznym, AON, Warszawa 2002.
3. Bajda A., Rodycz S., Podstawy organizacji łączności. Wojskowe systemy łączności, wyd. WAT, Warszawa 2002.
4. Cebrowski A., Garstka J., Network Centric Warfare - Its Origins and Future, Proceedings of the Naval Institute 1998
5. Cieślik P., Koncepcja walki sieciocentrycznej, Przegląd SP nr 9/2006
6. Coulouris G., Dollimore J., Kindberg T., Systemy rozproszone - podstawy i projektowanie, Warszawa, Wydawnictwa Naukowo-Techniczne 1998
7. C^4ISR Handbook for Integrated Planning, Washington 1998, s. 5-6, FM 11-55 Mobile Subscriber Equipment (MSE) Operations, Department of the Army, Washington 1999.
8. Czekaj J. Metody zarządzania informacją w przedsiębiorstwie, WAE, Kraków 2000.
9. Dalecki R., Nowosielski L., Tomaszewski B., Taktyczna sieć wymiany informacji z zastosowaniem szerokopasmowych radiostacji sieci IP-HCDR, Materiały z międzynarodowej konferencji naukowej nt. Sieci teleinformatyczne w działaniach sieciocentrycznych", Warszawa, AON 2007
10. Daniluk P., Radiowa służba stała i ruchoma, Warszawa, AON 2004
11. Daniluk P., Taktyczny system łączności radiowej wojsk lądowych, rozprawa habilitacyjna, AON, Warszawa 2006
12. Dela P., Klasyfikacja i obieg informacji w środowisku zautomatyzowanych systemów dowodzenia", referat z XIII Konferencji naukowej „Automatyzacji dowodzenia", Kraków 11-13 maj 2005.
13. Dela P., Sieci komputerowe stanowisk dowodzenia, AON, Warszawa 2007
14. Dowodzenia w środowisku zautomatyzowanych systemów, praca naukowo-badawcza, AON, Warszawa 2005
15. Dras M., Systemy sprzętowe do budowy polowych sieci teleinformatycznych na stanowiskach dowodzenia, materiały z sympozjum „Sieci teleinformatyczne stanowisk dowodzenia wojsk lądowych szczebla taktycznego", wyd. AON, Warszawa 2005.
16. Fiołna Zb., Sieć łączności związku operacyjnego, wyd. AON, Warszawa 2002.
17. Fiołna Zb. i inni, Podstawowe relacje dowodzenia oddziału, związku taktycznego i związku operacyjnego w działaniach wojsk lądowych, część II - album schematów, wyd. AON, Warszawa 2001.
18. FM 11-43 The Signal Leader's Guide, Department of the Army, Washington 1995.
19. Głowacki A., „Działanie grupy rekonesansowej w rejonie ześrodkowania batalionu", PWL nr 9/2002.
20. Gryfie R. W. Podstawy zarządzania organizacjami, PWN, Warszawa 1999

21. Huzarski M., Zagadnienia taktyki wojsk lądowych, Wydawnictwo Adam Marszałek, Toruń 1999

22. Huzarski M., Rozwój taktyki wojsk lądowych w aspekcie współczesnych konfliktów zbrojnych, praca naukowo-badawcza, AON, Warszawa 2005

23. Instrukcja łączności „Polowe węzły łączności związków operacyjnych", wyd. Szt. Gen WP, Warszawa 1966.

24. Instrukcja, Polowe węzły łączności związków taktycznych, oddziałów i pododdziałów, tom 1, wyd. Szt. Gen WP, Warszawa 1983.

25. Instrukcja, Polowe węzły łączności związków taktycznych, oddziałów i pododdziałów, tom II załączniki, tom 1, wyd. Szt. Gen WP, Warszawa 1983.

26. Instrukcja Wojennego Systemu Dowodzenia, wyd. Szt. Gen. WP, Warszawa 1998

27. IP routing in the Global Information Grid, and similar network, OSD NII 2006

28. Jajuga T., Jajuga K., Wrzosek S., Elementy teorii systemów i analizy systemowej, AE, Wrocław 1993

29. Janczak J., Daniluk P., Wisz A., Kierowanie mobilnymi systemami łączności wojsk lądowych, Część III, wyd. AON, Warszawa 2002.

30. Janczak J., Daniuk i inni, Środki dowodzenia, wyd. AON, Warszawa 2003.

31. Janczak J., Wisz A., System łaczności brygady, AON, Warszawa 2003

32. Janczak J. i inni, Mobilne sieci telekomunikacyjne – album schematów, Warszawa, Warszawa 2003

33. Janczak J. i inni, Metody i treść pracy dowództw jednostek wsparcia dowodzenia, wyd. AON 2004

34. Leksykon wiedzy wojskowej, MON, Warszawa 1979

35. Kaczmarek W., Struktury organizacyjne związków operacyjnych adekwatne do przewidywanych zadań, praca naukowo-badawcza, AON, Warszawa 1999

36. Kieżun W. Sprawne zarządzanie organizacją, SGH, Warszawa 1997

37. Klawitter Zb., i inni, Kierowanie mobilnymi systemami łączności wojsk lądowych. Cz. II. Odziały, pododdziały dowodzenia i łączności, wyd. AON, Warszawa 2003.

38. Koliński K. Kierunki rozwoju systemów dowodzenia w obronie powietrznej, AON, Warszawa 1996.

39. Kowalewski M., System łączności dywizji. Rozprawa habilitacyjna, AON, Warszawa, 1994

40. Kręcikij J., Wołejszo J. i inni, Podstawy dowodzenia, AON, Warszawa 2007

41. Kulma W., Mazurkiewicz J. W., System dowodzenia i łączności związku taktycznego, AON, Warszawa, 1996

42. Kuziak R., Strzelczyk K., Wirkus, Rozwój wojskowych systemów łączności" - Przegląd telekomunikacyjny nr 4, Warszawa 2001.

43. Kuziak R., Strzelczyk K.,, Wirkus, Łączność w Wojsku Polskim " - Przegląd telekomunikacyjny nr 4, Warszawa 2001.

44. Kuziak R., Weryfikacja szczegółowej architektury SSŁ ZO Wląd i rozwiązań technicznych na podstawie wyników badań laboratoryjnych, wyd. WIŁ Zegrze 2002.

45. Martyniak Z. Zarządzanie informacją i komunikacją: zagadnienia wybrane w świetle studiów i badań empirycznych, WAE, Kraków 2000.

46. Mazurkiewicz J., Leksykon łączności wojskowej, AON, Warszawa 1996

47. Michniak J. i inni, Metody i treść pracy zespołów funkcjonalnych na stanowisku dowodzenia wojsk lądowych, wyd. AON, Warszawa 2000.

48. Michniak J., Kierowanie mobilnymi systemami łączności wojsk lądowych. Cz. I. Główne problemy, AON, wyd. AON, Warszawa 2002.

49. Michniak J., Stanowiska dowodzenia w wojskach lądowych, wyd. AON Warszawa 2003.

50. Michniak J., Dowodzenie i Łączność, Akademia Obrony Narodowej, Warszawa 2005.

51. Michniak J., Dowodzenie w teorii i praktyce wojsk, AON, Warszawa 2003

52. Michniak J., Teoria wojskowych systemów łączności, AON, Warszawa 1996

53. Nowak J, Chojnacki M. Dowodzenie siłami powietrznymi cz. II. Systemy dowodzenia siłami powietrznymi, AON, Warszawa 2004.

54. Nożko K., Sztuka tworzenia przewagi w systemie obronnym RP, Bellona, Warszawa 1994

55. Olesiński J. Ekonomika informacji, PWE, Warszawa 2001.

56. Organizacja szkolenia dowództw i sztabów w siłach zbrojnych RP (D.D/7.1), wyd. Szt. Gen. WP, Warszawa 2004.

57. Piela J. Multilateral Interoperability Programme stan aktualny i kierunki rozwoju, materiały z XIII Konferencji „Automatyzacja dowodzenia", Kraków 2005

58. Praca zbiorowa pod kierunkiem Janczaka J., System Łączności Brygady, Warszawa, AON 2004

59. Program badawczy „Zaawansowane metody i techniki tworzenia świadomości sytuacyjnej w działaniach sieciocentrycznych" - Nr PBZ–MNiSW–DBO–02/I/2007

60. Pszczołowski T., Zasady sprawnego działania, wyd. WP Warszawa 1982.

61. Shelton H., Joint Doctrine for Information Operations, Joint Chiefs of Staff 1998.

62. Sieci teleinformatyczne stanowisk dowodzenia szczebla taktycznego wojsk lądowych, materiały z sympozjum ZSŁiI, Warszawa, AON 2006.

63. Sieci komputerowe węzłów łączności wojsk lądowych, praca naukowo-badawcza, AON, Warszawa 2006

64. Sienkiewicz P., Bezpieczeństwo informacyjne w erze globalizacji, Wydawnictwo Akademii Obrony Narodowej w Warszawie, Zeszyty Naukowe AON nr 3-4 (48-49) 2002.

65. Sienkiewicz P, Wielebna R, Wocial J. Wartość informacji w dowodzeniu i zarządzaniu: metoda oceny wartości informacji, AON, Warszawa 2003.

66. Sienkiewicz P. Wartość informacji w dowodzeniu i zarządzaniu: metodologia analizy potrzeb informacyjnych, AON, Warszawa 2002.

67. Small S., Terzis A., Monrose F., Scalable VPNs for the Global Information Grid, Johns Hopkins University.

68. Sobolewski G., Współczesne koncepcje budowy struktur organizacyjnych pododdziałów wojsk lądowych, praca naukowo-badawcza, AON, Warszawa 2008

69. Sołoma L., Metody i techniki badań socjologicznych, wybrane zagadnienia, wyd. WSP, Olsztyn 1995

70. Strzoda M., Prusiński N., System Dowodzenia. Terminologia. Część I., AON, Warszawa 2001Srzoda M. Zarządzanie informacją w organizacji, AON, Warszawa 2004.

71. Systemy teleinformatyczne na potrzeby kierowania reagowaniem kryzysowym, praca naukowo-badawcza, AON, Warszawa 2007

72. Szpakowicz R., Wojna w Iraku a koncepcja wojny sieciocentrycznej, Przegląd Wojsk Lotniczych i Obrony Powietrznej, nr 11/2003.

73. Szubrycht T., Współczesne systemy wsparcia dowodzenia jako przykłady wdrażania idei sieciocentryczności, materiały z XIII Konferencji „Automatyzacja dowodzenia", Kraków 2005

74. Ścibiorek Z., Wpływ nowych środków walki na działania bojowe wojsk lądowych, AON, Warszawa 1993

75. Ścibiorek Z., Wojna czy pokój?, Zakład Narodowy im. Ossolińskich, Wrocław–Warszawa–Kraków 1999

76. Tomaszewski B., Wnioski i doświadczenia z przygotowania, organizacji i rozwinięcia systemu łączności oraz informatycznego wspomagania polskiego kontyngentu wojskowego w większej sile do działań w dużym oddaleniu od terytorium kraju, Referat w .mat konf.:: Łączność w operacjach reagowania kryzysowego, wyd. AON, Warszawa 2003

77. Wisz A., Kierowanie polowymi systemami łączności, część IV, dokumenty i znaki łączności, wyd. AON, Warszawa 2001.

78. Wisz A., Sieć łączności dywizji wojsk lądowych SZ RP na współczesnym polu walki, wyd. AON, Warszawa 2005.

79. Wołejszo J., Metody i treść pracy zespołów funkcjonalnych na stanowisku dowodzenia wojsk lądowych Cz. IV. Rekonesans, wyd. AON, Warszawa 2001.

80. Wołejszko J. Dowództwa i stanowiska dowodzenia, organizacja, rozmieszczanie i przemieszczanie" wyd. AON, Warszawa 2002.

81. Wołejszo J., Więzi informacyjne stanowisk dowodzenia szczebla taktycznego WLąd. mat. sympozjum AON 2005.

82. Wołejszo J., Fiołna Z., Dowodzenie brygadą zmechanizowaną (pancerną) w obronie, AON, Warszawa 2002

83. Wołejszo J ., Fiołna Z., *Dowodzenie brygadą zmechanizowaną (pancerną) w marszu,* AON Warszawa 2002;

84. Wołejszo J., Fiołna Z., *Dowodzenie brygadą zmechanizowaną w działaniach opóźniających,* AON Warszawa 2000;

85. Współczesne środki dowodzenia dowództw szczebla taktycznego wojsk lądowych w działaniach wielonarodowych, praca naukowo-badawcza, AON, Warszawa 2008

86. Zawadzki W, Majewski T, Prusiński N. Informacyjne uwarunkowania procesu decyzyjnego, AON, Warszawa2002.

87. Zaskórski P., Automatyzacja procesów dowodzenia, wyd ECE Adam Marszałek Toruń, 2001.

88. Zasady przygotowania i opracowywania podstawowych dokumentów dowodzenia, wyd. Szt. Gen. WP, Warszawa 2002.

89. Zarządzanie informacjami w procesie dowodzenia na szczeblach taktycznych wojsk lądowych z wykorzystaniem sieci teleinformatycznych, praca naukowo-badawcza, AON, Warszawa 2006

90. Zarządzanie zasobami informacyjnymi w Siłach Powietrznych, materiały z sympozjum, Warszawa, AON 2001

Źródła elektroniczne:

1. http://infojama.pl/150,artykul.aspx;
2. http://www.technet.microsoft.com;
3. http://msdn.microsoft.com/en-us/library/aa366101(VS.85).aspx;
4. http://support.microsoft.com/kb/310996/PL;
5. http://freesoft.org/CIE/RFC/1035/13.htm;
6. http://en.wikipedia.org/wiki/SRV_record;
7. http://infojama.pl/177,artykul.aspx;
8. http://technet.microsoft.com/pl-pl/library/cc776927(WS.10).aspx;
9. http://pl.wikipedia.org/wiki/NTLM;
10. http://www.iana.org/domains/root/db/;
11. http://technet.microsoft.com/pl-pl/library/bb742582(en-us).aspx;
12. http://pl.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority;
13. http://pl.wikipedia.org/wiki/ICANN;
14. http://www.dmoz.org/World/Polski/Komputery/Internet/Domeny/;
15. http://pl.wikipedia.org/wiki/DNS;
16. http://www.dns.pl/rejestracja-domen.html#1;
17. http://www.dns.pl/essentials_pl.html;
18. http://dns.pl/porozumienie/partner.html;
19. http://dns.pl/index.html;
20. http://pl.wikipedia.org/wiki/Internationalized_Domain_Name;
21. http://dns.pl/IDN/info.html;
22. http://dns.pl/IDN/programy.html;
23. https://www.dns.pl/dnssec/theory_intro.html;
24. http://pl.wikipedia.org/wiki/UDP;
25. http://pl.wikipedia.org/wiki/TCP_(protok%C3%B3%C5%82);
26. https://www.dns.pl/dnssec/theory_intro.html;
27. http://kb.forpsi.pl/article.php?id=130;
28. http://technet.microsoft.com/pl-pl/library/cc787034(WS.10).aspx;
29. http://technet.microsoft.com/pl-pl/library/cc780347(WS.10).aspx;
30. http://pl.wikipedia.org/wiki/Atak_man_in_the_middle;
31. http://pl.wikipedia.org/wiki/VPN;
32. http://pl.wikipedia.org/wiki/VNC;
33. http://pl.wikipedia.org/wiki/Anycast";

34. http://system.opendns.com;
35. http://iname.pl/2008/03/open-dns-ciekawa-alternatywa/;
36. http://pl.wikipedia.org/wiki/BIND;
37. https://www.isc.org/solutions.