

## THE AIR FORCE NETWORK CENTRIC MANAGMENT

### SIECIOCENTRYCZNE ZARZĄDZANIE SIŁAMI POWIETRZNYMI

**Bogdan Grenda**

Akademia Obrony Narodowej  
[b.grenda@aon.edu.pl](mailto:b.grenda@aon.edu.pl)

**Abstract:** *The requirements of the modern battlefield are the crucial cause of building a wide range of flying platforms, where weapons and sensors are combined into one common information exchange network. Therefore, the article is attempt to identify the phenomenon of network centrality in the Polish Air Force (POLAF) and to review technical solutions to enable the functioning of the POLAF in these conditions. Furthermore, the author has analyzed the functioning of the POLAF management system in terms of network centric system, and formulated the requirements to ensure its improvement.*

**Keywords:** *Network centric, managment, command, air force*

**Streszczenie:** *Wymagania współczesnego pola walki stanowią główną przyczynę budowy szerokiej gamy platform latających, na których uzbrojenie i sensory łączone są w jedną wspólną sieć wzajemnej wymiany informacji. Artykuł stanowi, zatem próbę zidentyfikowania zjawiska sieciocentryczności w SP oraz dokonania przeglądu rozwiązań technicznych umożliwiających funkcjonowanie SP w tych warunkach. Ponadto, autor dokonał analizy funkcjonowania systemu zarządzania SP w warunkach sieciocentrycznych oraz sformułował wymagania zapewniające jego doskonalenie.*

**Słowa kluczowe:** *Sieciocentryczność, zarządzanie, dowodzenie, siły powietrzne*

## 1. Wstęp

Od zarania wieków teoretycy sztuki wojennej poszukują odpowiedzi na pytanie, jak skutecznie oddziaływać informacyjnie na przeciwnika, dezorganizować jego systemy informacyjne oraz chronić sprawność systemów własnych. Poszukiwania te doprowadziły do wypracowania nowej koncepcji walki sieciocentrycznej, która bazuje na nowym sposobie myślenia – myśleniu sieciocentrycznym. Nowa koncepcja walki wykorzystująca informację, zapoczątkowana została w Siłach Zbrojnych Stanów Zjednoczonych w latach 90 - tych<sup>1</sup>. Bazowała na zjawisku osiągania ekonomicznej przewagi lansowanej w biznesie i polegającej na uzyskaniu, gromadzeniu, analizowaniu i wykorzystaniu informacji w celu osiągnięcia zwycięstwa w rywalizacji pomiędzy firmami. Doświadczenia sektora komercyjnego stały się podstawą do adaptacji pojęcia przewagi informacyjnej dla potrzeb wojska. Traktując siły zbrojne jako przedsiębiorstwo, dostrzeżono możliwość podobnego zwiększenia efektywności poprzez radykalne poprawienie relacji „zaangażowane siły – uzyskany efekt (taktyczny, operacyjny, strategiczny)”. Zdolność do wykorzystania informacji tworzących wspólną sytuację operacyjną (Common Operational Picture – COP), dała możliwość działania z niezwykłą skutecznością oraz pozwoliła na wykorzystanie efektu synergii. Stało się to w wyniku transformacji tradycyjnych systemów dowodzenia, wykrywania i śledzenia dokonywanej zgodnie z nową koncepcją walki sieciocentrycznej (Network Centric Warfare - NCW)<sup>2</sup>. Szczególnie koncepcja NCW wpływa na rozwój i funkcjonowanie Sił Powietrznych, jednym z najbardziej zaawansowanych technologicznie rodzajów Sił Zbrojnych. Doświadczenia wyniesione z konfliktów zbrojnych w Iraku i Afganistanie jednoznacznie wskazują, iż skuteczne użycie SP w operacji wymagać będzie wysokiej sprawności realizacji procesu dowodzenia i warunkowane będzie, między innymi, dostępnością zaawansowanych technologicznie środków dowodzenia. Stąd, *celem niniejszego artykułu jest ustalenie możliwości zarządzania SP w warunkach sieciocentrycznych.*

Autor artykułu założył, że osiągnięcie tak sformułowanego celu będzie wymagało znalezienia odpowiedzi na pytanie, stanowiące problem ogólny artykułu: jak zorganizowany jest system zarządzania SP i jakie musi spełniać on wymagania, aby sprostać wymaganiom sieciocentrycznego pola walki?

---

<sup>1</sup> W roku 1998 po raz pierwszy użyto określenia Network Centric Warfare oraz przedstawiono nowy sposób prowadzenia działań militarnych w erze społeczeństw informacyjnych, podkreślając rolę technologii informacyjnych w podejmowanych działaniach. Źródło: A. Cebrowski, J. Garstka, *Network Centric Warfare . Its Origins and Future*, Proceedings of the Naval Institute, 1998.

<sup>2</sup> W literaturze przedmiotu znaleźć można różne tłumaczenia nazwy Network Centric Warfare np: „wojna sieciowa”, „walka sieciowa”, „walka sieciocentryczna”. W polskich publikacjach najczęściej spotyka się określenie „walka sieciocentryczna”, dlatego też, to pojęcie będzie używane w dalszej części artykułu na określenie oryginalnej nazwy koncepcji NCW.

Dążąc do osiągnięcia tak sformułowanego problemu badawczego, zasadnym jest odpowiedzieć na szereg pytań:

- Jak identyfikowane jest zjawisko walki sieciocentrycznej?
- Jak wygląda architektura sieciocentryczna Sił Powietrznych?
- Jak realizuje się zarządzanie Siłami Powietrznymi w warunkach sieciocentrycznych?
- Jakie wymagania powinien spełnić system zarządzania SP, aby realizował efektywnie swoje zadania na współczesnym polu walki?

## 2. Pojęcie walki sieciocentrycznej

Walka sieciocentryczna (Network Centric Warfare) 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, skuteczności uzbrojenia, odporności na uderzenia przeciwnika oraz stopnia synchronizacji działań<sup>3</sup>. Działania sieciocentryczne przekładają zatem, przewagę informacyjną na siłę bojową poprzez wydajne połączenie na polu (w przestrzeni) walki różnych jednostek organizacyjnych dysponujących wiedzą. Z kolei jako sieciocentryczne pole walki należy rozumieć przestrzeń, która obejmuje powietrze i przestrzeń kosmiczną, ląd, wodę, a także siły i środki własne i przeciwnika, pogodę, teren i spektrum elektromagnetyczne w obszarze działań oraz w obszarze zainteresowań<sup>4</sup>. Analizując powyższe można stwierdzić, że koncepcja NCW zakłada znaczące zwiększenie zdolności sił zbrojnych do szybkiego i efektywnego wykorzystania wszystkich dostępnych sił i środków w celu wykonania postawionego zadania. Działanie to odbywa się w taki sposób, aby można było generować zwiększoną siłę bojową przez lepszą synchronizację efektów na polu walki, szybszy i efektywniejszy proces dowodzenia oraz zwiększoną zdolność przetrwania<sup>5</sup>. Zwiększenie zdolności bojowych wynika z możliwości osiągnięcia wysokiego stopnia integracji we wszystkich wymiarach przestrzeni bitewnej oraz jest skutkiem zastąpienia masy informacji i zdolności do przemieszczania informacji zamiast sił i środków. Do podstawowych czynników (filarów) NCW należą:

- działanie organizacji w ramach wydajnej i odpornej sieci - co umożliwia dzielenie się posiadaną informacją,
- dzielenie się informacją - zdecydowanie polepsza jej jakość, tworzy tzw. wspólną świadomość sytuacji<sup>6</sup>,

---

<sup>3</sup> Z. Smutniak, *Dowodzenie siłami powietrznymi w środowisku sieciocentrycznym*, AON, Warszawa 2008, s. 8.

<sup>4</sup> *Concept for Future Joint Operations*, Joint Chiefs of Staff, 1997, s. 83.

<sup>5</sup> E. Smith, *Effects Based Operations (EBO) . Applying Network Centric Warfare in peace, crisis and war*, CCRP 2002, s. 61.

<sup>6</sup> Shared situational awareness - to stan, w którym dwa lub więcej podmioty podobnie oceniają zaistniałą sytuację.

- wspólna świadomość sytuacji – umożliwia ścisłą współpracę i synchronizację działań oraz wpływa na zwiększenie szybkości procesu dowodzenia,
- połączenie wszystkich czynników – istotnie zwiększa efektywność działań.

Przestrzeń walki sieciocentrycznej jest bardzo złożona ze względu na swoją wielowymiarowość oraz dużą liczbę zróżnicowanych elementów ją tworzących. Nie ogranicza się ona do przestrzeni trójwymiarowej, rozciąga się również na spektrum elektromagnetyczne oraz tzw. przestrzeń informacyjną. Przestrzeń, w której toczy się walka sieciocentryczna, można podzielić na wiele sposobów. Najbardziej rozpowszechnione są podziały na domeny, warstwy i sieci.

Podział przestrzeni walki sieciocentrycznej na domeny wyszczególnia:

- domenę fizyczną,
- domenę informacyjną,
- domenę poznawczą.

**Domena fizyczna** obejmuje działania tradycyjne; w jej zakres wchodzi uderzenia, obrona i manewr we wszystkich wymiarach (lądowym, morskim, powietrznym i kosmicznym). W domenie fizycznej znajdują się stanowiska dowodzenia, systemy uzbrojenia i sieci, które je łączą. Głównymi parametrami oceny efektywności działań bojowych w tej domenie będą dwie zasadnicze miary zdolności bojowej: skuteczność rażenia i odporność (zdolność do przetrwania).

**Domena informacyjna** obejmuje tworzenie, przetwarzanie i współużytkowanie informacji. W domenie informacyjnej następuje wymiana informacji między siłami biorącymi udział w walce, komunikowanie się odpowiednich ośrodków dowodzenia i sztabów oraz przekazywanie intencji dowódców. Domena ta musi być szczególnie chroniona i broniona, gdyż jej wpływ na wzrost zdolności bojowych jest bardzo duży, szczególnie w walce o zdobycie przewagi informacyjnej.

**Domena poznawcza** istnieje jedynie w umysłach uczestników walki sieciocentrycznej. Jest ona trudna do zidentyfikowania, tworzą ją bowiem takie elementy, jak: przywództwo, morale, spójność jednostki (pododdziału), jakość wyszkolenia, świadomość sytuacji, a nawet opinia publiczna. W tej domenie umiejscowione są: zamiar działania, doktryna, taktyka działania, procedury postępowania. Kolejnym sposobem przedstawienia struktury przestrzeni walki sieciocentrycznej jest podział na:

- warstwę dowodzenia,
- warstwę walki,
- warstwę informacyjną,
- warstwę sensorów.

**Warstwa dowodzenia** jest tą częścią składową przestrzeni walki sieciocentrycznej, w której odpowiednio wyszkolony personel dokonuje oceny sytuacji, analizuje zadania, planuje działania i bezpośrednio zarządza walką, wykorzystując rozwinięte systemy dowodzenia. Istnienie warstwy dowodzenia umożliwia utrzymanie pełnej kontroli działań w walce sieciocentrycznej.

**Warstwa walki** (bezpośredniego zaangażowania) to samoorganizująca się sieć elementów ugrupowania bojowego [platformy uderzeniowe, ich załogi (obsługi), elementy logistyczne itd.], bazująca na bieżącej, wiarygodnej (pozyskiwanej w czasie rzeczywistym) wiedzy o sytuacji bojowej.

W **warstwie informacyjnej** korelowane są dane z sensorów, a informacja dostarczana jest do systemów walki wszystkich szczebli (stosownie do uprawnień poszczególnych użytkowników).

**Warstwa sensorów** składa się z licznych różnorodnych urządzeń rozpoznawczych (np. bezzałogowych aparatów latających, naziemnych stacji radiolokacyjnych, czujników ruchu), których zadaniem jest zbieranie informacji o sytuacji na lądzie, morzu, w powietrzu oraz w przestrzeni elektromagnetycznej. Najczęściej przyjmowanym, a zarazem najszerzej opisanym, sposobem podziału przestrzeni walki sieciocentrycznej jest podział na sieci (subsieci):

- informacyjną,
- czujników,
- dowodzenia.

**Sieć informacyjna** umożliwia wymianę, przetwarzanie, przechowywanie i ochronę informacji. Składa się ona z kanałów łączności, węzłów informatycznych, systemów operacyjnych i aplikacji zarządzania informacjami. Możliwości techniczne sieci informacyjnej pozwalają na wygenerowanie przez sieć czujników świadomości sytuacyjnej, co jest podstawą uzyskania przewagi informacyjnej. O świadomości sytuacyjnej można mówić wtedy, gdy osiągnięty zostaje odpowiedni poziom informacji o siłach własnych, przeciwnika oraz neutralnych.

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

Czujniki (sensory) peryferyjne umieszczone są w przestrzeni kosmicznej, powietrznej, na lądzie, na powierzchni wody i pod nią oraz w przestrzeni informatycznej (cyberprzestrzeni). Mogą być zainstalowane zarówno na specjalistycznych platformach rozpoznawczych, jak i na platformach bojowych.

Trzecim elementem składowym sieci umożliwiającej prowadzenie walki sieciocentrycznej jest **sieć dowodzenia**. Najogólniej mówiąc, jest to sieć zapewniająca dowodzenie platformami bojowymi (grupami platform, oddziałami itd.) w przestrzeni walki. Sieć ta umożliwia wykorzystanie świadomości przestrzeni walki przez zapewnienie działającym siłom możliwości wykonania manewru, precyzyjnego uderzenia, pełnowymiarowej ochrony oraz ześrodkowania

zasobów logistycznych w wymaganym miejscu i czasie. Sieć dowodzenia zapewnia: wyprzedzające planowanie, czyli zdolność przejęcia inicjatywy w celu uniknięcia bezpośredniej konfrontacji; właściwą reakcję i wykorzystanie nadarzających się korzystnych okoliczności, gdy bezpośrednia konfrontacja jest nieunikniona, a także przeprowadzenie działań koniecznych do tego, by własny proces planowania 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 sił (narodowych lub koalicyjnych); możliwość prowadzenia działań w deficycie czasu (np. zdolność do szybkiego podejmowania newralgicznych decyzji). W skład sieci dowodzenia, tak jak w skład czujników, wchodzi platformy bojowe (shooter peripherals) i oprogramowanie platform bojowych (shooter applications), które działają z wykorzystaniem sieci informacyjnej. Platformy bojowe są rozmieszczone w przestrzeni kosmicznej, powietrznej, na lądzie, morzu oraz w przestrzeni informatycznej (cyberprzestrzeni).

### **3. Sieciocentryzm w Siłach Powietrznych**

Siły Powietrzne przechodzą obecnie gruntowną i najkosztowniejszą transformację strukturalno – techniczną w skali Sił Zbrojnych RP. Wynika ona z wymagań współczesnego i przyszłego pola walki. Równoległe ze zmianami geopolitycznymi oraz cywilizacyjnymi przewartościowaniu ulegają również doktryny oraz koncepcje użycia Sił Powietrznych. Ich rola oraz zadania ewoluują. Siły Powietrzne chcąc realizować misje adekwatne do swojego potencjału bojowego i możliwości, muszą posiadać zdolności do wykonywania całego spektrum zadań samodzielnie, jak również jako część komponentu zadaniowego. Warunkiem sprawnego ich działania jest szybki i możliwie niezawodny przepływ informacji między elementami systemu dowodzenia i kierowania. Przyjęto, że nowoczesny system dowodzenia musi spełniać następujące wymagania:

- zapewniać optymalne wykorzystanie wszystkich podległych sił i środków w ramach jednolitego systemu;
- zapewniać skuteczne dowodzenie podległymi siłami i środkami na wszystkich kierunkach zagrożenia oraz doraźnie tworzonymi zgrupowaniami sił i środków na wybranym kierunku zagrożenia;
- mieć prostą i elastyczną strukturę (znaczące zmniejszenie liczby szczebli dowodzenia), odpowiednią do jednoznacznie określonych zadań i kompetencji dowódców poszczególnych komponentów oraz szczebli dowodzenia;
- zapewniać pełną interoperacyjność z systemami dowodzenia państw alianckich;
- umożliwiać w jak najszerszym zakresie wykorzystanie posiadanej przez komponenty sił połączonych infrastruktury.

Aby system dowodzenia i kierowania właściwie spełniał swoje funkcje, powinien być użyteczny dla korzystających z niego elementów bojowych, pozwalać na tworzenie wielu obwodów funkcyjnych oraz umożliwiać rozdzielanie informacji

między różne obszary w zależności od wykonywanych zadań i przeznaczenia. System musi być także dynamiczny – zdolny do reagowania na szybko zmieniającą się sytuację taktyczną. W celu obsługi bardzo rozproszonych jednostek mobilnych, mogących funkcjonować w różnych, często zmiennych obszarach i warunkach działania istnieje konieczność budowy systemu łączności, który będzie skupiał w sobie funkcje telekomunikacyjne, nawigacyjne oraz identyfikacyjne. Mogą to być systemy transmisji danych LINK. Systemy te, składające się z sieci terminali, tworzą cyfrowy, wielofunkcyjny system dystrybucji informacji (Multifunctional Information Distribution System – MIDS). Ponadto zapewnia on utajniony, odporny na zakłócenia transfer informacji w czasie rzeczywistym pomiędzy mobilnymi jednostkami różnych rodzajów wojsk, co jest zgodne z koncepcją walki sieciocentrycznej (NCW). System ten pozwala przewyciężyć szereg właściwych dla istniejących systemów ograniczeń, związanych z pojemnością, stopniem pokrycia obszaru, interoperacyjnością, żywotnością oraz odpornością na przeciwdziałanie, redukując do minimum niebezpieczeństwo utraty lub przeterminowania informacji. Należy podkreślić, że celem istnienia tego systemu nie jest zastąpienie klasycznej sieci łączności mobilnej, lecz jej uzupełnienie, szczególnie w zakresie współpracy różnych rodzajów wojsk i obsługi wysoce mobilnych jednostek na wszystkich szczeblach dowodzenia. Szczególnie operacje powietrzne obejmują wiele funkcji dowodzenia i kierowania (np. opracowywanie i dystrybucja zobrazowania sytuacji, system wskazywania celów, planowanie zadań, przygotowywanie i rozpowszechnianie rozkazów i meldunków), które w znacznym stopniu uzależnione są od systemu transmisji danych. Podstawowymi mechanizmami wykorzystywanymi do przesyłania informacji o śledzeniu celów są taktyczne łącza danych zwane taktycznymi systemami transmisji danych (w NATO określanymi Tactical Data Link1, a w USA – Tactical Digital Information Link – TADIL)<sup>7</sup>. Obecnie są używane następujące łącza informacyjne: Link 1, Link 4, Link 11/11b, Link 14, Link 16, Link 22 (w fazie prób eksploatacyjnych).

**Link 1** jest cyfrowym, dupleksowym łączem zaprojektowanym pod koniec lat 50. XX w. przez instytucje NATO do celów wymiany informacji typu punkt–punkt przez jednostki obrony powietrznej. Łącze miało zapewniać wymianę zobrazowania sytuacji powietrznej między centrami kierowania i meldowania (Control and Reporting Centre – CRC) a połączonymi centrami operacji powietrznych (Combined Air Operation Centre – CAOC) z prędkością 1200/2400 b/s. Łącze nie ma możliwości szyfrowania danych, a pojemność wiadomości serii S jest ograniczona do obrazu przestrzeni powietrznej i danych zarządzających transmisją. Państwa notowskie wykorzystują Link 1 głównie w systemach obrony powietrznej. W łącza tego typu nadal jest wyposażona większość mobilnych CRC. Państwa NATO mają w bazach lotniczych i centrach dowodzenia obroną przeciwlotniczą krótkiego zasięgu urządzenia do odbierania wiadomości serii S działające jako systemy wczesnego ostrzegania.

---

<sup>7</sup> *Understanding LINK-16*. Northrop Grumman, San Diego 2001, s.1–3.

**Link 4A (TADIL C)** jest używany do naprowadzania samolotów myśliwskich. Nie zapewnia bezpieczeństwa transmisji. Jest to łącze sieciowe, działające na zasadzie podziału czasu w paśmie UHF z prędkością 5000 b/s. Istnieją dwa oddzielne łącza tego typu: Link 4A i Link 4C. Link 4A odgrywa ważną rolę w systemie teleinformatycznym sojuszu – dostarcza siłom połączonym informację taktyczną w formacie cyfrowym w kierunku ziemia–powietrze, powietrze–ziemia i powietrze–powietrze. Link 4 zaprojektowano w celu zastąpienia komunikacji fonicznej używanej do naprowadzania lotnictwa taktycznego łącznością cyfrową. Z czasem zastosowanie tego łącza znacznie poszerzono, aż do wymiany danych cyfrowych między platformami powietrznymi a naziemnymi. Użyty po raz pierwszy w latach 50. ubiegłego wieku Link 4A jest traktowany jako łącze stosunkowo pewne, chociaż wiadomości nie są szyfrowane ani odporne na zakłócenia. Jest prosty w obsłudze – za jego pomocą łatwo nawiązać i utrzymać łączność. Link 4C służy do zapewnienia komunikacji między samolotami myśliwskimi. Pierwotnie miał uzupełniać Link 4A, mimo że te dwa rodzaje linków bezpośrednio nie komunikują się ze sobą. Link 4C używa wiadomości serii F i w pewnej mierze jest odporny na zakłócenia elektromagnetyczne. Pojedyncza sieć korzystająca z tego łącza jednocześnie może obsługiwać do czterech samolotów. W przyszłości planuje się zastąpienie łącza Link 4C łączem Link 16. Jednak wydaje się, że pozostawienie Link 4C w wyposażeniu samolotu będzie niezbędne ze względu na wykonywanie automatycznego sprowadzania samolotu do lądowania.

**Link 11/11B (TADIL A/B)** jest to półdupleksowe, sieciowe łącze, które normalnie działa przez cykliczne odpytywanie przez stacje sieci kontroli (net control station – NCS). Może działać także w trybie rozgłoszeniowym (broadcast). LINK 11 może prowadzić transmisję w pasmach fal krótkich (KF) oraz ultrakrótkich (UKF). Link 11 wykorzystuje sieciowe techniki komunikacyjne i standardowy format wiadomości w celu wymiany informacji w formacie cyfrowym między systemami powietrznymi, naziemnymi i morskimi na wysokiej i bardzo wysokiej częstotliwości. Łącze to jest używane również przez liczne systemy służące do rozpoznania i wywiadu elektronicznego. Zabezpiecza wymianę cyfrowej łączności radiowej między terminalami komputerowymi wchodzącymi w skład systemu. Link 11 bazuje na technologii pochodzącej z lat 60. XX w. i jest relatywnie wolnym łączem. Może także pracować w trybie rozgłaszania, w którym pojedyncza transmisja danych lub seria pojedynczych transmisji jest dokonywana przez jednego uczestnika. Dlatego Link 11 stanowi łącze półdupleksowe. Jest to łącze bezpieczne, ale podatne na zakłócenia elektromagnetyczne. Pozwala na wymianę danych o trasach powietrznych, nawodnych i podwodnych, danych z systemu wczesnego ostrzegania oraz danych dowodzenia między elementami systemu dowodzenia, ale nie pozwala na sterowanie statkami powietrznymi. Link 11B stosuje dedykowane łącza typu *point-to-point*, pełen dupleks, z użyciem szeregowej transmisji ramek oraz standardowych formatów depech. Informacje są przesyłane za pośrednictwem w pełni automatycznych łączy danych, pracujących



z fazą ciągłą, w pełnym duplexie, z kluczkowaniem częstotliwości, z prędkością 1200 b/s oraz możliwościami operacyjnymi 600 i 2400 b/s (lub wielokrotnością 1200 b/s, np. 3600, 4800).

**Link 16 (TADIL J)** jest to wielofunkcyjne, bezpieczne, odporne na zakłócenia łącze danych przeznaczone do wymiany wiadomości o ustalonym formacie i fonicznych z użyciem połączonego taktycznego systemu dystrybucji informacji lub równoważnych terminali. LINK 16 pracuje w paśmie częstotliwości 969 – 1206 MHz, gdzie posiada 51 częstotliwości pracy. LINK 16 nie różni się istotnie od podstawowej koncepcji cyfrowej wymiany informacji taktycznej, prowadzonej od wielu lat z użyciem standardów Link 4 i Link 11. Link 16 oferuje pewne techniczne i operacyjne usprawnienia w stosunku do obecnie wykorzystywanych standardów oraz uzupełnia ich niedoskonałości (np. odporność na zakłócenia, wzrost bezpieczeństwa transmisji, wzrost prędkości przesyłania danych, identyfikowanie źródła danych, wzrost ilości/rozdrobienie wymienianej informacji, ograniczenie rozmiaru terminala danych). Łącze może być instalowane w kabinach samolotów bojowych, zapewnia bowiem prowadzenie bezpiecznej łączności fonicznej, względne nawigowanie oraz identyfikowanie informacji o położeniu wszystkich jednostek uczestniczących w operacji. Za pomocą Link 16 są przekazywane informacje o zagrożeniach załogom samolotów będących poza zasięgiem wykrywania ich radarów pokładowych i ostrzegających. Łącze to zasadniczo nie zmienia podstawowych koncepcji i funkcji spełnianych przez Link 4A i Link 11 w zakresie C3I, natomiast zapewnia znaczące techniczne i operacyjne usprawnienia. Wyróżnikiem tego standardu jest Połączony System Dystrybucji Informacji Taktycznej (Joint Tacical Information Distribution System JTIDS). Zapewnia on wymianę komunikatów rozpoznawczych, sygnałów dowodzenia i kierowania między centrami C2 a różnymi systemami uzbrojenia. Umożliwia wielokrotny dostęp, ma dużą pojemność, jest odporny na zakłócenia, zapewnia dane w formacie cyfrowym danych, a także bezpieczną łączność foniczną, nawigację oraz identyfikowanie różnego rodzaju platform.

**LINK 22** (zwany również usprawnionym linkiem 11) jest utajnionym, odpornym na zakłócenia wielokanałowym cyfrowym informacyjnym łączem transmisji danych w relacjach radiowych KF i UKF. LINK ten wykorzystuje standard wiadomości z LINK 16. Proces ostatecznego zdefiniowania tego standardu jeszcze trwa, a jego implementacja jest w początkowej fazie. Zgodnie z założeniami projektantów Link 22 powinien zapewnić połączenie powietrznych, morskich, podwodnych i lądowych zautomatyzowanych systemów taktycznych w sposób umożliwiający skompilowanie wspólnego obrazu sytuacji taktycznej, zarządzanie statusem i użyciem systemów uzbrojenia oraz dowodzenie i kierowanie. Aby spełnić te wymagania, Link 22 musi funkcjonować niezależnie od wysokości nad poziomem morza, pokrywać obszar do 1000 MM oraz prawidłowo działać w środowisku WE.

Podobnie jak Link 16, Link 22 wykorzystuje technologię wielokrotnego dostępu z podziałem czasu (TDMA), zapewniającą:

- wydzielenie dla każdej jednostki konkretnych przedziałów czasowych;
- utworzenie przedziałów czasowych przeznaczonych dla wiadomości o wysokim priorytecie;
- dynamiczne zmienianie bądź modyfikowanie przedziałów czasowych.

Możliwe jest połączenie do czterech jednocześnie działających sieci Link 22, każda na różnej, określonej częstotliwości z wcześniej zdefiniowanym pseudolosowym wzorem skokowej zmiany częstotliwości nośnej. Każdą sieć można podzielić na 32 podsieci, zwane MASN (Mission Area Sub Network), zgodnie z wyznaczonym zadaniem lub w celu efektywniejszego wykorzystania posiadanych sił i środków.

#### **4. Zarządzanie Siłami Powietrznymi w warunkach sieciocentrycznych**

System zarządzania lotniczym polem walki tworzą trzy główne komponenty:

- a) Komponent informacyjny. Informacja w oparciu o dane rozpoznawcze to czynnik decydujący o powodzeniu w walce. Posiadanie wiarygodnych i terminowych informacji o przeciwniku stanowi podstawę funkcjonowania systemu zarządzania współczesnymi Siłami Powietrznymi. Bez niego dowódca nie będzie w stanie podejmować racjonalnych decyzji i skutecznie dowodzić podległymi siłami. Elementy pozyskujące informację funkcjonują w warunkach ciągłej walki informacyjnej, która polega na zdobywaniu informacji, ich preparacji, weryfikacji i przekazywaniu danych, a także zakłócaniu i dezinformowaniu przeciwnika. Dokładne informacje o przeciwniku, położeniu jego ważnych celów i obiektów pozwalają precyzyjnie razić, uprzedzać w manewrze i w procesie decyzyjnym, co jest szczególnie ważne w operacjach głębokich i bezpośrednich.
- b) Komponent rozpoznania. Komponent rozpoznania odpowiedzialny jest za zdobywanie, udostępnianie oraz terminowe przekazywanie, dokładnej i wiarygodnej informacji o działaniach przeciwnika.
- c) Komponent dowodzenia. Zadaniem komponentu dowodzenia jest zapewnienie realizacji następujących funkcji:
  - efektywne wspomaganie procesu dowodzenia integracja procesu dowodzenia taktycznymi operacjami ofensywnymi i defensywnymi;
  - koordynacja wsparcia lotniczego na korzyść innych komponentów sił zbrojnych;
  - wymiana informacji pomiędzy stanowiskami dowodzenia na danym poziomie dowodzenia;
  - udostępnienie mechanizmów autoryzacji decyzji i rozdziału celów systemom uzbrojenia;
  - zapewnienie łączności ze wszystkimi elementami ugrupowania bojowego, w tym również w wymiarze sojuszniczym i koalicyjnym;
  - opracowywanie oraz dystrybucja informacji w czasie rzeczywistym, niezbędnych dowódcy i sztabowi w procesie decyzyjnym;
  - zapewnienie aktywnej i pasywnej obrony;

- umożliwienie szybkiego przemieszczania sił i osiągnięcia zdolności do działań;
- umożliwić „przecełowanie” – zmianę zadań, nawet środkiem będącym w powietrzu.

Praktyczne zarządzanie SP odbywa się w określonym systemie działania, który w literaturze jest definiowany w różny sposób. Najbardziej popularne jest określenie, że system jest to zestaw (zbiór) wzajemnie powiązanych elementów funkcjonujących jako całość<sup>8</sup>. W kolejnym ujęciu system (z gr. *systema*) jest uporządkowanym zbiorem elementów oraz związków i zależności między nimi tworzącym jakąś całość, który służy założonym celom<sup>9</sup>. Według P. Sienkiewicza<sup>10</sup> (...) *systemem nazywamy każdy złożony obiekt wyróżniony z badanej rzeczywistości, stanowiący całość tworzoną przez zbiór obiektów elementarnych (elementów) i powiązań między nimi. W ujęciu ekonomicznym system to (...) szczególnego rodzaju układ elementów sprzężonych w całość wyodrębniającą się w danym otoczeniu, w którym istotne są sprzężenia (związki relacje, zależności) między tymi elementami oraz między systemem a jego otoczeniem*<sup>11</sup>.

Przyjmując za podstawę zaprezentowane definicje, system zarządzania SP przedstawić można jako procedury, organy zarządzania (siły i środki) oraz powiązania informacyjne. Odnosząc się do pierwszego elementu tego systemu należy stwierdzić, że obecnie najważniejszym wyzwaniem dla systemu zarządzania SP jest dostosowanie procedur do możliwości technicznych systemów wspomagania dowodzenia. Ideę procesu dowodzenia najlepiej ilustruje opisany przez płk Johna Boyda, składający się z czterech faz, cykl OODA<sup>12</sup> (Observe, Orient, Decide, Act). Pierwsza faza (obserwowanie) polega na zbieraniu danych (informacji) o sytuacji przeciwnika i własnej z wszystkich dostępnych źródeł. Druga faza (orientowanie) polega na tworzeniu obrazu sytuacji na podstawie zebranych danych, z wykorzystaniem doświadczeń oraz intuicji osób uczestniczących w tym procesie. Końcowym rezultatem tej fazy jest uzyskanie możliwie pełnej wiedzy o polu bitwy. Na podstawie tej wiedzy w kolejnej fazie (decydowanie) odbywa się proces doboru sposobu działania do wymagań narzuconych przez przełożonego oraz do własnych możliwości, po czym następuje przekazanie decyzji w odpowiedniej formie do podległych sił i środków. Czwarta faza (działanie) polega na przekształceniu decyzji w efekty widoczne na polu walki. Nowoczesne technologie informacyjne umożliwiają skrócenie każdej fazy

<sup>8</sup> T. Pszczołowski, *Mała encyklopedia prakseologii i teorii organizacji*, Osolineum, Wrocław 1978, s. 50.

<sup>9</sup> W. Okoń, *Wprowadzenie do dydaktyki ogólnej*, Żak, Warszawa 1996, s.62

<sup>10</sup> P. Sienkiewicz, *Inżynieria systemów*, MON, Warszawa 1983.

<sup>11</sup> P. Tyrała, *Kierowanie, organizowanie, zarządzanie*, Wyd. Adam Marszałek, Toruń 2001, s. 11.

<sup>12</sup> E. Smith, *Effects Based Operations (EBO) . Applying Network Centric Warfare in peace, crisis and war*, CCRP 2002, s. 79.

cyklu w taki sposób, aby możliwe było włączenie do cyklu OODA mniej zaawansowanego technologicznie przeciwnika i jego zakłócenie. Przerwanie cyklu generowanego przez przeciwnika stawia go w całkowicie nowej sytuacji i zmusza do ponownego rozpoczęcia cyklu OODA. Takie rozwiązanie stanowi istotne wyzwanie dla systemu dowodzenia SP, gdyż musi on umożliwić zintegrowanie i optymalne wykorzystanie zdolności bojowych poszczególnych rodzajów wojsk lotniczych, poczynając od szczebla operacyjnego, a kończąc na szczeblu uzbrojenia platformy (samolotu).

Kolejny niezmiernie ważny element systemu zarządzania SP stanowią organy zarządzania (dowodzenia). Obecnie wyróżnić można dwa główne typy organów dowodzenia: planistyczne np. Centrum Operacji Powietrznych – COP oraz wykonawcze np. ODN realizujący zadania bezpośredniego kierowanie aktywnymi środkami walki, w tym samolotami bojowymi. Organy dowodzenia zorganizowane są w formie stanowisk dowodzenia, które mogą być rozmieszczone na lądzie (np. SD COP) jak i w powietrzu - AWACS (Airborne Warning and Control System, czyli Powietrzny System Ostrzegania i Kontroli). Stanowisko dowodzenia - to odpowiednio przygotowane i wyposażone miejsca (obiekty, rejony), w których rozmieszcza się organy dowodzenia oraz elementy zabezpieczenia. Stanowiska dowodzenia są ze sobą odpowiednio powiązane funkcjonalnie i informacyjnie w określonym układzie poziomym i pionowym. Stanowiska dowodzenia powinny zapewniać dowodzenie wojskami i kierowanie środkami rażenia w toku walki (operacji) oraz łączność dowodzenia i współdziałania, wykorzystując system łączności i informatyki, a w tym Zautomatyzowane Systemy Dowodzenia i Systemy Kierowania Środkami Walki.

Ostatni element systemu zarządzania Siłami Powietrznymi stanowią powiązania informacyjne. Umożliwiają one wzajemne informowanie się o wszelkich stanach rzeczy i ich zmianach. Należy wyjaśnić, że przez informacje rozumiemy treść zawiadomienia, przekazaną przez informatora i przyjętą do wiadomości przez informowanego. Przebiegają „z góry na dół” i „z dołu do góry”, po liniach pionowych (sprężenie służbowe), poziomych i skośnych. Przebiegają też w obie strony po liniach pokrywających się (lub nie) ze spiętrzeniami funkcjonalnymi i technicznymi. Najbardziej popularny podział obejmuje powiązania wewnętrzne i zewnętrzne. Pierwsze z nich powiązania wewnętrzne – związane są z przepływem informacji wewnątrz systemu łącząc jego osoby funkcyjne oraz komórki organizacyjno-funkcjonalne (np. komórki organizacyjne Stanowiska Dowodzenia). Powiązania zewnętrzne związane są z przepływem informacji między organami zarządzania (SD) oraz:

- szczeblem nadrzędnym (przełożonym);
- szczeblem podrzędnym (podwładnym);

- sąsiadami np. innymi jednostkami wojskowymi;
- aktywnymi środkami walki np. ODN - samolot.

Sprawny przepływ informacji w systemie zarządzania SP odbywa się przy wykorzystaniu zautomatyzowanych systemów dowodzenia, wśród których najbardziej znanym jest ICC (Integrated Command and Control). System ICC definiowany jest jako zintegrowane środowisko C3I zapewniające wsparcie procesu decyzyjnego oraz zarządzanie informacją stanowiska dowodzenia szczebla COP (CAOC) w okresie pokoju, kryzysu i wojny<sup>13</sup>. ICC zapewnia wsparcie najważniejszych obszarów funkcjonalnych związanych z dowodzeniem SP takich jak:

- planowanie i stawianie zadań (Planning & Tasking. Target Nomination);
- zarządzanie przestrzenią powietrzną (Airspace Management);
- tworzenie dystrybucji dokumentów rozkazodawczych;
- kontrolę operacji (Mission Monitoring)

Charakterystyczną cechą ICC jest zastosowanie koncepcji rozproszonego przetwarzania danych i w konsekwencji technologii rozproszonych baz danych (distributed database technology). Wymiana danych w systemie może odbywać się w różnych relacjach. Najprostszą z tych relacji jest wymiana danych pomiędzy użytkownikiem a najbliższą, lokalną bazą danych. Możliwy jest także zdalny dostęp użytkownika systemu do bazy danych zlokalizowanej w innym jego centrum – elemencie składowym (Remote Database Access).

## 5. Wymagania stawiane systemowi zarządzania SP

Największy wzrost wymagań SP funkcjonujących w warunkach sieciocentrycznych dotyczył będzie ich systemu dowodzenia i kierowania walką. Wymagać to będzie nowego podejścia do dowodzenia, polegającego na wykorzystywaniu wspólnej „świadomości” pola walki w celu osiągnięcia synchronizacji działań, przy jednoczesnym zachowaniu zdolności natychmiastowego dostosowania się do zmian sytuacji bojowej. Systemy zarządzania spełniające wymogi koncepcji walki sieciocentrycznej powinny realizować funkcje i mieć poniższe możliwości:

- zapewniać możliwość dostępu do wspólnego obrazu sytuacji operacyjnej (COP) tworzonego na podstawie informacji uzyskiwanej z zintegrowanych sensorów i środków walki;
- zapewniać dostęp do zintegrowanych baz danych oraz baz wiedzy (hurtowni danych) zawierających rezultaty działania systemów symulacyjnych i eksperckich;

---

<sup>13</sup> A. Glen, *Kierunki rozwoju systemów dowodzenia SP RP*, AON, Warszawa 2005, str. 57

- zapewniać rzeczywistą organizacyjno-technologiczną selekcję dostępu do danych, w przeciwieństwie do administracyjnej ochrony dostępu;
- zapewniać automatyzację procesów gromadzenia i wymiany danych (meldunki, rozkazy i komendy) oraz wspomagać proces podejmowania decyzji;
- zapewniać możliwości dowodzenia niezależnie od fizycznej lokalizacji elementu decyzyjnego w stosunku do wykonawcy (niezawodność i wiarygodność oraz działanie w czasie rzeczywistym).

W celu spełnienia tych wymagań należy zrealizować następujące przedsięwzięcia:

- dokonać integracji sensorów i systemów uzbrojenia;
- zintegrować istniejące resortowe systemy dowodzenia i bazy danych (należy zapewnić spójności modelu danych);
- ujednolicić procedury operacyjne SP;
- dokonać integracji systemów dowodzenia z systemami symulacyjnymi i eksperckimi;
- przeprowadzić zmiany organizacyjne pozwalające na decentralizację dowodzenia w oparciu o rozproszone ośrodki decyzyjne.

Pojęcie jednolitego, w czasie rzeczywistym, zobrazowania sytuacji operacyjnej jest wpisane w koncepcję walki sieciocentrycznej (Network Centric Warfare) i możliwość dostępu jest traktowana jako istotne wymaganie względem systemu dowodzenia. Zdolność do współużytkowania informacji tworzących wspólną sytuację operacyjną (Common Operational Picture – COP), dzięki efektywnym systemom dowodzenia i kierowania, ma umożliwić wykorzystywanie wspólnej „świadomości” pola walki, co powinno skutkować zwiększeniem efektywności działań oraz pozwoli na wykorzystanie efektu synergii. Jednolity obraz operacyjny (COP), powinien być tworzony na wszystkich szczeblach dowodzenia i powinien zawierać zbiorczą informację z podsystemów SP oraz z sensorów tworzących sieć środków rozpoznania (Sensor Grid).

## **6. Podsumowanie**

Jedną z właściwości dowodzenia siłami powietrznymi jest duża dynamika działań. Tempo zmian sytuacji w operacjach, bitwach i walkach powietrznych mierzy się w godzinach, minutach a nawet sekundach. Wzrastająca złożoność i tempo operacji militarnych wymaga niezwłocznego dostępu do bieżących danych i informacji niezbędnych do uzyskania przewagi nad przeciwnikiem. Przekonanie to, poparte wnioskami wypływającymi z prowadzonych ostatnio na świecie operacji militarnych, uzmysłowiło specjalistom SP tworzącym oraz eksploatującym system dowodzenia i rozpoznania potrzebę zweryfikowania podejścia do transformacji, sposobów przetwarzania i wykorzystywania informacji, dystrybucji danych oraz

informacji pomiędzy różnymi elementami komponentu sił powietrznych i innych komponentów SZ RP. Rozwiązaniem wychodzącym naprzeciw zarysowanej sytuacji problemowej staje się coraz szersze stosowanie technicznych środków dowodzenia automatyzujących niektóre procesy związane z przetwarzaniem i zobrazowaniem informacji. Technologia sieciowa jest praktycznie wykorzystywana w obecnych systemach dowodzenia. Obecnie systemy informatyczne i teleinformatyczne są immanentną częścią każdego, współczesnego systemu dowodzenia. Istotnym aspektem wykorzystania technologii sieciowych w perspektywnych systemach dowodzenia sił powietrznych jest zwiększanie w wymiarze geograficznym rozległości sieci w ramach rozwiązań „reach back capability”. W rozwiązaniach takich przewiduje się realizowanie w perspektywie najbliższych kilkunastu lat przetwarzania pierwotnych danych rozpoznawczych w macierzystych organach dowodzenia rozmieszczonych w miejscach stałej dyslokacji i przekazywanie przetworzonych informacji na potrzeby dowodzenia siłami powietrznymi rozwiniętymi na obszarze operacji. Kolejnym trendem w przetwarzaniu i zobrazowaniu informacji na potrzeby organów dowodzenia sił powietrznych staje się integracja w ramach jednego spójnego zobrazowania danych pochodzących z różnych źródeł i dotyczących zróżnicowanych aspektów realizacji zadań bojowych. W tym kontekście, ostatnie rozwiązania - wskazują na architektury usług informacyjnych jako technologiczne platformy budowy systemów informatycznych, w tym zautomatyzowanych systemów dowodzenia. Zważywszy na aktualne tendencje transformacji sił zbrojnych zgodnie z koncepcją wojny sieciocentrycznej, nie da się przecenić wpływu różnych klas usług informacyjnych na proces oraz cykl dowodzenia, a także interoperacyjność systemową.

## 7. Literatura

- [1] Cebrowski A., Garstka J., *Network Centric Warfare. Its Origins and Future*, Proceedings of the Naval Institute, 1998.
- [2] Smutniak Z., *Dowodzenie siłami powietrznymi w środowisku sieciocentrycznym*, AON, Warszawa 2008.
- [3] *Concept for Future Joint Operations*, Joint Chiefs of Staff, 1997.
- [4] Smith E., *Effects Based Operations (EBO). Applying Network Centric Warfare in peace, crisis and war*, CCRP 2002.
- [5] *Understanding LINK-16*. Northrop Grumman, San Diego 2001.
- [6] Pszczołowski T., *Mała encyklopedia prakseologii i teorii organizacji*, Osolineum, Wrocław 1978.
- [7] Okoń W., *Wprowadzenie do dydaktyki ogólnej*, Żak, Warszawa 1996.
- [8] Sienkiewicz P., *Inżynieria systemów*, MON, Warszawa 1983.

- [9] Tyrała P., *Kierowanie, organizowanie, zarządzanie*, Wyd. Adam Marszałek, Toruń 2001.
- [10] Smith E., *Effects Based Operations (EBO). Applying Network Centric Warfare in peace, crisis and war*, CCRP 2002.
- [11] Glen A., *Kierunki rozwoju systemów dowodzenia SP RP*, AON, Warszawa 2005.



**płk nawig. dr inż. Bogdan Grenda**, absolwent WSOSP, AON oraz AE w Poznaniu. Doktor nauk wojskowych w specjalności Siły Powietrzne. Uczestniczył w wielu ćwiczeniach narodowych i międzynarodowych oraz kursach specjalistycznych m.in. w Kursie oficerów sztabu w Słowacji. Służył w 62 Pułku Lotnictwa Myśliwskiego w Poznaniu, w Zarządzie Operacji SP Dowództwa Sił Powietrznych w Warszawie oraz na stanowisku zastępcy dowódcy 6 Bazy Lotniczej w Dęblinie. Obecnie pracuje w Akademii Obrony Narodowej na stanowisku Adiunkt – Kierownik Zakładu Systemów Dowodzenia Siłami Powietrznymi.