



AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ LOTNICTWA I OBRONY POWIETRZNEJ

SIECIOCENTRYCZNE POLE WALKI. WYMAGANIA WOBEC SIŁ POWIETRZNYCH

(II.6.6.1.0)

59584

WARSZAWA

2005



AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ LOTNICTWA I OBRONY POWIETRZNEJ



**SIECIOCENTRYCZNE POLE WALKI.
WYMAGANIA WOBEC SIŁ POWIETRZNYCH**

(II.6.6.1.0)

Zespół autorski:

1. Płk pil. dr hab. Stanisław ZAJAS – kierownik zespołu (wstęp, podrozdziały: 1.1, 1.4, 2,3, 3.4, zakończenie)
2. Płk nawig. dr Eugeniusz CIEŚLAK (podrozdziały: 2.1, 3.1, 3.2, 3.3)
3. Ppłk dr inż. Ryszard BARTNIK (podrozdział 1.3)
4. Kpt. mgr. Piotr CIEŚLIK (podrozdziały: 1.2, 2.2)

Recenzent:

Płk prof. dr hab. Adam TOMASZEWSKI

SPIS TREŚCI

	Strona
WSTĘP	3
Rozdział 1. WALKA SIECIOCENTRYCZNA. ISTOTA I PODSTAWOWE ZAŁOŻENIA	8
1.1. Istota walki sieciocentrycznej	9
1.2. Podstawowe założenia walki sieciocentrycznej	28
1.3. Właściwości implementacji założeń walki sieciocentrycznej	34
1.4. Wnioski	41
Rozdział 2. ARCHITEKTURA SIECIOCENTRYCZNEGO POLA WALKI ORAZ SPOSÓB JEGO FUNKCJONOWANIA	45
2.1. Architektura sieciocentrycznego pola walki	45
2.2. Sposób funkcjonowania sieciocentrycznego pola walki	71
2.3. Wnioski	83
Rozdział 3. WYMAGANIA WOBEC SIŁ POWIETRZNYCH W ASPEKCIE ICH UŻYCIA NA SIECIOCENTRYCZNYM POLA WALKI	87
3.1. Wymagania dla sił powietrznych w aspekcie domeny informacyjnej walki sieciocentrycznej	88
3.2. Wymagania dla sił powietrznych w aspekcie domeny społeczno-poznawczej walki sieciocentrycznej	96
3.3. Wymagania dla sił powietrznych w aspekcie domeny fizycznej walki sieciocentrycznej	103
3.4. Wnioski	109
ZAKOŃCZENIE	114
BIBLIOGRAFIA	116

WSTĘP

Zmiany polityczno-militarne zachodzące we współczesnym świecie spowodowały znaczące przewartościowania w podejściu do problemów bezpieczeństwa międzynarodowego i narodowego. Zanikł podział na dwa przeciwległe obozy polityczno-militarne, czego symbolicznym wyrażeniem był upadek muru berlińskiego, natomiast w sferze bezpieczeństwa pojawiły się nowe zagrożenia, do których obecnie zalicza się, jako jeden z najgroźniejszych, międzynarodowy terroryzm. Jednocześnie jesteśmy świadkami gwałtownego rozwoju nowych technologii, szczególnie w sferze zbioru, analizy i wykorzystywania informacji. Spowodowało to powstanie nowego podejścia do tworzenia i wykorzystania sił zbrojnych zarówno w celu zapobiegania konfliktom poprzez zarządzanie kryzysami, jak i do działań stricte militarnych.

W latach 90. XX w. w Stanach Zjednoczonych rozpoczęto prace nad nową koncepcją prowadzenia działań militarnych. Nazwano ją „Network Centric Warfare”, co w najczęściej stosowanym tłumaczeniu oznacza „walkę sieciocentryczną”. Do tej pory skutkowało to podjęciem badań w wielu krajach oraz powstaniem wielu opracowań teoretycznych. To nowe podejście do zastosowania sił militarnych wyszło poza ramy teoretyczne, bowiem założenia i niektóre rozwiązania walki sieciocentrycznej zastosowano w operacji „Enduring Freedom” przeciwko Talibom w Afganistanie w 2001 r. oraz w operacji „Iraqi Freedom” przeciwko reżimowi Saddama Hussejna w 2003 r.

Z analiz założeń prowadzenia walki sieciocentrycznej wynika, że w podejściu do użycia sił zbrojnych na współczesnym i perspektywicznym polu walki należy zastosować podejście systemowe, w którym poszczególne podsystemy, sensory i platformy połączone są wspólną siecią. W sieci tej dominującą rolę odgrywa informacja, która z jednej strony zapewnia tzw. „świadomość pola walki”, czyli wiedzę o zagrożeniach, ich sile, miejscu i czasie, a z drugiej wiedzę o dysponowanych siłach militarnych, ich położeniu i możliwościach. Dzięki temu zapewnione jest przeciwdziałanie zagrożeniom oraz ich likwidowanie we właściwym miejscu i czasie.

Takie założenia powodują potrzebę nie tylko zmiany podejścia do koncepcji użycia sił na polu walki, ale również nowego podejścia do rozwoju sił zbrojnych oraz tworzących je elementów, czyli rodzajów sił zbrojnych. Dostrzegając tę potrzebę w „Planie zadaniowo-finansowym działalności naukowej AON na rok 2005” zaplanowano przeprowadzenie badań oraz opracowanie tematu „Sieciocentryczne pole walki. Wymagania wobec sił powietrznych (II.6.6.1.0 – s. 14) w ramach zadania badawczego „Siły powietrzne w ramach sieciocentrycznego pola walki”.

Celem badań w ramach niniejszej pracy naukowo-badawczej, o charakterze studium teoretycznego, było ustalenie i scharakteryzowanie istoty założeń sieciocentrycznego pola walki, jego architektury oraz sposobu funkcjonowania, a także sprecyzowanie i scharakteryzowanie wynikających z nich wymagań wobec sił powietrznych. Ze zdefiniowanego w taki sposób celu badań wynikały następujące problemy badawcze:

1. W czym wyraża się istota założeń teoretycznych walki sieciocentrycznej?
2. Jaka jest architektura oraz sposób funkcjonowania sieciocentrycznego pola walki?
3. Jakie są wymagania wobec sił powietrznych w aspekcie ich funkcjonowania w ramach sieciocentrycznego pola walki?

Na podstawie przeprowadzonych przez zespół autorski badań wstępnych hipotetycznie założono, że:

1. Walka sieciocentryczna jest koncepcją prowadzenia operacji militarnych w wymiarze strategicznym, operacyjnym i taktycznym, opartą na przewadze informacyjnej, gdzie wzrost i użycie siły bojowej jest realizowane poprzez połączenie w obrębie wspólnej sieci sensorów, decydentów i systemów walki. Dzięki temu zapewnia się świadomość sytuacyjną oraz zwiększenie tempa i efektywności oddziaływania.
2. Sieciocentryczne pole walki jest przestrzenią, w której prowadzona jest walka sieciocentryczna. Architektura pola walki tworzona jest przez trzy płaszczyzny (domeny), czyli przez domenę fizyczną, informacyjną i społeczno-poznawczą. Domena fizyczna to przestrzeń trójwymiarowa, gdzie toczy się walka zbrojna i wykorzystywane jest spektrum elektromagnetycz-

ne. Domena informacyjna jest płaszczyzną, w której tworzy się, analizuje i przechowuje informację. Domena poznawcza obejmuje wiele niemierzalnych elementów, takich jak przywództwo, morale, jakość wyszkolenia i świadomość sytuacji. Sieciocentryczne pole walki funkcjonuje poprzez wykorzystanie sensorów, decydentów, platform bojowych, spiętych siecią informacyjną, co zapewnia, dzięki świadomości pola walki, użycie niezbędnych sił, tam gdzie jest to potrzebne i wtedy, kiedy jest to potrzebne.

3. Siły powietrzne powinny spełniać szereg wymagań, aby uzyskać zdolność do działań na sieciocentrycznym polu walki. Wymagania te będą dotyczyły zdolności do tworzenia oraz do łączenia w sieć wszystkich elementów składowych celem gromadzenia, analizy i wymiany informacji, wykorzystania tej informacji do tworzenia świadomości pola walki i podejmowania optymalnych decyzji oraz osiągania zdolności do realizacji zadań przez siły i środki sił powietrznych. Niezbędne będzie spełnienie tych wymagań w trzech domenach – informacyjnej, społeczno-poznawczej i fizycznej sił powietrznych.

W celu rozwiązania problemów badawczych oraz sprawdzenia hipotez badawczych sformułowano następujące zadania badawcze:

1. Zbadać założenia teoretyczne walki sieciocentrycznej w celu ustalenia jej istoty.
2. Na podstawie analizy i oceny założeń sieciocentrycznego pola walki ustalić jego architekturę oraz sposób jego funkcjonowania.
3. Sformułować wymagania wobec sił powietrznych w aspekcie ich funkcjonowania w ramach sieciocentrycznego pola walki.

Badania prowadzono głównie metodami teoretycznymi, czyli metodą analizy, syntezy, porównania, uogólnienia i abstrahowania. Metodami tymi badano założenia teoretyczne oraz doświadczenia praktyczne dotyczące walki sieciocentrycznej i sieciocentrycznego pola walki. Analizie i ocenie poddano bardzo szerokie spektrum literatury przedmiotu angielsko i polskojęzycznej. Do najważniejszych pozycji literatury należały, w zakresie identyfikacji istoty walki sieciocentrycznej, opracowanie Dawida Albertsa, Johna Garstki i Fredericka Steina „Network Centric Warfare: Developing and Leveraging Information Superiority” oraz

oficjalny dokument koncepcyjny „Net-Centric Environment. Joint Functional Concept” Departamentu Obrony USA.

Najcenniejszymi materiałami źródłowymi w zakresie analizy i oceny założeń architektury i funkcjonowania sieciocentrycznego pola walki były: koncepcja Biura Transformacji Sił Zbrojnych Departamentu Obrony USA: „Network Centric Operations. Conceptual Framework Version 2.0” z czerwca 2004 r. oraz „The Implementation of Network-Centric Warfare” ze stycznia 2005 r. Pomocnym materiałem było także opracowanie Korporacji RAND dla Szwedzkiej Agencji Badań Obronnych „Network-Based Operations for The Swedish Defence Force: An Assessment Methodology” z czerwca 2004 r., które dostarczyło cennych rozwiązań metodologicznych niezbędnych do sformowania wymagań wobec sił powietrznych w aspekcie ich funkcjonowania w ramach sieciocentrycznego pola walki.

W prowadzonych badaniach pomocne okazały się analizy narodowych planów USA, Wielkiej Brytanii i Australii w zakresie implementacji rozwiązań sieciocentrycznych, w tym przede wszystkim australijskiego planu „NWC Roadmap” z 2005 r. oraz brytyjskiego dokumentu „Network-Enabled Capability: An Introduction Version 1.0” z kwietnia 2004 r.

Do najważniejszych, wykorzystanych w opracowaniu niniejszego studium polskich pozycji związanych z problematyką walki sieciocentrycznej należały artykuły opublikowane w periodykach *Myśl Wojskowa* i *Przegląd Wojsk Lotniczych i Obrony Powietrznej*: „Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości” gen. Lecha Konopki oraz „Wojna w Iraku a koncepcja wojny sieciocentrycznej” Ryszarda Szpakowicza.

Rezultaty badań teoretycznych konfrontowano poprzez wywiady z oficerami sił powietrznych. Znacząca z tego punktu widzenia była też wizyta delegacji amerykańskiej, z Johnem Garstką na czele, w Akademii Obrony Narodowej, podczas której przedstawiono amerykańskie założenia walki sieciocentrycznej oraz strukturę i sposób funkcjonowania sieciocentrycznego pola walki.

Opracowana przez zespół autorski studium teoretyczne składa się ze wstępu, trzech rozdziałów merytorycznych, zakończenia i wykazu bibliografii.

We wstępie przedstawiono uzasadnienie potrzeby opracowania tematu oraz wszystkie założenia metodologiczne: cel badań i problemy badawcze, hipotezy robocze, zadania badawcze oraz scharakteryzowano zastosowaną procedurę badawczą.

Rozdział pierwszy zawiera ustalenia dotyczące istoty założeń teoretycznych walki sieciocentrycznej. Stanowi on bazę merytoryczną do przeprowadzenia badań oraz opracowania architektury i sposobu funkcjonowania sieciocentrycznego pola walki. Treści te są zawarte w rozdziale drugim. Na tej podstawie sformułowano wymagania wobec sił powietrznych w aspekcie ich użycia na sieciocentrycznym polu walki, co stanowi treść rozdziału trzeciego.

W zakończeniu dokonano podsumowania badań w ramach tematu badawczego oraz wskazano kierunki dalszych działań w tym zakresie.

Rozdział 1

WALKA SIECIOCENTRYCZNA. ISTOTA I PODSTAWOWE ZAŁOŻENIA

W latach 90. ubiegłego stulecia, w Stanach Zjednoczonych rozpoczęto prace nad nową koncepcją prowadzenia walki określaną jako „Network Centric Warfare”. W polskich publikacjach fachowych używane są określenia: „wojna sieciowa”¹, „walka sieciowa”², bądź też „walka sieciocentryczna”³. Najczęściej spotykanym w polskiej literaturze przedmiotu określeniem jest „walka sieciocentryczna”, dlatego to właśnie pojęcie będzie używane w dalszej części pracy dla określenia oryginalnej nazwy koncepcji „Network Centric Warfare”.

Pierwszy raz termin „walka sieciocentryczna” został zaprezentowany szerzej publiczności w roku 1998 w opublikowanym na łamach periodyku „Proceedings” artykule „Network Centric Warfare – Its Origins and Future”⁴. Artykuł ten przedstawił nowy sposób prowadzenia działań militarnych w erze społeczeństw informacyjnych. Od momentu ukazania się wspomnianej publikacji pojawiło się mnóstwo artykułów, opracowań, a nawet książek dotyczących walki sieciocentrycznej. Począwszy od pierwszych lat naszego wieku taki sposób prowadzenia działań militarnych wyszedł poza ramy teoretyczne, co udowodniły między innymi operacja przeciwko ugrupowaniom terrorystycznym i wspierającemu ich rządowi Talibów w Afganistanie pod kryptonimem „Enduring Freedom”, oraz operacja sił koalicyjnych wymierzona przeciwko reżimowi Saddama Husseina, przeprowadzona w Iraku pod kryptonimem „Iraqi Freedom”. Główny filar obu operacji – Siły Zbrojne Stanów Zjednoczonych, mają być w dalszej perspektywie czasowej w pełni dostosowane do prowadzenia działań metodą walki sieciocentrycznej (program Joint Vision 2020). Sojusz Północnoatlantycki oraz wiele państw również

¹ R. Szpakowicz, *Wojna w Iraku a koncepcja wojny sieciocentrycznej*, Przegląd Wojsk Lotniczych i Obrony Powietrznej nr 11/2003, s. 10.

² Tamże, s. 10.

³ L. Konopka, *Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości*, Myśl Wojska nr 2/2004, s. 74.

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

daży do umożliwienia swoim siłom zbrojnym prowadzenia działań sieciocentrycznych, rozwija teorię walki sieciocentrycznej, prowadząc szeroko zakrojone badania empiryczne oraz zwiększając nasycenie wojsk technologiami informacyjnymi.

Równoległość wysiłków badawczych w zakresie tworzenia teorii walki sieciocentrycznej oraz tempo rozwoju technologii informacyjnych powodują, iż pomimo zbieżności ogólnych założeń narodowych koncepcji sieciocentrycznych występują one również w rozważaniach strukturalnych i funkcjonalnych oraz w zakresie ich przewidywanej implementacji.

Stąd też w rozdziale dokonano analizy szerokiego spektrum teorii narodowych w celu rozwiązania problemu badawczego, w czym wyraża się istota i podstawowe założenia walki sieciocentrycznej.

1.1. Istota walki sieciocentrycznej

Początki teorii walki sieciocentrycznej związane są z przełomem w stosowaniu technologii informatycznych przez firmy prywatne oraz organizacje działające na wolnym rynku ekonomicznym. Obserwacja, w jaki sposób epoka informacyjna zmieniła warunki działania firm, jak zmieniły się ich możliwości funkcjonowania na rynku oraz jakie formy przybierała konkurencja ekonomiczna, dały impuls dla badań wojskowych zastosowań technologii informacyjnych.

Część specjalistów doszukuje się początków walki sieciocentrycznej we wcześniejszym okresie, jeszcze w czasie II wojny światowej. Ważnym momentem tworzenia warunków dla prowadzenia walki sieciocentrycznej stało się wprowadzenie systemów uzbrojenia, wykorzystujących organiczne środki do prowadzenia technicznej obserwacji pola walki (np. przestrzeni powietrznej, powierzchni morza i przestrzeni podwodnej), a w konsekwencji pozyskiwania informacji bez konieczności fizycznej bliskości z obserwowanym obiektem.

Aby podkreślić wagę powstania takich systemów, można posłużyć się przykładem radiolokatora pokładowego samolotów, jaki został opracowany i zastosowany bojowo w okresie II wojny światowej⁵. Na początku wojny lotnictwo myśliwskie dysponowało bardzo małymi możliwościami zwalczania przeciwnika

⁵ H. Mordawski, *Z dziejów radiolokacji*, cz. II, Wiraże nr 18/2004, s. 17.

w nocy oraz w dzień, przy dużym zachmurzeniu. Wykrycie samolotu przeciwnika za pomocą tylko i wyłącznie wzroku pilota bądź strzelca pokładowego było w warunkach ograniczonej widzialności niezmiernie trudne i istotnie zmniejszało stosunkowo duże możliwości taktyczno-techniczne ówczesnych samolotów myśliwskich. Skonstruowanie naziemnych stacji radiolokacyjnych stanowiło duży postęp w dziedzinie wykrywania samolotów w przestrzeni powietrznej, ale nie rozwiązywało tego problemu ze względu na liczne ograniczenia radiolokatorów naziemnych (np. mała dokładność wskazań, ograniczony zasięg i sektor wykrywania). Dlatego koniecznym stało się skonstruowanie urządzenia na tyle małego, by można było umieścić je w samolocie, lecz na tyle dokładnego, by wskazać załodze przestrzenne położenie samolotu przeciwnika i umożliwić użycie uzbrojenia pokładowego w celu jego zniszczenia. Był to system dość prymitywny, gdyż uzbrojeniem kierowano ręcznie, jednakże znacznie zwiększył możliwości zwalczania samolotów przeciwnika w warunkach ograniczonej widzialności. W czasie II wojny światowej opracowano także system uzbrojenia, który automatycznie kierował swoim integralnym środkiem ogniowym, a mianowicie armatę przeciwlotniczą kierowaną radiolokacyjnie.

Późniejszymi przykładami systemów uzbrojenia, w których organiczne środki były wykorzystywane do prowadzenia technicznej obserwacji pola walki, i które przetwarzały uzyskaną informację w czasie zbliżonym do rzeczywistego oraz kierowały ogniem danego typu środka uderzeniowego były na przykład: przeciwlotniczy zestaw rakietowy, pokładowy system obserwacyjno – celowniczy samolotu bojowego, bądź system kierowania ogniem czołgu lub bojowego wozu piechoty. Jednakże informacja zdobywana przez integralne techniczne środki obserwacji pola walki tychże systemów była wykorzystywana głównie dla potrzeb owych systemów uzbrojenia. Gromadzenie zdobytych informacji, ich obróbka, formułowanie wniosków i dystrybucja do innych użytkowników były w takim układzie prowadzone w sposób mniej lub bardziej tradycyjny (np. za pomocą meldunków radiowych bądź pisemnych), a cały proces był długotrwały. Wyjątek stanowiły środki obrony powietrznej, gdzie duża dynamika działań i szybkie zmiany sytuacji taktycznej wymusiły większy stopień integracji środków rozpoznania ze środkami walki. W tym celu zastosowano zautomatyzowane systemy dowodzenia, które co prawda usprawniły proces przekazywania i obróbki informacji, ale utworzone dzie-

ki nim sieci dystrybucji danych ograniczały się co do szczebla dowodzenia i rodzaju wojsk.

W drugiej połowie dwudziestego wieku podjęto próby ściślejszego powiązania środków rozpoznania ze środkami ogniowymi i przekazaniem informacji w czasie zbliżonym do rzeczywistego, tworząc tak zwane systemy rozpoznawczo-uderzeniowe. Były to jednakże zamknięte sieci, w których informacja dystrybuowana była tylko w obrębie danego systemu. Model sił zbrojnych oparty na takiej koncepcji jest obecnie nazywany „platform centric warfare”, czyli zamkniętych systemów rozpoznawczo-bojowych⁶.

Przeprowadzone analizy literatury przedmiotu⁷ wskazują, że w podejściu platformo – centrycznym każda załoga platformy bojowej (jaką jest na przykład samolot uderzeniowy) musi poszukiwać celu samodzielnie (lub przy ogólnym wskazaniu z zewnątrz), dokonując jego identyfikacji, a następnie wykonać atak wskazując cel systemowi kierowania ogniem. Przy takim sposobie działania efektywność wykorzystania uzbrojenia jest mocno ograniczona. Zasięg pokładowych sensorów ogranicza czas potrzebny na poszukiwanie, identyfikację, celowanie i użycie uzbrojenia. Powoduje to opóźnienia w otwarciu ognia i nie pozwala na pełne wykorzystanie możliwości uzbrojenia. Sytuacja taka ma miejsce szczególnie wtedy, gdy zasięg wykrywania sensorów pokładowych jest mniejszy niż zasięg uzbrojenia danej platformy bojowej.

Ponadto, sensory promieniujące energię, jak np. pokładowa stacja radiolokacyjna samolotu emitująca energię elektromagnetyczną zdradzają położenie platformy, często uniemożliwiając skryty atak i uzyskanie efektu zaskoczenia. Załoga takiej platformy bojowej musi również polegać na innym zestawie pokładowych sensorów, ostrzegających przed atakiem przeciwnika (np. czujniki informujące załogę samolotu o opromieniowaniu energią elektromagnetyczną emitowaną przez stację naprowadzania rakiet przeciwlotniczego zestawu rakietowego). Ostrzeżenie o takim ataku często jest środkiem niewystarczającym, gdyż przychodzi zbyt późno – platforma jest już wykryta i atakowana przez środki ogniowe

⁶ L. Konopka, *Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości*, op. cit., s. 65.

⁷ R. Szpakowicz, *Wojna w Iraku a koncepcja wojny sieciocentrycznej*, op. cit.; L. Konopka, *Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości*, op. cit.

przeciwnika. Jest to niebezpieczne dla platformy bojowej nie tylko w sensie fizycznym, ale utrudnia też załodze skoncentrowanie się na wykonaniu zadania, oddziałując na nią negatywnie w sensie psychologicznym.

Dysponowanie siecią wymiany informacji w czasie rzeczywistym umożliwia oddzielenie sensorów od platform bojowych. Pozwala bowiem na stworzenie ciągłego pola informacyjnego - jednolitego obrazu sytuacji taktycznej, który może być wykorzystywany przez każdą platformę bojową dysponującą odpowiednim urządzeniem odbiorczym i będącą w zasięgu nadajników emitujących ów jednolity obraz sytuacji taktycznej. Aby zilustrować istotę obrazu informacji taktycznej, można posłużyć się przykładem RAP (Recognized Air Picture), czyli jednolitym obrazem sytuacji powietrznej. Podczas gdy RAP ukazuje sytuację powietrzną opierając się na informacjach zdobytych przez wiele środków rozpoznawczych (Common Operational Picture – COP), jednolity obraz sytuacji taktycznej będzie ukazywał kompletną sytuację taktyczną na lądzie, w powietrzu, na powierzchni wody i w jej głębinach. Podobnie jak w przypadku jednolitego obrazu sytuacji powietrznej, do utworzenia owego obrazu wykorzystywane będą informacje zdobyte przez całe spektrum środków rozpoznawczych.

Posiadając dostęp do takiego jednolitego obrazu sytuacji taktycznej, platformy bojowe mogą skrycie użyć uzbrojenia na maksymalnej odległości od celu, ograniczonej tylko zasięgiem środka ogniowego. Ponadto, rezygnacja z sensorów pokładowych pozwala, w przypadku sił powietrznych, na zwiększenie udźwigu, a co za tym idzie, rozszerzenie możliwości uderzeniowych platform bojowych. Pełne ostrzeżenie o aktywności przeciwnika pozwala również na odpowiednio wczesną reakcję na zagrożenie, dając załogom platform komfort psychiczny pozwalający na skoncentrowanie się na postawionym zadaniu i skuteczniejsze jego wykonanie.

Przejęcie na sieciocentryczny sposób prowadzenia działań pozwala nie tylko na oddzielenie sensorów od platform uzbrojenia, ale również na oddzielenie operatorów od sensorów i platform. Obecność operatora na platformie przenoszącej sensory i uzbrojenie była dotychczas konieczna, było to bowiem jedyne miejsce, gdzie potrzebne do działania informacje dostępne były w odpowiednim czasie. Ewolucja koncepcji prowadzenia walki w kierunku działań sieciocentrycznych sprawiła, że taka konieczność zanikła. Stanowiska operatorów mogą być uloko-

wane w miejscu zapewniającym im bezpieczeństwo, z którego mogą obsługiwać platformy bojowe za pomocą zdalnego sterowania. Usunięcie załóg z platform przenoszących sensory i uzbrojenie umożliwia znaczną redukcję rozmiarów owych platform, czyniąc je trudniejszymi do wykrycia i zwalczania. W przypadku platform latających jest to o tyle istotne, że nieobecność załogi znosi dotychczasowe bariery związane z dopuszczalnymi dla organizmu ludzkiego przeciążeniami, które znacznie ograniczały manewrowość statków powietrznych.

Słuszność kierunku, w jakim dokonuje się przedstawiona powyżej ewolucja sposobu prowadzenia walki, została udowodniona podczas działań koalicji państw zachodnich przeciwko dyktaturze Saddama Husseina w Iraku w roku 2003, mimo, że siły prowadzące operację „Iraqi Freedom” nie osiągnęły jeszcze standardu technicznego, który wymagany jest do prowadzenia walki sieciocentrycznej w pełnym zakresie.

Walka sieciocentryczna została po raz pierwszy zdefiniowana przez Davida Albertsa, Johna Garstkę, i Frederica Steina, którzy są jednymi z twórców tej koncepcji. Zgodnie z zaproponowaną przez nich definicją: „(...) *Walka sieciocentryczna 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 samosynchronizowanie 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*”⁸.

⁸ D. Alberts, J. Garstka, F. Stein, *Network Centric Warfare*, DoD C4ISR Cooperative Research Program, 2000, s. 88.

W koncepcji Alberta, Garstki i Steina podkreślana jest jakość, jaką stanowi nowa sytuacja w odniesieniu do środowiska, w jakim będzie prowadzona walka epoki informacyjnej. Rosnące znaczenie operacji innych niż wojna, postęp technologiczny oraz asymetryczne formy działań zbrojnych doprowadziły, zdaniem autorów, do konieczności odchodzenia od identyfikowania „pola walki” na rzecz postrzegania środowiska prowadzenia walki sieciocentrycznej jako „przestrzeni realizacji zadań” (Mission Space). W przestrzeni tej nie będzie wyraźnej granicy oddzielającej walczących od ludności cywilnej, zmienić się może charakter przeciwnika oraz zniknąć oddalenie od konfliktu. Analogicznie do informacji, walka sieciocentryczna będzie wszechogarniająca, wieloaspektowa i wszechobecna. Na sieciocentrycznym polu walki siły zbrojne nie będą jedynym aktorem posiadającym informacje i zdolnym ją wykorzystać, lecz raczej jednym z wielu uczestników walki. W takim ujęciu walka sieciocentryczna jawi się jako element szerzej definiowanej walki informacyjnej lub konkurencji wielu podmiotów realizowanej z wykorzystaniem technologii i instrumentów informacyjnych.

W bardziej wąski sposób definiuje walkę sieciocentryczną Ryszard Szpakowicz. 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”⁹.

Wiele definicji walki sieciocentrycznej znaleźć można na oficjalnych stronach internetowych różnych instytucji i organizacji amerykańskich, brytyjskich, norweskich, czy australijskich. Traktują one z reguły walkę sieciocentryczną jako nowy sposób prowadzenia walki zbrojnej, lub też nowatorską koncepcję jej prowadzenia.

⁹ R. Szpakowicz, *Wojna w Iraku a koncepcja wojny sieciocentrycznej*, op. cit., s. 8.

Spośród wielu zbliżonych do siebie definicji, warto przytoczyć zamieszczoną na stronie amerykańskiego „Defence Technical Information Center” jedną z bardziej oryginalnych, która opisuje „Network Centric Warfare”, jako pochodną „network – centric computing”¹⁰. Słowo „computing”, podobnie jak np. „targeting”, nie doczekało się jednowyrazowego polskiego odpowiednika, tłumaczone jest jako „informatyka, przetwarzanie danych”¹¹. Według cytowanego źródła, prowadzenie walki przeszło podobną ewolucję jak informatyka, która zmieniała się od systemów platformocentrycznych do sieciocentrycznych. Umożliwiły to odkrycia w dziedzinie technologii informatycznej i oprogramowania, np. takie jak protokół przekazu różnorodnego tekstu (Hypertext Transfer Protocol – HTTP), język czytania różnorodnego tekstu (Hypertext Markup Language – HTML), czy też przeglądarki internetowe. To oprogramowanie, które umożliwiło współdziałanie komputerów posiadających różne systemy operacyjne oraz zapewniło możliwość szybkiego wyszukiwania i pozyskiwania informacji w sieci, spowodowało przełom w komercyjnych sektorach gospodarki. Firmy, które posiadają tak zwaną przewagę informacyjną, osiągają sukcesy w konkutowaniu z przedsiębiorstwami, które nie mogą uzyskać danych potrzebnych do skutecznego działania. Analogicznie, w walce sieciocentrycznej przewaga informacyjna ma zapewnić uzyskanie powodzenia w działaniach zbrojnych.

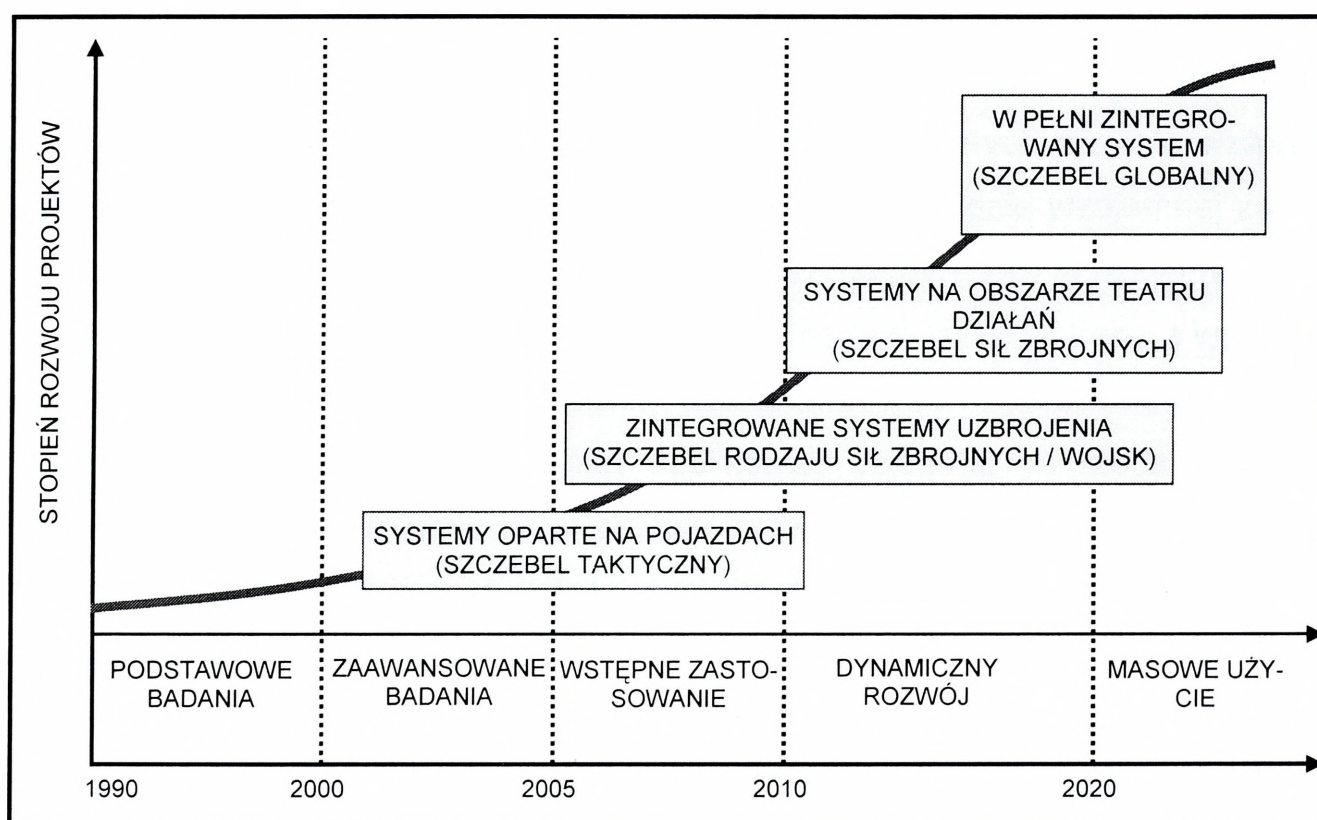
Według założeń amerykańskich walka sieciocentryczna będzie takim sposobem prowadzenia działań, w którym siły zbrojne, spięte w sieć informatyczną, będą wykorzystywać przewagę informacyjną i pełną świadomość sytuacji (strategicznej, operacyjnej i taktycznej) do prowadzenia szybkich i skutecznych działań, pozwalających na pokonanie przeciwnika przy możliwie najbardziej efektywnym i ekonomicznym wykorzystaniu sił własnych.

W literaturze przedmiotu uwidacznia się coraz wyraźniej polaryzacja poglądów na temat stopnia sieciocentryczności możliwego do osiągnięcia w użyciu sił wojskowych na polu walki. Obecny stopień rozwoju założeń koncepcyjnych walki sieciocentrycznej, wyposażenia oraz wyszkolenia wojsk, w opinii Johna Colemana, plasuje współczesne siły zbrojne na poziomie nie pozwalającym na prowadzenie działań sieciocentrycznych. Doświadczenia operacji

¹⁰ www.dtic.mil/jsc/j6/education/warfare.html

¹¹ YDP – *Collins English Polish Dictionary*.

w Afganistanie i Iraku wskazują, że w pełnym zakresie działania sieciocentryczne były możliwe w wymiarze taktycznym. Coleman twierdzi, że w perspektywie najbliższych kilku 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 (rys. 1.1). Należy podkreślić, że prognozy Colemana opierają się głównie na ocenie aspektów technologicznych i odzwierciedlają jedną z możliwych perspektyw postrzegania walki sieciocentrycznej.



Źródło: opracowanie własne na podstawie: www.directionsmag.com/images/articles/coleman/ncw/ncw3.gif

Rys. 1.1. Rozwój koncepcji walki sieciocentrycznej

Rozwój teorii walki sieciocentrycznej nie ogranicza się do środowisk wojskowych. Również przedsięwzięcia badawcze i projekty firm oraz konsorcjów przemysłowych rozwijających technologie komercyjne o zastosowaniach wojskowych ukierunkowane są na stworzenie oprogramowania oraz sprzętu przeznaczonego do walki sieciocentrycznej. Przykładem jest chociażby porozumienie w zakresie rozwijania koncepcji działań sieciocentrycznych, które podpisane zostało w listopadzie 2004 r. przez 27 firm z Europy i Stanów Zjednoczonych, o profilu lotniczym i technologii informacyjnych. Porozumienie to stanowi akt powołania specjalnego konsorcjum przemysłowego pod nazwą: Network Centric Operations In-

dustry Consortium – NCOIC. Liderem inicjatywy powołania owego konsorcjum była amerykańska firma Boeing, a jej działania poparł kolejny potentat na rynku zbrojeniowym – Lockheed Martin¹². Działania przedsiębiorstw informatycznych i zbrojeniowych są reakcją na założenia teoretyczne walki sieciocentrycznej, które zostały opracowane w wielu krajach. Państwem, które jest najbardziej zaawansowane, zarówno w założeniach teoretycznych jak i w działaniach praktycznych, w drodze do osiągnięcia standardu umożliwiającego prowadzenie walki sieciocentrycznej są Stany Zjednoczone.

W oficjalnym dokumencie Departamentu Obrony USA „Net-Centric Environment. Joint Functional Concept Vision 1.0” z kwietnia 2005 r. za kryterium odróżniające działania platformocentryczne od sieciocentrycznych przyjęto wzajemną zależność (Interdependence). Działania oparte na zasadzie wzajemnej zależności prowadzących ją sił cechują się tym, że poszczególne zaangażowane w nie siły (elementy, zgrupowania, zespoły zadaniowe, komórki sztabu) będą z wysokim stopniem zaufania wykorzystywać efekty działania innych i realizować określone funkcje na rzecz całości sił, zamiast duplikować działania na rzecz innych¹³. Obecnie wzajemna zależność sił występuje zazwyczaj na poziomie komponentu sił połączonych lub dowództwa połączonych sił zadaniowych. Stopień wzajemnej zależności zawiera się w przedziale poziomu integracji działania pomiędzy autonomią poszczególnych komponentów a dekonfliktowaniem ich użycia. W ocenie Departamentu Obrony USA tak niski poziom integracji sił wykorzystywanych na współczesnym polu walki prowadzi do sytuacji, w której zdolności operacyjne poszczególnych uczestników walki są niemal całkowicie odrębnie użyte, nawet w sytuacji realizacji wspólnych zadań. Powoduje to niewykorzystanie pełnego potencjału przez siły połączone pomimo fizycznego ich posiadania przez poszczególne komponenty sił połączonych i jednostki wchodzące w ich skład.

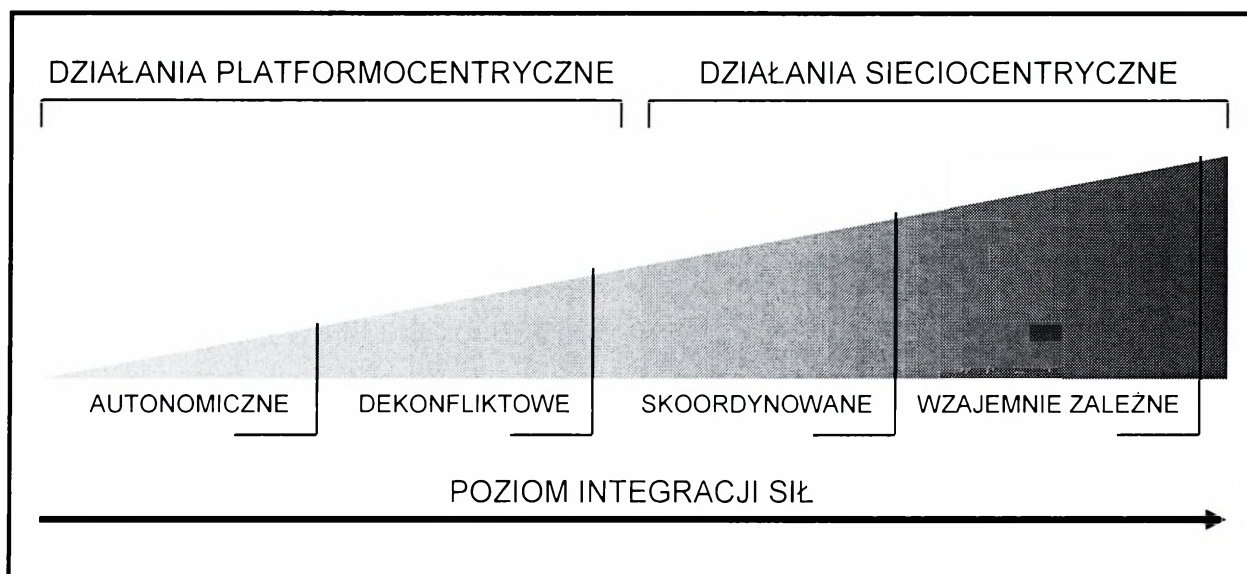
Usunięcie przeszkód w przepływie informacji oraz połączenie horyzontalne, rozproszonych geograficznie elementów składowych sił połączonych zapewni pełniejsze wykorzystanie potencjału poszczególnych uczestników walki w zakresie realizacji określonych funkcji na rzecz całości sił. W konsekwencji autonomiczność

¹² *Firmowe porozumienie na NCW*, Lotnictwo Wojskowe nr 11/2004, s. 4.

¹³ *Net-Centric Environment. Joint Functional Concept Vision 1.0*, Department of Defense, 2005, s. 18.

poszczególnych szczebli dowodzenia w zakresie realizacji niektórych funkcji operacyjnych będzie mogła ulec zmniejszeniu, gdyż możliwe będzie wykorzystanie zdolności innych uczestników walki do ich zabezpieczenia.

Zwiększenie zakresu integracji przekładać się będzie na wzrost skuteczności użycia sił. Wzajemna zależność sił na poziomie autonomiczności i dekonfliktowania będzie charakteryzować działania platformocentryczne (rys. 1.2). Natomiast wzajemna zależność na poziomie skoordynowania i pełnej zależności pozwalać będzie na określenie takich działań jako sieciocentrycznych.



Źródło: opracowanie własne na podstawie: *Net-Centric Environment. Joint Functional Concept Vision 1.0*, op. cit., s. 19

Rys. 1.2. Zależność charakteru działań od poziomu integracji sił

Taki stopień integracji sił pozwolić ma na wykorzystanie potencjalnych zdolności sił składowych, które nie mogłyby mieć miejsca bez sieciocentrycznej integracji sił połączonych w pełnym zakresie. W dokumencie „Net-Centric Environment Joint Functional Concept Vision 1.0” powyższy poziom integracji jest określony jako konstruktywna wzajemna zależność (Constructive Interdependence) i utożsamiany z pełną zdolnością do prowadzenia działań sieciocentrycznych¹⁴. Działania sieciocentryczne określane terminem „Network Centric Warfare” definiowane są obecnie w doktrynie amerykańskiej jako „zdolność geograficznie rozproszonych sił do osiągnięcia wysokiego poziomu świadomości przestrzeni walki, który może być wykorzystany do realizacji zamiaru działania dowódcy. Prowadzenie walki sieciocentrycznej zwiększa szybkość działania i umożliwia skorzy-

¹⁴ Tamże, s. 17-18.

stanie z osiągniętej przewagi informacyjnej”. Koncepcja walki sieciocentrycznej wspierana jest przez Sekretarza Obrony Stanów Zjednoczonych, Donalda Rumsfelda oraz przez samego prezydenta, George’a W. Busha, który stwierdził, że „(...) *Stany Zjednoczone muszą budować swoje Siły Zbrojne w oparciu o rewolucyjne postępy w dziedzinie technologii wojennych, takie, które polegają w większym stopniu na technologii stealth, broniach precyzyjnych i technologiach informacyjnych*”¹⁵. Słowa George’a W. Busha znajdują odzwierciedlenie w programach rozwoju sił zbrojnych i nowych koncepcjach operacyjnych zawartych w dokumentach Joint Vision 2010 i Joint Vision 2020.

Zakres wysiłków koncepcyjnych ukierunkowanych na rozwój teorii walki sieciocentrycznej oraz wypracowanie niezbędnych do jej prowadzenia rozwiązań funkcjonalnych i strukturalnych jest zróżnicowany w różnych państwach. Relatywnie najbardziej zaawansowane w porównaniu z innymi państwami (oprócz USA) prace nad rozwojem teorii walki sieciocentrycznej są prowadzone przez Wielką Brytanię. W Wielkiej Brytanii dostrzega się konieczność opracowania założeń teoretycznych i działań praktycznych w kierunku osiągnięcia zdolności do działań sieciocentrycznych, które określa się terminem „Networked Enabled Capability – NEC”¹⁶. Już sam termin „Network Enabled Capability”, w dosłownym tłumaczeniu „zdolności umożliwiane (zapewniane) przez sieć (połączenie w sieci)”, wskazuje na odmienne do amerykańskiego podejścia do działań sieciocentrycznych¹⁷.

Celem wykorzystania możliwości zapewnianych przez działanie w sieci jest poprawa zdolności sił brytyjskich do prowadzenia walki i odnoszenia zwycięstwa poprzez umożliwienie wymiany i wykorzystania informacji sprawniej i skuteczniej, także z siłami koalicjantów, jeśli będzie to potrzebne.

W założeniach teoretycznych opracowanych w Wielkiej Brytanii największy nacisk kładzie się na zdolność do zbierania, syntezy i rozprowadzania dokładnej, terminowej i wiarygodnej informacji, by zapewnić pełne zrozumienie sytuacji wśród dowódców na wszystkich szczeblach. Brytyjska teoria walki sieciocentrycznej nie zakłada całkowitej transformacji sił zbrojnych, ale raczej skupia się na kluczowych

¹⁵ K. Coleman, *Network Centric Warfare*, dostępne z: www.directionsmag.com

¹⁶ A. Borgu, *The Challenges and Limitations of „Network Centric Warfare” – the initial views of an NCW sceptic*, Australian Strategic Policy Institute, 2003, s. 4.

¹⁷ *Networked Enabled Capability. An Introduction*, UK MOD, 2004, s. 10.

elementach umożliwiających osiągnięcie większej efektywności działania. Punktem wyjściowym w koncepcji brytyjskiej jest nie tylko sama sieć, lecz także systemy uzbrojenia, stanowiska dowodzenia i sensory. Sieć ma służyć jedynie do połączenia powyższych elementów w sposób zapewniający dużą sprawność działania, rozstrzygającą skuteczność użycia sił wojskowych oraz większą prędkość i precyzję działania¹⁸.

Podobnie jak w koncepcjach amerykańskich, brytyjska teoria walki sieciocentrycznej nie ogranicza jej zakresu do rozwiązań technicznych, ale podkreśla wagę przewartościowań w zachowaniach zbiorowych i indywidualnych, które umożliwiłyby skuteczniejsze niż przeciwnik działanie na polu walki. Za kluczowy warunek przejścia od działań platformocentrycznych do sieciocentrycznych uważa się wyjście poza tradycyjną wymianę informacji i łączność dla wypracowania nowych zasad i sposobów zbioru, przechowywania i udostępniania informacji prowadzącym działania wojskom.

Podobne do brytyjskiego podejście do walki sieciocentrycznej prezentuje Australia. W doktrynie rozwoju sił zbrojnych ADF Force 2020 użyty jest termin „Network Enabled Operations – NEO”¹⁹, jako odpowiednik amerykańskiego „Network Centric Warfare”. Według poglądów australijskich działania sieciocentryczne osiągają swoją skuteczność dzięki efektywnemu połączeniu (zsieciowaniu) elementów sił zbrojnych prowadzących działania. Platformy bojowe i sensory są traktowane jako węzły sieci, która służy do zbierania i udostępniania informacji. W swojej doktrynie armia australijska zwraca również uwagę na konieczność uzyskania zdolności do połączenia narodowych i koalicyjnych sensorów, systemów uzbrojenia i decydentów w spójną i efektywną całość.

Rozwój australijskiej teorii walki sieciocentrycznej ma miejsce zarówno w odniesieniu do rozwiązań technologicznych, jak również dotyczy aspektów społeczno-kulturowych. W australijskiej koncepcji platformy bojowe, urządzenia, infrastruktura i środki materiałowe postrzegane są jako sieć węzłów i połączeń, w której informacja jest „obowiązująca walutą”²⁰. Uczestnicy walki uzyskują z sieci niezbędne do prowadzenia działań informacje, które są dla nich powszechnie do-

¹⁸ Tamże, s. 37-38.

¹⁹ *NCW Roadmap, Australian Government, Department of Defence, 2005, s. 4-6.*

²⁰ Tamże.

stępne. Pozwala to na bardziej kompleksowe zrozumienie sytuacji militarnej, w konsekwencji podejmowania odpowiednich działań na polu walki. Australijskie założenia teoretyczne walki sieciocentrycznej dotyczą również społecznych i kulturowych aspektów funkcjonowania indywidualnych uczestników i grup w warunkach środowiska sieciocentrycznego. Prowadzone badania ukierunkowane są na zagadnienia działania w warunkach nadmiaru informacji, współdziałania za pośrednictwem sieci oraz relacji człowiek – maszyna. Ważnym elementem rozwijanej w Australii teorii walki sieciocentrycznej jest uzyskanie odpowiedzi: jakie są reakcje ludzi na nowe technologie, w jaki sposób modyfikują ich działania oraz jakie implikacje dla walki zbrojnej mogą być tego wynikiem.

Rozwój teorii walki sieciocentrycznej ma miejsce również w Szwecji. Jako sposób transformacji od platformocentrycznych założeń prowadzenia obrony terytorium Szwecji do obrony opartej na rozwiązaniach sieciocentrycznych przyjęto filozofię obrony sieciowej (NetDefence)²¹. Walka sieciocentryczna postrzegana jest, jako sposób wykorzystania rozwiązań komercyjnych i cywilnych opartych na technologiach internetowych i sieciowych w celu uzyskania efektów synergicznych użycia zasobów cywilnych i wojskowych w obronie narodowej. Odmienne od założeń teoretycznych rozwijanych w innych państwach, w Szwecji kładzie się duży nacisk na wykorzystanie infrastruktury cywilnej, a nie tylko na budowie odrębnej sieci wojskowej²².

Prace koncepcyjne w zakresie wypracowania założeń operacyjnych użycia wojsk na sieciocentrycznym polu walki są prowadzone w szeregu państw. W dostępnej literaturze przedmiotu wymienia się między innymi Kanadę, Nową Zelandię, a także Chiny. Brakuje jednak obecnie wiarygodnych źródeł pozwalających na szczegółową analizę przyjętych przez powyższe państwa założeń, co do istoty walki sieciocentrycznej.

Walka sieciocentryczna staje się coraz ważniejsza w doktrynie Sojuszu Północnoatlantyckiego. Jednym z celów transformacji Sojuszu jest zapewnienie siłom sojuszniczym zdolności do osiągania przewagi informacyjnej (Information

²¹ Ministry of Defence, *The New Defence – Prepared for the Next Millenium*, 1999, cytowane w: *Network-Based Operations for the Swedish Defence Forces: An Assessment Methodology*, RAND Corporation, 2002, s. XII.

²² *Sweden's revolution in military affairs*, Financial Times, 2000, dostępne z: <http://specials.ft.com/ftit/october2000/FT3Wzevdc.html>

Superiority) będącej wspólnie ze zdolnościami zapewnianymi przez stosowanie przez NATO rozwiązań sieciowych (NATO Network-Enabled Capability – NNEC) bazę dla osiągnięcia przewagi decyzyjnej (Decision Superiority). Przewaga decyzyjna postrzegana jest w założeniach doktrynalnych NATO jako stan, kiedy dowódcy mogą zrozumieć sytuację, ocenić opcje działania, podejmować decyzje oraz inicjować ich realizację szybciej i skuteczniej niż przeciwnik. Założenia koncepcyjne walki sieciocentrycznej w NATO rozwijane są w wielu obszarach, w tym: doktryny, organizacji, szkolenia, środków materiałowych, przywództwa, zarządzania zasobami osobowymi, infrastruktury i interoperacyjności (Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities and Interoperability – DOTMLPFI)²³.

W płaszczyźnie osiągnięcia przewagi informacyjnej sojusznicze założenia walki sieciocentrycznej są ukierunkowane na tworzenie warunków, gdy poziom i jakość dostępnej informacji będzie wystarczająco wysoki, aby przekładać się na znaczącą przewagę w walce.

W odniesieniu do zdolności zapewnianych przez stosowanie przez NATO rozwiązań sieciowych (NNEC) celem implementacji założeń sieciocentrycznych ma być stworzenie środowiska, w którym elementy zbioru informacji (collectors), decydenci (decision makers) oraz wywierania wpływu (effectors) zintegrowani w ramach zintegrowanej super sieci (Network of Network) będą mogli poszukiwać i otrzymywać dane oraz informacje z jakiegokolwiek źródła w formacie i czasie adekwatnym do potrzeb odbiorcy.

Teoria walki sieciocentrycznej rozwija przez NATO zakłada, iż synergiczna implementacja założeń osiągnięcia przewagi informacyjnej oraz NNEC pozwoli na przekształcenie sił sojuszu w pełni usieciowione. Dzięki temu siły sojusznicze będą mogły współposiadać informację i współdziałać w przestrzeni wirtualnej. Zapewni to podejmowanie decyzji na wszystkich szczeblach dowodzenia oraz poprawi elastyczność, precyzję i spójność prowadzonych operacji w całym obszarze działania, zwiększając poprzez to potencjał bojowy i skuteczność użycia wojsk.

²³ *Information Superiority and NATO Network – Enabled Capability. Fact Sheet*, Allied Command Transformation, 2005, dostępne z: <http://specials.ft.com/ftit/october2000/FT3Wzevdc.html>

Przedstawione powyżej założenia doktrynalne różnych państw oraz działalność przedsiębiorstw zorientowana na rozwój teorii oraz tworzenie oprogramowania i sprzętu przeznaczonego do prowadzenia walki sieciocentrycznej wskazują jednoznacznie, że koncepcja działań sieciocentrycznych jest perspektywicznym sposobem działania sił zbrojnych XXI w. Nie brak jednakże opinii sceptyków, którzy wytykają słabe punkty owej teorii i wskazują jej nieadekwatność w odniesieniu do niektórych działań prowadzonych przez siły zbrojne (jak na przykład walka z siłami terrorystycznymi).

Dla przykładu, amerykański naukowiec Thomas Barnett, w jednym ze swoich artykułów porównuje słabe strony koncepcji walki sieciocentrycznej do chrześcijańskich siedmiu grzechów głównych²⁴. Według niego główne wady koncepcji walki sieciocentrycznej (opracowanej dla Sił Zbrojnych Stanów Zjednoczonych) to:

- koncentracja na ewentualnym przeciwniku posiadającym porównywalny potencjał wojskowy, niedostosowanie do zagrożeń asymetrycznych;
- spowolnienie tempa adaptacji Sił Zbrojnych Stanów Zjednoczonych do prowadzenia operacji reagowania kryzysowego;
- preferowanie użycia zaawansowanych technologicznie, ale drogich i nielicznych platform bojowych i stanowisk dowodzenia (niezgodnie z ogólną teorią działań sieciocentrycznych, w której kładzie się nacisk na zastosowanie dużej liczby tanich platform);
- błędne założenie, że dzięki zniszczeniu systemu łączności i przesyłu informacji przeciwnika, można kontrolować jego działania oraz poziom eskalacji konfliktu;
- koncentracja na osiągnięciu jak największej prędkości w cyklu dowodzenia, a nie na tym, jak najlepiej wykorzystać nadwyżkę czasu do podejmowania trafniejszych decyzji;
- niewłaściwe zastosowanie cywilnych założeń działań sieciocentrycznych (Network Centric Marketing) na gruncie wojskowym;

²⁴ T. Barnett, *The Seven Deadly Sins of Network – Centric Warfare*, dostępne z: www.nwc.navy.mil/newrulesets/default.htm

- nadmierne poleganie na zintegrowanym obrazie przestrzeni walki, który jest „przeładowany” informacją.

Warto przywołać również argumenty krytyczne Aldo Borgu, który jest dyrektorem programowym w Australijskim Instytucie Polityki Strategicznej (Australian Strategic Policy Institute) i zwolennikiem koncepcji walki sieciocentrycznej. Niemniej jednak, dostrzega on mniej pozytywne strony tej koncepcji, którymi są²⁵:

- skłonność do postrzegania zdolności do prowadzenia walki sieciocentrycznej jako celu samego w sobie, a nie narzędzia do osiągnięcia określonego celu;
- powstanie zestawu sieci różnych systemów dowodzenia i uzbrojenia zamiast zamierzonej jednej i jednolitej sieci informacyjnej;
- dążenie do przewagi informacyjnej, które powoduje „przeładowanie” informacją, której nie można przeanalizować;
- wywołanie zjawiska zwanego „głodem informacji”, powodującego niezdolność dowódców do podejmowania decyzji na podstawie niepełnych (szczątkowych) danych;
- wrażliwość systemu zbierania i przesyłu informacji na mylące działania przeciwnika;
- koncentracja na technicznych aspektach, z pominięciem założeń doktrynalnych;
- zmniejszenie możliwości działania sił zbrojnych w operacjach reagowania kryzysowego i akcjach antyterrorystycznych.

Przedstawione powyżej słabe strony koncepcji walki sieciocentrycznej nie przekreślają definitywnie tej koncepcji. Należy brać je pod uwagę jako głosy krytyczne, dzięki którym możliwe jest udoskonalenie założeń teoretycznych dotyczących walki sieciocentrycznej oraz lepszego przełożenia tej teorii na praktykę.

²⁵ A. Borgu, *The Challenges and Limitations of „Network Centric Warfare” – the initial views of an NCW sceptic*, op. cit., s. 2.

Nie ulega wątpliwości, że zdolność do prowadzenia walki sieciocentrycznej daje posiadającym ją siłom znaczną przewagę nad potencjalnym przeciwnikiem, natomiast od umiejętności podejmowania właściwych decyzji przez dowódców zależy, czy przewaga ta zostanie wykorzystana. Dlatego też należy traktować walkę sieciocentryczną nie jako cel sam w sobie, lecz jako narzędzie służące do osiągnięcia zamierzonego celu działania.

Walka sieciocentryczna, jako nowy sposób prowadzenia działań zbrojnych wymaga opisanie i zdefiniowania za pomocą nowych pojęć, nieco odmiennych od tych, za pomocą których dotychczas opisywano dotychczasową „tradycyjną” walkę zbrojną. Nieadekwatność dotychczasowych pojęć dobrze oddaje cytata dyrektora programu Zintegrowanego Systemu Obrony firmy Boeing, Jima Albaugha: *„(...) przez wiele lat chodziło o siłę. Teraz chodzi o sieciowanie – kto pierwszy dostrzeże (rozumie), ten pierwszy reaguje”*²⁶.

Dlatego też podstawowym pojęciem, które charakteryzuje walkę sieciocentryczną jest pojęcie przewagi informacyjnej. Przewaga informacyjna w sensie militarnym to: *„(...) 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”*²⁷.

Podkreślić należy, że osiągnięcie przewagi informacyjnej nie jest celem samym w sobie. Jest ona jedynie narzędziem, które pozwoli na uzyskanie przewagi w przestrzeni walki, a w konsekwencji doprowadzi do zwycięskiego rozstrzygnięcia konfliktu. Posiadanie przewagi informacyjnej pozwoli dowódcy na wyprzedzenie działań przeciwnika, maksymalnie skuteczne i efektywne wykorzystanie własnych sił oraz na wykorzystanie słabych stron przeciwnika. Osiągnięcie przewagi informacyjnej jest jedynie wstępnym warunkiem osiągnięcia sukcesu, jeżeli niewłaściwe będzie dowodzenie, lub systemy bojowe zostaną użyte w sposób nieodpowiedni, działania zbrojne nie zostaną uwieńczone powodzeniem, mimo posiadanej przewagi informacyjnej.

²⁶ Boeing Bets on „Net-Centric” Warfare, op. cit.

²⁷ L. Konopka, *Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości*, op. cit., s. 67.

Kolejnym pojęciem, charakteryzującym odmienną koncepcję walki sieciowej jest pojęcie przestrzeni walki. Dotychczas lokalizowano działania zbrojne używając terminu: pole walki. W rozumieniu tradycyjnym był to zamknięty geograficznie obszar, na którym prowadzono działania bojowe²⁸. Pojęcie to zawierało w sobie wszystkie uwarunkowania, w większości związane z owym obszarem geograficznym (np. przejezdność, ukształtowanie terenu, sieć hydrograficzną itd.). Do kanonów słownictwa wojskowego zaliczyć można bardzo powszechnie używany termin „współczesne pole walki”, który przestaje już niestety odpowiadać współczesności. Dzieje się tak dlatego, że uwarunkowania wpływające na działania bojowe (nawet na najniższym szczeblu taktycznym) w dużym stopniu pozostają poza wspomnianym obszarem geograficznym, tradycyjnie rozumianym jako pole walki. Będą to na przykład działania propagandowo-informacyjne związane z aktualnymi działaniami taktycznymi, które mogą mieć na celu chociażby uzyskanie poparcia opinii publicznej dla prowadzonych akcji. Jest to czynnik szczególnie istotny w przypadku działań zbrojnych podejmowanych przez państwa o ustroju demokratycznym. Utrata poparcia opinii publicznej może doprowadzić do zaprzestania działań, bądź nawet całkowitego wycofania wojsk, co miało miejsce w przypadku oddziałów hiszpańskich, wycofanych z operacji stabilizacyjnej w Iraku, w następstwie ataków terrorystycznych przeprowadzonych na terenie Hiszpanii. Działaniami prowadzonymi poza tradycyjnie pojmowanym polem walki może być także użycie sensorów o zasięgu globalnym (np. rozpoznawanie satelitarne, bądź satelitarny system nawigacyjny, używany do celów taktycznych), czy też zastosowanie środków ogniowych o globalnym zasięgu (np. bombowców strategicznych lub rakiet balistycznych). O geograficznie pojmowanym polu walki trudno też mówić w przypadku działań antyterrorystycznych, albowiem 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.

Z powyższych powodów pojęcie pola walki staje się nieco anachroniczne. Bardziej trafnym terminem jest „przestrzeń walki” (battlespace), która obejmuje wszystkie uwarunkowania związane z prowadzeniem działań na wszystkich szczeblach (strategicznym, operacyjnym i taktycznym), niezależnie od ich geogra-

²⁸ Tamże, s. 69.

ficznego ulokowania. Termin przestrzeni walki (battlespace) zastąpił pojęcie „pole walki” (battlefield) w terminologii opisującej przyszłe operacje połączone Sił Zbrojnych Stanów Zjednoczonych. Według poglądów amerykańskich przestrzeń walki to „powietrze, ląd, woda i przestrzeń kosmiczna, a także siły i środki własne i przeciwnika, pogoda, teren i spektrum elektromagnetyczne w obszarze działań oraz obszarze zainteresowania”²⁹.

Pojęcie „przestrzeń walki” jest bardziej adekwatne od terminu „pole walki”, ponieważ nawet działania na szczeblu taktycznym są uwarunkowane olbrzymią liczbą czynników, które w znacznej części znajdują się poza obszarem geograficznym, na którym są fizycznie prowadzone działania bojowe. W siłach zbrojnych zorganizowanych tradycyjnie (niepołączonych w jedną sieć wymiany informacji) dowódca taktyczny nie mógłby prowadzić skutecznych działań z powodu braku możliwości monitorowania i oceny sytuacji, a także uwzględniania w swoich decyzjach tych czynników, które są poza zasięgiem jego obserwacji i bezpośredniej łączności. Sieciocentryczne podejście do działań bojowych jest rozwiązaniem tego problemu. Stworzenie sieci centrycznej, zapewniającej terminowy dopływ dowolnej informacji, której źródło znajduje się w dowolnym punkcie globu, do właściwego użytkownika, pozwala na monitorowanie, analizę i uwzględnienie w podejmowaniu decyzji wszystkich tych czynników, które znajdują się poza zasięgiem obserwacji dowódcy i jego bezpośredniej łączności w tradycyjnym rozumieniu.

Do zapewnienia powodzenia i efektywności działań prowadzonych zgodnie z założeniami walki sieciocentrycznej, konieczne jest zapewnienie odpowiedniego poziomu wymiany informacji pomiędzy poszczególnymi jej komponentami, dostarczanie danych oraz odpowiedni poziom ich wykorzystania, niezbędny do prawidłowego współdziałania. Warunkiem, którego spełnienie zapewnia prowadzenie walki sieciocentrycznej jest interoperacyjność informacyjna. Według węgierskiego naukowca, profesora Sandora Munka, owo pojęcie oznacza: „(...) zdolność poszczególnych elementów (komponentów) do zapewnienia wzajemnej wymiany zrozumiałej dla nich informacji niezbędnej do odpowiedniej współpracy. W szerszym rozumieniu

²⁹ *Concept for Future Joint Operations*, Joint Chiefs of Staff, 1997, s. 83.

*interoperacyjność informacyjna oznacza też zrozumienie zjawisk i wydarzeń zachodzących w środowisku, opisywanych tymi informacjami*³⁰.

Interoperacyjność informacyjna warunkująca walkę sieciocentryczną musi zachodzić na trzech poziomach: technicznym, syntaktycznym i semantycznym³¹. Poziom techniczny jest poziomem podstawowym interoperacyjności informacyjnej, zapewnia bowiem odbieranie i przetwarzanie fizycznego materiału informacyjnego. Z kolei syntaktyczny poziom to zdolność do pośredniego (niefizycznego) przetwarzania otrzymanych informacji pod względem językowym oraz formatu ich zakodowania. Natomiast semantyczny poziom interoperacyjności informacyjnej to zdolność odbiorcy (odbiorców) informacji do zrozumienia otrzymanej informacji pod względem zamierzonego przez jej autora znaczenia treści. Mimo, że kluczową sprawą dla zapewnienia interoperacyjności informacyjnej będą kwestie techniczne, nie należy zapominać zwłaszcza o ostatnim, semantycznym poziomie. Ujednolicenie procedur działania i używanej terminologii (tak, jak ma to miejsce w Sojuszu Północnoatlantyckim) umożliwia bowiem właściwe zrozumienie intencji nadawcy informacji i ułatwia komunikowanie się i myślenie w tych samych kategoriach.

Przegląd zaprezentowanych nowych definicji i terminów określających i opisujących walkę sieciocentryczną wskazuje na to, że istnieje mocna podbudowa teoretyczna do rewolucyjnie nowego sposobu prowadzenia walki, jakim jest walka sieciocentryczna. Mnogość nowych definicji i ich treść jest dowodem na to, że walka sieciocentryczna nie jest zjawiskiem efemerycznym i chwilową „modą” w dziedzinie wojskowości, lecz nowym trendem traktowanym poważnie przez środowiska wojskowe i naukowe.

1.2. Podstawowe założenia walki sieciocentrycznej

Rozwinięcie na bazie teoretycznych założeń walki sieciocentrycznej zasad użycia sił zbrojnych na sieciocentrycznym polu walki stało się początkiem zmian w koncepcjach operacyjnych w USA. W ramach transformacji sił zbrojnych podjęto wysiłki opracowania koncepcji operacyjnych dla sił prowadzących działania na

³⁰ S. Munk, *Walka sieciocentryczna a interoperacyjność informacyjna*, Myśl Wojskowa nr 6/2004, s. 50.

³¹ Tamże.

sieciocentrycznym polu walki. Podstawowym dokumentem stała się koncepcja „Capstone Concept for Joint Operations Version 2.0” z sierpnia 2005 r., która tworzy bazę dla koncepcji operacyjnych dla działań bojowych, stabilizacyjnych, odstraszania strategicznego oraz bezpieczeństwa wewnętrznego. Zawarte w powyższych dokumentach założenia użycia sił zbrojnych na sieciocentrycznym polu walki pozwoliły na określenie głównych zasad prowadzenia działań na sieciocentrycznym polu walki. W dokumencie Biura Transformacji Departamentu Obrony USA „The Implementation of Network-Centric Warfare” opublikowanym 5 stycznia 2005 r. zdefiniowano podstawowe zasady prowadzenia walki sieciocentrycznej (NCW Governing Principles)³²:

- walka najpierw o przewagę informacyjną (fight first for Information Superiority);
- zapewnienie dostępu do informacji dla wspólnej świadomości sytuacyjnej (Access to Information: shared awareness);
- szybkość dowodzenia i podejmowania decyzji (speed of command and decision making);
- samosynchronizacja (self-synchronization);
- rozproszenie sił i delinearacja działań (dispersed Force: non-continuous operations);
- odejście od zmasowanych (koncentracji) sił (demassification);
- głęboki zasięg środków rozpoznania (deep sensor reach);
- zwiększenie tempa wpływania na zmianę sytuacji na polu walki (alert initial conditions at higher rates of change);
- kompresja działań i poziomów konfliktu zbrojnego (compressed operations and levels of war).

Podstawową zasadą prowadzenia działań na sieciocentrycznym polu walki jest dążenie do wywalczenia i utrzymania przewagi informacyjnej poprzez zapewnienie siłom własnym bardziej terminowej, dokładnej i adekwatnej do potrzeb in-

³² *The Implementation of Network Centric Warfare*, DOD Office of Force Transformation, 2005, s. 7.

formacji niż jest w posiadaniu przeciwnika. Sposobem zdobycia i trzymania przewagi informacyjnej na sieciocentrycznym polu walki ma być³³:

- zwiększenie potrzeb informacyjnych przeciwnika, ograniczenie jego możliwości w zakresie dostępu do informacji oraz zwiększenie stopnia jego niepewności;
- zapewnienie siłom własnym dostępu do informacji poprzez połączenie ich w sieć i utrzymanie interoperacyjności, ochrona własnych systemów informacyjnych, w tym systemów zdobywania informacji (sensor systems);
- ograniczenie generowania potrzeb informacyjnych sił własnych poprzez zwiększenie zdolności do wykorzystywania przez nie wszystkich dostępnych środków zdobywania informacji.

Wspólna świadomość sytuacyjna jako zasada prowadzenia działań bojowych na sieciocentrycznym polu walki opisywana jest w amerykańskich materiałach źródłowych w aspekcie systematycznego procesu przetwarzania dostępnych danych, informacji i wiedzy w adekwatną do potrzeb poszczególnych uczestników operacji informację pozwalającą na świadomość i zrozumienie sytuacji na polu walki (the requisite level of common understanding and situational awareness). Cel ten ma być osiągany w działaniach sieciocentrycznych poprzez tworzenie rozległej sieci współdziałających użytkowników (a collaborative network of network), w której dostępne byłyby systematycznie uaktualniane informacje rozpoznawcze, przetwarzane oraz nie przetwarzane dane rozpoznawcze i inne, pozwalające wszystkim na osiąganie i utrzymywanie adekwatnej do potrzeb zbiorowej świadomości sytuacyjnej. Zapewnienie w działaniach sieciocentrycznych zbiorowej świadomości sytuacyjnej zgodnie z proponowanymi zasadami wymagać będzie, aby użytkownicy informacji stawali się jednocześnie jej dostarczycielami. Niezbędne dla realizacji powyższej zasady jest ponadto zapewnienie dostępu do danych bez względu na położenie na polu walki.

Szybkość dowodzenia i podejmowania decyzji w działaniach na sieciocentrycznym polu walki ma pozwolić na szybsze podejmowanie trafniejszych decyzji w oparciu o dostęp do informacji niemożliwych do uzyskania w działaniach płat-

³³ Tamże, s. 8.

formocentrycznych. Taka sytuacja prowadzi będzie do progresywnego eliminowania swobody wyboru opcji działania przez przeciwnika przy jednoczesnym zachowaniu własnej swobody w tym zakresie (option dominance).

Zasada samosynchronizacji w działaniach sieciocentrycznych opiera się 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. Zwiększenie możliwości przejawiania inicjatywy przez podwładnych, ma wpływać na zwiększenie tempa działań oraz poprawę zdolności sił zaangażowanych w walce na zmiany w sytuacji operacyjno-taktycznej (responsiveness). Zasada samosynchronizacji tworzy wymagania w stosunku do poziomu wyszkolenia sił wojskowych na wszystkich szczeblach dowodzenia. Tylko wysoce profesjonalni podwładni będą w stanie wspomóc dowódcę w realizacji jego zamiaru. Również proaktywne dostosowywanie się zgrupowań taktycznych do istotnych zmian na polu walki wymaga wysokiego poziomu wyszkolenia wojsk. W amerykańskich materiałach źródłowych podkreśla się, że oddolna samosynchronizacja pozwalać będzie na odejście od charakterystycznej dla działań platformocentrycznych sekwencyjności procesu decyzyjnego i działań na poszczególnych szczeblach dowodzenia³⁴.

Rozproszenie sił na polu walki oraz odejście od linearnego użycia wojsk w działaniach sieciocentrycznych łączy się ze zmianą filozofii osiągania przewagi na polu walki. W działaniach sieciocentrycznych mniej ważna jest fizyczna okupacja określonego obszaru niż zdolność sił do realizacji tam w pożądanym czasie określonej funkcji. Pozostawanie w rozproszeniu zwiększa zdolność sił do przeżycia i powoduje, iż wchodzi one w kontakt z przeciwnikiem tylko wtedy, gdy wymaga tego realizacja zadań bojowych. Rozproszenie sił kompensowane ma być wzrostem możliwości pozyskiwania informacji rozpoznawczej, uzyskiwania wsparcia ogniowego oraz bardziej wydolnym zabezpieczeniem logistycznym. Pozwolić to ma na osiągnięcie krótkotrwałej przewagi w wymiarze taktycznym bez konieczności koncentracji wojsk.

³⁴ Tamże, s. 9.

Odejście od zmasowania (koncentracji) sił w działaniach na sieciocentrycznym polu walki powiązane jest z zasadą pozostawania w rozproszeniu. Istotą zasady niekoncentrowania sił jest założenie, że pożądane efekty na polu walki można osiągnąć poprzez zwiększenie dostępności informacji o określonym obszarze geograficznym jako substytutu fizycznego rozmieszczenia tam wojsk. Odchodzenie od koncentracji wojsk ma zwiększać tempo działań oraz prędkość manewru sił na polu walki, a także utrudniać przeciwnikowi wybór obiektów (własnych sił) do zwalczania.

Zasada zapewnienia w działaniach prowadzonych zgodnie z założeniami walki sieciocentrycznej głębokiego zasięgu środków rozpoznania jest bezpośrednią implikacją paradygmatu przewagi informacyjnej jako warunku prowadzenia działań na sieciocentrycznym polu walki. Zgodnie z powyższą zasadą w działaniach sieciocentrycznych konieczne będzie rozwinięcie połączonych w sieć środków zdobywania informacji rozpoznawczej w taki sposób, aby użyteczne operacyjnie dane były uzyskiwane na odległościach i w czasie umożliwiającym uzyskanie decydujących wyników użycia wojsk. Środkiem rozpoznania w działaniach sieciocentrycznych może być każda platforma bojowa albo pojedynczy żołnierz, a zatem manewr sił na polu walki będzie tożsamy z manewrem środków rozpoznawczych. Istotnym novum w stosunku do działań platformocentrycznych jest traktowanie w doktrynie operacji sieciocentrycznych środków rozpoznania jako potencjalnego substytutu dla zgrupowań taktycznych wojsk. Zakłada się, że użycie sensorów może eliminować potrzebę rozmieszczenia zgrupowań wojsk, gdy zdobywanie informacji jest ich podstawowym zadaniem. Przewiduje się również możliwość wykorzystania środków rozpoznania jako elementu demonstrowania zdecydowania dla użycia siły. W ten sposób środki te mogą pełnić funkcję sił odstraszania militarnego³⁵.

Zwiększenie wpływu na zmianę sytuacji na polu walki jako zasady walki sieciocentrycznej postuluje wykorzystanie wszystkich atrybutów sił połączonych w ramach wspólnej sieci dla dynamicznego wpływania na rozwój sytuacji operacyjno-taktycznej w celu pozbawienia inicjatywy sił przeciwnika. We wcześniejszych materiałach zasadę tę opisywano jako „wchodzenie w cykl decyzyjny przeciwnika” (acting inside enemy's OODA Loop). Dzięki szybszej obserwacji sytuacji na polu

³⁵ Tamże, s. 9-11.

walki i jej dynamiczniejszej, bardziej kompleksowej ocenie dowódcy sił sieciocentrycznych mogą podejmować decyzje i inicjować ich realizację szybciej niż dowódcy sił platformocentrycznych, którzy w tym samym czasie mogą wciąż pozostawać na etapie oceny sytuacji. Skrócenie czasu cyklu decyzyjnego w stosunku do sił przeciwnika oraz stopnia niepewności w podejmowaniu decyzji, umożliwiane przez zastosowanie rozwiązań sieciocentrycznych, powodować będzie, że siły platformocentryczne będą zmuszone do ciągłego reagowania z opóźnieniem na działania sił sieciocentrycznych. Szybsze, uprzedzające działania przeciwnika użycie sił sieciocentrycznych, wywiera również trudny do przecenienia efekt psychologiczny, co jak potwierdza szereg przykładów historycznych, może wpływać na końcowe rozstrzygnięcie wyników konfliktu.

Ważnym elementem założeń koncepcyjnych użycia sił zbrojnych na sieciocentrycznym polu walki będzie realizacja w praktyce zasady kompresji działań i poziomów konfliktu zbrojnego. Filozofia eliminowania proceduralnych przeszkód w spójnym, harmonijnym użyciu zasobów różnych rodzajów sił zbrojnych na najniższych szczeblach dowodzenia ma pozwalać na szybkie osiąganie decydujących efektów przez zgrupowania taktyczne sił połączonych. Wyeliminowane mają zostać odrębne dla każdego rodzaju sił zbrojnych procesy organizacji, przemieszczenia, użycia oraz podtrzymania ciągłości działań i zastąpione zintegrowanymi systemami jednakowymi w skali sił zbrojnych. Kompresja działań przekładać się też ma na integrację w wymiarze sił połączonych rozpoznania, operacji i logistyki³⁶.

Na podstawie badań, których rezultaty zaprezentowane zostały w pierwszym rozdziale można stwierdzić, że w wielu państwach prowadzone są prace nad założeniami teoretycznymi walki sieciocentrycznej oraz działalność praktyczna (np. rozwijanie i zakup nowych systemów rozpoznawczych oraz środków uderzeniowych, łączności itd.), której celem jest zapewnienie siłom zbrojnym możliwości prowadzenia walki sieciocentrycznej w pełnym zakresie.

Opracowano wiele definicji, których analiza wskazuje na to, że walka sieciocentryczna to taki sposób prowadzenia działań, w którym siły zbrojne, spięte w sieć informatyczną, wykorzystują przewagę informacyjną i pełną świadomość

³⁶ *Net-Centric Environment. Joint Functional Concept*, op. cit., s. V-VI I 1-2.

sytuacji (strategicznej, operacyjnej i taktycznej) do prowadzenia szybkich i skutecznych działań, pozwalających na pokonanie przeciwnika przy możliwie najbardziej efektywnym i ekonomicznym wykorzystaniu sił własnych.

W koncepcji walki sieciocentrycznej kluczową rolę odgrywają efektywne, kompatybilne i odpowiednio zabezpieczone komputerowe systemy rozpoznania, łączności i dowodzenia, które zapewniają odpowiednią architekturę informacyjną. Natomiast prowadzenie walki sieciocentrycznej wymaga połączenia realizujących ją sił i środków w sieć, która składa się z trzech komponentów (sub – sieci): sieci informacyjnej, sieci czujników i sieci dowodzenia.

Założenia doktrynalne różnych państw oraz działalność przedsiębiorstw zorientowana na projektowanie i produkcję oprogramowania i sprzętu przeznaczonego do prowadzenia walki sieciocentrycznej wskazują jednoznacznie, że koncepcja działań sieciocentrycznych jest perspektywicznym sposobem działania sił zbrojnych XXI w. Należy jednak zauważyć, że koncepcja walki sieciocentrycznej nie jest pozbawiona wad, które wytykają jej liczni sceptycy, np. niedostosowanie do zagrożeń asymetrycznych, nadmierna koncentracja na skróceniu czasu podejmowania decyzji przez dowódców, nadmierne poleganie na zintegrowanym obrazie przestrzeni walki, który jest „przeładowany” informacją itd. Mimo to, prace nad teorią i praktyką walki sieciocentrycznej są kontynuowane w celu udoskonalenia owej koncepcji i dostosowania jej do wymagań współczesnych konfliktów zbrojnych.

1.3. Właściwości implementacji założeń walki sieciocentrycznej

Przeprowadzone przez zespół autorski analizy dostępnych materiałów źródłowych wskazują, że teoria walki sieciocentrycznej nie jest w żadnym z państw zbiorem ostatecznie sformułowanych twierdzeń, koncepcji rozwiązań strukturalnych czy funkcjonalnych. Znacząca część założeń doktrynalnych ma charakter hipotez, które są obecnie weryfikowane w ramach szeroko zakrojonego programu ćwiczeń, jak również w trakcie operacji. Istniejące różnice w narodowych poglądach na temat istoty walki sieciocentrycznej, jej zakresu oraz implikacji implementacji jej podstawowych założeń prowadzą do przyjmowania przez poszczególne

państwa odmiennych koncepcji tworzenia warunków dla przystosowania ich sił zbrojnych prowadzenia działań na sieciocentrycznym polu walki.

Przeprowadzone przez zespół autorski studia literatury przedmiotu wskazują, że amerykańskie plany implementacji rozwiązań sieciocentrycznych w siłach zbrojnych opierają się na trzech zasadniczych kierunkach działania³⁷:

- określeniu priorytetów dla rozwoju oraz implementacji założeń i rozwiązań sieciocentrycznych;
- określeniu celów implementacji założeń sieciocentrycznych i przyjęciu narzędzi pomiaru dla zmierzenia postępu ich osiągania;
- pokonaniu przeszkód w osiąganiu postępu w zakresie implementacji założeń sieciocentrycznych.

Proponowana przez Departament Obrony USA „Strategia implementacji walki sieciocentrycznej” zawiera siedem kluczowych elementów tego procesu³⁸:

- walidacja teorii walki sieciocentrycznej;
- stosowanie rozwiązań sieciocentrycznych w całym systemie obronnym;
- przyspieszenie usieciowienia sił połączonych;
- przyspieszenie eksperymentów związanych z koncepcjami i zdolnościami sieciocentrycznymi;
- poszukiwanie rozwiązań dla problemów prowadzenia operacji sieciocentrycznych wspólnie z sojusznikami i koalicjantami;
- wypracowanie taktyki i procedur dla prowadzenia operacji sieciocentrycznych.

Pierwszym etapem implementacji walki sieciocentrycznej w siłach zbrojnych USA jest realizowana obecnie walidacja założeń teoretycznych. Proces ten obejmuje z jednej strony ciągły proces doskonalenia wszystkich elementów składowych teorii, z drugiej zaś strony ich weryfikację w trakcie eksperymentów i opera-

³⁷ *The Implementation of Network-Centric Warfare*, op. cit., s. 11.

³⁸ Tamże, s. 11-12.

cji. Upewnienie się, że leżące u podstaw decyzje o implementacji założeń teoretycznych są słuszne, tworzyć ma warunki dla zastosowania rozwiązań sieciocentrycznych w całym systemie obronnym USA. W amerykańskich planach implementacji walki sieciocentrycznej przyjmuje się, że standardy sieciocentryczne nie mogą być wprowadzone selektywnie jedynie w części jednostek, ale muszą dotyczyć wszystkich elementów organizacyjnych systemu obronnego.

Od kilku lat w USA następuje przyspieszenie usieciowienia sił połączonych. O ile jednak do tej pory proces ten był realizowany przede wszystkim przez poszczególne rodzaje sił zbrojnych, to docelowo preferowanym sposobem ma być ujednolicenie standardów technicznych i organizacyjnych w skali sił zbrojnych, tak aby połączenia sieciocentryczne były możliwe nie tylko na szczeblach strategicznych i operacyjnych, lecz również na wszystkich szczeblach taktycznych.

Począwszy od operacji „Allied Force” w Kosowie w 1999 r. następuje jakościowa akceleracja wprowadzania do arsenałów systemów uzbrojenia zoptymalizowanych do użycia na sieciocentrycznym polu walki. Są one wykorzystywane jeszcze w formie testów przez docelowych użytkowników, dzięki czemu możliwe jest wprowadzenie modyfikacji i korygowanie błędów technicznych przed masowym wyposażeniem sił zbrojnych w powyższe systemy.

Ważnym, szeroko zakrojonym i zinstytucjonalizowanym elementem implementacji założeń walki sieciocentrycznej w siłach zbrojnych USA jest prowadzenie eksperymentów z koncepcjami i zdolnościami sieciocentrycznymi. Departament Obrony USA oraz dowództwa poszczególnych rodzajów sił zbrojnych realizują kompleksowe testy założeń operacyjnych walki sieciocentrycznej w ramach ćwiczeń i operacji. Doświadczenia zdobyte w ich ramach są następnie wykorzystywane dla doskonalenia przyjętych wcześniej założeń i rozwiązań.

W amerykańskich planach implementacji założeń walki sieciocentrycznej dużą wagę przykładą się do wypracowania rozwiązań technicznych i funkcjonalnych, które umożliwią siłom zbrojnym USA współdziałanie w operacjach sieciocentrycznych z siłami sojusznicznymi bądź koalicyjnymi. Szczególnie intensywnie poszukiwane są rozwiązania zapewniające współpracę z mniej zaawansowanymi technologicznie partnerami, tak aby nie zaprzepaścić potencjału narodowych rozwiązań sieciocentrycznych.

Ostatecznym etapem implementacji rozwiązań sieciocentrycznych w siłach zbrojnych USA ma stać się opracowanie założeń doktrynalnych, taktyki rodzajów wojsk dla operacji sieciocentrycznych oraz szczegółowych procedur działania w tym zakresie (Develop Doctrine and Tactics, Techniques and Procedures – TTP – for Network Centric Operations).

W dokumencie Ministerstwa Obrony Wielkiej Brytanii „Networked Enabled Capability: An Introduction” opublikowanym w kwietniu 2004 r. implementacja założeń walki sieciocentrycznej postrzegana jest jako długofalowy proces realizowany na szeregu wzajemnie przenikających się płaszczyznach. Brytyjskie podejście zakłada, iż pełne wdrożenie rozwiązań sieciocentrycznych wymusi zmiany w³⁹:

- strukturach organizacyjnych i procesach w siłach zbrojnych (Structures and Process);
- koncepcjach operacyjnych i doktrynie (Concepts and Doctrine);
- szkoleniu (Training);
- możliwościach taktyczno-technicznych sprzętu i wyposażenia (Equipment Capability);
- zdolnościach podtrzymania ciągłości działań (Sustainment);
- kształtowaniu stanów osobowych (Personnel).

Filozofia wdrożenia rozwiązań sieciocentrycznych w Siłach Zbrojnych Wielkiej Brytanii postrzegana jest przez pryzmat cyklu zorganizowanego działania obejmującego trzy podstawowe etapy⁴⁰:

- określenie wymagań dla pożądanых rozwiązań sieciocentrycznych (Development of Requirements);
- prowadzenie badań, eksperymentów i demonstracji nowych rozwiązań (Research, Experimentation and Demonstration) ;
- dostarczenie siłom zbrojnym docelowych długotrwałych rozwiązań zwiększających zdolności sieciocentryczne (Delivery of Sustained Capability Increments).

³⁹ *Network Enabled Capability. An Introduction*, op. cit., s. 23.

⁴⁰ Tamże, s. 24.

Charakterystyczne dla brytyjskiej filozofii implementacji rozwiązań sieciocentrycznych, jest to że kolejność realizacji wyżej wymienionych etapów może być zmieniona, jeśli będzie to wynikać z rozwoju sytuacji. Można przewidywać, że inicjowane samodzielnie przez producentów badania mogą prowadzić do wdrożenia nowych rozwiązań sieciocentrycznych, a w konsekwencji do zmiany wcześniej formułowanych wymagań (np. ich zwiększenie).

Kompleksowość przedsięwzięć związanych z implementacją rozwiązań sieciocentrycznych, w tym koszty rozwoju nowych technologii, spowodowały że siły zbrojne Wielkiej Brytanii mają przejść pełną transformację sieciocentryczną w trzech wyraźnie wyodrębnionych fazach⁴¹:

- fazie wstępnej („Initial”);
- fazie przejściowej („Transitional”);
- fazie dojrzałej („Mature”).

Przewidywana faza wstępna implementacji rozwiązań sieciocentrycznych ma być realizowana do 2007 r. i koncentrować się na doskonaleniu systemów łączności, głównie na eliminowaniu konieczności wykorzystywania łączności fonicznej i coraz szersze zastępowanie jej łączami danych (Links). Zmiany organizacyjne w tym etapie mają być niewielkie i bazować na obecnych rozwiązaniach doktrynalnych, strukturalnych i funkcjonalnych. Wzrost zdolności operacyjnych ma być uzyskany w szybkim tempie poprzez modernizację aktualnie posiadanego sprzętu i selektywny zakup nowego.

Faza przejściowa implementacji rozwiązań sieciocentrycznych ukierunkowana ma być na zwiększeniu zdolności operacyjnych, które wymagają dłuższego czasu wdrożenia. W fazie tej mają nastąpić głównie zmiany organizacyjne w siłach zbrojnych oraz integracja techniczna systemów informacyjnych, tak aby stworzyć warunki dla kolektywnego rozumienia sytuacji na polu walki. Faza przejściowa ma trwać do około 2015 r.⁴²

Przewidywana w planach Ministerstwa Obrony Wielkiej Brytanii faza „dojrzałej” implementacji rozwiązań sieciocentrycznych prognozowana jest na lata

⁴¹ Tamże.

⁴² Tamże, s. 25.

2020-2030. W jej ramach ma nastąpić pełna integracja zdolności sieciocentrycznych w skali sił zbrojnych, a także wdrożona doktryna, struktury organizacyjne, procedury i sprzęt niezbędny do prowadzenia działań na sieciocentrycznym polu walki.

Australijskie plany transformacji sił zbrojnych w organizację sieciocentryczną zakładają osiągnięcie pełnych zdolności do funkcjonowania na sieciocentrycznym polu walki w ciągu około piętnastu lat, czyli około 2020 r. Okres ten podzielono na trzy etapy po pięć lat. W pierwszym etapie, od 2005 do 2010, w australijskich siłach zbrojnych implementowane mają być wstępne rozwiązania sieciocentryczne w poszczególnych rodzajach sił zbrojnych oraz rozwinięty zarys teorii walki sieciocentrycznej. W latach 2010-2015 ma mieć miejsce testowanie rozwiązań, ich doskonalenie i zwiększenie zdolności sieci. Do 2015 r. przewidywane jest przekroczenie „masy krytycznej” w implementacji rozwiązań sieciocentrycznych, a okres 2015-2020 ma być ukierunkowany na zakończenie implementacji docelowych, rozwiniętych i sprawdzonych w latach 2005-2015 rozwiązań.

Narodowe filozofie dochodzenia do rozwiązań i standardów sieciocentrycznych poszczególnych państw członkowskich NATO, w tym głównie USA i Wielkiej Brytanii, znalazły swoje odzwierciedlenie w sojuszniczej wizji wdrażania założeń walki sieciocentrycznej w siłach zbrojnych NATO.

W informacji Dowództwa Transformacji NATO „Information Superiority and NATO Network-Enabled Capability” określone zostały cztery kluczowe etapy implementacji rozwiązań sieciocentrycznych w NATO⁴³:

- wypracowanie ogólnych założeń implementacji rozwiązań sieciocentrycznych;
- opracowanie i przeprowadzenie serii eksperymentów;
- przygotowanie rozwiązań organizacyjnych pozwalających na implementację rozwiązań sieciocentrycznych w siłach NATO i państwach członkowskich sojuszu;
- pełne informowanie państw członkowskich o sojuszniczych założeniach walki sieciocentrycznej w filozofii ich implementacji.

⁴³ *Information Superiority and NATO Network-Enabled Capability*, op. cit., s. 1.

Plany Dowództwa Transformacji NATO (Allied Command Transformation – ACT) w zakresie wypracowania ogólnych założeń implementacji rozwiązań sieciocentrycznych obejmują szereg przedsięwzięć. Przewiduje się wypracowanie ogólnej strategii (Strategic Framework), w której ma zostać zawarta wizja i koncepcja przewagi informacyjnej i sojuszniczych zdolności umożliwiających, przez stosowanie rozwiązań sieciowych (Information Superiority and NATO Network-Enabled Capability – IS-NNEC), ogólnej architektury systemu, filozofia implementacji (roadmap) oraz pierwszy etap planu wdrażania rozwiązań sieciocentrycznych⁴⁴.

Etap opracowania i przeprowadzenia testów rozwiązań sieciocentrycznych przez NATO ma objąć realizację badań i rozwoju nowych technologii niezbędnych do implementacji założeń walki sieciocentrycznej. W tym etapie zostaną zdefiniowane precyzyjne wymagania odnośnie zdolności sieciocentrycznych, tak aby mogły stanowić podstawę do sformułowania rekomendacji dla NATO i państw członkowskich w zakresie implementacji.

Trzecim etapem implementacji rozwiązań sieciocentrycznych w NATO ma być przygotowanie planów wdrożenia wymaganego sprzętu i rozwiązań organizacyjnych w Siłach Odpowiedzi NATO (NATO Response Force – NRF) oraz umieszczenie problematyki walki sieciocentrycznej w procesie planowania obronnego NATO (NATO Defence Planning Processes).

Analizowane wcześniej etapy implementacji przez Sojusz Północnoatlantycki rozwiązań niezbędnych do osiągnięcia pełnych zdolności do prowadzenia walki sieciocentrycznej mają być przedstawione wszystkim państwom członkowskim NATO. Dzięki temu powinno zostać osiągnięte kolektywne zrozumienie w skali sojuszu problematyki walki sieciocentrycznej i rozwiązań sieciowych (IS-NNEC). Cel ten ma być osiągnięty poprzez kształcenie oraz programy edukacyjne, a także wymianę poglądów w ramach corocznych konferencji.

Odmienność sojuszniczej filozofii implementacji założeń walki sieciocentrycznej od filozofii narodowych wynika ze sposobu finansowania. NATO w procesie planowania obronnego w przeważającej części formułuje jedynie propozycje rozwijania określonych zdolności, ale ich nie finansuje. Decyzje te pozostają w gestii państw członkowskich. Zatem pomimo wstępnego ustalenia roku 2020,

⁴⁴ Tamże.

jako daty osiągnięcia standardów zapewniających działanie sieciocentryczne sił sojuszu, nie można tej daty traktować w sposób niepodważalny.

Z badań przeprowadzonych przez zespół autorski wynika, że ogólna filozofia implementacji założeń walki sieciocentrycznej i rozwiązań umożliwiających jej prowadzenie jest zbieżna w większości państw. We wszystkich analizowanych przypadkach zakłada się stopniowe osiąganie standardów umożliwiających użycie sił wojskowych na sieciocentrycznym polu walki. Pierwszym etapem jest zwykle zwiększenie możliwości wymiany informacji osiągane poprzez modernizację systemów łączności. W kolejnych etapach mają następować zmiany w organizacji sił oraz doktrynie i taktyce ich użycia na polu walki.

Horyzont czasowy implementacji rozwiązań sieciocentrycznych zawiera się w przedziale od 15 do 25 lat. Nakreślony okres dzielony jest zwykle na etapy doskonalenia teorii, osiągania rozwiązań pośrednich oraz stanu docelowego. Ogólność przyjętych ustaleń oraz ich uzależnienie od postępu technologicznego powoduje, że nakreślony przez większość państw horyzont czasowy należy traktować jako próbę określenia pożądanych ram czasowych, a nie harmonogram implementacji założeń walki sieciocentrycznej i rozwiązań gwarantujących jej prowadzenie.

1.4. Wnioski

Z badań przeprowadzonych w rozdziale 1 wynika, że początki teorii walki sieciocentrycznej są rezultatem przełomu w stosowaniu technologii informatycznych na wolnym rynku ekonomicznym. Rozwiązania tam stosowane szybko zostały zaadoptowane do działań związanych z użyciem sił zbrojnych, czyli do działań militarnych.

Przejście na sieciocentryczny sposób prowadzenia walki zapewnia oddzielenie sensorów od platform uzbrojenia, a także operatorów od sensorów i platform. Stanowiska operatorów mogą być ulokowane w miejscu zapewniającym im bezpieczeństwo, z którego mogą zdalnie sterować platformami bojowymi.

Badania potwierdziły, że istnieje wiele definicji walki sieciocentrycznej. Z ich analizy wynika, że walka sieciocentryczna jest takim sposobem prowadzenia działań, w którym siły zbrojne, spięte siecią informatyczną, uzyskują przewagę infor

macyjną oraz świadomość sytuacyjną na wszystkich poziomach prowadzenia działań (strategicznym, operacyjnym i taktycznym), co zapewnia możliwość prowadzenia szybkich i skutecznych działań militarnych przy możliwie najbardziej efektywnym i ekonomicznym wykorzystaniu sił własnych.

Obecne wyposażenie oraz wyszkolenie sił zbrojnych pozwala na prowadzenie walki sieciocentrycznej na poziomie taktycznym, co potwierdziły doświadczenia z operacji prowadzonych w Afganistanie i Iraku. Przewiduje się, że w perspektywie najbliższych kilku lat możliwe będzie, w ramach wspólnej sieci systemów, prowadzenie takich działań w skali rodzajów sił zbrojnych, a około 2020 roku możliwe będzie osiągnięcie pełnej implementacji standardów w tym zakresie.

Najbardziej zaawansowane badania oraz wdrażanie rozwiązań w zakresie walki sieciocentrycznej prowadzone są w siłach zbrojnych Stanów Zjednoczonych. W Wielkiej Brytanii w założeniach teoretycznych największy nacisk kładzie się na zdolność zbierania, analizy oraz dystrybucji dokładnej i terminowej informacji w celu zapewnienia rozumienia i świadomości sytuacji na wszystkich szczeblach. Według tych założeń systemy uzbrojenia, stanowiska dowodzenia i sensory spięte są siecią informatyczną przez co zapewnia się dużą sprawność działania oraz większą prędkość i precyzję działania.

Badania teorii walki sieciocentrycznej prowadzone też są w wielu innych państwach (np. Szwecja, Kanada, Australia, Nowa Zelandia czy Chiny) oraz w NATO. W doktrynie sojuszu walka sieciocentryczna staje się jedynym z celów transformacji. Zamierza się go osiągnąć poprzez zapewnienie siłom sojuszniczym zdolności do osiągania przewagi informatycznej oraz decyzyjnej. Dzięki temu możliwe będzie użycie w walce zbrojnej sił, które są niezbędne w miejscu, gdzie jest to niezbędne i w czasie, który pozwala wyprzedzić działanie przeciwnika.

Główną zasadą prowadzenia działań na sieciocentrycznym polu walki jest dążenie do wywalczenia i utrzymania przewagi informacyjnej. Oznacza to zapewnienie siłom własnym bardziej terminowej, dokładnej i adekwatnej do aktualnej sytuacji informacji niż może to zrobić przeciwnik. Poprzez tworzenie rozległej sieci współdziałających użytkowników, w której dostępne są systematycznie uaktualniane informacje rozpoznawcze i dane o własnych siłach oraz ich możliwościach zapewnia się osiągnięcie i utrzymanie adekwatnej do potrzeb zbiorowej świadomości sytuacyjnej. Z kolei szybkość dowodze-

nia i podejmowania decyzji w działaniach na sieciocentrycznym polu walki ma pozwolić na szybsze i precyzyjne użycie niezbędnych sił w oparciu o dostęp do informacji nie-
możliwych do uzyskania w działaniach platformocentrycznych.

Inną, wiodącą zasadą w działaniach sieciocentrycznych jest zasada samosynchronizacji. 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. Poprzez zwiększanie możliwości przejawiania inicjatywy przez podwładnych osiąga się zwiększenie tempa działań oraz poprawę zdolności sił zaangażowanych w walce. Zasada ta tworzy wymagania wobec poziomu wyszkolenia sił wojskowych na wszystkich szczeblach dowodzenia. Tylko profesjonalnie przygotowani podwładni będą w stanie wspierać swojego dowódcę w realizacji jego zamiaru.

Przeprowadzone analizy wskazują też, że rozproszenie sił na polu walki oraz odejście od linearnego użycia wojsk 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 wykonywane zadania.

W koncepcji walki sieciocentrycznej kluczową rolę odgrywają kompatybilne i odpowiednio zabezpieczone komputerowe systemy rozpoznania, łączności i dowodzenia, które zapewniają odpowiednią architekturę informacyjną. Siły i środki na sieciocentrycznym polu walki połączone są siecią, składającą się z trzech elementów – sieci informacyjnej, sieci czujników i sieci dowodzenia.

Stan zaawansowania w badaniach nad teorią walki sieciocentrycznej jest zróżnicowany w poszczególnych państwach. Również implementacja tych założeń na obcym etapie charakteryzuje się zróżnicowanym zaawansowaniem. W Stanach Zjednoczonych proces implementacji założeń teoretycznych jest najbardziej zaawansowany. Obejmuje on ciągły proces doskonalenia wszystkich elementów teorii, z drugiej zaś ich weryfikację w trakcie eksperymentów i prowadzonych operacji. W planach amerykańskich zwraca się uwagę na wypracowanie rozwiązań technicznych i funkcjonalnych, które umożliwiają siłom zbrojnym USA udział i współdziałanie w operacjach sieciocentrycznych z siłami sojuszniczymi lub koalicyjnymi.

Ostatnim etapem implementacji założeń walki sieciocentrycznej będzie opracowanie założeń doktrynalnych, taktyki rodzajów wojsk oraz szczegółowych procedur działania.

W Wielkiej Brytanii implementacja założeń walki sieciocentrycznej zaplanowana jest jako proces długotrwały. Obejmuje on trzy podstawowe etapy – określenie wymagań, prowadzenie badań, elementów i demonstracji nowych rozwiązań oraz dostarczenie siłom zbrojnym docelowych, długoterminowych rozwiązań technicznych, organizacyjnych, doktrynalnych i taktycznych zwiększających zdolności sieciocentryczne.

Natowskie plany implementacji założeń walki sieciocentrycznej przewidują też szereg przedsięwzięć. Po opracowaniu strategii i wizji w zakresie przewagi informacyjnej i sojuszniczych zdolności opracowana zostanie ogólna architektura systemu oraz sposób implementacji tych rozwiązań.

Założenia sojusznicze są odmienne od np. amerykańskich, co wynika ze sposobu ich finansowania. W procesie planowania gremia sojusznicze NATO formułują jedynie propozycje rozwijania zdolności sieciocentrycznych, lecz ich nie finansują. Decyzje te pozostają w gestii państw członkowskich.

Badania potwierdziły też, że ogólna filozofia implementacji założeń walki sieciocentrycznej i rozwiązań zapewniających jej prowadzenie jest podobna w większości państw. Zakłada się stopniowe osiąganie standardów umożliwiających użycie sił wojskowych na sieciocentrycznym polu walki. W pierwszej kolejności zakłada się zwiększenie możliwości zbioru, analizy i dystrybucji informacji, następnie przewiduje się zmiany organizacyjno-techniczne, doktrynalne i taktyczne. Perspektywa wdrażania tych rozwiązań to 15 – 25 lat.

Rozdział 2

ARCHITEKTURA SIECIOCENTRYCZNEGO POLA WALKI ORAZ SPOSÓB JEGO FUNKCJONOWANIA

Dokonana przez zespół autorski analiza założeń teoretycznych walki sieciocentrycznej ukierunkowana na zidentyfikowanie jej istoty, zakresu i zasad stanowi wystarczającą bazę do podjęcia próby określenia ogólnej architektury sieciocentrycznego pola walki oraz poznania sposobu funkcjonowania na nim sił wojskowych. Wyniki przeprowadzonych badań zawarte w niniejszym rozdziale zgrupowano w dwóch podrozdziałach. W pierwszym ujęte zostały zagadnienia związane z uwarunkowaniami tworzenia typologii elementów składowych sieciocentrycznego pola walki oraz analiza funkcjonujących w teorii założeń. Ocena i wnioski zawarte w drugim podrozdziale stanowią próbę odpowiedzi na pytanie, w jaki sposób funkcjonują (działają) na sieciocentrycznym polu walki siły wojskowe i co jest źródłem przewagi sił użytych zgodnie z założeniami sieciocentrycznymi nad siłami prowadzącymi działania platformocentryczne.

2.1. Architektura sieciocentrycznego pola walki

Analiza założeń teoretycznych walki sieciocentrycznej wskazuje, że sieciocentryczne pole walki jest bardzo złożone ze względu na swoją wielowymiarowość oraz dużą liczbę zróżnicowanych, pozostających w dynamicznie zmiennych interakcjach, hierarchicznych i horyzontalnych elementów składowych. W przeciwieństwie do typowego dla epoki industrialnej trójwymiarowego, linearnego postrzegania pola walki oraz rzutowanego rozmieszczenia na nim hierarchicznie zorganizowanych sił wojskowych, epoka informacyjna przyniosła szersze i bardziej kompleksowe postrzeganie tych problemów. Pole walki w operacjach z epoki informacyjnej nie ogranicza się do przestrzeni trójwymiarowej, ale rozciąga się również na spektrum elektromagnetyczne oraz tzw. „przestrzeń informacyjną”. W dostępnej literaturze przedmiotu istnieje wiele klasyfikacji podziału pola, czy też przestrzeni, w jakiej toczy się walka sieciocentryczna. Różne ośrodki naukowe, stosując różne kryteria dzielą sieciocentryczne pole walki na domeny, warstwy bądź sieci. Za-

uważyć można, że w początkowym okresie kręgi techniczne oraz wojskowe przedstawiały architekturę sieciocentrycznego pola walki poprzez pryzmat elementów je tworzących, zgrupowanych pod względem technicznym (np. systemy informatyczne, sensory, platformy bojowe).

Podejście takie zostało w ostatnim okresie zmodyfikowane, sieciocentryczne pole walki postrzegane jest również przez pryzmat interakcji społecznych i przewartościowań w kulturze organizacyjnej.

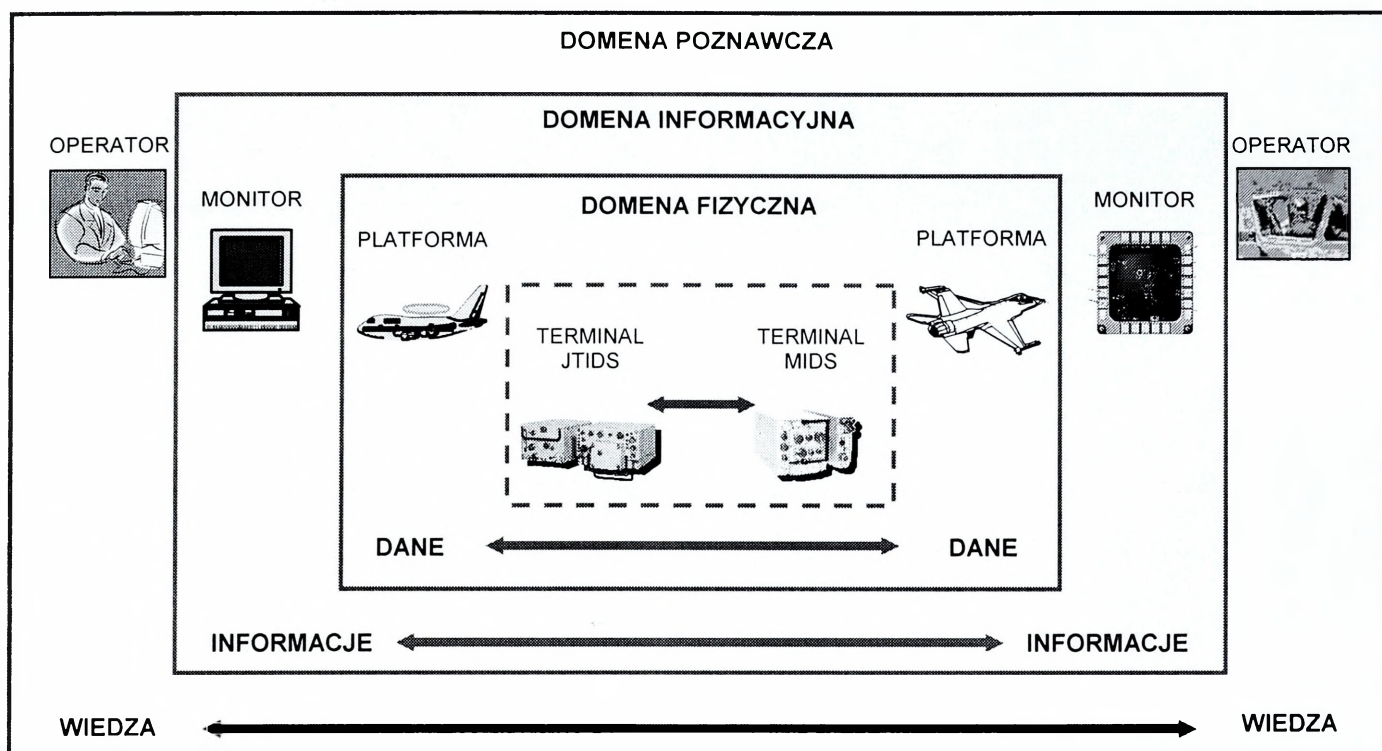
Jednym ze sposobów opisu architektury sieciocentrycznego pola walki, mającym swoje źródło w opublikowanej w 1999 r. koncepcji walki sieciocentrycznej Garstki i Cebrowskiego jest jego podział na domeny. Wyróżnia on trzy płaszczyzny przestrzeni (domeny), w jakich prowadzona jest walka sieciocentryczna (rys. 2.1) obejmujące⁴⁵:

- domenę fizyczną;
- domenę informacyjną;
- domeną poznawczą.

Zgodnie z założeniami teoretycznymi zawartymi w opracowaniu „Network Centric Warfare: Developing and Leveraging Information Superiority” domena fizyczna definiowana jest jako tradycyjna przestrzeń, w której toczy się walka zbrojna, obejmująca przestrzeń fizyczną (trójwymiarową) oraz spektrum elektromagnetyczne. W tej domenie występują platformy i systemy komunikacyjne oraz informatyczne łączące je w sieć. Domenę fizyczną łatwo zdefiniować, ponieważ tworzą ją elementy istniejące fizycznie, o znanych i mierzalnych cechach i charakterystykach, stosunkowo łatwych do określenia (np. żywotność danego systemu, prawdopodobieństwo trafienia celu dla rakiety powietrze-powietrze, itp.).

Uważana w początkowym okresie rozwoju teorii walki sieciocentrycznej za najważniejszą domena informacyjna jest strefa, w której zachodzi tworzenie, obróbka i przechowywanie informacji. W tej domenie ma miejsce przepływ informacji między elementami działającymi na sieciocentrycznym polu walki (rozkazy, sygnały dowodzenia, przekazanie zamiaru działania przełożonego, itd.). Domena

⁴⁵ A. Money, *Report on Network Centric Warfare. Sense of the Report*, 2001, s. 5.



Źródło: opracowanie własne na podstawie: P. Phister, I. Plonisch, *Military Applications of Information Technologies*, Air and Space Power Journal, 2004, s. 34.

Rys. 2.1. Domeny sieciocentrycznego pola walki

informacyjna jest szczególnie ważna w architekturze sieciocentrycznej ze względu na konieczność uzyskania i utrzymania przewagi informacyjnej nad przeciwnikiem, dlatego też musi być we właściwy sposób chroniona i zabezpieczona przed ofensywnymi działaniami przeciwnika.

Ważnym elementem w teorii walki sieciocentrycznej Dawida Albertsa, Johna Garstki oraz Fredericka Steina jest wyodrębnienie domeny poznawczej jako równorzędnej w stosunku do domeny fizycznej i informacyjnej obszarów prowadzenia walki. Domena poznawcza nie jest tworem materialnym, lecz istnieje wyłącznie w umysłach uczestników działań na sieciocentrycznym polu walki. Domena ta jest trudna do zidentyfikowania, gdyż tworzą ją takie elementy jak: przywództwo, morale, spójność jednostki (pododdziału), jakość wyszkolenia, świadomość sytuacji a nawet opinia publiczna. W domenę poznawczą umiejscowiony jest zamiar działania, doktryna, taktyka działania, czy też procedury postępowania. Atrybuty tej domeny są niemierzalne.

Przyjęty w latach 90., w początkowym okresie rozwoju amerykańskich założeń walki sieciocentrycznej podział środowiska, w jakim ta walka może być prowadzona na trzy domeny (fizyczną, informacyjną oraz poznawczą) został rozwinię-

ty przez Biuro Transformacji Sił Zbrojnych Departamentu Obrony USA (Office of Force Transformation – OFT) dokumencie koncepcyjnym „Network Centric Operations Conceptual Framework Version 2” zidentyfikowano cztery główne, uznane za kluczowe domeny prowadzenia walki sieciocentrycznej⁴⁶:

- domenę fizyczną;
- domenę informacyjną;
- domenę poznawczą (kognitywną)⁴⁷;
- domenę społeczną.

Domena fizyczna definiowana jest w przywoływanym dokumencie jako środowisko fizyczne, w którym toczy się walka zbrojna (na lądzie, morzu, w przestrzeni powietrznej i w kosmosie) oraz istnieje infrastruktura zabezpieczająca prowadzenie walki sieciocentrycznej.

Domena informacyjna postrzegana jest jako „cyberprzestrzeń” prowadzenia walki zbrojnej, w której informacja jest wytwarzana, przetwarzana, rozwijana i wzbogacana (value – added) oraz współposiadana (shared). W porównaniu z wcześniejszymi założeniami teoretycznymi, wyraźnie zauważalne jest położenie nacisku na korelacje i syntezę oraz udostępnianie informacji w obrębie domeny informacyjnej.

Domena poznawcza (kognitywna) walki sieciocentrycznej obejmuje sferę percepcji, świadomości, zrozumienia, podejmowania decyzji, przekonań (wierzeń) oraz systemu wartości cechujących uczestników tej walki.

Nowo zdefiniowana **domena społeczna** walki sieciocentrycznej postrzegana jest w konceptualnej wizji Biura Transformacji Sił Zbrojnych Departamentu Obrony USA jako przestrzeń, w której zachodzą relacje pomiędzy grupami (zbiorami) uczestników tej walki (force entities). W domenie społecznej prowadzenia walki sieciocentrycznej powyższe zbiorowości wchodzi w wzajemne interakcje, wypracowują wspólne postrzeganie (świadomość) sytuacji oraz zrozumienie kon-

⁴⁶ *Network Centric Operations Conceptual Framework Version 2.0*, EBR, 2004, s. 13.

⁴⁷ Kognitywny – poznawczy, dotyczący poznania (łac. cognito – poznanie). *Słownik wyrazów obcych*, PWN, 1980, s. 362.

ty przez Biuro Transformacji Sił Zbrojnych Departamentu Obrony USA (Office of Force Transformation – OFT) dokumencie koncepcyjnym „Network Centric Operations Conceptual Framework Version 2” zidentyfikowano cztery główne, uznane za kluczowe domeny prowadzenia walki sieciocentrycznej⁴⁶:

- domenę fizyczną;
- domenę informacyjną;
- domenę poznawczą (kognitywną)⁴⁷;
- domenę społeczną.

Domena fizyczna definiowana jest w przywoływanym dokumencie jako środowisko fizyczne, w którym toczy się walka zbrojna (na lądzie, morzu, w przestrzeni powietrznej i w kosmosie) oraz istnieje infrastruktura zabezpieczająca prowadzenia walki sieciocentrycznej.

Domena informacyjna postrzegana jest jako „cyberprzestrzeń” prowadzenia walki zbrojnej, w której informacja jest wytwarzana, przetwarzana, rozwijana i wzbogacana (value – addend) oraz współposiadana (shared). W porównaniu z wcześniejszymi założeniami teoretycznymi, wyraźnie zauważalne jest położenie nacisku na korelacje i syntezę oraz udostępnianie informacji w obrębie domeny informacyjnej.

Domena poznawcza (kognitywna) walki sieciocentrycznej obejmuje sferę percepcji, świadomości, zrozumienia, podejmowania decyzji, przekonań (wierzeń) oraz systemu wartości cechujących uczestników tej walki.

Nowo zdefiniowana **domena społeczna** walki sieciocentrycznej postrzegana jest w konceptualnej wizji Biura Transformacji Sił Zbrojnych Departamentu Obrony USA jako przestrzeń, w której zachodzą relacje pomiędzy grupami (zbiorami) uczestników tej walki (force entities). W domenie społecznej prowadzenia walki sieciocentrycznej powyższe zbiorowości wchodzi w wzajemne interakcje, wypracowują wspólne postrzeganie (świadomość) sytuacji oraz zrozumienie kon-

⁴⁶ Network Centric Operations Conceptual Framework Version 2.0, EBR, 2004, s. 13.

⁴⁷ Kognitywny – poznawczy, dotyczący poznania (łac. cognito – poznanie). *Słownik wyrazów obcych*, PWN, 1980, s. 362.

sekwencji z tego wynikających (understandings), a także podejmują kolektywne (zbiorowe) decyzje⁴⁸.

W najnowszych amerykańskich założeniach teoretycznych na temat operacji sieciocentrycznych (Network Centric Operations – NCO) wyraźnie podkreślone jest wzajemne przenikanie się poszczególnych domen prowadzenia walki sieciocentrycznej. Pomimo wyraźnej odrębności od innych domen, domena społeczna przenika domenę poznawczą i informacyjną. W szczegółowych wyjaśnieniach tego zjawiska w teorii walki sieciocentrycznej jako przykład takiego przenikania się domen podawany jest proces przechodzenia od zachodzących w umysłach poszczególnych uczestników walki procesów poznawczych do kolektywnego postrzegania (uświadamiania) sytuacji na polu walki i jej konsekwencji oraz podejmowania decyzji przez zbiorowych uczestników walki.

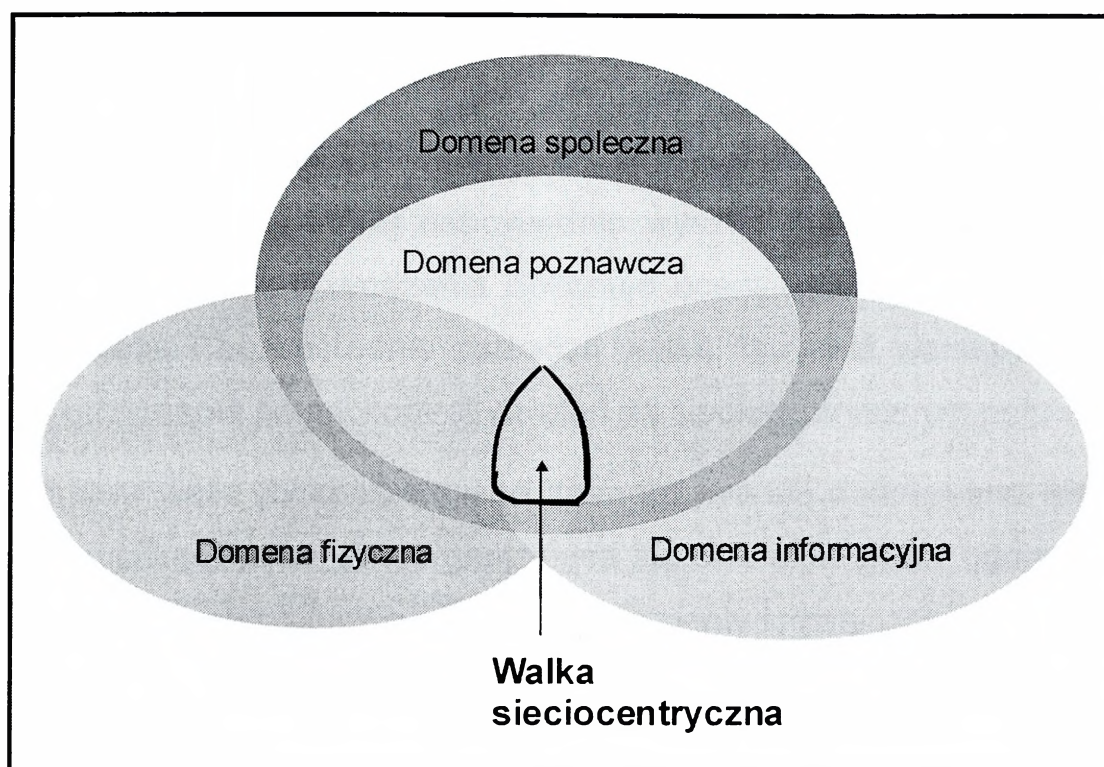
Kolektywne procesy poznawcze są w takim przypadku powiązane z relacjami społecznymi charakterystycznymi dla określonej zbiorowości, co w konsekwencji czyni je działaniem społeczno-poznawczym (socio-cognitive activity), a tym samym zawierającym się zarówno w domenie poznawczej (kognitywnej), jak i społecznej (rys. 2.2)⁴⁹.

W polskojęzycznej literaturze przedmiotu podstawowym sposobem przedstawienia struktury sieciocentrycznego pola walki jest jego podział na warstwy (rys. 2.3). Wśród warstw sieciocentrycznego pola walki wyróżniane są:

- warstwa dowodzenia;
- warstwa walki;
- warstwa informacyjna;
- warstwa sensorów.

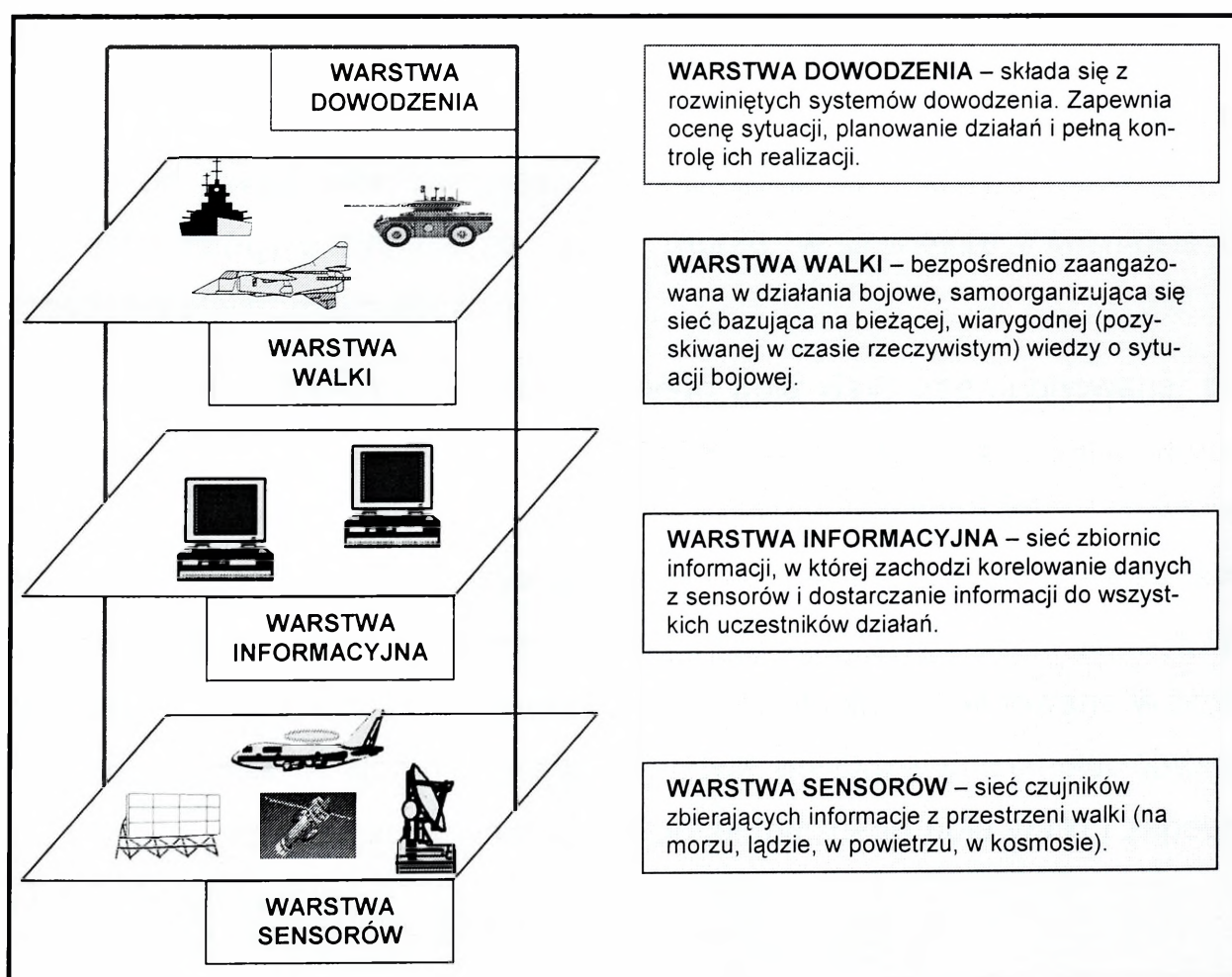
⁴⁸ Tamże, s. 14.

⁴⁹ *The Implementation of Network – Centric Warfare*, op. cit. cit., s. 21.



Źródło: opracowanie własne na podstawie: *The Implementation of Network – Centric Warfare*, op. cit. cit., s. 23.

Rys. 2.2. Podstawowe domeny walki sieciocentrycznej i relacje między nimi



Źródło: opracowanie własne na podstawie: L. Konopka, *Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości*, op. cit., s. 77.

Rys. 2.3. Warstwowa struktura sieciocentrycznego pola walki

W opublikowanym w 2004 r. artykule zastępcy Szefa Sztabu Generalnego Wojska Polskiego gen. Lecha Konopki „Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości” warstwa dowodzenia jest utożsamiana z tą częścią składową pola walki, w której odpowiednio wyszkolony personel, przy pomocy rozwiniętych systemów dowodzenia dokonuje oceny sytuacji, analizuje zadania, planuje działania i bezpośrednio zarządza walką. Istnienie warstwy dowodzenia umożliwia utrzymanie pełnej kontroli działań na sieciocentrycznym polu walki.

Warstwa walki (bezpośredniego zaangażowania) definiowana jest w przywoływanej publikacji jako samoorganizująca się sieć elementów ugrupowania bojowego (platformy uderzeniowe, ich załogi, elementy logistyczne itd.), bazująca na bieżącej, wiarygodnej i pozyskiwanej w czasie rzeczywistym wiedzy o sytuacji bojowej.

W warstwie informacyjnej sieciocentrycznego pola walki zachodzi korelowanie danych z sensorów oraz dostarczanie informacji do systemów walki wszystkich szczebli (w zakresie uprawnień przydzielonych poszczególnym użytkownikom).

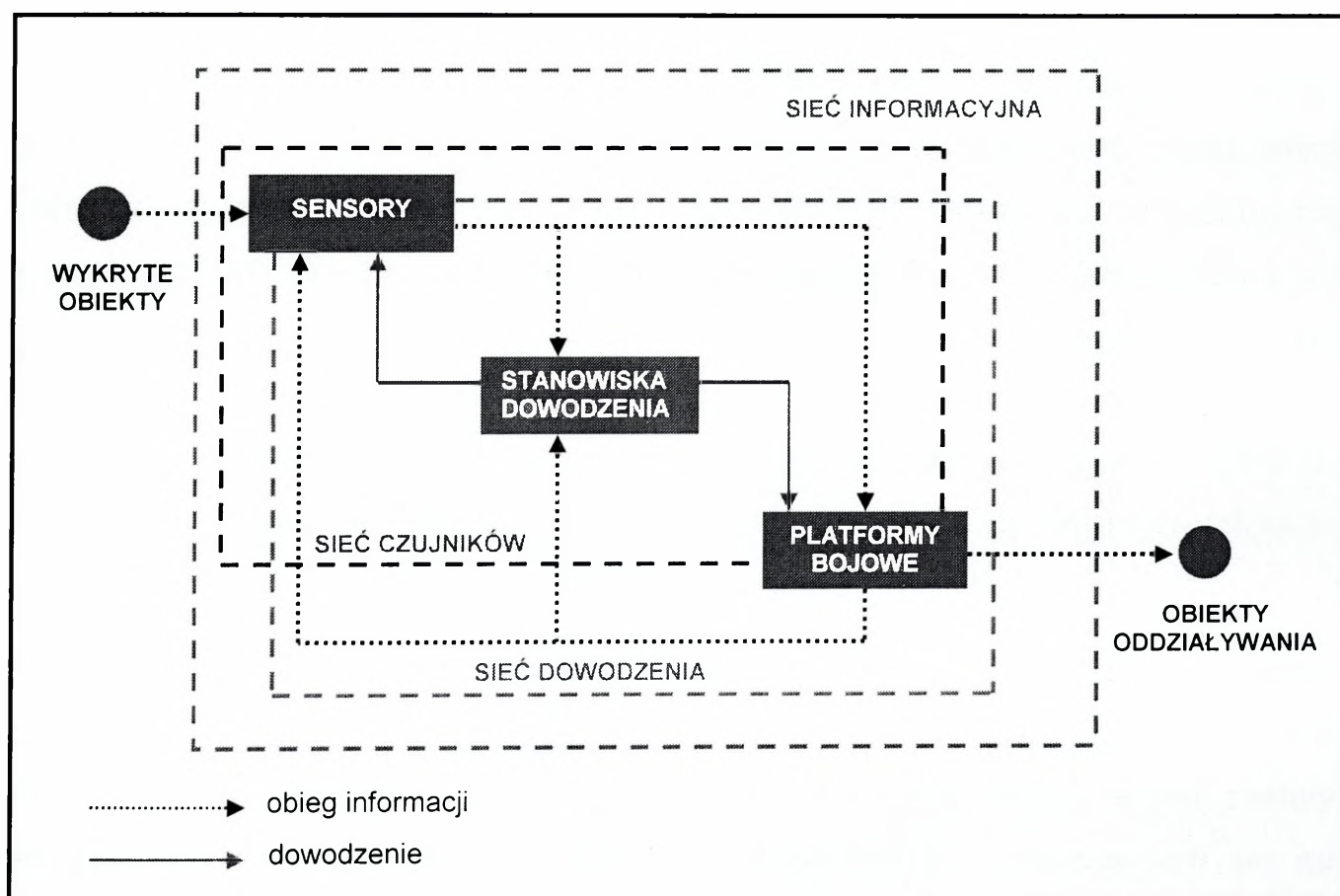
Warstwa sensorów składa się z czujników (np. bezpilotowe aparaty latające, naziemne stacje radiolokacyjne, czujniki ruchu itd.), których zadaniem jest zbieranie informacji o sytuacji na lądzie, morzu, w powietrzu i kosmosie oraz w przestrzeni elektromagnetycznej.

Analiza architektury sieciocentrycznego pola walki zaproponowanej przez gen. Konopkę wskazuje, że podstawą przyjętej przez niego typologii nie są domeny prowadzenia walki sieciocentrycznej, ale procesy związane ze zdobywaniem, korelacją, przesyłaniem i wykorzystywaniem informacji. O ile warstwa sensorów jest odpowiedzialna za zdobywanie danych i informacji, to ich korelacja i dystrybucja są realizowane w warstwie informacyjnej, a działania podejmowane w oparciu o nie mają miejsce w warstwie walki. Warstwa dowodzenia stanowi natomiast element integrujący pozostałe warstwy sieciocentrycznego pola walki i zapewniająca ich funkcjonowanie.

Najczęściej przyjmowaną, a zarazem najszerzej opisaną w literaturze przedmiotu architekturą sieciocentrycznego pola walki jest podział na sieci (sub – sieci)⁵⁰. W amerykańskich opracowaniach przyjmuje się, że powyższą architekturę tworzą:

- sieć informacyjna;
- sieć czujników;
- sieć dowodzenia.

Poszczególne sieci są ze sobą ściśle powiązane. Zależności między sieciami są przedstawiane zazwyczaj w aspekcie ich wzajemnego przenikania się i zawierania w sobie (rys. 2.4).



Źródło: opracowanie własne na podstawie: www.dtic.mil/jsc/j6/education/warfare.html

Rys. 2.4. Zależności pomiędzy sub – sieciami sieciocentrycznego pola walki

⁵⁰ Podział taki przedstawiony jest na przykład w opracowaniu *Information paper – Observations on the Emergence of Network – Centric Warfare*, dostępne z: www.dtic.mil/jsc/j6/education/warfare.html

Zgodnie z amerykańskimi założeniami walki sieciocentrycznej, sieć informacyjna to komponent, który jest infrastrukturą łączności i przetwarzania danych. Zapewnia ona środki dla odbioru, obróbki, przesyłu, przechowywania i ochrony informacji na rzecz sił prowadzących walkę sieciocentryczną. Jest to sieć podstawowa, bez której niemożliwe byłoby osiągnięcie przewagi informacyjnej. Jest ona zbiorem sieci, składającym się z kanałów łączności, węzłów informatycznych, systemów operacyjnych i aplikacji zarządzania informacjami, które umożliwiają przetwarzanie danych i łączność w całej przestrzeni walki. Możliwości techniczne sieci informacyjnej zapewniają tworzenie świadomości sytuacyjnej dla sieci czujników, co jest podstawą uzyskania przewagi informacyjnej. Świadomość sytuacyjna pojawia się wtedy, gdy osiągnięty zostaje odpowiedni poziom informacji dotyczącej sił własnych, przeciwnika oraz warunków działania.

Sieć informacyjna składa się z dwóch podsystemów: wojskowego i cywilnego (komercyjnego). Służy do transmisji informacji zróżnicowanych, co do treści i sposobu przekazu. Dane oraz informacje w postaci dźwiękowej, wizualnej lub w postaci plików danych mogą być przesyłane bezpośrednio do danego źródła lub drogą okrężną, jeżeli bezpośredni transfer nie jest możliwy. Informacje, które przesyłane są za pomocą owej sieci muszą być w odpowiedni sposób zabezpieczone, by nie mogły zostać pozyskane przez przeciwnika. Właściwości sieci informacyjnej zapewniają walczącym siłom szybki dostęp do wymaganych informacji, co umożliwia dominację na wszystkich poziomach konfliktu.

Kolejnym komponentem składającym się na całość architektury sieci służącej do prowadzenia walki sieciocentrycznej jest sieć czujników. Zapewnia ona walczącym siłom świadomość przestrzeni walki. Jest ona postrzegana jako zestaw tak zwanych czujników peryferyjnych (sensor peripherals) znajdujących się na platformach rozpoznawczych oraz oprogramowania czujników (sensor applications). Zarówno czujniki, jak i oprogramowanie są „nałożone” na sieć informacyjną, czyli podłączone do niej tak, by zapewnić przepływ informacji.

Czujniki (sensory) peryferyjne zabezpieczające prowadzenie walki sieciocentrycznej, mogą być umieszczone w przestrzeni kosmicznej i powietrznej, na lądzie, na powierzchni wody i pod nią oraz w przestrzeni informatycznej (cyberprzestrzeni). Sensory mogą być zainstalowane zarówno na specjalistycznych platformach rozpoznawczych, jak i na platformach bojowych. Mogą być również prze-

noszone przez pojedynczych żołnierzy. Należy zauważyć, że sensory nie służą tylko do pozyskiwania informacji o lokalizacji wojsk własnych i przeciwnika, ale śledzą również ilość środków, które podlegają zużyciu: paliwa, amunicji itd.

Elementem składowym sieci czujników jest oprogramowanie czujników składających się z części związanej z konkretnymi, wyspecjalizowanymi czujnikami oraz z części, która umożliwia sterowanie czujnikami oraz syntezę uzyskanych przez nie danych.

Już w początkowym okresie tworzenia teorii walki sieciocentrycznej zakładano, że sieć czujników może być zarówno stała, jak i tymczasowa. Przyjmowano, że sieć doraźna będzie tworzona dla przeprowadzenia konkretnego działania, na przykład w celu obezwładnienia obrony powietrznej przeciwnika. W takim przypadku architektura sieci czujników będzie organizowana w ten sposób, aby operatorzy mogli dynamicznie stawiać zadania jej podsystemom w celu wspierania działań konkretnych platform bojowych. Rozmiar, skład i złożoność takiej tymczasowej sieci uzależniona będzie od poziomu świadomości przestrzeni walki, jaki wymagany jest dla osiągnięcia celu działania. Zakładano, że liczba i rodzaj sensorów wymaganych do wsparcia konkretnego działania będzie się zwiększać lub zmniejszać w stosunku do sieci stałej w zależności od rozmiaru i rodzaju przestrzeni walki (na przykład od rodzaju terenu), a także w zależności od składu oraz możliwości sił własnych i sił przeciwnika.

W literaturze przedmiotu podkreśla się, że architektura sieci czujników ma wpływ na zwiększenie świadomości przestrzeni walki, a także pozwala na wykorzystanie tej świadomości podczas działań zbrojnych. Możliwości te osiągane są dzięki zastosowaniu dynamicznego sterowania sensorami, syntezie danych oraz właściwej dystrybucji informacji w sieci informacyjnej.

Dynamiczne sterowanie czujnikami zapewnia dowódcom elastyczność działania oraz możliwość synchronizacji podejmowanych czynności, a także regulowanie tempa działań. Owa operacyjna elastyczność jest możliwa do osiągnięcia dzięki zdolności sieci czujników do pracy w różnych trybach. Pierwszy tryb to działanie sieci w sposób uprzednio zaplanowany (pre-planned mode), drugi natomiast, to natychmiastowa reakcja na dane wprowadzane dynamicznie, w czasie trwania działań (real-time mode). Podczas pracy sieci w trybie uprzednio zaplanowanym

wszystkie sensory, zarówno aktywne (np. radary), jak i pasywne (np. czujniki optyczne) są zaprogramowane tak, aby uzyskiwać informację w sposób najbardziej dogodny i zapewnić poziom świadomości przestrzeni walki, konieczny do przeprowadzenia uprzednio zaplanowanych działań. Dla przykładu, uzyskiwanie informacji pozwalających na ocenę rezultatów działań będzie realizowane poprzez działanie sieci czujników w trybie uprzednio zaplanowanym. Operatorzy czujników pracujących w tejże sieci już na etapie planowania uderzenia będą mogli wprowadzić komendy programujące pracę sensorów w celu uzyskania wymaganych informacji. Dysponowanie nadwyżką czasu umożliwia również zaplanowanie pracy czujników w sposób maksymalnie efektywny i optymalny. Z kolei zdolność sieci czujników do szybkiego przejścia do funkcjonowania w trybie dynamicznym zapewnia dowódcy możliwość stawiania zadań rozpoznawczych w czasie rzeczywistym i uzyskiwanie wysokiego poziomu świadomości przestrzeni walki „na żądanie”, np. na szczególnie ważnym kierunku działań.

Synteza danych jest tą możliwością sieci czujników, która umożliwia szybkie tworzenie świadomości przestrzeni walki. Uzyskuje się ją dzięki łączeniu danych wielospektralnych, czyli uzyskanych z różnego typu sensorów (radiolokatory, czujniki podczerwieni, noktowizyjne, optyczne itd.). Zwiększa to prawdopodobieństwo wykrycia oraz identyfikacji obiektów znajdujących się w przestrzeni walki. Ponadto, informacje pozyskiwane przez sensory różnego typu zwiększają zdolność śledzenia celów ruchomych i skracają czas identyfikacji, co z kolei umożliwia dokonanie szybkiego uderzenia na wykryte, rozpoznane i nieustannie śledzone cele.

Trzecim elementem składowym sieci umożliwiającej prowadzenie walki sieciocentrycznej jest sieć dowodzenia. Nazwa polska nie jest dokładnym tłumaczeniem oryginału (Engagement Grid), oddaje jednak sens tej nazwy. Najogólniej mówiąc jest to sieć zapewniająca dowodzenie platformami bojowymi (grupami platform, oddziałami itd.) w przestrzeni walki. Sieć ta umożliwia wykorzystanie świadomości przestrzeni walki poprzez zapewnienie działającym siłom możliwości wykonania manewru, precyzyjnego uderzenia, pełnowymiarowej ochrony oraz ześrodkowania zasobów logistycznych w wymaganym miejscu i czasie.

W założeniach walki sieciocentrycznej przyjmuje się, że sieć dowodzenia jako jeden z głównych elementów architektury sieciocentrycznego pola walki powinna zapewnić:

- wyprzedzające planowanie, czyli zdolność przejęcia inicjatywy w celu uniknięcia bezpośredniej konfrontacji (poprzez zastosowanie środków alternatywnych). Umożliwiać ono powinno również właściwą reakcję i wykorzystanie nadarzających się korzystnych okoliczności, gdy bezpośrednia konfrontacja jest nieunikniona, a także przeprowadzenie działań koniecznych do tego, by własny cykl decyzyjny był krótszy niż cykl decyzyjny przeciwnika;
- zintegrowane kierowanie siłami, czyli możliwość osiągnięcia dynamicznej synchronizacji prowadzonych działań oraz wykorzystanie sił i środków z różnych komponentów oraz różnych źródeł (narodowych bądź koalicyjnych);
- możliwość prowadzenia działań w deficycie czasu, czyli zdolność do szybkiego poszukiwania, lokalizacji, identyfikacji i niszczenia celów w krótkim okresie czasu (np. celów mobilnych).

Dzięki posiadaniu wyżej wymienionych możliwości, które zapewnia sieć dowodzenia, siły prowadzące walkę sieciocentryczną będą mogły właściwie wykonywać wysoki poziom osiągniętej świadomości przestrzeni walki. W wyniku tego, sieć dowodzenia umożliwiać będzie:

- zmasowanie efektu działania platform bojowych rozproszonych geograficznie w przestrzeni kosmicznej i powietrznej, na lądzie i w wodzie, w najbardziej odpowiedni, dokładny i skuteczny sposób;
- prowadzenie działań w bardzo szybkim tempie;
- kształtowanie przestrzeni walki w pożądanym sposób;
- maksymalizację możliwości ogniowych własnych sił;
- uniemożliwienie realizacji wariantu działania wybranego przez przeciwnika.

Sieć dowodzenia może również znacznie zwiększyć możliwości bojowe własnych sił poprzez skrócenie czasu przydzielenia celów uderzenia wybranym platformom bojowym. Osiąga się to poprzez zastosowanie oprogramowania automatycznie przydzielającego cele platformom bojowym, przy pomocy specjalnych algorytmów. Dzięki zastosowaniu owych algorytmów szybko wypracowana zostaje optymalna decyzja przydzielenia celu w dynamicznie zmieniających się warunkach w przestrzeni walki (zmieniająca się liczba celów i ich priorytet, pozostałość środków rażenia na platformach bojowych, prawdopodobieństwo trafienia celu środkami rażenia, jakie pozostały do dyspozycji itd.). Należy zaznaczyć, że owe algorytmy nie powodują wyłączenia dowódcy z procesu decyzyjnego, a jedynie umożliwiają zawarcie całej wiedzy i intuicji dowódców i naukowców w oprogramowaniu, które umożliwia znaczne zwiększenie możliwości bojowych. Oprogramowanie w oparciu o opracowane algorytmy w krótkim czasie wypracowuje rekomendacje decyzji o przydzieleniu celu i proponuje je dowódcy do akceptacji.

W amerykańskich założeniach tworzenia i funkcjonowania sieciocentrycznej architektury pola walki zakłada się, że podobnie jak sieć czujników, sieć dowodzenia również może być stała lub tymczasowa. Analogicznie do sieci czujników, składać się ona może z peryferyjnych platform bojowych (shooter peripherals) i oprogramowania platform bojowych (shooter applications), które działają w oparciu o sieć informacyjną.

Peryferyjne platformy bojowe sieci dowodzenia mogą być rozmieszczone w przestrzeni kosmicznej, powietrznej, na lądzie, morzu oraz w przestrzeni informatycznej (cyberprzestrzeni). Oprogramowanie platform bojowych składać się będzie z części zapewniającej dowodzenie, oraz części umożliwiającej użycie uzbrojenia.

Z istoty walki sieciocentrycznej oraz dokonanych powyżej podziałów architektury sieciocentrycznego pola walki wynika, że kluczowym elementem analizowanej architektury są elementy umożliwiające spięcie całości sił i środków w sieć oraz przesyłanie, przetwarzanie, udostępnianie i przechowywanie informacji. Wśród kluczowych technologii (w tym także oprogramowania), które są (lub będą

w przyszłości) podstawą funkcjonowania architektury sieciocentrycznego pola walki można wymienić⁵¹:

- protokół internetowy, wersja 6 (Internet Protocol version 6 – IPv6) – kolejna generacja oprogramowania umożliwiającego komunikację między różnymi systemami i środkami komunikacji;
- uniwersalny system telefonii komórkowej (Universal Mobile Telephony System – UMTS) – trzecia generacja telefonii komórkowej, o znacznie rozbudowanych możliwościach;
- lokalna sieć bezprzewodowa (Wireless Local Area Network – WLAN) – umożliwiająca połączenie z siecią z dowolnego miejsca;
- komputerowy system zarządzania – narzędzie do zarządzania siecią;
- system zabezpieczenia informacji – zapewniający bezpieczeństwo informacji dystrybuowanych przez sieć;
- system syntezy informacji i danych – umożliwiający zebranie i połączenie informacji uzyskiwanych z różnych źródeł i platform, a następnie stworzenie jednolitego obrazu sytuacji, który usprawni i zwiększy efektywność dowodzenia;
- doraźne połączenia sieciowe – nowy sposób komunikacji między grupami użytkowników, nie wymagający infrastruktury technicznej i systemów zarządzających;
- sieć bezobsługowych sensorów naziemnych (Unmanned Ground Sensor Network – USGN) – przeznaczona do wykrywania i śledzenia celów naziemnych;
- technologie przyszłości – wszystkie technologie, które są w trakcie opracowywania (lub będą wynalezione), których zastosowanie może być użyteczne w walce sieciocentrycznej.

⁵¹ www.b2ncw.com/index.php

Analizowane wcześniej teoretyczne założenia w zakresie architektury sieciocentrycznego pola walki nie stanowią jedynego podejścia badawczego. Zastosowanie zasad walki sieciocentrycznej w działalności firm komercyjnych spowodowało, że architekturę pola walki zaczęto postrzegać szerzej, w aspekcie możliwych interakcji systemowych. W opublikowanych w maju 2004 r. w „Directions Magazine” artykule „Network Centric Warfare”, jego autor John Coleman⁵² przedstawia architekturę sieciocentrycznego pola walki jako zbiór systemów (podsystemów). Według zaproponowanego przez niego podziału, architekturę sieciocentrycznego środowiska działania tworzą następujące elementy⁵³:

- zintegrowana sieć wieloplatformowa (system);
- zabezpieczony przed ingerencją z zewnątrz system identyfikacji i zarządzania zasobami;
- system dystrybucji informacji geograficznych (Geographic Information System – GIS);
- zautomatyzowany system meldowania i zbierania informacji (w czasie rzeczywistym);
- zintegrowany system identyfikacji częstotliwości radiowych (Integrated Radio Frequency Identification Technology – RFID);
- system graficznego i dźwiękowego zobrazowania danych;
- zintegrowany system zarządzania i monitorowania zasobów;
- zintegrowany system planowania, stawiania zadań i śledzenia działań.

Z powyższych klasyfikacji wynika, że kluczowymi technologiami sieciocentrycznego środowiska działania, w tym sieciocentrycznego pola walki są technologie informatyczne związane z gromadzeniem, obróbką i dystrybucją informacji. Technologie stricte wojskowe (np. bezzałogowe – rozpoznawcze i uderzeniowe aparaty latające, wyspecjalizowane pojazdy, precyzyjne środki rażenia itd.), również są niezwykle ważną częścią sieciocentrycznego pola walki, jednakże jego

⁵² Były szef strategii rozwoju firmy Netscape.

⁵³ K. Coleman, *Network Centric Warfare*, op. cit.

„układem nerwowym” są właśnie urządzenia i systemy informatyczne, których rozwój w sektorze komercyjnym przebiega obecnie dynamiczniej niż w militarnym.

Zbliżone do amerykańskich założeń walki sieciocentrycznej rozwiązania w zakresie architektury sieciocentrycznego pola walki zawarte zostały w opracowaniu analitycznym Szwedzkiej Agencji Badań obronnych oraz europejskiego działu korporacji RAND „Network-Based Operations for the Swedish Defence Force: An Assessment Methodology” opublikowanym w czerwcu 2004 r. Wyniki badań zawarte w powyższym opracowaniu, wskazują, że walka sieciocentryczna, a w szerszym ujęciu użycie sił zbrojnych z wykorzystaniem wsparcia sieciocentrycznego mogą mieć miejsce w ramach: działań bojowych, działań w czasie pokoju, współpracy z instytucjami państwowymi oraz koalicyjnych operacji o charakterze niebojowym.

Podkreślić należy, iż implikacją przyjęcia takiej koncepcji funkcjonowania i użycia Szwedzkich Sił Zbrojnych jest funkcjonowanie sieciocentrycznej architektury już w czasie pokoju. Szwedzkie założenia tworzenia sieci operacyjnej (Operational Network) postulują połączenia w jej ramach nie tylko sił wojskowych, ale również instytucji rządowych, organizacji pomocy humanitarnej oraz sił sojuszniczych lub koalicyjnych. Zakres dostępu poszczególnych uczestników działań prowadzonych w oparciu o sieć operacyjną do danych funkcji czy aplikacji ma być zróżnicowany, w zależności od przewidywanych do realizacji funkcji. W szwedzkich koncepcjach przyjmuje się, że sieć operacyjna ze względu na zakres dostępu, stopień bezpieczeństwa oraz ważność i terminowość zawartych w niej danych i informacji może być postrzegana jako system czterech wyspecjalizowanych sieci (rys. 2.5)⁵⁴:

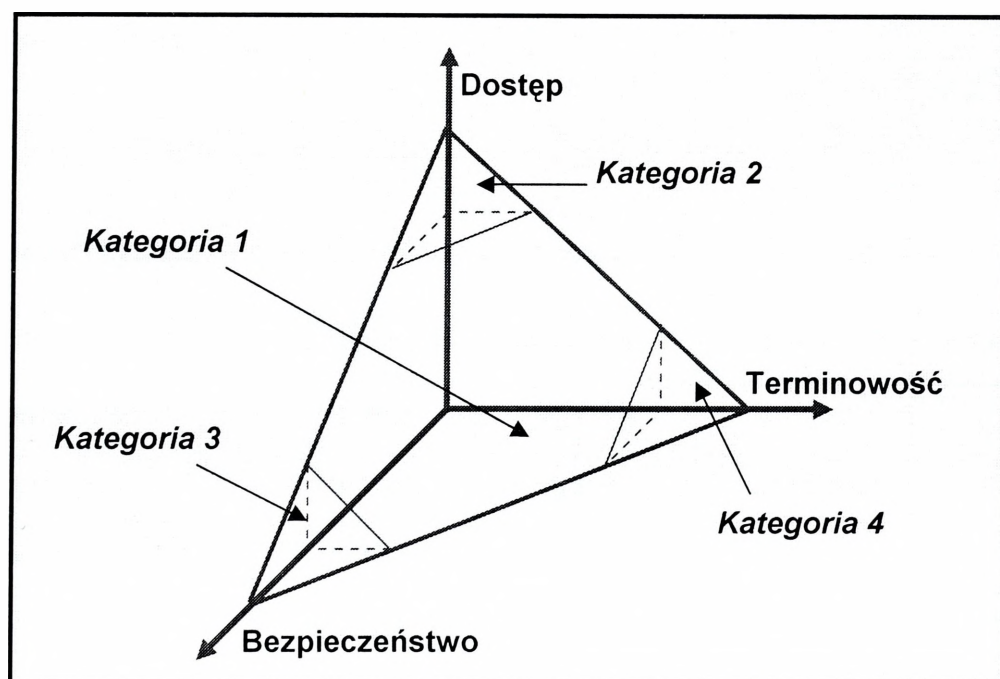
- sieci interakcji wyspecjalizowanych (specialised interaction) określanych jako Kategoria 1;
- sieci interakcji szerokiego dostępu (ubiquitous interaction) – Kategoria 2;
- sieci interakcji utajnionych (secure interaction) – Kategoria 3;

⁵⁴ *Network-Based Operations for The Swedish Defence Forces*, op. cit., s. 21-22.

- sieci interakcji w czasie rzeczywistym (real-time interaction) – Kategoria 4.

W **sieci interakcji wyspecjalizowanych** wymagania i uprawnienia w zakresie dostępu do informacji są różne dla poszczególnych użytkowników. Poziom dostępu, terminowości i bezpieczeństwa w sieci tej kategorii definiowany jest na poziomie od średniego do niskiego.

Sieć interakcji szerokiego dostępu łączy dużą liczbę użytkowników i cechuje się zbliżonym poziomem uprawnień dostępu do danych i informacji na temat wszystkich aspektów prowadzonych działań dla większości połączonych w sieci użytkowników.



Źródło: opracowanie własne na podstawie: *Network-Based Operations for the Swedish Defence Forces*, op. cit., s. 23.

Rys. 2.5. Kategorie interakcji w sieci operacyjnej

W przypadku **sieci interakcji utajnionych** głównym wymaganiem będzie zachowanie bezpieczeństwa fizycznego i informacyjnego, zarówno samej sieci, jak i informacji w niej.

Sieć interakcji w czasie rzeczywistym obejmować będzie wąską grupę użytkowników, którzy potrzebować będą dostępu do krytycznie ważnych danych w czasie rzeczywistym oraz posiadać zdolność przekazywania powyższych da-

nych innym uczestnikom, nawet w warunkach przerzucania części połączeń i wyeliminowaniu węzłów sieci operacyjnej.

Identyfikacja czterech kategorii interakcji w szwedzkiej koncepcji tworzenia sieciocentrycznego pola walki nie przekłada się bezpośrednio na tworzenie fizycznie istniejących sieci identycznych z powyższymi kategoriami. Powyższa typologia pozwala na analizę charakteru interakcji występujących w poszczególnych domenach i sieciach pola walki, a poprzez to na optymalizację ich konfiguracji. Architektura sieciocentrycznego pola walki, w tym charakter sieci składowych w ramach sieci operacyjnej, determinować będą dobór kategorii interakcji w zależności od funkcji operacyjnych. Za punkt wyjściowy do przyjmowania konkretnych rozwiązań, w szwedzkiej koncepcji, przyjęto czynniki charakteryzujące poszczególne kategorie interakcji. Dane przedstawiono w tab. 1.

Tabela 1

Czynniki charakteryzujące poszczególne kategorie interakcji w sieci operacyjnej

Czynnik	Kategoria 1	Kategoria 2	Kategoria 3	Kategoria 4
Intensywność	średnia	wysoka	średnia	niska
Pojemność	średnia	wysoka	średnia	niska
Zakres informacji	średni	wysoki	średni	niski
Zasięg sieci	średni	wysoki	niski	niski
Monitorowanie informacji	średnie	niskie	wysokie	wysokie
Żywotność sieci	średnia	niska	wysoka	Wysoka
Bezpieczeństwo informacji	średnie	niskie	wysokie	średnie
Terminowość informacji	średnia	niska	średnia	wysoka

Źródło: opracowanie własne na podstawie: *Network-Based Operations for the Swedish Defence Forces*, op. cit., s. 36.

W szwedzkich założeniach koncepcyjnych w zakresie tworzenia architektury sieciocentrycznej na potrzeby operacji wojskowych prowadzonych w oparciu o rozwiązania sieciowe za sieć uznaje się w najbardziej ogólnym ujęciu zbiór węzłów połączonych ze sobą w różny sposób.

W architekturze sieciocentrycznego pola walki wyróżniane są dwie zasadnicze sieci⁵⁵:

- sieć informacyjna;
- sieć operacyjna.

Sieć informacyjna utożsamiana jest z infrastrukturą walki sieciocentrycznej. Dzięki sieci informacyjnej możliwe jest przesyłanie i przechowywanie danych, dostęp do nich, a także utrzymywanie łączności wewnątrz sił prowadzących operacje sieciocentryczne oraz z organizacjami zewnętrznymi. W studium „Network – Based Operations for The Swedish Defence Force” sieć informacyjna definiowana jest jako rodzaj sieci potrzebnej do zabezpieczenia operacji wojskowych tworzonej przez zbiór węzłów operacyjnych, łączności, zbioru (pozyskiwania) danych (senso-rów) oraz przetwarzania danych zdolnych do komunikowania się między sobą za pomocą określonego sposobu łączności.

Architektura sieci informacyjnej proponowana w rozwiązaniach szwedzkich identyfikuje następujące elementy składowe tej sieci⁵⁶:

- środki pozyskiwania danych (sensors);
- ośrodki korelacji (fuzji) pozyskiwanych danych (fusion centres);
- terminale użytkowników (terminal facilities);
- elementy zabezpieczające przechowywanie danych (data storage);
- systemy przekaźnikowe łączności (communications relay facilities);
- systemy kontroli sieci (network controllers);
- systemy transmisji łączności (communications transmission facilities).

Przeznaczone do zbioru informacji zabezpieczającej podejmowanie decyzji w trakcie działań prowadzonych na sieciocentrycznym polu walki środki pozyskiwania danych (sensory) sieci informacyjnej składają się z następujących elementów składowych:

⁵⁵ *Revolution in Military Affairs – the Swedish Programme*, w: *Swedish Journal of Military Technology*, Vol. 3, 2000, s. 6.

⁵⁶ *Network-Based Operations for the Swedish Defence Force*, op. cit., s. 9.

- urządzeń pozyskiwania danych (sensor equipment);
- platform, na których są umieszczone urządzenia pozyskiwania danych (platform);
- oprogramowania do obróbki pozyskiwanych danych (processing code – software);
- urządzeń łączności (communications equipment).

Przyjęcie takiej dekompozycji środków pozyskiwania danych (sensorów) sieci informacyjnej powoduje, że na potrzeby architektury sieciocentrycznego pola walki jako sensory postrzegane mogą być nie tylko techniczne środki rozpoznania, ale także osobowe źródła informacji oraz rozpoznania (HUMINT). Sensory dostarczają informacji do sieci w formie nieprzetworzonych bądź przetworzonych danych.

Ośrodki korelacji (fuzji) pozyskiwanych danych (fusion centres) pełną w sieci informacyjnej rolę integratorów danych dostarczanych przez zróżnicowane sensory i źródła informacji w spójne, wspólne zobrazowanie sytuacji na polu walki (common picture of the battlespace). Ośrodki korelacji sieci informacyjnej obejmują, zgodnie z szwedzkimi założeniami tworzenia architektury sieciocentrycznego pola walki, następujące elementy składowe⁵⁷:

- urządzenia zobrazowania danych terminali użytkowników (terminal display equipment);
- narzędzia wspomagania podejmowania decyzji (decision support tools);
- analityków danych pozyskiwanych przez sensory (exploitation analysts);
- systemy przechowywania i wyszukiwania danych (data storage and retrieval);
- oprogramowanie (algorytmy) korelacji (fuzji) danych (fusion algorithms);
- urządzenia łączności (communications equipment).

⁵⁷ Tamże.

Terminale użytkowników sieci informacyjnej zabezpieczają ich funkcjonowanie na sieciocentrycznym polu walki poprzez zapewnienie im niezbędnej łączności oraz zobrazowania sytuacji. W szwedzkiej koncepcji architektury sieciocentrycznego pola walki terminale użytkowników sieci informacyjnej dekomponowane są na następujące elementy składowe:

- urządzenia zobrazowania danych terminali;
- urządzenia wspomagania podejmowania decyzji;
- urządzenia współpracy (współdziałania) z innymi użytkownikami sieci (network collaboration tools);
- systemy przechowywania i wyszukiwania danych;
- personel zabezpieczający funkcjonowanie terminali użytkowników;
- urządzenia łączności.

Systemy przekaźnikowe łączności wyodrębnione w szwedzkiej koncepcji architektury sieciocentrycznego pola walki definiowane są jako węzły łączności przeznaczone wyłącznie do przekazywania łączności pomiędzy terminalami użytkowników lub innymi węzłami przekaźnikowymi. W skład systemów przekaźnikowych łączności sieci informacyjnej zaliczane są⁵⁸:

- urządzenia przekaźnikowe łączności (communications relay equipment);
- oprogramowanie sterowania połączeniami (switching software);
- personel zabezpieczający;
- urządzenia łączności.

Ważnym elementem sieci informacyjnej w szwedzkiej koncepcji sieciocentrycznego pola walki są systemy kontroli sieci. Jako systemy kontroli rozumiane są urządzenia lub osoby zarządzające funkcjonowaniem sieci, posiadające uprawnienia do ograniczania jej użycia oraz zmiany uprawnień dla wykorzystania jej zasobów. Systemy kontroli sieci obejmują:

⁵⁸ Tamże.

- wyposażenie ośrodków kontroli (control centre equipment);
- personel zabezpieczający;
- oprogramowanie monitorujące funkcjonowanie sieci (monitoring software);
- narzędzia przydzielania zasobów sieci (resource – allocation tools);
- urządzenia łączności.

Systemy transmisji łączności wchodzące w skład sieci informacyjnej tworzą media transmisji danych wykorzystywane do łączenia terminali użytkowników oraz węzłów przekaźnikowych. W ich skład wchodzi media transmisji danych (UHF, HF, itp.), personel zabezpieczający oraz urządzenia łączności.

Architektura **sieci operacyjnej** zgodnie z założeniami szwedzkiej koncepcji operacji sieciocentrycznych obejmuje połączenia logiczne pomiędzy uczestnikami walki (rys. 2.6). Generyczna architektura sieci operacyjnej obejmuje⁵⁹:

- użytkowników (subscribers);
- podsieci (subnetworks);
- wirtualne zespoły współdziałania (virtual collaboration teams);
- kontrolerów sieci (network controllers).

Sieć operacyjna funkcjonuje w oparciu o fizycznie istniejącą sieć informacyjną. Ułatwia podejmowanie decyzji poprzez zapewnienie dostępu do informacji dla decydentów oraz wykorzystanie przez nich narzędzi wspierających proces decyzyjny. Sieć operacyjna umożliwia, po podjęciu decyzji, dystrybucję informacji o tym, kontrolę sił realizujących zadania oraz synchronizację ich użycia.

Użytkownicy sieci operacyjnej tworzą węzły użytkowników (subscriber nodes) zaangażowanych w realizację określonej funkcji operacyjnej⁶⁰. Użytkownicy wyposażeni są w środki umożliwiające im włączenie do sieci w celu wymiany informacji związanej z realizowaną funkcją.

⁵⁹ Tamże, s. 11.

⁶⁰ Funkcja operacyjna postrzegana jest w sposób analogiczny do zadania operacyjnego, np. zapewnienie obrony powietrznej.

- wyposażenie ośrodków kontroli (control centre equipment);
- personel zabezpieczający;
- oprogramowanie monitorujące funkcjonowanie sieci (monitoring software);
- narzędzia przydzielania zasobów sieci (resource – allocation tools);
- urządzenia łączności.

Systemy transmisji łączności wchodzące w skład sieci informacyjnej tworzą media transmisji danych wykorzystywane do łączenia terminali użytkowników oraz węzłów przekaźnikowych. W ich skład wchodzi media transmisji danych (UHF, HF, itp.), personel zabezpieczający oraz urządzenia łączności.

Architektura **sieci operacyjnej** zgodnie z założeniami szwedzkiej koncepcji operacji sieciocentrycznych obejmuje połączenia logiczne pomiędzy uczestnikami walki (rys. 2.6). Generyczna architektura sieci operacyjnej obejmuje⁵⁹:

- użytkowników (subscribers);
- podsieci (subnetworks);
- wirtualne zespoły współdziałania (virtual collaboration teams);
- kontrolerów sieci (network controllers).

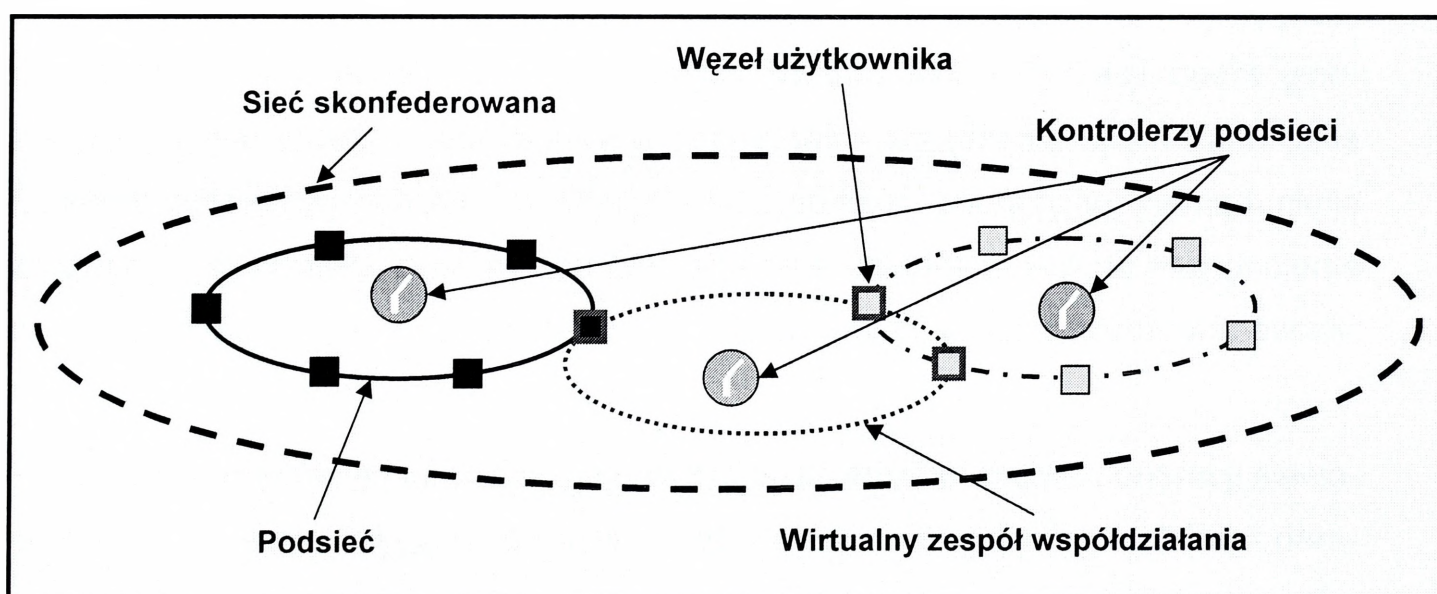
Sieć operacyjna funkcjonuje w oparciu o fizycznie istniejącą sieć informacyjną. Ułatwia podejmowanie decyzji poprzez zapewnienie dostępu do informacji dla decydentów oraz wykorzystanie przez nich narzędzi wspierających proces decyzyjny. Sieć operacyjna umożliwia, po podjęciu decyzji, dystrybucję informacji o tym, kontrolę sił realizujących zadania oraz synchronizacją ich użycia.

Użytkownicy sieci operacyjnej tworzą węzły użytkowników (subscriber nodes) zaangażowanych w realizację określonej funkcji operacyjnej⁶⁰. Użytkownicy wyposażeni są w środki umożliwiające im włączenie do sieci w celu wymiany informacji związanej z realizowaną funkcją.

⁵⁹ Tamże, s. 11.

⁶⁰ Funkcja operacyjna postrzegana jest w sposób analogiczny do zadania operacyjnego, np. zapewnienie obrony powietrznej.

Podsieci (subnetworks) w ramach sieci operacyjnej rozumiane są jako ściśle powiązane ze sobą techniczne środki dowodzenia, przetwarzania danych, rozpoznania i łączności oraz użytkownicy (a tightly linked set of Command and Control, Communications, Computing, Intelligence, Surveillance and Reconnaissance equipment and subscribers) wykorzystujący wspólne wyposażenie i oprogramowanie oraz przeznaczony w sposób ciągły do realizacji określonej funkcji operacyjnej. Podsieci są zazwyczaj łączone w sposób hierarchiczny albo w ramach horyzontalnych sieci rozległych (distributed network). Przykładem podsieci w ramach sieci operacyjnej mogą być sieci tworzone na potrzeby zabezpieczenia logistycznego lub stałe, permanentnie funkcjonujące, sieci dowodzenia. Podsieci tworzone dla realizacji określonej funkcji operacyjnej zazwyczaj funkcjonują w ramach szerokiej skonfederowanej (wspólnie działającej) sieci⁶¹.



Źródło: opracowanie własne na podstawie: *Network-Based Operations for the Swedish Defence Force*, op. cit., s. 11.

Rys. 2.6. Ogólna architektura sieci operacyjnej

Sieć skonfederowana (federated network) identyfikowana w ramach sieci operacyjnej tworzona jest przez komplet technicznych środków dowodzenia, łączności i rozpoznania wykorzystywanych przez wszystkich uczestników walki sieciocentrycznej (nie tylko siły zbrojne) zaangażowanych w realizację określonej funkcji operacyjnej. Sieć skonfederowana może składać się z podsieci cywilnych i wojskowych, narodowych, sojuszniczych lub koalicyjnych. Przykładem sieci skonfede-

⁶¹ *Revolution in Military affairs – the Swedish Programme*, op. cit., s. 7-9

rowanej może być amerykańska globalna sieć informacyjna (US Global Information Grid – GIG).

Wirtualne zespoły współdziałania w ramach sieci operacyjnej definiowane są w szwedzkiej koncepcji architektury sieciocentrycznego pola walki jako doraźnie tworzone połączenia użytkowników i technicznych środków dowodzenia na potrzeby realizacji określonego zadania w ramach zdefiniowanej funkcji operacyjnej. Przykładem zespołu wirtualnego tworzonego doraźnie w ramach sieci operacyjnej może być komórka targetingu dynamicznego łącząca sensory, źródła rozpoznawcze oraz personel kierowania wsparciem ogniowym. Cechą charakterystyczną zespołów wirtualnych jest to, że składają się one często z węzłów użytkowników pochodzących z różnych podsieci (subnetworks).

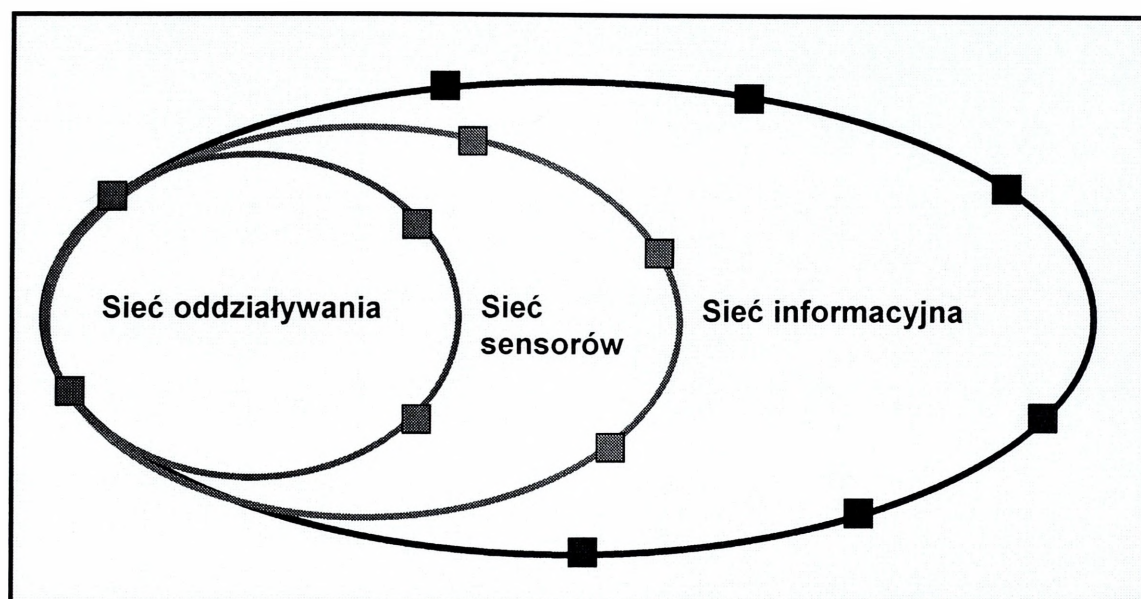
Kontrolerzy sieci operacyjnej są odpowiedzialni za jej monitorowanie i kontrolowanie podsieci lub zespołów wirtualnych oraz zarządzanie nimi w przypadku zmian w środowisku prowadzonych działań lub w sytuacji operacyjno-taktycznej. Kontrolerzy sieci (zarówno osoby, jak i urządzenia spełniające takie funkcje), egzekwujących zasady korzystania z podsieci operacyjnej pełnią funkcje zbliżone do kontrolera sieci, ale ich działanie ukierunkowane jest na zaspokojenie wymagań związanych z realizacją funkcji operacyjnych, a nie z fizycznymi aspektami funkcjonowania sieci informacyjnej.

Sieć informacyjna i operacyjna tworzą w szwedzkim modelu operacji sieciocentrycznych bazę fizyczną (swoistą infrastrukturę) prowadzenia walki w operacjach opartych o założenia sieciocentryczne. Model koncepcyjny architektury sieciocentrycznego pola walki przyjęty w rozwiązaniach szwedzkich zakładała istnienie w ramach sieci trzech siatek: informacyjnej (information grid), środków zdobywania danych (sensor grid) oraz oddziaływania (engagement grid)⁶².

Wzajemne zależności poszczególnych siatek sieci przedstawione są w szwedzkiej koncepcji operacji sieciocentrycznych w dwa różne sposoby. Najczęściej stosowany model koncepcyjny sieciocentrycznego pola walki zakłada, że siatka oddziaływania jest podsiecią siatki sensorów, a ta z kolei stanowi podsieć w ramach siatki informacyjnej (rys. 2.7). Siatki sensorów, informacyjna i oddziaływania mogą być w modelu koncepcyjnym sieciocentrycznej architektury pola walki

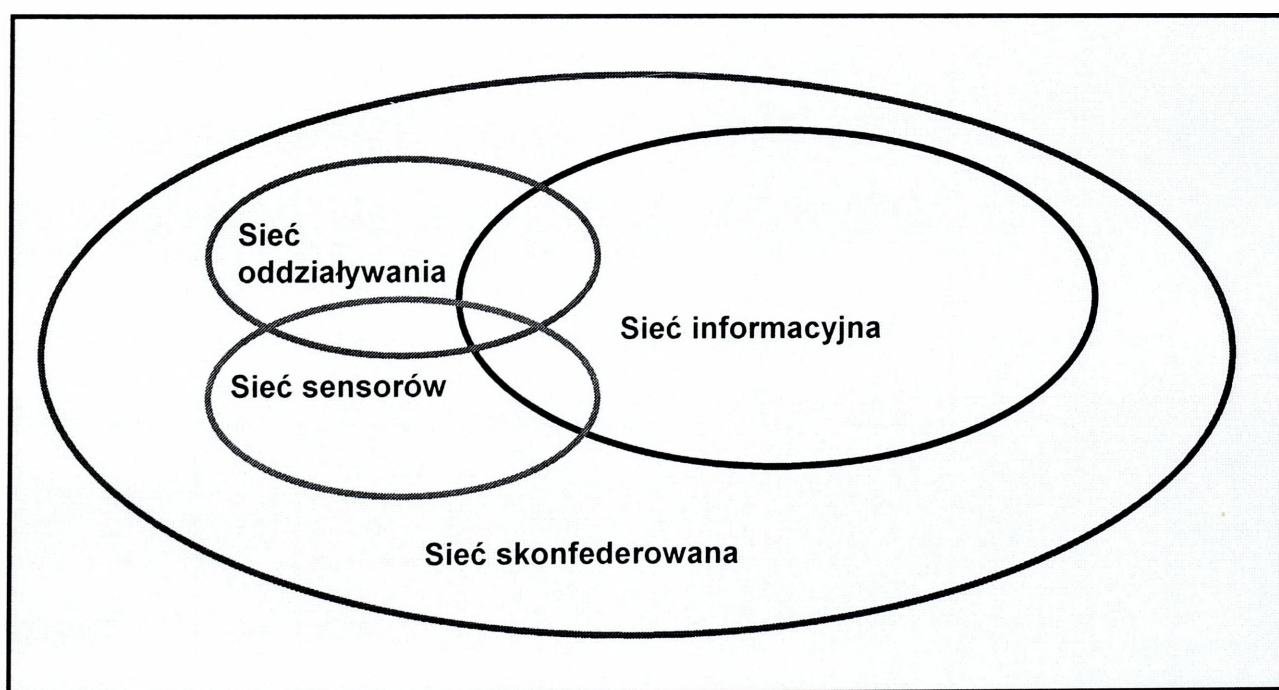
⁶² Tamże, s. 13-14.

postrzegane również jako nakładające się częściowo podsieci w ramach jednej wspólnej sieci skonfederowanej (rys. 2.8)⁶³.



Źródło: opracowanie własne na podstawie: *Revolution in Military affairs – the Swedish Programme*, op. cit., s. 12.

Rys. 2.7. Model sieci współzależnej



Źródło: opracowanie własne na podstawie: *Revolution in Military affairs – the Swedish Programme*, op. cit., s. 12.

Rys. 2.8. Model sieci skonfederowanej

⁶³ Tamże.

Zgodnie z szwedzkimi koncepcjami tworzenia architektury sieciocentrycznego pola walki siatka informacyjna zapewnia infrastrukturę dla „odbioru, przetwarzania, przesyłania oraz ochrony informacji na potrzeby sił połączonych oraz wielonarodowych”. Rozległość siatki informacyjnej oraz jej struktura determinują zdolność sił do działania na sieciocentrycznym polu walki.

Siatka sensorów jest siecią, która wykorzystuje te sensory w siatce informacyjnej, które są potrzebne do realizacji danej funkcji operacyjnej. Siatka sensorów pozwala na generowanie wysokiego poziomu świadomości uczestników operacji w zakresie sytuacji na polu walki (battlespace awareness) poprzez współposiadanie przez nich danych i informacji oraz ich korelację (fuzję). Siatka sensorów przyczynia się również do skutecznej oddolnej synchronizacji użycia sił⁶⁴.

W szwedzkich założeniach tworzenia architektury sieciocentrycznego pola walki siatka sensorów nie jest utożsamiana wyłącznie z tradycyjnymi technicznymi środkami rozpoznania. Sensor identyfikowany jako środek pozyskiwania danych może stanowić urządzenie techniczne i programy komputerowe monitorujące przemieszczanie wojsk własnych albo funkcjonowanie zabezpieczenia logistycznego⁶⁵. Siatka sensorów konfigurowana ma być adekwatnie do potrzeb prowadzonych operacji. Implikacją przyjęcia takiego założenia będzie każdorazowa harmonizacja wielkości obszaru pokrycia sensorów z obszarem operacji, optymalizacja rodzaju technicznych środków rozpoznania do przewidywanych obiektów działań oraz redundancja siatki sensorów adekwatna do jej żywotności rozpatrywanej w aspekcie przewidywanych warunków działań. Wyraźnie artykułowana w szwedzkich założeniach walki sieciocentrycznej jest filozofia dostosowania charakteru siatki sensorów do konkretnej funkcji operacyjnej, na potrzeby której ma być tworzona. Podkreśla się również znaczenie dostosowania konfiguracji siatki informacyjnej do architektury siatki sensorów, tak aby możliwy był niezakłócony zbiór, przetwarzanie oraz dystrybucja informacji o sytuacji na polu walki w sposób zapewniający sprawną realizację zadań.

⁶⁴ Dostrzegalna jest tu zbieżność z założeniami amerykańskimi w odniesieniu do samosynchronizacji sił (self-synchronization).

⁶⁵ Tamże, s. 14.

Siatka oddziaływania, określana także jako siatka łącząca podejmującego decyzję z wykonawcą (The Engagement – Decision – Shooter Grid) jest strukturą, która może się dynamicznie zmieniać. Ze względu na rodzaj funkcji operacyjnej, na potrzeby której tworzona będzie siatka oddziaływania, będą integrowane w jej ramach określone elementy (węzły) siatki sensorów oraz siatki informacyjnej. Istotne znaczenie dla skuteczności użycia sił wojskowych prowadzących działania bojowe zgodnie z założeniami walki sieciocentrycznej będzie mieć zdolność zabezpieczenia przez architekturę sieciocentryczną doraźnego, dynamicznego tworzenia siatek oddziaływania na każdym ze szczebli prowadzenia działań (taktycznym, operacyjnym i strategicznym). Spełnienie powyższego postulatu zabezpieczy zarówno scentralizowane, jak i zdecentralizowane podejmowanie decyzji oraz użycia systemów oddziaływania (czy w węższym ujęciu systemów rażenia ognio-
wego i elektronicznego).

Przedstawione założenia teoretyczne w zakresie architektury sieciocentrycznego pola walki wskazują na to, że architektura taka istnieje w każdej z domen prowadzenia walki sieciocentrycznej. Podstawowym warunkiem użycia sił wojskowych zgodnie z założeniami sieciocentrycznymi jest istnienie fizycznej infrastruktury informacyjnej zapewniającej połączenie we wspólnej sieci decydentów, wykonawców oraz środków zdobywania informacji. Wspólną cechą analizowanych rozwiązań w zakresie tworzenia architektury sieciocentrycznego pola walki jest jej otwartość oraz podatność na kształtowanie w zależności od potrzeb prowadzonych operacji. Podkreślenia wymaga też fakt występowania we wszystkich koncepcjach architektury sieciocentrycznego pola walki systemów zarządzania siecią. Pomimo wielości i różnorodności połączeń i relacji uczestników walki sieciocentrycznej, takie rozwiązanie hierarchizuje przepływ informacji i normuje zakres wykorzystania zasobów sieciowych.

2.2. Sposób funkcjonowania sieciocentrycznego pola walki

Jednym z głównych elementów koncepcji użycia sił wojskowych na sieciocentrycznym polu walki jest próba odpowiedzi na pytanie, w jaki sposób funkcjonują i działają sieciocentrycznie zorganizowane i wykorzystywane zgrupowania operacyjne i taktyczne. Poszukiwanie odpowiedzi na tak sformułowane pytanie pro-

wadzi do prób wyjaśnienia podstawowych różnic pomiędzy działaniami sieciocentrycznymi i platformocentrycznymi oraz określenia źródeł przewagi w operacjach sieciocentrycznych. Wyniki uzyskanych badań w tym zakresie zostały zawarte w niniejszym podrozdziale.

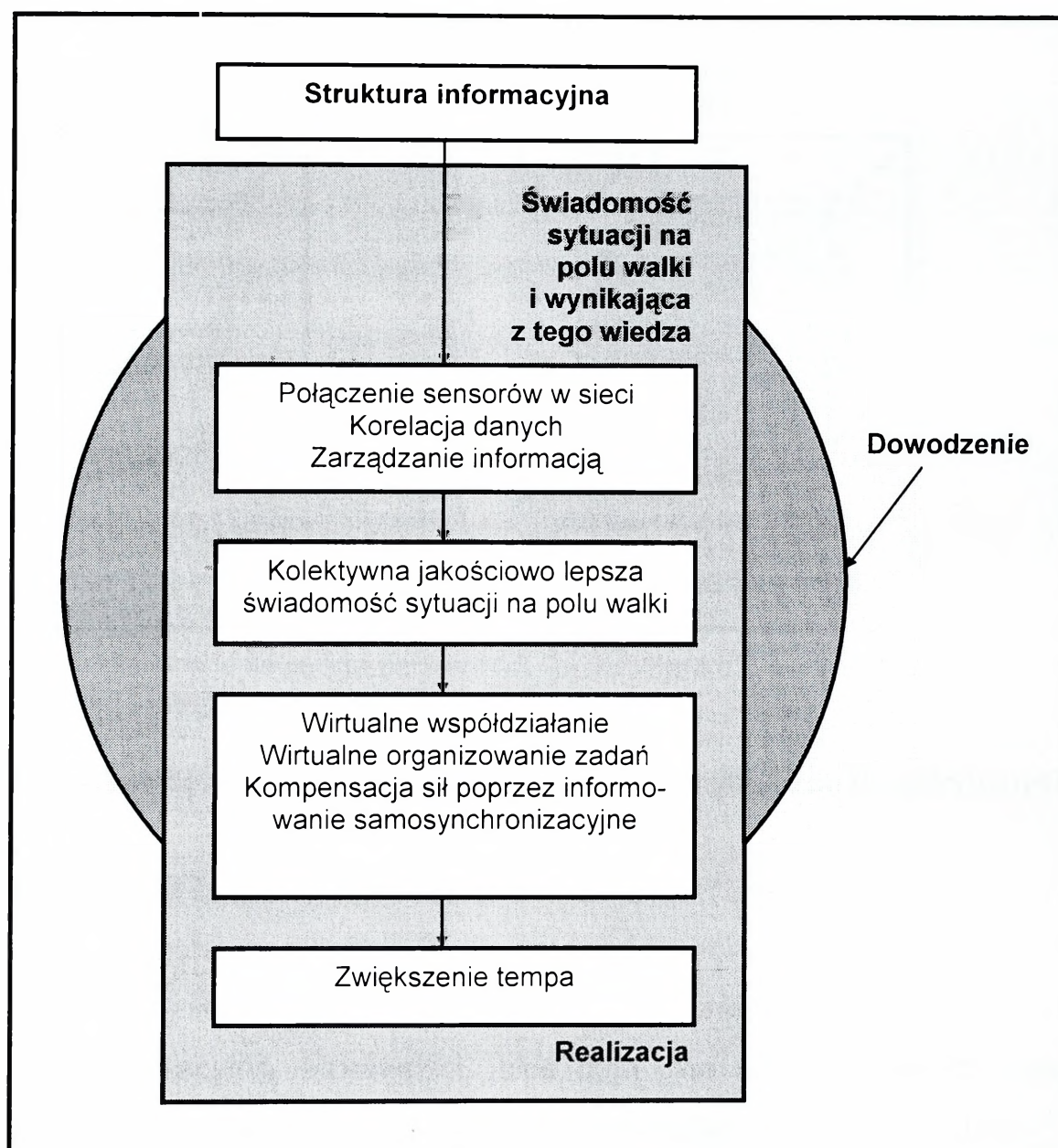
Ogólna koncepcja użycia sił według założeń walki sieciocentrycznej zakłada, że wyższa jakość sieciowego połączenia wojsk i związana z tym poprawa wymiany informacji, wpłynie na zdynamizowanie dowodzenia, a w tym konsekwencji na skuteczniejsze użycie sił na polu walki. W początkowym okresie rozwoju teorii walki sieciocentrycznej, w 1999 r. przyjęto ogólny algorytm zależności determinujących prowadzenie tej walki.

Struktura informacyjna postrzegana jako koszt osiągnięcia zdolności do prowadzenia działań sieciocentrycznych (tzw. „the entry fee”) umożliwić miało proces generowania świadomości sytuacji na polu walki poprzez łączenie w sieć poszczególnych sensorów, korelacji (fuzji) pozyskiwanych danych oraz zarządzanie posiadaną informacją.

Wygenerowana w ten sposób jakościowo lepsza w stosunku do tradycyjnych rozwiązań platformocentrycznych wspólna dla całości sił świadomość sytuacji na polu walki (Vastly Improved Shared Awareness) tworzyła warunki do jej wykorzystania w działaniach bojowych. Proces wykorzystania powyższej wspólnej świadomości sytuacji na polu walki osiągnąć miał być, według założeń z 1999 r. w formie wirtualnego współdziałania (Virtual Collaboration), wykorzystania wirtualnych organizacji zadaniowych (Virtual Organization), kompensowania informacji sił (ludzi i sprzętu) na polu walki (Substitution of Info for People and Material) oraz oddolnej samosynchronizacji wojsk (self-synchronization)⁶⁶.

W rezultacie tego procesu ma ulec zwiększeniu tempo działań (increased tempo) oraz zdolność reagowania na zmiany w sytuacji (increased responsiveness). Jednocześnie zmniejszać się ma ryzyko użycia sił wojskowych (lower risk) oraz koszty (lower costs), co w konsekwencji zwiększać będzie ekonomiczność działań bojowych tworząc „większe zyski” (higher profits) (rys. 2.9).

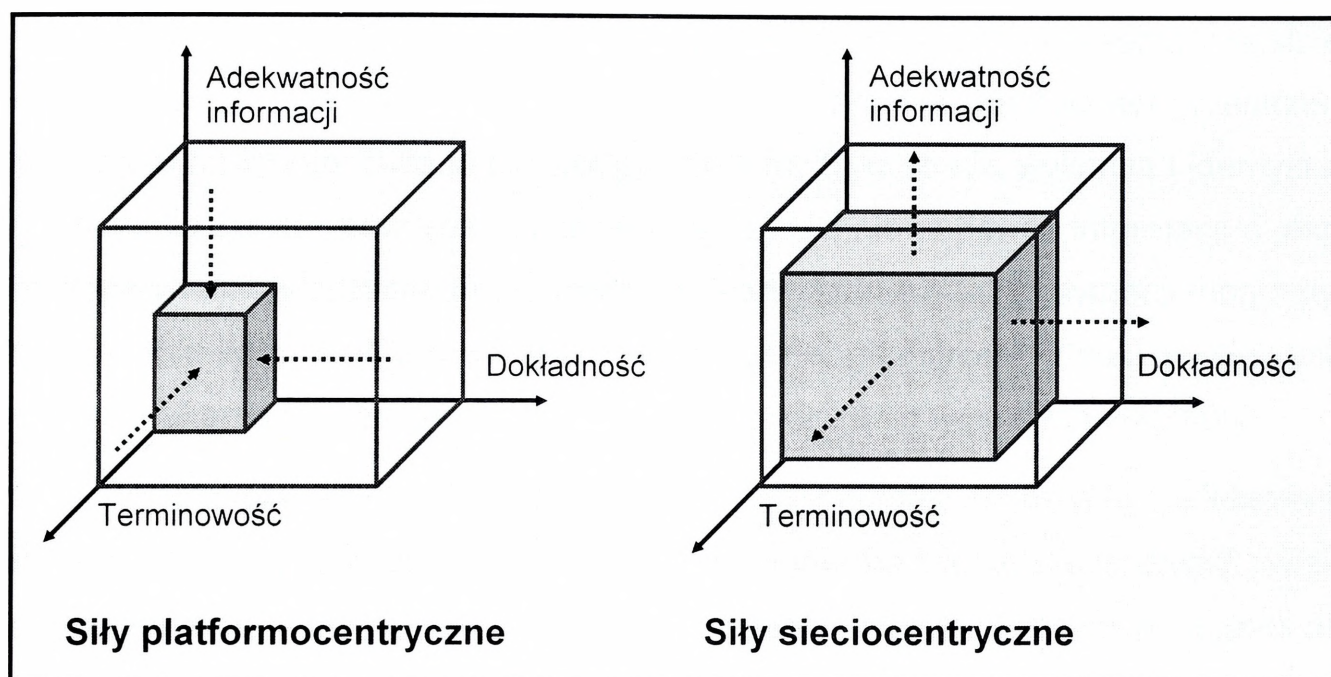
⁶⁶ *Network Centric Warfare: Developing and Leveraging Information Superiority*, op. cit., s. 88.



Źródło: opracowanie własne na podstawie: *Network Centric Warfare: Developing and Leveraging Information Superiority*, op. cit., s. 89.

Rys. 2.9. Zależności między czynnikami walki sieciocentrycznej

Obrazowo przedstawione porównanie skuteczności użycia sił sieciocentrycznych i platformocentrycznych poprzez pryzmat posiadania przewagi informacyjnej zostało zwarte w opracowaniu teoretycznym kładącym podwaliny założeń walki sieciocentrycznej „*Network Centric Warfare: Developing and Leveraging Information Superiority*” z 1999 r. Poprzez porównanie stopnia terminowości, dokładności oraz adekwatności (do potrzeb) posiadanej informacji porównano graficznie zakres swobody użycia sił sieciocentrycznych i platformocentrycznych. Na rys. 2.10 wyraźnie widoczny jest malejący wraz z stopniem dokładności, adekwatności i terminowości informacji zakres swobody użycia sił, a w konsekwencji ich zdolności operacyjnej.



Źródło: opracowanie własne na podstawie: *Network Centric Warfare: Developing and Leveraging Information Superiority*, op. cit., s. 56.

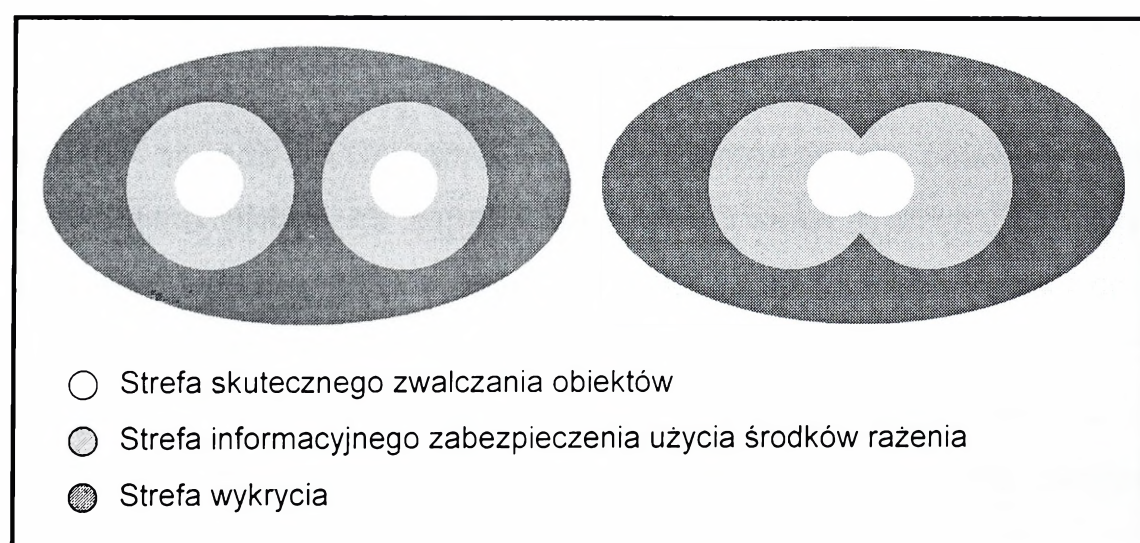
Rys. 2.10. Skuteczność użycia sił platformocentrycznych i sieciocentrycznych

Na poziomie strukturalnym, funkcjonowanie sieciocentrycznego pola walki umożliwiają trzy elementy składające się na całość sieci łączącej siły prowadzące działania: sieć czujników oraz sieć dowodzenia rozwinięte w oparciu o wysokiej jakości sieć informacyjną. Możliwości, jakie dają owe sieci są wykorzystywane i poszerzane dzięki stosowaniu odpowiednich procedur dowodzenia, których automatyzacja umożliwia osiągnięcie znacznego tempa prowadzenia działań.

Dysponowanie siecią wymiany informacji w czasie rzeczywistym umożliwia oddzielenie sensorów od platform bojowych. Pozwala bowiem na stworzenie ciągłego pola informacyjnego – jednolitego obrazu sytuacji taktycznej, który może być wykorzystywany przez każdą platformę bojową dysponującą odpowiednim urządzeniem odbiorczym i będącą w zasięgu nadajników emitujących ów jednolity obraz sytuacji taktycznej. Aby zilustrować istotę obrazu informacji taktycznej, można posłużyć się przykładem RAP (Recognized Air Picture), czyli jednolitym obrazem sytuacji powietrznej. Podczas gdy RAP ukazuje sytuację powietrzną (opierając się na informacjach zdobytych przez wiele środków rozpoznawczych), jednolity obraz sytuacji taktycznej będzie ukazywał kompletną sytuację taktyczną na lądzie, w powietrzu, na powierzchni wody i w jej głębinach. Podobnie jak w przypadku jednolitego obrazu sytuacji powietrznej, do utworzenia owego obrazu wykorzystywane będą informacje zdobyte przez całe spektrum środków rozpoznawczych.

W przypadku działań platformocentrycznych, połączenie sensora z nosicielem środka rażenia powodowało niepełne wykorzystanie możliwości przestrzennych środka rażenia. Było to spowodowane tym, że w strefie wykrycia i identyfikacji obiektów sensor powiązany z platformą bojową nie zapewnił informacji o jakości zapewniającej zużycie środka rażenia. Rozwiązaniem takiej sytuacji mogło być zwiększenie ilości platform bojowych w określonej przestrzeni w celu zwiększenia strefy uzyskania informacji zabezpieczającej zwalczanie wykrytych obiektów.

W przypadku oddzielenia sensorów od platform bojowych, zwiększenie wielkości strefy skutecznego zwalczania obiektów będzie możliwe dzięki zwiększeniu ilości sensorów oraz połączeniu ich w sieć. Jakość informacji dostępnej dla platformy bojowej rosnąć będzie też poprzez korelację zewnętrznej informacji z danymi uzyskiwanymi przez sensory platformy. W wyniku przyjęcia rozwiązań sieciocentrycznych wzrosną zatem zarówno wskaźniki przestrzenne, jak i skuteczności bojowej w trakcie realizacji zadań bojowych (rys. 2.11).



Źródło: opracowanie własne na podstawie: *Network Centric Warfare: Developing and Leveraging Information Superiority*, op. cit., s. 102.

Rys. 2.11. Relacje zachodzące między sensorem a platformą bojową

Posiadając dostęp do takiego jednolitego obrazu sytuacji taktycznej, platformy bojowe mogą skrycie podejść do celu i użyć uzbrojenia na maksymalnej odległości od celu, ograniczonej tylko zasięgiem środka ogniowego. Ponadto, rezygnacja z sensorów pokładowych pozwala na zwiększenie udźwigu, a co za tym idzie, rozszerzenie możliwości uderzeniowych platform bojowych. Pełne ostrzeżenie o aktywności przeciwnika pozwala również na odpowiednio wczesną reakcję

na zagrożenie, dając załogom platform komfort psychiczny pozwalający na skoncentrowanie się na postawionym zadaniu i skuteczniejsze jego wykonanie.

Przejsie na sieciocentryczny sposób prowadzenia działań pozwala nie tylko na oddzielenie sensorów od platform uzbrojenia, ale również na oddzielenie operatorów od sensorów i platform. Obecność operatora na platformie przenoszącej sensory i uzbrojenie była dotychczas konieczna, było to bowiem jedyne miejsce, gdzie potrzebne do działania informacje dostępne były w odpowiednim czasie. Ewolucja koncepcji prowadzenia walki w kierunku działań sieciocentrycznych sprawiła, że taka konieczność zanikła. Stanowiska operatorów mogą być ulokowane w miejscu zapewniającym im bezpieczeństwo, z którego mogą obsługiwać platformy bojowe za pomocą zdalnego sterowania. Usunięcie załóg z platform przenoszących sensory i uzbrojenie umożliwia znaczną redukcję rozmiarów owych platform, czyniąc je trudniejszymi do wykrycia i zwalczania. W przypadku platform latających jest to o tyle istotne, że nieobecność załogi znosi dotychczasowe bariery związane z dopuszczalnymi dla organizmu ludzkiego przeciążeniami, które znacznie ograniczały manewrowość statków powietrznych.

Opisując sposób funkcjonowania sieciocentrycznego pola walki należy zwrócić szczególną uwagę na aspekty związane z dowodzeniem. Według słów Teda Campbella, wiceprezydenta programu Advanced Concepts firmy Lockheed Martin „dowodzenie jest sercem działań sieciocentrycznych”⁶⁷. Zdanie to określa bardzo trafnie wagę dowodzenia na sieciocentrycznym polu walki. Od właściwego dowodzenia zależy bowiem to, czy przewaga informacyjna i wysoka świadomość sytuacyjna zostaną w odpowiedni sposób wykorzystane.

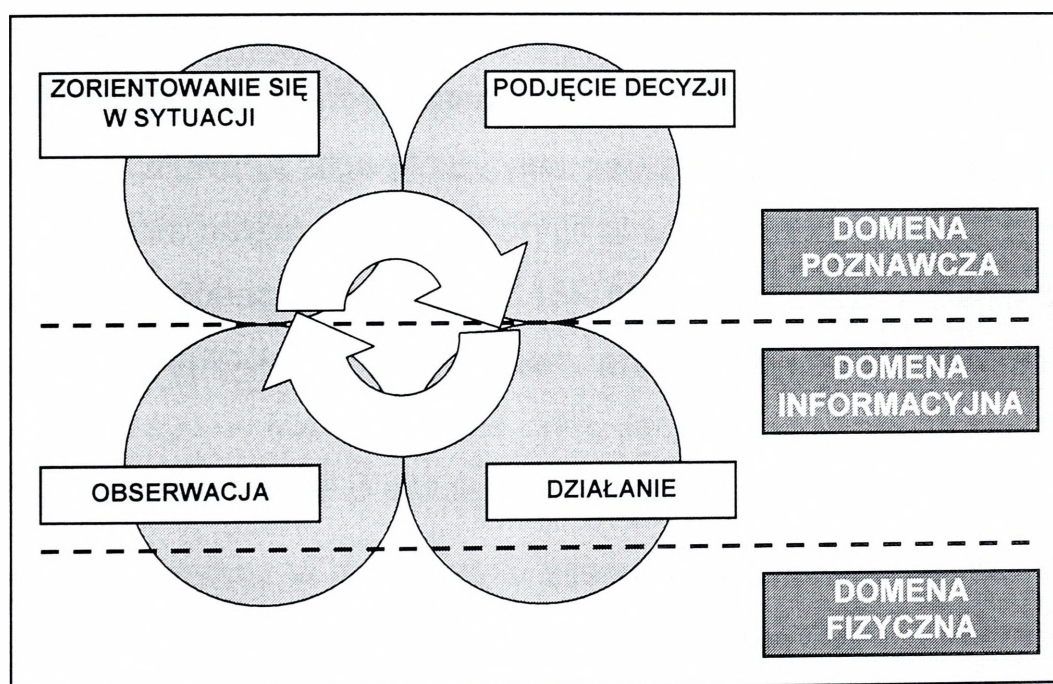
Aby dostosować proces dowodzenia do środowiska sieciocentrycznego, musi przejść ono pewną ewolucję. Nowoczesne technologie stosowane w siłach zbrojnych stwarzają bowiem potencjalnie duże możliwości, które nie mogą być wykorzystane przy zastosowaniu „tradycyjnego” cyklu dowodzenia. W tradycyjnym procesie dowodzenia decyzja podejmowana jest w czterofazowym cyklu działania⁶⁸: obserwacja, zorientowanie się w sytuacji, podjęcie decyzji, działanie⁶⁹. Cykl ten przedstawiony jest na rys. 2.12.

⁶⁷ *Net-Centric Operations*, Aviation Week and Space Technology Market Supplement, 2003, s. 56.

⁶⁸ OODA Loop – Observe, Orient, Decide, Act.

Fazy cyklu dowodzenia nałożone są na domeny, które omówione zostały szerzej w poprzednim podrozdziale:

- fizyczną, w której jest prowadzona walka oraz są realizowane decyzje;
- informacyjną, gdzie mają miejsce procesy informacyjne;
- poznawczą, w której dokonywana jest ocena sytuacji oraz podejmowane są decyzje.



Źródło: opracowanie własne na podstawie: D. Alberts, J. Garstka, R. Hayes, D. Signori, *Understanding Information Age Warfare*, op. cit., s. 132.

Rys. 2.12. Czterofazowy cykl dowodzenia (OODA Loop)

Taki sposób podejmowania decyzji jest szeroko stosowany na wszystkich szczeblach dowodzenia oraz w działaniach pojedynczych żołnierzy. W opinii twórców koncepcji walki sieciocentrycznej jest to sposób błędny, gdyż nadmiernie upraszcza proces podejmowania decyzji oraz powoduje, że owe decyzje są zbyt jednostronne⁷⁰. W wieloszczeblowym systemie dowodzenia w tradycyjnych działaniach platformocentrycznych cykle decyzyjne na wyższych szczeblach są dłuższe, ale zarazem rzadsze, muszą więc wybiegać daleko w przyszłość. Ponadto, występuje w nich specjalizacja funkcjonalna (np. logistyka, rozpoznanie itd.), co

⁶⁹ D. Alberts, J. Garstka, R. Hayes, D. Signori, *Understanding Information Age Warfare*, 2001, s. 132.

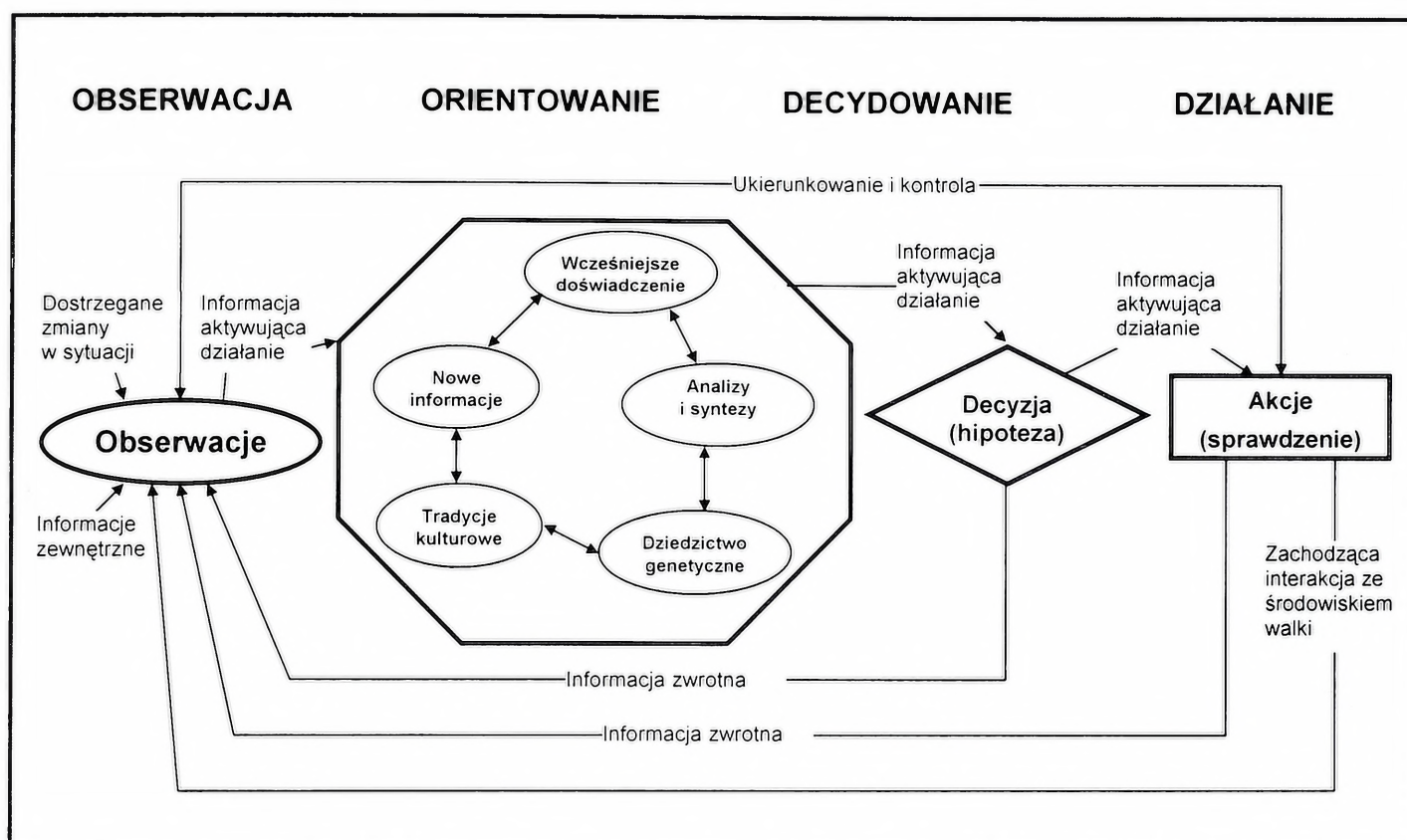
⁷⁰ Tamże s. 133.

utrudnia wymianę informacji między specjalistami reprezentującymi różne piony funkcjonalne. Połączenie wielu szczebli i pionów funkcjonalnych dowodzenia (o zróżnicowanych cyklach decyzyjnych) w jedną całość, powoduje duże problemy z koordynacją użycia sił wojskowych, zarówno podczas planowania, jak i działania.

W przypadku walki sieciocentrycznej, proces decyzyjny jest wynikiem zachodzących we wszystkich fazach cykli interakcji pomiędzy podmiotami (elementami składowymi sił prowadzącymi działania). Uwzględniany jest również wpływ czynnika czasowego oraz przestrzennego. Stąd też w dokumencie Office of Force Transformation „*Network Centric Operations Conceptual Framework Version 2.0*” za podstawę formułowania algorytmu cyklu decyzyjnego w warunkach sieciocentrycznego pola walki przyjmowany jest oryginalny opis modelu cyklu decyzyjnego stworzonego przez Johna Boyda (rys. 2.13). Model ten zakłada ciągłe interakcje decydentów i wykonawców ze środowiskiem, przeciwnikiem i siłami współdziałającymi, w wyniku czego, w każdym etapie cyklu decyzyjnego pojawia się informacja zwrotna mogąca modyfikować precyzję, zrozumienie, wybór bądź działanie.

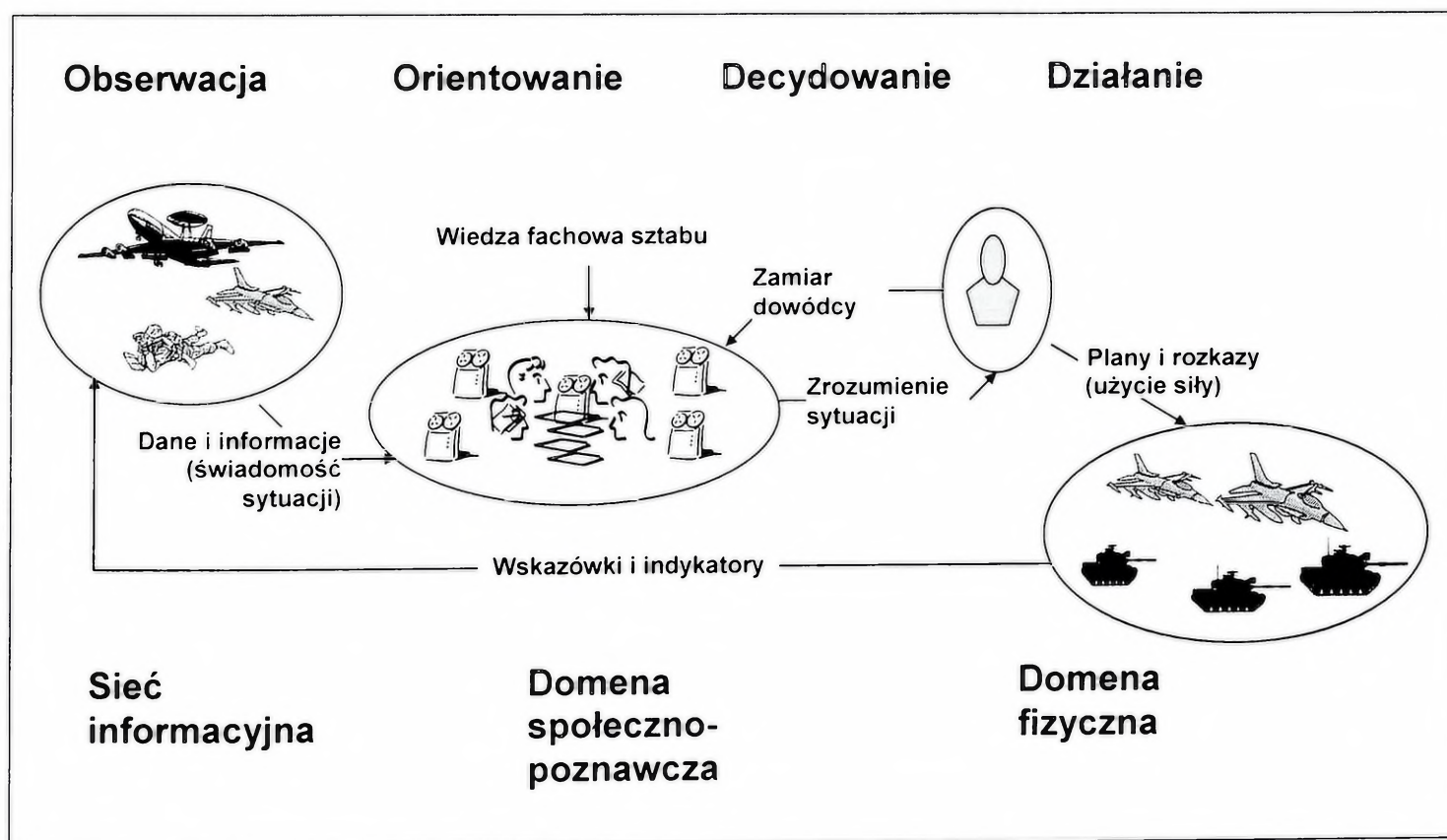
Zasadnicze zmiany w dowodzeniu siłami wojskowymi działającymi na sieciocentrycznym polu walki wiążą się z zastosowaniem systemów informacyjnych. Rozwój możliwości przechowywania informacji oraz zwiększenie mocy obliczeniowych, jaki dokonał się podczas ostatnich dwóch dekad, umożliwił tworzenie baz danych o dużej dostępności dla uprawnionych użytkowników. Zwiększa to możliwości bojowe wojsk poprzez zwiększoną dostępność informacji niezbędnych do podejmowania decyzji i działań, pozwalającą na szybkie i elastyczne użycie sił zbrojnych w szerokim spektrum operacji (rys. 2.14).

Charakterystyczne dla funkcjonowania i użycia sił wojskowych na sieciocentrycznym polu walki jest połączenie w ramach jednej rozległej sieci informacyjnej organów dowodzenia, środków rozpoznania oraz systemów (środków) rażenia ogniowego i elektronicznego. Obok dominujących obecnie powiązań hierarchicznych, implementacja założeń walki sieciocentrycznej ma pozwolić na elastyczne stosowanie kombinacji horyzontalnych i hierarchicznych połączeń informacyjnych, w zależności od potrzeb wynikających z celu działań oraz warunków, w jakich są one prowadzone. Siły posiadające zdolności sieciocentryczne będą w stanie lepiej



Źródło: opracowanie własne na podstawie: *Network Centric Operations Conceptual Farework Version 2.0*, op. cit., s. 34.

Rys. 2.13. Model cyklu decyzyjnego sieciocentrycznego pola walki



Źródło: opracowanie własne na podstawie: *Network Centric Operations Conceptual Farework Version 2.0*, op. cit., s. 48.

Rys. 2.14. Wspólne zrozumienie sytuacji na tle domen walki sieciocentrycznej

niż dotychczasowe wymieniać informację taktyczną, co pozwoli na bardziej precyzyjną, aktualną i spójną ocenę sytuacji przez wszystkie zaangażowane siły. Posiadanie przez dowódców poszczególnych szczebli dowodzenia ujednoliconej, aktualnej oceny sytuacji ma z kolei zwiększyć możliwości współdziałania oraz trwałości i szybkości dowodzenia.

Zgodnie z amerykańskimi założeniami walki sieciocentrycznej zawartymi w raporcie „Network Centric Warfare: Developing and Leveraging Information Superiority” funkcjonowanie sił wojskowych na sieciocentrycznym polu walki ma cechować⁷¹:

- samosynchronizacja działań (self-synchronization) polegająca na podejmowaniu niezbędnych w określonych sytuacjach taktycznych działań przez współdziałające siły bez konieczności stosowania tradycyjnego rozkazodawstwa;
- pogłębione zrozumienie zamiaru działania przełożonego;
- poprawa zrozumienia sytuacji operacyjno-taktycznej na wszystkich szczeblach dowodzenia;
- zwiększenie dostępu do informacji, którymi dysponują siły własne w rejonie operacji i miejscach stałej dyslokacji.

Zastosowanie założeń walki sieciocentrycznej w dowodzeniu ograniczać będzie odrębność kompetencji decyzyjnych pomiędzy poszczególnymi poziomami: strategicznym, operacyjnym i taktycznym. W wyniku „zapełnienia” przestrzeni o wymiarze strategicznym szczegółową informacją o wymiarze taktycznym postępować będzie spłaszczenie struktur dowodzenia oraz ich integracja⁷². Dotychczasowe oceny sytuacji, dokonywane przez każdy szczebel dowodzenia oddzielnie (fragmentaryczne oceny sytuacji taktycznej w wymiarze teatru działań pozwalały na dokonanie oceny sytuacji operacyjnej, a cząstkowe oceny operacyjne w skali globalnej umożliwiały stworzenie obrazu sytuacji strategicznej) zostaną zintegrowane, bowiem infostruktura sieci technicznej zapewni: dopływ szczegółowej in-

⁷¹ D. Alberts, J. Garstka, F. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, op. cit., s. 54-58.

⁷² L. Konopka, *Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości*, op. cit., s. 74.

formacji bezpośrednio na dowolny szczebel dowodzenia, przetworzenie tej informacji i dokonywanie natychmiastowych ocen sytuacji strategicznej czy operacyjnej.

Egzemplifikacją powyższych rozwiązań sieciocentrycznych w funkcjonowaniu wojsk na polu walki jest koncepcja „reach back capability”. „Sięganie do tyłu” umożliwia siłom rozmieszczonym w rejonie operacji dostęp do baz danych systemu rozpoznania w miejscach stałej dyslokacji oraz korzystanie z ich potencjału analitycznego. Podobna filozofia „reach forward” („sięganie do przodu”) zapewnia zobrazowanie dla dowódców oraz sztabów szczebla operacyjnego i strategicznego wybranych taktycznych aspektów użycia wojsk na sieciocentrycznym polu walki.

Analogicznie do coraz szerszego stosowania założeń sieciocentrycznych w dowodzeniu nowe rozwiązania wykorzystywane są w użyciu platform bojowych oraz zgrupowań taktycznych wojsk na polu walki.

Zacieranie się wspomnianych granic w zakresie wykorzystania platform bojowych powoduje, że środki pozostające w dyspozycji dowódców strategicznych mogą być użyte w wykonywaniu zadań bojowych w przypadku dynamicznych zmian w sytuacji taktycznej w określonym rejonie. Także taktyczne środki ogniowe mogą być wykorzystywane do atakowania celów o charakterze strategicznym⁷³. Umożliwia to właśnie szybki, szeroki przepływ informacji pomiędzy organami dowodzenia sił połączonych. Dla dowódców szczebla strategicznego bardziej opłacalne może być wykorzystanie środka taktycznego znajdującego się w położeniu dogodnym do porażenia obiektu o znaczeniu strategicznym niż użycie środka strategicznego. Jednocześnie dowódca taktyczny będzie miał wiedzę o położeniu środków walki pozostających w dyspozycji dowódców operacyjnych lub strategicznych, o których wykorzystanie może poprosić w sytuacji, gdy uzasadnia to rozwój sytuacji taktycznej odcinka walki i ekonomia użycia sił w wymiarze strategicznym⁷⁴.

⁷³ Tamże.

⁷⁴ Tamże, s. 78.

Wykorzystanie platform bojowych według powyższych założeń było szczególnie wyraźnie widoczne w operacji „Enduring Freedom” w Afganistanie, gdzie samoloty lotnictwa bombowego B-52, B-1 i B-2 wykorzystywano do realizacji zadań bezpośredniego wsparcia lotniczego na wezwanie z pola walki.

Teoria walki sieciocentrycznej zmniejsza w użycia sił na polu walki znacznie zasady scentralizowanego dowodzenia, zakładając, że przewagę dawać będzie możliwość decentralizacji dowodzenia i prowadzenia efektywnych działań przy „samosynchronizowaniu” działań poszczególnych dowódców taktycznych. W tradycyjnym platformocentrycznym systemie prowadzenia działań bojowych dowódca posiadał niewielką część informacji niezbędnych do podjęcia optymalnej w konkretnej sytuacji operacyjno-taktycznej decyzji, dlatego też jego możliwości w zakresie manewru i oddziaływania ogniowego były ograniczone. Poszczególne elementy kompleksowego, spójnego obrazu sytuacji były w formie informacji przekazywane przez dowódców niższego szczebla do dowódcy wyższego szczebla, który miał pełniejszy obraz sytuacji, mógł przekazywać odpowiednie zadania swoim podwładnym. W przypadku szybkich, dynamicznych działań dowódca szczebla operacyjnego (na przykład dowódca komponentu sił połączonych) nie był w stanie wypracować optymalnych zadań dla wszystkich podwładnych w odpowiednim czasie, ani też właściwie zsynchronizować zabezpieczenia logistycznego. Natomiast w koncepcji walki sieciocentrycznej dowódcy szczebla taktycznego mają dużą wiedzę, która pozwala na podejmowanie, w większym niż ma to miejsce w operacjach platformocentrycznych zakresie, samodzielnych decyzji. Znając ogólny zamiar przełożonego (nawet jeśli jest on dynamicznie modyfikowany w zależności od rozwoju sytuacji) dowódcy szczebla taktycznego mogą skutecznie kierować swoimi działaniami i jednocześnie synchronizować je z działaniami innych (o których są na bieżąco informowani) w celu realizacji wspomnianego zamiaru przełożonego. Zachodzi tu więc zjawisko samosynchronizacji dowodzenia na niższym szczeblu, nadzorowane tylko ogólnie ze szczebla nadrzędnego), nieznane w tradycyjnie zorganizowanych siłach zbrojnych⁷⁵. Zmniejszona zostaje wspomniana wcześniej jednostronność podejmowania decyzji, zwiększa się natomiast udział szerokiego kolektywu dowódczego w procesie podejmowania decyzji. Koncepcja walki sieciocentrycznej ogranicza zakres stosowania zasady jednoosobo-

⁷⁵ Tamże.

wości dowodzenia. Jedność wysiłku w działaniach osiągnięta jest nie przez generowanie decyzji z wysokiego szczebla dowodzenia, lecz dzięki wiedzy, którą posiadają dowódcy na niższych szczeblach. Takie nowatorskie podejście do problemu dowodzenia wymaga dużych zmian w mentalności, sposobie dowodzenia oraz szkoleniu, a zatem w domenie społecznej prowadzenia walki sieciocentrycznej.

Założenia funkcjonowania sieciocentrycznego pola walki wprowadzają również duże zmiany w zakresie umiejscowienia geograficznego stanowisk dowodzenia. Przykładem może być dyslokowanie Centrum Działań Powietrznych (AOC – Air Operations Centre). Dotychczas takie stanowisko dowodzenia o licznej obsadzie musiało znajdować się jak najbliżej obszaru działań, bowiem tylko tam jego personel mógł posiadać dostęp do aktualnej i w miarę pełnej informacji. W walce sieciocentrycznej na teatrze działań można розміścić tylko niewielką, wysuniętą grupę dowodzenia bojowego, natomiast zasadnicze centrum może pozostać na własnym terytorium, gdyż dostęp do pełnej i aktualnej informacji może być zapewniony w dowolnym punkcie globu. W związku z tym, przestaje być potrzebna organizacja rozbudowanej ochrony i obrony stanowiska dowodzenia, znika także konieczność jego zaopatrywania na odległym obszarze geograficznym⁷⁶.

2.3. Wnioski

Badania przeprowadzone w rozdziale drugim ukierunkowane były na poznanie i opisanie architektury oraz sposobu sieciocentrycznego pola walki w kontekście użycia ma nim sił wojskowych.

Z badań wynika, że pole walki w operacjach epoki informacyjnej nie ogranicza się do przestrzeni trójwymiarowej, ale obejmuje również spektrum elektromagnetyczne oraz „przestrzeń informacyjną”.

Badania teoretyczne prowadzone w różnych krajach nie są w pełni zgodne, co do architektury sieciocentrycznego pola walki. Według założeń amerykańskich z 1999 r. wyróżnia się trzy płaszczyzny przestrzeni, zwane domenami sieciocentrycznego pola walki, czyli domeną fizyczną, informatyczną i poznawczą. Domenę fizyczną definiuje się jako trójwymiarową przestrzeń fizyczną oraz spektrum elek-

⁷⁶ Tamże, s. 79.

tromagnetyczne. W tej domenie wyróżnia się platformy i systemy komunikacyjne oraz informatyczne, które łączą je w sieć. Badania dowiodły również, że domenę fizyczną łatwo jest określić, gdyż składa się z elementów znanych i łatwych do zmierzenia parametrach.

Z kolei domena informacyjna jest obszarem, w którym obrabiana i przechowywana jest informacja. W dymieniu tej zachodzi przyływ informacji – rozkazów, meldunków, sygnałów dowodzenia i innych – między elementami działającymi na sieciocentrycznym polu walki. Odgrywa ona szczególnie ważną rolę ze względu na potrzebę uzyskania i utrzymania przewagi informacyjnej.

Trzecią domeną, według poglądów amerykańskich, jest domena poznawcza. Nie jest ona tworem materialnym, lecz tworzona jest w umysłach uczestników walki sieciocentrycznej. Tworzą go także elementy jak: przywództwo, morale, spójność uczestników walki, jakość wyszkolenia, opinia publiczna, czy świadomość sytuacji. To w tej domenie umiejscowiona jest doktryna, zamiar działania procedury postępowania czy taktyka.

Ten podział sieciocentrycznego pola walki został obecnie rozwinięty i wyróżnia się w nim oprócz wymienionych domen również domenę społeczną. Określa się ją jako przestrzeń, w której zachodzą relacje pomiędzy uczestnikami tej walki. Wymienione zbiorowości wchodzą we wzajemne relacje, uzyskują świadomość pola walki oraz rozumieją konsekwencje z tego wynikające, co w rezultacie pozwala na podejmowanie kolektywnych decyzji.

W niezbyt licznych polskich opracowaniach przyjmuje się podział sieciocentrycznego pola walki na warstwy – warstwę dowodzenia, walki, informacyjną i sensorów. Według tych założeń warstwa dowodzenia umożliwia podejmowanie i zarządzanie walką przy pomocy odpowiednio wyszkolonego personelu i stanowisk dowodzenia. Warstwa walki jest samoorganizującą się siecią elementów ugrupowania bojowego, którymi są platformy uderzeniowe, ich załogi, które prowadzą walkę na bazie bieżącej, wiarygodnej i pozyskiwanej w czasie rzeczywistym wiedzy o sytuacji bojowej.

Zgodnie z tymi założeniami w warstwie informacyjnej zachodzi skorelowanie danych otrzymywanych z sensorów oraz dostarczanie informacji do systemów walki wszystkich szczebli.

Warstwę sensorów tworzą czujniki, czyli aparaty latające z aparaturą rozpoznawczą, naziemne i powietrzne stacje radiolokacyjne, środki rozpoznania radioelektronicznego, czujniki ruchu, itp., których zadaniem jest zbieranie informacji o sytuacji na lądzie, morzu, w powietrzu i kosmosie oraz w przestrzeni elektromagnetycznej.

Z analizy tych założeń wynika, że podstawą przyjętej typologii nie są domeny walki sieciocentrycznej, ale procesy związane ze zdobywaniem, korelacją, przesyłaniem i wykorzystywaniem informacji. Za to odpowiedzialna jest warstwa sensorów. Warstwa informacyjna jest odpowiedzialna za korelację i dystrybucję informacji, a działania podejmowane w oparciu o nie mają miejsce w warstwie walki.

Reasumując, kluczowymi technologiami sieciocentrycznego pola walki są technologie informatyczne związane z gromadzeniem, obróbką i dystrybucją informacji. Inne technologie, aparaty latające, środki uderzeniowe, rozpoznawcze i wyspecjalizowane pojazdy są połączone przy pomocy systemów informatycznych, co zapewnia efektywne działania oraz zmniejszenie własnych strat.

Sposób funkcjonowania sieciocentrycznego pola walki jest konsekwencją jego architektury i wynikających stąd możliwości. Ogólna koncepcja zakłada, że wyższa jakość sieciowego połączenia wojsk i związana z tym poprawa wymiany informacji wpływa na zdynamizowanie dowodzenia, a w konsekwencji na skuteczniejsze użycia sił na polu walki.

Funkcjonowanie sieciocentrycznego pola walki umożliwiają elementy, które tworzą całość sieci łączącej siły prowadzące działania, czyli sieć czujników oraz sieć dowodzenia rozwinięte w oparciu o wysokiej jakości sieć informacyjną. Poprzez zastosowanie odpowiednich procedur dowodzenia wykorzystywane są możliwości, jakie dają te sieci, co umożliwia osiągnięcie wysokiej efektywności i tempa działań.

Poprzez dysponowanie siecią wymiany informacji w czasie rzeczywistym możliwe jest oddzielenie sensorów od platform bojowych. Jest to możliwe w wyniku stworzenia jednolitego obrazu sytuacji taktycznej, który może być wykorzystywany przez każdą platformę bojową, dysponującą odpowiednim urządzeniem odbiorczym i znajdującą się w zasięgu nadajników dystrybuujących ten obraz.

Oddzielenie sensorów od platform bojowych pozwala na zwiększenie wielkości strefy zwalczania obiektów. Jest to możliwe w rezultacie posiadania odpowiedniej sieci sensorów. Dzięki temu wzrastają zarówno wskaźniki przestrzenne, jak skuteczności bojowej. Posiadanie dostępu do jednolitego obrazu sytuacji taktycznej umożliwia skryte podejście platform uderzeniowych do celu i użycie uzbrojenia na maksymalnej odległości do celu, ograniczonej zasięgiem środków rażenia. Rezygnacja z sensorów pokładowych pozwala na zwiększenie udźwigu i rozszerzenie możliwości uderzeniowych platform. Z kolei świadomość sytuacji taktycznej oraz przewaga informacyjna zapewniają pełne rozpoznanie przeciwnika oraz odpowiednio wczesną reakcję na zagrożenie.

Sieciocentryczny sposób prowadzenia działań pozwala nie tylko na oddzielenie sensorów od platform, ale również na oddzielenie od nich operatorów. Stnowiska operatorów mogą znajdować się w miejscach zapewniających im bezpieczeństwo, z których mogą obsługiwać platformy bojowe za pomocą zdalnego sterowania. Dzięki temu znosi się wiele ograniczeń platform bojowych, zwiększa ich udźwig i manewrowość.

Na sieciocentrycznym polu walki model procesu decyzyjnego zakłada ciągłe interakcje decydentów i wykonawców ze środowiskiem działania, przeciwnikiem i siłami współdziałającymi. Dzięki temu w każdym etapie cyklu decyzyjnego pojawia się sprzężenie (informacja) zwrotna, która może modyfikować decyzje i działanie.

Charakterystyczne dla użycia sił wojskowych na sieciocentrycznym polu walki jest połączenie w ramach jednej rozległej sieci informacyjnej organów dowodzenia, środków rozpoznania oraz systemów rażenia ogniowego i elektronicznego.

Zastosowanie założeń walki sieciocentrycznej w dowodzeniu ogranicza odrębność kompetencji decyzyjnych między poszczególnymi poziomami dowodzenia – strategicznym, operacyjnym i taktycznym. Zapewni to elastyczne reagowanie na zagrożenia i wyprzedzenie działań przeciwnika, a w efekcie na pokonanie go.

Rozdział 3

WYMAGANIA WOBEC SIŁ POWIETRZNYCH W ASPEKCIE ICH UŻYCIA NA SIECIOCENTRYCZNYM POLU WALKI

Formułowanie wymagań wobec sił powietrznych w aspekcie ich funkcjonowania na sieciocentrycznym polu walki uwarunkowane jest szeregiem różnorodnych czynników odnoszących się do różnych dziedzin użycia sił powietrznych.

Wyniki badań przedstawione w poprzednich rozdziałach studium wskazują, że skuteczne działanie w środowisku sieciocentrycznym wymagać będzie nie tylko posiadania niezbędnej infrastruktury umożliwiającej łączenie we wspólną sieć środków zdobywania informacji, decydentów oraz wykonawców. Również ważne będzie bowiem: umiejętność twórczego wykorzystania jakościowo bogatszych danych i informacji oraz przygotowanie stanów osobowych do wykorzystania potencjalnych możliwości oferowanych przez technologie informacyjne stosowne do rozwiązań sieciocentrycznych. Osiąganie standardów pozwalających na użycie sił powietrznych w ramach sieciocentrycznego pola walki prowadzić będzie w dalszej perspektywie do ich transformacji. Stąd też formułowanie wymagań powinno uwzględnić ich dwa poziomy: średniookresowy umożliwiający siłom powietrznym w ich obecnym kształcie funkcjonowanie w środowisku sieciocentrycznym oraz długofalowy, gdy wymogi te będą kształtować struktury i funkcjonowanie sił powietrznych⁷⁷.

Przeprowadzone przez zespół autorski badania problematyki walki sieciocentrycznej wskazują, że jednym ze sposobów konceptualizacji wymagań wobec sił powietrznych może być przyjęcie algorytmu zastosowanego przez zespół Garstki, Steina i Alberta w opracowaniu „Network Centric Warfare” dla opisania łańcucha wartości dodanej w walce sieciocentrycznej. Wymagania dotyczyłyby zatem w logicznej kolejności⁷⁸:

⁷⁷ P. K. Davis i in., *Transforming the Force. Suggestions for DoD Strategy*, Issue Paper, Rand National Defense Research Institute, 1998, dostępne z: www.rand.org/publications/IP/IP179/index.html

⁷⁸ J. Garstka, F. Stein, D. Alberts, *Network Centric Warfare: Developing and Leveraging Information Superiority*, op. Cit., s. 94.

- zdolności do łączenia w sieć oraz wymiany informacji;
- zdolności do przetwarzania informacji w wiedzę i podejmowania decyzji;
- zdolności do realizacji zadań.

Przyjęcie takiego podejścia badawczego nakazuje określenie wymagań w stosunku do sił powietrznych w aspekcie ich funkcjonowania na sieciocentrycznym polu walki w trzech domenach:

- domenie informacyjnej;
- domenie społeczno-poznawczej;
- domenie fizycznej.

3.1. Wymagania dla sił powietrznych w aspekcie domeny informacyjnej walki sieciocentrycznej

Dla pełniejszego oszacowania wymagań dla każdej z powyższych domen prowadzenia walki sieciocentrycznej można zastosować model organizacyjny interoperacyjności zaproponowany przez Clarka i Moona oraz grupę roboczą CRISR (LISI)⁷⁹.

Uznając określony poziom interoperacyjności z rozwiązaniami sieciocentrycznymi jako warunek funkcjonowania sił powietrznych na sieciocentrycznym polu walki można ocenić, jaki poziom w odniesieniu do kluczowych aspektów użycia sił powietrznych jest niezbędny lub pożądany, dla funkcjonowania w ramach takiego pola walki.

Model grupy LISI zakłada ocenę czterech obszarów determinujących zdolność sił wojskowych, w tym również sił powietrznych, do funkcjonowania na sieciocentrycznym polu walki. Są to postrzegane kompleksowo następująco elementy:

- infrastruktura (Infrastructure);
- dane (Data);

⁷⁹ *Network-Based Operations for the Swedish Defence Forces*, op. cit., s. 38.

- aplikacje (Applications);
- procedury (Procedures).

Ocena wymagań w stosunku do infrastruktury zapewniającej prowadzenie walki sieciocentrycznej obejmuje między innymi kompatybilność sprzętu i oprogramowania sieci w ramach ogółu użytkowników.

Ocena wymagań wobec danych ukierunkowana jest na ich format i modele, a aplikacje oceniane są przez pryzmat zdolności do wykorzystania wspólnych danych i ich wymiany. Procedury w modelu LISI oceniane są natomiast w aspekcie funkcjonowania użytkowników sieci, tworzenia wspólnego zobrazowania sytuacji operacyjnej i taktycznej oraz bezpieczeństwa informacji.

Wykorzystując zatem powyższy model dla formułowania ogólnych wymagań wobec domeny informacyjnej sił powietrznych w aspekcie ich funkcjonowania na sieciocentrycznym polu walki można dokonać dekompozycji szczegółowych wymagań dla każdego z wcześniej analizowanych obszarów.

Wymagania w stosunku do infrastruktury domeny informacyjnej sił powietrznych można postrzegać zarówno dla połączeń w sieci, jak również węzłów sieciowych (Net-Ready Nodes). Analiza wyników badań zawartych w dostępnej literaturze wskazuje, że połączenia w sieci oceniać należy poprzez ich zasięg (rozległość), stopień redundancji, bezpieczeństwa i terminowości przesyłania danych, a także przepustowość. Z kolei wymagania w stosunku do węzłów sieci powinny być określone w aspekcie ich czasu dostępu do sieci, ilości i rodzaju zabezpieczonych uczestników walki sieciocentrycznej, ilości połączeń z innymi węzłami, dostępności informacji w węźle oraz bezpieczeństwa danego węzła⁸⁰.

Dla ogólnego formułowania wymagań sieciocentrycznych można przyjąć, że rozległość sieci pozwalająca na realizację przez siły powietrzne zadań na sieciocentrycznym polu walki powinna być adekwatna do wielkości i charakteru zgromadzeń wykorzystywanych w konkretnym rodzaju działań i w środowisku właściwym dla działań powietrznych. W przypadku użycia wydzielonych komponentów ze składu sił powietrznych w operacjach reagowania kryzysowego poza obszarem kraju rozległość konfigurowanej na potrzeby danej operacji sieci winna objąć or-

⁸⁰ *Net-Centric Environment. Joint Functional Concept*, op. cit., s. 24-25.

gana dowodzenia, środki rozpoznania oraz autonomiczne moduły taktyczne, wydzielone do użycia w operacji, a także organa dowodzenia i zabezpieczenia w pokojowych, stałych miejscach dyslokacji realizujące zadania ich wsparcia i zabezpieczenia. Rozległość sieci sił powietrznych w wymiarze geograficznym będzie determinowana wielkością obszaru operacji, obszarem rozpoznawczego zainteresowania oraz rozmieszczeniem organów dowodzenia sił powietrznych, ich organicznych środków rozpoznania i zgrupowań wojsk realizujących zadania w operacji. Sieć sił powietrznych rozpatrywana w taki sposób obejmować będzie de facto trzy rodzaje podsieci (siatek) informacyjną, sensorów i oddziaływania o zbliżonej rozciągłości geograficznej.

Stopień redundancji (zwielokrotnienia) danych połączeń w sieci, jako jedno ze szczegółowych wymagań w stosunku do sił powietrznych działających na sieciocentrycznym polu walki, powinien być określony przez pryzmat roli i względnej ważności określonych połączeń dla realizacji zadań przez siły powietrzne. Tak więc stopień redundancji kluczowych połączeń w sieci powinien być wyższy niż połączeń w mniejszym znaczeniu. Redundancja może być przy tym osiągnięta poprzez zwiększenie ilości połączeń międzywęzłowych albo dywersyfikację sposobów wymiany danych (łączność radiowa, przewodowa, łącza danych).

Kolejnym kryterium określania wymagań dla domeny informacyjnej sił powietrznych na sieciocentrycznym polu walki jest bezpieczeństwo i terminowość przesyłania danych w sieci. Z doświadczeń szeregu sił zbrojnych różnych państw wynika, że kryterium funkcjonowania określonych relacji w sieci w czasie niemal rzeczywistym odnosi się do relatywnie niewielkiej części ogółu relacji sieciowych. W przypadku sieci sił powietrznych wymóg przesyłania danych w czasie niemal rzeczywistym będzie dotyczyć między innymi działań systemu obrony powietrznej, zwalczania mobilnych obiektów naziemnych (nawodnych) o dużym znaczeniu (Time Sensitive Target – TST), a także kierowania walką w działaniach ofensywnych. Cechą charakterystyczną relacji, które implikować będą wymianę danych w czasie niemal rzeczywistym będzie ograniczona ilość użytkowników w nie zaangażowanych, jak również doraźność tworzenia takich relacji. Tworzenie wymagań w stosunku do domeny informacyjnej sił powietrznych w kontekście ich funkcjonowania na sieciocentrycznym polu walki musi uwzględnić też określenie poziomu niezbędnej i pożądanej przepustowości dla różnych kategorii relacji w sieci. Prze-

pustowość poszczególnych relacji powinna być określona odmiennie dla użytkowników zaangażowanych w planowanie działań, stawianie zadań i kontrolę ich realizacji, niż dla użytkowników pełniących głównie funkcje wykonawcze lub koordynacyjne. W sieci sił powietrznych największe potrzeby w zakresie sumarycznej przepustowości relacji w sieci będzie mieć Centrum (Ośrodek) Operacji Powietrznych oraz Dowództwo Komponentu Powietrznego, co wynikać będzie z ilości i charakteru wykorzystywanych przez nie relacji informacyjnych. Wielkość przepustowości relacji w sieci sił powietrznych łączącej organa dowodzenia i moduły wykonawcze będzie w ogólnym wymiarze zdecydowanie mniejsza. Tym niemniej forma i rodzaj wymienionych danych mogą powodować, że przepustowość relacji, nawet na tych szczeblach, będzie musiała pozostawać relatywnie wysoka, tak aby umożliwiać w pełni prowadzenie operacji sieciocentrycznych. Wymóg ten jest szczególnie widoczny w przypadku przesyłania informacji w formie statycznego obrazu bądź sekwencji video pomiędzy środkami rozpoznania, a platformami bojowymi w trakcie zwalczania obiektów o dużym znaczeniu (TST)⁸¹.

Wymogi w stosunku do infrastruktury domeny informacyjnej walki sieciocentrycznej dla sił powietrznych, obok relacji sieciowych, dotyczą również węzłów sieci. Ponieważ węzły sieci sił powietrznych tworzyć będą trzy rodzaje użytkowników, których opisowo można określić jako: decydenci, wykonawcy i dostarczyciele danych, wymagania dla każdej z tych grup muszą być formułowane w nieco odmienny sposób.

W przypadku węzłów sieci tworzonych przez środki przekazywania informacji, w tym środki rozpoznania, ważnymi kryteriami dla formułowania wymagań będą: czas dostępu, zakres dostępności informacji oraz żywotność (bezpieczeństwo) takiego węzła. W przypadku naziemnych środków pozyskiwania informacji, wykorzystujących relacje łączności przewodowej, takich jak stacje radiolokacyjne wstępnego wykrywania systemu obrony powietrznej ważnym elementem będzie zwielokrotnienie połączeń danego węzła z siecią, dla zwiększenia dostępności informacji. W odniesieniu do powietrznych środków rozpoznania, takich jak: samoloty AWACS, czy JSTARS albo bezzałogowe rozpoznawcze statki powietrzne ważnym elementem formułowania wymagań będzie zdolność innych węzłów sieci do odbioru informacji zdobywanych przez nie.

⁸¹ *The US Force Transformation Flight Plan*, HQ USAF/XPXC, 2004, s. 48.

Formułowanie wymagań dla danych sfery informacyjnej walki sieciocentrycznej sił powietrznych powinno uwzględniać, w jakim stopniu format i postać danych zdobywanych i zbieranych w sieci jest dostępny dla wszystkich sił zaangażowanych w działania. Wymóg ten określony często jako „zasięg docierania informacji” (Information reach) powinien być formułowany z uwzględnieniem potrzeb informacyjnych użytkowników sieci oraz determinować ich wyposażenie w sprzęt pozwalający na wykorzystanie danych będących w sieci adekwatnie do potrzeb operacyjnych.

Wymagania dla aplikacji stosowanych w sieci sił powietrznych powinny być formułowane w aspekcie ich funkcjonowania w ramach sieciocentrycznego pola walki. Aplikacje stosowane we wszystkich podsieciach (siatkach) sieci sił powietrznych mogą być oceniane poprzez pryzmat możliwości współdziałania, jakie umożliwiają użytkownikom sieci (Collaboration) oraz dostępu do danych przechowywanych w sieci. Analiza modelu LISI stosowanego dla określenia poziomu interoperacyjności warunkującej skuteczne działanie na sieciocentrycznym polu walki pozwala przyjąć, iż wymagania w stosunku do aplikacji sieci sił powietrznych winny być formułowane w oparciu przede wszystkim o wymagania szczegółowe determinujące możliwości współdziałania użytkowników sieci oraz dostępu do danych, które się w niej znajdują. Szczegółowe wymagania w stosunku do aplikacji domeny informacyjnej uwzględnić zatem powinny⁸²:

- intensywność współdziałania (Collaboration intensity);
- zakres (głębść) współdziałania (Collaboration richness);
- zasięg (rozległość) współdziałania (Collaboration reach);
- żywotność (odporność na przeciwdziałanie) współdziałania (Collaboration robustness);
- terminowość współdziałania (Collaboration timeliness).

W zależności od potrzeb określonych użytkowników sieci sił powietrznych determinowanych przez funkcje realizowane przez nich (planowanie, stawianie i nadzór nad realizacją zadań oraz koordynowanie i realizację zadań bojowych)

⁸² *Network-Based Defence for the Swedish Defence Forces*, op. cit., s. 40, table 4.1 Components of LISI Model and Associated Metrics.

intensywność współdziałania mierzona ilością interakcji w trakcie pełnego cyklu decyzyjnego (lub jednostki czasu) będzie zróżnicowana. Odmienne kształtować się także będzie intensywność współdziałania w poszczególnych etapach cyklu decyzyjnego dla planistów, wykonawców i koordynatorów. Powinno to znaleźć swoje odzwierciedlenie w szczegółowych wymaganiach formułowanych dla sił powietrznych. Przy definiowaniu wymagań dla aplikacji domeny informacyjnej należy uwzględnić zakres współdziałania pomiędzy określonymi użytkownikami, przekładający się na ich rolę we wspólnym wypracowaniu pewnych rozwiązań, jak również wzajemną zależność w odniesieniu do realizacji określonych funkcji. Ważnym elementem określania wymogów dla aplikacji domeny informacyjnej sieci sił powietrznych będzie określenie do jakiej części ogółu użytkowników sieci będzie mieć zastosowanie wymóg bycia zdolnym do pełnego lub częściowego współdziałania w ramach sieci.

Przeprowadzone przez zespół autorski studia literatury przedmiotu wskazują, że przy określaniu szczegółowych wymagań niezbędne będzie dokonanie kategoryzacji uprawnień poszczególnych użytkowników w zakresie funkcji realizowanych w ramach współdziałania z innymi, co umożliwi stworzenie hierarchii wirtualnych podsieci w oparciu o miejsce i rolę określonych użytkowników w realizacji konkretnych zadań. Ściśle powiązane z powyższymi wymaganiami szczegółowymi w zakresie zapewnienia możliwości współdziałania użytkowników przez aplikacje domeny informacyjnej sieci sił powietrznych są wymogi, co do zapewnienia ciągłości tego współdziałania oraz jego terminowości⁸³.

Obok wymagań określonych dla aplikacji stosowanych w domenę informacyjną w aspekcie zapewnienia współdziałania użytkowników sieci, formułowanie szczegółowych wymagań technicznych i organizacyjnych winno uwzględniać dostęp do informacji w sieci oraz jej przechowywanie.

W literaturze przedmiotu podkreśla się przede wszystkim znaczenie terminowości dostępu do informacji oraz łatwości wyszukiwania niezbędnych konkretnemu użytkownikowi sieci sił powietrznych danych oraz informacji. Z punktu widzenia żywotności sieci sił powietrznych ważnym elementem wymogów dla domeny informacyjnej powinno być odpowiednie rozmieszczenie zasobów informacyj-

⁸³ *Network Centric Operations Conceptual Framework Version 2.0*, op. cit., s. 49-52.

nych w obrębie sieci, tak aby eliminowanie części węzłów nie powodowało utraty zawartych w bazach danych sieci. Istotne znaczenie ma w tym aspekcie również organizacja przechowywania informacji w sieci sił powietrznych i dostępu do nich przez poszczególnych użytkowników.

Tworzenie wymagań dla sił powietrznych w aspekcie ich funkcjonowania w ramach sieciocentrycznego pola walki powinno uwzględniać procedury funkcjonowania sieci. W celu określenia szczegółowych wymagań w tym zakresie uwzględnić należy procedury organizacji kontroli funkcjonowania sieci sił powietrznych, w tym⁸⁴:

- kontrolę dostępu do sieci;
- bezpieczeństwo dostępu i bezpieczeństwo danych w sieci;
- kontrolę czasu dostępu;
- kontrolę zakresu dostępu i użytkowania;
- monitorowanie pracy sieci;
- kontrolę wykorzystania częstotliwości;
- procedury odtwarzania zdolności funkcjonowania sieci.

W świetle doświadczeń funkcjonowania szeregu sieci wojskowych wykorzystujących komercyjne środki łączności można założyć, że szczególnie ważnym wymogiem dla procedur funkcjonowania sieci sił powietrznych powinna być kontrola dostępu oraz bezpieczeństwa dostępu i danych. Ważnym elementem wymagań będą w warunkach sieciocentrycznego pola walki procedury odtwarzania zdolności sieci sił powietrznych do funkcjonowania w przypadku wykonania na nią uderzeń ogniowych bądź elektronicznych⁸⁵.

⁸⁴ *Network-Based Defence for the Swedish Defence Forces*, op. cit., s. 40, table 4.1 Components of LISI Model and Associated Metrics.

⁸⁵ M. Bruno, *Western Iraq Most Networked In History of War*, Official Says, w: *Aerospace Daily and Defense Report*, 2005, dostępne z: [www.oft.osd.mil/library/library-files/article_473_Aerospace %20Daily.doc](http://www.oft.osd.mil/library/library-files/article_473_Aerospace%20Daily.doc)

Dokonana przez zespół autorski analiza szczegółowych wymagań technicznych i organizacyjnych w zakresie tworzenia i funkcjonowania domeny informacyjnej sił powietrznych funkcjonujących w ramach sieciocentrycznego pola walki pozwala na wygenerowanie ogólnych wymagań w tym zakresie.

Podstawowym wymogiem funkcjonowania sił powietrznych w ramach sieciocentrycznego pola walki będzie fizyczne istnienie infrastruktury informacyjnej w postaci sieci. Sieć tworzona i utrzymywana na potrzeby sił powietrznych powinna obejmować: środki zdobywania informacji, w tym środki rozpoznania (sensory), organy dowodzenia (decydentów) z elementami wykonawczymi (platformami bojowymi, zgrupowaniami taktycznymi).

Strukturę powiązań hierarchicznych i horyzontalnych w sieci sił powietrznych powinna cechować immanentna otwartość i elastyczność, które będą pozwalać na doraźne, adekwatne do potrzeb wynikających z rozwoju sytuacji operacyjno-taktycznej, konfigurowanie sieci zadaniowych, w ramach ogólnej sieci sił powietrznych oraz sił połączonych.

Połączenia w sieci sił powietrznych funkcjonujących w ramach sieciocentrycznego pola walki powinny zapewniać żywotność sieci osiąganą poprzez zwiększenie ilości połączeń każdego węzła z innymi lub redundancję sposobów wymiany danych.

Niezbędnym wymaganiem jest terminowość w funkcjonowaniu domeny informacyjnej. Połączenia w sieci powinny zatem zapewnić terminowość wymiany i dostępu do informacji oraz jej bezpieczeństwo adekwatnie do potrzeb określonych użytkowników sieci sił powietrznych wynikających z realizowanych przez nich funkcji.

Zdolność do funkcjonowania sił powietrznych w ramach sieciocentrycznego pola walki warunkowana będzie przez gotowość węzłów sieci tworzonych przez środki rozpoznania, organa dowodzenia i moduły bojowe sił powietrznych, do funkcjonowania w środowisku sieciocentrycznym. Niezbędnym warunkiem użycia sił powietrznych na sieciocentrycznym polu walki będzie spełnienie przez wszystkich użytkowników sieci sił powietrznych tworzących jej węzły kryteriów inteoperacyjności sieciocentrycznej, rozumianej jako ich zdolność do wspólnego działania.

Sieć sił powietrznych musi zapewnić dostęp do danych i informacji dla wszystkich jej użytkowników adekwatnie do ich potrzeb i realizowanych funkcji (planistycznych, stawiania zadań, koordynacji i realizacji zadań).

Aplikacje domeny informacyjnej sieci sił powietrznych powinny zapewnić wirtualne współdziałanie użytkowników sieci, w zakresie i w sposób umożliwiający im realizację zadań. Aplikacje powinny również umożliwiać terminowy dostęp do baz danych oraz pozwalać na gromadzenie danych i informacji w nich przez uprawnionych użytkowników.

Skuteczne użycie sił powietrznych na sieciocentrycznym polu walki uzależnione będzie również od procedur kontroli sieci. Stąd też niezbędne jest, aby system kontroli funkcjonowania sieci sił powietrznych obejmował procedury: kontroli i analizy dostępu, monitorowania funkcjonowania oraz odtwarzania zdolności do działania przez sieć.

3.2. Wymagania dla sił powietrznych w aspekcie domeny społeczno-poznawczej walki sieciocentrycznej

Jednym z zasadniczych elementów transformacji zasad walki zbrojnej są nowe wymagania w stosunku do sił powietrznych w aspekcie ich funkcjonowania w ramach sieciocentrycznego pola walki w jego domenie społeczno-poznawczej.

W przeciwieństwie do działań platformocentrycznych, w których istnieje wyraźny podział odpowiedzialności pomiędzy poszczególnymi uczestnikami walki w zakresie oceny sytuacji, podejmowania decyzji i jej realizacji, w działaniach sieciocentrycznych zwiększa się zakres uprawnień i odpowiedzialności każdego uczestnika. Jakościowo zwiększony dostęp do informacji na wszystkich szczeblach dowodzenia sił powietrznych oraz w każdym etapie cyklu decyzyjnego tworzy sytuację, gdzie użytkownicy sieci stają się nie tylko odbiorcami informacji, ale również jej wytwórcami. Tworzy to sytuację, gdzie indywidualni użytkownicy sieci wchodzi w interakcje społeczne z innymi użytkownikami działając jako twórcy informacji, manipulatorzy (przetwarzający informację) oraz jej konsumenci. Analogiczne interakcje cechować będzie współpraca zbiorowych użytkowników sieci sił powietrznych, takich jak: piony funkcjonalne sztabów, komórki specjalistyczne organów dowodzenia itp.

W dokumencie koncepcyjnym Departamentu Obrony USA „Net-Centric Environment. Joint Functional Concept” dokonano podziału zdolności i atrybutów determinujących możliwości organizacji wojskowej funkcjonowania na sieciocentrycznym polu walki. Wyróżniane są one w dwóch obszarach: technicznym (Technical Area) oraz wiedzy (Knowledge Area)⁸⁶. Domena społeczno-poznawcza walki sieciocentrycznej w przeważającej mierze determinowana będzie zdolnościami i atrybutami w obszarze wiedzy. W koncepcji amerykańskiej przyjmuje się, że to właśnie w obszarze wiedzy będą mieć miejsce interakcje pomiędzy poszczególnymi uczestnikami operacji (zarówno indywidualnymi, jak i zbiorowymi). W ramach tych interakcji będzie następowała wymiana informacji, tworzona świadomość sytuacji na polu walki oraz wypracowywane kolektywne zrozumienia możliwych implikacji wyływających z jej rozwoju. W obszarze wiedzy będzie mieć miejsce współdziałanie w ramach kolektywnego wypracowania decyzji (collaborative decisionmaking). Zwiększenie zakresu współdziałania pomiędzy poszczególnymi uczestnikami operacji oraz ich grupami ma prowadzić do podejmowania decyzji szybciej i w oparciu o lepsze przesłanki⁸⁷. W amerykańskich koncepcjach prowadzenia walki sieciocentrycznej zakłada się, że współdziałanie w podejmowaniu decyzji będzie mieć miejsce w doraźnie tworzonych organizacjach zadaniowych, gdzie poszczególni członkowie będą dobierani w zależności od potrzeb konkretnego zadania i będą funkcjonować w oparciu o minimalny zbiór zasad i procedur⁸⁸.

Aby poszczególni użytkownicy sieci sił powietrznych oraz ich zbiorowości mogli skutecznie funkcjonować w domenie społeczno-poznawczej walki sieciocentrycznej konieczne jest spełnienie przez nich szeregu wymogów. Wymogi te determinować będą w konsekwencji zdolność sił powietrznych do funkcjonowania w ramach sieciocentrycznego pola walki.

⁸⁶ *Net-Centric Environment. Joint Functional Concept*, op. cit., s. 11-12.

⁸⁷ A. Cebrowski, *The Power of Information Comes from the Ability to Share*, w: *Defender*, Vol. 2. No. 3, 2005, s. 2-3, dostępne z: www.oft.osd.mil/library/library-files/article_448_Defeder-NetCentric.pdf

⁸⁸ *Net Centric Operations Conceptual Framework*, op. cit., s. 31-35.

Do podstawowych wymagań w stosunku do personelu sił powietrznych zaangażowanego w funkcjonowanie tego rodzaju sił zbrojnych w ramach środowiska sieciocentrycznego w świetle ustaleń amerykańskiej koncepcji, należy zaliczyć⁸⁹:

- umiejętność tworzenia pożądaných odpowiednio do realizowanych zadań relacji organizacyjnych;
- umiejętność współdziałania;
- umiejętność kooperacji pozytywnej w ramach samosynchronizacji działań;
- umiejętność dzielenia się świadomością sytuacji na polu walki z innymi użytkownikami;
- umiejętność dzielenia się zrozumieniem sytuacji na polu walki z innymi użytkownikami sieci;
- umiejętność prowadzenia zespołowego planowania i podejmowania decyzji;
- umiejętność osiągania konstruktywnej współzależności.

Umiejętność tworzenia, pożądaných w stosunku do potrzeb wynikających z realizowanych zadań, relacji organizacyjnych (ability to establish appropriate organizational relationships) warunkujących zdolność funkcjonowania sił powietrznych w domenie społeczno-poznawczej walki sieciocentrycznej rozumiana jest jako umiejętność tworzenia, zmiany i utrzymywania relacji organizacyjnych, które są optymalne w świetle realizowanych zadań i funkcji.

W amerykańskiej teorii walki sieciocentrycznej podkreśla się rolę nieformalnych powiązań organizacyjnych pojedynczych osób i zbiorowości zaangażowanych w realizację wąsko określonych funkcji, tak zwanych „społeczności o wspólnych zainteresowaniach” (communities of interest – COI). Społeczności te grupujące osoby o eksperckim poziomie wiedzy w określonej, wąskiej specjalności, połączone w sieci będą w stanie wspierać dowódców w podejmowaniu decyzji. Warunkiem pełnego wykorzystania tego rozproszonego w całych siłach powietrznych potencjału będzie zdolność do połączenia ich w ramach wirtualnych dynamicznie

⁸⁹ *Net-Centric Environment. Joint Functional Concept*, op. cit., s. 22-23.

zmiennych organizacji zadaniowych. Wymagać to będzie w sferze społeczno-poznawczej walki sieciocentrycznej gotowości personelu sił powietrznych (indywidualnie i jako zespół) do działania w sytuacji zmieniających się relacji przełożony – podwładny oraz wspierany – wspierający. Szczególnie wysokie wymagania w tym zakresie dotyczyć będą dowódców i sztabów sił powietrznych, gdyż to oni będą inicjatorami tworzenia, zmiany i utrzymania doraźnych relacji organizacyjnych pożądanых dla skutecznej realizacji zadań w warunkach sieciocentrycznego pola walki.

Szereg szczegółowych wymogów dla domeny społeczno-poznawczej prowadzenia działań sieciocentrycznych przez siły powietrzne wynikać będzie z zwiększania umiejętności i zdolności organów dowodzenia sił powietrznych do współdziałania za pośrednictwem sieci. W środowisku sieciocentrycznym współdziałanie rozproszonych geograficznie organów dowodzenia ze wszystkimi siłami zaangażowanymi do realizacji zadań będzie musiało cechować się ciągłością istniejących struktur organizacyjnych i funkcjonalnych. Przewiduje się, że siły powietrzne, a w szerszym ujęciu siły zbrojne, będą musiały przygotować dowódców i oficerów sztabu do funkcjonowania w warunkach kolektywnego wypracowania decyzji, nowych rozwiązań strukturalnych, doktrynalnych i kulturowych odmiennych od tych, które cechują rozwiązania platformocentryczne stosowane obecnie. Sytuacja taka powoduje konieczność kształcenia i szkolenia personelu sił powietrznych ukierunkowanego na kształtowanie umiejętności i zdolności współdziałania w środowisku sieciocentrycznym⁹⁰.

Aby skutecznie funkcjonować w warunkach sieciocentrycznego pola walki siły powietrzne, będą musiały wypracować i wdrożyć procedury umożliwiające oddolną samosynchronizację działań podstawowych modułów operacyjnych, tak aby mogły one szybciej wykorzystywać zmiany na polu walki i reagować na działania przeciwnika.

Poważnych zmian w stosunku do wymagań dla funkcjonowania sił powietrznych w domenie społeczno-poznawczej walki sieciocentrycznej należy upatrywać w definiowanych w amerykańskich koncepcjach NCW postulatach zdolno-

⁹⁰ Wymóg ten jest bezpośrednio wyartykułowany w szeregu dokumentów koncepcyjnych państw implementujących rozwiązania sieciocentryczne, między innymi w: amerykańskim *The Implementaion of Network Centric Warfare*, op. cit., s. 55-56, czy australijskim *NCW Roadmap*, op. cit., s. 14.

ści poszczególnych uczestników walki oraz ich zbiorowości do współdzielenia świadomości sytuacji oraz jej zrozumienia (situational awareness).

Ocena sytuacji dokonywana przez określone osoby lub zespoły funkcjonalne w warunkach sieciocentrycznego pola walki będzie musiała być wymieniana w ramach szerokiego kręgu zainteresowanych nią organów dowodzenia, wykonawców i innych uczestników operacji. Wymiana tego typu informacji w przypadku świadomości sytuacji wymagać będzie od włączanych w sieć użytkowników zdolności do informowania o tym: kto, co i gdzie na polu walki robi. W przypadku współdzielenia zrozumienia sytuacji wymagane jest, aby użytkownik sieci informował innych, co może wynikać z zaobserwowanych przez niego działań przeciwnika i sił własnych. Taki wymóg będzie generować poważne wymagania w stosunku do oficerów pełniących funkcje dowódcze i sztabowe w aspekcie ich zdolności do kompleksowej oceny sytuacji i generowania rekomendacji działań. Przekładać się to będzie na wymagania w zakresie kształcenia i szkolenia personelu sił powietrznych w zakresie treści, form i metod przygotowania adekwatnych do środowiska walki sieciocentrycznej.

W amerykańskiej koncepcji „Net-Centric Environment. Joint Functional Concept” podkreśla się znaczenie zdolności dowódców i sztabów do kolektywnego decydowania i realizacji planowania⁹¹. Przewiduje się, że w środowisku sieciocentrycznym w procesie podejmowania decyzji dowódcy, w zdecydowanie większym niż obecnie zakresie, będą konsultować się z innymi dowódcami i „społecznościami o wspólnych zainteresowaniach”. Wyzwaniem dla dowódców będzie szybka analiza potencjalnych wariantów działania oraz możliwych pośrednich i długofalowych skutków powodowanych realizacją podjętej decyzji (potential second and third order effects). Wyzwaniem dla domeny społeczno-poznawczej walki sieciocentrycznej będą również zdolność i gotowość do wzajemnej konstruktywnej współzależności, gdy zdolność i potencjał różnych modułów sił będą mogły być w pełni wykorzystywane w zależności od potrzeb pola walki, bez względu na ich miejsce w organizacji.

⁹¹ *Net-Centric Environment. Joint Functional Concept*, op. cit., s. 15-17.

Dokonane przez zespół autorski analizy wymagań formułowanych w stosunku do funkcjonowania sił wojskowych w domenie społeczno-poznawczej walki sieciocentrycznej pozwalają na wygenerowanie ogólnych wniosków w tym zakresie w stosunku do sił powietrznych.

Można przypuszczać, że w odniesieniu do domeny społeczno-poznawczej walki sieciocentrycznej wymagania w stosunku do sił powietrznych formułowane powinny być w trzech głównych obszarach⁹²:

- doktryny;
- kształcenia i szkolenia;
- przywództwa.

Przemiany cywilizacyjne epoki informacyjnej powodować będą konieczność szerszego niż obecnie uwzględnienia w doktrynie sił powietrznych roli informacji w działaniach bojowych. Rozwiązania taktyczne będą musiały również uwzględnić wzrost możliwości bojowych wynikających ze stosowania rozwiązań sieciocentrycznych. Biorąc pod uwagę zdynamizowanie procesu przemian w założeniach operacyjnych i doktrynie pożądane jest zwiększenie zakresu sprawdzania słuszności przyjmowanych założeń i rozwiązań w trakcie gier wojennych, eksperymentów i testów⁹³.

Niezbędne wydaje się w siłach powietrznych implementowanie rozwiązań doktrynalnych zapewniających zdolność do funkcjonowania w ramach połączonych zgrupowań sił zadaniowych modułów sił powietrznych na coraz niższych szczeblach dowodzenia.

Przygotowanie sił powietrznych do funkcjonowania w warunkach sieciocentrycznego pola walki wymagać będzie intensyfikacji szkolenia indywidualnego i zbiorowego oraz przewartościowań w kształceniu zasobów osobowych. Programy szkolenia dowództw i sztabów sił powietrznych oraz wojsk będą musiały ulec modyfikacjom, tak aby pogłębić wiedzę, budować doświadczenie oraz kształtować umiejętności niezbędne dla skutecznego działania w ramach środowiska siecio-

⁹² Tamże, s. 26.

⁹³ D. A. Deptula, *Effects-Based Operations: Change in the nature of war*, Aerospace Education Foundation, 2001, s. 25-26.

centrycznego. Konieczne jest zwiększenie tempa dostosowywania procesu szkolenia do zmieniających się rozwiązań stosowanych w praktyce operacji.

Ćwiczenia sił powietrznych powinny być ukierunkowane w większym stopniu na współdziałanie z siłami i organami dowodzenia z pozostałych rodzajów sił zbrojnych oraz organizacjami militarnymi, tak aby przygotować personel sił powietrznych do funkcjonowania w środowisku sił połączonych i cywilno-wojskowym. W ćwiczeniach eksponować należy wykorzystanie systemów informacyjnych i sieci jako podstawowego medium zapewniającego współdziałanie. Aby kontynuować zasadę realizmu szkolenia (szkół się jak będziesz walczył, walczyć jak się szkolisz) dowództw, sztabów i wojsk sił powietrznych, w ćwiczeniach należy realizować wymóg wykorzystywania elementów realnie istniejących sieci operacyjnych. Wymóg ten jest niezbędny dla kształtowania właściwych nawyków funkcjonowania na sieciocentrycznym polu walki.

W kształtowaniu personelu sił powietrznych uwzględnione muszą być wymogi poznawcze i kulturowe warunkujące jego działanie w środowisku sieciocentrycznym. Konieczne jest szersze wykorzystanie potencjału intelektualnego instytucji edukacyjnych dla prowadzenia badań problematyki funkcjonowania sił powietrznych w ramach sieciocentrycznego pola walki, w tym analiz perspektywicznych koncepcji operacyjnych.

Wymogi związane z funkcjonowaniem sił powietrznych w ramach sieciocentrycznego pola walki w obszarze przywództwa wynikać będą z odmiennego od środowiska platformocentrycznego rozłożenia uprawnień decyzyjnych, relacji przełożony – podwładny oraz działania w warunkach braku kontaktu fizycznego pomiędzy dowódcami i podległymi im siłami oraz między siłami współdziałającymi. Wypracowania wymagają zasady i procedury kierowania działalnością w doraźnie tworzonych sieciach zadaniowych (communities of interest). Niezbędne jest przygotowanie przez siły powietrzne przyszłych dowódców do podejmowania decyzji w warunkach zwiększonego obciążenia informacją w środowisku sieciocentrycznym.

Szczegółowych badań wymagać będzie w siłach powietrznych problematyka przygotowania dowódców i wojsk do podejmowania inicjatywy oddolnej samosynchronizacji, a także godzenia jej z zasadą jedności dowodzenia.

3.3. Wymagania dla sił powietrznych w aspekcie domeny fizycznej walki sieciocentrycznej

Wymagania w stosunku do sił powietrznych formułowane w aspekcie ich funkcjonowania w domenie fizycznej walki sieciocentrycznej ukierunkowane są na te cechy zgrupowań taktycznych (modułów bojowych), organów dowodzenia oraz środków rozpoznania sił powietrznych, które umożliwiają ich użycie na sieciocentrycznym polu walki.

Analizując podstawowe założenia funkcjonowania elementów składowych sieci na polu walki można przyjąć, że możliwe jest określenie mierzalnych wskaźników pomiaru wymagań dla poszczególnych elementów składowych sieci sił powietrznych w aspekcie ich użycia na sieciocentrycznym polu walki. Wskaźniki takie powinny w opinii zespołu autorskiego odnosić się do:

- zdolności do manewru na polu walki;
- zdolności do przerzutu do rejonu operacji;
- zdolności do przeżycia na polu walki;
- zdolności do podtrzymania ciągłości działań.

W amerykańskiej koncepcji „Net-Centric Environment. Joint Functional Concept”, zdolności determinowane przez charakterystyki techniczne rozpatrywane są przez pryzmat spełnienia przez nie bardziej szczegółowych wymagań tak zwanych atrybutów. Przyjmuje się, że rozwiązania techniczne warunkujące działania sił powietrznych na sieciocentrycznym polu walki powinny cechować się⁹⁴:

- pewnością wykorzystania (assured);
- wysoką niezawodnością (robust);
- wysoką adaptacyjnością (agile);
- łatwością obsługi i wykorzystania (manageable);
- przystosowaniem do działań ekspedycyjnych (expeditionary);
- jakością (quality).

⁹⁴ *Net-Centric Environment. Joint Functional Concept*, op. cit., s. 27.

Podejmując zatem próbę stworzenia podstaw dla wygenerowania wymagań w stosunku do sił powietrznych w aspekcie ich funkcjonowania w domenie fizycznej walki sieciocentrycznej należy określić, w jaki sposób powinny być mierzone rozwiązania techniczne.

Pewność wykorzystywania utożsamiana powinna być z poziomem zaufania, iż dane rozwiązanie będzie funkcjonować poprawnie i niezawodnie może być mierzona poprzez⁹⁵:

- określeniem autentyczności informacji, nadawcy i odbiorcy;
- stopniem ochrony niejawności;
- dostępnością do danego rozwiązania usług, itp.

Wysoka niezawodność funkcjonowania elementów sieci sił powietrznych w domenie fizycznej walki sieciocentrycznej wymagać będzie spełnienia przez nie szeregu wymogów szczegółowych, w tym między innymi⁹⁶:

- określonym stopniem żywotności;
- redundancją w możliwości realizacji podstawowych funkcji;
- zasięgiem funkcjonowania;
- zdolnością do odzyskania zdolności działania na polu walki.

Przekładając powyższe założenia koncepcyjne na wymagania w stosunku do elementów sieci sił powietrznych należy podkreślić, że żywotność cechująca organa dowodzenia (decydentów), platformy i moduły bojowe (wykonawców) i środki rozpoznania (sensory) będzie zróżnicowana. Powinna być również szczegółowo opisana w aspekcie warunków zewnętrznych, minimalnego akceptowalnego poziomu realizacji funkcji oraz jej długotrwałości.

Ważnym elementem wymagań w stosunku do elementów sieci sił powietrznych będzie stopień redundancji w możliwości podstawowych funkcji. W naturalny sposób wymagania w stosunku do poziomu redundancji będą rosły w przypadku niemożności zapewnienia wysokiego stopnia żywotności określonych elementów sieci. Zasięg funkcjonowania elementów sieci sił powietrznych w aspekcie fizycz-

⁹⁵ Tamże.

⁹⁶ Tamże, s. 28.

nym uzależniony będzie od możliwości czasowych i przestrzennych cechujących platformy i moduły bojowe oraz środki rozpoznania. W ogólnym ujęciu zasięg i długotrwałość lotu platformy przenoszącej dany techniczny środek rozpoznania albo rażenia będzie musiał zapewnić rozpoznanie obiektów w całym obszarze rozpoznawczego zainteresowania oraz ich zwalczania na całą głębokość obszaru operacji.

W świetle przeprowadzonych badań dostępnej literatury przedmiotu można przyjąć, iż szczegółowe wymagania dla sił powietrznych w aspekcie ich funkcjonowania w domenie fizycznej walki sieciocentrycznej powinny odnosić się również do atrybutów zapewniających wysoką adaptacyjność na polu walki.

W przypadku platform i modułów bojowych oraz środków rozpoznania stanowiących część sieci sił powietrznych adaptacyjność powinna być postrzegana przez pryzmat elastyczności, dynamiczności i wszechstronności. Sieci sensorów sił powietrznych powinny być przystosowane do multispektralnego pozyskiwania informacji zarówno w sposób aktywny, jak pasywnie, w odniesieniu do szerokiego spektrum potencjalnych obiektów rozpoznania. Adaptacyjność platform i modułów bojowych będących organami wykonawczymi sieci sił powietrznych wymuszać będzie zwiększenie stopnia ich przystosowania do autonomicznego funkcjonowania na polu walki w określonym dla poszczególnych środkach rażenia ogniowego i elektronicznego zakresie⁹⁷.

Ważne dla użycia sił powietrznych w środowisku sieciocentrycznym będzie przystosowanie ich obecnych i perspektywicznych systemów uzbrojenia, sprzętu i wyposażenia do spełniania wymogu łatwości wykorzystywania. Biorąc pod uwagę zasady prowadzenia walki sieciocentrycznej łatwość wykorzystania będzie związana bezpośrednio z szeregiem atrybutów cechujących systemy uzbrojenia, sprzęt i wyposażenie sił powietrznych. Atrybuty te mogą obejmować⁹⁸:

- zdolność do funkcjonowania w szerszej architekturze systemowej i działania modułowego (scalable);
- zdolność do rekonfiguracji (reconfigurable);

⁹⁷ *Jumper on Airpower*, w: Air Force Magazine on Line, 2000, Vol. 83, No. 7, dostępne z: www.afa.org/magazine/July2000/07000jumper.asp

⁹⁸ *Net-Centric Environment. Joint Functional Concept*, op. cit., s. 28-29.

- możliwość kontroli (controllable)
- łatwość utrzymywania w sprawności technicznej (maintanable);
- podatność modernizacyjną (upgradeable);
- łatwość naprawy (repairable).

Zauważyć należy, że atrybuty powyższe są pochodną wysokiego stopnia interoperacyjności technicznej systemów uzbrojenia, sprzętu i wyposażenia sił powietrznych z analogicznymi systemami pozostałych rodzajów sił zbrojnych oraz siłami sojuszników potencjalnych koalicjantów. Analiza rozwiązań technologicznych przewidywanych do wprowadzenia w siłach powietrznych państw, które realizują transformacje sił zbrojnych zgodnie z założeniami walki sieciocentrycznej wskazują, że jednymi z kluczowych atrybutów są zdolność do rekonfiguracji i podatność modernizacyjna.

Obecny i przewidywany rozmach przestrzenny użycia sił powietrznych wymagał będzie bowiem współpracy z sensorami innych rodzajów sił zbrojnych oraz wykorzystania lokalnych sieci do współdziałania z siłami w rejonie realizacji zadań bojowych. Wzrastać powinny wymagania w stosunku do zdolności autonomicznego użycia na sieciocentrycznym polu walki platform bojowych, modułów taktycznych oraz środków rozpoznania sił powietrznych.

Z punktu widzenia długofalowego utrzymania zdolności do użycia w warunkach dynamicznie zmieniającego się pola walki bezwzględnie wymaganym atrybutem systemów uzbrojenia, sprzętu i wyposażenia sił powietrznych musi być ich podatność modernizacyjna. Pozwalać ona będzie na dokonywanie w ciągu cyklu użytkowania szeregu modernizacji o zakresie i charakterze adekwatnym do zmieniających się wymagań operacyjnych. Podatność modernizacyjna jako wymóg determinujący możliwości użycia sił powietrznych na sieciocentrycznym polu walki powinna być postrzegana jako element wydłużenia okresu użytkowania danego systemu oraz rozszerzenia elastyczności jego użycia. Ze względu na długotrwałość rozwijania technologii militarnych, celowe jest poszukiwanie dostępnych na rynku technologii komercyjnych, które mogą być wykorzystane do zapewnienia użycia systemów uzbrojenia, sprzętu i wyposażenia sił powietrznych w warunkach sieciocentrycznego pola walki. Charakter zagrożeń bezpieczeństwa oraz położenia geograficzne ich źródeł powodują, że wzrasta coraz wyraźniej wymóg zdolno-

ści do użycia w działaniach ekspedycyjnych wydzielonych komponentów sił zbrojnych. Wymóg ten ze względu na charakter zadań sił powietrznych jest szczególnie mocno zaakcentowany w stosunku do lotnictwa sił powietrznych oraz elementów zabezpieczających jego użycie. W świetle wyników analiz amerykańskich wymagań w stosunku do technicznych rozwiązań umożliwiających prowadzenie walki sieciocentrycznej można przyjąć, że formułowanie wymagań dla sił powietrznych w aspekcie ich użycia na sieciocentrycznym polu walki w operacjach o charakterze ekspedycyjnym powinno uwzględnić spełnianie przez systemy uzbrojenia, sprzęt i wyposażenie standardów w zakresie⁹⁹:

- zdolności do przetrzutu do rejonu operacji (deployable);
- zdolności do samodzielnej realizacji manewru (maneuverable);
- modułowości (modular);
- przystosowania do transportu na obszarze operacji (transportable);
- zdolność do funkcjonowania w niekorzystnych warunkach geograficznych i klimatycznych (rugged);
- zdolności do funkcjonowania z rozmachem przestrzennym adekwatnym do realizowanych zadań (reach);
- łatwości osiągania zdolności bojowych po transporcie do rejonu operacji (employable);
- podatności na utrzymanie ciągłości działania (sustainable).

O ile samoloty lotnictwa sił powietrznych mogą samodzielnie realizować przetrzut do rejonu operacji, to siły je zabezpieczające oraz moduły bojowe innych rodzajów wojsk sił powietrznych będą wymagały przetransportowania tam drogą powietrzną, morską bądź lądową. To właśnie w stosunku do nich winny być precyzyjnie określone standardy zdolności do przetrzutu i przystosowania do transportu na obszarze operacji. Pożądane jest zwiększenie zdolności systemów uzbrojenia i sprzętu sił powietrznych do samodzielnej realizacji manewru na sieciocentrycznym polu walki, co przekładałoby się na zwiększenie elastyczności ich operacyjnego użycia, a także zmniejszałoby potrzeby transportu na obszarze operacji.

⁹⁹ Tamże, s. 29.

W świetle wyników uzyskanych w trakcie studiów dostępnych materiałów źródłowych można stwierdzić, że użycie sił powietrznych w operacjach o charakterze ekspedycyjnym, w warunkach sieciocentrycznego pola walki wymagać będzie spełnienia wymogów modularności przez siły wydzielone do takich operacji. Platformy bojowe, moduły taktyczne oraz środki rozpoznania ze składu sił powietrznych przewidywane do użycia w operacjach o charakterze ekspedycyjnym winny posiadać zdolność do automatycznego wpinania się w doraźnie tworzone systemy sieciocentryczne o różnorodnej architekturze i przeznaczeniu¹⁰⁰.

Rozważyć należy określenie wymagań dla systemów uzbrojenia i sprzętu sił powietrznych w zakresie osiągania zdolności bojowych po przetransportowaniu do rejonu operacji oraz poziomu zabezpieczenia, jaki będzie niezbędny dla utrzymania ciągłości ich działania.

Jakość rozwiązań technicznych warunkujących użycie sił powietrznych w warunkach sieciocentrycznego pola walki jest postrzegana w amerykańskich koncepcjach funkcjonowania sił zbrojnych w środowisku sieciocentrycznym głównie poprzez pryzmat jakości informacji. Transformując zawarte w dokumencie „Net-Centric Environment. Joint Functional Concept” zapisy na wymagania w stosunku do sił powietrznych w aspekcie ich funkcjonowania w ramach sieciocentrycznego pola walki można założyć, iż jakość rozwiązań technicznych powinna zapewnić przede wszystkim:

- dokładność realizacji zakładanych funkcji (accurate);
- podatność na obserwację realizowanych funkcji (traceable);
- kompletność oferowanych rozwiązań (complete);
- wewnętrzną spójność i zgodność realizacji zakładanych funkcji (consistent);
- terminowość realizacji zakładanych funkcji (timely).

W amerykańskiej filozofii tworzenia wymagań w stosunku do rozwiązań technicznych na potrzeby prowadzenia walki sieciocentrycznej zwraca się uwagę na zakres wymagań w odniesieniu do realizacji określonej funkcji (integrated). Za-

¹⁰⁰ D. A. Deptula, *Air Force Transformation: Past, Present and Future*, w: *Aerospace Power Journal* Fall 2001, dostępne z: www.airpower.maxwell.af.mil/airchronicles/apj/apj01/fal01/phifal01.html

kłada się, że zintegrowane wymagania w stosunku do rozwiązań technicznych powinny cechować się:

- interoperacyjnością (interoperable);
- dostępnością (accessible);
- przejrzystością dostępu (visible);
- łatwością wykorzystania (usable).

Działanie w środowisku sieciocentrycznym będzie wymagać od sił powietrznych osiągania i utrzymania określonego poziomu inteoperacyjności z siłami współdziałającymi. Poziom ten, jak wskazują wstępne badania nie musi być jednakowy dla wszystkich elementów składowych sieci sił powietrznych. W świetle rozwiązań stosowanych w siłach powietrznych Sojuszu Północnoatlantyckiego można założyć, że dla sił wydzielonych do operacji o charakterze ekspedycyjnym pożądany poziom integracyjności powinna stanowić wspólność (community) rozwiązań technicznych i organizacyjnych. W przypadku elementów sieci sił powietrznych przewidywanych do użycia na obszarze kraju nie ma potrzeby spełniania przez nie kryterium inteoperacyjności na poziomie wspólności, ale wystarczającą będzie kompatybilność rozwiązań technicznych oraz odpowiednie wyszkolenie personelu gwarantujące inteoperacyjność współdziałających sił. Ważnym wymaganiem dla docelowych rozwiązań technicznych implementowanych w celu zapewnienia zdolności sił powietrznych do ich użycia na sieciocentrycznym polu walki powinna stać się łatwość wykorzystania. Łatwość wykorzystania, mierzona stopniem przygotowania stanów osobowych do wykorzystania rozwiązań technicznych wpływać będzie bowiem na zakres kształcenia i szkolenia niezbędnego do pełnego wykorzystania możliwości dostępnych dzięki technologiom sieciocentrycznym.

3.4. Wnioski

Podsumowując badania przeprowadzone w rozdziale trzecim podkreślić należy, że funkcjonowanie sił powietrznych na sieciocentrycznym polu walki wymaga spełnienia szeregu wymagań, które w swojej istocie są spójne i często tożsame z wymaganiami wobec innych uczestników walki zbrojnej w wymiarze sieciocen-

trycznym. Oznacza to, że siły powietrzne, oprócz posiadania odpowiednich sił i środków w postaci sensorów dostarczających informacje oraz różnego typu i rodzaje platform bojowych będą musiały posiadać infrastrukturę umożliwiającą łączenie we wspólną sieć środków zdobywania informacji, decydentów oraz wykonawców. Będzie to możliwe po uzyskaniu zdolności do łączenia w sieć oraz wymiany informacji, do przetwarzania tej informacji w wiedzę umożliwiającą podejmowanie racjonalnych decyzji oraz osiąganiu zdolności do realizacji zadań na sieciocentrycznym polu walki. Wymagania wobec sił powietrznych w kontekście ich użycia na sieciocentrycznym polu walki powinny być spełnione w trzech płaszczyznach (domenach) – informacyjnej, społeczno-poznawczej i fizycznej.

W odniesieniu do domeny informacyjnej sił powietrznych wymagania dotyczą zarówno połączeń w sieci jak i węzłów sieci. Połączenia w sieci ocenia się przez ich zasięg (rozległość), stopień zwielokrotnienia (redundancji), zapewnienie terminowości i bezpieczeństwa informacji. Natomiast wymagania w stosunku do węzłów sieci ocenia się przez pryzmat czasu dostępu w sieci, ilości i rodzaju użytkowników – uczestników walki sieciocentrycznej, ilości połączeń z innymi węzłami oraz dostępność informacji w węźle i jego bezpieczeństwo.

Rozległość sieci musi być adekwatna do wielkości i charakteru prowadzonej operacji oraz wielkości komponentu powietrznego. Szczególnie podczas operacji reagowania kryzysowego zasięg sieci musi zapewnić realizacji zadań na sieciocentrycznym polu walki również poza obszarem Sojuszu.

Węzły sieci tworzyć będą trzy rodzaje użytkowników: decydenci, wykonawcy i dostarczyciele danych. W odniesieniu do węzłów sieci tworzonych przez środki przekazywania informacji spełnione muszą być wymagania dotyczące czasu dostępu, zakresu dostępności informacji oraz żywotności. W przypadku naziemnych środków zdobywania informacji, np.: stacji radiolokacyjnych wstępnego wykrywania systemu obrony powietrznej, połączonych siecią łączności przewodowej ważnym wymaganiem będzie możliwość zwielokrotnienia połączeń danego węzła z siecią w celu zwiększenia dostępności informacji. Z kolei w odniesieniu do powietrznych sensorów, powietrznych środków rozpoznania takich jak: załogowe i bezzałogowe statki powietrzne, samoloty obserwacji powietrznej typu AWACS i JSTARS węzły sieci muszą być zdolne do odbioru informacji z tych środków.

Ważnym wymaganiem jakie spełnić powinna domena informacyjna sił powietrznych jest kategoryzacja uprawnień poszczególnych użytkowników w zakresie funkcji realizowanych w ramach współdziałania z innymi użytkownikami. Oznacza to potrzebę stworzenia wirtualnych podsieci w oparciu o hierarchię (miejsce i rolę) określonych użytkowników w realizacji określonych zadań.

Z analizy procedur funkcjonowania sił powietrznych wynika, że niezbędne jest, aby zapewnić bardzo restrykcyjną kontrolę dostępu do sieci i do danych sieci. Niezbędne też jest zapewnienie odpowiednich procedur odtwarzania zdolności sieci do funkcjonowania po wykonaniu na nią uderzeń ogniowych bądź elektro-nicznych.

Przeprowadzone badania wskazują, że strukturę powiązań hierarchicznych i horyzontalnych powinna cechować otwartość i elastyczność, które zapewnią do-rażne, adekwatne do potrzeb konfigurowanie sieci.

Niezbędne też jest zapewnienie terminowości w funkcjonowaniu domeny in-formacyjnej. Połączenia w sieci powinny zapewnić dostęp do i wymianę informacji we właściwym czasie oraz jej bezpieczeństwo adekwatnie do potrzeb określonych użytkowników sieci wynikających z pełnionych przez nich funkcji.

Jednak najważniejszym kryterium, jakie musi spełnić domena informacyjna sił powietrznych jest osiągnięcie interoperacyjności przez wszystkich użytkowni-ków sieci, rozumianej jako zdolność do wspólnego działania.

Jakościowo nowy dostęp do informacji na wszystkich szczeblach dowodze-nia sił powietrznych oraz w każdym etapie cyklu decyzyjnego tworzy sytuację, gdzie użytkownicy sieci stają się nie tylko odbiorcami, ale i twórcami informacji. Przez to indywidualni użytkownicy sieci wchodzi w interakcje społeczne z innymi użytkownikami działając jako twórcy i konsumenci informacji, ale także jako mani-pulatorzy (przetwarzający) informacji. To powoduje, że niezbędne jest spełnienie szeregu wymagań w odniesieniu do domeny społeczno-poznawczej sił powietrz-nych. Domena ta powinna być w przeważającej mierze determinowana zdolno-ściami i atrybutami w obszarze wiedzy, bowiem właśnie w nim zachodzić będą interakcje pomiędzy indywidualnymi i zbiorowymi uczestnikami walki sieciocen-trycznej.

Personel sił powietrznych zaangażowany w działania na sieciocentrycznym polu walki powinien posiadać umiejętność tworzenia odpowiednich relacji organizacyjnych, współdziałania, zespołowego planowania i podejmowania decyzji, a także umiejętność dzielenia się świadomości sytuacji na polu walki z innymi użytkownikami oraz do kooperacji pozytywnej w ramach samosynchronizacji działań.

W związku z tym, iż w środowisku sieciocentrycznym współdziałanie rozproszonych geograficznie organów dowodzenia ze wszystkimi siłami uczestniczącymi w walce będzie musiało się charakteryzować ciągłością, to będzie to miało wpływ na permanentną zmianę i doskonalenie istniejących struktur organizacyjnych.

Niezbędne też będzie, aby w warunkach sieciocentrycznego pola walki wypracować i wdrożyć procedury umożliwiające samosynchronizację działań podstawowych modułów operacyjnych w celu szybszego reagowania na zmiany na polu walki i działania przeciwnika.

W środowisku sieciocentrycznym w procesie podejmowania decyzji, dowódcy będą w zdecydowanie większym niż obecnie zakresie konsultować się z innymi dowódcami lub osobami odpowiedzialnymi za kierowanie w różnych sferach walki sieciocentrycznej.

Powyższe uwarunkowania spowodują, że konieczne będzie szersze ujęcie w doktrynie sił powietrznych roli informacji w działaniach sieciocentrycznych. Rozwiązania taktyczne będą także musiały uwzględnić wzrost możliwości bojowych wynikających ze stosowania rozwiązań sieciocentrycznych.

Przygotowanie sił powietrznych do funkcjonowania w warunkach sieciocentrycznego pola walki wymaga intensyfikacji szkolenia indywidualnego i zbiorowego oraz dokonania zmian i przewartościowań w kształceniu i szkoleniu personelu. Jest wskazane, aby ćwiczenia sił powietrznych w znacznym stopniu ukierunkować na współdziałanie z siłami i organami dowodzenia pozostałych rodzajów sił zbrojnych oraz organizacjami uczestniczącymi w walce sieciocentrycznej.

Zgromadzenie odpowiedniej wiedzy oraz jej twórcze wykorzystanie, a także odpowiednie przygotowanie dowódców i wszystkich uczestników walki sieciocen-

trycznej będzie zasadniczym wymaganiem w odniesieniu do domeny społeczno-poznawczej.

W odniesieniu do domeny fizycznej walki sieciocentrycznej wymagania powinny być ukierunkowane na osiągnięcie i doskonalenie tych cech zgrupowań taktycznych (modułów bojowych), organów dowodzenia oraz środków rozpoznania sił powietrznych, które umożliwiają ich użycie na sieciocentrycznym polu walki. Te pożądane cechy to osiągnięcie zdolności do przerzutu do rejonu operacji i manewru na polu walki, zdolności do przetwarzania oraz do podtrzymywania ciągłości działań. Są one pochodną założeń uzyskania zdolności do działań poza obszarem Sojuszu oraz wysokiej efektywności działań przy minimalnych stratach własnych.

Do wymagań w ramach tej domeny należy też zaliczyć takie wymagania techniczne jak: wysoka niezawodność i pewność wykorzystania, wysoka adaptacyjność do nowych uwarunkowań, wysoką jakość i zdolność do działań o charakterze ekspedycyjnym.

Z koncepcji oraz rozmachu przestrzennego użycia sił powietrznych na sieciocentrycznym polu walki wynika, że konieczna będzie też współpraca z sensorami innych rodzajów sił zbrojnych oraz współdziałanie z lokalnymi sieciami w rejonie wykonania zadań bojowych. Jednocześnie należy dążyć do tego, aby platformy bojowe, środki rozpoznania i moduły bojowe były też zdolne do autonomicznego użycia.

Z faktu, że systemy uzbrojenia, wyposażenia i sprzęt bojowy muszą spełniać wysokie wymagania, aby mogły być użyte na sieciocentrycznym polu walki wynika, że technika ta jest bardzo droga. Dlatego niezbędne jest, aby była podatna na modernizację w celu dostosowania do nowych wymagań operacyjnych w długim okresie.

Reasumując badania, których rezultaty są przedstawione w rozdziale trzecim można stwierdzić, że aby siły powietrzne mogły być użyte zgodnie z koncepcją funkcjonowania sieciocentrycznego pola walki muszą spełniać szereg bardzo ważnych i trudnych wymagań. Dlatego perspektywa wdrożenia takich rozwiązań musi być rozłożona na kilka najbliższych dekad. Wymagać też będzie znacznego wysiłku intelektualnego i finansowego.

ZAKOŃCZENIE

Przełom XX i XXI wieku przyniósł nowe zagrożenia i wyzwania w obszarze bezpieczeństwa. Są one pochodną procesów politycznych zachodzących w świecie. Jednocześnie następuje ogromny skok technologiczny, który obejmuje wszystkie sfery życia. W obszarze bezpieczeństwa przewartościowaniom ulegają koncepcje, funkcje i sposoby wykorzystania sił zbrojnych. W Sojuszu Północnoatlantyckim zmiany te są szczególnie widoczne. Obecnie siły zbrojne państw NATO, nie są przygotowywane do konfrontacji totalnej, lecz do zapobiegania i zarządzania kryzysami, a w ostateczności do obrony własnego terytorium. A ponieważ kryzysy najczęściej powstają poza terytorium Sojuszu, to siły zbrojne muszą być mobilne i gotowe do sprostania nowym wyzwaniom.

Rozwój technologii, szczególnie w zakresie zbioru, analizy, dystrybucji i wykorzystania informacji spowodował, że powstają nowe koncepcje prowadzenia działań militarnych. Do rozwiązywania kryzysów wydziela się odpowiednie siły zadaniowe, które mają działać według nowej filozofii prowadzenia walki zbrojnej. Tą nową filozofią jest koncepcja sieciocentrycznego pola walki oraz walki sieciocentrycznej. W walce tej uczestniczą komponenty wydzielane z wszystkich rodzajów sił zbrojnych, w tym z sił powietrznych. Koncepcja walki sieciocentrycznej nie jest powszechnie znana i w pełni stosowana. Dlatego badania prezentowane w niniejszym studium zapoczątkowały proces naukowego podejścia do poznania problematyki użycia sił powietrznych w warunkach sieciocentrycznego pola walki.

Koncepcja walki sieciocentrycznej bazuje na nowej filozofii myślenia i oznacza koncepcję prowadzenia operacji militarnych opierającej się na przewadze informacyjnej. Koncepcja ta zakłada osiągnięcie, poprzez połączenie w sieć informacyjną sensorów, decydentów i systemów walki, świadomości sytuacyjnej oraz zwiększenie tempa i skuteczności działań militarnych.

Przeprowadzone badania dowiodły, że siły powietrzne spełniać będą znaczącą rolę w walce sieciocentrycznej, ze względu na swoje właściwości, takie jak globalny zasięg, szybkość działania i skuteczność, łatwość dostępu z powietrza. Na sieciocentrycznym polu walki wykorzystywane będą naziemne i powietrzne

sensory, platformy bojowe oraz elementy sieci informacyjnej ze składu sił powietrznych.

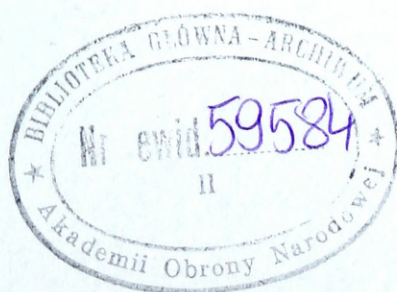
Badania ukierunkowane przedstawionymi we wstępie założeniami badawczymi pozwoliły na rozwiązanie problemów badawczych oraz osiągnięcie celu badań. Badania prowadzone różnymi metodami potwierdziły podstawowe założenia hipotez roboczych. Niniejsze studium teoretyczne stanowi pierwszą część zadania badawczego "Siły powietrzne w warunkach sieciocentrycznego pola walki". Ustalenia zawarte w pracy a dotyczące wymagań wobec sił powietrznych w aspekcie ich użycia na sieciocentrycznym polu walki stanowić będzie podstawę merytoryczną do dalszych badań i opracowania kolejnych części zadania badawczego.

BIBLIOGRAFIA

1. Alberts D., Garstka J., Hayes R., Signori D., *Understanding Information Age Warfare*, 2001.
2. Alberts D., Garstka J., Stein F., *Network Centric Warfare*, DoD C4ISR Cooperative Research Program, 2000.
3. Associated Press, *Boeing Bets on „Net-Centric” Warfare*, dostępne z: www.siliconvalley.com
4. Barnett T., *The Seven Deadly Sins of Network – Centric Warfare*, dostępne z: www.nwc.navy.mil/newrulesets/default.htm
5. Barnett T., *The Seven Deadly Sins of Network – Centric Warfare*, dostępne z: www.nwc.navy.mil/newrulesets/default.htm
6. *Boeing Bets on „Net-Centric” Warfare*, dostępne z: www.siliconvalley.com
7. Borgu A., *The Challenges and Limitations of „Network Centric Warfare” – the initial views of an NCW sceptic*, Australian Strategic Policy Institute, 2003.
8. Cebrowski A., Garstka J., *Network Centric Warfare – Its Origins and Future*, Proceedings of the Naval Institute, 1998.
9. Cebrowski A., *The Power of Information Comes from the Ability to Share*, w: *Defender*, Vol. 2. No. 3, 2005, s. 2-3, dostępne z: www.oft.osd.mil/library/library-files/article_448_Defeder-NetCentric.pdf
10. Coleman K., *Network Centric Warfare*, dostępne z: www.directionsmag.com
11. *Concept for Future Joint Operations*, Joint Chiefs of Staff, 1997.
12. Davis P. K., i in., *Transforming the Force. Suggestions for DoD Strategy*, Issue Paper, Rand National Defense Research Institute, 1998, dostępne z: www.rand.org/publications/IP/IP179/index.html
13. Deptula D. A., *Air Force Transformation: Past, Present and Future*, w: *Aerospace Power Jurnal* Fall 2001, dostępne z: www.airpower.maxwell.af.mil/airchronicles/apj/apj01/fal01/phifal01.html

14. Deptula D. A., *Effects-Based Operations: Change in the nature of war*, Aerospace Education Foundation, 2001.
15. *Firmowe porozumienie na NCW*, Lotnictwo Wojskowe nr 11/2004.
16. *Information Superiority and NATO Network – Enabled Capability. Fact Sheet*, Allied Command Transformation, 2005, dostępne z:
<http://specials.ft.com/ftit/october2000/FT3Wzevdc.html>
17. *Jumper on Airpower*, w: Air Force Magazine on Line, 2000, Vol. 83, No. 7, dostępne z: www.afa.org/magazine/July2000/07000jumper.asp
18. Konopka L., *Walka sieciocentryczna sposobem działania sił zbrojnych w przyszłości*, Myśl Wojska nr 2/2004.
19. M. Bruno, *Western Iraq Most Networked In History of War*, Official Says, w: Aerospace Daily and Defense Report, 2005, dostępne z:
[www.oft.osd.mil/library/library-files/article_473_Aerospace %20Daily.doc](http://www.oft.osd.mil/library/library-files/article_473_Aerospace%20Daily.doc)
20. Ministry of Defence, *The New Defence – Prepared for the Next Millenium*, 1999.
21. Money A., *Report on Network Centric Warfare*, Sense of the Report, 2001.
22. Mordawski H., *Z dziejów radiolokacji, cz. II*, Wiraże nr 18/2004.
23. Munk S., *Walka sieciocentryczna a interoperacyjność informacyjna*, Myśl Wojskowa nr 6/2004.
24. *NCW Roadmap*, Australian Government, Department of Defence, 2005.
25. *Net-Centric Environment. Joint Functional Concept Vision 1.0*, Department of Defense, 2005.
26. *Net-Centric Operations*, Aviation Week and Space Technology Market Supplement, 2003.
27. *Network Centric Operations Conceptual Framework Version 2.0*, EBR, 2004.
28. *Network-Based Operations for the Swedish Defence Forces: An Assessment Methodology*, RAND Corporation, 2002.
29. *Networked Enabled Capability. An Introduction*, UK MOD, 2004.

30. Phister P., Plonisch I., *Military Applications of Information Technologies*, Air and Space Power Journal, 2004.
31. *Revolution in Military Affairs – the Swedish Programme*, w: Swedish Journal of Military Technology, Vol. 3, 2000.
32. *Słownik wyrazów obcych*, PWN, 1980.
33. *Sweden's revolution in military affairs*, Financial Times, 2000, dostępne z: <http://specials.ft.com/ftit/october2000/FT3Wzevdc.html>
34. Szpakowicz R., *Wojna w Iraku a koncepcja wojny sieciocentrycznej*, Przegląd Wojsk Lotniczych i Obrony Powietrznej nr 11/2003.
35. *The Implementation of Network Centric Warfare*, DOD Office of Force Transformation, 2005.
36. *The US Force Transformation Flight Plan*, HQ USAF/XPXC, 2004.
37. www.b2ncw.com/index.php
38. www.directionsmag.com/images/articles/coleman/ncw/ncw3.gif
39. www.dtic.mil/jsc/j6/education/warfare.html
40. YDP – *Collins English Polish Dictionary*.



s/6432
11,80