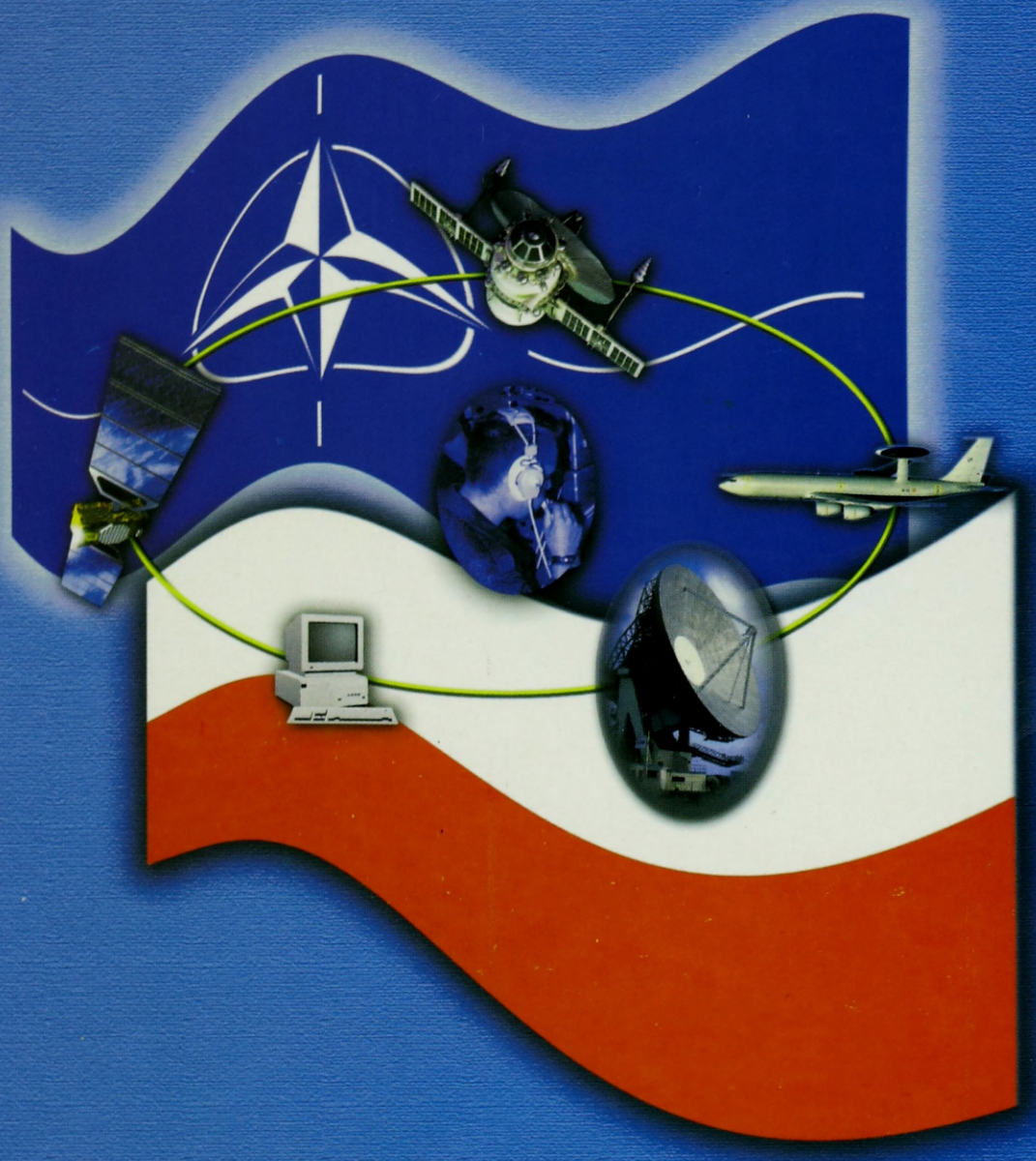


INFORMACJE W OBRONIE POWIETRZNEJ – POTRZEBY, WYMAGANIA, ZAGROŻENIA

AKADEMIA OBRONY NARODOWEJ

A K A D E M I A O B R O N Y N A R O D O W E J

WYDZIAŁ LOTNICTWA I OBRONY POWIETRZNEJ
KATEDRA OBRONY POWIETRZNEJ

AON 5428/02

INFORMACJE W OBRONIE POWIETRZNEJ – POTRZEBY, WYMAGANIA, ZAGROŻENIA

Materiały z sympozjum naukowego – 28 marca 2002 r.

Opracował
ppłk dr Zdzisław MAŚLAK

WARSZAWA **2002**

Konsultacja naukowa
płk dr hab. Ryszard KURIATA

Organizacja sympozjum i opracowanie materiałów
ppłk dr inż. Zdzisław MAŚLAK

Redaktor
Jerzy Wajs

Redaktor techniczny
Beata Klarowska

Projekt okładki
Ewa Wiśniewska

Korekta
Małgorzata Sęktas

Opracowano na podstawie materiałów wystąpień,
dostarczonych i zaprezentowanych przez autorów.

Wystąpienia uczestników sympozjum, opublikowane za ich zgodą,
nie są autoryzowane.

Skład, druk i oprawa: Akademia Obrony Narodowej – Wydział Wydawniczy
00-910 Warszawa, al. gen. A. Chruściela 103, tel./faks 681-37-52
zam. nr 596/2001

SPIS TREŚCI

ppłk dr inż. Zdzisław Maślak

Wydział Lotnictwa i Obrony Powietrznej AON

SPRAWOZDANIE Z PRZEBIEGU SYMPOZJUM

Sympozjum było poświęcone szeroko rozumianej problematyce zarządzania informacjami[1] w obronie powietrznej. Tematy na nim poruszane są tym bardziej aktualne, że żyjemy w okresie nazywanym w literaturze czasem tworzenia społeczeństwa informacyjnego (A. Toffier, J. Naisbitt, P. Aburdene). Wysoko rozwinięte kraje, dominujące we współczesnym świecie, wychodzą już z ery społeczeństwa konsumpcyjnego. To przeistaczanie dokonuje się za pomocą technologii informacyjnej. To właśnie dzięki niej można zastosować nowoczesne instrumenty zarządzania, co w konsekwencji pozwala na decentralizację i pluralizm decydowania lub też może wzmacniać centralizację, o ile jest taka wola decydentów organizacji czy instytucji. O istocie problemu świadczy to, że prawie w każdym współczesnym podręczniku o zarządzaniu, co najmniej jeden rozdział jest poświęcony zagadnieniu zarządzania informacjami. Polska w obszarze obronności, a tym bardziej w obszarze obrony powietrznej, nie jest, co należy ze smutkiem zauważyć, w czołówce dokonujących się zmian. A jest to obszar ważny dla sprawnego funkcjonowania państwa[2]. Nie zawsze, jak wykazują badania, decydenci obrony powietrznej dostrzegają, że każda działalność w obronie powietrznej ma dwie składowe – *fizyczną i informacyjną*, i że aby osiągnąć sukces, każdy komponent obrony powietrznej winien zwiększyć wysiłki w celu doskonalenia i rozwinięcia składowej informacyjnej w odniesieniu do działalności koncepcyjnej oraz skuteczności działania. Sympozjum, którego owocem jest niniejsze opracowanie, dotyczyło współ-

---

[1] Autor celowo używa terminu „*zarządzanie informacjami*" mając świadomość, że termin ten wzbudza kontrowersje w środowisku naukowym. Jednak studiując literaturę problemu wielokrotnie spotkał się właśnie z takim terminem, odnoszącym się do szeroko rozumianego zarządzania zasobami informacji. Zob.: Z. Martyniak, *Elementy zarządzania informacją i komunikacją w przedsiębiorstwie*, Akademia Ekonomiczna Kraków 1997; P. Beynon-Davies, *Inżynieria systemów informacyjnych*, WNT, Warszawa 1999. Również jedną z funkcji przyszłościowego Systemu Dowodzenia Lotnictwem i OP PSP NATO szczebla taktycznego (Air Command and Control System – ACCS) określa się *zarządzaniem informacjami* (Information Management). Autor uważa, że termin ten, coraz częściej pojawiający się w literaturze, znajdzie w przyszłości swe miejsce w nauce.

[2] Autor nawiązuje do ataku z dnia 11 września 2001 r., przy użyciu samolotów pasażerskich, na centrum finansowe świata mieszczące się w wieżowcach Nowego Jorku oraz Pentagon.

czesnych poglądów na zarządzanie informacjami w obronie powietrznej oraz systemami informacyjnymi je wspomagającymi, ich budowę i zastosowanie. Intencją organizatora sympozjum było także przekonanie audytorium, które stanowili wybitni znawcy tematu – przedstawiciele dowództwa WLOP i dowództw KOP, pracownicy naukowi WIŁ, kadra naukowo-dydaktyczna AON – że należy zmienić mentalność polskich decydentów obrony powietrznej. Powinni oni myśleć o kwestii doskonalenia zarządzania informacjami jako o jednym z głównych czynników przynoszących sukces; czyniących obronę powietrzną szczelniejszą i skuteczniejszą.

Ramy sympozjum oraz niniejszego opracowania zostały w zasadzie ograniczone do obszaru obrony powietrznej, lecz większość poruszanych i zawartych w opracowaniu treści ma bardziej uniwersalny charakter. Skupienie się na dziedzinie obrony powietrznej wynika z tego, że zdaniem organizatora sympozjum charakteryzuje się ona największą dynamiką zmian.

Niniejsze sympozjum miało na celu m.in. dokonanie przeglądu aktualnego stanu prac badawczych, prowadzonych także w Akademii Obrony Narodowej, a dotyczących różnych aspektów zarządzania informacjami w tak specyficznym środowisku, jak obrona powietrzna.

Podstawę dyskusji stanowiły wystąpienia uczestników, przede wszystkim zaś – referat wprowadzający; ppłk. dr. inż. Zdzisława Maślaka na temat: *Zarządzanie informacjami w obronie powietrznej – rozwiązywanie problemów i podejmowanie decyzji*; płk. dr. hab. Mariana Cieślarczyka na temat: *Człowiek – silny czy słaby element w systemie informacyjno-decyzyjnym sił powietrznych*; płk. dr. inż. Ryszarda Szpakowicza na temat: *Kierunki rozwoju systemów informacyjnych obrony powietrznej*; płk. dr. inż. Marka Grzybowskiego na temat: *Wymagania informacyjne wobec potrzeb kontroli przestrzeni powietrznej w ramach systemu OP NATO*; ppłk. dr. inż. Andrzeja Gałeckiego na temat: *Problemy racjonalnego podejmowania decyzji*; mjr. dr. inż. Zbigniewa Skwarka na temat: *Zdobywanie informacji w obronie powietrznej*; ppłk. dr. inż. Gabriela Nowackiego i mjr. mgr. inż. Wiesława Błażejczyka na temat: *Zagrożenia informacyjne w obronie powietrznej*.

Ponadto w dyskusji mjr mgr Wojciech Burakowski przedstawił projektowany Cyfrowy Zintegrowany System Teleinformacyjny Wojsk Lotniczych i Obrony Powietrznej (system CZST WLOP). W swojej wypowiedzi dokonał przeglądu głównych założeń do sieci łączności systemu CZST WLOP. Potwierdził, iż architektura sieci uwzględnia zarówno obecny stan zaawansowania dostępnych technik telekomunikacyjnych (stan standaryzacji, urządzenia dostępne na rynku, dotychczasowe doświadczenia), jak i konieczne usługi sieciowe w celu realizacji efektywnego przekazu informacji związanych z różnymi aplikacjami (usługami) oferowanymi w sieci. Usługi te będą dysponowały odpowiednimi mechanizmami zapewniającymi wymagania dotyczące jakości przekazu poszczególnych rodzajów informacji. Nadmienił także że projektowany system ma szansę być eksploatowany przez wiele lat, ponieważ cechuje się elastycznością i możliwością rozbudowy.

Ppłk dr inż. Andrzej Gałecki w swoim wystąpieniu nawiązał do zagadnienia informacji w podejmowaniu decyzji. Powiedział m.in.: „*...mimo że problem podejmowania decyzji jest przedmiotem wieloletnich badań, do dziś zalicza się do naj-*

bardziej frapujących zagadnień naukowych, chociażby ze względu na jego rolę w funkcjonowaniu życia człowieka". Ponieważ informacja odbierana przez różnych ludzi jest często niejednolicie odbierana, zarówno w zakresie jej zapamiętywania (sposobu gromadzenia), jak również reakcji skierowanej na konkretne działanie.

Ppłk dr inż. Tomasz Jakusz, na przykładzie bojowych 60 dywizjon rakiet OP podczas ćwiczenia NATO „STRONGE RESOLVE 2002", zilustrował jak starcie zbrojne może być przeniesione w wymiar walki informacyjnej i jakie wymierne efekty w zakresie możliwości bojowych mogą być uzyskane bez fizycznego oddziaływania. Przekonywał, że przykład ten uzasadnia konieczność nowego spojrzenia na zagadnienie walki jako na proces sterowany za pomocą informacji, gdzie racjonalne jest skierowanie oddziaływania nie tylko na elementy wykonawcze – jednostki walczące – lecz również na szeroko pojmowany system informacyjny.

Ppłk dr Adam Halama w swoim wystąpieniu dokonał syntetycznej analizy roli informacji w procesach i zjawiskach, które stanowią obszar zainteresowania dowódców obrony przeciwlotniczej i należą do najtrudniejszych, a dotyczą prognozowania działań przeciwnika.

Na zakończenie kpt. pil. mgr inż. Dariusz Sarnecki przedstawił szereg własnych spostrzeżeń na temat roli i funkcji informacji w obronie powietrznej, które są wynikiem jego badań prowadzonych w ramach dysertacji doktorskiej.

Ożywiona dyskusja prowadzona na sympozjum świadczy o tym, że poruszane kwestie wzbudzają zainteresowanie nie tylko w środowisku akademickim, ale również w wojskach. Świadczą także zarówno o trafności i aktualności problematyki badawczej zawartej w referacie wprowadzającym, jak i o osiągnięciu celów założonych przez organizatora sympozjum.

Z wypowiedzi wynika, że prezentowane treści w referacie wprowadzającym znalazły akceptację, a wyrażane opinie służyły głównie ich niezbędnemu uzupełnieniu. Stwierdzono jednoznacznie, że w tak specyficznym obszarze jak obrona powietrzna, nakazem chwili jest konieczność stosowania naukowych zasad zarządzania informacjami.

Jednocześnie wskazano na wiele wątpliwości, które powinny zostać wyjaśnione w czasie dalszych prac. Dotyczą one przede wszystkim:

1) sposobu ustalania podziału kompetencji, gdyż dostęp do jednolitej informacji powoduje zbliżenie, a nawet przenikanie się dotąd wyraźnie wydzielonych szczebli dowodzenia;

2) zasad i skuteczności przekazywania uprawnień do dowodzenia oraz autoryzacji stawianych zadań w świetle skrócenia drogi od sensora do systemów uzbrojenia;

3) możliwości opracowania skutecznego systemu filtracji, zapobiegającego nadmiarowi informacji na poszczególnych stanowiskach pracy.

ppłk dr inż. Zdzisław Maślak
Wydział Lotnictwa i Obrony Powietrznej AON

ZARZĄDZANIE INFORMACJAMI W OBRONIE POWIETRZNEJ – ROZWIĄZYWANIE PROBLEMÓW I PODEJMOWANIE DECYZJI

„Im bardziej organizacja staje się nieefektywna, tym bardziej wykazuje tendencję do produkowania prawdziwych informacji dla mało istotnych i z reguły dobrze ustrukturyzowanych problemów oraz mało znaczących informacji dla problemów istotnych".

(Ch. Argyris)

Doświadczenia z wojen i konfliktów lokalnych ostatnich lat potwierdzają tezę, iż uderzenia z powietrza przesądzają o przebiegu dalszych działań bojowych. Wzrost znaczenia obrony powietrznej jest szczególnie widoczny po ostatnich atakach na wieżowce Nowego Jorku. Wobec tego, priorytetem każdego państwa staje się silna i dobrze zorganizowana obrona powietrzna. Posiadanie dobrze zorganizowanej i skutecznej obrony powietrznej jest obecnie jednym z podstawowych kryteriów przygotowania państwa czy bloku państw pod względem militarnym[1].

Biorąc pod uwagę tezę, że zasoby informacyjne spełniają szczególną rolę w każdej instytucji czy firmie, należy wnioskować, że funkcjonowanie obrony powietrznej w czasie pokoju, konfliktu regionalnego czy wojny na szerszą skalę, zależy także od zarządzania jej zasobami informacji.

Skuteczność obrony powietrznej ściśle zależy od jakości zarządzania jej zasobami. Jakość zarządzania obroną powietrzną, za pomocą którego można nią kierować w sposób celowy i planowy, chyba najbardziej zależy dzisiaj od posiadanych informacji, których liczbę i różnorodność jest coraz trudniej skutecznie kontrolować.

Dzisiaj zasoby informacyjne decydują o tzw. inteligencji instytucji, tj. o sposobie wykorzystania przez nią posiadanych możliwości, zdolnościach dostosowania się do nowych sytuacji i programowania swojej przyszłej działalności, a więc o zdolnościach osiągania stałych sukcesów w warunkach ciągłych zmian i trakto-

[1] Por. B. Zdrodowski, *Obrona powietrzna*, AON, Warszawa 1993.

wania tych zmian nie tylko w kategoriach zagrożeń, lecz jako szans na rozwijanie nowej skutecznej działalności[2].

Uważa się, że zasoby informacyjne[3] są dzisiaj strategicznym zasobem[4] obrony powietrznej, stanowiącym główne źródło przewagi i sukcesu.

Zmiany zachodzące w obronie powietrznej w okresie ostatnich lat, wynikające z powstawania społeczeństwa informacyjnego, wymuszają potrzebę nowego spojrzenia na kształt i funkcjonowanie sytemu zbierania, przetwarzania i dystrybucji informacji, a więc de facto na zarządzanie informacjami w obronie powietrznej. Obecne i dające się przewidzieć w niedalekiej przyszłości uwarunkowania zewnętrzne i wewnętrzne obrony powietrznej kraju czy grupy państw związanych sojuszem, takie jak: zagrożenie z powietrza, założenia doktryny wojennej oraz wynikające z nich funkcje i zadania obrony powietrznej, działanie obrony powietrznej w sytuacji pokoju, kryzysu i wojny, stanowią podstawę przyszłościowych rozwiązań zarządzania informacjami[5] w obronie powietrznej.

W warunkach dzisiejszego rozwoju cywilizacyjnego świata, wraz z jego negatywnymi zjawiskami, tak złożony organizm jak obrona powietrzna, powinien dobrze znać swoje zasoby informacyjne; wiedzieć, jakie informacje są niezbędne nie tylko decydentom do wykonywania ich podstawowych funkcji i działań, tworzenia oraz realizowania programów i planów, ale także, jakie są potrzeby wszystkich innych odbiorców. Powinna też określić, jakie potrzeby informacyjne są zaspokajane, a także w jakim stopniu przepływy informacji służą decydentom w podejmowaniu decyzji i sprawnym kierowaniu zasobami. Przy olbrzymiej liczbie i różnorodności informacji zachodzi konieczność sprawnego nimi zarządzania, tak aby każda z nich – w odpowiednim czasie i formie – znalazła się u właściwego odbiorcy.

Przystępując do zbadania problemu zarządzania informacjami w obronie powietrznej, należałoby zadać sobie pytanie: czy jest możliwe zarządzanie informacjami w obronie powietrznej i czy jest takie pojęcie jak „zarządzanie informacjami w obronie powietrznej". Zatem kilka zdań na potwierdzenie tezy, że takie pojęcie ma swoje miejsce we współczesnej nauce.

---

[2] Por. P. F. Drucker, *Innowacja i przedsiębiorczość. Praktyka i zasady*, PWE, Warszawa 1992, s. 36–37.

[3] Zasoby informacyjne – celowo uporządkowana konfiguracja zbiorów informacyjnych obrony powietrznej, takich jak:

– normy, wartości, zachowania, wiedza, umiejętności, możliwości i kompetencje stanów osobowych;

– zbiory informacji – możliwości ich pozyskiwania, przetwarzania, dystrybucji oraz możliwości ich użycia;

– kompetencje poszczególnych elementów obrony powietrznej;

– możliwości łączenia i koordynacji zasobów informacyjnych poszczególnych komponentów obrony powietrznej;

– możliwości wszechstronnego wykorzystania zbiorów informacyjnych w celu osiągnięcia sukcesu.

[4] Zasoby strategiczne – celowo uporządkowana konfiguracja zapas materialnych i niematerialnych obrony powietrznej.

[5] Zarządzanie informacjami – całość zagadnień dotyczących sposobów użytkowania wszelkich informacji funkcjonujących w systemie. Do zarządzania informacjami należy: formułowanie i kształtowanie informacji, ich podział, adresowanie, wspólne wykorzystanie, bezpieczeństwo użycia.

Jest oczywiste, że w naukach społecznych przywiązuje się duże znaczenie do ich podstawowych, fundamentalnych założeń i ewolucji. Początki studiów nad dziedziną zarządzania sięgają lat trzydziestych XX wieku. Uczeni, publicyści i praktycy tego okresu sprecyzowali dwie grupy podstawowych założeń dotyczących istoty zarządzania. Pierwsza odnosi się do zarządzania jako nauki, natomiast druga koncentruje się na praktyce zarządzania. W ramach poszczególnych grup zostały sformułowane następujące tezy:

W odniesieniu do zarządzania jako nauki:

1. Pojęcie zarządzania odnosi się do istoty instytucji i zasad jego funkcjonowania.
2. Istnieje lub powinna istnieć jedna idealna struktura organizacyjna.
3. Istnieje lub powinien istnieć jeden właściwy sposób kierowania zasobami.

W odniesieniu do praktyki zarządzania:

1. Zarządzanie opiera się na dostępnych technologiach oraz jest nakierowane na efekt finalny tego działania.
2. Zakres zarządzania jest prawnie określony.
3. Zarządzanie jest skoncentrowane na wnętrzu danej organizacji.
4. Ekonomia, w wąskim pojęciu, jest ekologią instytucji i zarządzania.

Do wczesnych lat osiemdziesiątych ubiegłego stulecia takiego rodzaju stwierdzenia uznawano za odpowiadające rzeczywistości i wykorzystywano w badaniach, nauce i praktyce zarządzania. Obecnie natomiast głosi się pogląd, że są one przeszkodą w rozwoju badań nad zarządzaniem oraz w dużo większym stopniu również dla praktyki zarządzania, z powodu znacznych rozbieżności zachodzących między teorią a rzeczywistością. Dlatego konieczne jest przeanalizowanie dotychczasowych i stworzenie nowych fundamentalnych zasad, dzięki którym rozwój teorii oraz praktyki zarządzania będą kontynuowane. Takie tendencje we współczesnej nauce są już zauważalne.

Dla większości osób związanych, jak też niezwiązanych z zarządzaniem, stwierdzenie, że dotyczy ono tylko zarządzania biznesem, jest jak najbardziej oczywiste. Zarówno piszący o tym praktycy, jak i teoretycy zarządzania oraz laicy w tej dziedzinie, niekiedy podświadomie utożsamiają pojęcie zarządzania z biznesem.

Nie zawsze tak było w przeszłości i nie jest tak dzisiaj. Do roku 1930 pisarze i myśliciele, począwszy od Fredericka Winslowa Taylora[6], twórcy naukowego zarządzania, a skończywszy na Chesterze Barnardzie głosili, że „*zarządzanie biznesem jest jedynie pochodną teorii zarządzania*" nie różniącą się od zarządzania jakąkolwiek inną organizacją. Bardzo dobrym przykładem na potwierdzenie tej opinii jest fakt, że pierwsze zastosowanie teorii zarządzania miało miejsce w agencjach rządowych i firmach, które nie były nastawione na zysk. Przykładem nauko-

---

[6] F. W. Taylor (1856–1915), amerykański ekonomista, inżynier i wynalazca (uzyskał ponad 100 patentów), twórca podstaw naukowej organizacji i kierownictwa, założyciel w 1911 r. *Society to Promote the Science of Management* (Towarzystwo Promocji Naukowego Kierownictwa). Obserwując marnotrawstwo czasu pracy i poszukując sposobów zwiększenia wydajności maszyn i urządzeń opracował pierwszy, oparty na naukowych podstawach, system organizowania i zarządzania procesami wytwórczymi w przedsiębiorstwie tayloryzm. Główna praca: *Zarządzanie warsztatem wytwórczym* (1903, wydanie polskie 1926). wiem.onet.pl.

wego zarządzania, na jaki powołał się Taylor podczas przesłuchania w Kongresie w 1912 r., nie było przedsiębiorstwo, lecz klinika Mayo, organizacja nie nastawiona na zysk. Najbardziej znana publikacja na temat zastosowania taylorowskiego „naukowego zarządzania" nie dotyczyła biznesu, lecz rządowego arsenału armii amerykańskiej. Również pojęcie „kierownika" w obecnym znaczeniu nie zostało po raz pierwszy przez niego użyte jako określenie stanowiska osoby pełniącej ważną funkcję w przedsiębiorstwie, lecz jako osoby odpowiedzialnej za nadzór nad miastem. Pierwsze świadome użycie zwrotu „zasady zarządzania", także nie miało odniesienia do biznesu, lecz do reorganizacji armii amerykańskiej przez Elihu Roota[7] w 1901 r., który piastował wówczas urząd sekretarza ds. obrony w rządzie Theodora Roosevelta. Pierwszy kongres na temat zarządzania został zorganizowany w Pradze w 1922 r. przez Herberta Hoovera[8], ówczesnego sekretarza ds. handlu i Thomasa Masaryka[9], słynnego historyka i pierwszego prezydenta Republiki Czeskiej, a nie, jak można by sądzić, przez ludzi związanych z biznesem. Mary Parker Follett, która rozpoczęła w tym czasie swoje badania nad istotą zarządzania, również nie różnicuje zarządzania na zarządzanie związane i nie związane z pojęciem biznesu, uważając, że te same założenia dotyczące zarządzania odnoszą się do wszystkich organizacji, zarówno tych, które kierują się zasadą rentowności, jak i tych, które nie są nastawione na zysk.

Ciekawostką jest to, że w czasach wielkiego kryzysu wyrażenie „zarządzanie" było pomijane z uwagi na brak jego akceptacji, a co ważniejsze – ideologii, jaką ono reprezentuje. W okresie powojennym, do roku 1950, rzeczownik „zarządzanie" wrócił do łask, głównie z powodu działań przeprowadzonych przez amerykańskie dowództwo podczas II wojny światowej.

Obecnie pogląd, że zarządzanie jest przede wszystkim zarządzaniem biznesem, jest nadal żywy. Niemniej jednak, należy z całą pewnością stwierdzić, że teza ta jest błędna, podobnie jak błędne jest stwierdzenie, że np. bezpieczeństwo państwa to tylko sprawne funkcjonowanie jego sił zbrojnych. Oczywiście, istnieją różnice między organizacjami, bowiem ich misja definiuje strategię, a strategia ma wpływ na strukturę organizacji i zarządzanie nimi. Nie ulega wątpliwości, że odmienny charakter będzie miało zarządzanie bazą lotniczą, szpitalem czy firmą produkującą

---

[7] E. Root (1845–1937), amerykański prawnik i polityk. 1905–1909 jako sekretarz stanu dążył do zacieśnienia współpracy z krajami Ameryki Południowej. 1909–1915 senator. Od 1910 r. członek trybunału haskiego. Zwolennik arbitrażu w stosunkach międzynarodowych. W 1912 r. otrzymał pokojową Nagrodę Nobla. W 1917 r. stał na czele specjalnej misji dyplomatycznej do Rosji. Tamże.

[8] H. C. Hoover (1874–1964), polityk republikański, prezydent USA w latach 1929–1933. W czasie I wojny światowej organizował pomoc humanitarną dla ofiar wojny w Europie (głównie Belgii). Pod koniec wojny rozpoczął pracę w administracji federalnej, m.in. w 1919 r. był ekspertem ekonomicznym w czasie paryskiej konferencji pokojowej. W latach 1921–1928 pełnił funkcję sekretarza handlu. Był głównym krytykiem tzw. *nowego ładu*. Prace naukowe w dziedzinie ekonomii (m.in. noblisty M. Friedmana) wykazały, iż to on miał słuszność. Polityka *nowego ładu*, wydłużyła bowiem kryzys, a nie ograniczyła go. W latach 50. pełnił funkcję przewodniczącego komisji Kongresu do spraw przerostów w administracji. Autor m.in. dwutomowych *Pamiętników* (1951–1952). Tamże.

[9] T. G. Masaryk (1850–1937), uczony i polityk czeski. Od 1882 r. profesor filozofii na uniwersytecie w Pradze. W 1918 r., po utworzeniu Czechosłowacji, wybrany na urząd prezydenta. Autor licznych prac z zakresu filozofii, socjologii i historii. Tamże.

oprogramowanie komputerowe. Poszczególne organizacje różnią się od siebie, przede wszystkim używaną terminologią i sposobem zastosowania w praktyce propagowanych metod zarządzania. Jednak po głębszej analizie, różnice w sposobie zarządzania tymi organizacjami nie są tak znaczne, jak mogliby przypuszczać dowódcy wojskowi, dyrektorzy szpitali czy menedżerowie firm produkujących oprogramowania. Niewielkie różnice występują natomiast w rozumieniu zasad, na jakich opiera się zarządzanie, w precyzowaniu konkretnych zadań oraz wyzwań, którym organizacje muszą sprostać i będą musiały sprostać w przyszłości. Za dobry przykład, potwierdzający tę tezę, może posłużyć fakt, iż obecnie prowadzone badania potwierdzają, że decydenci czy kierownicy organizacji o odmiennym charakterze, przeznaczają tyle samo czasu na rozwiązywanie problemów bardzo do siebie podobnych. Około 90 procent problemów, jakimi zajmuje się organizacja ma charakter ogólny. Pozostałe 10 procent spraw wynika z indywidualnej misji, historii, kultury i terminologii charakterystycznej dla danej organizacji.

Z analizy założeń leżących u podstaw zarządzania jest więc stwierdzenie, że zarządzanie jest specyficzną i wyróżniającą się cechą każdej organizacji lub instytucji.

Badacze problemów zarządzania, w tym zarządzania informacjami (A. Drevet, H. Simon) stwierdzają, że gdyby dokonać analizy funkcji kierowniczej ze względu na jej pracochłonność, okazałoby się prawdopodobnie, że praca z informacjami pochłania decydentom najwięcej czasu.

Analizując i zastanawiając się nad treścią tej funkcji kierowniczej, można wyróżnić składające się na nią funkcje cząstkowe, takie jak.:

- określenie potrzeb informacyjnych,
- gromadzenie informacji,
- przetwarzanie i przechowywanie informacji,
- dystrybucja informacji.

Stosownie do następstwa wymienionych funkcji cząstkowych, można wyróżnić szereg zasad, które podnoszą sprawność pracy z informacjami. Jako pierwszą często wymienia się zasadę selekcji, lansowaną przez francuską badaczkę A. Drevet. Stwierdziła ona, że współczesny decydent bywa źle poinformowany nie ze względu na niedostatek informacji, lecz na ich nadmiar[10]. Dlatego w odniesieniu do każdego stanowiska kierowniczego, nieodzowne jest stosowanie zasady selekcji informacji, określanej również mianem „zasada 20–80" Okazuje się bowiem, że tylko 20 procent informacji docierających do kierownictwa dotyczy spraw kluczowych i te 20 procent w 80 procentach przesądza o wynikach działalności[11]. **Określenie puli informacji o kluczowym znaczeniu, stanowi istotę zasady selekcji w odniesieniu do pracy z informacjami**.

---

[10] A. Drevet, *Les grandes methodes d'actiona lusage des dirigeands*, Paryż 1971, s. 57.

[11] Relację 20–80 należy traktować jako umowną. W rzeczywistości mogą występować dość znaczne odchylenia od tej proporcji, lecz główna idea zasady pozostaje zazwyczaj nie zmieniona.

Znaczenie tej zasady podkreśla także znany amerykański teoretyk organizacji H. Simon[12], który stwierdził, że „w dzisiejszych czasach krytycznym zadaniem nie jest [...] generowanie, przechowywanie lub przekazywanie informacji, lecz jej filtrowanie"[13].

Właśnie to wcześniej wspomniane określenie puli informacji o kluczowym znaczeniu, jak wykazują badania, jest jednym z trudniejszych do przezwyciężenia problemów dla współczesnego decydenta, a jak sądzę dla decydenta obrony powietrznej szczególnie. Dzieje się tak dlatego, że proces zarządzania, z metodycznego punktu widzenia, to ciąg decyzji[14]. Podejmowanie decyzji, jest bowiem podstawową cechą każdego decydenta obrony powietrznej na każdym etapie czy poziomie dowodzenia, czy kierowania. Decyzje te polegają na dokonywaniu wyboru jednego spośród dwóch lub więcej wariantów możliwych do realizacji. Podejmowanie decyzji ma miejsce w trakcie realizacji podstawowych funkcji decyzyjnych (kierowniczych), tj. planowania, organizowania, prowadzenia i kontrolowania działań bojowych. W każdej decyzji występuje tzw. problem decyzyjny,[15] który powstaje na tle różnicy pomiędzy oceną stanu aktualnego a stanem pożądanym. Decyzję może podejmować jedna osoba, tj. dowódca określonego poziomu – w nauce zwana *decydentem indywidualnym* – bądź grupa osób, np.: kolegium, sztab, sekcja, zwana *decydentem kolegialnym*. Zarówno w obronie powietrznej, jak i w całym systemie dowodzenia siłami zbrojnymi występują te dwa rodzaje decydentów, przy czym decyzje indywidualne często stanowią kontynuację, a ściślej realizację, decyzji podjętych kolegialnie. W przygotowaniu decyzji, oprócz decydenta, z reguły uczestniczą członkowie danej jednostki organizacyjnej lub specjaliści (eksperci) spoza tej jednostki, wspomagani informacyjnie specjalistycznymi programami i informacjami z baz danych.

---

[12] H. A. Simon (1916–), amerykański ekonomista i socjolog. Od 1949 r. profesor Uniwersytetu w Pittsburghu. Zajmuje się teorią organizacji firmy i problematyką podejmowania decyzji ekonomicznych. Podważył powszechne założenie o dążeniu firm do maksymalizacji zysku, uważając, że firmę zadowala zysk „satysfakcjonujący". W 1978 r. otrzymał Nagrodę Nobla za badania dotyczące sposobu podejmowania decyzji ekonomicznych. Główne prace: *Models of Man* (1957), *Teoria organizacji* (1958, wspólnie z J. Marchem, wydanie polskie 1964), *Essays on the Structure of Social Science Models* (1963), *Models of Discovery and Topics in the Methods of Science* (1977), *Models of Thought*, (t. 1–2,). wiem.onet.pl.

[13] H. Simom, *Podejmowanie decyzji kierowniczych*, PWE, Warszawa 1982, s. 158.

[14] Decyzja – postanowienie, rozstrzygnięcie; oparty na dostępnej informacji ostateczny wybór sposobu działania w celu rozwiązania określonego problemu. Jeśli informacja jest niedokładna lub niepełna, decyzja może być błędna. Skuteczną decyzję musi charakteryzować wysoki stopień racjonalności (ważny jest wybór najkorzystniejszy) oraz możliwość jej zastosowania. Na decyzję składa się: cel – wynik decyzji; możliwości – to, co można wybrać; ryzyko – czy poprzez wybraną możliwość osiągnie się cel. R. Smolski, M. Smolski, E. H. Stadtmüller, *Słownik encyklopedyczny*. wiem.onet.pl.

[15] Problem decyzyjny – zagadnienie, zadanie, sprawa, kwestia sporna, które wymagają rozstrzygnięcia na podstawie dostępnych informacji w celu rozwiązania określonego problemu. Jeśli informacja jest niedokładna lub niepełna, problem decyzyjny może być błędnie rozstrzygnięty.

Problem decyzyjny zawsze się wiąże z określonymi warunkami działań bojowych, które – łącznie z tym problemem[16] – są określane w literaturze mianem sytuacji problemowej[17].

Identyfikacja i opis sytuacji problemowej są początkiem procesu podejmowania decyzji. W turbulentnie zmieniającej się sytuacji, w warunkach ograniczeń czasowych, w warunkach niepewności i przy niedostatecznej znajomości podstawowych informacji, sytuacja problemowa nie zawsze może być w pełni określona. W tych warunkach, dla pełniejszego określenia sytuacji problemowej, często niezbędne jest zbudowanie jednej lub kilku sytuacji hipotetycznych, tworzących zbiór dwóch lub więcej sytuacji możliwych do wyboru. Jednocześnie każda sytuacja hipotetyczna zawiera wszelkiego rodzaju ograniczenia, np.: międzynarodowe, sojusznicze, prawne, materiałowe i inne, które powinny być uwzględnione przy podejmowaniu decyzji w określonej sytuacji problemowej.

Decyzje podejmowane wówczas, można podzielić na dwie grupy:

1) rutynowe, powtarzalne, pewne;

2) nierutynowe, niepowtarzalne, niepewne.

Pierwsza grupa – to decyzje proste, bieżące, nie wymagające specjalnego przygotowania i nadające się do opracowania uogólnionej procedury podejmowania decyzji. Dotyczy to przykładowo wprowadzenia wyższych stanów gotowości bojowej w wyznaczonych jednostkach OP, uruchomienia pewnych procedur postępowania w sytuacjach szczególnych, przeprowadzania kontroli. Decyzje tego typu są wysoko programowalne, to znaczy są wcześniej zaplanowane, uzgodnione i uruchamiane prostymi – zazwyczaj też powszechnie znanymi – hasłami lub sygnałami.

Natomiast druga grupa decyzji wymaga poszukiwania niestandardowych kombinacji, opracowania i ocenienia wcześniej nieznanych alternatyw, ale mieszczących się w ogólnie przyjętych i wcześniej ustanowionych ramach, takich, które zwiększają do maksimum powodzenie misji. Tak więc każda decyzja tej grupy, wymaga szczegółowego podejścia do jej przygotowania. W rozwiązywaniu problemów decyzyjnych omawianej grupy dużą rolę odgrywają opinie wysoko kwalifikowanych specjalistów.

Przedstawiłem jeden podział typologiczny, który jest wymieniany w literaturze przedmiotu. Są jeszcze inne, powszechnie znane, i dlatego nie będę ich tutaj przytaczał. Łączy je natomiast, moim zdaniem, jedna prawidłowość: w decyzji jest ważne zarówno sformułowanie właściwego pytania, jak i właściwej odpowiedzi. Nawet najlepsza odpowiedź na źle sformułowane pytanie jest bezwartościowa.

Proces decyzyjny jest różnie opisywany i przedstawiany przez badaczy. Według P. F. Druckera w procesie decyzyjnym występują następujące etapy:

---

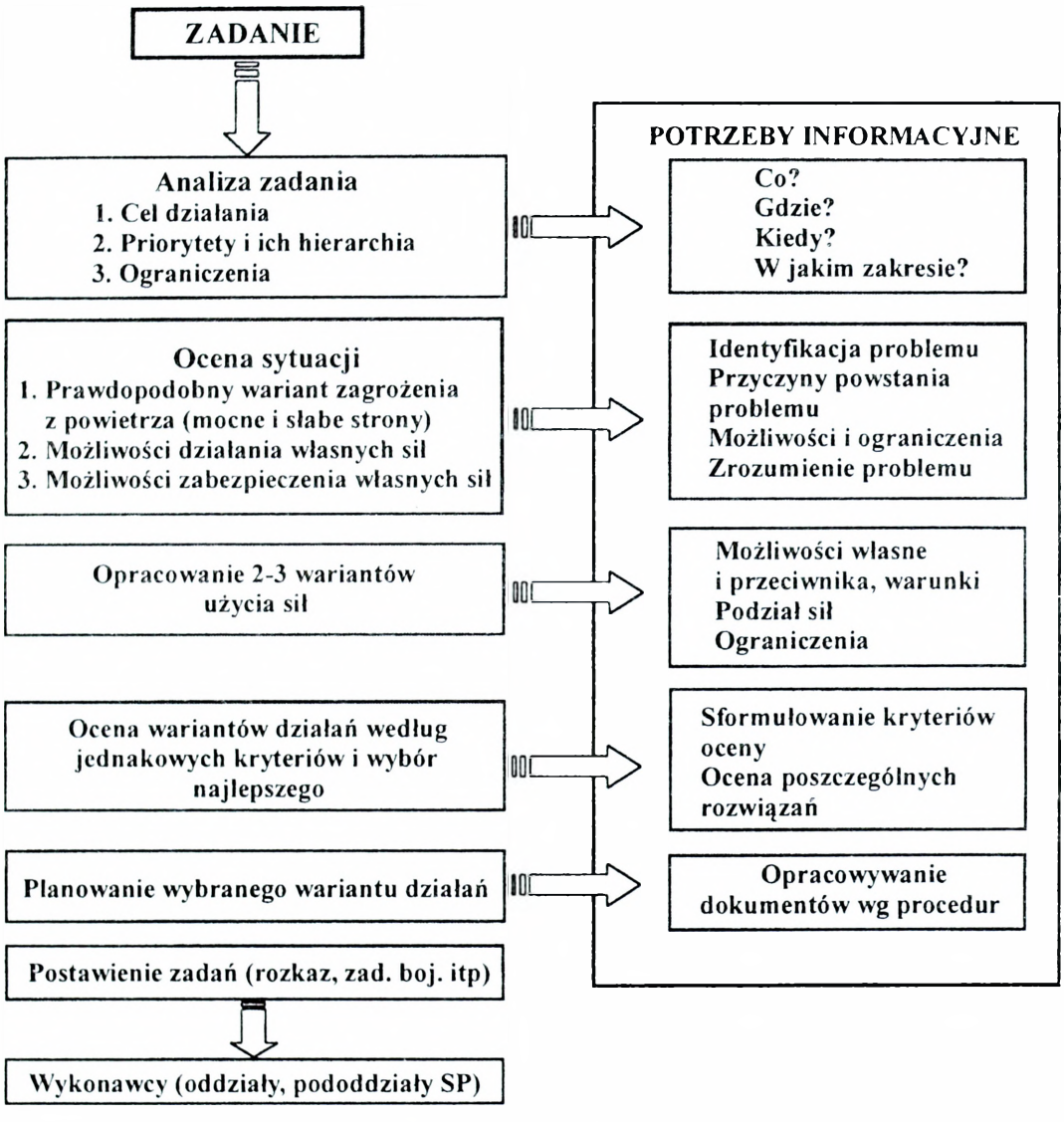
[16] Problem – 1. zagadnienie, zadanie, które wymaga rozwiązania. 2. sprawa, kwestia sporna wymagająca rozstrzygnięcia; kłopot, wiem.onet.pl.

Sytuacja – 1. ogół warunków, w których się coś odbywa; położenie, w którym się ktoś znajduje. *Słownik wyrazów obcych*, M. Jarosz i zespół pod red. I. Kamińskiej-Szmaj. wiem.onet.pl.

[17] Sytuacja problemowa – ogół warunków, w których są rozstrzygane: zagadnienie, zadanie, sprawa, kwestia sporna – wymagające rozstrzygnięcia.

1. Zdefiniowanie problemu (sformułowanie pytania).
2. Analiza problemu.
3. Wypracowanie wariantów rozwiązań.
4. Poszukiwanie rozwiązania optymalnego.
5. Podjęcie decyzji i nadanie jej skuteczności.

Należy przy tym zauważyć, że w obronie powietrznej nadanie skuteczności decyzji to już w pewnym sensie etap następny, zapewniający pomyślną realizację podjętej decyzji. Proces podejmowania decyzji obrazuje rys. 1.



Rys. 1. Proces podejmowania decyzji i potrzeby informacyjne

W procesie podejmowania decyzji, bardzo istotną rolę odgrywa stosowany system dostarczania wszelkich informacji. Ma on zresztą znaczenie nie tylko w procesie decyzyjnym, ale również w edukacji kadry, zwłaszcza na stanowiskach decyzyjnych wszystkich poziomów dowodzenia obroną powietrzną.

Aby informacje w obronie powietrznej spełniały właściwą rolę, powinny być opracowywane według określonych wymogów. Innymi słowy, powinny tworzyć system, który zapewniałby, przede wszystkim, dobór i kompletność informacji oraz jej szybkość umożliwiającą wykorzystanie w procesie decyzyjnym.

W szczególności budowa systemu informacyjnego w obronie powietrznej powinna zapewnić dopływ informacji do decydentów z taką częstotliwością i w takich terminach, ażeby mogły być uwzględniane przy podejmowaniu decyzji.

Podstawowe kryteria budowy systemu to przede wszystkim:

a) *dostosowanie do odbiorcy*, to znaczy, że przekazywane informacje powinny być dostosowane do potrzeb adresata, tj. decydenta na określonym poziomie dowodzenia (dowódcy CAOC, dowódcy CRC, dowódcy zgrupowania WR, szefów określonych komórek organizacyjnych CAOC lub CRC itp.);

b) *możliwość potwierdzenia informacji oraz wiarygodność źródła i danych*, które to wymagania może spełnić korzystanie przede wszystkim z kilku niezależnych źródeł;

c) *aktualność informacji*, to jest przekazywanie takich informacji, które mogą być uwzględniane przy podejmowaniu decyzji;

d) *komunikatywność informacji*, to jest posługiwanie się językiem zrozumiałym, powszechnie używanym w obronie powietrznej, bez zbędnych definicji i pojęć teoretycznych, mających swe odpowiedniki w języku codziennej praktyki kierowania obroną powietrzną;

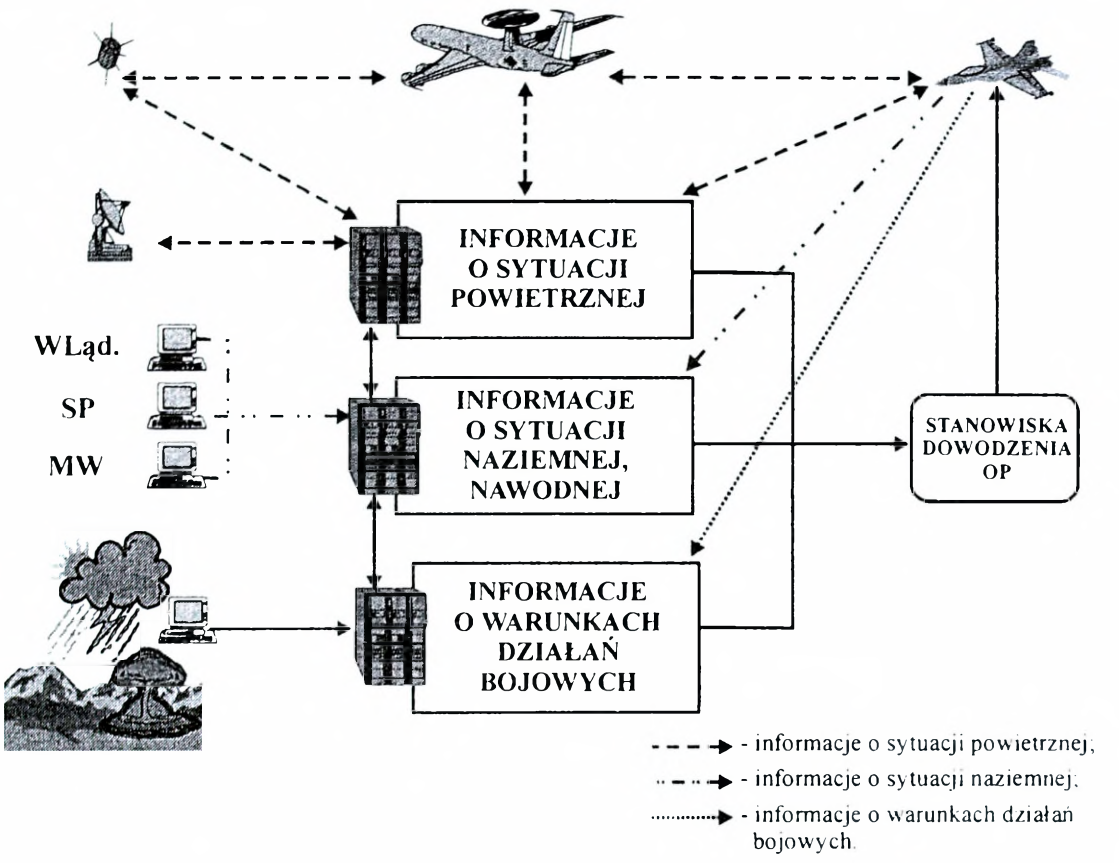
e) *obiektywizm informacji*, to znaczy wykluczenie jakichkolwiek manipulacji jej kontekstami znaczeniowymi;

f) *ekonomiczność informacji*, co oznacza, że przekazywane meldunki, rozkazy, polecenia – w zależności od ich przeznaczenia – powinny zapewniać wszystkie dane istotne, a jednocześnie nie powinny zawierać informacji zbędnych;

g) *stabilność układu informacyjnego i jednolitość stosowanych form*, co pozwala łatwiej przyswajać przekazywane informacje, dzięki przyzwyczajeniom adresatów otrzymywanych informacji.

Przedmiotem informacji winny być, przede wszystkim dane dotyczące sytuacji powietrznej, naziemnej i warunków działania (rys. 2), stopień wykonania zadań planowanych na dany okres (etap) przygotowania i prowadzenia walki oraz wyniki analizy przyczyn występowania niepożądanych odchyleń od założeń. O doborze formy, układu i stopnia szczegółowości informacji, winien decydować główny adresat, po konsultacji z właściwymi szefami merytorycznymi.

W związku z tym, że przedmiotem moich badań jest zarządzanie informacjami istotnymi do racjonalnego użycia zasobów obrony powietrznej, dokonałem oceny stanu faktycznego obecnego SI OP. Badanie prowadziłem pod kątem przesłanek merytorycznych i metodologicznych uwzględniających specyficzny rodzaj zadań i warunków w jakich są wykonywane.



Rys. 2. Ogólna koncepcja SI obrony powietrznej

Przy ocenie stanu faktycznego SI OP, starałem się uzyskać odpowiedź na następujące pytanie: *jakie mechanizmy warunkują realizowanie w nim procesu zarządzania informacjami oraz jakie są rezultaty ich oddziaływania*? Wszystkie prace badawcze na tym etapie diagnozowania miały na celu opracowanie wniosków do sformułowania podstaw teorii zarządzania informacjami w obronie powietrznej. Należy jednak podkreślić różnorodność specyfiki zdobywania, pozyskiwania, przetwarzania i dystrybucji oraz wynikającą z tego różną jakość informacji, często czyniącą ją nieprzydatną do wykorzystania w procesie dowodzenia OP.

Przeprowadzone w tym celu badania, w tym badania techniką ankietowania, między innymi dotyczyły ustalenia: w jakim stopniu są zapewniane potrzeby informacyjne decydentów OP? Respondenci odnieśli się krytycznie do działania istniejącego SI OP. Tylko 5% respondentów oceniło, że funkcjonujący system w pełni zaspokaja potrzeby informacyjne decydentów. 64% respondentów oceniło, że system zaspokaja potrzeby informacyjne w średnim stopniu, 22% – w małym

stopniu i aż 12% respondentów oceniło, że system nie zapewnia potrzeb informacyjnych decydentów OP[18].

Poszukując przyczyn takiego stanu rzeczy założyłem, że do właściwego funkcjonowania obrony powietrznej już nie wystarcza doskonała jakość informacji. Współcześnie prowadzone badania wykazują, że każda działalność, w której partycypują niejednokrotnie doskonale funkcjonujące oddzielnie elementy składowe, jest często postrzegana jako mało efektywna z powodu złej jakości powiązań informacyjnych pomiędzy nimi, a w konsekwencji niedostatecznej koordynacji funkcjonowania całości. Często ta zła jakość powiązań informacyjnych, powoduje niską efektywność globalną instytucji przy nieraz wysokiej efektywności pracy poszczególnych jej elementów. W tak złożonej działalności, jaką jest obrona powietrzna, problem ten jest szczególnie ważny. Składa się bowiem ona z wielu elementów całkowicie się różniących pod względem funkcjonowania wewnętrznego, ale tworzących pewnego rodzaju całość, która tylko wtedy wypełnia swoją rolę właściwie, gdy jej elementy są doskonale powiązane informacyjnie.

Niestety, zdarza się często, że decydenci obrony powietrznej nie mają świadomości tych kwestii, a tym samym nie są przygotowani do stosowania elementów zarządzania ogromną liczbą informacji[19]. W badaniach na pytania zawarte w ankiecie (tabela 1) pozytywnej odpowiedzi udzieliło 75% ankietowanych oficerów, głównie decydentów średniego stopnia (dowództwo eskadry, bazy lotniczej, brygady lotnictwa taktycznego, korpusu sił powietrznych, szefostwa WLOP).

Tabela 1

FRAGMENT KWESTIONARIUSZA OCENY ŚWIADOMOŚCI DECYDENTÓW OBRONY POWIETRZNEJ O STRATEGICZNYM ZNACZENIU INFORMACJI

Mam całkowitą świadomość tego, że:		
– każda działalność w obronie powietrznej ma dwie składowe: fizyczną i informacyjną;	Tak	Nie
– każdy komponent obrony powietrznej winien zwiększyć wysiłki w celu doskonalenia i rozwinięcia składowej informacyjnej w odniesieniu do działalności koncepcyjnej i skuteczności działania;	Tak	Nie
– efektywność globalna obrony powietrznej, którą postrzega przeciwnik, opiera się w równej mierze na jakości każdego jej komponentu, jak i na jakości koordynacji i współdziałania tych elementów;	Tak	Nie
– jakość koordynacji i współdziałania komponentów obrony powietrznej nie jest czymś oderwanym, ale stanowi jej jakość globalną, którą weryfikujemy tak samo, jak jakość w ramach każdego z jej elementów.	Tak	Nie

[18] Zob.: Z. Maślak, *System informacyjnego zabezpieczenia lotnictwa myśliwskiego w działaniach bojowych*, AON, Warszawa 1999, *Wyniki badań*, załącznik 16, p. 1, (rozprawa doktorska).

[19] Dane uzyskane na podstawie badań ankietowych. Badaniem objęto celowo wybranych słuchaczy PSOS, KTO WLOP i Kursu integracji z NATO w latach 2000–2002.

Prowadzone w ostatnim dziesięcioleciu badania zdecydowanie wykazują niezwykle istotną rolę informacji jako czynnika determinującego także postawy indywidualne i grupowe zarówno w samej obronie powietrznej, jak i w jej otoczeniu. W obronie powietrznej, tak jak w każdym złożonym systemie, gdzie elementami są także ludzie, zadaniem informacji jest kształtowanie ich zachowań w taki sposób, by działania były jak najbardziej dostosowane do pomyślnej realizacji założonych celów, ponieważ od jakości komunikowania się w podsystemie społecznym obrony powietrznej zależy, czy efekty zbiorowego wysiłku będą zwielokrotnione na zasadzie synergii, czy też przeciwnie – przy wielkich nakładach energii zespołów ludzkich, osiągać się będzie mizerne efekty.

Informacja może też odegrać ogromną rolę w kształtowaniu korzystnych dla obrony powietrznej działań otoczenia, a w szczególności pozostałych komponentów sił zbrojnych, infrastruktury militarnej państwa, przedstawicieli władz, grup nacisku itp.

Pomimo oczywistego wpływu informacji na efektywność obrony powietrznej, znane są tylko nieliczne przykłady podejmowania problemów zarządzania informacją w tym obszarze. Przyczyną takiego stanu rzeczy jest to, że informacje są najczęściej postrzegane w postaci fragmentarycznej, rozproszonej. Tego rodzaju optyka decydentów obrony powietrznej sprawia, że podejmowane działania nie mają w rezultacie postaci globalnej.

Bardzo często jeszcze w systemie obrony powietrznej spotyka się jej komponenty i szefów różnorodnych komórek, którzy czują się właścicielami pewnych modułów informacyjnych, np. informacje rodzajów wojsk. Jeszcze trudno znaleźć sprawnie działające służby, odpowiedzialne za spójne i skoordynowane przepływy informacji w skali całego systemu obrony powietrznej.

płk dr hab. Marian Cieślarczyk
Wydział Lotnictwa i Obrony Powietrznej AON

CZŁOWIEK – SILNY CZY SŁABY ELEMENT W SYSTEMIE INFORMACYJNO-DECYZYJNYM SIŁ POWIETRZNYCH?

Wstęp

Tak postawione pytanie może budzić różne refleksje i skojarzenia. Po pierwsze kieruje naszą uwagę w stronę człowieka. Człowieka, jakby zapomnianego ogniwa czy – jak kto woli – elementu różnych systemów. Systemów informacyjno-decyzyjnych, ale i systemów działań. Możemy do nich zaliczyć również siły zbrojne i ich struktury organizacyjne.

Przyjęcie systemowego sposobu myślenia, umożliwia postrzeganie człowieka z jednej strony jako względnie autonomicznego systemu informacyjno-decyzyjnego i działaniowego; z drugiej zaś – jako elementu szerszego systemu, jakimi są niewątpliwie siły zbrojne, a w nich siły powietrzne. Czy i w jakim stopniu istnieje kompatybilność tych dwóch elementów rzeczywistości i czy sprzyja to uzyskiwaniu efektu synergii[1], jako jednego z podstawowych warunków rozwoju każdego systemu, w tym również SZ (SP)? Jest to pytanie, na które trudno dziś udzielić jednoznacznej odpowiedzi. Nie oznacza to jednak, że prób takich nie należy podejmować.

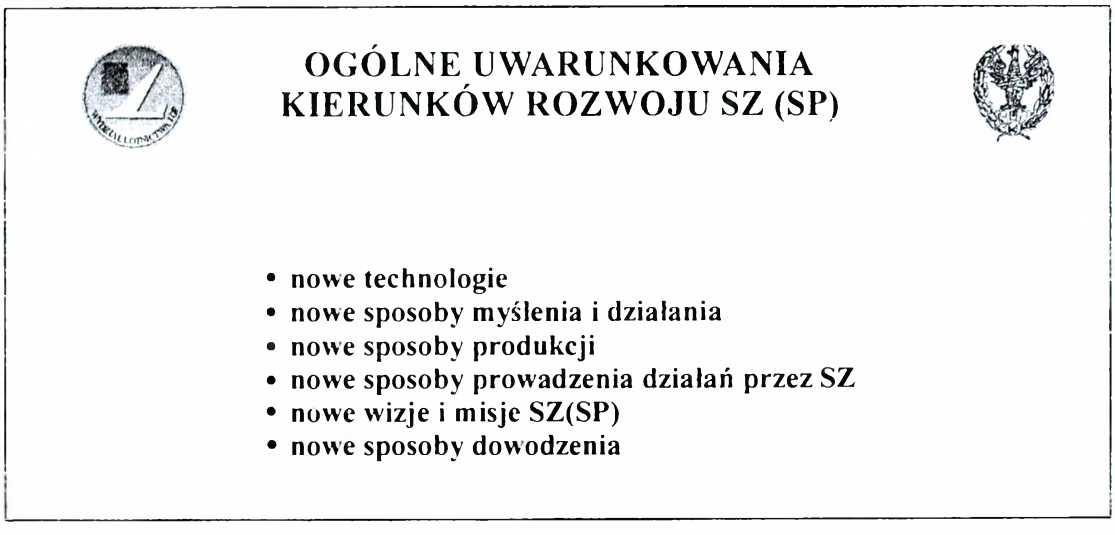
Po drugie – przemiany cywilizacyjne[2] i związany z nimi proces transformacji sił zbrojnych, a w nich sił powietrznych, przynoszą wiele zmian w obszarze teorii i praktyki ich funkcjonowania. Niektóre teorie, pojęcia i zjawiska przechodzą do lamusa historii; w ich miejsce wchodzą nowe, bardziej adekwatnie opisujące i wyjaśniające rzeczywistość. Rzeczywistość – która się staje. Stanowi to ważne wyzwanie dla nauk wojskowych (nauk o bezpieczeństwie), ale także dla humanistów w siłach zbrojnych. Nauki te bowiem powinny być przydatne nie tylko do opisywania i wyjaśniania stającej się rzeczywistości, ale również do przewidywania kierunków rozwoju tej rzeczywistości i jej projektowania. Refleksja ta dotyczy także systemów informacyjno-decyzyjnych, systemów dowodzenia i roli w nich

[1] Por. L. J. Krzyżanowski, *O podstawach kierowania organizacjami inaczej*, Warszawa 1999.
[2] Zob.: A. Toffler, *Trzecia fala*, Warszawa 1986; A. i H. Toffler, *Wojna i antywojna*, Warszawa 1997.

człowieka jako użytkownika tych systemów, a zarazem ich elementu. Tak postrzeganą rolą człowieka we współczesnych SZ (SP) zamierzam się zająć w swoim referacie. W jego pierwszej części przedstawię obiektywne uwarunkowania kierunków rozwoju współczesnych sił zbrojnych, a w nich sił powietrznych. W części trzeciej zaś postaram się ukazać niektóre procesy i zjawiska postrzegane wewnątrz naszych SZ (SP), ze zwróceniem szczególnej uwagi na problemy informacyjno-komunikacyjne. Swoistym łącznikiem między pierwszą i trzecią częścią mojego wystąpienia są rozważania teoretyczne, które się mogą okazać przydatne zarówno przy analizie i interpretacji niektórych procesów i zjawisk wewnątrz SZ (SP) i w ich otoczeniu, jak też przy formułowaniu sugestii i wniosków zawartych w ostatniej części mojego wystąpienia.

Niektóre uwarunkowania kierunków rozwoju współczesnych SZ (SP)

Jakość i sposób funkcjonowania sił zbrojnych, zawsze były związane z ogólnym rozwojem cywilizacyjnym człowieka. Obecny etap tego rozwoju – cywilizacja informacyjna – niesie ze sobą wiele zmian, również w odniesieniu do SZ (SP). Zasadnicze z nich przedstawiono na rysunku 1.



Rysunek 1.

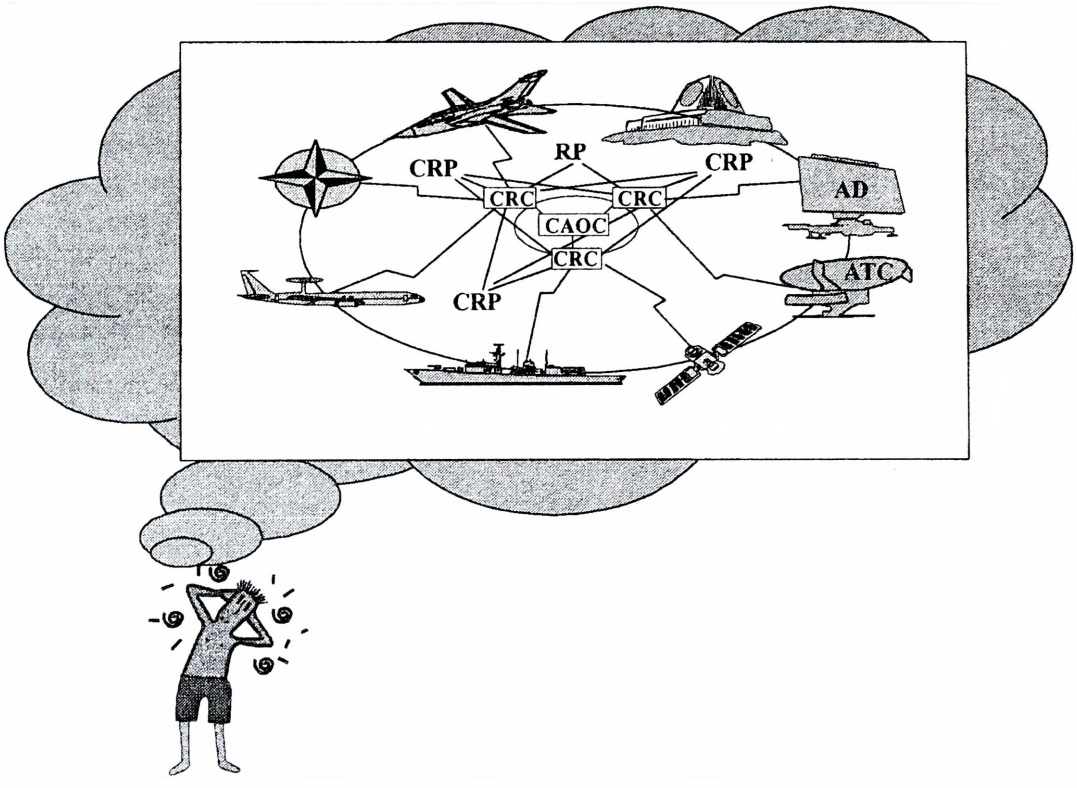
Jakość tych zmian we współczesnym świecie, ich tempo i zakres powodują, że *otoczenie* człowieka i organizacji, w którym funkcjonują te podmioty, jawi się im jako:

a) turbulentne;

b) szybko się zmieniające;

c) trudno przewidywalne.

Dlatego też czasami czujemy się w nich zdezorientowani i zagubieni.



Rysunek 2.

Mówiąc o tendencjach zmian w SZ, należy podkreślić, że w ostatnim dziesięcioleciu XX wieku pojawiła się nowa forma prowadzenia działań bojowych, która dość wiernie odwzorowuje formę tworzenia dóbr materialnych. Przykładowo biorąc, w „Pustynnej Burzy" działania bojowe prowadzono według reguł odpowiadających wojnom III fali (cywilizacji informacyjnej), przy jednoczesnych działaniach charakterystycznych dla wojen II fali, czyli okresu przemysłowego. Pierwszy rodzaj kampanii przypominał precyzyjną operację układu nerwowego przeciwnika, drugi zaś niósł ze sobą śmierć wielu żołnierzy i cywilów. Ten pierwszy rodzaj działań bojowych miał za zadanie „oślepić" przeciwnika, zniszczyć jego urządzenia przekazujące rozkazy, odciąć łączność, przejąć inicjatywę, uderzyć głęboko. Jednocześnie starano się uniemożliwić wykorzystanie przez przeciwnika jego odwodów, zintegrować operacje powietrzne, lądowe i morskie, zsynchronizować układ takich operacji. Przede wszystkim zaś, wiedziano co czyni przeciwnik i zapobiegano temu, by on wiedział, co my czynimy. Pojawiły się więc dosyć wyraźne elementy walki i wojny informacyjnej.

Ogólnie biorąc, w działaniach tych informacja i wiedza spełniały rolę tarczy i miecza jednocześnie, a *potencjał intelektualny okazał się coraz bardziej znaczącym elementem potencjału bojowego*. Z dostępnych źródeł wynika, że pod koniec „Pustynnej Burzy" w strefie wojny funkcjonowało ponad trzy tysiące komputerów połączonych w system. Pracowali na nich nie tylko wojskowi, ale i cywile. Oczy-

wiście, dotyczyło to w różnym stopniu poszczególnych rodzajów wojsk i sił zbrojnych. W najszerszym zakresie było widoczne w działaniach sił powietrznych. Z całą wyrazistością uwidocznił się wówczas fakt, że współczesny pilot nie działa samotnie, zamknięty w kabinie, chociaż i na taką ewentualność powinien być przygotowany. Jest on częścią bardzo złożonego systemu interakcyjnego, wspieranego informacyjnie zarówno przez naziemne radary i „latający intelekt", jakim jest np. system AWACS, jak też przez sztaby odpowiednio przygotowanych analityków i innych specjalistów.

Faktem jest...

Tworząca się **LUKA**
między:
Tempem rozwoju
systemów techniczno-informacyjnych

↑

a

↓

Przygotowaniem człowieka do ich
efektywnego wykorzystania

Rysunek 3.

Wskazuje to, że na współczesnym polu walki wielu żołnierzy musi umieć, między innymi, sprawnie przetwarzać olbrzymią ilość informacji, podejmować decyzje o dużym stopniu trudności, dostosowując się do dynamicznie zmieniającej się sytuacji. Coraz większego znaczenia nabiera więc sposób dowodzenia przez cele. Jednak, jak trafnie zauważył prof. E. Zabłocki: „*... aby dowodzić przez cele, należy umieć cele te formułować*"[3]. Kieruje to naszą uwagę w stronę człowieka i czynnika ludzkiego na współczesnym polu walki. Nie pomniejszając roli techniki można stwierdzić, że czynnik ludzki w dalszym ciągu pozostaje decydującym, chociaż jeszcze nie zawsze docenianym elementem coraz bardziej złożonych systemów. W armiach najbardziej rozwiniętych rola tego czynnika (kapitału ludzkiego) rośnie. Niemniej jednak, nawet tam się uwidacznia coraz wyraźniej luka między współczesną techniką a czynnikiem ludzkim. Bardziej konkretnie, a zarazem obrazowo, możemy myśl tę przedstawić w następujący sposób: luka ta się powiększa szczególnie wyraźnie w państwach i armiach słabiej rozwiniętych. Z powodu braku nowoczesnej techniki nie inwestują one wystarczająco w potencjał ludzki,

[3] „Przegląd Wojsk Lotniczych i Obrony Powietrznej", wrzesień 1996.

powodując powiększanie się wyżej wspomnianej luki. Potem, jeśli nawet pojawi się możliwość nabycia nowoczesnej techniki, trudno im będzie jednak dogonić czas[4].

Zasygnalizowane wyżej zjawisko luki między tempem rozwoju systemów techniczno-informacyjnych a przygotowaniem człowieka do efektywnego ich wykorzystania, jest widoczne chociażby w odniesieniu do potencjalnych możliwości dostępnego już dziś sprzętu komputerowego.

Rola człowieka i nowoczesnych struktur organizacyjnych, w połączeniu z nowoczesną techniką, uwidoczniła się szczególnie wyraźnie w działaniach bojowych w rejonie Zatoki Perskiej. Opierając się na doświadczeniach z operacji „Pustynna Burza" warto przypomnieć, że w przeciwieństwie do wojsk irackich siły alianckie nie były maszyną, lecz systemem o wewnętrznym sprzężeniu zwrotnym, lepszej komunikacji i zdolności do autoregulacyjnych poprawek. Były więc inteligentnym systemem, charakterystycznym dla cywilizacji informacyjnej.

W kontekście powyższych rozważań zatrzymajmy się jeszcze przy zagadnieniu bitwy powietrzno-lądowej. Termin, ale i zjawisko bitwy powietrzno-lądowej, zwraca uwagę na potrzebę ścisłej koordynacji działań powietrznych i lądowych w relacjach do newralgicznych elementów systemu przeciwnika. Nie chodzi w tym przypadku li tylko o jego wojska, ale również o te elementy szeroko rozumianego systemu społeczno-organizacyjnego, od którego jest uzależnione funkcjonowanie sił zbrojnych. W miarę szczegółowa analiza operacji prowadzonych w rejonie Zatoki Perskiej i w Kosowie, pozwala dostrzec narodziny nowego paradygmatu prowadzenia działań zbrojnych. Najogólniej biorąc, sprowadza się on do pozbawienia przeciwnika woli walki, a nie fizycznego jego zniszczenia. Idea ta jest głównie realizowana metodą, którą można nazwać dekompozycją systemową. Szczególnie wyraźnie uwidoczniła się ona w Kosowie. Trudno przecenić rolę, jaką odegrały tam siły powietrzne.

Wracając do głównego nurtu rozważań warto zauważyć, że nowe doktryny uwzględniają wykorzystanie siły na dużą odległość w jak najkrótszym czasie. Czas staje się dziś coraz bardziej docenianym elementem potencjału bojowego. Chociaż, obiektywnie biorąc, zawsze odgrywał on w działaniach bojowych bardzo ważną rolę, jednak świadomość znaczenia czasu w działaniach współczesnych SZ (SP), systematycznie rośnie. Wiąże się to, między innymi, z coraz lepiej rozpoznawanym i wykorzystywanym na potrzeby sił zbrojnych zjawiskiem synergii[5]. Jest ono osiągane, między innymi poprzez synchronizację i koordynację działań i współdziałań poszczególnych elementów systemu. Do osiągnięcia tego efektu, niezbędnym czynnikiem jest odpowiednia informacja przekazywana w czasie zbliżonym do rzeczywistego, ale również umiejętność efektywnego korzystania z informacji.

Czy, w związku z tym, bezzasadne może być pytanie: w jakim stopniu i zakresie jesteśmy do tego przygotowani? Przecież odpowiedni sprzęt może się pojawić stosunkowo szybko. Jednak właściwe przygotowanie człowieka do obsługiwania i efektywnego wykorzystania tego sprzętu, wymaga wielu lat żmudnej, wytrwałej

---

[4] Por. A. Targowski, *Dogonić czas*, Warszawa 1993.

[5] Zob. L. J. Krzyżanowski, op. cit.

pracy, biorąc pod uwagę nie tylko realizację procesu dydaktycznego i szkoleniowego, ale również potrzebę opracowania adekwatnych do potrzeb programów kształcenia i szkolenia, – tym bardziej, że nie chodzi li tylko o przygotowanie do działań wojennych, ale również do operacji innych niż wojna[6].

Tym samym zbliżyliśmy się do funkcji, jakie obecnie pełnią siły zbrojne, a w nich siły powietrzne. Mówiąc o funkcjach SZ (SP) mam na myśli zarówno funkcje faktycznie spełniane, jak też wyobrażenia i oczekiwania społeczne w tym zakresie. Weźmy np. pod uwagę fakt, że jeszcze w drugiej połowie lat 90. podstawową funkcją SZ (SP), jaka jawiła się w świadomości naszego społeczeństwa, była funkcja obrony terytorium kraju[7]. Jeśli funkcja ta – w wymiarze obiektywnym – traci na znaczeniu i aktualności, to czy powyższa sytuacja będzie sprzyjać legitymizacji SZ (SP) w społeczeństwie i łożeniu przez to społeczeństwo konkretnych świadczeń materialnych i osobowych na rozwój SZ (SP)? Jest to problem, który powinien być systematycznie monitorowany, chociażby za pomocą odpowiednich badań socjologicznych.

Na funkcjonowanie sił zbrojnych i sposoby prowadzenia wojen, niezaprzeczalny wpływ wywierają również przemiany technologiczne. Jednak nie zawsze pamiętamy o tym, że dopiero zmiany fundamentalnych zasad prowadzenia tej swoistej gry, jaką jest konflikt zbrojny, zmienia istotę samej gry. Dotyczy to, między innymi reguł jej prowadzenia, wyposażenia, rozmiarów i organizacji struktur. W związku z tym zmieniają się również zasady kształcenia i szkolenia, doktryna, taktyka itd., a także relacje między siłami zbrojnymi a społeczeństwem.

Polscy znawcy tych zagadnień (B. Balcerowicz, S. Koziej, R. Wróblewski, W. Michalak, B. Zdrodowski, Z. Scibiorek, M. Wiatr i inni) dosyć zgodnie stwierdzają, że współcześnie o sukcesie w działaniach SZ decydują takie podstawowe parametry, jak *zasięg, śmiercionośność* i *szybkość*. Niektóre z nich, jak np. śmiercionośność, nie muszą być stosowane. Wystarczy istnienie potencjalnej możliwości ich wykorzystania. Uwidacznia się więc coraz wyraźniej wypełniana przez siły zbrojne, a szczególnie siły powietrzne, funkcja odstraszania[8]. Nie ulega wątpliwości, że we współczesnym świecie jedynym rodzajem sił zbrojnych (rodzajem wojsk), które spełniają te warunki, są siły powietrzne. One przede wszystkim wpływają na teraźniejsze sposoby prowadzenia wojen, ale również odgrywają podstawową rolę w działaniach innych niż wojna. One prawdopodobnie będą również wywierać podstawowy wpływ na opanowanie przestrzeni kosmicznej, która może decydować o naszej przyszłości na Ziemi.

---

[6] W *„Doktrynie operacyjnej wielonarodowych połączonych sił Sojuszu AJP-01"* do działań innych niż wojna zalicza się: zapobieganie konfliktom, kontrola zbrojeń i działania przeciwdziałające rozprzestrzenianiu broni, operacje wspierania pokoju, budowanie pokoju, operacje niesienia pomocy humanitarnej, operacje ewakuacyjne o charakterze niebojowym. W Akademii Obrony Narodowej w Warszawie funkcjonuje od niedawna Zakład Działań Połączonych, kierowany przez płk. dr. hab. M. Wiatra.

[7] Zob. badania WIBS.

[8] Zob. R. Olszewski, *Siły powietrzne w odstraszaniu militarnym*, Warszawa 1999.

Zwiększona zdolność sił powietrznych do dostępu, przetwarzania i przechowywania informacji, połączona z olbrzymim wzrostem zależności tych sił od systemów i infrastruktury informacyjnej, doprowadziły siły powietrzne do ponownego zbadania i przedefiniowania sposobu, w jaki siły te integrują działalność informacyjną ze swoimi podstawowymi funkcjami. Zatem – jak stwierdzono w AFDD 1 (podstawowej doktrynie sił powietrznych) – dominacja w sferze informacyjnej jest obecnie równie ważna, jak w przeszłości ważna była kontrola przestrzeni powietrznej i kosmicznej czy okupowanie terenu. Dominacja ta jest widziana jako nierozerwalny i synergiczny element potęgi powietrznej.

Siły powietrzne są więc tym komponentem sił zbrojnych, w których połączenie specyficznych cech – przestrzeni powietrznej jako obszaru działań zbrojnych oraz prymatu jakości uzbrojenia, wyszkolenia i zabezpieczenia (w tym również informacyjnego) nad czynnikiem ilościowym – decyduje o powodzeniu w walce[9]. Należy podkreślić, że gwałtowny rozwój technologii informacyjnej (komputerów, procesorów i narzędzi wspomagania procesów decyzyjnych) w zasadniczy sposób zmienił zarówno systemy wojskowe sił powietrznych, jak i koncepcje ich wykorzystania. Obecnie trudno znaleźć jakiś główny system uzbrojenia sił powietrznych czy inny system, który nie byłby uzależniony od zaawansowanej elektroniki i precyzyjnej informacji. Zależność ta ciągle wzrasta. W świecie, gdzie procesory komputerowe podwajają swoją prędkość co kilkanaście miesięcy i są natychmiast dostępne na rynku, siły powietrzne muszą być zdolne do adaptacji zarówno nowych technologii, jak i koncepcji działań jeszcze szybciej niż czynią to dzisiaj. W tej sytuacji reaktywność i elastyczność stają się dla potęgi powietrznej jeszcze bardziej znaczącym czynnikiem niż kiedyś.

Efektem wzrastającego powiązania zależnych od informacji systemów broni jest wyniesienie, śledzenia i rozpoznania pola walki (ISR) do rangi podstawy sukcesu wszelkich działań militarnych. Zasoby ISR dążą do uzyskania doskonałego rozumienia informacji przeciwnika oraz jego słabych i mocnych stron w celu przeprowadzenia analizy wrażliwości informacyjnej. W niektórych przypadkach trudno jest określić, co jest zdolnością śledzenia i rozpoznania pola walki w porównaniu do zdolności walki informacyjnej; faktycznie czasami platforma czy system może być jednym i drugim. Zatem śledzenie i rozpoznanie pola walki są równie ważną częścią obronnej infrastruktury informacyjnej i muszą być chronione, ponieważ dostarczają kluczowych informacji pozwalających na ochronne, odwetowe i ofensywne działania w tym zakresie[10]. Zdaniem dyrektora Centralnej Agencji Wywiadowczej istnieją dowody na to, że duża liczba państw na świecie rozwija doktrynę, strategie i narzędzia do prowadzenia ataków informacyjnych na komputery wojskowe[11].

Czy – w związku z tym – jesteśmy przygotowani do prowadzenia działań w takich warunkach, jeśli nawet bez tego utrudnienia mamy nierzadko problemy z po-

---

[9] Por. W. Michalak, Wykład inauguracyjny komendanta Wydziału WLOP AON w 1999 r.

[10] Zob.: R. Szpyra, *Walka informacyjna w przyszłych działaniach sił powietrznych*, AON, Warszawa 2000; L. Ciborowski, *Wojna informacyjna*, Warszawa 1999.

[11] „The Washington Post", 26 June 1996.

dejmowaniem najkorzystniejszych decyzji oraz działań? Czy i jak poradzimy sobie bez komputerów, w przypadku ewentualnego wyeliminowania ich z tej specyficznej gry, jaką są działania bojowe? Są to pytania tylko z pozoru teoretyczne. Wiadomo przecież, że nowoczesne armie muszą gromadzić, przechowywać i wykorzystywać duże ilości informacji. Do celu tego służą odpowiednie systemy, składające się z wielu wzajemnie powiązanych elementów. W systemach tych najszybciej się zmienia element techniczny, najwolniej zaś element ludzki (kapitał ludzki). Stanowi więc on najważniejsze, ale jednocześnie często najsłabsze ogniwo tego systemu[12]. Potwierdzają to wyniki badań[13], z których wynika, że szeroko rozumiana kultura informacyjna naszej kadry (nie chodzi li tylko o kulturę informatyczną) pozostawia jeszcze wiele do życzenia. Jest to jak dotychczas jeszcze słabo rozpoznane zagadnienie.

Warto jednak pamiętać, że kształtowaniu kultury informacyjnej oraz taktycznej i operacyjnej wyobraźni, tak potrzebnych współczesnemu dowódcy wraz z umiejętnością oceny sytuacji i podejmowania decyzji, służą odpowiednie systemy symulacji komputerowej[14]. Również w tej dziedzinie nasze siły zbrojne, a w nich siły powietrzne, mają jeszcze wiele do zrobienia. Pojawiające się na horyzoncie pierwsze jaskółki rozwiązania tego problemu, prawdopodobnie nie czynią jeszcze przysłowiowej wiosny. Ważne jednak, że problem ten jest już przedmiotem zainteresowania zarówno decydentów, jak i wysokiej klasy specjalistów[15].

W kontekście powyższych rozważań należy zauważyć, że sieci informatyczno-informacyjne wpływają nie tylko na zmianę charakteru i sposób funkcjonowania struktur organizacyjnych, ale również struktur myślowych. Poziome przepływy informacji powodują, że struktury organizacyjne stają się coraz bardziej spłaszczone, wskutek czego obniża się ich środek ciężkości. Jednocześnie wzrasta poczucie podmiotowości i odpowiedzialności ludzi funkcjonujących w tych strukturach. Również to zjawisko uwidacznia się najszybciej i najbardziej wyraźnie w siłach powietrznych.

Podsumowując tę część rozważań chciałbym stwierdzić, że o ile posiadanie i wykorzystanie informacji zawsze było ważną częścią działań wojennych, to w przyszłości może ono się stać głównym czynnikiem wpływającym na wynik konfliktu. Powtórzmy więc raz jeszcze wcześniej postawione pytanie: czy i w jakim zakresie jesteśmy do tego przygotowani?

Próbę odpowiedzi na to pytanie, którą podjąłem w ostatniej części mojego referatu, chciałbym poprzedzić kilkoma refleksjami teoretycznymi, przydatnymi – jak się wydaje – przy interpretacji wielu nowych procesów i zjawisk we współczesnych siłach powietrznych.

---

[12] Zob. J. Babula, *Potrzeby i możliwości usprawnienia systemów kierowania*, „Myśl Wojskowa" nr 2, 1993.

[13] Zob. M. Cieślarczyk, *Diagnozowanie zjawisk komunikacji i obiegu informacji na potrzeby dowodzenia*. Sprawozdanie z badań WBBS, Warszawa 1997.

[14] Imponującym dorobkiem w tym zakresie może się pochwalić Akademia Dowodzenia w Hamburgu.

[15] Chodzi o podejmowane w Akademii Obrony Narodowej prace koncepcyjne i organizacyjne (z wykładu prof. P. Sienkiewicza w Wydziale WLOP AON).

Procesy informacyjno-decyzyjne w życiu człowieka i organizacji – kilka refleksji teoretycznych

Przekazywanie i wykorzystanie informacji towarzyszyło człowiekowi od zarania jego dziejów. Zawsze miało ono na celu kształtowanie przyszłych zdarzeń, chociaż działo się to pośrednio. Eliminowanie niepewności co do przyszłości jest nie tylko jedną z przyczyn naszej ciekawości, ale także stymulatorem aktywności człowieka i jej mądrego wykorzystywania. Ma więc znaczenie praktyczne, również w sferze militarnej. Już bowiem sukcesy militarne Rzymian były związane z systemem przekazywania informacji, głównie na piśmie i przez posłańca. Również sukcesy Napoleona w dużym stopniu wiązały się z umiejętnym, szybkim i dokładnym przekazywaniem informacji militarnych i ekonomicznych[16]. Trudną do przecenienia rolę i znaczenie informacji, ale i dobrej organizacji dla współczesnych sił zbrojnych, a w nich sił powietrznych, potwierdzają wspomniane wcześniej doświadczenia z działań militarnych w rejonie Zatoki Perskiej oraz na terenie byłej Jugosławii.

Znaczenie informacji dla współczesnego człowieka, w sposób syntetyczny przedstawia następujący cytat: „*Wyprowadzać wnioski – to wielkie zadanie życia. Każdy człowiek co dzień, co godzina, co chwila musi przyjmować jako stwierdzone fakty, których nie obserwował bezpośrednio. I to nie ze względu na jakiś cel ogólny, by powiększyć swój zasób wiedzy, lecz dlatego, że fakty same przez się mają znaczenie dla jego interesów czy też jego zajęć. Zadaniem sędziego, dowódcy wojskowego, pilota, lekarza, rolnika, jest po prostu wydawać sąd o danych i odpowiednio działać*"[17].

W myśli tej zwraca uwagę wyraźnie zarysowana zależność między informacją a działaniem, a właściwie takimi jego aspektami, jak sprawność, skuteczność i efektywność. Tylko w działaniu i współdziałaniu sprawnym, skutecznym i efektywnym, osiągamy bowiem efekt synergii[18], jako warunek sine gua non trwania przetrwania i rozwoju pojedynczego człowieka, grup społecznych i społeczeństw Istota tego zjawiska w siłach zbrojnych najwyraźniej uwidacznia się w działaniach (operacjach) połączonych.

W wielu pozycjach literatury znajdziemy argumenty na poparcie tezy, że uzyskanie efektu synergii jest możliwe tylko w sytuacji działania i współdziałania dobrze zorganizowanego. Wskazuje to, że sposób zorganizowania się i poziom organizacji społeczeństw, grup społecznych i zawodowych oraz ich struktur organizacyjnych, wywiera przemożny wpływ na sprawność, skuteczność i efektywność działania poszczególnych podmiotów, a tym samym na wypełnianie przez nie swych funkcji i osiąganie zakładanych celów. Refleksja ta ma szczególne znaczenie dla sił zbrojnych, a w nich sił powietrznych.

---

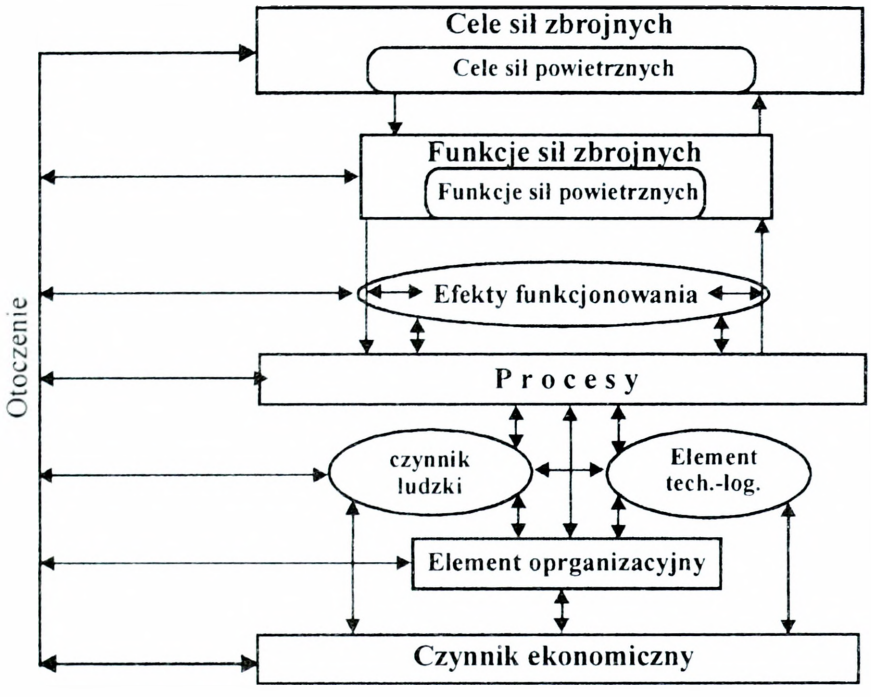
[16] Zob. J. F. Mączyński, *O niektórych anomaliach (sprzecznościach) wewnętrznych społeczeństwa informacyjnego*. [w:] *Społeczeństwo informacyjne*, (red. nauk.), L. Zacher, Warszawa 1999, s. 21.

[17] Op. cit., s. 43.

[18] Por. L. J. Krzyżanowski, op. cit.

Swoistą metafunkcją i podstawowym celem struktur organizacyjnych sił powietrznych jest budowanie i umacnianie ich potencjału bojowego oraz kształtowanie umiejętności i mechanizmów efektywnego korzystania w potrzebie z tego potencjału. Swoistym kluczem do uruchomienia procesu budowania potencjału bojowego struktur organizacyjnych SP jest już wspomniany efekt synergii. Jednym z warunków zaistnienia tego efektu są właściwe relacje między elementami systemu społeczno-organizacyjnego i informacyjno-komunikacyjnego. W pewnym uproszczeniu, przedstawia to rysunek 4.

Struktury organizacyjne SP jako systemy działania i elementy SZ



Rysunek 4.

Stwierdzenie właściwe relacje odnosi się nie tylko do każdego systemu, ogólnie biorąc. Chodzi również, a może przede wszystkim, o właściwe relacje w odpowiednim czasie i w odpowiednim miejscu, czyli w konkretnej sytuacji. Jest to jeden z istotnych aspektów szeroko rozumianej elastyczności struktur organizacyjnych, ale także struktur myślowych. Służy temu odpowiedni system informacji i komunikowania oraz adekwatne do potrzeb mechanizmy społeczne, takie np., jak procedury dowodzenia, procedury działania. Ich kompatybilność ma trudne do przecenienia znaczenie w działaniach sojuszniczych. Dzięki efektowi synergii w siłach zbrojnych (SP) budujemy potencjał bojowy poszczególnych struktur organizacyjnych oraz SZ (SP) jako całości. Jak już wspomniano – potencjał ten po-

wstaje w działaniu i współdziałaniu. Także w działaniu, np. na polu walki[19] czy na ćwiczeniach – jest on uaktywniany i wykorzystywany. Jeśli zachodzi taka potrzeba jest również wykorzystywany, a może przede wszystkim, do osłabienia (rozładowania) potencjału przeciwnika.

W kontekście powyższych rozważań, warto skorzystać z poglądów P. Sienkiewicza na temat potencjału bojowego. Autor ten rozgranicza istnienie *potencjału bazowego i potencjału bojowego*[20]. Zarówno w jednym, jak i w drugim przypadku uwzględnia on współczynnik systemotwórczy. Współczynnik ten zależy od potencjału ludzkiego, technicznego, energomateriałowego i sterowniczego, a także od czasu t. Nie ulega wątpliwości, że ogniwem spajającym, ale i uruchamiającym wszystkie pozostałe elementy potencjału jest jednak czynnik ludzki.

Rozważania o potencjale bojowym kierują naszą uwagę w stronę pojęć organizacja oraz informacja i komunikowanie, a także ściśle z nimi związanymi pojęciami kultura organizacyjna i kultura informacyjno-komunikacyjna. Organizację traktuje się najczęściej jako twór celowy; w węższym zaś znaczeniu – jako racjonalny i przemyślany logicznie system metod i środków, służący efektywnemu osiąganiu celu (celów)[21]. Taki pogląd prezentuje, między innymi H. A. Simon. Autor ten dużą wagę przywiązuje do systemu informacji i komunikowania, który w organizacji (strukturze) jest czasami porównywany do układu nerwowego. Ten układ „nerwowy" w dużym stopniu warunkuje aktywność i reaktywność danego podmiotu (systemu) oraz jego elementów. Wpływa także na sprawność, skuteczność i efektywność działania oraz szeroko rozumianą „żywotność" systemu i jego elementów. Istotnym czynnikiem wyżej wspomnianej żywotności struktur organizacyjnych sił powietrznych jest ich elastyczność. Cecha ta nabiera szczególnego znaczenia w świetle doświadczeń z ostatnich konfliktów zbrojnych. Mówiąc o elastyczności mamy na myśli wspomnianą wcześniej elastyczność struktur organizacyjnych, ale także elastyczność struktur myślowych oraz związaną z tym elastyczność działania. W sytuacji częstych zmian otoczenia i jego dużej nieokreśloności jest to cecha i wartość bardzo cenna.

Obok elastyczności warto jednak również pamiętać o konsekwencji i wytrwałości w działaniu. Chodzi jednak o mądrą konsekwencję i mądrą wytrwałość. Wiąże się to zarówno z technologią intelektu[22] i technologią struktur organizacyjnych, ale także ze wspominanym już wielokrotnie systemem informacji i komunikowania. Spełniają one w działaniach SZ (SP) trudną do przecenienia rolę.

Konkludując należy stwierdzić, że właściwa informacja w konkretnych działaniach pozwala decydentowi (dowódcy) umiejętnie łączyć te z pozoru sprzeczne cechy, jakimi są: z jednej strony elastyczność, z drugiej zaś konsekwencja i wytrwałość w dążeniu do celu. Są to cechy i wartości dowódcy, zachowujące ponad-

---

[19] Pojęcie „pole walki" rozumiemy szeroko, uwzględniając również działania inne niż wojna.

[20] Zob. P. Sienkiewicz *Metodologiczne podstawy oceny potencjałów i efektywności bojowej systemów wojskowych*, AON, Warszawa 1992.

[21] Por. J. G. March, H.A. Simon, *Teoria organizacji*, Warszawa 1964.

[22] Por. M. Marody, *Technologie intelektu*, Warszawa 1987.

czasową aktualność. Ich znaczenie dla sił zbrojnych, a szczególnie sił powietrznych, będzie wzrastać.

Razem z niezbędną informacją i umiejętnością jej wykorzystania duża rola przypada także nowoczesnej technice, w tym technice komputerowej. Warto teraz przywołać jedną z wielu interesujących refleksji S. Lema[23]. Uważa on, że szybki rozwój techniki ma olbrzymie konsekwencje kulturowe. Może bowiem spowodować przerwanie ciągłości ludzkiego doświadczenia, nawet w obrębie dwóch następujących po sobie pokoleń. Jest to sytuacja, która powoduje uruchomienie mechanizmu: wyzwanie – reakcja, a kultura, jaka się rodzi jest nowością, która może okazać się nawet swoistym cyfrowym opium.

Z drugiej strony upowszechnia się przekonanie, że istotą przemian prowadzących do społeczeństwa informacyjnego nie jest rozwój środków technicznych, czyli komputerów, infostrad, multimediów itp., lecz kształtowanie struktur i mechanizmów społecznych, zdolnych z pożytkiem wykorzystać posiadaną technikę i uzyskane informacje. Ma to szczególne znaczenie dla sił zbrojnych, a w nich sił powietrznych. Warto jednak pamiętać, że to *ludzie projektują struktury i to oni w nich funkcjonują. Ludzie o określonych wartościach, predyspozycjach i kwalifikacjach; ludzie o określonej technologii intelektu, o określonej mentalności; ludzie o określonym poziomie kultury informacyjno-komunikacyjnej i organizacyjnej, ludzie charakteryzujący się określoną kulturą dowodzenia i zarządzania.*

Nie można jednak pomijać faktu, że ludzie ci funkcjonują w konkretnych, obiektywnych warunkach, wywierających określony wpływ zarówno na możliwości i efekty ich działania i współdziałania, jak też na ich świadomość oraz inne elementy szeroko rozumianego morale.

Nie ulega wątpliwości, że jednym z warunków pomyślnej realizacji idei nowoczesnych SZ, a szczególnie SP, i ich współpracy w wymiarze koalicyjnym jest wysoka kultura organizacyjna i jej istotny element – kultura informacyjno-komunikacyjna. Znaczenie tych zagadnień dla sił zbrojnych cywilizacji III fali, szczególnie zaś dla sił powietrznych, będzie rosło. Mogą na to wskazywać nie tylko argumenty wcześniej przedstawione, ale również to, że poziom kultury informacyjno-komunikacyjnej i organizacyjnej kadry sił powietrznych staje się – w cywilizacji informacyjnej – wartością autoteliczną, a jednocześnie coraz bardziej znaczącym elementem potencjału bojowego struktur organizacyjnych SZ w wymiarze narodowym i sojuszniczym. Wiąże się to, między innymi z potrzebą uzyskiwania wspomnianego już efektu synergii, jako warunku sine qua non budowania potencjału bojowego. W związku z powyższym, pozwolę sobie przypomnieć, że sens tworzenia, istnienia i rozwoju całości zorganizowanego działania zasadza się na przekonaniu, że w rezultacie pozyskania z otoczenia adekwatnych dla danej domeny działalności osobowych, naturalnych i sztucznych komponentów rzeczowych tworzonej organizacji, będących niejako nośnikami działań, oraz właściwego ich połączenia więziami formalnymi (vide: np. procedury – M. C.) i zespolenia

[23] Por. S. Lem, *Noc z Kleopatrą*, „Wprost" z 8 czerwca 1997 r.

rzeczywistymi wzajemnymi oddziaływaniami materialnymi, energetycznymi i informacyjnymi, zostanie osiągnięty dodatkowy efekt synergiczny[24].

Zdaniem Krzyżanowskiego mechanizm powstawania efektu synergii można wyjaśnić w ten sposób, że współdziałanie wyzwala w podmiotach to, co poprzednio pozostawało w utajeniu, jakieś dotąd nie ujawnione ich właściwości. Współdziałanie wzmacnia więc niejako poszczególne podmioty. Podobne rozumienie synergii spotyka się także u innych autorów[25].

Ogólnie biorąc, należy stwierdzić, że warunkiem istnienia, czyli trwania i rozwoju organizacji jest działanie i współdziałanie z otoczeniem, czyli wzajemne interakcje, w tym również informacyjno-komunikacyjne. Mogą one przynosić efekt pozytywny – synergiczny (budowanie potencjału) bądź negatywny – dyssynergiczny. Jest to jeden z mechanizmów wykorzystywanych, między innymi w tzw. walce lub wojnie informacyjnej[26]. Dokładniejsze zrozumienie tego zjawiska i jego wpływu na kształtowanie i wzmacnianie potencjału bojowego, wymaga jednak przybliżenia pojęcia i zjawiska działania, szczególnie zaś działania informacyjno-komunikacyjnego i organizacyjnego, oraz ściśle z nimi związanego zjawiska kultury organizacyjnej i kultury informacyjno-komunikacyjnej.

Działania zespołowe stanowią istotę działań w siłach zbrojnych, a w nich w siłach powietrznych. Na poparcie tej tezy warto przytoczyć fakt, że nawet pilot współczesnego samolotu bojowego, wykonując samotnie otrzymane zadanie, jest silnie związany krwioobiegiem, czy – jak kto woli – nerwem informacyjno-komunikacyjnym z pozostałymi elementami systemu. Zerwanie tej specyficznej więzi jest często celem działań podejmowanych przez stronę przeciwną. Utrudnia bowiem to bardzo istotnie wykonanie zadania, a nierzadko nawet uniemożliwia jego realizację. Oznacza to, że system informacji i komunikowania, jako specyficzny układ nerwowy systemu dowodzenia i kierowania, stanowi istotny element ich potencjału bojowego. Jednocześnie stanowi bardzo ważny czynnik decydujący o wykorzystaniu pozostałych elementów tego potencjału.

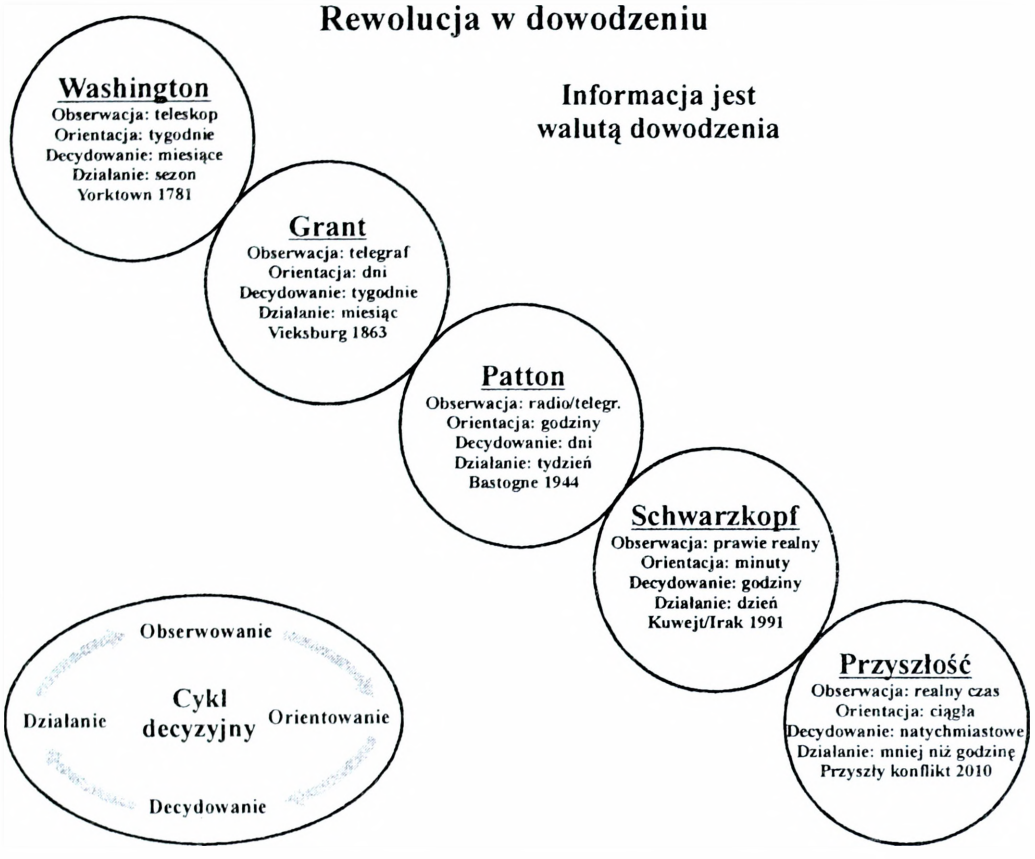
Wraz z rozwojem sił zbrojnych, zmieniał się również, doskonalił wspomniany wyżej układ nerwowy, czyli system dowodzenia, a w nim system informacji i komunikowania. Obserwowane w tym zakresie tendencje zmian, przedstawia rys. 5. Uzupełnię go kilkoma zdaniami komentarza.

---

[24] Por. L. J. Krzyżanowski, op. cit.

[25] M. Cieślarczyk, Psychospołeczne i organizacyjne elementy bezpieczeństwa i obronności, Warszawa 1997.

[26] Zob. L. Ciborowski, *Walka informacyjna*, Toruń 1999; R. Szpyra, *Walka informacyjna w przyszłych działaniach sił powietrznych*. Opracowanie pod kryptonimem „Cyberawiator" AON, Warszawa 2000.



Źródło: opracowanie własne na podstawie *Force XXI Operations Tradoc Pamphlet 525-5*, August 1994.

Rysunek 5.

W cywilizacji II fali materia (surowce), energia i kapitał decydowały o osiąganych efektach zarówno w sferze produkcji, jak również w działaniach sił zbrojnych. Dzisiaj pierwszoplanową rolę zaczyna odgrywać szeroko rozumiana wiedza, informacja, kultura i wartości. Wiedza, umiejętnie stosowana, staje się najlepszym substytutem pozostałych czynników. W odróżnieniu od tych pozostałych czynników, może się nią posługiwać jednocześnie wiele podmiotów. Co zaś najistotniejsze – nie zużywa się ona przy tym, a wręcz przeciwnie – przybywa jej. Stwierdzenie to możemy odnieść zarówno do wiedzy i informacji wykorzystywanych w procesach produkcyjnych, jak też do działań destrukcyjnych, do których zalicza się działania bojowe. Wywiera to niewątpliwy wpływ na systemy dowodzenia. Czasami mówi się nawet o rewolucji w dowodzeniu. Jeden z możliwych sposobów myślenia o zmianach w dowodzeniu[27] na przestrzeni ostatnich wieków, przedstawiono w syntetyczny sposób na rysunku 5. Warto jednak pamiętać, że przemiany w cywilizacji informacyjnej dotyczą również sfery organizacyjnej. Struktury się

[27] Zob. *Force XXI Operations Tradoc Pamphlet 525-5*, August 1994.

reorganizują, uwzględniając głównie zachodzące w nich procesy, a nie wydzielone specjalności. Zarządzanie taką strukturą wymaga nowych metod kierowania i wysokiego stopnia integracji systemowej. To się z kolei wiąże ze zwielokrotnieniem przepływów informacyjnych, nie tylko integrujących, ale i napędzających to swoiste perpetum mobile. Ramiona tej elektronicznej sieci obejmują również kosmos. Było to już dosyć wyraźnie widoczne w czasie operacji „Pustynna Burza". Sprzyjało podejmowaniu decyzji w czasie rzeczywistym, a nawet antycypację przebiegu wydarzeń i procesów. Wymagało jednak odpowiedniej klasy specjalistów, ale też nowoczesnych struktur organizacyjnych. Ogólnie biorąc, kierunek ich zmian prowadzi do coraz większej reaktywności, czyli skracania ich czasu reakcji, ale także precyzji działania. Używając obrazowego porównania, możemy powiedzieć, że kiedyś oddziały wojskowe pod względem czasu i precyzji reagowania przypominały, na przykład nosorożca, podczas gdy dzisiaj raczej się kojarzą z lampartem.

Warto jednak pamiętać, że funkcjonowanie struktur organizacyjnych związane jest z działaniami zespołowymi. Podejmując działania zespołowe pojedynczy ludzie i grupy społeczne napotykają różne problemy, ograniczenia i trudności. Jednym ze sposobów identyfikacji tych problemów i trudności jest ujawnianie i wyjaśnianie niezamierzonych lub odwrotnych od zamierzonych efektów działalności zespołowej, zwanych przez Mertona[28] nieoczekiwanymi konsekwencjami działania. Problem ten uwidocznił się, między innymi w Kosowie. Niemniej jednak względnie harmonijne wypełnianie przez SZ (SP) ich podstawowych funkcji, sprzyja rozwojowi systemu i budowaniu jego potencjału, ale także podnoszeniu na wyższy poziom morale stanów osobowych. Jednocześnie zaś, jak wynika z dotychczasowych badań, wysoki poziom morale sprzyja wypełnianiu tych funkcji i osiąganiu efektu synergii. Nie jest to jednak możliwe bez odpowiedniej kultury informacyjno-organizacyjnej, którą – jak wynika z badań[29] – można kształtować.

Zagadnienie kultury organizacyjnej, czy jeszcze szerzej biorąc – kultury informacyjno-organizacyjnej – nabiera szczególnego znaczenia w siłach powietrznych, szczególnie zaś w relacjach sojuszniczych. Zasadnym więc wydaje się przypomnienie postawionego już wcześniej pytania: czy zagadnienia te są uwzględniane w programach kształcenia uczelni wojskowych? Uwagę bowiem zwraca, między innymi fakt, że współcześnie do tradycyjnych kryteriów racjonalności, takich jak: zaufanie, rygorystyczność w egzekwowaniu zobowiązań, wzajemność, minimalna przynajmniej szybkość i skuteczność działania, na których opiera się istnienie każdego społeczeństwa i każdej zorganizowanej grupy społecznej, i którym możemy przypisać charakter uwarunkowań ogólnych i powszechnych, dochodzi coraz więcej kryteriów specyficznych, odnoszących się do coraz bardziej wyspecjalizowanych systemów i coraz bardziej zróżnicowanych form racjonalności. Pojawiają się takie pojęcia, jak racjonalność techniczna, administracyjna, finansowa itd. W po-

---

[28] Zob. R. K. Merton, *Struktura biurokratyczna a osobowość*,[w:] *System społeczny przedsiębiorstwa*, red. A. Sarapata, J. Kulpińska, Warszawa 1966.

[29] Zob. M. Cieślarczyk, *Informacyjno-organizacyjna kultura funkcjonowania człowieka i zorganizowanych grup społecznych*, AON, Warszawa 2000.

szczególnych kulturach i społeczeństwach mogą być one nieco inaczej odczytywane i interpretowane. Są to jednak istotne czynniki rozwoju danych podmiotów, a jednocześnie znaczące elementy ich potencjału, w tym również obronnego. W odniesieniu do struktur organizacyjnych SZ (SP) możemy mówić o nich jako o elementach potencjału bojowego, traktowanego nie tylko w wymiarze wewnętrznym danej armii, ale również w wymiarze koalicyjnym. Warto bowiem zauważyć, że uwarunkowania kulturowe, w tym również kultura organizacyjna i kultura informacyjno-komunikacyjna[30], wywierają znaczące piętno na procesy decyzyjne oraz sposobach działania i współdziałania struktur organizacyjnych SZ. „Problemy mentalnościowe" – sygnalizowane przez kadrę uczestniczącą w sojuszniczych ćwiczeniach – mogą być potwierdzeniem zasadności powyższych rozważań teoretycznych. Wprawdzie na tym etapie współpracy sojuszniczej problemy te nie są wyraźnie artykułowane, nie oznacza to jednak potrzeby chowania głowy w piasek i udawania, że one nie istnieją. Chociaż, wraz z upływem czasu ostrość tych problemów w sposób naturalny może się stawać mniej odczuwalne, nie oznacza to jednak, że przestaną one istnieć. Z tego chociażby powodu powinny być one podejmowane w działalności naukowo-badawczej i dydaktycznej.

Warto również pamiętać, że usprawnienie mechanizmów racjonalnego funkcjonowania całości społecznej, wymaga nieustannego wysiłku konstruowania i rekonstruowania systemów działań – pod warunkiem, że są one wystarczająco plastyczne. Jest to jeden z istotnych warunków ich zmian i rozwoju. Pomimo że wysiłek w tym kierunku bywa często podejmowany na podstawie fałszywych przesłanek, to nie przestaje on trwać i owocować skutkami. Plastyczność, czy raczej elastyczność struktur organizacyjnych i myślowych stają się więc jednym z istotnych elementów kultury organizacyjnej, a zarazem istotnym elementem ich potencjału. Wydawać by się mogło, że refleksja ta – ze względu na specyfikę sił zbrojnych – nie dotyczy ich struktur organizacyjnych. Czy jednak współcześnie te cechy (elastyczność struktur organizacyjnych i myślowych) – również w SZ nie stanowią znaczącego elementu ich potencjału bojowego? Wiele na to wskazuje, jednak jest to hipoteza, która powinna być zweryfikowana empirycznie.

W literaturze spotyka się również pogląd, że człowiek jest niewolnikiem środków organizacyjnych, które zmuszony jest wykorzystywać w swoim działaniu. Środki te cechują się nierzadko znaczną inercją, podobnie jak struktury myślowe niektórych ludzi. W im mniejszym stopniu człowiek rozumie i uwzględnia te ograniczenia, jakie te środki mu narzucają, tym bardziej wymykają się one spod jego kontroli. Warto jednak w tym momencie zwrócić uwagę na kolejny psychospołeczny mechanizm zorganizowanego działania. Wykorzystując szanse, jakie dostrzegamy dla siebie wewnątrz naszych sfer swobody, stukturalizujemy naszymi działaniami obszary, w których operują inni. Jest to jeden ze społecznych mechanizmów kooperacji pozytywnej. Warunkiem wstępnym każdego działania zbiorowego, jest bowiem odkrycie rzeczywistego marginesu własnej swobody danego podmiotu, a następnie ewentualne jego poszerzanie. Jest to element działań innowa-

[30] Op. cit.

cyjnych. Jednak przejście do działań innowacyjnych i korygujących, wymaga uprzedniego adaptowania się i reagowania na już istniejące ograniczenia.

Zdobycie wiedzy o realiach funkcjonowania systemu można uznać za pierwszy krok, warunkujący wszystkie dalsze w procesie transformacji. Jeśli uświadomimy sobie, że każda zmiana ma sens tylko w odniesieniu do systemu, który podważa, a zatem cele i środki, służące jej wprowadzaniu, można zrozumieć i ocenić tylko w kontekście właściwości tego systemu, natomiast podstawowe zasoby, z jakich będzie się korzystać, tylko częściowo mają charakter pewny, częściowo zaś stanowią potencjał, który trzeba będzie najpierw wyzwolić, to stwierdzimy, że wiedza o realiach systemu odgrywa fundamentalną rolę w procesie zmian. Otwarte pozostaje pytanie o zakres tej wiedzy na różnych poziomach struktury społecznej. Jednak ta ogólna zasada dotyczy w różnym stopniu poszczególnych podmiotów życia społecznego. Wskazuje to na wzrastającą rolę i znaczenie efektywnego systemu edukacji, informacji i komunikowania. Jedną z bardziej istotnych funkcji tych systemów jest kształtowanie kultury informacyjno-komunikacyjnej i kultury organizacyjnej danego podmiotu.

W działaniach związanych ze zmianami społecznymi decydującą rolę odgrywa nie tyle wiedza ogólna, lecz niezbędna do jej stworzenia znajomość możliwości i zasobów istniejących teoretycznie, oraz na poziomie danego systemu, a także znajomość metodologii analizy i metodologii eksperymentowania. Niestety, współczesne społeczeństwa aż kipią od nadmiaru spekulacji teoretycznych opartych na ogromnej masie informacji dotyczących kontekstów i problemów, a jednocześnie w sposób zadziwiający ignorują realia swoich własnych systemów funkcjonujących w praktyce. Każda zmiana, nie oparta na właściwym rozpoznaniu gier toczących się w systemie i regulatorów rządzących systemem, na który chcemy oddziaływać, pociąga za sobą reakcje obronne. System bowiem przystosowuje się przez pewien ciąg zachowań kompensacyjnych, zmieniając przy tym mniej lub bardziej całkowicie sens zmian, starając się zachować swoją tożsamość. Trzeba jednak pamiętać, że zarówno każda organizacja, jak i każde społeczeństwo, chociażby najbogatsze, zawsze żyje w świecie ograniczonych zasobów[31]. Chociaż w systemach otwartych groźba ta jest jakby mniej wyczuwalna, to jednak praktyka wdrażania wielu zmian i reform wskazuje, że nie jest to zagrożenie abstrakcyjne.

Aby móc dobrze kierować działaniami, nie wystarczy jednak dysponować wiedzą o realiach konkretnego systemu społecznego. Wiedza ta powinna być uzupełniona wiedzą o ludzkich reakcjach oraz o aktualnych i potencjalnych zdolnościach zarówno jednostek, jak i całych zespołów ludzkich. Również wiedza na temat kultury organizacyjnej i kultury informacyjno-komunikacyjnej może się okazać przydatna do lepszego rozumienia wielu procesów i zjawisk w sferze działania i współdziałania różnych struktur organizacyjnych SZ (działania połączone), zarówno w narodowych siłach zbrojnych, jak i w działaniach sojuszniczych (koalicyjnych). Porozumiewanie się ludzi między sobą, czyli komunikowanie się, rodzi specyficz-

[31] Zob. M. Crozier, E. Friedberg, *Człowiek i system. Ograniczenia działania zbiorowego*, Warszawa 1982, s. 375–381.

ne działanie ludzkie, wytwarza określone więzi społeczne. System informacyjny jest to jakby technologia zbierania, przetwarzania i przesyłania informacji. System komunikowania obejmuje również sposoby wykorzystania technicznych systemów informacyjnych, sposoby generowania informacji, ich odbioru itp. Komunikowanie się jest to więc pewna kategoria działania społecznego; system informacji zaś, jest to wyspecjalizowany układ techniczno-organizacyjny, dotyczący ściśle określonego celu oraz potrzeby informacyjnej człowieka. Wytwarzamy, przetwarzamy i przesyłamy informacje, aby stworzyć wokół siebie pewien ład. Tam, gdzie funkcjonują odpowiednie środki informacji, tam następuje większy ład. Ośrodkami generującymi informacje i wpływającymi na ten ład są poszczególni ludzie, środowiska społeczne i społeczeństwa, a także – w pewnym sensie – urządzenia techniczne. Spotyka się stwierdzenia, że wszędzie tam, gdzie człowiek działa w kierunku zwiększenia ładu, tam następuje ubytek entropii. *Entropia*, jako miara degradacji dowolnego systemu, może być także wskaźnikiem skuteczności działania człowieka. *Negentropia* zaś jest warunkiem zaistnienia efektu synergii (efektu systemowego) oraz początkiem procesu budowania potencjału, w tym również potencjału bojowego. Jest jednocześnie czynnikiem wprowadzania ładu w systemie.

Współcześnie dostrzega się wiele zjawisk i elementów wprowadzających określony ład dynamiczny, umożliwiających przebieg wielu procesów społecznych, kulturalnych i produkcyjnych. Zbyt często jednak pojęcia „wiadomość" i „informacja" są traktowane zamiennie, co nie sprzyja lepszemu rozumieniu procesów i zjawisk informacyjno-komunikacyjnych oraz wprowadzaniu ładu w sferze teorii. Można więc za niektórymi autorami dokonać rozróżnienia, przyjmując, że wiadomości płyną do nas zewsząd, informacja zaś rodzi się w nas. Wiadomość dająca się spożytkować w działaniu czy zachowaniu staje się informacją. Dzięki stałemu dopływowi informacji organizm jest zdolny z jednej strony do permanentnej adaptacji swego zachowania w stosunku do otoczenia, czyli przeciwstawiania się degradacji behawiorystycznej, z drugiej zaś do przeciwstawiania się degradacji motywacji o charakterze twórczym[32]. Jednak nadmiar informacji może również wpływać szkodliwie na obie te sfery, podobnie jak jej brak. Wpływa to niekorzystnie na funkcjonowanie człowieka i zorganizowanych grup społecznych oraz utrudnia osiąganie efektu synergii.

Wiele wskazuje na to, że społeczeństwa najwyżej rozwinięte lepiej wyczuwają wartość informacji, tak jak pływak wyczuwa wodę pod ręką czy pod wiosłem, a żeglarz wiatr. Są to istotne elementy kultury informacyjno-komunikacyjnej, a zarazem liczące się elementy potencjału bojowego struktur organizacyjnych sił zbrojnych.

Rodzi się więc pytanie: czy nasze umiejętności poruszania się w tym specyficznym żywiole, jakim jest kłębiąca się wokół nas informacja, sprzyjają wykorzystywaniu jej na potrzeby pełnionych przez nas ról i funkcji dla osiągania stojących przed nami celów i realizacji określonych zadań? Wyniki badań wskazują, że kadra zawodowa jednostek wojskowych sił powietrznych odczuwa wyraźny deficyt in-

[32] Por. E. Kowalczyk, *O istocie informacji*, Warszawa 1981, s. 66–75.

formacji potrzebnej jej do wykonywania obowiązków służbowych. Sygnalizują jednocześnie występowanie braków w zakresie szeroko rozumianej kultury informacyjno-komunikacyjnej kadry zawodowej[33].

Czy jednak problematyka ta znajduje wystarczające odzwierciedlenie w naszych programach kształcenia, ale i w programach naukowo-badawczych? Warto się także zastanowić, czy jako społeczeństwo nie jesteśmy w jakimś stopniu analfabetami informacyjnymi, biorąc chociażby pod uwagę brak wiedzy w tak zasadniczych kwestiach, jak – przykładowo biorąc – rozumienie różnic między informacją, wiadomością, wiedzą. Dla wielu z nas rozgraniczenia te nie mają większego znaczenia. A przecież są to jakby elementy swoistego alfabetu, stanowiące podstawę kultury informacyjnej, umożliwiające lepsze rozumienie wielu zjawisk w sferze informacji i komunikowania oraz wykorzystanie tej wiedzy w działalności praktycznej. Dotykamy w tym momencie swoistego wierzchołka góry lodowej, którą – jak już wspomniałem – możemy nazwać kulturą informacyjną bądź – jeszcze szerzej biorąc – kulturą informacyjno-organizacyjną. Armie najwyżej rozwinięte poświęcają tym zagadnieniom znaczną uwagę zarówno w wymiarze dydaktycznym (vide: Akademia Dowodzenia Bundeswehry), jak też w działalności praktycznej.

W armiach i uczelniach wojskowych krajów najwyżej rozwiniętych, bardziej docenia się rolę i znaczenie informacji, ale także wiedzę kadry w tym zakresie. Może o tym świadczyć chociażby fakt, że w Akademii Dowodzenia w Hamburgu problemami informacji i komunikowania na potrzeby dowodzenia zajmuje się specjalna struktura organizacyjna. Może być to postrzegane jako jeden z wyznaczników wysokiej kultury informacyjnej danego kraju, armii czy uczelni.

Kultura informacyjna ściśle się wiąże z kulturą dowodzenia jako istotnym czynnikiem sprawności, skuteczności i efektywności działania, ale również istotnym – chociaż trudno zauważalnym – elementem potencjału bojowego danej struktury organizacyjnej. O znaczeniu kultury informacyjno-organizacyjnej i kultury dowodzenia dla sił powietrznych, szczególnie zaś na współczesnym polu walki, nie trzeba nikogo przekonywać. Znaczenie kultury informacyjno-organizacyjnej, a w jej ramach kultury dowodzenia, traktowanych jako elementy potencjału bojowego, można dostrzec dopiero w konkretnych działaniach analizowanych pod kątem ich sprawności, skuteczności i efektywności, nie tylko w wymiarze wewnętrznym poszczególnych armii, lecz także w wymiarze koalicyjnym.

Z dotychczasowych badań wynika, że zarówno kultury informacyjno-organizacyjnej, jak i komunikacji międzykulturowej można się nauczyć. Zależy to jednak od zdolności przynajmniej częściowego zdystansowania się wobec wyznawanych wcześniej poglądów i przyzwyczajeń w tym zakresie. Kłopoty mogą mieć jednak osoby o nadmiernie wygórowanym ego oraz niskiej tolerancji niepewności. Przede wszystkim jednak ważne jest poznanie własnego zaprogramowania umy-

[33] Zob. M. Cieślarczyk, Z. Maślak, S. Sirko, *Informacyjno-komunikacyjne i organizacyjne uwarunkowania jakości dowodzenia i sprawności funkcjonowania jednostek wojsk lotniczych i obrony powietrznej*, AON, Warszawa 2002.

słowego i zrozumienie, czym ono się różni od zaprogramowania ludzi z innych kultur.

Warto przy tym pamiętać, że rozwój umiejętności komunikowania się z innymi kulturami przebiega w trzech fazach: uświadomienia, wiedzy i umiejętności. Punktem wyjścia jest jednak uświadomienie sobie, ze każdy z nas został inaczej wychowany i ma inne zaprogramowanie umysłowe. Umożliwia to posiadanie *„życzliwego poczucia humoru, które pozwala uznawać motywy kierujące ludźmi, którzy są zupełnie od nas różni"*[34]. Jest to początek bardzo ważnego procesu, poprzedzającego zdobycie wiedzy i umiejętności. One mogą być jednak kształtowane w konkretnym działaniu i współdziałaniu. Bogate doświadczenia w tym zakresie posiada prawdopodobnie kadra korpusu wielonarodowego, która może być doskonałym źródłem wiedzy na ten temat.

Niektóre procesy i zjawiska społeczne postrzegane wewnątrz SZ (SP)

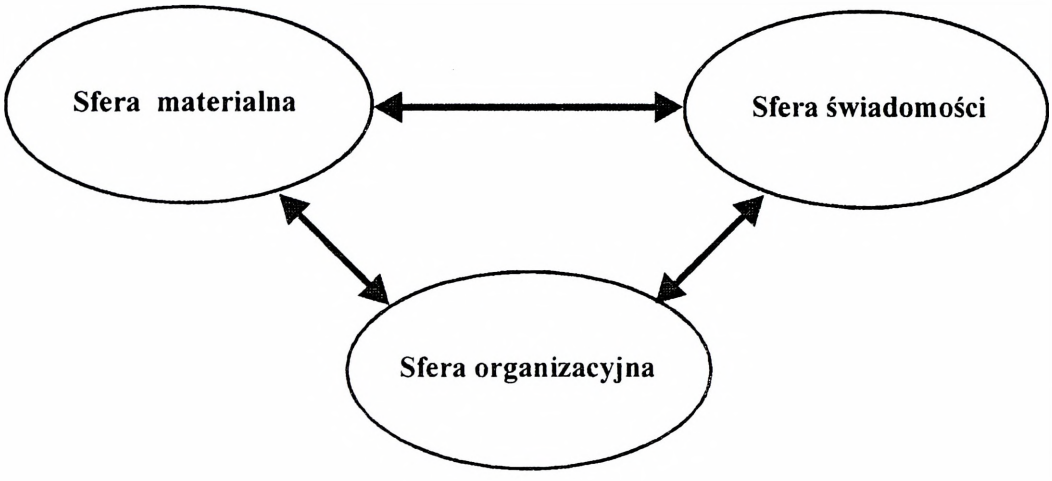
Społeczeństwo polskie, a wraz z nim siły zbrojne, od kilku lat przechodzą przyspieszony proces transformacji z cywilizacji przemysłowo-rolniczej do cywilizacji informacyjnej. Nie jest to droga łatwa ani krótka. Widać na niej liczne wyboje, ale i zakręty. Nie można wykluczyć, że na tej drodze pojawi się jeszcze wiele problemów wymagających nie tylko wiedzy i mądrości, ale także wytrwałości wszystkich uczestników wspomnianego procesu. Problemy te, najogólniej biorąc, jawią się w trzech podstawowych sferach: **materialnej, świadomościowej i organizacyjnej**. W uproszczony sposób przedstawia to rysunek 6.

Mogą one się okazać przydatne nie tylko w myśleniu o siłach powietrznych, ale także w podejmowanych decyzjach i działaniach praktycznych na różnych szczeblach. Chociaż konkretne problemy, występujące w przedstawionych na rysunku 6 trzech zasadniczych sferach rzeczywistości, wzajemnie się warunkują, to jednak nie muszą występować i uwidaczniać się w tym samym czasie. Nie oznacza to jednak, że przynajmniej część tych problemów nie można próbować przewidzieć. Jest to znaczące wyzwanie, przede wszystkim dla ośrodków naukowo-badawczych stanowiących warunek sine qua non rozwoju społeczeństwa informacyjnego.

W poprzednim zdaniu celowo użyłem pojęcia „wyzwanie". Jest bowiem ono kategorią znacznie szerszą niż np. zagrożenie. Wyzwanie oznacza sygnał lub komunikat, jaki dociera do danego podmiotu z jego bliższego lub dalszego otoczenia bądź sytuację, w jakiej się znalazł dany podmiot. Wyzwania właściwie odczytane oraz podjęte w odpowiednim czasie stwarzają dla danego podmiotu szanse. Natomiast błędnie odczytane, nie podejmowane bądź podejmowane z opóźnieniem – stają się często zagrożeniami.

[34] G. Hofstede, *Kultury i organizacje*, Warszawa 2000.

Trzy podstawowe grupy problemów w Siłach Powietrznych RP



Rysunek 6.

W związku z tym rodzą się pytania: w jaki sposób najczęściej postrzegamy sygnały płynące z bliższego i dalszego otoczenia oraz jak reagujemy na nie? Czy np. podejmowane przez nas decyzje i związane z nimi działania uwzględniają przyszłe konsekwencje w odniesieniu do wszystkich trzech przedstawionych na rys. 6 sfer rzeczywistości; czy może raczej w naszych decyzjach bierzemy pod uwagę tylko jeden aspekt jakiegoś problemu, nie zwracając uwagi na dysfunkcjonalne działania w odniesieniu do pozostałych sfer rzeczywistości? Wiele przykładów zdaje się potwierdzać częstsze występowanie tej drugiej sytuacji. Może to wskazywać, że naszemu myśleniu o SZ (SP) i podejmowanym na różnych szczeblach działaniom nie zawsze towarzyszy spojrzenie systemowe, przystępnie opisane w literaturze fachowej[35]. A przecież warunkiem występowania wszelkich zmian jest doskonalenie systemu informacji i komunikowania oraz wytworzenie nowych zdolności organizacyjnych bądź systemowych[36].

Analizując przedstawione na rys. 6 grupy czynników, warto zwrócić uwagę na to, że siły zbrojne w Polsce, a w nich siły powietrzne, znajdują się w dość szczególnej sytuacji. Z jednej strony bowiem integracja z Sojuszem, w którym przeważają kraje i armie cywilizacji informacyjnej, powinna sprzyjać i sprzyja procesom transformacyjnym, z drugiej strony zaś oddziaływanie wielu niekorzystnych czynników wyraźnie opóźnia te procesy. Jak już wspomniano, czynniki te się lokują – najogólniej biorąc – w trzech wymienionych wyżej sferach, tzn. materialnej, świadomościowej i organizacyjnej.

---

[35] Zob. P. Sienkiewicz, *Nowoczesne badania systemowe*, „Zeszyty Naukowe AON", Warszawa 1990.

[36] Por. M. Crozier, E. Friedberg, *Człowiek i system. Ograniczenia działania zespołowego*, Warszawa 1982.

Sfera materialna to przede wszystkim deficyt środków finansowych, w większości przestarzały sprzęt bojowy, widoczny stan infrastruktury itp. Chociaż deficyt środków materialnych jest odczuwany jako najbardziej uciążliwy i będzie prawdopodobnie korygowany, to jednak w najbliższych latach trudno spodziewać się zdecydowanej poprawy sytuacji w tym zakresie. Wprawdzie czasami słyszy się stwierdzenia, że sposób wykorzystania posiadanych środków powinien być dalej doskonalony, to jednak – ogólnie biorąc – tzw. pole manewru w sferze materialnej wydaje się być stosunkowo niewielkie. Sytuacja ta kieruje naszą uwagę w stronę dwu pozostałych obszarów (grup czynników), tzn. czynnika ludzkiego (świadomościowego) i organizacyjnego. Badania wykazują, że w obu tych obszarach istnieją potencjalnie największe możliwości ich doskonalenia w najbliższych latach. Dlatego też im właśnie chciałbym poświęcić nieco więcej uwagi.

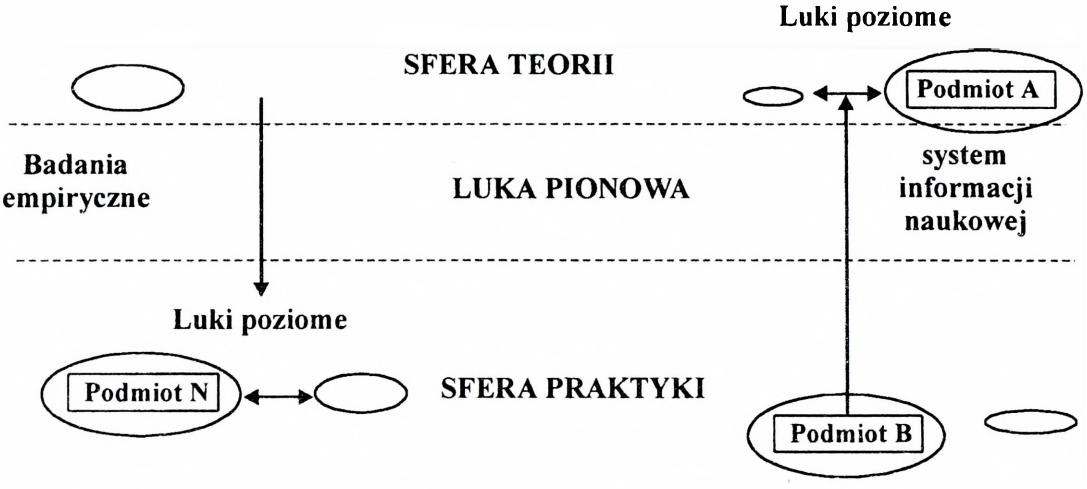
Wykorzystanie przedstawionego na rys. 6. modelu oraz kategorii myślenia systemowego, przy decyzjach dotyczących sił zbrojnych (sił powietrznych) i ich poszczególnych elementów, może sprzyjać również złagodzeniu skutków dosyć powszechnie odczuwanego w jednostkach liniowych zjawiska **deficytu sił, środków, czasu i informacji w stosunku do ilości realizowanych przez nie zadań**[37]. Powoduje ono wiele niekorzystnych skutków społecznych, takich jak trudności w realnym planowaniu i inne zakłócenia organizacyjne, a także przyśpieszone, psychofizyczne wypalanie się kadry zawodowej.

Przedstawione wyżej zjawisko przyczynia się także do powstawania i oddziaływania kolejnego negatywnego czynnika, potocznie nazywanego w jednostkach *bierzączką*. Te niekorzystne zjawiska, wraz z poczuciem tymczasowości i brakiem stabilizacji, wywierają zdecydowanie negatywny wpływ na samopoczucie kadry zawodowej. Nie sprzyja to perspektywicznemu myśleniu i działaniu oraz inwestowaniu w osobisty rozwój kadry zawodowej. W tej sytuacji trudno jest raczej myśleć o przyszłości macierzystej jednostki czy instytucji.

Warto zwrócić również uwagę na kolejny negatywny czynnik. Nazwijmy go **enklawowym sposobem myślenia i działania**. Upraszczając, możemy to przedstawić jak na rysunku 7.

Ogólnie biorąc, sygnalizuje on istnienie **różnego rodzaju luk** w sferze teorii i praktyki, ale także w relacjach między nimi. zarówno poziomych, jak i pionowych. Najbardziej uwidacznia się jednak luka między teorią a praktyką. Wymaga to poprawy funkcjonowania systemu informacji i komunikowania, większej ilości i lepszego wykorzystania badań empirycznych oraz przewartościowania sposobu myślenia o współczesnych siłach powietrznych.

[37] Por. wyniki badań Wojskowego Instytutu Badań Socjologicznych i WBBS.



Rysunek 7.

Jak już wcześniej wspomniano, niektóre teorie zdają się przechodzić do lamusa historii i zostają zastępowane przez te, które w miarę adekwatnie opisują aktualną rzeczywistość, starają się ją wyjaśniać oraz być użytecznymi do jej przewidywania i projektowania. Wydaje się, że coraz bardziej użyteczna, również dla współczesnych SP, może być teoria potencjałów[38], ale także nowoczesna teoria działania[39] czy wspominana już wcześniej teoria systemów[40].

Mogą być one pomocne przy konstruowaniu modeli funkcjonowania współczesnych sił zbrojnych, a w nich sił powietrznych. W kontekście przedstawionych wcześniej uwarunkowań zewnętrznych i wewnętrznych, szersze wykorzystanie modeli w myśleniu o siłach powietrznych wydaje się niezbędnym warunkiem umożliwiającym lepsze rozumienie rzeczywistości i sprawniejsze w niej funkcjonowanie. Przykład jednego z takich modeli pokazano na rys. 8.

Wróćmy jednak jeszcze do najprostszego, a zarazem najbardziej uniwersalnego modelu przedstawionego na rys. 6. Zatrzymajmy się dłużej przy tych grupach czynników, które dotyczą sfery świadomości oraz sfery organizacyjnej, a także relacji i wzajemnych uwarunkowań między nimi. Chodzi, między innymi o takie kwestie, jak: potrzeba elastyczności struktur organizacyjnych i struktur myślowych oraz związany z nimi w dużym stopniu realizm planowania i działania; potrzeba poszerzania zakresu podmiotowości, samodzielności myślenia, decydowania i działania zarówno struktur organizacyjnych, jak i poszczególnych osób funkcyjnych; potrzeba upowszechniania się dowodzenia przez cele; potrzeba doceniania czynnika czasu i umiejętne jego wykorzystywanie; potrzeba uwzględniania wielofunkcyjności i modułowości sprzętu bojowego. W sposób przejrzysty przedstawia to rys. 9.

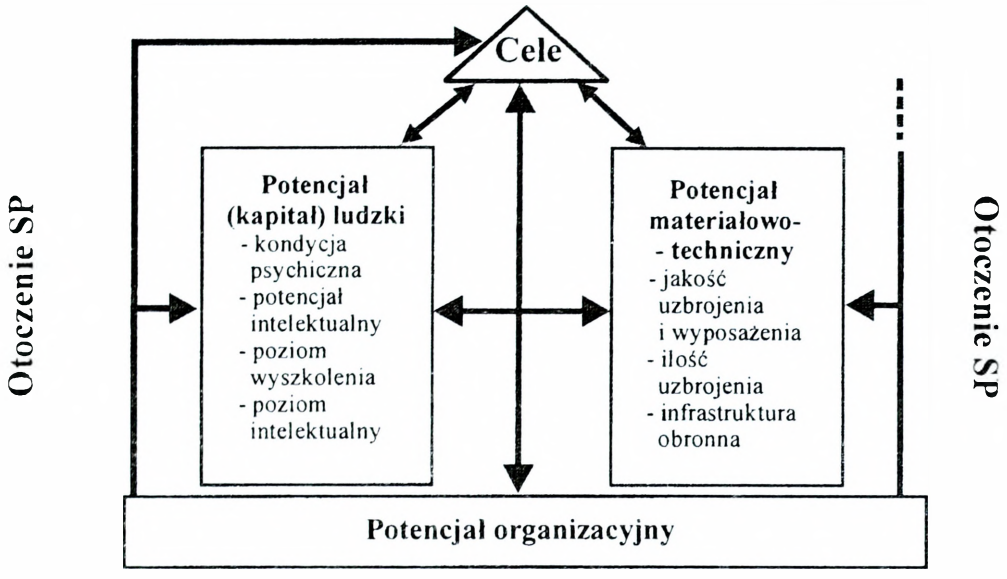
---

[38] Zob. np. K. Ficoń, *Symulacyjne modelowanie potencjału bojowego okrętowych sił morskich państw nadbałtyckich w aspekcie prognozowania obronnego*, „Zeszyty Naukowe", AMW 1995, nr 124A.

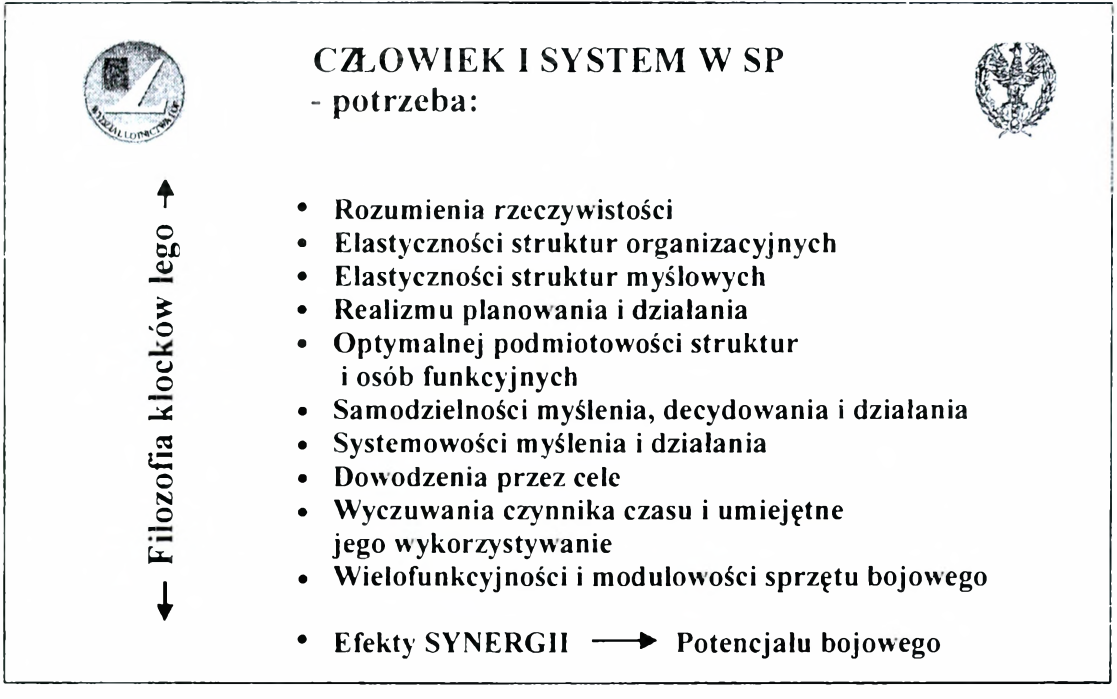
[39] Zob. np. Z. Krasnodębski, *Działanie i jego racjonalność w perspektywie prakseologicznej i socjologicznej*, „Prakseologia" 1991 nr 1–2 (110–111).

[40] Zob. np. liczne prace prof. P. Sienkiewicza.

Zasadnicze elementy systemu społeczno-organizacyjnego SP



Rysunek 8.



Rysunek 9.

Przedstawione na rys. 9 cechy i właściwości można kształtować. Kieruje to naszą uwagę w stronę odpowiednio przygotowanego człowieka, ale również systemu edukacji, który temu celowi służy. Stanowi to konkretne wyzwanie, także w stosunku do szkolnictwa wojskowego. Nie jest ono łatwe, patrząc na system szkolnictwa wojskowego chociażby przez pryzmat mało wyrazistej jeszcze wizji sił zbrojnych, która powinna być w miarę adekwatna do ich misji. Biorąc to pod uwagę oraz uwzględniając prawie permanentny proces zmian w SZ, jawi się refleksja dotycząca potrzeby wyposażenia studentów nie tylko w konkretny zasób wiedzy (która stosunkowo szybko może ulegać dezaktualizacji), lecz również, a może aktualnie przede wszystkim, w przedstawiony na rysunku 9 **umysłowy program operacyjny**, zwany również **technologią intelektu**[41]. Pozwala on lepiej rozumieć zmieniającą się rzeczywistość oraz procesy w niej zachodzące, ale także pomaga rozwiązywać wiele nowych i trudno przewidywalnych problemów i zadań. Jest to zarazem zgodne z wymaganiami współczesnego pola walki i celami stojącymi przed siłami powietrznymi cywilizacji informacyjnej. Tak rozumiany **program umysłowy studenta** może bardziej przypominać – używając obrazowego porównania – **program operacyjny** komputera niż jego pamięć trwałą. W tym operacyjnym programie umysłowym może się mieścić zarówno wspomniana już wcześniej praktyczna umiejętność myślenia systemowego, elastyczność struktur myślowych, samodzielność myślenia i rozwiązywania problemów, optymalna wyobraźnia, umiejętność komunikowania się i sprawnego posługiwania się informacją, rozumienie złożonych mechanizmów współpracy cywilno-wojskowej i współpracy z mediami itp. Kwestie te nie stoją w opozycji do zagadnień stricte fachowych, a raczej są rozwijane na ich bazie. Powinno to również sprzyjać łączeniu teorii z praktyką, z pożytkiem dla obu tych sfer rzeczywistości. Jednocześnie może przyczyniać się do zmniejszania przedstawionych na rysunku 7 luk dysfunkcjonalnych, sprzyjając uzyskiwaniu efektu synergii zarówno w wymiarze strukturalnym, jak i personalnym.

Zamiast podsumowania

Zamieszczone w tytule referatu pytanie, może być odczytywane jako rodzaj prowokacji intelektualnej, chociaż nie było to moim zamiarem. Jeśli jednak się okaże, że warto było choć przez chwilę zastanowić się nad rolą i znaczeniem człowieka we współczesnych siłach zbrojnych, a przy okazji pomyśleć o aktualnym stanie humanistyki w naszym wojsku – autor potraktuje to jako osobisty sukces.

---

[41] Por. M. Marody, *Technologie intelektu*, Warszawa 1987.

płk dr inż. Ryszard Szpakowicz

Zarząd Dowodzenia i Łączności WLOP

KIERUNKI ROZWOJU SYSTEMÓW INFORMACYJNYCH OBRONY POWIETRZNEJ

Wojna jest produktem swego czasu, gdyż narzędzia oraz taktyka, jaką stosujemy w czasie walk, zawsze rozwija się i zmienia wraz z rozwojem nauki i technologii. Zatem wojna (działania wojenne) ery informacji, w której żyjemy, również nieuchronnie będzie ucieleśnieniem właściwości, które tę erę odróżniają od poprzedniej. Te właściwości oddziaływają zarówno na zdolności, możliwości bojowe, jak i na naturę otoczenia, w jakim konflikt się pojawia.

Bardzo często w przeszłości, to właśnie siły zbrojne były pionierem zarówno w zakresie rozwijania technologii, jak i jej wdrażania. Jednak tak nie jest obecnie. Największe postępy w technologii informacji wynikają z potrzeb rynku i gospodarki. Co więcej, technologia informacji w celu zaspokojenia potrzeb gospodarczych jest wdrażana w takim zakresie, że zmienia sposób prowadzenia interesów na całym świecie.

Dlatego od wielu lat w Stanach Zjednoczonych jest realizowany program badawczy *DoD C4ISR Cooperative Research Program (CCRP)*[1], którego celem jest wskazywanie przedstawicielom najwyższych władz, jak wielki wpływ na bezpieczeństwo narodowe USA ma era informacji. Ten program rozwija również teoretyczne podstawy przewagi informacyjnej oraz koncepcję wojny sieciocentrycznej (*Network Centric Warfare – NCW*), bazując na wnioskach z analizy współcześnie funkcjonującego rynku i konkurujących na nim przedsiębiorstw.

Samo pojęcie „wojna sieciocentryczna", jak i jego definicja, jest wynikiem przeniesienia wniosków z analizy funkcjonowania przedsiębiorstw w warunkach ostrej konkurencji na globalnym rynku ery informacji do „ekosystemu" walki zbrojnej, z uwzględnieniem jego specyfiki i potrzeb. Definicja ta bazuje na następujących, dostosowanych do specyfiki walki zbrojnej, właściwościach ery informacji, które w istotny sposób odróżniają ją od ery przemysłu:

– zmianą sposobu tworzenia zysku (bogactwa);

[1] Zob. D. S. Alberts, J. J. Garstka, F. P. Stein – *Network Centric Warefare: Developing and Leveraging Information Superiority*, CCRP publication series, 2001.

– zmianą sposobu podziału władzy;
– wzrostem złożoności procesów gospodarczych;
– zmniejszeniem znaczenia czynnika odległości;
– kompresją (ściskanie) czasu, wzrostem tempa życia.

Właściwe rozumienie tych wzajemnie powiązanych cech ery informacji jest kluczem do poznania jej istoty. Szczególnie pierwsza z nich oddaje rewolucyjność zmian, które dotknęły proces gospodarowania. Osiągnięcie jak najwyższego zysku (bogactwa) było i jest celem każdego przedsięwzięcia gospodarczego. Pierwotna recepta, właściwa dla ery rolnictwa, na tworzenie bogactwa (zysku), obejmuje trzy podstawowe składniki: grunt, siłę roboczą i kapitał. W erze przemysłu relatywnie zmalała rola gruntów, ponieważ fabryki potrzebowały głównie kapitału i siły roboczej. Kapitał był niezbędny na zakup maszyn i surowca (surowego materiału). Zapotrzebowanie na siłę roboczą, ciągle niezbędną w procesie produkcji, maleje w miarę wzrostu wydajności. Proces tworzenia bogactwa (zysku) wymaga dodania również pewnej wartości w celu przemiany surowców (surowych składników) w nowy produkt. Do zrealizowania tej przemiany jest niezbędna energia, w takiej czy innej formie. Jedną z metod zwiększania zysku jest stosowanie wydajniejszych i tańszych źródeł energii. Erę przemysłu charakteryzuje wykorzystywanie w procesie produkcji kolejno: maszyn parowych, spalinowych, elektryczności, a w ostatnim okresie energii jądrowej. W początkowym okresie ery informacji wykorzystujemy w dalszym ciągu duże ilości paliw związanych z poprzednią erą, ale postęp technologiczny sprawił, że udział tego tradycyjnego zasilania w realizacji określonych zadań ciągle maleje. Gwałtowny wzrost zysków (bogactwa) przedsiębiorstw ery informacji wypływa z tego, że *informacja w procesach gospodarczych jest traktowana jako produkt, surowiec (surowy składnik) oraz jako paliwo (zasilanie).* Informacja, własność intelektualna, ma coraz większy udział w wytwarzanych obecnie skomplikowanych produktach końcowych. Ważność informacji jako surowca będzie stale rosła, wraz z rozpowszechnianiem się produktów wykonanych z informacji. Te z kolei, służą innym przedsiębiorstwom jako zasilanie, np.: informacyjne produkty, pozwalające menedżerom przedsiębiorstw handlowych określać nawyki konsumentów i wykorzystać tę wiedzę do zwiększenia efektywności działań. W przedsiębiorstwach, które świadczą usługi informacyjne, to właśnie informacja jest głównym surowcem, dominującym paliwem i produktem, np. Agencja Reutersa. W modelowych przedsiębiorstwach ery informacji – firmach informatycznych – oprogramowanie raz wykonane, może być powielane i rozprowadzane bez dodatkowych dużych nakładów finansowych. Informacja pozwala zatem zwiększać zysk przedsiębiorstw poprzez zmniejszenie udziału kapitału, siły roboczej, surowców i energii (paliwa) w produkcie końcowym.

Bogactwo i władza były zawsze ściśle powiązane. Kapitał był i jest niezbędny do tworzenia i utrzymywania instrumentów władzy – systemów uzbrojenia i sił zbrojnych. Jednak nie tylko broń może być instrumentem władzy. Często się mówi, że informacja to władza, ale w czasach, gdy ukuto to powiedzenie, informacja była stosunkowo droga, mało dostępna, a często była nawet towarem zakazanym. Dziś to powiedzenie ma znacznie większe zastosowanie niż kiedykolwiek, ale w zupeł-

nie innym sensie. Technologie informacji znacząco zwiększyły nasze zdolności zbierania, przechowywania, przetwarzania i analizy danych w celu tworzenia i szerokiego rozpowszechniania informacji. Informacja stała się relatywnie tania, ogólnie dostępna, a nawet trudna do ocenzurowania czy ukrycia. Ta eksplozja informacji spowodowała zmianę podziału władzy w ramach społeczeństwa i między społeczeństwami, ponieważ z jednej strony ludzie mają dostęp do niemal pełnej informacji o działaniach rządów i opozycji, a z drugiej strony rządy są coraz bardziej świadome tego, co myślą ludzie, a wszystko to się dzieje w czasie rzeczywistym. W tej sytuacji rządzący muszą coraz bardziej liczyć się z opinią publiczną, aby utrzymać poparcie społeczne.

Znakiem czasu są również tzw. wirtualne organizacje, które skupiają niezbędnych ludzi i procesy w celu realizacji określonego zadania. Po zakończeniu misji, te siły i środki mogą być przesunięte do wykonywania innych zadań. Wirtualne organizacje, dzięki połączeniom (sieciom), umożliwiają wykorzystywanie potencjalnego przyrostu możliwości produkcyjnych, który jest związany z wirtualną współpracą, wirtualną integracją i specjalizacją, bazujących na wspólnej świadomości i wiedzy o rynku w ramach przedsiębiorstwa, a nawet kilku kooperujących przedsiębiorstw. Zatem od czasu, gdy połączenia (sieci) zmniejszyły ważność odległości, zwiększyły się możliwości współpracy, integracji i specjalizacji.

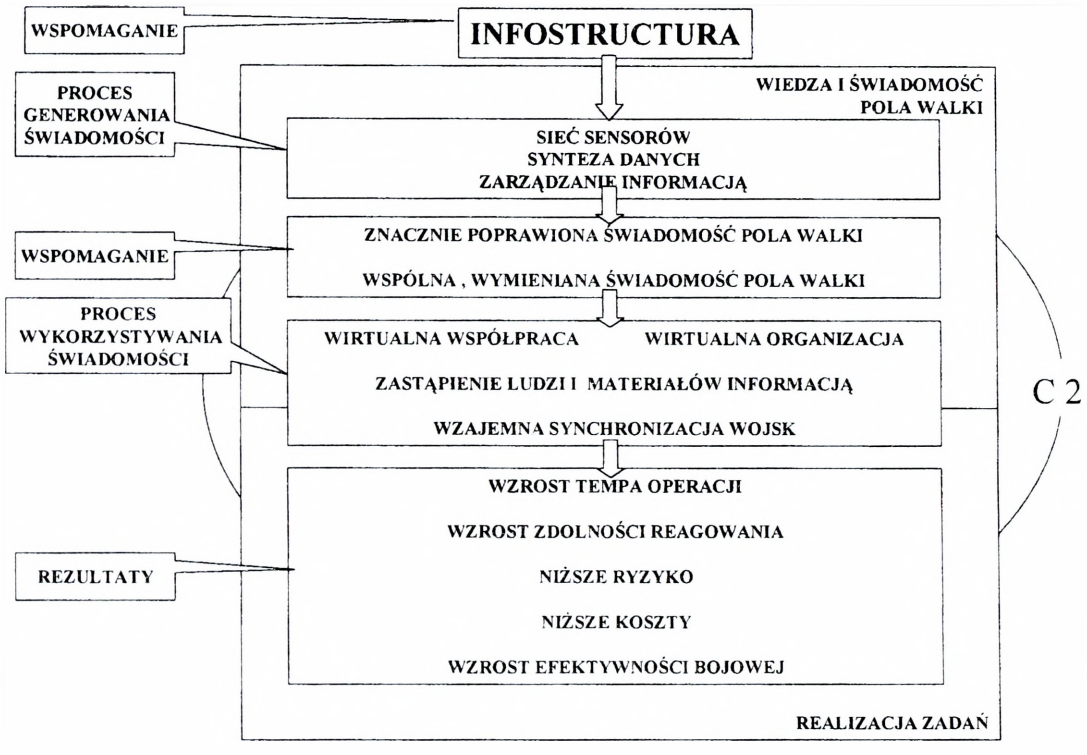
W wyniku tak rozumianej roli informacji w procesie gospodarowania i możliwości stwarzanych przez wdrażanie osiągnięć technologii informacji, konkurencyjność przedsiębiorstw wiąże się z pojęciem ***„przewaga informacyjna"*** – *definiowanym jako stan, który jest osiągany, kiedy przewaga we współzawodnictwie wypływa ze zdolności wykorzystania pozycji lepiej poinformowanego.*

Przedstawione w dużym skrócie rozważania, stały się podstawą do opracowania modelu: siły zbrojne jako przedsiębiorstwo sieciocentryczne (rys. 1), który jest istotą koncepcji wojny sieciocentrycznej.

„Wojna sieciocentryczna" (Network Centric Warfare – NCW) jest najlepszym terminem wypracowanym do chwili obecnej do opisania sposobu organizowania i prowadzenia walki w erze informacji. NCW jest definiowana jako bazująca 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. *Zatem NCW przekłada przewagę informacyjną na siłę bojową poprzez wydajne połączenia dysponujących wiedzą różnego typu jednostek organizacyjnych na polu walki.*

Stąd też pojęcie „wojna sieciocentryczna" dotyczy ludzi i organizacyjnego postępowania i bazuje na adaptacji nowego sposobu myślenia – myślenia sieciocentrycznego – oraz zastosowania go w operacjach wojskowych. NCW skupia się na możliwościach bojowych, które mogą być generowane poprzez efektywne połączenia informacyjne lub sieci informacyjne walczącego przedsiębiorstwa. Charakterystyczną cechą NCW jest zdolność geograficznie rozlokowanych wojsk (jedno-

stek) do tworzenia i wspólnego wykorzystania jednolitej świadomości pola walki, co prowadzi do synchronizacji działań w celu spełnienia zamiaru dowódcy, a więc *NCW wspiera proces dowodzenia poprzez konwersję pozycji dającej przewagę informacyjną w działania bojowe. Zatem przez analogię, pojęcie „przewaga informacyjna" można zdefiniować jako stan, który jest osiągany, kiedy przewaga w walce zbrojnej wypływa ze zdolności wykorzystania pozycji dającej lepszą informację.*



Rys. 1. Siły zbrojne jako przedsiębiorstwo sieciocentryczne

Ponadto NCW znacznie zbliża szczeble dowodzenia. Zatem NCW to nie tylko technologia, ale filozofia odpowiedzi sił zbrojnych na wyzwania wieku informacji. Aby można było jednak wykorzystać wszystkie potencjalne możliwości, **NCW musi być zakorzeniona w sztuce operacyjnej, ponieważ nie można w sposób prosty, bezpośredni zastosować nowych technologii do istniejących organizacji, doktryny wojennej czy systemów uzbrojenia, gdyż organizacje, doktryny i technologie muszą wspólnie ewoluować w „ekosystemie" walki zbrojnej**. Zatem przełożenie koncepcji NCW na rzeczywiste możliwości operacyjne, wymaga dużo więcej niż proste wprowadzenie nowoczesnej technologii informacji w formie infrastruktury informacyjnej czy infostruktury. Wymaga to nowej koncepcji operacyjnej, odpowiedniego podejścia do procesu decyzyjnego, nowych struktur organizacyjnych oraz doktryny ukierunkowanej na maksymalne wykorzystanie

całej dostępnej informacji, a więc NCW znaczy dużo więcej niż sieć informacyjna. Siła NCW wypływa z wydajnego, efektywnego połączenia lub włączenia w sieć dysponujących wiedzą różnych jednostek organizacyjnych, rozlokowanych w sensie geograficznym oraz hierarchicznym. Te połączenia umożliwiają im jednak korzystanie ze wspólnej informacji, współpracę w zakresie tworzenia wspólnej świadomości i wiedzy oraz synchronizacji działań. Tak rozumiana sieć powoduje wzrost siły bojowej.

Przejawem praktycznego stosowania elementów koncepcji wojny sieciocentrycznej jest przedstawiana w prestiżowych czasopismach przez analityków i rządowych przedstawicieli USA rewolucja w sprawach wojskowych (Revolution in Military Affairs – RMA)[2]. Według przedstawianej tam klasycznej definicji – RMA to radykalna zmiana w organizacji i wykorzystaniu sił zbrojnych, która jest możliwa, a nawet konieczna w wyniku wdrażania nowej technologii wojskowej.

Wojna w Afganistanie pokazuje stan rzeczywisty rewolucji, jaka się dokonała w siłach zbrojnych USA. Jednak większość obserwatorów widzi osiągnięcia RMA jedynie w rozwoju sensorów, systemów kierowania uzbrojeniem i samego uzbrojenia. Dużo uwagi poświęca się też rosnącym możliwościom systemów powietrznych i kosmicznych. Jest to jednak spojrzenie zbyt wąskie i w rzeczywistości zaciemnia wagę i charakter problemu. W istocie RMA przenika wszystkie rodzaje sił zbrojnych i służb. Oczywiście, obejmuje ona inwestowanie w nowe zestawy sensorów, nowe programy i systemy łączności w celu zdobywania informacji, ale co ważniejsze, RMA tworzy nową architekturę sił zbrojnych, wymusza nowe doktryny i koncepcje operacyjne w celu wykorzystania nowych możliwości, wymusza więc zmiany sposobu myślenia o działaniach bojowych i to jest rzeczywista istota tej rewolucji.

Jednak wydaje się, że precyzyjne i terminowe określanie położenia różnych obiektów na polu walki w tak rozumianej, nowoczesnej wojnie jest podstawą sukcesu[3]. Wymaga to rozwiązań w następujących płaszczyznach:

– po pierwsze utworzenia organów, które będą kierować realizacją zarówno zadań wywiadu, rozpoznania, nadzorowania przestrzeni powietrznej i rozpoznania powietrznego (intelligence, surveillance i reconnaissance – ISR), jak i natychmiastowymi, precyzyjnymi uderzeniami;

– po drugie doskonalenia zdolności określania położenia wojsk swoich i przeciwnika: od wykrycia poprzez identyfikację i śledzenie do przydzielenia celów do zwalczania;

– po trzecie zapewnienia zdolności natychmiastowego i skutecznego użycia właściwych sił i środków przeciwko precyzyjnie zlokalizowanemu i wskazanemu celowi przeciwnika.

---

[2] Zob. D. Goure, *Intelligence, Surveillance and Reconnaissance*, „Jane's Defence Weekly", vol. 37, 27.02.2002.

[3] D. Goure – vice president of Lexington Institute, Arlington, Virginia – w powyższym artykule stwierdza również „...być we właściwym miejscu i we właściwym czasie jest podstawą sukcesu w nowoczesnej wojnie".

W pierwszej płaszczyźnie USA w wyniku ogromnych nakładów finansowych uzyskały ogromny postęp w zakresie dowodzenia w kosmosie i przestrzeni powietrznej. Ostatnia dekada to również ogromne inwestycje w programy drugiej płaszczyzny – sensory, programy i systemy łączności, w wyniku czego znacznie wzrosła szybkość reagowania i dokładność precyzyjnych uderzeń. Najlepszym tego przykładem jest rozwój systemów satelitarnych GPS, które są podstawą zdolności sił zbrojnych USA do kierowania precyzyjnymi operacjami (tzw. chirurgicznymi uderzeniami) w dowolnym punkcie naszej planety.

Możliwości wynikające z implementacji RMA pierwszy raz były demonstrowane już w latach 1990–1991, podczas wojny w Zatoce Perskiej, gdzie z dobrym skutkiem wykorzystano rozwojowe wersje Joint STAR, wyposażone w systemy wykrywania poruszających się celów lądowych (Ground Moving Target Indicator – GMTI) oraz niewielka liczba stosunkowo prostych, bezzałogowych statków powietrznych (Unmanned Air Vehicle – UAV). W Kosowie w 1999 roku do tego zestawu dodano UAV Predator z optycznym systemem wykrywania i laserowym systemem wskazywania celów. W Afganistanie siły zbrojne USA były już w stanie rozwinąć i wykorzystywać całą gamę systemów sensorów: satelity wywiadu fotograficznego i elektronicznego, E-3 AWACS, Joint STAR, RC-135 Rivet Joint, P-3 Orion, Predator oraz nowy, dalekiego zasięgu, UAV RQ-4A Global Hawk. Użycie wielu typów sensorów pozwoliło na znaczne zwiększenie jakości informacji. Obraz satelitarny był podstawą do wskazywania obszarów, które następnie były przeszukiwane przez system Joint STAR, a rezultaty przesyłane do Predatora, który przekazywał dane – ale już o odpowiednio dobrej jakości – systemom uderzeniowym.

Dużo uwagi w środkach masowego przekazu poświęcono pierwszej w historii misji bojowej uzbrojonego UAV Predatora, jednak rzeczywistą i kluczową innowacją była zdolność do wymiany informacji między różnorodnymi źródłami i użytkownikami, włącznie z przekazem obrazu video w czasie rzeczywistym z kamer Predatora. W rzeczywistości kluczem do efektywnego wykorzystania możliwości tych wszystkich sensorów w trakcie operacji nie jest ich liczba czy nawet różnorodność, ale łączące je systemy łączności i transmisji danych. Jednolity, taktyczny system dystrybucji informacji (Joint Tactical Information Distribution System) SP USA, bazujący na systemie transmisji danych LINK 16, zapewnia połączenia między kosmicznymi, powietrznymi, naziemnymi platformami wykrywania i obserwacji a samolotami w powietrzu. System ten pozwala nie tylko na bezpośrednie połączenia między różnymi sensorami, sensorami a systemami uzbrojenia, ale również między systemami uzbrojenia a decydentami. W prowadzonej operacji w Afganistanie, oficerowie CAOC, rozwiniętego w bazie lotniczej Prince Sultan w Arabii Saudyjskiej, mogli oglądać obraz video w czasie rzeczywistym, który był przekazywany z Predatora wykonującego misje nad Kunduz czy Kandaharem. Samoloty B-52 nawet w czasie lotu były przecelowywane na podstawie informacji o nowych celach uderzeń, przekazywanych przez grupy sił specjalnych działające na lądzie, tak więc bombowce strategiczne realizowały zadania bezpośredniego wsparcia wojsk lądowych.

Obecnie SP USA opracowały cały pakiet nowych koncepcji operacyjnych, które między innymi dotyczą:

– utworzenia systemu ciągłego rozpoznawania i wykrywania (ISR), co wymaga rozwijania systemu sensorów kosmicznego, powietrznego i naziemnego bazowania oraz systemu kierowania ich działalnością;

– tworzenia systemów eksperckich „wiedzy i świadomości przewidywanego pola walki", które bazując na znajomości procedur i wzorców zachowywania się potencjalnego przeciwnika, jego doktryn, zwyczajów, sposobów szkolenia itp., zwiększą możliwości przewidywania jego działań.

Według ekspertów amerykańskich ten cel można osiągnąć poprzez poziomą integrację sensorów załogowych, bezzałogowych oraz kosmicznego bazowania. Planuje się nawet wykorzystanie w tym systemie tzw. inteligentnych samolotów tankowania (smart tanker), które oprócz swego podstawowego zadania, realizowałyby również misje ISR. Taki układ nazwano „Multisensor Command and Control Constellation – MC2C" – rys. 2. Podstawową cechą tego układu (konstelacji) będzie zdolność wymiany informacji między poszczególnymi jego elementami bez udziału ludzi. Do zarządzania tą konstelacją planuje się utworzyć jedno lub kilka powietrznych stanowisk dowodzenia (Multisensor Command and Control Aircraft – MC2A), które będą realizowały funkcje obecnie wykonywane przez następujące autonomiczne podsystemy: AWACS, Joint STAR, RC-135, samolot Airborne Commmand, Control and Communication i EC-130H Compass Call.

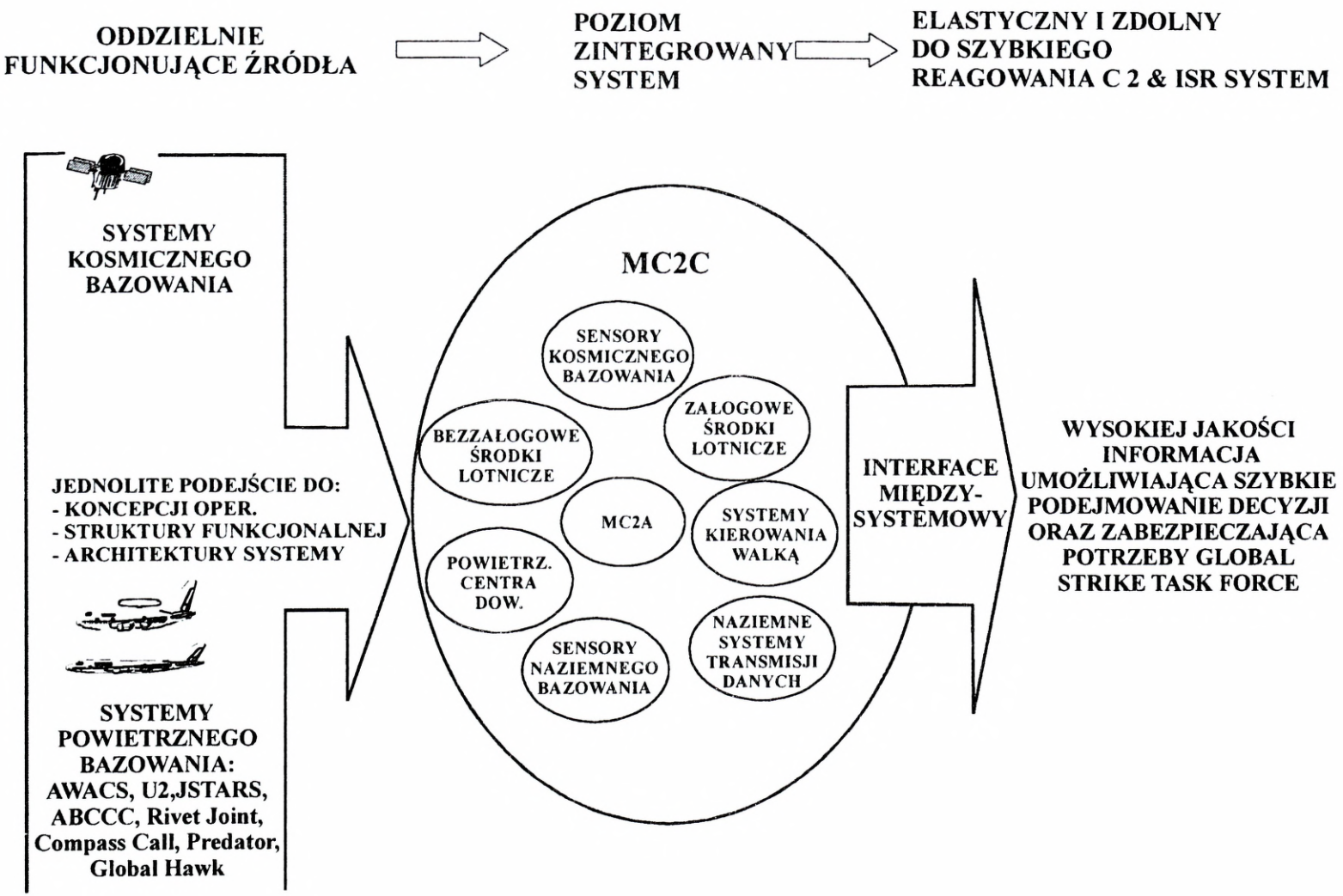
Utworzenie takiej wielosensorowej i wielozadaniowej konstelacji, będzie rzeczywiście aktem rewolucyjnym, co ze swej natury budzi wiele obaw, a w tym:

– czy taki system stwarza właściwe warunki do przekazywania uprawnień decyzyjnych na najniższy szczebel dowodzenia odpowiedzialny za realizację misji lub zadania, jak chcą tego zwolennicy RMA;

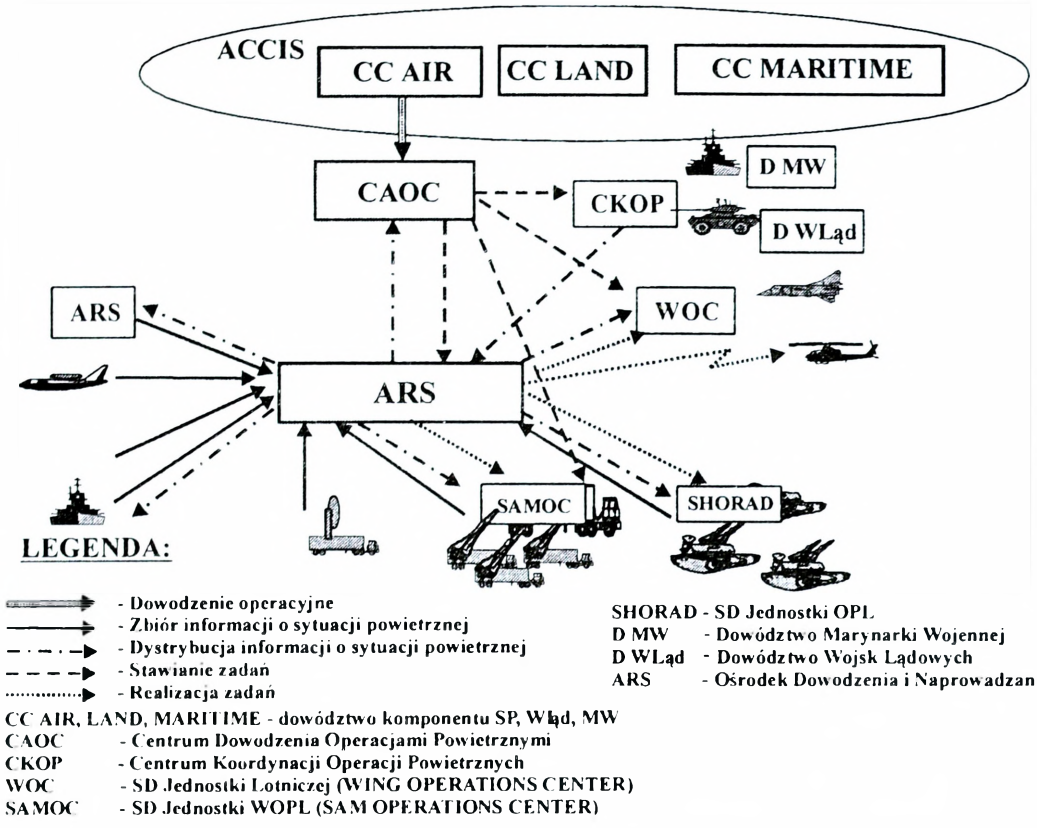
– czy stworzenie globalnej sieci bazującej na wydajnych połączeniach między jej użytkownikami w czasie rzeczywistym nie doprowadzi do centralizacji dowodzenia jako wyniku naturalnej skłonności wyższych przełożonych.

Ponadto do rozwiązania pozostał jeszcze inny problem, ale ściśle związany z wyżej wymienionymi: jak dane zebrane przez ten wszystkowidzący system ISR mają być przetwarzane i rozsyłane, czy powinny być gromadzone i kojarzone w wielkich centrach, a po przetworzeniu przekazywane użytkownikom, czy też surowe dane mają być dostarczone natychmiast do właściwych stanowisk dowodzenia i walczących jednostek.

W NATO również od wielu lat są prowadzone programy badawcze, których rezultaty mają być odpowiedzią na wyzwania ery informacji. Jednym z nich jest System Dowodzenia Lotnictwem i OP PSP NATO szczebla taktycznego (Air Command and Control System – ACCS). W lipcu 1999 roku został wreszcie podpisany kontrakt na realizację pierwszego etapu systemu ACCS , tzw. LOC1 (First Level of Operational Capability) między NATO-wską Agencją ds. Zarządzania Programem ACCS (NATO ACCS Management Agency – NACMA) a firmą Air Command Systems International (ACSI). Jest to pierwszy realny krok w kierunku wdrożenia tego systemu do pracy bojowej po wielu latach trudnych negocjacji, decyzji i uzgodnień.



Rys. 2. Multisensor Command and Control Constellation - MC2C



Rys. 3. Struktura organizacyjno-funkcjonalna systemu ACCS

System ACCS ma zapewnić efektywne oraz jednolite dowodzenie lotnictwem i OP w taktycznych operacjach ofensywnych, defensywnych i wsparcia – rys. 3. Pakiet LOC 1 został tak zaprojektowany, aby zintegrować wszystkie (w tym i narodowe) obecnie funkcjonujące systemy dowodzenia, które będą eksploatowane jeszcze przez 10–15 lat. Elementy mobilne – opracowane w ramach tego programu – mają sprostać wymaganiom wynikającym z implementacji koncepcji sił zadaniowych (Combined Joint Task Force – CJTF), czyli zapewnić dowodzenie komponentem SP w operacjach prowadzonych poza rejonem odpowiedzialności NATO.

System ACCS ma wspierać realizację następujących funkcji:

1) zarządzanie zasobami systemu dowodzenia (Command and Control Resource Management) obejmujące planowanie i zarządzanie wykorzystaniem środków C2 w celu efektywnego wspierania realizacji zaplanowanych operacji;

2) zarządzanie środkami walki (Force Management) obejmujące: planowanie, przydzielanie zadań, koordynację i realizację misji przez aktywne środki walki;

3) zarządzanie przestrzenią powietrzną (Airspace Management) obejmujące planowanie i utrzymanie strukturalnego podziału przestrzeni powietrznej, umożliwiającego bezkolizyjne jej wykorzystywanie przez środki różnych RSZ;

4) rozpoznanie przestrzeni powietrznej (Air Surveillance) obejmujące:

a) zarządzanie procesem tworzenia RAP, a w tym środkami wykrywania;

b) tworzenie RAP;

c) rozpowszechnianie RAP;

d) odbieranie i zobrazowanie informacji o obiektach lądowych, nawodnych i podwodnych;

5) kierowanie realizacją misji (Air Mission Control) obejmujące – w odniesieniu do wszystkich zaplanowanych operacji i misji:

a) kierowanie operacjami i misjami;

b) zapewnienie bezpieczeństwa własnym samolotom w strefach ognia własnych naziemnych środków OP;

c) monitorowanie misji realizowanych przez lotnictwo;

d) udzielanie wskazówek załogom;

e) przydzielanie podległym jednostkom WOPL celów do zwalczania;

f) monitorowanie przebiegu operacji;

6) kontrola ruchu lotniczego (Air Trafific Control) obejmująca: radarową kontrolę obszarową, kontrolę lotów w strefie lotnisk, udzielanie pomocy załogom w sytuacjach szczególnych oraz wspieranie działań SAR;

7) zarządzanie systemem (System Management) – funkcja systemowa – obejmująca: konfigurowanie poległych elementów systemu, określanie zasad obsług i kontroli oprogramowania i sprzętu, wprowadzanie trybów pracy systemu (ćwiczenia i treningi, symulacja);

8) zarządzanie informacjami (Information Management) – funkcja systemowa – obejmująca: zapewnienie spójności informacji gromadzonej w systemie, kontrolę dostępu do niej odpowiednio do ustalonych reguł, zapewnienie właściwej wymiany informacji między elementami systemu ACCS oraz z innymi systemami, archiwizowanie danych o zdarzeniach systemowych oraz ich analizę.

System ACCS zapewni również wymianę informacji z dowództwami komponentów sił powietrznych, lądowych i morskich oraz organami politycznymi NATO poprzez zautomatyzowany system dowodzenia i wymiany informacji (Automated Command Control Information Sysem – ACCIS).

Po zatwierdzeniu *Nowej Koncepcji Strategicznej NATO* podczas szczytu waszyngtońskiego w 1999 roku, która wytycza cele Sojuszu w XXI wieku, nasiliła się krytyka systemu ACCS. Z jednej strony podkreśla się ogromne koszty tego programu, z drugiej strony wskazuje się na przestarzałe rozwiązania, które zdaniem krytyków nie sprostają wymogom ery informacji i koncepcji rozszerzonej obrony powietrznej (NATO Extended Integrated Air Defence – NATINEAD). Ponadto wskazuje się, że wdrożenie tego systemu nie zmniejszy dystansu dzielącego kraje europejskie NATO i USA w dziedzinie dowodzenia operacjami powietrznymi. Podkreśla się, że przyjęte rozwiązania nie wykorzystują możliwości, jakie dają mechanizmy rozległych sieci, a bazują na przestarzałej koncepcji stałych, dedykowanych połączeń między poszczególnymi elementami systemu. Ponieważ ACCS ma integrować obecnie funkcjonujące systemy, zostanie wyposażony w różnego rodzaju interfejsy międzysystemowe, dlatego przez krytyków bywa nazywany

systemem interfejsów. Opracowane sprzężenia z systemami innych RSZ nie zapewniają jednak utworzenia jednolitego operacyjnego obrazu pola walki.

Dlatego już w pierwszym kwartale 2000 roku, na forum Komitetu OP NATO (NATO Air DefenceCommittee – NADC), omawiano założenia następnej wersji systemu dowodzenia lotnictwem i OP NATO[4]. Określono następujące główne kierunki doskonalenia tego systemu:

1) biorąc pod uwagę, że siły kosmiczne i powietrzne będą w dalszym ciągu odgrywały zasadniczą rolę w operacjach NATO, prowadzonych zarówno zgodnie z artykułem 5, jak i poza tym artykułem, zatem przyszły system musi zapewniać dowodzenie tymi siłami w rejonie odpowiedzialności NATO i poza nim;

2) zwiększenie elastyczności i niezawodności systemu poprzez szerokie wykorzystanie osiągnięć technologii informacji, ze szczególnym uwzględnieniem mechanizmów sieciowych;

3) stworzenie spójnego systemu rozpoznania, nadzoru przestrzeni kosmicznej i powietrznej (Intelligence, Surveillance and Reconnaissance – ISR) poprzez integrację różnego rodzaju źródeł informacji;

4) wprowadzenie mechanizmów dystrybucji informacji zapewniających wspólną wiedzę i świadomość pola walki na wszystkich szczeblach dowodzenia oraz wskazanych organów cywilnych;

5) szerokie zastosowanie programów (systemów) eksperckich:

a) przygotowujących propozycje decyzji i wskazujących najlepsze rozwiązania;

b) dokonujących szybkiej oceny przewidywanych oraz rzeczywistych skutków uderzeń, na podstawie dostarczanej informacji z systemu ISR;

6) stworzenie możliwości dynamicznego organizowania struktur zadaniowych, odpowiednio do potrzeb pola walki, składających się z jednostek, komórek organizacyjnych różnych RSZ i służb, a nawet innych resortów lub organizacji pozarządowych;

7) dokonanie rzeczywistej integracji systemów różnych RSZ i służb na potrzeby operacji połączonych poprzez opracowanie i wykorzystanie wspólnego języka do opisywania struktur organizacyjnych, jednostek, uzbrojenia i wyposażenia, zdarzeń na polu walki oraz implementację wspólnych procedur, np.: identyfikacji obiektów powietrznych, naziemnych, nawodnych i podwodnych.

Jednocześnie wskazuje się na wiele wątpliwości, które powinny zostać wyjaśnione w trakcie dalszych prac, które dotyczą:

– sposobu ustalania podziału kompetencji, gdyż dostęp do jednolitej informacji powoduje zbliżenie, a nawet przenikanie się dotąd wyraźnie wydzielonych szczebli dowodzenia;

– zasad i skuteczności przekazywania uprawnień do dowodzenia oraz autoryzacji stawianych zadań w świetle skrócenia drogi sensor–system uzbrojenia;

– możliwości opracowania skutecznego systemu filtracji zapobiegającego nadmiarowi informacji na poszczególnych stanowiskach pracy.

---

[4] *A vision for the command and control of NATO aerospace forces in joint operations beyond ACCS LOC1* – syg. NADC-D/215 oraz *Future aerospace command and control capabilities – beyond ACCS LOC1* – syg. NADC-D/243.

płk dr inż. Marek Grzybowski
Szefostwo Wojsk Radiotechnicznych WLOP

ZDOBYWANIE INFORMACJI O SYTUACJI POWIETRZNEJ W STRUKTURACH SOJUSZNICZYCH I NARODOWYCH

Występowanie zjawiska popytu informacyjnego jest wyrazem potrzeb informacyjnych związanych z uzyskaniem odpowiedniej informacji o określonej jakości. W obronie powietrznej istotne znaczenie ma informacja o różnorodnych czynnikach kształtujących sytuację panującą w przestrzeni powietrznej. Popyt na te wiadomości spowodował utworzenie różnorodnych systemów rozpoznania w przestrzeni powietrznej, w tym także systemów opartych na aktywnych i pasywnych środkach rozpoznania radiolokacyjnego.

Funkcjonujący w ramach Zintegrowanego Systemu Obrony Powietrznej Organizacji Traktu Północnoatlantyckiego – NATINADS (NATO Integrated Air Defence System) System Rozpoznania i Kontroli Przestrzeni Powietrznej – ASACS (Air Surveillance and Control System), obok wykonywania zadań dotyczących kierowania uzbrojeniem w obronie powietrznej, jest głównym źródłem informacji o sytuacji powietrznej. Opierając się na stanowiskach dowodzenia typu CRC (Control and Reporting Center), naziemnych posterunkach radiolokacyjnych RRP (Radar Remote Post) i samolotach wczesnego wykrywania systemu AWACS (Airborne Warning and Control System) produkuje rzeczywisty obraz sytuacji powietrznej, nazywany w nomenklaturze NATO RAP (Recognize Air Picture). Włączenie wydzielonych sił i środków Systemu Obrony Powietrznej RP do systemu OP NATO, wymusiło w tym wypadku także potrzebę dostosowania systemu rozpoznania radiolokacyjnego funkcjonującego obecnie w naszych siłach zbrojnych do potrzeb tworzenia obrazu RAP.

Obraz ten jest definiowany jako elektronicznie produkowane zobrazowanie na podstawie informacji pochodzącej z radarów lub innych źródeł zapewniających pokrycie przestrzeni powietrznej w trzech wymiarach, w których odebrane sygnały elektroniczne są oceniane w celu ich zidentyfikowania i nadania określonego numeru dla obiektu powietrznego. Obraz ten musi odwzorowywać położenie obiektów powietrznych w czasie rzeczywistym oraz mieć przyporządkowaną dla każdego wykrytego obiektu powietrznego określoną cechę wynikającą z jego identyfikacji. Obecnie w naszym systemie rozpoznania, możliwości w zakresie produkcji

tego typu zobrazowania, posiada jedynie Narodowy System Wsparcia Operacji Powietrznych – ASOC (Air Sovereignty Operat ion Center) rozwinięty w Centrum Operacji Powietrznych. Kompatybilność tego systemu ze środowiskiem naziemnej obrony powietrznej NATO, którą można było osiągnąć wykorzystując standardowe łącze transmisji danych LINK-1, umożliwia wykorzystanie tego systemu w charakterze jedynego ogniwa przesyłania i wymiany obrazu RAP z obszaru polskiej przestrzeni powietrznej.

Rozwiązanie tego typu jest jednak tylko rozwiązaniem tymczasowym, gdyż system ASOC nie jest w stanie pełnić funkcji kierowania przydzielonymi środkami walki w obronie powietrznej. Koncepcja budowy systemu dowodzenia polską OP zakłada w tym wypadku budowę nowej struktury, która zapewni w pełnym zakresie dowodzenie i kierowanie lotniczymi systemami uzbrojenia i WOPL zgodnie ze standardami NATO oraz zapewni wymianę informacji z systemem wczesnego ostrzegania i wykrywania. Zadanie to zamierza się wykonać na podstawie Ośrodków Dowodzenia i Naprowadzania (ODN). Ośrodki te, utworzone na bazie istniejących stanowisk dowodzenia obroną powietrzną, mają być zasadniczym organem wykonawczym kierowania systemami uzbrojenia oraz produkcji i dystrybucji obrazu RAP, czyli będą realizować pełne zadania oraz funkcje przypisane CRC w obecnie funkcjonującym systemie ASACS.

Stworzony w latach dziewięćdziesiątych System Rozpoznania Przestrzeni Powietrznej Sił Zbrojnych RP opierał się na jednorodnej strukturze brygad i batalionów radiotechnicznych, które na bazie funkcjonujących stanowisk dowodzenia realizowały kompleksowo zadania związane z rozpoznaniem radiolokacyjnym oraz zabezpieczeniem radiolokacyjnym działań bojowych wojsk na terytorium kraju. Pod pojęciem „rozpoznania radiolokacyjnego" określaliśmy w tym wypadku realizację trzech podstawowych funkcji: zdobywania informacji, jej opracowania oraz dystrybucji do określonych użytkowników.

Przejęcie w połowie lat dziewięćdziesiątych sił i środków rozpoznania radiolokacyjnego wojsk lądowych oraz dostosowanie ich struktur i zasad szkolenia do nowych zadań, zmieniło dotychczasowy sposób działania systemu radiolokacyjnego z charakteru typowo stacjonarnego na charakter manewrowy. Taki charakter działań umożliwił skupienie wysiłku na kierunku głównego zagrożenia, stworzenie nowego elementu w ugrupowaniu bojowym, jakim jest drugi rzut posterunków radiolokacyjnych, oraz efektywniejsze użycie odwodów do odtworzenia naruszonego ugrupowania. Dzięki temu obecna struktura systemu rozpoznania przestrzeni powietrznej pozwala na utworzenie zarówno stacjonarnych, manewrowych, jak i odwodowych posterunków radiotechnicznych.

W czasie pokoju stały dyżur bojowy pełnią stacjonarne posterunki radiolokacyjne, w tym posterunki wydzielone do systemu ASOC, a także utrzymuje się dodatkowo w gotowości do pracy bojowej niezbędną ilość posterunków zabezpieczających szkolenie lotnicze i działania dyżurnych sił lotnictwa w misjach Air Policing. Pozostałe posterunki realizują zadania szkoleniowe lub zabezpieczają radiolokacyjnie ćwiczenia wojsk w miejscu stałej dyslokacji lub na poligonach. W czasie kryzysu i wojny dyżur bojowy pełnią wszystkie stacjonarne posterunki

radiolokacyjne oraz rozwija się dodatkowo posterunki manewrowe. Część tych posterunków tworzy drugi rzut, wzmacniając strefę rozpoznania radiolokacyjnego na zagrożonym kierunku, umożliwiając zachowanie ciągłości śledzenia celów powietrznych na bardzo małych wysokościach oraz umożliwiając zabezpieczenie radiolokacyjne działań bojowych podczas dynamiki działań zbrojnych w czasie trwania operacji obronnej. Pozostałe posterunki stanowią odwód, zdolny zarówno do rozwinięcia nowych posterunków, jak i odtworzenia naruszonego ugrupowania bojowego.

Rozpoczęty w tym roku proces tworzenia ośrodków dowodzenia i naprowadzania jest ściśle związany z nowymi zasadami zdobywania informacji o sytuacji powietrznej. Bieżący obieg informacji o sytuacji powietrznej jest niejednorodny i ciągle modyfikowany. Jest oparty na dwóch systemach. Jednym z nich jest system narodowy, zbierający poprzez stanowiska dowodzenia brygad radiotechnicznych informację o sytuacji powietrznej z rejonów odpowiedzialności Połączonych Stanowisk Dowodzenia. Mimo że teraz wszystkie posterunki radiolokacyjne przekazują informację o sytuacji powietrznej w sposób cyfrowy, poziom techniczny urządzeń pracujących w systemie narodowym uniemożliwia tworzenie obrazu sytuacji powietrznej o charakterze rzeczywistym, dotyczącym terytorium całego kraju lub choćby rejonu obrony korpusu. Kilkuminutowe opóźnienia, występujące w tym systemie, powodują określone trudności w zastosowaniu tego obrazu do procesu dowodzenia walką.

Drugim systemem jest już wspomniany system ASOC, który zbiera bezpośrednio informacje z radiolokacyjnych posterunków. Współcześnie z tym systemem współpracuje system DUNAJ, rozwinięty na ODN, który także zbiera bezpośrednio informację ze wszystkich środków radiolokacyjnych znajdujących się w swoim sektorze odpowiedzialności. Dzięki temu system ASOC ma możliwość zbierania informacji i tworzenia na tej podstawie rzeczywistego obrazu sytuacji powietrznej z większej ilości posterunków. Dodatkowo na systemie DUNAJ może być zobrazowana informacja także z posterunków manewrowych, na podstawie której będzie można dowodzić aktywnymi środkami walki.

Dalsze przedsięwzięcia zmierzające do utworzenia pozostałych ośrodków dowodzenia i naprowadzania i ich bezpośrednie podłączenie do systemu dowodzenia NATO spowodują, że jedynie te ogniwa będą zbierać i opracowywać informacje o sytuacji powietrznej, tworząc jeden, jednorodny system rozpoznania przestrzeni powietrznej. System ASOC, w tym wypadku, zakończy swoje funkcjonowanie. Taka struktura zmieni zasadniczo realizację zadań w zakresie rozpoznania radiolokacyjnego.

Batalionom radiotechnicznym, a w zasadzie tylko będących w ich strukturze posterunkom radiolokacyjnym, pozostawia się w tym wypadku jedynie funkcję zdobywania informacji, obarczając wykonywaniem pozostałych funkcji w zakresie rozpoznania radiolokacyjnego ośrodkom dowodzenia i naprowadzania. Ośrodki te – jako samodzielne jednostki organizacyjne – będą bezpośrednio podporządkowane Centrum Operacji Powietrznych, wszystkie zaś źródła informacji o sytuacji powietrznej batalionom i brygadom radiotechnicznym. Wynika z tego, że struktura

organizacyjna systemu rozpoznania radiolokacyjnego nie będzie spójna ze strukturą operacyjną, jednak nie znaczy to, że do wykonywania zadań w tym zakresie nie będziemy podchodzić systemowo.

Opierając się na naziemnych stacjonarnych i mobilnych posterunkach radiolokacyjnych, samolotach wczesnego wykrywania oraz ośrodkach dowodzenia i naprowadzania, zostanie stworzony system rozpoznania i kontroli przestrzeni powietrznej na wzór natowskiego systemu ASACS, który obok typowych zadań związanych rozpoznaniem przestrzeni powietrznej, będzie także kierował aktywnymi systemami walki w tej przestrzeni.

Rozpoznanie przestrzeni powietrznej będzie realizowane poprzez wykrywanie przez aktywne i pasywne systemy rozpoznania radiolokacyjnego obiektów powietrznych, ich identyfikację oraz opracowanie i dystrybucję rzeczywistego obrazu sytuacji powietrznej. Kierowanie aktywnymi systemami obrony powietrznej będzie polegać na zabezpieczeniu działania lotnictwa myśliwskiego oraz innych rodzajów lotnictwa w zakresie naprowadzania i zwalczania celów powietrznych oraz osłony lotnictwa uderzeniowego, wykorzystując formy i metody dostosowane do sytuacji taktycznej, rodzaju misji i zdolności danego stanowiska dowodzenia. Polegać będzie także na zabezpieczeniu działań bojowych jednostek OPL dostarczając obraz RAP, wskazując cele powietrzne oraz zapewniając bezpieczeństwo własnego lotnictwa w strefie ich działania.

Podjęte przedsięwzięcia restrukturyzacyjne, wymuszają także przeprowadzenie głębokich zmian w systemie szkolenia jednostek radiotechnicznych. Pełne zautomatyzowanie procesu zbierania i opracowania informacji o sytuacji powietrznej i umiejscowienie tego procesu w scentralizowanym ogniwie dowodzenia, jakim jest ODN, powoduje sytuacje, że obsługi stacji radiolokacyjnych nie wykonują żadnych czynności operacyjnych związanych z tym zadaniem. Z tego też względu, dotychczasowy wysiłek szkoleniowy w tych pododdziałach – skupiony głównie na doskonaleniu umiejętności poprawnego analizowania sytuacji powietrznej – zostanie przeniesiony na uzyskanie wymaganego poziomu wiedzy techniczno-operacyjnej oraz umiejętności taktycznych umożliwiających sprawne wykonanie manewru, osiągnięcie gotowości bojowej oraz przetrwanie w różnorodnych warunkach współczesnego pola walki.

Jednocześnie zmiany bojowe tworzonych ODN-ów muszą przejąć na siebie wszystkie zadania związane z tworzeniem rzeczywistego obrazu sytuacji powietrznej, co się wiąże nie tylko z odpowiednim wykonaniem czynności związanych z opracowaniem trasy na podstawie informacji źródłowej, lecz także ze skutecznym kierowaniem pracą bojową tych źródeł oraz z umiejętnym zastosowaniem procedur dotyczących identyfikacji obiektów powietrznych.

Docelowa struktura systemu rozpoznania przestrzeni powietrznej zakłada, przede wszystkim spełnienie wymagań sojuszniczych co do realizacji tego zadania. Wymagania te przewidują możliwość wykrywania obiektów powietrznych na minimalnie małych wysokościach nad całym terytorium oraz stworzenie strefy informacji radiolokacyjnej na dużą głębokość od granicy NATO. Do tej pory główny wysiłek rozpoznania w NATO był rozłożony na dwa elementy. Po pierwsze utwo-

rzenie ciągłej strefy informacji radiolokacyjnej na średnich wysokościach opartej na naziemnym stacjonarnym systemie rozpoznania dalekiego zasięgu radarów klasy „Backbone". Po drugie – obniżenie tej strefy do małych wysokości opierając się na systemie AWACS.

Nie ulega wątpliwości, że system AWACS jest bardzo skutecznym narzędziem zabezpieczającym dowodzenie we wszelkiego rodzaju operacjach prowadzonych na lądzie, morzu i w powietrzu. Polska, znając rolę tego systemu, od początku akcesji aktywnie uczestniczy w pracach odpowiednich komitetów odpowiedzialnych w NATO za program wczesnego wykrywania. Jednak uczestnictwo w tym programie w charakterze uprawnionego członka wymaga poważnego wkładu finansowego w tę organizację ze strony naszego kraju. Suma zapewniająca uczestnictwo w pełnym wymiarze, z możliwością wykorzystania tego środka rozpoznania także w celach narodowych, jest bardzo duża. Z tego też względu nie należy sądzić, że Polskę będzie stać w niedługim czasie oprzeć swoje rozpoznanie przestrzeni powietrznej na samolotach typu AWACS. Na pewno będziemy dążyć do integracji z tym systemem, instalując odpowiednie interfejsy umożliwiające wymianę informacji oraz wykorzystanie tego systemu nad naszym terytorium w czasie wspólnych operacji NATO. Ponadto należy zaznaczyć, że system AWACS powoli się starzeje i wymaga pilnej modernizacji, szczególnie w zakresie radaru oraz samego samolotu. Wymaga to także bardzo dużych nakładów finansowych i rozłożenie tej modernizacji w czasie. Dlatego w rozpoznaniu przestrzeni powietrznej NATO zamierza kompleksowo wykorzystać także całą gamę dostępnych systemów radarowych, takich jak:

– trójwspółrzędne radary stacjonarne dalekiego zasięgu klasy „BACBONE";
– trójwspółrzędne radary mobilne średniego i małego zasięgu;
– stacjonarne i mobilne radary określające tylko dwie współrzędne;
– radary wykorzystywane w systemach przeciwlotniczych różnych rodzajów wojsk;
– brzegowe radary obserwacji sytuacji powietrznej i nawodnej;
– radary kontroli obszaru zainstalowane na okrętach marynarki wojennej;
– pierwotne i wtórne radary kontroli ruchu lotniczego;
– pasywne systemy radarowe i radioelektroniczne wykorzystywane do namierzania i lokalizacji obiektów powietrznych.

Uwarunkowania te powodują, że rola naziemnych systemów radarowych staje się coraz większa oraz następuje ich ciągły i dynamiczny rozwój. Doświadczenia ostatnich konfliktów zbrojnych wskazują także na potrzebę wprowadzenia nowych rozwiązań technicznych w aspekcie wykorzystania tych systemów w warunkach pokoju, kryzysu i wojny.

Konflikt zbrojny w Zatoce Perskiej wykazał, że satelitarny system „gwiezdnych wojen" nie jest w stanie w pełni zapewnić zniszczenia balistycznych pocisków rakietowych o zasięgu taktycznym. Stosunkowo krótki czas od momentu odpalenia rakiety do jej uderzenia w cel wynoszący tylko 450 s przy zasięgu rakiety do 1000 km powoduje, że systemy antyrakietowe nie mogą dokonać skutecznego przechwycenia, mimo że sam start rakiety został wykryty przez system satelitarny. Radar systemu PATRIOT, który był używany w tym konflikcie, zbyt późno

wykrywał irańskie pociski rakietowe typu SCUT, żeby móc w czasie wypracować odpowiednie dane do skutecznego odpalenia rakiety.

Na podstawie tych doświadczeń eksperci z krajów NATO doszli do wniosku, że problem ten może być rozwiązany poprzez zapewnienie wykrycia i śledzenia rakiety na torze stroboskopowym. Dzięki aproksymacji tej trasy w dalszej części trajektorii lotu rakiety jest możliwe opracowanie wstępnych danych dla systemów antyrakietowych i ich skuteczne użycie do zniszczenia tego typu obiektów. Zadanie to mają realizować radary z odpowiednio przystosowanym do tego torem wykrywania taktycznych rakiet balistycznych, tzw. przystawką TBM (Tactical Ballistic Missile), która ma zapewnić, obok wydania oddzielnych plotów informacyjnych dotyczących wykrytych i śledzonych pocisków balistycznych, także takie informacje, jak: punkt startu i uderzenia rakiety, czas startu oraz aproksymacje trajektorii jej lotu. Wymagania NATO w tym zakresie określają, że między innymi wszystkie nowe radary typu „Backbone" powinny posiadać takie możliwości. Wskazane jest także zaimplementowanie tej funkcji w innych radarach, zwłaszcza w tych, które planuje się rozmieszczać na granicach Sojuszu.

Innym bardzo silnie akcentowanym elementem dotyczącym rozpoznania radiolokacyjnego jest obrona radioelektroniczna. Wykorzystywane w warunkach bojowych radary powinny mieć w tym wypadku możliwość wykrycia i wyróżnienia spośród innych obiektów powietrznych, także specjalistycznych pocisków rakietowych naprowadzających się na źródło promieniowania elektromagnetycznego. Wykrywanie tych pocisków, tzw. funkcja ARM Detection oraz odpowiednie możliwości operacyjne i układy elektroniczne, umożliwiają zakłócenie procesu naprowadzania tego pocisku. Walka z tego typu pociskami jest oparta głównie na sterowaniu emisją radaru pierwotnego oraz na aktywacji w odpowiednim czasie systemu pozorującego emisję listków bocznych anteny danego radaru. Przyszłościowe radary powinny także skuteczniej lokalizować źródła zakłóceń poprzez wyposażenie je w pasywny system lokalizacji źródła zakłóceń oraz uzyskanie zdolności estymacji obszaru rozprzestrzeniania się celowych zakłóceń biernych.

Obecna koncepcja obrony powietrznej NATO zakłada szersze wykorzystanie do celów rozpoznania przestrzeni powietrznej także radarów pasywnych. Pod tym pojęciem określa się tylko te środki rozpoznania radioelektronicznego, na podstawie których można produkować rzeczywisty obraz – RAP. Rozpatruje się zatem systemy oparte na rozpoznaniu wszelkiego rodzaju emisji elektromagnetycznej, którą może prowadzić autonomicznie statek powietrzny, oraz rozpoznanie emisji elektromagnetycznej odbitej od statku powietrznego, tzw. technika PCL (Passive Coherent Location). Występuje jeszcze technika opracowania trasy na podstawie namiaru na źródło zakłóceń radioelektronicznych PET „Passive ESM Locators", jednak według poglądów ekspertów z NATO nie może być ona bezpośrednio wykorzystana do tworzenia RAP. System, który jest oparty na tej technice „Passive Jammer Locators", wspiera jedynie w tym względzie funkcję radaru aktywnego. Ten rodzaj rozpoznania jest szczególnie preferowany w wersji manewrowej. W tej wersji stanowiska dowodzenia typu ARS – jako komponent rozpoznania – mają także funkcjonować radary pasywne. Ze względu na stosunkowo niski koszt tego

rozwiązania, część ekspertów NATO naciska na szersze wprowadzenie tego typu radarów do różnego rodzaju projektów, nawet kosztem radarów aktywnych. Wydaje się jednak, że takie podejście do tematu nie jest w pełni do zaakceptowania. Rozpoznanie oparte na środkach pasywnych powinno być jedynie uzupełnieniem strefy rozpoznania radiolokacyjnego, tworzonej przez systemy aktywne.

Istotnym problemem w zakresie zdobywania informacji o sytuacji powietrznej jest dzisiaj brak w NATO kompleksowego rozwiązania odnośnie do integracji radarów z systemami dowodzenia obroną powietrzną, szczególnie w aspekcie funkcjonowania systemu ACCS. Obecnie trwają prace nad zatwierdzeniem wspólnego formatu wymiany informacji w systemie ACCS, określanego jako AWCIES. Format ten, oczywiście, obok innych sekwencji informacyjnych, które są zawarte w formacie LINK 1, 11 czy 16, ma zawierać, między innymi także dane uzyskiwane bezpośrednio z wyjścia radaru oraz informację umożliwiającą realizację funkcji zdalnej kontroli i sterowania radarem. Współcześnie w NATO funkcjonuje wiele różnych rozwiązań. Jedną z propozycji jest zastosowanie w nowym formacie protokołów ASTERIX do wymiany danych o sytuacji powietrznej oraz oddzielnych protokołów w zakresie kontroli i sterowania radarem przewidzianych dla wyspecjalizowanej do tego celu konsoli radiolokacyjnej, w którą wyposażone muszą być zgodnie ze standardem NATO stanowiska dowodzenia obroną powietrzną. Konsola taka zapewnia jednoczesne zdalne sterowanie czterema radarami oraz monitorowanie pracy bojowej co najmniej dwunastoma źródłami informacji.

Ponadto, aby móc w pełni wykorzystać naziemne systemy radiolokacyjne do rozpoznania przestrzeni powietrznej, muszą być rozwiązane w najbliższym czasie następujące problemy techniczno-konstrukcyjne:

– zwiększenie skuteczności rozpoznania obiektów powietrznych, przy jednoczesnym obniżeniu emisji energii elektromagnetycznej;

– zróżnicowanie kształtu i polaryzacji charakterystyk promieniowania;

– inna konstrukcja urządzeń antenowych;

– wydłużenie czasu pracy i zwiększenie niezawodności poszczególnych układów elektronicznych;

– wprowadzenie nowych rozwiązań dotyczących identyfikacji obiektów powietrznych.

Obecnie możliwości środków rozpoznania radiolokacyjnego, będących na wyposażeniu naszych sił zbrojnych, utrudniają zastosowanie procedur i zasad obowiązujących w NATO. Jednak ich znaczny potencjał bojowy skłania nas do szukania kompromisu pomiędzy spełnieniem wymogów kompatybilności operacyjnej w ramach sojuszu a pełnym i kompleksowym wykorzystaniem tego rodzaju rozpoznania w polskiej przestrzeni powietrznej.

Z osiągnięciem pełnego standardu NATO w zakresie rozpoznania radiolokacyjnego jest związana budowa systemu „Backbone". Na podstawie prowadzonych analiz, w Naczelnym Dowództwie Połączonych Sił w Europie – SHAPE, opracowano „SHAPE Radar Plan", który zakładał stworzenie systemu składającego się ze stacjonarnych radarów dalekiego zasięgu. Ogniwa tego łańcucha obecnie funkcjonują w krajach NATO w dwóch ugrupowaniach:

– północnym – rozwiniętym na terenie Norwegii, Islandii, Wielkiej Brytanii, Danii, Holandii;

– południowym – rozwiniętym na terenie Turcji, Włoch, Grecji i Portugalii.

W wyniku wstąpienia w struktury Sojuszu trzech nowych członków, konieczne było uzupełnienie tego systemu o trzeci łańcuch, obejmujący terytorium Polski, Republiki Czech i Węgier. Zgodnie ze standardem, radary pracujące na tych posterunkach, powinny spełniać następujące wymagania:

– wykrywać, śledzić i określać trzy współrzędne obiektów powietrznych od odległości około 470 km;

– identyfikować obiekty powietrzne zgodnie z formatem Mark XII A, wraz z modem „S";

– pracować 24 godz. na dobę przez cały rok;

– posiadać co najmniej 25–letni okres eksploatacji.

Program ten w przypadku naszego kraju dotyczy sześciu posterunków, w tym dwóch budowanych od podstaw, na których zamierzamy rozwinąć trzy radary produkcji krajowej oraz trzy radary zakupione w ramach przetargu międzynarodowego ze środków NATO. Fundusz NATO pokryje także całość kosztów związanych z realizacją rozbudowy infrastruktury inżynieryjnej i technicznej wszystkich posterunków a także wyposażenia radarów w osłony anten typu RANDOM oraz integracji tych radarów z systemem łączności i dowodzenia. Ponadto, radary zakupione w ramach przetargu międzynarodowego, zostaną dodatkowo wyposażone w aparaturę do wykrywania taktycznych rakiet balistycznych – TBM.

Uzupełnieniem systemu radarów klasy „Backbone" będzie system radarów manewrowych, oparty na zmodernizowanych zestawach radarowych NUR-31 oraz radarach nowej generacji, zakupionych z rodzimego przemysłu. Bezpośrednie porównanie naszych osiągnięć w dziedzinie bojowej techniki radiolokacyjnej, z osiągnięciami najwyżej rozwiniętych państw Europy Zachodniej i Ameryki, w tym wypadku nie wypada najgorzej. Co więcej, każdorazowa prezentacja naszych osiągnięć dla ekspertów zajmujących się profesjonalnie tą tematyką w NATO, wzbudza wielkie zdziwienie z powodu osiągniętego poziomu technologicznego w tym zakresie.

Zbudowanie systemu rozpoznania przestrzeni powietrznej w przedstawionym kształcie, umożliwi wykorzystanie pełnych możliwości naszych sił i środków obrony powietrznej również w wymiarze narodowym, także jeżeli chodzi o zabezpieczenie działań bojowych wojsk lądowych i marynarki wojennej oraz zabezpieczenie informacyjne wybranych elementów obrony terytorialnej czy obrony cywilnej. Z tego też względu, posiadanie w polskich siłach zbrojnych silnego komponentu rozpoznania w przestrzeni powietrznej, powinno być w interesie wszystkich rodzajów wojsk i sił zbrojnych oraz pozostałych elementów systemu obronnego państwa. Tylko sprawny system dowodzenia obroną powietrzną, oparty na skutecznym i niezawodnym rozpoznaniu, zapewni nam korzyści wynikające z wejścia do NATO w dziedzinie nienaruszalności naszej przestrzeni powietrznej poprzez możliwość użycia w tej przestrzeni także sił i środków walki innych członków Paktu.

płk dr inż. Marek Grzybowski
Szefostwo Wojsk Radiotechnicznych WLOP

INFORMACJA O IDENTYFIKACJI JAKO PODSTAWOWY ELEMENT DECYZJI UŻYCIA UZBROJENIA

Decyzja o użyciu nowoczesnych środków bojowych, musi zapewnić uzyskanie maksymalnych korzyści operacyjnych oraz być na tyle pewna, by wyeliminować możliwość uderzenia lub oddziaływania na własne wojska, a także na siły i środki niezaangażowane w konflikt zbrojny. Akcja zbrojna w tym wypadku nie powinna być konsekwencją jedynie wykrycia określonego zjawiska, obiektu czy osoby, lecz przede wszystkim nadaniem im określonej cechy przynależności. Dostarczona do decydenta w tym wypadku informacja, musi zawierać nie tylko określenie czy wykryty obiekt jest własny, obcy, czy neutralny, ale także czy posiada on cechę militarną lub cywilną. Dane te powinny także charakteryzować jego klasę, typ, narodowość i zamiar działania.

W celu zbierania, przetwarzania i przekazywania danych identyfikacyjnych, zamierza się integrować różnorodne systemy informacyjne poprzez wymianę w czasie rzeczywistym tych danych w środowisku systemów dowodzenia i kontroli uzbrojenia, wspieranym rozległą siecią komputerowej WAN lub innym skutecznym i wydajnym systemem komunikacyjnym. W skład tych systemów wchodzą funkcjonalnie ze sobą powiązane specjalistyczne urządzenia techniczne, wykorzystywane w celu zastosowania przyjętych procedur operacyjnych do wyznaczenia danemu obiektowi cechy przynależności.

Funkcjonujący w ramach Zintegrowanego Systemu Obrony Powietrznej NATO System Rozpoznania i Kontroli Przestrzeni Powietrznej, obok wykonywania innych zadań, jest głównym elementem identyfikacji obiektów powietrznych. Oparty na stanowiskach dowodzenia, naziemnych posterunkach radiolokacyjnych i samolotach wczesnego wykrywania, wytwarza rzeczywisty obraz sytuacji powietrznej – RAP, w którym każdy obiekt powietrzny ma przyporządkowaną określoną cechę wynikającą z jego identyfikacji. W systemie dowodzenia polską OP, zasadniczym elementem produkcji obrazu RAP będą ośrodki dowodzenia i naprowadzania (ODN) wyposażone w nowy, zautomatyzowany system dowodzenia

DUNAJ, który w tym wypadku będzie realizował wszystkie funkcje dotyczące identyfikacji obiektów powietrznych.

Osoby funkcyjne, odpowiedzialne za identyfikację, pracujące na tym systemie, mając do dyspozycji informację z poszczególnych źródeł i stosując określone procedury, muszą w ciągu dwóch minut nadać każdemu wykrytemu obiektowi powietrznemu określoną cechę identyfikacyjną, w innym wypadku obiekt ten zostaje zdjęty ze śledzenia. Jest to proces skomplikowany oraz pracochłonny i bez programowych algorytmów wspomagających pracę tych osób występują problemy z wykonaniem tego zadania, szczególnie w czasie ćwiczeń gdy stosuje się procedury przyjęte dla stanu zagrożenia lub wojny. Na typowych stanowiskach dowodzenia OP w NATO, wyposażonych w starszą generację zautomatyzowanych systemów dowodzenia, problem ten rozwiązuje się zwiększając znacznie ilość osób funkcyjnych zajmujących się identyfikacją obiektów powietrznych. W nowszych systemach stosuje się określone algorytmy wspomagające prace tych osób, zwłaszcza w zakresie identyfikacji lotnictwa nie wykonującego zadań operacyjnych. Najnowsze systemy posiadają funkcje zapewniającą automatyczną identyfikację zarówno w czasie wojny, jak i pokoju, oparte na cyfrowym przetwarzaniu danych z identyfikacji.

Źródłem informacji identyfikacyjnej są głównie urządzenia techniczne rozwinięte na określonych pozycjach lub przenoszone przez różnorodne typy uzbrojenia i sprzętu, także znajdującego się poza użyciem militarnym. Podstawowym, wyspecjalizowanym źródłem identyfikacji jest radiolokacyjny system identyfikacji „swój–obcy" IFF (Identification Friend or Foe) opierający swoją zasadę pracy na radiolokacji wtórnej. W odróżnieniu od radiolokacji pierwotnej, nie występuje tu pojęcie echa radiolokacyjnego, lecz odpowiedzi (odzewu). System ten musi się składać co najmniej z dwóch urządzeń aktywnych: urządzenia zapytującego (interrogatora) i urządzenia odzewowego (transpondera). Zapytanie jest wysyłane przez urządzenie zapytujące na jednej częstotliwości nośnej w kierunku obiektu wyposażonego w urządzenia odzewowe. W urządzeniu odzewowym zapytanie jest odbierane i dekodowane, a następnie zostaje wysłana zakodowana odpowiedź na fali nośnej o innej częstotliwości. Odebrany przez urządzenie zapytujące sygnał odpowiedzi, po obróbce i zdekodowaniu, zostaje w odpowiedni sposób zobrazowany, najczęściej w postaci umownych symboli, w powiązaniu z echem radarowym zapytywanego obiektu. Zdekodowanie sygnału odpowiedzi wymaga stosowania tego samego kodu przez urządzenia odzewowe i urządzenia dekodujące tę odpowiedź. Jeżeli tak jest, odpowiadający jest uznawany za „swój", w przeciwnym wypadku jest traktowany jako obiekt niezidentyfikowany lub „obcy". Częstotliwości nośne do zapytania i odpowiedzi, a także sposoby modulacji, są normowane przez parametry techniczne poszczególnych systemów. W większości systemów identyfikacji zapytanie jest nadawane anteną kierunkową, natomiast odpowiedź jest emitowana dookólnie. Aby zwiększyć możliwości identyfikacji, na przestrzeni lat wprowadzano różne rodzaje pracy (mody) systemu identyfikacji.

W NATO są stosowane systemy identyfikacyjne, które swoim rodowodem sięgają lat czterdziestych XX wieku. W ciągu tego czasu funkcjonowały systemy IFF,

określane jako MARK III i MARK V. W latach pięćdziesiątych wprowadzono na uzbrojenie system MARK X, zaś od początku lat sześćdziesiątych rozpoczęto użytkowanie systemu MARK XII.

Obecnie na szczeblu operacyjnym znajdują się systemy oznaczone jako MARK XA i MARK XII. Wersja podstawowa systemu IFF MARK XA może pracować z różnymi rodzajami zapytań, zwanymi modami, które się różnią między sobą liczbą możliwych kombinacji kodowych, a także zasobem przekazywanych informacji w odpowiedzi. System ten pracuje w modzie 1, 2 i 3/A oraz posiada możliwość pracy w systemie radarów wtórnych SSR (Secondary Surveillance Radar) wykorzystując dodatkowo mod C, który dostarcza dane o wysokości samolotu, mierzonej na podstawie ciśnienia barometrycznego. MARK XII obok wszystkich modów pracy wyszczególnionych w systemie MARK XA, posiada także zaszyfrowany mod bezpieczny. System IFF na tym poziomie jest jednak obarczony szeregiem niedoskonałości, takich jak:

– prosta, podatna na zakłócenia modulacja;

– niemożliwość ukrycia faktu emisji zarówno zapytania, jak i odpowiedzi;

– wspólne pasmo częstotliwości i mody pracy ze służbami cywilnej kontroli ruchu lotniczego;

– mała, ze względu na długość fali, rozróżnialność, a co za tym idzie kłopot w prawidłowym dowiązaniu identyfikacji do celu;

– mała odporność na zakłócenia.

Te niedoskonałości miało wyeliminować zastąpienie dotychczas używanych urządzeń identyfikacyjnych IFF MARK XII urządzeniami systemu „zapytania i odpowiedzi" Q & A (Question and Answer) MARK XV – pracującymi w milimetrowym zakresie częstotliwości. Zakładano także, poprzez zautomatyzowanie procesu przetwarzania danych, integrację w środowisku określonych systemów dowodzenia innych dostępnych źródeł informacji identyfikacyjnej zarówno współpracujących (cooperative target identification), jak i nie współpracujących (noncooperative target identification) z użytkownikiem dokonującym identyfikacji. Przyszły system identyfikacji powinien charakteryzować się następującymi cechami:

– prostotą;

– dopasowaniem do źródeł informacji dostępnych dla środków ogniowych;

– operacyjną niezawodnością;

– zdolnością skutecznego przeciwdziałania przed przejęciem przez przeciwnika;

– odpornością na zakłócenia;

– krótkim czasem reakcji.

Jednak rozwój sytuacji politycznej związany z ociepleniem stosunków politycznych oraz znaczny wzrost szacowanych nakładów finansowych na opracowanie urządzeń MARK XV spowodował zaniechanie tego programu. W NATO zdecydowano w tym wypadku, że nowym systemem identyfikacji, określanym jako Next Generation IFF – NGIFF, ma być system MARK XIIA będący wersją rozwojową systemu MARK XII poszerzoną o nowe mody pracy – mod S i mod 5.

Mod S powstał w celu usprawnienia kontroli ruchu lotniczego w przestrzeni powietrznej. Zapytanie interrogatora modu S wymusza określony format transmisji

danych z transpondera, którego także selekcjonuje się na podstawie żądanego adresu spośród innych transponderów obecnych na danym kontrolowanym obszarze. Mod S ma głównie zastosowanie cywilne do kontroli ruchu lotniczego. Ze względu jednak na wspólne wykorzystywanie przestrzeni powietrznej przez lotnictwo cywilne i wojskowe, przewiduje się wyposażyć w transpondery modu S wszystkie wojskowe statki powietrzne. Ponadto dane uzyskane z modu S usprawniają funkcjonowanie wojskowego Systemu Rozpoznania i Kontroli Przestrzeni Powietrznej, zwłaszcza w czasie pokoju.

Z wojskowego punktu widzenia docelowym modem pracy ma być jednak mod 5. Mod ten używa nowy rodzaj emisji elektromagnetycznej, który umożliwia eliminowanie wzajemnej interferencji odpowiedzi (degarbling) oraz dostarcza większe możliwości wymiany danych i zapewnienia ich bezpieczeństwa. Jednocześnie zastosowanie tych technik nie wyklucza wykorzystywania dotychczasowego odbiornika i nadajnika urządzenia IFF MARK XII pracującego z modem S, co minimalizuje koszt modernizacji urządzenia. W tym wypadku sprowadzono do minimum konieczność użycia dodatkowych układów, które są także w pełni kompatybilne z formą oraz kształtem aktualnego wyposażenia IFF.

Rezygnacja z implementacji rozwiązań MARK XV spowodowała także załamanie się wspólnej koncepcji identyfikacji pola walki w relacji powietrze–ziemia oraz ziemia–ziemia, gdyż wykorzystanie w tym celu urządzeń MARK XIIA, ze względu na ich niewystarczającą rozróżnialność, jest bardzo problematyczne. Tendencje w tym względzie dążą do uzyskania identyfikacji każdego obiektu na polu walki, od śmigłowca, stanowisk ogniowych artylerii i pocisków rakietowych, czołgów lub innego rodzaju pojazdów bojowych do pojedynczego żołnierza włącznie.

Analiza strat spowodowanych ostrzałem własnych sił i środków w czasie ostatnich konfliktów zbrojnych, szczególnie dotyczących konfliktu w Zatoce Perskiej oraz konfliktu na Bałkanach, wykazała wyraźną tendencję wzrostową w tym zakresie, mimo użycia najnowocześniejszych technik dotyczących identyfikacji. Ponadto konflikty te wykazały kłopoty we wspólnym użyciu koalicyjnych sił z powodu stosowania różnorodnych technik i systemów identyfikacyjnych. W konflikcie na Bałkanach doszły jeszcze poważne problemy z uniknięciem uderzeń na ludność cywilną, niezaangażowaną w konflikt. Dlatego też podjęto intensywne prace zmierzające do opracowania systemów identyfikacyjnych służących identyfikacji obiektów naziemnych – BTID (Battlefield Target Identification Device) oraz żołnierzy z indywidualnym i zbiorowym uzbrojeniem – DSID (Dismounted Soldier ID Device).

Opracowano, między innymi systemy oparte na niektórych rozwiązaniach technicznych systemu MARK XV. Są to urządzenia wysyłające kierunkowe zapytania w paśmie 37-38 GHz oraz uzyskujące odpowiedź z dookólnie pracującego transpondera. Innym rozwiązaniem jest wykorzystanie kierunkowego zapytania laserem oraz dookólnie wysyłanych odpowiedzi na częstotliwości 1090 MHz. Jeszcze innym rozwiązaniem jest konstrukcja systemu oparta na urządzeniach beakonowych. Zasada pracy tego typu urządzeń polega na ciągłej emisji przez własne obiekty określonych zakodowanych sygnałów, czytelnych wyłącznie dla wojsk

własnych. Beacony mogą pracować zarówno w zakresie mikrofal, jak i w podczerwieni. Proponowane rozwiązanie wykorzystuje pasmo 94 MHz. Istnieją także systemy oparte na istniejącej sieci łączności radiowej. Na przykład, modyfikowane programowo radiostacje pokładowe śmigłowca i czołgu lub pojazdu bojowego wymieniają relacje z częstotliwością ok.1 zapytania na sekundę. Wsparcie GPS-em powoduje aktualizację danych o pozycji obiektów własnych i zapobiega przypadkowemu ich zniszczeniu. Osobną klasę stanowią urządzenia identyfikacji pojedynczego żołnierza – CIDDS (Combat ID Dismounted Soldier), w większości bazujące na idei laserowego zapytania i odpowiedzi na bardzo wysokie częstotliwości – w zakresie od 900 MHz do 2,5 GHz.

Według założeń NATO docelowy system identyfikacji ma się składać z dwóch podstawowych elementów: środowiska operacyjnego opartego na funkcji IDCP oraz ściśle związanych z nim różnorodnych źródeł informacji identyfikacyjnej. Identyfikacja dotyczy trzech zasadniczych poziomów dowodzenia: poziomu strategicznego, operacyjnego, taktycznego, a także występuje na poziomie systemu uzbrojenia.

Na poziomie strategicznym i operacyjnym informacja identyfikacyjna, wspólnie z danymi uzyskanymi z szeroko rozumianego rozpoznania (w niektórych przypadkach dane te są także informacją identyfikacyjną) oraz celami kampanii lub operacji, jest zasadniczym elementem umożliwiającym planowanie działań zbrojnych i sprecyzowanie zamiaru walki, szczególnie w zakresie określenia listy obiektów uderzeń. Na poziomie taktycznym informacja identyfikacyjna, włączając w to także dane z rozpoznania i innych dostępnych źródeł informacji, jest podstawą do orientacji w zakresie aktualnej sytuacji taktycznej (situation awareness). Umożliwia to, w przypadku delegowania na ten szczebel uprawnień dowodzenia taktycznego TACOM (Tactical Command) lub kontroli taktycznej TACON (Tactical Control), skuteczne wykonanie postawionych zadań. Na poziomie systemów uzbrojenia (samoloty myśliwskie i uderzeniowe, systemy rakietowe i artyleryjskie itp.) informacja identyfikacyjna, dostarczona do operatora tego systemu razem z inną niezbędną informacją, umożliwia mu podjęcie właściwej decyzji co do użycia tego systemu i wybranie najbardziej odpowiedniego środka walki.

Informacja identyfikacyjna powinna zawierać czytelne dane, czy wykryty obiekt jest własny (friend), obcy (foe), czy neutralny (neutral), wskazać klasę platformy (class) i jej typ (type) oraz narodowość (nationality) i zamiar działania (intend), a także określić czy obiekt ten jest obiektem militarnym (military), czy cywilnym (civil). Jest to wymaganie dotyczące wszystkich powyższych poziomów, niemniej jednak charakterystyki te są używane w różny sposób. Dodatkowo, ranga tych charakterystyk jest inna na każdym rozpatrywanym poziomie, w zależności od środowiska działań zbrojnych (ziemia, powietrze, woda), zasięgu wykonania zadań i innych czynników.

W czasie działań zbrojnych identyfikacja jest jednym z zasadniczych etapów tworzenia rzeczywistego obrazu sytuacji nawodnej – RMP (Recognised Maritime Picture), sytuacji powietrznej – RAP (Recognised Air Picture) i sytuacji naziemnej – RLP (Recognised Land Picture) oraz uzyskania orientacji w sytuacji taktycznej –

SA (Situation Awareness). Rzeczywisty obraz danej sytuacji, w którym są zawarte obiekty posiadające informacje zarówno obligatoryjne, jak i dodatkowe dane identyfikacyjne jest dostarczany do wszystkich elementów, które mają lub mogą mieć nadane uprawnienia kontroli taktycznej nad podległymi jednostkami, na przykład w celu wykonania takich zadań, jak: poderwanie lotnictwa, podejście do celu, przechwycenie i oddziaływanie wewnątrz wyznaczonej strefy odpowiedzialności – AOR (Area of Responsibility). Orientacja w sytuacji taktycznej odnosi się do wszystkich elementów rozlokowanych na ziemi, morzu i w powietrzu, które muszą stale utrzymywać zdolność do oddziaływania. Umożliwia to zniszczenie przeciwnika, przy jednoczesnym uniknięciu niebezpieczeństwa oddziaływania na elementy neutralne (collateral damage) lub wojska własne (fratricide).

Generalnie proces identyfikacji rozpoczyna się w czasie, gdy z dostępnego źródła informacji otrzymamy pozycyjne dane o wykrytym obiekcie. Do danych tych następnie dowiązuje się i uogólnia wszystkie dodatkowe informacje pomocne w identyfikacji. Informacja w takiej formie jest następnie oceniana zgodnie z obowiązującymi kryteriami i na tej podstawie, w zależności od panującej sytuacji taktycznej, nadaje się określoną rekomendację, która w zależności od obowiązujących w danym czasie zasad użycia uzbrojenia RoE (Rules of Engagement) i innych uzyskanych informacji, stanowi, dla elementu upoważnionego do podjęcia decyzji o ostatecznej identyfikacji – IA (Identification Authority), podstawę do wyznaczenia określonej kategorii identyfikacyjnej dla tego obiektu. Tak przygotowana informacja jest przekazywana do elementów wykonawczych oraz utrzymywana w skorelowanej z nią trasie. Przebieg tego procesu jest nieco zróżnicowany, w zależności czy jest on wykorzystywany do celów produkcji rzeczywistego obrazu sytuacji powietrznej, nawodnej lub lądowej, czy jest on stosowany bezpośrednio w systemie uzbrojenia.

Do celów produkcji rzeczywistego obrazu sytuacji powietrznej, nawodnej lub lądowej proces identyfikacji można podzielić na sześć zasadniczych kroków: wykrycie (detect), kojarzenie (assess), informowanie (inform), ocenę (evaluate), nadanie określonej kategorii identyfikacyjnej (identity), dystrybucję do użytkowników (disseminate).

Wykrycie polega na uzyskaniu w czasie rzeczywistym – lub zbliżonym do czasu rzeczywistego – wszelkich dostępnych danych o interesującym nas obiekcie przez określone źródła informacji (także wykorzystywane poza siłami zbrojnymi).

Kojarzenie jest procesem polegającym na uogólnieniu tej informacji w celu wytworzenia możliwie najlepszego raportu o wykrytym obiekcie. Powinien on być realizowany na poziomie źródła, w sposób automatyczny lub z ingerencją operatora, z jednoczesnym podjęciem decyzji czy raport o tym obiekcie ma być przesłany do danego ośrodka dowodzenia i kontroli w celu jego identyfikacji.

Informowanie polega na przesyłaniu odpowiednich raportów do elementów dowodzenia upoważnionych do identyfikacji – IA. Po zakończeniu proces kojarzenia, wszystkie dane o wykrytych obiektach powinny być przesłane przez najszybsze środki do określonego ogniwa w celu ich oceny i nadania określonej identyfikacji. Raporty można przekazywać cyfrowo lub foniczne.

Ocena obejmuje analizę i syntezę różnorodnych danych uzyskanych ze źródeł w celu nadania wykrytemu obiektowi określonej rekomendacji identyfikacyjnej. Ocenia się informację pochodzącą z ogólnie rozumianego rozpoznania, plany lotów, procedury operacyjne, informację z różnego rodzaju środków radiolokacyjnych opartych na radiolokacji pierwotnej i wtórnej, informacji o wystąpieniu zakłóceń radioelektronicznych oraz prowadzonym przeciwdziałaniu radioelektronicznym, danych ze środków elektro-optycznych, rozpoznania wzrokowego, meldunków pilota, różnego rodzaju rozkazów bojowych oraz rozkazów i deklaracji wyższych przełożonych.

Nadanie identyfikacji polega na takim scharakteryzowaniu wykrytego obiektu, które umożliwia podjęcie w czasie rzeczywistym odpowiedniej decyzji z wysokim stopniem pewności. Po zakończeniu oceny i uzyskaniu konkretnej rekomendacji, element upoważniony do identyfikacji wyznacza dla danego obiektu odpowiednią kategorię identyfikacyjną, biorąc pod uwagę obowiązujące zasady użycia uzbrojenia.

Dystrybucja polega na przesyłaniu informacji w postaci rzeczywistego obrazu sytuacji powietrznej, naziemnej lub nawodnej od ogniwa upoważnionego do identyfikacji do wyższych przełożonych, sąsiednich ogniw, systemów uzbrojenia oraz innych użytkowników. Wymaga się aby informacja ta była terminowa oraz na tyle dokładna, by umożliwiła podjęcie decyzji w czasie rzeczywistym na wszystkich szczeblach.

W działaniach bojowych może się zdarzyć, że system uzbrojenia nie ma dostępu do rzeczywistego obrazu sytuacji naziemnej, nawodnej lub powietrznej. W tym wypadku system uzbrojenia musi się przede wszystkim upewnić, że wykryty przez niego obiekt jest właściwym celem, na którego ma oddziaływać. Dlatego też proces identyfikacji, w tym przypadku, składa się jedynie z trzech kroków: wykrycia celu, oceny wszystkich danych o tym celu oraz podjęcia decyzji o oddziaływaniu.

Wykrycie celu zarówno wskazanego przez nadrzędny system dowodzenia, jak i w czasie działań autonomicznych, polega na uzyskaniu w każdych warunkach występujących na polu walki informacji o tym celu, w tym także określonych charakterystyk identyfikacyjnych poprzez dostępne środki rozpoznawcze rozmieszczone na systemie uzbrojenia. Ocena zawiera analizę dostępnej na systemie informacji pod kątem uzyskania możliwie najlepszej rekomendacji identyfikacyjnej. Proces ten może być realizowany automatycznie lub ręcznie przez operatora obsługującego uzbrojenie. Rekomendacja identyfikacyjna, uzyskana z oceny w odniesieniu do występujących w danym czasie i rejonie zasad użycia bojowego danego systemu uzbrojenia, umożliwia podjęcie o wysokim stopniu pewności decyzji co do oddziaływania na wykryty cel.

W celu uniknięcia błędów dotyczących realizacji procesu identyfikacji, określa się, że wszystkie informacje dotyczące identyfikacji, które możemy uzyskać z dostępnych źródeł, powinny być automatycznie zbierane, uogólniane i w określony sposób przetwarzane. To wymaganie spełnia funkcja cyfrowego przetwarzania danych z identyfikacji, określana jako IDCP (Identification Data Combining Process), która w sposób automatyczny dowiązuje do wykrytych obiektów informację

identyfikacyjną uzyskaną z wielu różnorodnych źródeł. Funkcja ta może być zaimplementowana w szerokiej gamie systemów bazowych funkcjonujących w powietrzu, na lądzie i morzu w celu przydzielenia do wykrytych przez te systemy obiektów określonej identyfikacji. Dzięki temu wykryte obiekty zobrazowane zarówno w rzeczywistym obrazie sytuacji powietrznej, jak też naziemnej lub nawodnej mają nadane określone cechy i charakterystyki, które mogą być kluczowym elementem do osiągnięcia sukcesu w czasie działań zbrojnych. Funkcja ta zapewnia także zbiór i gromadzenie wszelkiej fragmentarycznej informacji uzyskiwanej ze środków elektronicznych lub innych źródeł o danej trasie eksponowanej w tym zobrazowaniu.

Funkcja IDCP przyjmuje informacje identyfikacyjną jednocześnie z wielu źródeł, przywiązując ją do właściwych tras i przekształca w dogodną formę celem przeprowadzenia procesu uogólnienia. Informacja uogólniona jest przedstawiona jako określona kategoria identyfikacyjna, która jest rekomendacją dla upoważnionego operatora – IA (Identification Authority), który odpowiada za końcową identyfikację. W celu bieżącej oceny wyniku identyfikacji można w każdym czasie sprawdzić gromadzoną w systemie informację identyfikacyjną. Funkcja IDCP zapewnia ponadto rozszerzenie tej informacji o dodatkowe dane, które mogą być wymieniane zarówno lokalnie, jak i w ramach współdziałania z innymi systemami. Jeśli jest to możliwe, informacje identyfikacyjne są wymieniane poprzez istniejące w systemach bazowych linie łączności i systemy komunikacyjne. W innym wypadku wprowadza się dodatkowe możliwości wymiany danych.

Celem funkcji IDCP jest rozszerzenie możliwości identyfikacyjnej systemów dowodzenia i kontroli oraz systemów uzbrojenia na morzu, lądzie i w powietrzu. Funkcja ta uogólnia wszelkie informacje identyfikacyjne otrzymywane z wielu różnorodnych źródeł i dostarcza możliwie najlepsze oszacowanie wyników identyfikacji wykrytych obiektów. W celu skrócenia czasu realizacji procesu identyfikacji, zastosowano komputerowe przetwarzanie danych połączone z odpowiednią reakcją człowieka. Umożliwia to racjonalne oszacowanie, zgromadzenie i włączenie w system bazowy informacji identyfikacyjnych otrzymywanych z różnych sensorów i źródeł w podobny sposób, jak realizuje to operator dokonujący subiektywnej oceny wartości informacji. Jednocześnie funkcja ta nie może ograniczać lub przeszkadzać w wymianie innych informacji używanych w systemie bazowym.

Koncepcja NATO i wynikające z niej standardy zakładają użycie funkcji IDCP w szerokiej gamie bazowych systemów w strukturze natowskiej i narodowej, w różnorodnych architekturach operacyjnych. Fundamentalną podstawą tej koncepcji jest fakt, że będzie ona osadzona w określonym systemie bazowym (np. system dowodzenia i kontroli lub system uzbrojenia), dlatego też funkcja ta jest realizowana na bazie dostępnego w tym systemie wyposażenia technicznego, oprogramowania oraz środków łączności. Forma danych wyjściowych z funkcji IDCP jest na tyle elastyczna, by została zaadaptowana przez system bazowy i wykorzystana zgodnie ze specyficznymi dla danego systemu wymaganiami.

Przetwarzanie danych z identyfikacji opiera się na czterech podstawowych podfunkcjach:

– kojarzeniu i korelacji z trasami (Association and Track Data Correlation);
– przetwarzaniu danych źródłowych (Single Source Processing – SSP);
– syntezie informacji (fusion);
– nadaniu ostatecznej cechy identyfikacyjnej (final identity category decision).

Kojarzenie (association) jest procesem włączania danych z identyfikacji do tras systemu bazowego. Wszystkie dane ze źródeł identyfikacji muszą być skojarzone z konkretnym zbiorem tras przed ich użyciem w procesie cyfrowego przetwarzania. System bazowy inicjuje i zawiązuje trasy na informacji z jednego źródła lub na podstawie uogólnienia danych pozycyjnych przychodzących z kilku różnych źródeł. Proces ten jest nazwany korelacją tras (track correlation). Część danych źródłowych używanych w czasie korelacji tras zawiera również dane identyfikacyjne. Dane te są kojarzone w ramach procesu korelacji. Te dane identyfikacyjne, które nie są używane w czasie korelacji mogą być użyte w dalszym procesie identyfikacji. Kojarzenie danych wejściowych może być przerywane automatycznie lub ręcznie przez operatora, co spowoduje usunięcie dotychczasowej informacji i skojarzenie nowej informacji identyfikacyjnej z trasą.

Przetwarzanie danych przychodzących z poszczególnych źródeł identyfikacji polega na konwersji, uogólnieniu, a także, jeśli jest to potrzebne, przekształceniu tych danych w format wymagany do przeprowadzenia procesu ich syntezy. Proces ten realizuje się oddzielnie dla każdego typu źródła, dlatego też każda część informacji dowiązana do trasy jest kojarzona do jednego ze standaryzowanego typów źródła (data routing) i skierowania do odpowiedniej sekcji realizującej konwersje i uogólnienie tych danych.

Dane identyfikacyjne, uzyskane ze źródła lub z procesu uogólniania, zazwyczaj nie są w formie dogodnej do przeprowadzenia procesu syntezy. Dlatego też funkcja przetwarzania danych identyfikacyjnych zawiera proces, który przekształca dane identyfikacyjne w standaryzowaną formę, nazwany **konwersją** (conversion). Proces ten jest oparty na użyciu odpowiedniej macierzy prawdopodobieństw, która reprezentuje prawdopodobieństwo uzyskania na wyjściu źródła każdej możliwej charakterystyki identyfikacyjnej dotyczącej danego typu obiektu. Wszystkie dane uzyskane z procesu konwersji są przedstawione w formie zbioru określonych prawdopodobieństw, zwanego inaczej wektorem prawdopodobieństwa (likelihood vector – LV). Prawdopodobieństwa te zależą od deklaracji charakterystyk nadanych obiektowi przez dane źródło. Istnieją źródła, które mają możliwość dostarczania danych bezpośrednio w formie wektora prawdopodobieństwa, w tym wypadku dane te nie są przekształcane w procesie konwersji.

W trakcie realizacji funkcji IDCP możemy mieć do czynienia z danymi wejściowymi pochodzącymi z wielu źródeł o tym samym typie, ze źródeł o różnych typach oraz ze źródeł, które posiadają kilka różnych metod uzyskiwania danych identyfikacyjnych (np. system „swój–obcy" IFF może uzyskiwać dane w modzie 1, 2, 3 itp.). Ponadto, może nastąpić sytuacja, że dane wyjściowe z danego źródła są powtórzone. Każda z tych sytuacji wymaga **uogólnienia informacji** (combining) na różnych poziomach procesu przetwarzania danych. Sytuacja ta może też wystą-

pić przed procesem konwersji (pre-combining) lub po tym procesie (post-conversion combining).

Przekształcenie informacji w format wymagany do przeprowadzenia syntezy (mapping), polega na przekształceniu wektora prawdopodobieństwa otrzymanego z danego źródła w formie charakterystyki identyfikacyjnej obiektu, w wektor opisujący klasę obiektu wyrażony w formie dogodnej do użycia w procesie syntezy na podstawie informacji bazowej. Uzyskuje się to poprzez określone wartościowanie danych identyfikacyjnych, gdzie wartości wagowe zależą w tym wypadku od statusu procedur operacyjnych systemu bazowego, czy są zadeklarowane dla stanu wojny, czy dla stanu pokoju. Przekształcenie w zależności od typu źródła może wystąpić zarówno przed procesem konwersji, jak i po nim.

Na wyjściu procesu przetwarzania danych źródłowych otrzymujemy pojedynczy wektor prawdopodobieństwa dla każdego typu źródła w klasie obiektu możliwej do określenia na podstawie dostępnej informacji identyfikacyjnej.

Synteza danych (fusion) polega na przetworzeniu informacji identyfikacyjnej w formie wektorów prawdopodobieństwa w różnych klasach obiektu w jeden wektor, opisujący klasę obiektu w formie standardowej.

Nadanie określonej cechy identyfikacyjnej (identity category decision) jest przekształceniem danych wyjściowych uzyskanych z syntezy w formę, która jest wymagana przez system bazowy.

Głównym efektem zastosowania funkcji IDCP powinno być zapewnienie skuteczności wykonania zadań identyfikacyjnych przez określony system bazowy. Adaptacja tej funkcji do specyficznych potrzeb systemu bazowego oraz do określonego środowiska operacyjnego, jest osiągana poprzez zawarcie w bazie danych następujących informacji:

– parametrów technicznych opisujących możliwości poszczególnych sensorów i źródeł;

– wartości wagowych lub współczynników wartościujących (mapping values) wynikających z sytuacji operacyjnej i rozkazów bojowych potrzebnych do przekształcenia danych wejściowych w określoną identyfikację;

– inne parametry, ustalone przez właściwy organ decyzyjny, wynikające z procedur operacyjnych i specyficznych funkcji systemu bazowego, stosowane do wewnętrznej kontroli mechanizmów funkcji IDCP i weryfikujące proces nadania cechy identyfikacji.

W celu zapewnienia powyższej informacji wymagane jest właściwe przetłumaczenie procedur identyfikacyjnych oraz odpowiednia interpretacja warunków środowiskowych w zbiór danych, który będzie użyty w funkcji IDCP w konkretnym systemie bazowym.

Identyfikacja wykrytych obiektów jest możliwa dzięki uzyskaniu odpowiedniej informacji o tych obiektach z dostępnych źródeł. Obok wyspecjalizowanego źródła identyfikacji systemu „swój–obcy" IFF, funkcja IDCP może wykorzystywać następujące źródła informacji:

– pasywne systemy rozpoznania radioelektronicznego;

– plany lotów i procedury operacyjne;

– zachowanie się obiektów;
– status pochodzenia trasy;
– określone raporty w transmisji Link 16;
– możliwości identyfikowanej platformy;
– inne narodowe środki identyfikacji.

Pasywne systemy rozpoznania elektronicznego (electronics support measures – ESM systems) mają zaprogramowaną listę danych o sygnałach radioelektronicznych, jakie mogą występować w środowisku, w którym działają i poprzez porównanie tych danych z emisją są w stanie określić klasę obiektu, przekazując tę informację do systemu IDCP. Na wyjściu tego typu systemów zwykle możemy otrzymać trzy rodzaje danych:

1) pomierzone parametry sygnału (measured signal parameter data), takie jak rodzaj emisji i częstotliwość;

2) rezultat porównania emisji z danymi zawartymi w oprogramowaniu (database matching results);

3) azymut, odległość i kąt elewacji źródła promieniowania (signal location).

Plany lotów są podstawowym narzędziem wspierającym proces identyfikacji. Dane te są także źródłem dla systemu IDCP i są głównie wykorzystywane w czasie pokoju. Natomiast w czasie ćwiczeń oraz działań bojowych źródłem identyfikacji w tym wypadku są plany misji. W tym celu wykorzystuje się także dane wynikające z podziału przestrzeni powietrznej (procedural routing) zawarte w ACP (Airspace Control Procedure), które określają drogi lotnicze na małej wysokości LLTRs (Low Level Transit Routes) oraz czasowo uaktywniane korytarze powietrzne – TMRRs (Temporary Minimum Risk Routes). Tego typu źródła informacji wykorzystuje się do identyfikacji własnego lotnictwa.

Do identyfikacji wrogiego lotnictwa stosuje się procedury wynikające z położenia obiektu (track behaviour). W tym celu odpowiednio definiuje się te elementy przestrzeni powietrznej, w których należy spodziewać się nieprzyjaciela (hostile profiles).

Innym źródłem identyfikacji dla systemu IDCP jest status pochodzenia trasy (Identification by Origin – IDBO). Porównanie wykrycia pierwszej pozycji trasy obiektu z zawartymi informacjami o bazowaniu lotnictwa i rozmieszczeniu lotnisk umożliwia identyfikację.

Samoloty i inne platformy posiadające możliwość transmisji danych w formacie Link 16 mogą przekazywać określone raporty (Precise Participant Location and Identification – PPLI) zawierające pozycję, kurs, identyfikację, rodzaj misji i status. Ze względu na fakt, że transmisja ta jest zakodowana z dużym poziomem bezpieczeństwa, stanowi ona także źródło identyfikacji dla systemu IDCP.

Warunkiem wstępnym uzyskania na wejściu funkcji IDCP informacji wejściowych jest skojarzenie z konkretną trasą danych identyfikacyjnych generowanych z różnych źródeł. Trasa ma przydzielony specjalny numer wynikający z procedur przetwarzania danych określonych dla systemu bazowego. Część źródeł identyfikacyjnych dostarcza zarówno dane pozycyjne, jak i dane identyfikacyjne, które są już skojarzone z odpowiednią trasą. Ta informacja może być przesłana bezpośred-

nio, zaraz po zawiązaniu trasy, pomijając proces kojarzenia, do dalszego przetwarzania raz do bazy danych. Dane identyfikacyjne, które nie są pierwotnie skojarzone z pozycją obiektu, powinny być dołączone do trasy w czasie procesu kojarzenia. Źródła generujące tego typu dane muszą dodatkowo dostarczać odpowiednie informacje o identyfikowanym obiekcie, takie jak: czas, pozycja, kurs lub prędkość, które umożliwią dołączenie informacji identyfikacyjnej do konkretnej trasy. W czasie kojarzenia stosowany jest podobny algorytm jak podczas korelacji, jednak ze względu na fakt, że różne źródła identyfikacyjne mogą dostarczać kombinację różnych informacji identyfikacyjnych, nie specyfikuje się ogólnego algorytmu dla tego procesu.

Przedstawione problemy związane z informacją o identyfikacji wykrytych obiektów w różnych środowiskach powinny się znajdować w kręgu zainteresowania wszystkich rodzajów sił zbrojnych. Obecnie informacja ta jest wymagana głównie w stosunku do obiektów działających w przestrzeni powietrznej, takich jak: samolotów myśliwskich i uderzeniowych, manewrujących pocisków rakietowych, środków bezpilotowych oraz środowiska morskiego zarówno w stosunku do obiektów pływających, jak i podwodnych. W niedalekiej przyszłości identyfikacja, w tym rozumieniu, ma dotyczyć także obiektów kosmicznych i pocisków balistycznych oraz środowiska lądowego w zakresie śmigłowców, artyleryjskich i rakietowych systemów uzbrojenia, pododdziałów pancernych i zmechanizowanych oraz żołnierzy z indywidualnym i zespołowym uzbrojeniem. Procedury operacyjne w zakresie zbierania, przetwarzania i przekazywania tego typu informacji są bardzo skomplikowane i – jak wynika z przedstawionego materiału – wymagają wspomagania informatycznego, co jak to ma miejsce w każdym systemie informatycznym, pozwoli uzyskać znaczne skrócenie czasu realizacji całego procesu identyfikacji oraz dostarczy człowiekowi stosowne narzędzia umożliwiające optymalną reakcję w czasie pokoju, zagrożenia i wojny.

płk dr inż. Marek Grzybowski
Szefostwo Wojsk Radiotechnicznych WLOP

WYMAGANIA INFORMACYJNE WOBEC POTRZEB KONTROLI PRZESTRZENI POWIETRZNEJ W RAMACH SYSTEMU OP NATO

Podejmowanie decyzji – zwiększenie jej trafności i operatywności – bardzo zależy od liczby i jakości informacji, jakimi dysponują organy decyzyjne. Właściwa realizacja zadań związanych z szeroko rozumianą obroną powietrzną, także jednoznacznie zależy od informacji, w tym wypadku, szczególnie zaś od informacji o sytuacji powietrznej. Funkcjonujący w NATO System Rozpoznania i Kontroli Przestrzeni Powietrznej ASACS (Air Surveillance and Control System) jest głównym elementem kontroli przestrzeni powietrznej, gdyż stanowi z jednej strony podstawowe źródło informacji o sytuacji powietrznej, a z drugiej strony jest także głównym elementem kierowania uzbrojeniem w obronie powietrznej.

Na ten system składa się sieć elementów dowodzenia i rozpoznania, ogniw przetwarzających informację oraz kanałów jej przesyłania, rozmieszczonych na ziemi i w powietrzu. Obejmuje ona pewne terytorium i jest funkcjonalnie powiązana w celu wykrycia, identyfikacji, przechwycenia i zniszczenia środków napadu powietrznego. W skład systemu wchodzą: naziemne stacjonarne i mobilne posterunki radiolokacyjne, samoloty wczesnego wykrywania oraz stanowiska dowodzenia – **CRC**, a do jego podstawowych zadań należy:

– rozpoznanie obiektów w przestrzeni powietrznej;
– identyfikacja;
– wymiana danych o sytuacji powietrznej;
– kierowanie aktywnymi systemami obrony powietrznej;
– walka z zakłóceniami radioelektronicznymi.

Rozpoznanie obiektów w przestrzeni powietrznej polega na ciągłym obserwowaniu wyznaczonego sektora przestrzeni powietrznej przez aktywne lub pasywne systemy rozpoznania radiolokacyjnego oraz wykrywaniu, śledzeniu i przekazywaniu informacji o obiektach powietrznych, które:

– naruszają określoną przestrzeń powietrzną;
– naruszają obowiązujące przepisy lotów;
– wlatują do zastrzeżonych obszarów;

– naruszają plany lotów;
– znajdują się w niebezpieczeństwie;
– są uprowadzone lub porwane.

Identyfikacja ma na celu określenie typu i przynależności obiektu powietrznego, wykorzystując jeden lub więcej z poniższych środków:
– korelację z planami lotów;
– elektroniczne zapytanie;
– zachowanie się obiektów w przestrzeni powietrznej;
– rozpoznanie wzrokowe.

Każde stanowisko dowodzenia systemu ASACS prowadzi samodzielnie identyfikację obiektów powietrznych, otrzymując z systemu kontroli ruchu lotniczego obraz sytuacji powietrznej oraz plany lotów. Każdy rozkaz podjęcia walki i zniszczenia celu powietrznego wydany na tym stanowisku, musi być poprzedzony ostatecznym potwierdzeniem identyfikacji obiektu powietrznego.

Wymiana danych o sytuacji powietrznej polega na opracowaniu i dystrybucji rzeczywistego obrazu sytuacji powietrznej RAP. W tym celu wszystkie elementy systemu ASACS muszą być wyposażone w zautomatyzowane systemy dowodzenia zapewniające wymianę danych oraz sterowanie środkami rozpoznania.

Kierowanie aktywnymi systemami obrony powietrznej polega na skoordynowanym użyciu lotnictwa do naprowadzania i zwalczania celów powietrznych oraz osłony lotnictwa uderzeniowego. Elementy systemu ASACS zabezpieczają działania lotnictwa uderzeniowego, stosując formy i metody dostosowane do sytuacji taktycznej, rodzaju misji i zdolności danego stanowiska dowodzenia. Zabezpieczają także działania bojowe jednostek OPL dostarczając obraz sytuacji powietrznej RAP, wskazując cele powietrzne do zniszczenia oraz zapewniając bezpieczeństwo własnego lotnictwa w strefie ich działania.

Walka z zakłóceniami radioelektronicznymi polega na utrzymywaniu zdolności do rozpoznania zakłóceń oraz skutecznym przeciwdziałaniu w celu zapewnienia zdolności do prowadzenia działań bojowych przez własne środki. Aby to osiągnąć lokalizuje się pozycję nosiciela zakłóceń i prowadzi działania zmierzające do jego wyeliminowania.

W systemie ASACS informowanie o sytuacji powietrznej jest oparte na rzeczywistym obrazie sytuacji powietrznej RAP, który jest definiowany jako elektronicznie produkowane zobrazowanie na podstawie informacji pochodzącej z radarów lub innych źródeł zapewniających pokrycie przestrzeni powietrznej w trzech wymiarach, w których odebrane sygnały elektroniczne są oceniane w celu ich zidentyfikowania i nadania określonego numeru dla obiektu powietrznego. Obraz ten ma dwie zasadnicze cechy:

1) odwzorowuje położenia obiektów powietrznych w czasie rzeczywistym;

2) przyporządkowuje każdemu obiektowi powietrznemu określoną cechę, wynikającą z jego identyfikacji.

Obraz RAP charakteryzują wskaźniki przestrzenne, jakościowe i ilościowe.

Wskaźniki przestrzenne są określone parametrami strefy informacji radiolokacyjnej (radar covering). Strefa informacji radiolokacyjnej jest częścią przestrzeni wypełnioną energią elektromagnetyczną, w której granicach środki rozpoznania radiolokacyjnego mogą wykrywać i identyfikować określone obiekty powietrzne z założonym prawdopodobieństwem. Tworzą ją zasięgi wykrywania radarów pierwotnych i wtórnych prowadzących rozpoznanie na posterunkach radiolokacyjnych. Strefę informacji radiolokacyjnej charakteryzuje jej głębokość, dolna i górna granica, przekrój poziomy na danej wysokości oraz współczynnik przekrycia. Powyższe parametry ulegają zmianie w warunkach stosowania przez przeciwnika zakłóceń radioelektronicznych, co uwzględnia współczynnik degradacji.

Głębokość strefy informacji radiolokacyjnej to podwójna odległość mierzona od linii ugrupowania posterunków radiolokacyjnych (naziemnych, nawodnych, powietrznych) do granicy maksymalnego zasięgu wykrywania obiektów powietrznych przez radary rozmieszczone na tych posterunkach. Zasięg wykrywania dla radarów pracujących impulsowo możemy określić z wyrażenia:

$$R = \sqrt[4]{\frac{PG^2\lambda^2\sigma}{P_o(4\pi)^3}}$$

gdzie:

P_{sr} – moc promieniowanej energii przez nadajnik radaru;

t_i – czas trwania impulsu;

G – zysk kierunkowy anteny;

λ – długość fali;

σ – skuteczna powierzchnia odbicia;

P_o – czułość odbiornika.

Wyrażenie to jest prawdziwe dla swobodnej propagacji fal radiowych nieuwzględniającej oddziaływania atmosfery oraz ukształtowania terenu i krzywizny ziemi. Atmosfera ziemska, w której rozchodzą się fale elektromagnetyczne generowane przez radary nie jest jednorodna, lecz zachodzą w niej zmiany takich parametrów, jak: temperatura, wilgotność i ciśnienie w funkcji wysokości. Powoduje to zmiany stałej dielektrycznej atmosfery, a poprzez to odchylenie toru fali elektromagnetycznej od prostoliniowego, zwane refrakcją atmosferyczną fal elektromagnetycznych. Charakter refrakcji zależy od wartości gradientu współczynnika załamania fal elektromagnetycznych i można wyróżnić trzy charakterystyczne przypadki dla różnych warunków meteorologicznych:

1) refrakcja ujemna – tor fali elektromagnetycznej jest odchylany w górę, co powoduje zmniejszenie zasięgu radaru;

2) refrakcja zerowa – tor fali jest prostoliniowy;

3) refrakcja dodatnia – tor fali elektromagnetycznej jest odchylany w kierunku powierzchni ziemi, co powoduje zwiększenie zasięgu radaru.

Liczbowa ocena wpływu refrakcji na zasięg wykrywania radarów wymaga dla każdego przypadku znajomości współczynnika załamania fal w zależności od wysokości. Wskutek silnych i szybkich zmian warunków meteorologicznych w troposferze problem ten nie jest rozwiązany. Dlatego też wpływ refrakcji na zasięg wykrywania radarów jest uwzględniony jedynie dla troposfery standardowej – normalnej, która występuje najczęściej w klimacie umiarkowanym. Dla troposfery normalnej gradient współczynnika załamania fal elektromagnetycznych jest ujemny, a refrakcja dodatnia, powodująca zwiększenie zasięgu wykrywania radaru o około 15% dla fal przyziemnych.

Powierzchnia ziemi nie jest idealnie gładka, w związku z tym odbicie od niej fal elektromagnetycznych nie zawsze jest odbiciem lustrzanym. Jeśli występuje warunek:

$$h_t = \frac{\lambda}{16 \sin \beta}$$

gdzie:
β – kąt odbicia fal elektromagnetycznych od wzniesienia;
H_t – wysokość terenu.

Wówczas odbicie fal elektromagnetycznych od powierzchni ziemi jest rozproszone, co powoduje wytworzenie jednolistkowej charakterystyki, którą trudno jest opisać matematycznie.

Głębokość strefy informacji radiolokacyjnej może być ograniczona strefami i stożkami martwymi, jeśli nie są one pokryte zasięgami wykrywania radarów rozmieszczonych na sąsiednich posterunkach. Strefa martwa jest to przestrzeń wokół osi radaru, w której granicach nie może on wykrywać obiektów powietrznych ze względu na bezwładność czasową urządzeń elektronicznych. Promień tej strefy określa się z zależności:

$$R_{sm} = \frac{c}{2}(\tau + \tau_1) + 1{,}3\frac{L_1}{L}C$$

gdzie:
c – prędkość rozchodzenia się fal radiowych w atmosferze;
τ_1 – czas przełączenia układu antenowego z nadajnika na odbiornik;
L – skala wskaźnika radaru;
L_1 – długość podstawy czasu wskaźnika;
C – średnica wiązki elektronów na ekranie wskaźnika.

Stożek martwy jest to przestrzeń położona wokół osi radaru ograniczona w płaszczyźnie pionowej maksymalnym kątem wzniesienia charakterystyki promieniowania tego radaru, a jego promień można obliczyć z wyrażenia:

$$R_{sm} = H\ tg_{\varepsilon \max}$$

gdzie:

ε_{max} – maksymalny kąt wzniesienia charakterystyki promieniowania radaru;

H – wysokość, dla której dokonujemy obliczeń.

Przekrój poziomy strefy informacji radiolokacyjnej na założonej wysokości jest to płaszczyzna, która obrazuje kształt i wymiary tej strefy dla danej wysokości. Powierzchnię tej płaszczyzny można określić, korzystając z zależności:

$$S_p = R_H\ N_{RLP}\ K$$

gdzie:

S_p – powierzchnia poziomego przekroju strefy informacji radiolokacyjnej;

R_H – zasięg wykrywania posterunków radiolokacyjnych na danej wysokości;

N_{RLP} – liczba posterunków radiolokacyjnych;

K – współczynnik uwzględniający sposób rozmieszczenia posterunków (w trójkąt K = 2,6, w kwadrat K = 2).

Dolna granica strefy informacji radiolokacyjnej jest to minimalna wysokość (H_d), powyżej której środki rozpoznania radiolokacyjnego mogą wykrywać określone obiekty powietrzne na danym kierunku. Zależy ona głównie od sposobu rozmieszczenia posterunków radiolokacyjnych oraz od ukształtowania terenu, nad którym ta strefa jest organizowana. Wyznacza się ją poprzez porównanie przekrojów poziomych stref informacji radiolokacyjnej i określenie wysokości, od której ich powierzchnia stanowi ciągłą płaszczyznę na rozpatrywanym kierunku. W tym wypadku wartość zasięgu wykrywania obiektów powietrznych powinna uwzględniać wpływ krzywizny ziemi i ukształtowanie terenu, i obliczamy ją korzystając z wyrażenia:

$$R_H = K_\alpha \sqrt[8]{\frac{P_i \tau G^2 \lambda^2 \sigma 4\pi h^4 H_c^{\ 4}}{P_{prog}\ \lambda^2}}$$

przy spełnieniu warunku, że:

$$R_H < 4.12(\sqrt{h} + \sqrt{H_c})$$

gdzie:

h – wysokość zawieszenia elementu promieniującego anteny radaru;

H_c – wysokość lotu obiektu powietrznego;

K_α – współczynnik kąta zakrycia pozycji rozmieszczenia radaru.

Współczynnik kąta zakrycia pozycji rozmieszczenia radaru, możemy określić z wyrażenia:

$$K_\alpha = \sqrt{1 + \frac{R_z}{2H_c}\sin^2\alpha} - \sin\alpha\sqrt{\frac{R_z}{2H_c}}$$

gdzie:

R_z – ekwiwalentny promień ziemi dla standardowej troposfery;

α – kąt zakrycia pozycji rozwinięcia radaru, określany z zależności:

$$\alpha = 57{,}33\frac{h_p h_{RLS} h_z}{d_p}$$

gdzie:

h_p – wysokość przeszkody terenowej;

h_{RLS} – wysokość elementu promieniującego radaru;

h_z – poprawka wysokości związana z krzywizną ziemi, którą określamy z zależności:

$$h_z = \frac{d_{p^2}}{R_z}$$

gdzie:

R_z – promień ziemi.

Górna granica strefy informacji radiolokacyjnej jest to maksymalna wysokość, do której środki rozpoznania radiolokacyjnego mogą wykrywać obiekty powietrzne. Wysokość górnej granicy strefy informacji radiolokacyjnej zależy od maksymalnego pułapu wykrywania radarów. Wyznacza się ją podobnie jak dolną granicę, porównując przekroje poziome stref informacji radiolokacyjnej i określając maksymalną wysokość, do której ich powierzchnia stanowi ciągłą płaszczyznę na rozpatrywanym kierunku.

Współczynnik przekrycia strefy informacji radiolokacyjnej charakteryzuje wielowarstwowość tej strefy w danym punkcie. Cecha ta zwiększa prawdopodobieństwo wykrycia i śledzenia obiektów powietrznych. Współczynnik przekrycia (K_p) jest wartością liczbową, która wskazuje, ile zasięgów wykrywania posterunków radiolokacyjnych w tym punkcie zachodzi na siebie i wzajemnie przenika. Można go określić, korzystając z następującej zależności:

$$K_p = 1.2\left[\frac{R_{hp}}{R_{hd}}\right]^2$$

gdzie:

R_{hp} – średni zasięg wykrywania posterunków radiolokacyjnych na wysokości danego punktu;

R_{hd} – średni zasięg wykrywania posterunków radiolokacyjnych dlawysokości dolnej granicy strefy rozpoznania.

Współczynnik degradacji określa wpływ zakłóceń radioelektronicznych stosowanych przez przeciwnika na pracę radarów, a tym samym na strefę informacji radiolokacyjnej. W czasie działań bojowych przeciwnik celowo wytwarza sygnały radiowe, które po wprowadzeniu do kanału odbiorczego radaru powodują obniżenie jego efektywności lub stłumienia pracy. Ze względu na sposób wytwarzania zakłóceń radioelektronicznych, dzielą się one na zakłócenia **aktywne** – wytwarzane przez specjalne nadajniki zakłóceń i **pasywne** – wytwarzane w wyniku odbioru fal elektromagnetycznych odbitych od różnych elementów odbijających.

Ze względu na oddziaływanie na stacje radiolokacyjne, zakłócenia dzieli się na dwa typy: **maskujące i imitujące**. Maskujące są wytwarzane przez wąskopasmowe i szerokopasmowe nadajniki zakłóceń ciągłych i bramkowanych, nadajniki zakłóceń impulsowych i pasywne odbijacze dipolowe. Zakłócenia imitujące (dezinformujące) mogą być wytwarzane przez nadajniki zakłóceń typu odzewowego i przez specjalne imitatory. Efektem działania tych zakłóceń jest gubienie celu w odległości i w kącie położenia, a także imitacja fałszywych celów.

W zależności od generowanego widma częstotliwości zakłócenia mogą być **zaporowe i skierowane**. Zakłócenia skierowane mają zakres widma tego samego rzędu, co pasmo przepuszczania zakłócanego radaru. Charakteryzują się one stosunkowo wysokim poziomem widmowej gęstości mocy. Zakłócenia zaporowe są wytwarzane w szerokim paśmie częstotliwości celem jednoczesnego zakłócania kilku urządzeń pracujących na różnych częstotliwościach. Zakłócenia te nie są dokładnie zestrojone z częstotliwością zakłócanego urządzenia. Mogą występować także zakłócenia śledzące, będące kompromisem pomiędzy zakłóceniami skierowanymi a zaporowymi. W tym wypadku częstotliwość nadajnika zakłóceń zmienia się z dużą szybkością w szerokim zakresie częstotliwości.

Współczynnik degradacji (k) jest stosunkiem mocy sygnału zakłócającego do mocy sygnału użytecznego na wejściu odbiornika zakłócanego radaru, w odniesieniu do charakterystyki pasma przepuszczania tego odbiornika. Współczynnik ten dla zakłóceń aktywnych, można określić z zależności:

$$k = \frac{P_z G_z D_s \, 4\pi}{P_s G_s D_{z^2} \delta} F^2(\Theta_z \Phi_z) \frac{f_s}{F_z} \gamma_z 10^{-0.1\alpha\,(Ds\,-\,Dz)}$$

gdzie:

P_z – sumaryczna wielkość widmowa mocy zakłóceń;

G_z – zysk kierunkowy anteny nadajnika zakłóceń;

D_s – odległość maskowanego obiektu od radaru;

P_s – moc zakłócanego radaru;

G_s – zysk kierunkowy anteny zakłócanego radaru;

D_z – odległość źródła zakłóceń od radaru;

δ_c – skuteczna powierzchnia odbicia maskowanego obiektu powietrznego;

Θ_z Φ_z – współrzędne biegunowe źródła zakłóceń określane w stosunku do maksimum charakterystyki promieniowania zakłócanego radaru;

F – funkcja opisująca znormalizowaną charakterystykę promieniowania zakłócanej stacji;

f_s – szerokość pasma przepuszczania odbiornika;

F_z – szerokość widma zakłóceń;

γ_z – współczynnik uwzględniający różnicę w polaryzacji fali nadajnika zakłóceń i radaru;

α – współczynnik uwzględniający tłumienie fal elektromagnetycznych w atmosferze.

Wartość funkcji opisującej znormalizowaną charakterystykę promieniowania zakłócanego radaru, można określić z następującej zależności:

$$F^2(\Theta_s, \Phi_s) = \frac{D_H}{D_{\max}} F^2(\Theta_s)$$

gdzie:

D_H – zasięg wykrywania radaru na wysokości H;

D_{max} – maksymalny zasięg wykrywania radaru w swobodnej przestrzeni;

$$F^2(\Theta_s) = \frac{1}{1 + (\frac{2\Theta}{\Theta 0.5})^2}; \quad dla \Theta_s < \Theta_o$$

$$F^2(\Theta_s) = 0{,}01; \quad dla \Theta_s > \Theta_o$$

gdzie:

Θ_s – szerokość charakterystyki promieniowania radaru na poziomie połowy mocy.

Dla zakłóceń pasywnych współczynnik degradacji określamy z zależności:

$$k = \frac{P_{zp}}{P_u}$$

gdzie:

P_{zp} – moc sygnału odbitego od chmur dipoli odbijających;

P_u – moc sygnału użytecznego.

W praktyce, ze względu na ciągłą zmianę współrzędnych biegunowych położenia obiektów powietrznych, w tym także źródła zakłóceń i obiektów maskowanych oraz szerokich możliwości stosowania różnych rodzajów form i metod zakłócania przez przeciwnika, trudno jest konkretnie określić wpływ zakłóceń na parametry strefy informacji radiolokacyjnej. Dlatego też współczynnik degradacji nie jest jednoznacznym wskaźnikiem charakteryzującym nam obraz RAP w warunkach stosowania zakłóceń radioelektronicznych. Stanowi on jedynie wartość po-

równawczą, określającą te możliwości w stosunku do przewidywanych zagrożeń ze strony przeciwnika powietrznego w określonej sytuacji operacyjno-taktycznej.

Wymagania systemu ASACS w zakresie wskaźników przestrzennych dla obrazu RAP są następujące:

– głębokość strefy informacji radiolokacyjnej – 100 mM od granicy NATO;

– dolna granica strefy informacji radiolokacyjnej – 100 m

– górna granica strefy informacji radiolokacyjnej – 30 000 m dla samolotów i 200 km dla rakiet balistycznych (Tactic Balistic Misile – TBM)

Oprogramowanie systemu zautomatyzowanego rozmieszczonego na CRC powinno zapewnić stały i szybki dostęp do bieżącego zobrazowania przekrojów poziomych strefy informacji radiolokacyjnej na wysokościach 100, 300, 500, 1000, 3000, 5000 i 10 000 m, w tym w przedziale od 100 do 1000 m z uwzględnieniem ukształtowania płaszczyzny ziemi, oraz współczynniki przekrycia w określonych rejonach. Możliwości oprogramowania powinny także zapewniać określanie współczynnika degradacji, jeśli jesteśmy w stanie określić charakter i typ źródła zakłóceń.

Wskaźniki jakościowe charakteryzujące obraz RAP to: aktualność obrazu RAP, jego wiarygodność oraz kompletność informacji zawartej w tym obrazie. Informację o sytuacji powietrznej uznaje się za aktualną, jeżeli jej zobrazowanie odzwierciedla (w dopuszczalnych granicach błędów) rzeczywisty stan w rejonie działań bojowych w wymiarze powietrznym. Granicę błędu w systemie rozpoznania przestrzeni powietrznej determinują dopuszczalne wartości takich wskaźników, jak: czas opóźnienia, dyskretność przekazywanej informacji i jej dokładność.

Czas opóźnienia to parametr charakteryzujący szybkość przepływu informacji o sytuacji powietrznej. Jest to różnica między czasem dostarczenia tej informacji do określonego użytkownika a czasem ich zdobycia przez środki rozpoznania w przestrzeni powietrznej, czas ten określamy korzystając z następującej zależności:

$$t_{op} = t_c + \sum_{m=1}^{M} t_{pr} + \sum_{n=1}^{N} t_i + t_{pz}$$

gdzie:

t_c – czas potrzebny na wykrycie obiektu powietrznego;

t_{pr} – czas opracowania informacji;

t_i – czas identyfikacji obiektu powietrznego;

t_{pz} – czas przekazania informacji o wykrytym obiekcie powietrznym;

M – liczba elementów biorących udział w opracowaniu informacji o wykrytym obiekcie;

N – liczba szczebli dowodzenia biorących udział w identyfikacji obiektów powietrznych.

Obecne wymagania dla systemów elektronicznych tworzących obraz RAP jednoznacznie określają, że czas wykrycia obiektu i czas opracowania informacji powinien być bliski zeru. Podobnie wymaganie dotyczące wymiany danych w czasie

rzeczywistym powoduje, że czas przekazywania informacji także powinien być bliski zeru. Ponieważ wszelkie procesy związane z tworzeniem obrazu RAP muszą być realizowane na jednym szczeblu wykonawczym, jakim jest CRC, czas opóźnienia informacji o sytuacji powietrznej w tym przypadku zależy jedynie od czasu identyfikacji obiektów powietrznych. W systemie ASACS czas ten nie może przekraczać dwóch minut. Jeżeli po tym czasie obiekt powietrzny nie został jednoznacznie zidentyfikowany, powinien on zostać automatycznie zdjęty ze śledzenia. W przyszłościowym systemie ACCS zakłada się pełną automatyzację procesu identyfikacji i czas ten zostanie skrócony do trzydziestu sekund. Ponieważ zasady dystrybucji obrazu RAP określają, że obraz ten może być rozesłany, jeśli jest w pełni zidentyfikowany, można określić, **że czas opóźnienia w obrazie RAP, zgodnie z aktualnymi normami, nie przekracza dwóch minut, natomiast w przyszłym systemie ACCS nie może przekraczać trzydziestu sekund**.

Do zobrazowania sytuacji w rejonie działań bojowych w wymiarze powietrznym, potrzebny jest ciąg informacji – począwszy od położenia obiektów powietrznych w przestrzeni powietrznej, a kończąc na charakterystycznych cechach tych obiektów. Minimalny przedział czasu między dwoma kolejnymi odczytami lub zapisami tej samej informacji na urządzeniach zobrazowania, określa się jako **dyskretność** w przekazywaniu informacji o sytuacji powietrznej. Dyskretność informacji udostępnianej użytkownikom, zależy głównie od rozwiązań technicznych urządzeń wykorzystywanych do jej zbioru i opracowania oraz od przepustowości kanałów informacyjnych. Wymagania w tym zakresie dla obrazu RAP określają, że dyskretność przekazywanej informacji powinna być na tyle mała, żeby zapewnić odwzorowanie tej informacji w czasie rzeczywistym. Na wielkość tego parametru nie może mieć także wpływu liczba śledzonych obiektów powietrznych.

Dokładność informacji o sytuacji powietrznej określa błąd, jaki może wystąpić w zobrazowaniu tej informacji i dotyczy położenia obiektu w przestrzeni powietrznej oraz jego przemieszczania. Można ją określić korzystając z następujących zależności:

$$X_r - X_z = \delta_x \quad \text{lub} \quad D_r - D_z = \delta_h$$
$$Y_r - Y_z = \delta_y \quad \text{lub} \quad \beta_r - \beta_z = \delta_h$$
$$H_r - H_z = \delta_h \quad \text{lub} \quad H_r - H_z = \delta_h$$

gdzie:

X_r Y_r – współrzędne topograficzne rzeczywistego miejsca położenia rozpoznawanych obiektów;

X_z Y_z – współrzędne topograficzne zobrazowania położenia rozpoznawanych obiektów;

D_r β_r – współrzędne biegunowe rzeczywistego miejsca położenia rozpoznawanych obiektów;

D_z β_z – współrzędne biegunowe zobrazowania rozpoznawanych obiektów powietrznych;

H_r – rzeczywista wysokość lotu rozpoznawanego obiektu;

H_z – zobrazowana wysokość lotu rozpoznawanego obiektu;

δ_x δ_y – dokładność informacji o położeniu rozpoznawanych obiektów, zobrazowanych w układzie współrzędnych topograficznych;

δ_d δ_β – dokładność informacji o położeniu rozpoznawanych obiektów, zobrazowanych w układzie współrzędnych biegunowych;

δ_h – dokładność informacji o wysokości lotu rozpoznawanych obiektów.

Ukazanie obiektów powietrznych w obrazie RAP różni się od rzeczywistego ich położenia o błędy wnoszone przez wszystkie ogniwa uczestniczące w jego tworzeniu. Błędy te dzielimy na błędy statyczne i dynamiczne. Błędy statyczne wynikają z technicznych charakterystyk źródeł i urządzeń tworzących obraz RAP, i składają się z:

– błędów orientowania i dowiązania topograficznego;
– błędów radaru jako przyrządu pomiarowego;
– błędów zamiany odległości pochyłej na poziomą;
– błędów zdejmowania współrzędnych;
– błędów przedstawiania na urządzeniach tworzących obraz.

Błąd ten (δ_s) określa się korzystając z następującej zależności:

$$\delta_s = \sqrt{\sum_{i=1} \delta_i^{\,2}}$$

gdzie:

δ_i – średniokwadratowy błąd wnoszony przez i-te ogniwo systemu uczestniczące w tworzeniu RAP.

Błędy dynamiczne określania współrzędnych wynikają z dyskretnego charakteru przekazywania informacji o sytuacji powietrznej i jej opóźnienia. Wartość tych błędów może się zmieniać w dowolnym przedziale, w zależności od czasu ekstrapolacji i manewrowych możliwości celu, i wynosi:

$$\delta_d = \sqrt{\delta_s^{\,2} + (\delta_v t_e)^2}$$

gdzie:

t_e – czas ekstrapolacji;

δ_v – średniokwadratowy błąd określenia prędkości celu.

Wypadkowy błąd określania współrzędnych obiektu powietrznego, obliczamy ze wzoru:

$$\delta_w = \sqrt{\delta_s^{\,2} + \delta_d^{\,2}}$$

W związku z tym, że dyskretność przekazywanej informacji musi zapewnić odwzorowanie obrazu RAP w czasie rzeczywistym, błędy dynamiczne w tym wypadku nie mają wpływu na dokładność obrazu RAP.

W przypadku błędów statycznych powinien być minimalizowany wpływ poszczególnych czynników. Błędy wynikające z orientowania i dowiązania topograficznego poszczególnych źródeł nie mogą przekraczać wartości określonych w ich formularzach technicznych. Podobnie w przypadku rozróżnialności radaru, jej wartość jest określona w tych dokumentach. Wartość wypadkowa błędów nie powinna przekraczać 500 m w odległości i wysokości oraz 1° w azymucie.

Błąd zamiany odległości pochyłej na poziomą jest błędem systematycznym i powinien być wyeliminowany w systemie zautomatyzowanym. Błąd zobrazowania informacji, w przypadku gdy RAP jest zobrazowany na monitorze komputerowym, zależy jedynie od jego rozdzielczości i może być w zasadzie wyeliminowany przez dobór odpowiedniej skali tego zobrazowania.

W tym wypadku, największy wpływ na dokładność informacji będzie miał błąd zdejmowania współrzędnych. Wartość tego błędu będzie mniejsza w przypadku automatycznego wykrywania i śledzenia obiektów, natomiast będzie znaczna, gdy ta funkcja będzie wykonywana ręcznie. Dlatego przy tworzeniu obrazu RAP jest wykluczone ręczne śledzenie obiektów. W pracy automatycznej zaś, jako podstawowy rodzaj pracy, wykorzystuje się śledzenie na podstawie głównego reprezentanta. Aproksymowanie położenia obiektu powietrznego na podstawie informacji z kilku źródeł jest w tym wypadku niewskazane.

W zasadzie nie ma określonych konkretnych danych liczbowych dla dokładności informacji w obrazie RAP. Wymagania dotyczą jednak zapewnienia możliwości realizacji procesu naprowadzania samolotów myśliwskich na cele powietrzne na podstawie sytuacji zobrazowanej na szczeblu CRC. Do realizacji tej funkcji błędy w zobrazowaniu położenia obiektów powietrznych nie powinny przekraczać wartości wypadkowej błędu wynikającego z orientowania i dowiązania topograficznego oraz rozróżnialności radaru. Natomiast błąd wypadkowy w położeniu obiektu w obrazie RAP zobrazowanym na szczeblu CAOC, powinien się mieścić w bramce 3 mM.

Informację uważa się za wiarygodną, jeśli istnieje określony stopień pewności, że jest ona prawdziwa lub ścisła. Wykrywanie obiektów powietrznych jest procesem, który polega na stwierdzeniu obecności lub braku tych obiektów w obserwowanej przestrzeni powietrznej (obszarze operacyjnego zainteresowania). Odbywa się on w okolicznościach, gdy obiekt rzeczywiście się znajduje w tej przestrzeni oraz gdy takiego obiektu rzeczywiście tam nie ma. Stosownie do tych warunków, można podjąć cztery różne decyzje dotyczące wykrywania obiektu powietrznego.

W sytuacji, kiedy obiekt jest rzeczywiście w przestrzeni obserwowanej, stwierdzenie, że obiekt tam jest, będzie wykryciem poprawnym, a stwierdzenie, że obiektu tam nie ma, będzie wówczas przepuszczeniem obiektu. W sytuacji, gdy obiektu rzeczywiście nie ma w przestrzeni, stwierdzenie, że obiektu tam nie ma, będzie niewykryciem właściwym, a stwierdzenie, że obiekt tam jest, będzie fałszywym alarmem. Ponieważ sygnały użyteczne i zakłócenia są przypadkowymi funkcjami czasu, podjęcie każdej decyzji dotyczącej wykrycia obiektu ma również charakter przypadkowy, dlatego wiarygodność informacji (W_i) będzie wyrażona następującą funkcją:

$$W_i = f\{ P_w, P_n, P_p, P_{fa} \}$$

gdzie:

P_w – prawdopodobieństwem prawidłowego wykrycia obiektu;

P_n – prawdopodobieństwem prawidłowego jego niewykrycia;

P_p– prawdopodobieństwem przepuszczenia obiektu powietrznego;

P_{fa} – prawdopodobieństwem fałszywego alarmu.

Ponieważ poprawne wykrycie i przepuszczenie obiektu oraz poprawne nie wykrycie i fałszywy alarm tworzą grupę zdarzeń przeciwnych (niezgodnych), niezależne są tylko dwie wielkości. Dlatego do scharakteryzowania wiarygodności informacji o sytuacji powietrznej, przyjmuje się zwykle wskaźnik dotyczący prawdopodobieństwa wykrycia obiektu i prawdopodobieństwa fałszywego alarmu.

W praktyce, w rozpoznaniu radiolokacyjnym, prawdopodobieństwo wykrycia obiektów powietrznych w granicach określonych możliwościami przestrzennymi waha się w granicach od 0,5 do 0,9, dla prawdopodobieństwa fałszywego alarmu od 10^{-10} do 10^{-6}, jednak wartości te są bardzo trudne do określenia w trakcie prowadzenia rozpoznania. Dlatego **w przypadku obrazu RAP wskaźnik wiarygodności informacji oblicza się na podstawie liczby uzyskanych sygnałów odbitych od obiektu powietrznego za każdy obrót anteny radaru**. Gdy za każdym obrotem anteny uzyskujemy sygnał odbity od obiektu powietrznego, wartość tego wskaźnika wynosi 7. Gdy za jakimkolwiek obrotem anteny radaru nie otrzymamy sygnału, wartość wskaźnika obniża się o 1, aż do wartości zero. W systemach funkcjonujących na szczeblu CRC, przy wartości tego wskaźnika mniejszym od 3, obiekt powietrzny jest zdejmowany ze śledzenia.

Wiarygodność informacji zawartej w obrazie RAP określa także stopień prawdopodobieństwa poprawnej identyfikacji obiektów powietrznych. Wskaźnik ten zależy od możliwości dostępu do określonych środków umożliwiających identyfikację. W czasie pokoju uważa się, że informacja w tym zakresie jest wiarygodna, jeśli jest skorelowana z planami lotów i potwierdza to elektroniczne zapytanie przez urządzenie IFF w modzie 3A, natomiast w czasie wojny i zagrożenia – jeśli jest skorelowana z rozkazem o zarządzaniu przestrzenią powietrzną (Air Coordination Order – ACO) oraz potwierdzona elektronicznie w modzie 1 lub 4.

Informacje uznaje się za kompletną, jeśli zawiera wszystkie elementy potrzebne użytkownikowi. W przypadku obrazu RAP są to następujące informacje:

1. Numer obiektu (NATO Track Number – NTN), składający się z dwóch liter i trzech cyfr. Litery są przyporządkowane określonemu CRC, cyfry zaś nadaje losowo system zautomatyzowany.

2. Źródło (source) trasy obiektu powietrznego. Może to być trasa skorelowana z kilku radarów (correlator) lub pochodząca z pojedynczego źródła (single source).

3. Status obiektu powietrznego (status), mówiący, czy jest to obiekt rzeczywisty (live), czy symulowany (simulated).

4. Cecha identyfikacji obiektu powietrznego (identification) w postaci jednego z dziesięciu umownych określeń.

5. Pozycja obiektu powietrznego (position) podana według siatki współrzędnych geograficznych GERGEW, LATLONG i UTM.

6. Indeks pilota (callsing), jeśli jest to własny samolot bojowy.

7. Prędkość obiektu powietrznego (speed) podana w węzłach (in knots).

8. Kurs obiektu powietrznego (heading) w stopniach.

9. Wysokość obiektu powietrznego (height) podana w hektostopach (in Flight Levels).

10. Mod 1 pochodzący z urządzenia IFF w postaci dwóch cyfr.

11. Mod 2 pochodzący z urządzenia IFF w postaci czterech cyfr.

12. Mod 3/A pochodzący z urządzenia IFF w postaci czterech cyfr.

13. Mod 4 pochodzący z urządzenia IFF w postaci jednej litery.

14. Standard informacji, jakim jest przekazywana trasa obiektu (Interim JTIDS Message Standard).

15. Sygnał niebezpieczeństwa, jeśli obiekt powietrzny emituje (emergency).

17. Jakość trasy obiektu powietrznego (quality) wyrażona w skali od 1 do 7.

18. Przydział celu (allocation), jeśli jest przydzielony dla wojsk rakietowych lub lotnictwa (to SAM or Fighters).

Skład (strenght).

Grupa wskaźników liczbowych dotyczy możliwości wojsk radiotechnicznych w zakresie uzyskiwania informacji o rozpoznawanych obiektach powietrznych i ich zobrazowania, i jest określana jako liczba informacji o rozpoznawanych obiektach powietrznych. Zależy ona, przede wszystkim od możliwości technicznych urządzeń realizujących zbiór, przetwarzanie i zobrazowanie informacji oraz od rozdzielczości środków rozpoznania, liczby kanałów łączności i poziomu wyszkolenia osób funkcyjnych.

W zakresie tworzenia obrazu RAP wymagania odnośnie do tego wskaźnika, są określone prawdopodobnym natężeniem obiektów powietrznych w strefie odpowiedzialności CRC oraz jego sąsiadów. Obecne wymagania określają, że system zautomatyzowany na tym szczeblu powinien mieć **możliwość śledzenia 300 i zobrazowania 1000 tras**. Natomiast w przyszłościowym systemie ACCS wymaga się śledzenia **1000 i zobrazowania około 2000–3000 tras**.

mjr mgr Andrzej Stańczak
mgr Wojciech Burakowski

Wojskowy Instytut Łączności

SYSTEM ŁĄCZNOŚCI NOWEJ GENERACJI DLA WOJSK LOTNICZYCH I OBRONY POWIETRZNEJ RP

Wstęp

Program modernizacji SZ RP, wynikający z przystąpienia Polski do NATO, obejmuje wiele istotnych punktów. Wśród nich ważnym zagadnieniem jest interoperacyjność systemu dowodzenia obroną powietrzną RP oraz NATINADS (NATO Integrated Air Defence System). Do realizacji powyższego celu jest projektowany Cyfrowy Zintegrowany System Teleinformacyjny Wojsk Lotniczych i Obrony Powietrznej (system CZST WLOP). Architektura projektowanego systemu łączności powinna spełniać wymagania stawiane systemom C4 wykorzystującym najnowsze techniki telekomunikacyjne, tj. ATM, ISDN, LAN.

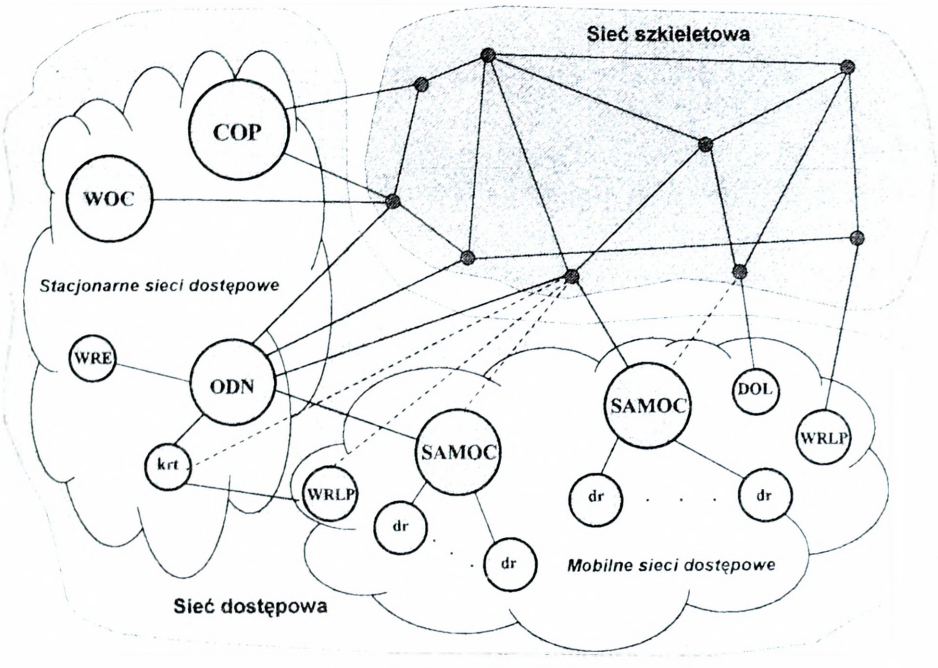
W artykule dokonano przeglądu głównych założeń dla sieci łączności systemu CZST WLOP. Architektura sieci uwzględnia zarówno obecny stan zaawansowania dostępnych technik telekomunikacyjnych (stan standaryzacji, urządzenia dostępne na rynku, dotychczasowe doświadczenia), jak i konieczne usługi sieciowe do realizacji efektywnego przekazu informacji związanych z różnymi aplikacjami (usługami) oferowanymi w sieci. Wspomniane usługi sieciowe powinny mieć zaimplementowane odpowiednie mechanizmy celem zapewnienia wymagań dotyczących jakości przekazu poszczególnych rodzajów informacji. Należy nadmienić, iż projektowany system powinien być eksploatowany przez wiele lat, zatem powinien się cechować elastycznością i możliwością rozbudowy.

Sieć łączności CZST WLOP (rys. 1) zawiera sieć szkieletową oraz sieć dostępową (stacjonarną i mobilną). Sieć szkieletowa obejmuje swoim zasięgiem całe terytorium Polski. Posiada typową architekturę sieci WAN (Wide Area Networks) i jest budowana na podstawie techniki ATM, integrującej różne typy przenoszonych informacji (mowa, dane, wideo etc.). Warto zauważyć, iż obecnie ATM jest techniką w pełni dojrzałą i trudną do zastąpienia przez inne techniki telekomunikacyjne.

Sieć dostępowa systemu CZST WLOP obejmuje lokalne sieci stacjonarne i sieci mobilne. Sieci stacjonarne służą do przyłączenia stałych systemów dowodzenia

i kierowania (np. Centrum Operacji Powietrznych – COP, Ośrodek Dowodzenia i Naprowadzania – ODN etc.). Mobilna sieć dostępowa służy do przyłączenia jednostek mobilnych (np. centrum kierowania pociskami ziemia-powietrze – SAMOC (Surface to Air Missiles Operations Centre], dywizjony rakietowe).

Opisujemy architekturę mobilnej sieci dostępowej. De facto, istnieje pewne podobieństwo pomiędzy rozważaną siecią i sieciami taktycznymi, które obecnie wchodzą w zakres projektu TACOMS Post-2000.



COP – Centrum Operacji Powietrznych, DOL – drogowy odcinek lotniskowy, dr – dywizjon rakietowy, krt – kompania radiotechniczna, ODN – Ośrodek Dowodzenia i Naprowadzania, SAMOC (Surface to Air Missiles Operations Centre) – stanowisko dowodzenia przeciwlotniczymi zestawami rakietowymi, WOC (Wing Operations Centre) – stanowisko dowodzenia jednostką lotnictwa taktycznego, WRE – walka radioelektroniczna, WRLP – wysunięty posterunek radiolokacyjny.

Rys. 1. Sieć łączności systemu CZST WLOP

Wymagania dla sieci łączności systemu CZST WLOP

Modelem odniesienia dla systemu dowodzenia obroną powietrzną RP jest system NATINADS. Sieć łączności systemu CZST WLOP uwzględnia zarówno ten model, jak i dodatkowe uwarunkowania istniejącego systemu narodowego.

Podstawowe wymagania dla systemu CZST WLOP można wyszczególnić następująco:

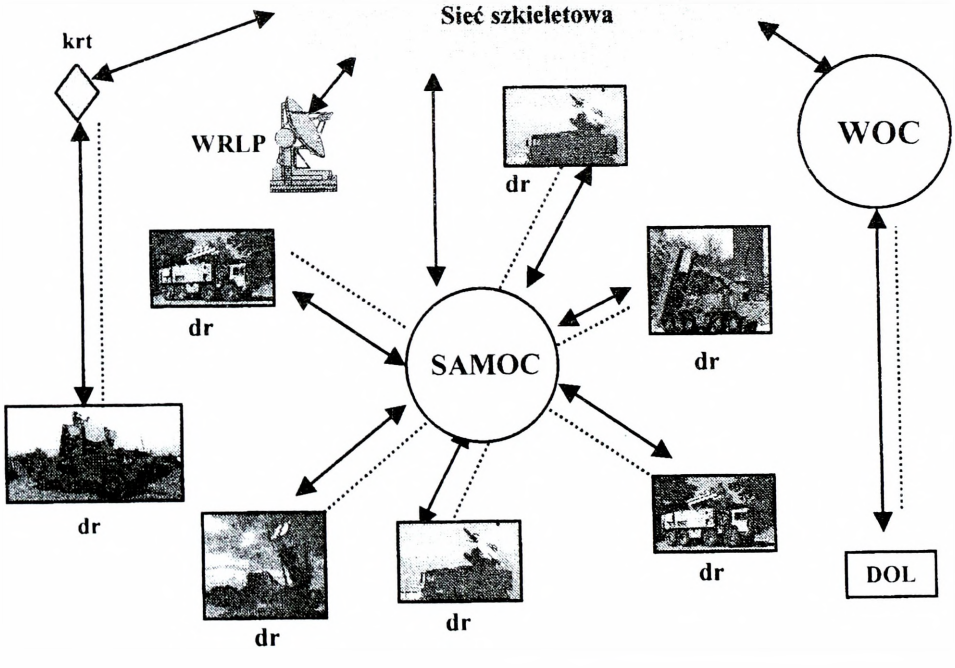
– zgodność ze standardami NATO (współpraca z systemem NATINADS),

– wymiana informacji niejawnych zgodnie ze standardami narodowymi,
– efektywny system zarządzania,
– efektywny przekaz różnych typów informacji (np. mowa, dane, wideo),
– przekaz pilnych wiadomości (np. RAP – Recognised Air Picture) z priorytetem,
– dynamiczne zarządzanie ruchem,
– odporna topologia sieci.

Sieć szkieletowa powinna dodatkowo zawierać odpowiednie styki urządzenia do zapewnienia współpracy z istniejącymi sieciami wojskowymi i cywilnymi.

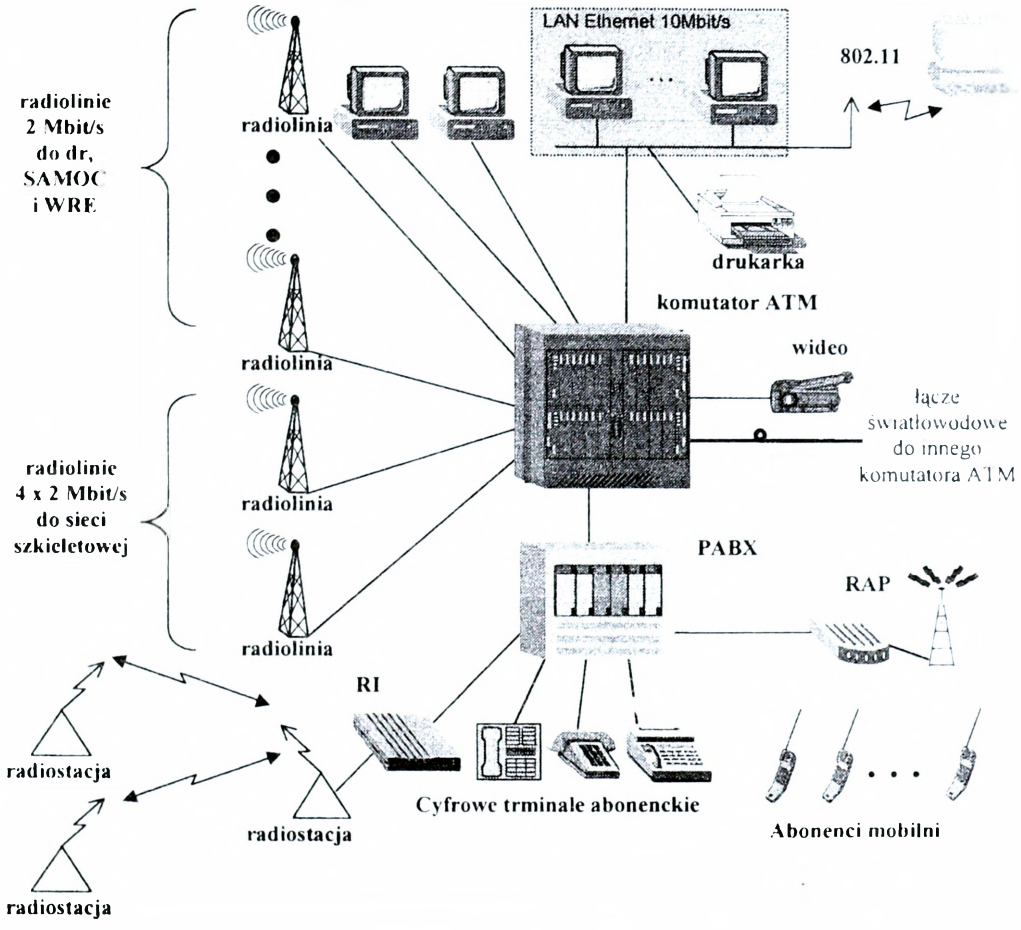
Architektura mobilnej sieci dostępowej

Zasadniczą część mobilnej sieci dostępowej systemu CZST WLOP (rys. 2) stanowi węzeł łączności SAMOC. Jest on dołączony do węzłów łączności wielu dywizjonów rakietowych, tworząc topologię gwiazdy. Węzeł SAMOC jest dołączony do sieci szkieletowej. Podstawowymi łączami transmisyjnymi, używanymi w mobilnej sieci dostępowej, są łącza radioliniowe o przepustowości od 2 do 8 Mbit/s. Łączami zapasowymi są łącza radiowe (przedstawione na rys. 2 linią przerywaną).



Rys. 2. Architektura mobilnej sieci dostępowej

Organizację węzła SAMOC przedstawiono na rys. 3. Centralnym elementem węzła jest komutator ATM, który integruje ruch mowy (generowany przez centralę PABX) i ruch danych (generowany przez rozwijaną w systemie dowodzenia sieć LAN, zazwyczaj typu Ethernet). Dodatkowo do utrzymania telefonicznej łączności bezprzewodowej, do PABX jest dołączony punk dostępu radiowego (RAP – Radio Access Point). Interfejs radiowy – RI (Radio Interface) służy do dołączenia PABX do zapasowych łączy radiowych. Komutator ATM jest dołączony przez łącza radioliniowe zarówno do innych węzłów, jak i do sieci szkieletowej.



RI (Radio Interface) – interfejs radiowy, RAP (Radio Access Point) – punkt dostępu radiowego, PABX (Private Automatic Branch Exchange) – centrala telefoniczna z komutacją kanałów.

Rys. 3. Organizacja węzła łączności SAMOC

Typy aplikacji

Poniżej przedstawiono krótki przegląd potencjalnych aplikacji dostępnych w nowoczesnych systemach dowodzenia, z punktu widzenia ich charakterystyk ruchu (tzw. profili ruchowych) i wymagań co do jakości usługi (QoS). Ponadto sklasyfikowano te aplikacje pod względem wymagań transmisyjnych ATM. Listę przykładowych aplikacji wraz z wymaganą przepustowością łącza, jakością usługi, potrzebą sterowania zgłoszeniami i preferowaną kategorią usługi ATM, przedstawiono w tabeli 1.

Wymagania QoS są reprezentowane przez opóźnienie i straty na poziomie komórek i przez prawdopodobieństwo blokady na poziomie wywołań. Tabela 1 pokazuje, że ruch generowany przez sieć LAN w sieci taktycznej nie jest jednorodny. W konsekwencji, część ruchu wymaga wyższych gwarancji (niski poziom strat, małe opóźnienie) niż inne. To wprowadza potrzebę klasyfikacji i oznaczania różnych usług ATM, zależnie od wymagań QoS.

Ocena architektury sieci

Celem zweryfikowania zdolności proponowanej architektury do efektywnej obsługi różnych typów informacji, zbudowano instalację pilotażową systemu w laboratorium Wojskowego Instytutu Łączności. Niżej przedstawiamy wyniki pomiarów dotyczące efektywności obsługi ruchu danych i mowy. Do usługi przekazu mowy była testowana usługa CES (Circuit Emulation Service) dostępna w ATM, podczas gdy dla przekazu danych wymagających zróżnicowania QoS, wykorzystano różne usługi ATM (CBR, VBR i UBR).

Obsługa ruchu danych

Obecnie dostępne usługi ATM do przenoszenia ruchu danych są ograniczone do CBR, VBR i UBR. W rzeczywistości istnieje jeszcze usługa ABR (Available Bit Rate), ale wymaga ona dodatkowych mechanizmów w aplikacjach, które nie są obecnie dostępne (co najmniej w oprogramowaniu komercyjnym). Zakładamy (rys. 3), że usługa CBR będzie dedykowana dla ruchu strumieniowego (sterowanego przez UDP), wymagającego solidnych gwarancji QoS. Ważne wiadomości przekazywane przy użyciu TCP (Transfer Control Protocol) będą przenoszone przez usługę VBR z właściwymi kontraktami ruchowymi dla poszczególnych strumieni danych. Do poszczególnych połączeń będzie gwarantowane minimalne pasmo, wyznaczone na podstawie deklaracji ruchu. Pozostały ruch danych (z minimalnymi wymaganiami QoS) będzie używał usługi UBR.

Tabela 1

TYPY APLIKACJI WRAZ Z WYMAGANIAMI

Aplikacje	Całkowita wymagana przepustowość	Wymagania QoS			Sterowanie zgłoszeniami	Preferowana kategoria usługi
		Poziom komórek		Prawdopodobieństwo blokady wywołań		
		Opóźnienie	Straty			
Mowa z różnymi priorytetami:						
– pilne (1a)	N x 64 (16) kbit/s	niskie	średnie	0	nie wymagane*	CBR (gorąca linia)
– normalne (1b)	N x 64 (16) kbit/s	niskie	średnie	10^{-2}	wymagane**	CBR lub VBR REM
Pilne wiadomości (2)	do 100 kbit/s	średnie	niskie	0	nie wymagane	VBR RSM
E-mail (3)	do 50 kbit/s	wysokie	niskie	0	nie wymagane	VBR RSM
Dane związane ze zdalnym sterowaniem (4)	kilka kbit/s	średnie	niskie	0	nie wymagane	CBR (gorąca linia)
Przekaz pilnych plików (5)	128 kbit/s	średnie	niskie	10^{-2}	wymagane	VBR RSM
Obrazy nieruchome:					nie wymagane	VBR RSM
- pilne (6a)	do 256 kbit/s	średnie	niskie	0		
- normalne (6b)		średnie	średnie	10^{-2}	wymagane	VBR RSM
Dostęp do bazy danych (7)	kilka kbit/s	wysokie	niskie	10^{-2}	wymagane	VBR RSM
Wideo (8) (wideokonferencje)	N × 128 kbit/s	niskie	średnie	10^{-2}	wymagane	CBR lub VBR REM

Uwagi:

* nie wymagane sterowanie zgłoszeniami oznacza, że wywołania powinny być oferowane bez blokady,

** wymagane sterowanie zgłoszeniami oznacza, że pewne wywołania mogą nie być akceptowane ze względu na chwilowy natłok w sieci,

VBR (Variable Bit Rate) – zmienna szybkość bitowa,

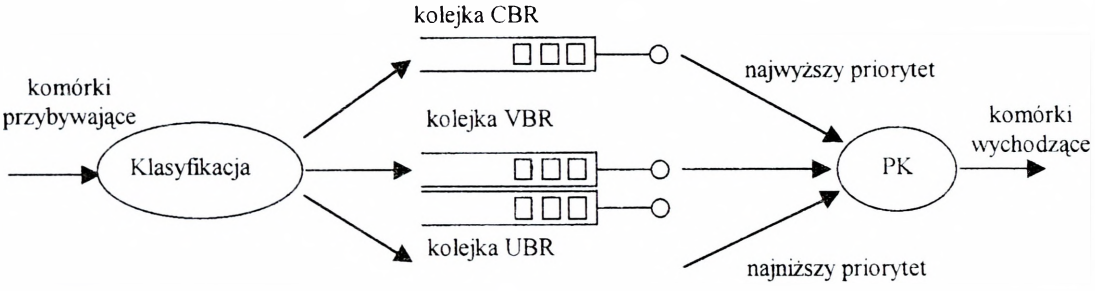
CBR (*Constant Bit Rate*) – stała szybkość bitowa,

REM (*Rate Envelope Multiplexing*) – metoda multipleksacji ATM dla ruchu wymagającego przekazu w czasie rzeczywistym,

RSM (*Rate Sharing Multiplexing*) – metoda multipleksacji ATM dla ruchu nie wymagającego przekazu w czasie rzeczywistym.

Zaimplementowanie rozróżniania QoS dla danych, wymaga zastosowania metody klasyfikacji ruchu danych. Taka klasyfikacja pozwoli na wyselekcjonowanie strumieni wymagających gwarancji QoS i przydzielenie tym strumieniom odpowiedniej usługi ATM gwarantującej rezerwację żądanego pasma. Należy zauważyć, że szybki transfer pilnych wiadomości jest ważniejszy niż przekaz mowy. Do przekazu mowy w ATM jest dedykowana usługa CBR, która zapewnia gwarancję jakości obsługi wymaganą dla mowy. Może to prowadzić do nienormalnej sytuacji, kiedy niepilna mowa jest przesyłana szybciej niż pilne dane.

Po procesie klasyfikacji następnym krokiem jest przydzielenie właściwej kategorii usługi ATM, stosownie do wymagań co do jakości usługi. Celem osiągnięcia powyższego, komórki należące do różnych klas ruchu danych są ustawiane we właściwej kolejce wyjściowej, związanej z daną kategorią usługi, jak to pokazano na rys. 4. Kolejki wyjściowe są opróżniane w zależności od przydzielonego priorytetu – wyższy priorytet jest przydzielany do CBR, średni do VBR, a najniższy do UBR. Ponadto do osiągnięcia minimalnej przepływności połączeń TCP dla korzystających z usługi VBR, zastosowano mechanizm monitorowania szybkości nadawania.



PK – wybieranie priorytetu kolejkowania (powszechnie stosowane w komutatorach ATM)

Rys. 4. Sterowanie komórek danych z różnymi wymaganiami QoS

Testowana konfiguracja sieci jest przedstawiona na rys. 5. Topologia jest typu „bottleneck", z dwoma komutatorami ATM (MARCONI, ASX200BX) połączonymi bezpośrednio przez łącze radioliniowe 2 Mbit/s (E1 ATM), które jest typowe dla sieci taktycznej. Do każdego komutatora ATM dołączono centralę PABX (DGT 3450WW) oraz generator/analizator ruchu ATM (InterWatch 95000).

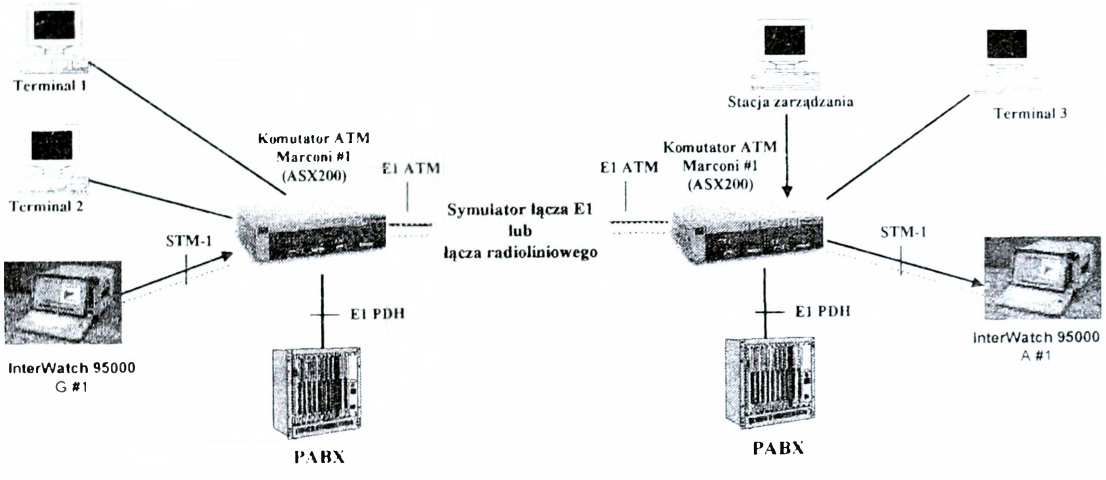
Celem pomiarów było zilustrowanie efektywności rozpatrywanego podejścia do rozróżniania ruchu danych. W eksperymencie przyjęliśmy, że łącze typu „bottleneck" (E1 ATM) przenosi ruch mowy i danych. Ruch mowy wiąże się z usługą CES (ruch generowany pomiędzy parą central PABX), podczas gdy ruch danych jest generowany przez dołączone terminale i generator ruchu. Dla usługi CES było dedykowane 20% przepustowości łącza, wystarczające do ustanowienia maksymalnie pięciu jednoczesnych połączeń głosowych (bez kompresji mowy).

Badany scenariusz zakładał dwa strumienie danych, którymi były:

– strumień #1 generowany przez aplikacje sterowane protokołem UDP z niskimi wymaganiami na straty i opóźnienie. Ten ruch miał stałą szybkość bitową – 64 kbit/s. Mierzonymi parametrami QoS, ilustrującymi jakość przekazu rozważanego ruchu, były: maksymalne opóźnienie przekazu komórek (maxCTD – Cell Transfer Delay), zmienność opóźnienia przekazu komórek (CDV – Cell Delay Variation) i współczynnik strat komórek (CLR – Cell Loss Ratio).

– strumienie #2, #3 i #4 generowane przez identyczne źródła TCP. W tym przypadku parametry QoS są wyrażane ze względu na charakterystyki przepustowości.

Przypadek 1: bez ruchu podkładowego w sieci, przypadek 2: w obecności ruchu podkładowego UBR w sieci.



Rys. 5. Testowana topologia sieci dla eksperymentu przekazu danych

Ten scenariusz zakłada, że:

a. strumień #1 danych jest obsługiwany przez usługę CBR,

b. strumień #2 danych jest obsługiwany przez usługę VBR z gwarantowanym kontraktem 250 kbit/s,

c. strumień #3 danych jest obsługiwany przez usługę VBR z gwarantowanym kontraktem 500 kbit/s,

d. strumień #4 danych jest obsługiwany przez usługę UBR.

Na podstawie wyników pomiarów przedstawionych w tabeli 2, widzimy, iż strumień #1 danych jest obsługiwany bez strat komórek i prawie ze stałym opóźnieniem przekazu komórek, co jest niezmiernie pożądane dla tego typu ruchu. Możemy zatem wnioskować, że używając usługi CBR jesteśmy w stanie obsłużyć ruch danych niemalże w czasie rzeczywistym. W przypadku strumieni #2 i #3 osiągane wartości przepustowości/przepływności są wyższe niż minimalnie gwarantowane (250 kbit/s dla strumienia #2 i 500 kbit/s dla strumienia #3). Oznacza to,

że usługa VBR zabiera większą przepustowość łącza niż zadedykowana. Ta dodatkowa przepływność jest uzyskiwana kosztem z usługi UBR i jest dzielona pomiędzy połączenia VBR proporcjonalnie do deklarowanego kontraktu ruchowego. W konsekwencji strumień #4, który jest obsługiwany przez usługę UBR, osiąga bardzo niską wartość przepływności. Warto nadmienić, że nie jesteśmy w stanie kontrolować tej wartości.

Tabela 2

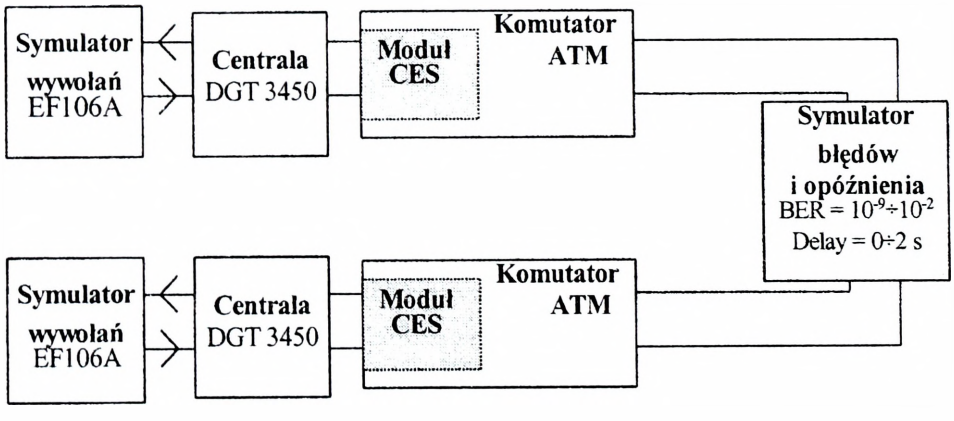
JAKOŚĆ PRZEKAZU DANYCH

przypadek badawczy	strumień danych #2			strumień danych #2		strumień danych #3		strumień danych #4	
	max CTD [ms]	CDV [ms]	CLR [%]	*through put* [kbit/s]	*goodput* [kbit/s]	*through put* [kbit/s]	*goodput* [kbit/s]	*throughput* [kbit/s]	*goodput* [kbit/s]
bez ruchu podkładowego	9.0	7.1	0*	760	748,6	380	373	30	24
z ruchem podkładowym	10.0	7.1	0*	700	684,8	350	341,6	20	19,2

* bez strat komórek

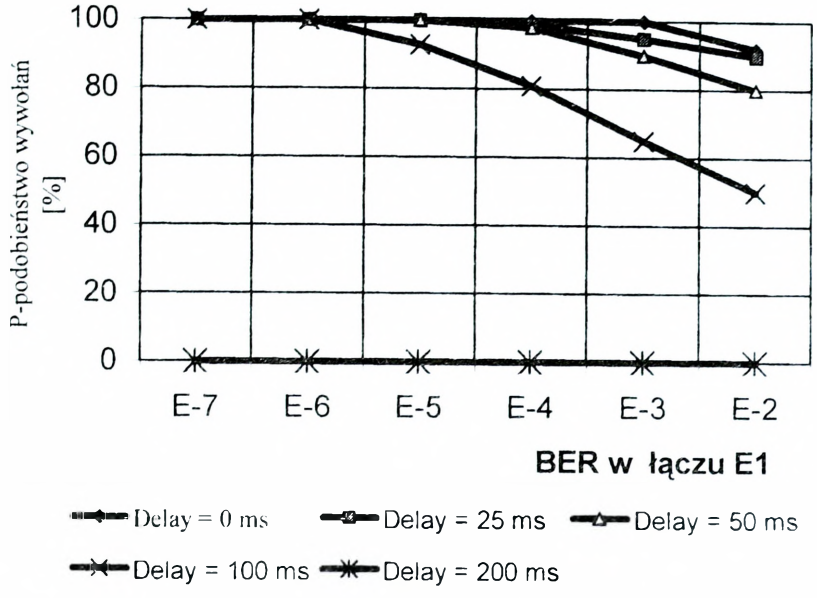
Obsługa ruchu mowy

Poniżej przedstawiamy wyniki pomiarów, pokazujące efektywność wykorzystania usługi CES ATM dla połączeń głosowych. Zmierzono następujące parametry: (1) prawdopodobieństwo blokady oraz (2) subiektywną jakość mowy. Prawdopodobieństwo blokady jest parametrem pokazującym efektywność realizacji połączeń telefonicznych. W przeprowadzonym eksperymencie obciążenie ruchu było stałe i tak dobrane, aby ewentualne odrzucenie wywołania było spowodowane jedynie błędami sygnalizacji.



Rys. 6. Testowana topologia z jednym łączem E1 pomiędzy komutatorami

Scenariusz sieci złożonej z dwóch komutatorów ATM i dwóch central PABX jest pokazany na rys. 6. Połączenie między PABX odbywa się poprzez komutatory ATM, które są połączone przez bezpośrednie łącze radioliniowe 2 Mbit/s. W tym celu zastosowano w komutatorze ATM usługę CES.



Rys. 7. Prawdopodobieństwo pomyślnie zakończonych wywołań w funkcji błędów i opóźnienia

Symulator łącza pozwala wprowadzać błędy bitowe (z różnymi wartościami bitowej stopy błędów – BER) oraz dodatkowe opóźnienie. Symulator wywołań telefonicznych, dołączony do central PABX, był wykorzystywany do generowania wywołań (ruch oferowany) z różnymi profilami ruchowymi. Dodatkowo do central PABX były dołączone telefony, służące do oceny jakości przekazywanej mowy.

Celem przeprowadzonych badań było sprawdzenie wrażliwości usługi CES na błędy bitowe i opóźnienie. Usłudze CES przydzielono w eksperymencie część łącza E1 wynoszącą 5×64 kbit/s. To pozwalało na jednoczesne generowanie przez symulator do pięciu wywołań telefonicznych. Wartości BER były zmieniane w zakresie od 0 do 10^{-2}, a opóźnienia w zakresie od 0 do 200 ms.

Straty komórek były obserwowane, gdy BER = $10^{-5} \div 10^{-2}$. Wpływ opóźnienia był istotny. Zwiększanie opóźnienia powodowało wzrost blokady wywołań. Ten wpływ był spowodowany przez tzw. *time-out*, specyficzny dla protokołu sygnalizacji zaimplementowanego w centralach PABX. W każdym razie, ten wpływ jest niepożądany, ponieważ w łączach satelitarnych można oczekiwać nawet większych wartości opóźnienia.

Podsumowanie

Przedstawiono krótki przegląd obecnie projektowanej sieci łączności dla Wojsk Lotniczych i Obrony Powietrznej. Główną uwagę skierowano na koncepcję mobilnej sieci dostępowej. Zawarte wyniki testów laboratoryjnych potwierdzają oczekiwania. Projektowana sieć może zapewnić efektywną realizację usługi danych i mowy, stosownie do wymagań sieciowych. Warto zauważyć, że szczególnie interesujące jest rozróżnianie jakości usługi dla ruchu danych.

ppłk dr inż. Andrzej Gałecki

Wydział Elektroniki Wojskowej Akademii Technicznej

ROZWIĄZYWANIE PROBLEMÓW DECYZYJNYCH W OKRESIE DEFICYTU INFORMACYJNEGO

Każdemu działaniu towarzyszy zapotrzebowanie na informację, której jakość często decyduje o mniejszych bądź większych możliwościach podejmującego decyzję.

Istnieje wiele definicji informacji, spośród których na uwagę zasługuje między innymi ta, którą określa ją jako [...] *czynnik, dzięki któremu obiekt odbierający go (człowiek, organizm żywy, organizacja, urządzenie automatyczne) może polepszyć swoją znajomość otoczenia i bardziej sprawnie przeprowadzić celowe działanie*[1]. *Inna definicja wskazuje na to, że: informacja to powiadomienie, zakomunikowanie, wiadomość; w socjotechnice – oznacza przekazywanie określonej treści przez nadawcę do odbiorcy za pośrednictwem kanału (środka przekazywania informacji)*. Ze względu na charakter informacji można nadać cechy prawdziwości lub niezgodności z rzeczywistością. W socjotechnice służy ona do wywoływania pożądanych przemian w postawach lub zachowaniach społecznych. W teorii informacyjnej stanowi czynnik, który zmniejsza skalę niewiedzy o danym zjawisku i umożliwia sprawniejsze działanie. Uogólniając, za informację można uznać jakąkolwiek wiadomość o zachodzących zmianach (występujących zdarzeniach), które dotąd nie były dla odbiorcy znane (wiadome).

W węższym sensie pojęcie informacji wiąże się ze środowiskiem, w którym jest ona wykorzystywana, np. informacja o sytuacji powietrznej jest niezbędnym komponentem skutecznego funkcjonowania systemu dowodzenia obrony powietrznej.

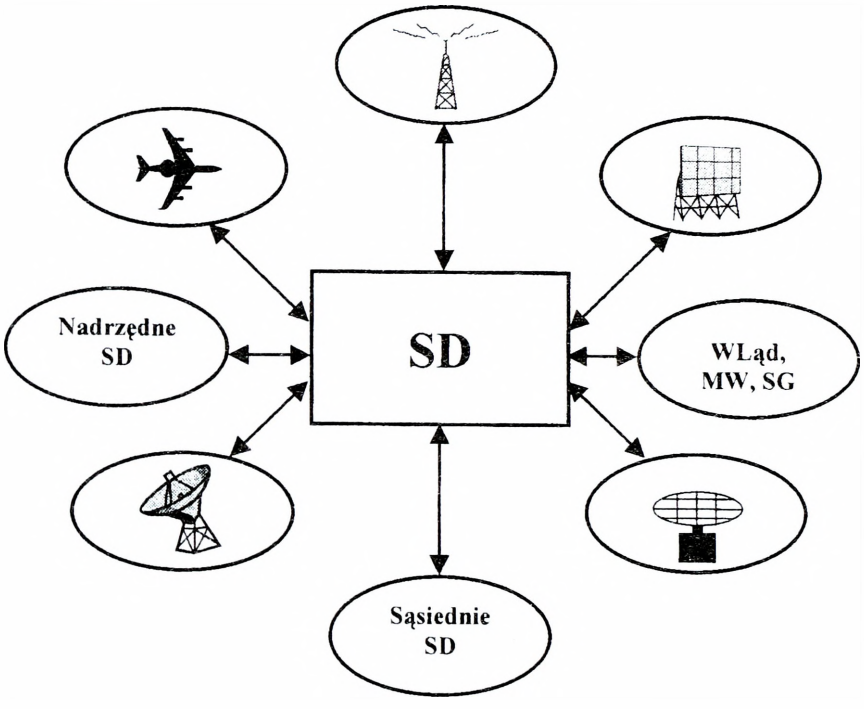
Z kolei informację o sytuacji powietrznej należy rozumieć jako zbiór wiadomości o działalności obiektów powietrznych nad określonym obszarem, przekazywanych adresatom (decydentom) w postaci sformalizowanych treści. Dla dowódcy WLOP stanowi ona podstawę do podjęcia decyzji o użyciu podległych mu sił i środków, dowodzenia nimi w działaniach bojowych oraz wprowadzania wyższych stanów i stopni gotowości bojowej.

---

[1] *Ilustrowany leksykon techniczny*, wyd. 3, WNT, Warszawa 1994.

Dość osobliwy pogląd w tym obszarze reprezentuje P. Lasoń, uznający brak informacji za informację, ponieważ taka sytuacja sprzyja ocenie częstotliwości występowania określonych zdarzeń[2]. Niedocenianie tego faktu może prowadzić do pewnej skłonności przeceniania faktów czy też zdarzeń, a jednocześnie dewaluacji tych, które się nie pojawiły. Tego rodzaju skłonności mogą prowadzić do zagrożenia w wyniku tendencyjnego korzystania z tzw. dostępności informacyjnej, sprzyjającej powstawaniu wielu błędów w interpretacji otrzymywanych informacji.

Trudno jednak wyobrazić sobie działanie np. systemu dowodzenia OP bez informacji o sytuacji powietrznej, o własnych i współdziałających siłach i środkach, której źródła informacji ilustruje rys. 1.



Rys. 1. Źródła informacji o sytuacji powietrznej

Sam problem podejmowania decyzji mimo że jest przedmiotem wieloletnich badań, do dziś zalicza się do najbardziej frapujących zagadnień naukowych, chociażby ze względu na jego rolę w funkcjonowaniu życia człowieka. Informacja odbierana przez różnych ludzi jest często niejednolicie odbierana, zarówno w zakresie jej zapamiętywania (sposobu gromadzenia), jak również reakcji skierowanej na konkretne działanie. Analizując proces decyzyjny, W. Flakiewicz wyróżnił dwa rodzaje percepcji – zmysłową i intuicyjną[3].

---

[2] Por. P. Lasoń, *Rola inklinacji poznawczych w podejmowaniu decyzji konsumenckich*, Politechnika Wrocławska, Wrocław 2000.

[3] Por. W. Flakiewicz, *Informacyjne systemy zarządzania*, PWE, Warszawa 1990.

Według Flakiewicza percepcja zmysłowa dokonuje się wyłącznie za pomocą pięciu zmysłów człowieka, opierając się na faktach, które występują w rzeczywistości.

Percepcja intuicyjna oparta jest na procesach skojarzeniowych, co ma wpływ na postrzeganie nie tylko samych obiektów, ale także ich możliwości. Ma to szczególne znaczenie w procesie podejmowania decyzji w systemie dowodzenia obrony powietrznej, gdzie ocena przeciwnika, jego właściwości i możliwości są niezbędne do podejmowania decyzji. Sama percepcja informacji jest uwarunkowana typami osobowościowymi, będącymi spójnią osądu myślowego i uczuciowego. Manson i Mitroff wyróżnili w ten sposób:

– typ intuicyjny, który koncentruje się na formułowaniu hipotez nie zawsze opartych na dostępnych faktach;

– typ myślący, skierowany zasadniczo na procesy poznawcze, rozważane w obszarze prawdy i fałszu;

– typ zmysłowy, opierający działania na dostępnych informacjach – bez ryzyka ich wyboru;

– typ uczuciowy, skłaniający się do nieuwzględniana racji rozumowych, lecz kierujący się wyłącznie emocjami.

Właściwości percepcyjne odbiorcy informacji są nierozerwalnie związane z jego właściwościami osobowościowymi, które w konsekwencji mogą się przekładać na określone reakcje decyzyjne. Jest to problem o tyle istotny, że błędna ocena dostarczonej informacji, już na wstępnym etapie procesu decyzyjnego, rodzi przypuszczenie, że podjęta decyzja będzie również błędna.

Podejmowanie decyzji można traktować jako transformację informacji wejściowych bądź sytuacyjnych w informację kierującą, decyzyjną (rys. 2).

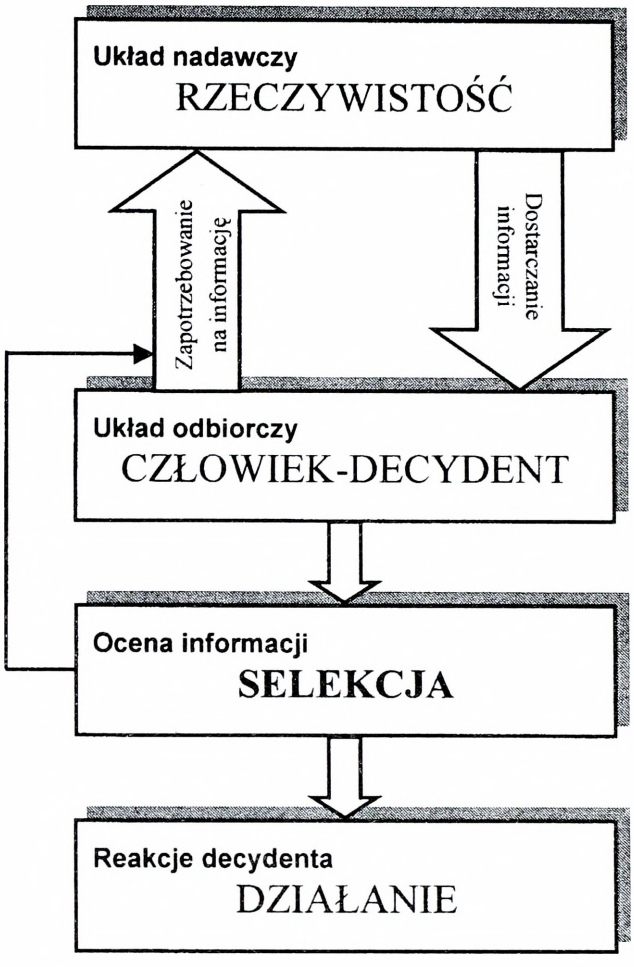
Charakter podejmowanych decyzji umożliwia wyróżnienie:

– decyzji informacyjnych – tzw. oceny jakościowej informacji, czyli podjęcie decyzji o tym „co jest prawdą";

– decyzji operacyjnych, które mają określić „jak działać", aby postawione zadanie wykonać[4].

W przygotowaniu decyzji informacyjnej w systemie OP biorą udział określone osoby funkcyjne stanowisk dowodzenia, do których zadań należy, między innymi zbiór i opracowanie danych o sytuacji powietrznej, w tym także: odrzucanie fałszywych i niewiarygodnych informacji, sprawdzanie wątpliwych, selekcjonowanie najważniejszych oraz konfrontowanie danych aktualnych z poprzednimi. Otrzymane rezultaty analizy sytuacji powietrznej, umożliwiają przygotowanie i opracowanie danych niezbędnych do powzięcia decyzji informacyjnej, na podstawie której jest możliwe sprecyzowanie i podjęcie decyzji operacyjnej.

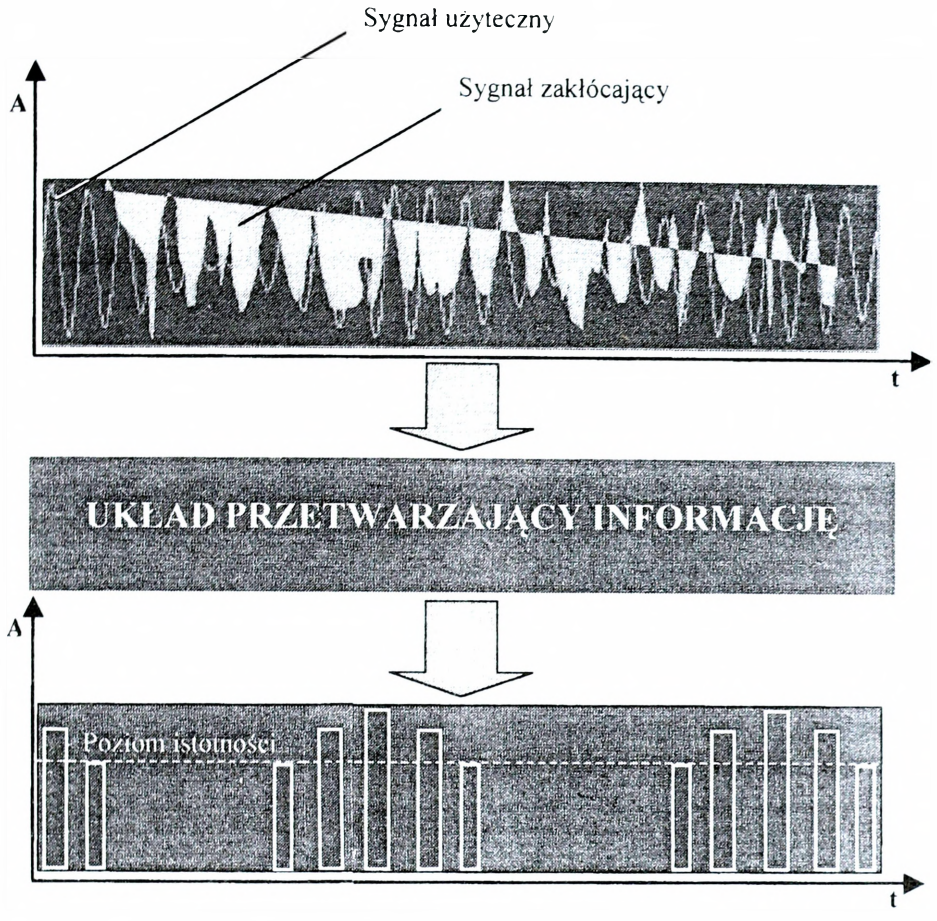
[4] Zob. G. Nakielski, *Wspomaganie procesów decyzyjnych w systemie dowodzenia obroną powietrzną RP*, AON, Warszawa 1997, (rozprawa doktorska).



Rys. 2. Komunikacja informacyjno-decyzyjna

Głównym komponentem informacji o sytuacji powietrznej jest informacja radiolokacyjna, która występuje w postaci pierwotnej oraz wtórnej. Charakteryzujące ją takie parametry, jak: ilość, dokładność, dyskretność oraz czas opóźnienia, określają jej przydatność w systemie dowodzenia obroną powietrzną. Decyzje podejmuje się na podstawie informacji uzyskanych w określonym czasie, którego deficyt często powoduje dezaktualizację sytuacji powietrznej, zobrazowanej na stanowiskach dowodzenia. Czas ten zależy przede wszystkim od technologii obiegu i przetwarzania informacji oraz od szczebla dowodzenia.

Zobrazowana na stanowiskach dowodzenia informacja o sytuacji powietrznej, niejednokrotnie odbiega od rzeczywistej. Przyczyną tego mogą być zakłócenia informacji radiolokacyjnej utrudniające wyselekcjonowanie użytecznego sygnału, sprzyjając tym samym tworzeniu fałszywego obrazu powietrznego. W takich przypadkach konieczne jest wyselekcjonowanie wszelkich zakłóceń, a następnie przetworzenie informacji do takiej postaci, aby była dostępna jej racjonalna ocena (rys. 3).



Rys. 3. Selektywny odbiór informacji

W obszarze podejmowania decyzji można wyróżnić dwa podstawowe stanowiska – matematyczne (racjonalne) oraz psychologiczne (heurystyczne)[5].

Zgodnie z pierwszym charakter procesów decyzyjnych umożliwia pełną ich kwantyfikację i formalizację, natomiast w myśl stanowiska drugiego – procesów tych nie można przedstawić w sposób formalny, gdyż opierają się one na indywidualnych i dynamicznych mechanizmach postępowania, mają charakter adaptacyjny, zaś wybór decyzji jest zawsze subiektywny i obciążony skłonnością do ryzyka.

Jest to podział, który ze względu na istotę funkcjonowania człowieka wiąże się z powstawaniem, tzw. układu samodzielnego, poprzedzonego:

– procesem poznawczym, którego celem jest zdobycie i zarejestrowanie informacji niezbędnych układowi do podjęcia decyzji;

– procesem decyzyjnym, którego celem jest dokonanie wyboru sposobu działania układu[6].

---

[5] Zob. G. Nakielski, op. cit.

[6] Por. J. Kossecki, *Tajniki sterowania ludźmi*, KAW, Warszawa 1984.

Deficyt informacji w procesie decyzyjnym jest, oczywiście, zjawiskiem niepożądanym. Występujące przypadki deficytu informacyjnego (luki informacyjne) bądź też działania dezinformacyjne (zakłóceniowe) nie są czymś odosobnionym na współczesnym polu walki. Dlatego w takich sytuacjach nie należy tylko opierać się na określonych szablonach (regułach) postępowania – konieczne jest skorzystanie z rozwiązań niekonwencjonalnych.

Jednym z takich sposobów jest wykorzystanie intuicji, uważanej za szósty zmysł człowieka. Jest ona tym czynnikiem, który nadaje pewien potencjał twórczy wszelkim działaniom, niekoniecznie decyzyjnym. Wytworzony w umyśle człowieka obraz wizualizacji sprzyja zdolności przewidywania, umożliwiając tym samym (w formie przekonania) odniesienie się do zaistniałego problemu. Takie wyobrażenie jest nieodłącznym atrybutem działania intuicyjnego, odnoszącego się do obrazów wytworzonych w przeszłości, a mogących zaistnieć w chwili obecnej. Patrząc z empirycznego punktu widzenia, wizualizacja jest bardziej logiczna niż wyobraźnia, gdyż wizualizować można coś, co jest już znane lub co już było, natomiast wyobraźnia dopuszcza wszystko, co człowiek może sobie wymyślić. Niestety, istnieje wielu sceptyków stosowania intuicji w procesach decyzyjnych, ponieważ uznają ją za coś mało namacalnego, niewytłumaczalnego zjawiska i dlatego wolą się opierać na jednoznacznie sprawdzonej informacji.

Innym podejściem w okresie deficytu informacyjnego jest kreatywne myślenie, wspierające określone metody poszukiwania pomysłów, których zastosowanie jest pewną szansą rozwiązania trudnych problemów decyzyjnych.

Mówiąc o myśleniu należy mieć na myśli czynność heurystyczną[7], która wprawdzie nie daje gwarancji rozwiązania określonego zadania, jednakże może być jedynym sposobem osiągnięcia sukcesu w sytuacjach złożonych (nieprzewidywalnych), również takich, w których występuje brak zasilania informacyjnego.

Wykorzystując do tego celu prace wielu psychologów (między innymi J. Dewey'a), można przy zastosowaniu reguł heurystycznych wyróżnić kilka głównych faz rozwiązywania problemów[8].

W fazie początkowej jest dostrzegany problem, czyli uświadomienie, że posiadany zasób wiedzy nie wystarcza do osiągnięcia planowanych celów. Psychologowie opracowali różnorodne techniki kształtowania umiejętności dostrzegania problemów. Jedna z nich polega na zapoznaniu ludzi z regułami heurystycznymi, które odgrywają szczególną rolę w tej fazie. Jane Asher sformułował trzy wskazówki ułatwiające odkrywanie problemów[9]. Pierwsza nakazuje wykonać schemat sytuacji (zjawiska, urządzenia), który ułatwia zidentyfikowanie problemu. W schemacie tym należy określić obszar niewiedzy danej sytuacji. Druga wskazówka dotyczy zbadania przebiegu procesu zapoznawania się z daną sytuacją w celu ewentualnego pozbycia się błędnych założeń. Trzecia wskazówka jest związana ze stworzeniem alternatywnej sytuacji, gdyż nowa sytuacja, często zupełnie nierealna, może po-

[7] Zob. K. Piech, *Wprowadzenie do heurystyki*, SGH, Warszawa 1998.
[8] Por. J. Dewey. *Jak myślimy?*, KiW, Warszawa 1987.
[9] Zob. *Psychologia ogólna*, red. T. Tomaszewski, Warszawa 1992.

zwolić dostrzec błędne założenia i wady sytuacji. Po odkryciu problemu następuje przejście do drugiej fazy, czyli do aktywnego badania celu oraz danych początkowych, które są zawarte w sytuacji problemowej. W fazie tej zasadniczą rolę odgrywa myślenie reproduktywne[10].

W sytuacji problemowej są zawarte różnorodne dane początkowe, czyli informacje zakodowane w postaci spostrzeżeń, wyobrażeń i pojęć. Chcąc rozwiązać problem, należy wyodrębnić ważne dane, natomiast nieważne odrzucić. Ważne dane[11] są informacjami, które po wprowadzeniu do bloku pamięci krótkotrwałej, podlegają przetwarzaniu w procesie myślenia. W sytuacjach problemowych istotne dane często są zamaskowane, a w ich wykrywaniu ważną rolę odgrywają czynności interpolacyjne i ekstrapolacyjne. Pierwsze z nich polegają na wypełnianiu luk i przerw w środku bezpośrednio dostępnych układów danych. Czynności ekstrapolacyjne natomiast, umożliwiają odkrywanie brakujących danych końcowych określonego układu.

Kolejnym krokiem w rozwiązaniu problemu jest faza wytwarzania pomysłów, w której są tworzone nowe hipotezy i metody. W tej fazie nie można jednoznacznie zidentyfikować przebiegu heurystycznego łańcucha operacji. Istnieje opracowany przez psychologa niemieckiego K. Dunckera model wytwarzania pomysłów, według którego pomysły rozwiązań powstają stopniowo[12]. W procesie tym można wyróżnić trzy zasadnicze części, zwane też poziomami. W pierwszej części wybierany jest ogólny kierunek poszukiwań rozwiązania, który ogranicza w pewnym sensie rejon poszukiwań i decyduje o dalszym przebiegu procesu wytwarzania pomysłów. Kierunek poszukiwań jest wyznaczony przez reguły heurystyczne. Dla większości problemów istnieje możliwość wyboru spośród wielu kierunków poszukiwań pomysłu rozwiązania. Wybór – lub inaczej mówiąc – odkrycie właściwego kierunku poszukiwań jest kluczową operacją w wytwarzaniu pomysłu, decydującą o powodzeniu w rozwiązywaniu problemów. Zgodnie z wybranym kierunkiem są tworzone pomysły cząstkowe, które stanowią zarys rozwiązania. Pomysł cząstkowy nie jest w pełni określony i sprecyzowany, zawiera luki, które w przyszłości powinny zostać uzupełnione.

W trzecim poziomie powstawania następuje skonstruowanie ostatecznego pomysłu, którego odrzucenie wiąże się z koniecznością stworzenia kolejnych pomysłów cząstkowych oraz pomysłu końcowego. Jeżeli to nie daje pozytywnego rezultatu, trzeba zmienić kierunek poszukiwań. Postępując zgodnie z nowym kierunkiem, ponownie definiuje się różnorodne pomysły cząstkowe i końcowe. W fazie tej dopuszcza się dowolność co do kierunku poszukiwań.

W końcowym etapie procesu rozwiązywania problemów następuje weryfikacja pomysłów, polegająca na ocenie (ewolucji) efektów myślenia w świetle posiadanych informacji. W wyniku tej weryfikacji następuje przyjęcie bądź odrzucenie pomysłu. Wśród metod weryfikacji można wyróżnić weryfikację sukcesywną oraz

---

[10] Por. J. Kozielecki. *Percepcja. Myślenie. Decyzje*, PWN, Warszawa 1992.

[11] O tym, co jest ważne w sytuacji problemowej decyduje cel, jaki należy osiągnąć.

[12] J. Kozielecki, op. cit.

weryfikację jednoczesną. Pierwsza z nich polega na wysuwaniu pomysłu wraz z jednoczesną jego weryfikacją. Jeśli jego ocena da wynik negatywny, to jest tworzony następny pomysł, który ponownie podlega weryfikacji. Proces weryfikacji trwa tak długo, aż jeden z pomysłów zostanie zaakceptowany jako ostateczne rozwiązanie.

Złożoność sytuacji współczesnego pola walki, charakteryzująca się dużą dynamiką działań bojowych, niekompletną informacją, (niejednokrotnie dezinformacją) wpływa na jakość procesu podejmowania decyzji operacyjnej, którego realizacja w tak ekstremalnych warunkach jest zadaniem bardzo trudnym.

Informacja zawsze stanowiła podstawowy komponent zasilania procesu, dlatego jej brak powinien dopingować do nowych rozwiązań idących w kierunku rozwiązywania złożonych problemów decyzyjnych. Do tego celu na stanowiska dowodzenia systemu OP powinny być przygotowane osoby o szczególnych predyspozycjach psychofizycznych, potrafiące wykorzystać własne zasoby intelektualne, intuicyjne oraz specjalistyczne, umożliwiające inicjowanie twórczych procesów.

Wydaje się, że wykorzystanie intuicji oraz reguł heurystycznych w sytuacjach, gdy występują działania dezinformacyjne lub luki informacyjne jest często jedyną rozsądną drogą postępowania w procesie decyzyjnym. Stąd spopularyzowanie takiego podejścia powinno przynieść korzystne rozwiązania odnośnie do skuteczności działania systemu dowodzenia obrony powietrznej.

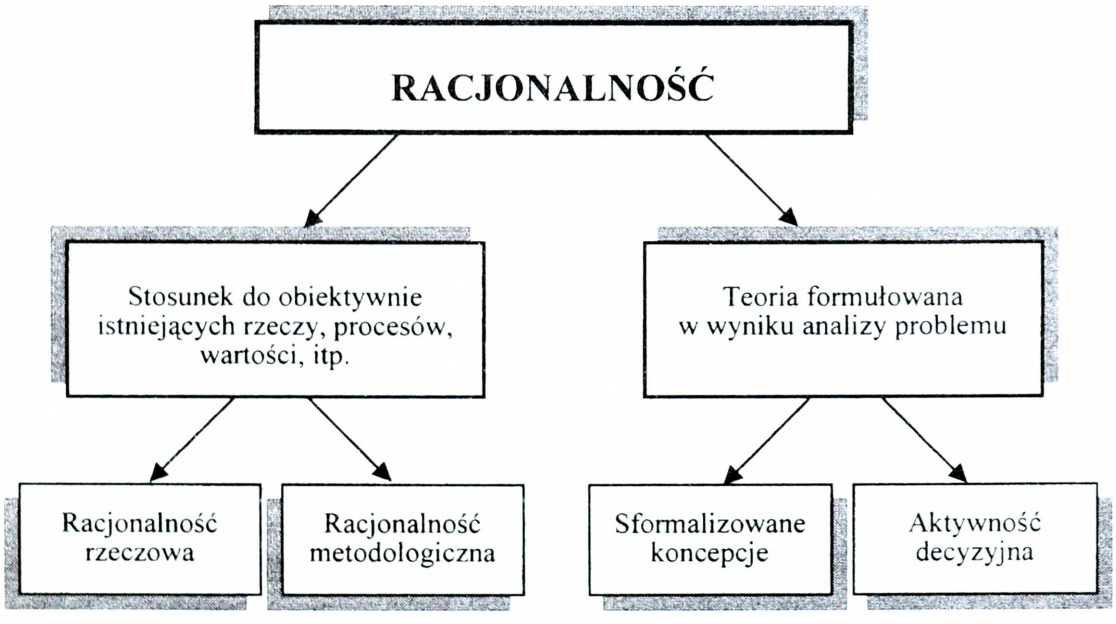
ppłk dr inż. Andrzej Gałecki

Wydział Elektroniki Wojskowej Akademii Technicznej

PROBLEMY RACJONALNEGO PODEJMOWANIA DECYZJI

Jedną z najważniejszych czynności ludzkich jest podejmowanie decyzji. Podejmowanie decyzji jest wysoce skomplikowanym procesem myślowym, którego jakość w głównej mierze zależy od trzech komponentów: sprawnego myślenia, predyspozycji decydenta oraz jego otoczenia.

Spośród istotniejszych określeń jakości podejmowanych decyzji, wyróżnia się pojęcie racjonalności. W teorii decyzji racjonalnych, racjonalność jest rozpatrywana w dwóch podstawowych obszarach (rys. 1):



Rys. 1. Dwuobszarowy podział racjonalności podejmowania decyzji

– w pierwszym wyróżnia się stosunek do konkretnego działania czy wyboru do rzeczywistości;

– w drugim mamy do czynienia z rodzajem teorii formułowanej w wyniku analizy problemu[1].

Występująca w pierwszym obszarze racjonalność rzeczowa ma miejsce wtedy, gdy dobór środków jest odpowiedni w stosunku do istniejącej sytuacji. W takim przypadku występuje równowaga rzeczowej racjonalności ze skutecznością. Tadeusz Kotarbiński uważa, że *„działanie będzie bardziej racjonalne w rozumieniu rzeczowym, jeżeli jest ono przystosowane do okoliczności i w ogóle do wszystkiego, cokolwiek w sądzie prawdziwym stwierdzić można"*[2].

Natomiast gdy działaniu towarzyszy racjonalny, z punktu widzenia posiadanej przez decydenta wiedzy, wybór środków, to wtedy mamy do czynienia z racjonalnością metodologiczną. Inaczej mówiąc, racjonalne działanie pod względem metodologicznym to takie działanie, w którym decydent postępuje zgodnie z posiadaną wiedzą. W praktyce wojskowej racjonalność metodologiczna sprowadza się do określonego wyboru (wariantu) działania.

Występująca w drugim obszarze koncepcja podejmowania decyzji opiera się na teorii wyboru (język matematyki, statystyki, logiki formalnej), w której rezultacie możliwe jest określenie przyszłego działania. Drugi element tego obszaru dotyczy samej aktywności decyzyjnej, która jest nazywana podejmowaniem decyzji lub rozwiązywaniem problemów[3].

Niezależnie od szczegółowości rozważań można na wstępie stwierdzić, że określenie warunków, jakie muszą być spełnione, aby decyzje były racjonalne jest niezmiernie trudne. Uzasadnienie powyższego wynika zasadniczo ze specyfiki procesu decyzyjnego, istniejących różnorodnych ograniczeń racjonalnego podejmowania decyzji, a także z predyspozycji decydenta.

W takim razie nasuwa się pytanie: jakiego decydenta można uznać za racjonalnie podejmującego decyzję? Za Edwardem Nowakiem: „[...] *decydent racjonalny, to człowiek analizujący zgodnie z zasadami logiki wszystkie możliwe warianty działania i umiejący wybrać najlepszy z nich, a przy tym, co dla wojskowych decydentów jest szczególnie ważne, to jak działać »z zimną krwią« również w sytuacjach stresowych, ekstremalnych, w sytuacjach pola walki*[4]. Według Wacława Gabary: *racjonalnie zachowuje się ten, kto w swym działaniu powściąga emocje, odrzuca podszepty i utarte schematy, kieruje się natomiast własnym doświadczeniem oraz wiedzą, jaką mu daje faktyczne uczestnictwo w społeczeństwie*"[5].

Rosnąca złożoność procesów decyzyjnych, związana z występowaniem wielu sytuacji trudno przewidywalnych, bezpośrednio wpływa na potencjał zdolności decydentów do formułowania racjonalnych decyzji, zwiększając tym samym margines popełniania błędów. Mogą one wynikać z niedokładnej informacji (lub cał-

---

[1] Por. S. Antczak, K. Koliński, *Dowodzenie siłami powietrznymi*, AON, Warszawa 2001.

[2] T. Kotarbiński, *Traktat o dobrej robocie*, wyd. 3, Ossolineum, Wrocław–Warszawa–Kraków 1965.

[3] Por. S. Antczak, K. Koliński, op. cit.

[4] E. Nowak, *Decydowanie istotą dowodzenia*, AON, Warszawa 1992.

[5] W. Gabara, *Przesłanki racjonalnego zarządzania*, KiW, Warszawa 1993, s. 31.

kowitego jej braku w określonej chwili), presji przełożonych, braku motywacji, predyspozycji psychofizycznych decydenta itp. Szczególnie ostatni z wymienionych czynników zasługuje na uwagę, występujące bowiem w procesach decyzyjnych psychologiczne bariery bardzo utrudniają racjonalne podejmowanie decyzji. Józef Penc[6] wyróżnił z tego tytułu szereg słabości decydenta, a mianowicie:

– odprężone unikanie – występujący brak aktywności decydowania jest konsekwencją oceny, że przewidywane skutki braku działania nie będą poważne;

– odprężona zmiana – powierzchowna (mało wnikliwa) analiza sprowadza się do wyboru pierwszej możliwości, stwarzającej pozornie warunki niewielkiego ryzyka;

– defensywne unikanie – trudności w rozwiązaniu problemu skłaniają decydenta do odłożenia go na później lub wyboru rozwiązania najbardziej oczywistego;

– panika – brak realistycznej oceny sytuacji, a także następstw ewentualnego wyboru, spowodowany obawą narażenia się na krytykę bądź konsekwencje decyzji;

– stosowanie reguły dominacji – preferowanie wcześniej wybranej możliwości rozwiązania problemu, w której upatruje się jedynie zalety, pomijając istniejące wady;

– dodatni obraz samego siebie – preferowanie sprawdzonych w przeszłości rozwiązań w celu przedstawienia korzystnego obrazu własnych możliwości, utwierdzają w osiągniętym poczuciu siły i pewności siebie.

– uprzedzenia – złe nastawienie do danego problemu może powodować zwłokę w podejmowaniu decyzji, z nadzieją, że w międzyczasie problem sam się rozwiąże bądź wyjaśni;

– nadmiar logiki – dążenia do racjonalnych przesłanek i otrzymania dokładnych informacji, pozbawiają decydenta, między innymi twórczego podejścia do problemu;

– niski stopień tolerancji niepewności – mała skłonność do ryzyka i do zmian, działania zachowawcze;

– ograniczona racjonalność – oznacza, że podejmujący decyzję posługując się, między innymi systemem swych wartości i umiejętności, skłania się w kierunku poszukiwania rozwiązań do czasu, aż osiągnie założony wymóg wystarczalności;

– emocje i stres – na skutek występowania ujemnych emocji powstaje distres, powodujący liczne zaburzenia i dolegliwości psychosomatyczne, utrudnienia logicznego myślenia i podejmowania decyzji.

Powszechnie wiadomo, że informacja stanowi podstawowy komponent wszelkich systemów zarządzania, dowodzenia itp. Istniejące luki informacyjne są częstą przyczyną podejmowania decyzji ryzykownych, których skutki nie są do końca przewidywalne. Stąd w warunkach tzw. niepewności zasadniczymi argumentami decyzyjnymi są doświadczenie oraz intuicja. Zdarzają się sytuacje, w których działania instynktowne są zawodne, skłaniając decydenta do korzystania z tzw. dostępności informacji[7]. Takie działanie często bywa zgubne, wprowadzając decydenta w swoistą pułapkę informacyjną. Jednym z przykładów dostępności zakłóca-

---

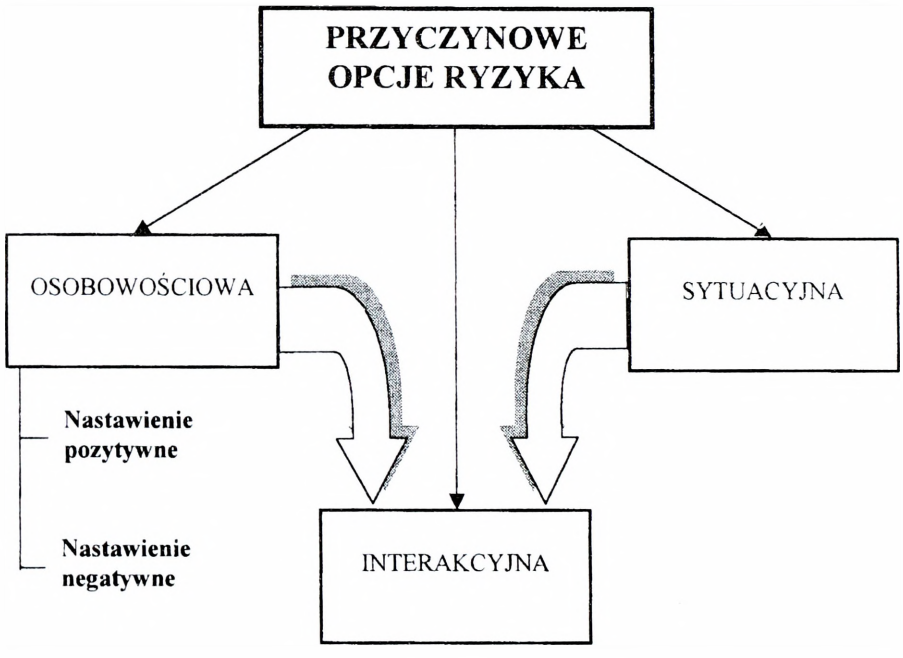
[6] Zob. J. Penc, *Zarządzanie dla przyszłości*, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 1998.

[7] Zob. A. Leight, *Doskonałe podejmowanie decyzji*, Dom Wydawniczy Rebis, Poznań 1999.

nej w procesie podejmowania decyzji jest konserwatyzm poglądów, który nie pozwala odrzucić myśli, że jest się w błędzie. Powodem tego może być chęć korzystania z najwygodniejszych dostępnych informacji, umożliwiających łatwiejsze podejście do zaistniałego problemu. Znamienne jest tu określenie Michała Zielińskiego: *„iluzją jest racjonalny wybór zależny od w pełni dostępnych, kompletnych informacji. Na naszą decyzję bardzo silnie wpływa bowiem sposób, w jaki owe informacje zostaną podane"*[8]. Stąd w procesie decyzyjnym dostępność informacyjna powinna być traktowana z określonym dystansem, chociażby dlatego, aby na jej podstawie uniknąć powierzchownej oceny sytuacji.

Wiarygodność i dostępność informacji zawsze decydowała o potencjale niepewności, a w konsekwencji o ryzyku stanowiącym nieodłączny element funkcjonowania człowieka w procesie podejmowania decyzji. Z punktu widzenia przyczynowego, ryzyko można określić w trzech opcjach (rys. 2):

– osobowościowej;
– sytuacyjnej;
– interakcyjnej[9].



Rys. 2. Opcje ryzyka

[8] M. Zieliński, *Chłopak z Chicago i nasze wybory*, „Rzeczpospolita" z 20 października 2000 r.
[9] *Psychologia w wojsku*, red. nauk. M. J. Dyrda, MON, Warszawa 1997.

W pierwszej z nich zaakcentowano wątek psychicznej natury człowieka, z dwoma określonymi sposobami podejścia do ryzyka:

1) niezależnie od zaistniałych trudnych (skomplikowanych) problemów czy też sytuacji odznaczających się potencjalnym zagrożeniem osiągnięcia niepowodzenia, obserwuje się pozytywne nastawienie. Takie podejście można wyrazić stwierdzeniem: „jest źle, ale nie beznadziejnie";

2) odznaczające się negatywnym nastawieniem do rozwiązywania problemów o charakterze trudnym, w otoczeniu niepewności. Można by tego rodzaju podejście porównać z pesymistycznym określeniem: „stoję z góry na straconej pozycji".

Osoby będące pozytywnie nastawione do tak zwanych sytuacji trudnych, wymagających podejmowania ryzyka, niekonwencjonalnego myślenia cechują się twórczym podejściem do rozwiązywania wszelkich problemów. Według Mirosława Dyrdy można stwierdzić, że „*znamienitą ich właściwością jest odważne i rozważne działanie*"[10]. Z pewnością pewnego rodzaju ideałem byłoby, gdyby wszyscy decydenci odznaczali się wspomnianym pozytywnym nastawieniem.

Niewybaczalnym błędem byłoby bezkrytyczne odniesienie się do podejścia osób z negatywnym nastawieniem. Otóż, osoby prezentujące takie podejście cechują się nadmierną asekuracyjnością, preferencją konserwatywno-dogmatycznych wartości. W procesie decyzyjnym opierają się (zgodnie ze wcześniejszym określeniem) na dostępności informacji. Przyczyną stosowania działań asekuracyjnych może być, między innymi obawa, np. o potencjalnie poniesione straty, a także obawa o narażenie prestiżu własnej osoby. Taka postawa jest szczególnie niepożądana.

Opcja sytuacyjna określa ryzyko szczególną właściwością otoczenia, w którym znajduje się człowiek. Otoczenie to należy rozumieć w szerszym sensie jako uwarunkowania sytuacyjno-zadaniowe, wraz bezpośrednim środowiskiem jego funkcjonowania. Występuje tutaj bardzo silne powiązanie stopnia zagrożenia, stopnia złożoności sytuacji, ograniczenia czasowego oraz potencjału podejmowanego ryzyka. Taki wyróżnik wyraźnie implikuje zjawisko stresu.

W trzeciej, przyczynowej, opcji ryzyka obserwuje się pewnego rodzaju kompromis, stanowiący kombinację dwóch poprzednich. Praktycznie sprowadza się to do spostrzegania ryzyka zależnego od interakcji cech osobowościowych człowieka podejmującego decyzję oraz sytuacji, w której on funkcjonuje.

Niezbędnym komponentem procesu decyzyjnego jest zasilanie informacyjne, bez którego wybór (najlepszego rozwiązania) zawsze będzie mocno ograniczony. Wybór działania w sytuacjach niepełnej (ograniczonej) wiedzy informacyjnej lub jej całkowitym braku, często sprowadza się do decyzji o charakterze intuicyjnym. W takich sytuacjach trudno przewidzieć rezultat podjętych przez człowieka decyzji, a negatywne skutki jej podjęcia mogą znacząco obniżyć pewność jego dalszego działania.

Mimo wielkiego postępu współczesnej cywilizacji, liczba utrudnień ograniczających racjonalne podejmowanie decyzji nie maleje, a wręcz przeciwnie – rośnie. Taki stan rzeczy jest spowodowany, między innymi wzrostem złożoności oraz

[10] Ibidem, s. 77.

dynamiki działań bojowych współczesnego pola walki. To wszystko sprzyja wzrostowi emocji w procesie podejmowania decyzji.

Przyjmując za miarę racjonalności efektywność działania, można stwierdzić, że decyzje racjonalne powinny zawierać czynnik emocjonalny[11], którego we współczesnych działaniach bojowych nie brakuje. Jednocześnie należy pamiętać, że długotrwałe występowanie napięć psychicznych może być przyczyną powstania stresu, który znacznie ogranicza podejmowanie racjonalnych decyzji.

[11] Wprawdzie uważa się, że skrajne natężenie emocji może wprawdzie zakłócić procesy poznawcze, ale również ich całkowity brak może obniżyć efektywność myślenia. P. Lasoń, *Rola indykacji poznawczych w podejmowaniu decyzji konsumenckich*, PW, Wrocław 2000.

mjr dr inż. Zbigniew Skwarek

Adiunkt Katedry Obrony Powietrznej Wydziału Lotnictwa i OP AON

ZDOBYWANIE INFORMACJI W OBRONIE POWIETRZNEJ

Ciągły rozwój środków walki, jakimi posługuje się człowiek, już od stuleci powoduje, że proces ten nie jest i nie będzie zakończony. Dotyczy to wszystkich dziedzin, które są opanowane technologicznie i uznawane przez człowieka za użyteczne i skuteczne w jego realnej walce lub też w trakcie przygotowywania się do niej. Aby jak najlepiej przygotować się do przyszłych działań, zawsze badano wszelkie aspekty i sposoby użycia systemów walki oraz kierunki ich rozwoju. Do tych systemów – może nie bezpośrednio oddziaływających ogniowo, natomiast bardziej wspomagającym inne – są zaliczane systemy zdobywania informacji. Ich decydującej roli nie da się pominąć we współczesnych działaniach bojowych, a przede wszystkim w obronie powietrznej.

Rozwój sił i środków biorących udział w obronie powietrznej, podobnie zresztą jak rozwój każdej organizacji, obejmuje: racjonalizację procesów informacyjno-decyzyjnych, tworzenie nowych źródeł informacji oraz środków jej zdobywania, przechowywania, przetwarzania i przekazywania.

Podejmowanie decyzji – zwiększenie jej trafności i operatywności – zależy w dużej mierze od liczby i jakości informacji, jakimi dysponują organy decyzyjne. Wyrazem potrzeb informacyjnych jest zjawisko popytu informacyjnego, związanego z tendencją do zlikwidowania (minimalizowania), tzw. luki informacyjnej[1]. Istnienie jej jest przyczyną powstania każdego systemu informacyjnego. W obronie powietrznej decydujące znaczenie ma dostarczenie do organów decyzyjnych określonych wiadomości o różnorodnych czynnikach kształtujących sytuację panującą w przestrzeni powietrznej na podejściach do granicy państwa. Popyt na te wiadomości, będący wyrazem potrzeb obrony powietrznej, spowodował tworzenie różnorodnych systemów zdobywania informacji opartego na środkach rozpoznania radiolokacyjnego i radioelektronicznego, rozmieszczonych w powietrzu, kosmosie, na ziemi i na wodzie.

Według teorii informacji każdy sygnał zmniejszający stopień nieznajomości (nieokreśloności) interesującego zjawiska, umożliwiający człowiekowi sprawniej-

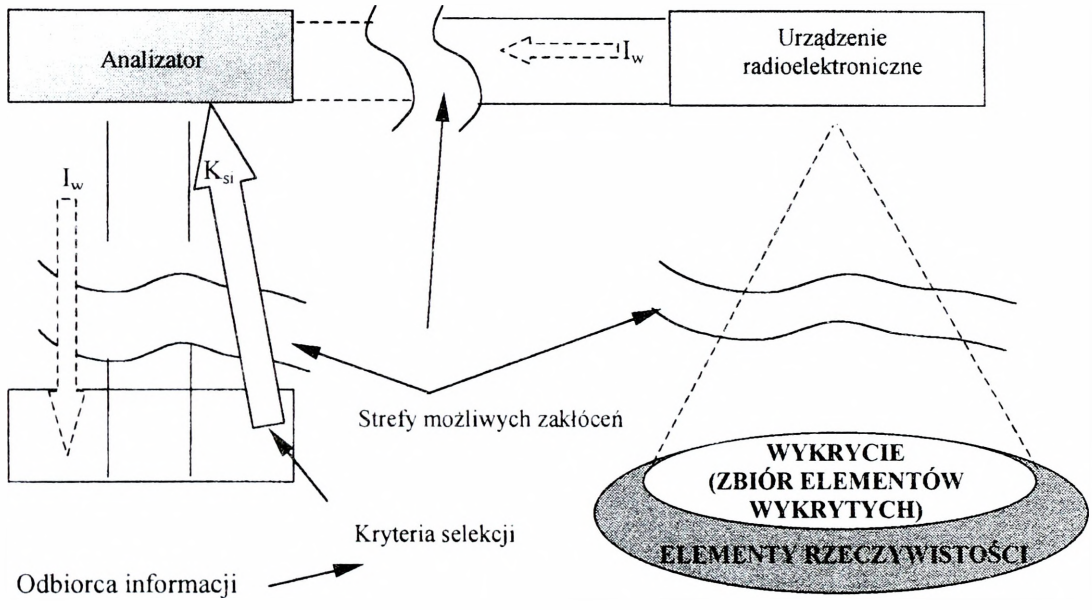
[1] M. Mazur, *Jakościowa teoria informacji*, Warszawa 1970.

szą realizację określonej celowej działalności, jest informacją[2]. Ponieważ wiadomości o obiektach znajdujących się w przestrzeni powietrznej zmniejszają stopień nieznajomości sytuacji panującej w tej przestrzeni, stanowią one informacje o sytuacji powietrznej. Informacje te są wykorzystywane przy podejmowaniu decyzji w co do użycia aktywnych środków walki obrony powietrznej oraz powiadamiania o zagrożeniu ze strony środków napadu powietrznego.

Popyt na informacje o sytuacji powietrznej, będący wyrazem potrzeb obrony powietrznej, powinien powodować doskonalenie systemów zdobywania informacji. Jednym z podstawowych zadań tych systemów jest informowanie, czyli zbiór wiadomości ze źródła i przekazanie ich do obiektu przeznaczenia oraz powiadamianie o istniejących zagrożeniach ze strony środków napadu powietrznego.

Zdobywanie informacji, jako proces, powinno obejmować swym zakresem znaczeniowym procesy wykrywań (ujawnienia) i identyfikowania.

Proces zdobywania informacji ilustruje jego model (rys. 1).



Rys. 1. Model procesu zdobywania informacji

Proces zdobywania informacji prowadzony przez urządzenie radioelektroniczne polega na zdobywaniu informacji o zbiorze elementów wykrytych (I_w), należących do zbioru elementów rzeczywistości. Charakter informacji o elementach wykrytych od specyficznych cech środka radioelektronicznego, zdeterminowanych jego możliwościami. Jest on w stanie wykryć tylko te elementy rzeczywistości, które mieszczą się w jego zasięgu i które wyróżniają się z tła wystarczającym sygnałem bądź wielkością.

[2] Por. *Encyklopedia techniki wojskowej*, MON, Warszawa 1987.

Możliwości w tym zakresie wynikają głównie z rozwiązań technicznych urządzenia. Informacja (I_w) jest przekazywana do analizatora, który dokonuje jej wyboru na podstawie określanych przez odbiorcę informacji kryteriów (K_{si}) Tak wyselekcjonowaną informację analizator przekazuje odbiorcy. Na tym etapie procesu zdobywania informacji w grę wchodzą czynniki dotyczące możliwości taktycznych, taktyczno-operacyjnych i strategicznych przeciwnika.

Za kryteria selekcji często się przyjmuje: zadany przez użytkownika zbiór parametrów procesu zdobywania informacji. W niektórych przypadkach analizator steruje czynnościami środka radioelektronicznego, ograniczając je do możliwości wykrywania elementów rzeczywistości ściśle odpowiadających kryteriom selekcji.

Możliwe jest również połączenie funkcji wszystkich trzech podmiotów wykrywania w jednym. Sformalizowany zapis wykrywania i identyfikacji przedstawia następująca zależność matematyczna:

$$P(AB) = P(A) \times P(B\backslash A)$$

gdzie:
A – wykrycie;
B – zidentyfikowanie.

Zależność ta opisuje **prawdopodobieństwa jednoczesnego** wystąpienia zdarzeń A i B, które zawsze są równe iloczynowi prawdopodobieństwa wystąpienia zdarzenia A (**wykrycie**) i prawdopodobieństwa wystąpienia zdarzenia B (**zidentyfikowanie**), przy założeniu, że A wystąpiło. Stąd, gdy P(A)=0, także P(AB)=0, czyli P(A) musi być większe od 0.

Warunkiem koniecznym do wystąpienia zdarzenia B (zidentyfikowanie) z określonym prawdopodobieństwem, jest prawdopodobne wystąpienie zdarzenia A (wykrycie).

Stąd: **Warunkiem niezbędnie koniecznym do identyfikacji jest wykrycie**.

Inaczej: **Nie ma identyfikacji bez wykrycia**.

Rozwiązywanie problemu zdobywania informacji wymaga sprecyzowania sposobu rozumienia terminu „identyfikacja". Ta zaś w wydawnictwach leksykalnych jest definiowana następująco:

„*Identyfikacja* [łac.], *ustalenie tożsamości badanego obiektu lub zjawiska na podstawie jego najbardziej charakterystycznych cech*[...]"[3].

Słownik podstawowych terminów wojskowych podaje definicję identyfikacji obiektów powietrznych jako: „*ustalenie przynależności samolotów i bezpilotowych środków napadu powietrznego do danego państwa i jego sił zbrojnych*".

Również *Leksykon wiedzy wojskowej* przedstawia definicję identyfikacji obiektów powietrznych, która brzmi: „*Identyfikacja obiektów powietrznych – zespół czynności mających na celu ustalenie przynależności państwowej wykrytego obiektu powietrznego*".

---

[3] *Encyklopedia powszechna*, PWN, Warszawa 1974, s. 256.

Przytoczone definicje zawierają nieścisłości. Odnoszą się jedynie do ustalenia przynależności państwowej obiektów powietrznych przy użyciu specjalistycznych środków jej rozpoznania (identyfication „friend or foe" – IFF). Identyfikacja obiektów powietrznych powinna umożliwić ustalenie przynależności państwowej, określenie składu i ugrupowania wykrytych obiektów powietrznych, a na podstawie analizy informacji o tych obiektach powietrznych również ich typu i przeznaczenia taktycznego.

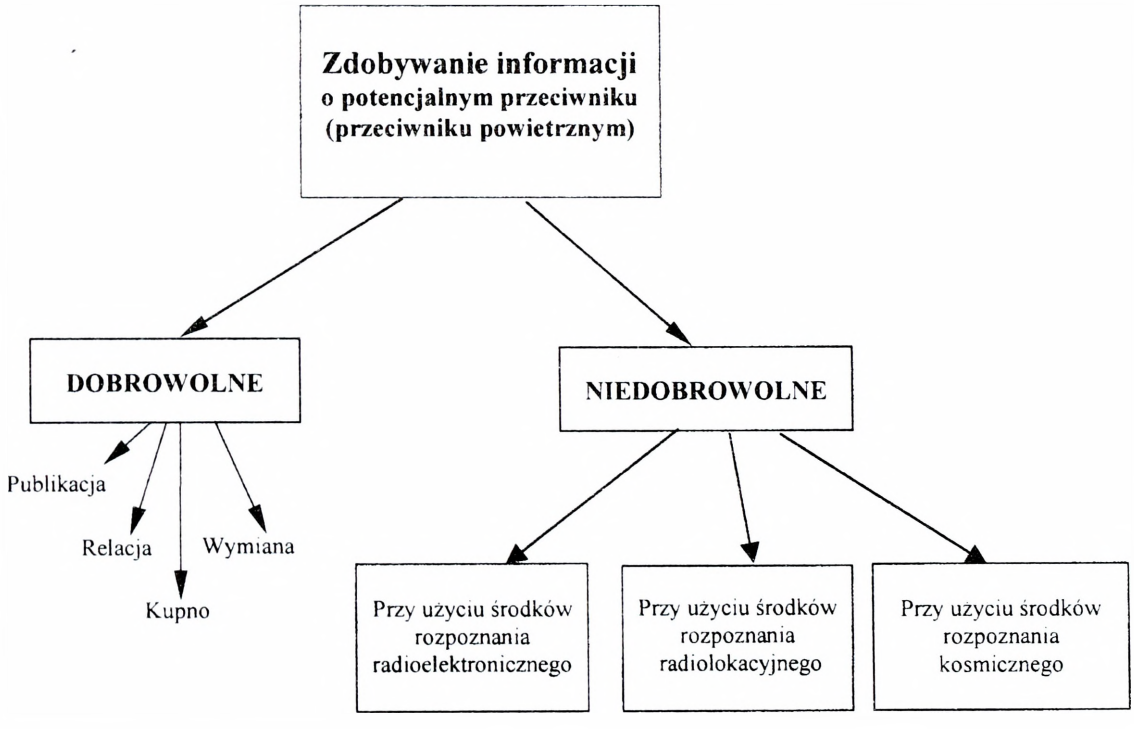
„Zdobyć informację – znaczy dowiedzieć się czegoś, czego się nie wiedziało przedtem lub dowiedzieć się czegoś więcej o tym, o czym wiedziało się mniej"[4].

W celu realizacji tej potrzeby niezbędna jest wymiana informacji prowadzona przez ludzi między sobą. Przekaz informacji zachodzi pomiędzy minimum dwoma podmiotami i może nastąpić w trybie:

a) pośrednim – gdy informacja zostaje powielona w całości lub w części i przekazaniu podlega oryginał lub kopia;

b) bezpośrednim – gdy informacja zmienia właściciela w całości lub w części.

Oba tryby zdobywania informacji mogą mieć charakter dobrowolny lub niedobrowolny.



Rys. 2. Zdobywanie informacji o przeciwniku powietrznym

[4] *Filozoficzny zarys cybernetyki*, KiW..., Warszawa, s. 71.

Formami dobrowolnymi zdobywania informacji są[5]: publikacja, relacja, kupno i wymiana – najczęściej przeprowadzane w trybie pośrednim. Taka forma zdobywania informacji jest wynikiem zgodnego co do celu oddziaływania obu podmiotów aktu przekazywania, nie wywołuje więc kontrakcji ze strony żadnego z nich.

Formy niedobrowolne to zdobywanie informacji przy użyciu środków rozpoznania radioelektronicznego, radiolokacyjnego i kosmicznego. Można tutaj również wyróżnić zdobywanie informacji agenturalnej. Takie postępowanie jest wynikiem sprzecznego co do celu działania obu podmiotów. Jeden z nich (posiadacz informacji) dąży do samodzielnego jej posiadania, drugi zaś może dążyć do jej pozyskania. Oznacza to, że ewentualny przeciwnik, odpowiednio oddziałujący na środki systemu wczesnego wykrywania, będzie dążył do zniekształcenia informacji, umożliwiającej jej właściwą interpretację.

Pojęcie „informacja" występuje jako jeden z podstawowych terminów we współczesnej filozofii oraz praktyce sterowania systemami, w tym również systemami technicznymi. Mimo że pojęcia „informacja" używa się we wszystkich dziedzinach nauki, jest ono różnie definiowane. Na ogół autorzy zadowalają się mniej lub bardziej wyczerpującym objaśnieniem aspektów informacji, które ich szczególnie interesują w związku z prowadzonymi badaniami.

Informacja jest zbiorem otwartym sądów ogólnych o wybranym obszarze rzeczywistości. Jako taka nie posiada samoistnego bytu; „[...] *informacja nie jest ani materią, ani energią*[...]"[6]. Gdyby było inaczej, to zachowywałaby się zgodnie z podstawowym prawem zachowania materii (masy, energii). Tymczasem, wiele osób może zdobywać informacje czytając, np. książkę, a mimo to pozostanie w niej nie zmieniona liczba informacji, nic z niej nie ubędzie. Informacja generowana przez człowieka w postaci sądów o faktach rzeczywistych obejmuje obszar rzeczywistości subiektywnie przez niego dobierany lub możliwy do zinterpretowania przez niego; „[...] *informacja jest nazwą treści zaczerpniętej ze świata zewnętrznego*[...]"[7].

Sądy, aby przekazano je innym ludziom, muszą mieć postać materialną. Przyjmują więc różne formy od werbalnych (nietrwałych), poprzez różnorodne formy fizyczne (np.: sygnał radiolokacyjny, kod cyfrowy) po formy trwałe (zmaterializowane), takie jak obraz, książka itp.

H. Greniewski, analizując pojęcie informacji, stwierdza, że w sensie potocznym jest ona zwykle rozumiana następująco:[8]

– każda informacja jest wiadomością o czymś;
– informację uzyskuje tylko człowiek przez obserwację lub czynność umysłową;
– informację przekazuje tylko człowiek człowiekowi.

S. Koziej określa informację jako niematerialny czynnik zespalający pozostałe czynniki walki zbrojnej w zharmonizowaną całość starcia zbrojnego[9].

---

[5] Por. A. Szydłowski, *Zarys teorii przeciwrozpoznania*, WAT, Warszawa 1997, s.10.
[6] N. Weiner, *Kibernetika*, „Sowietskoje Radio" 1958, s. 166.
[7] Ibidem *Cybernetyka i społeczeństwo*, KIW 1960, s. 16.
[8] H. Greniewski, *Cybernetyka niematematyczna*, PWN, Warszawa 1969 r.
[9] St. Koziej: *Czynniki walki zbrojnej*. „Zeszyty Naukowe AON" 1993 nr 4, s. 57–62.

Natomiast R. Kwećka i A. Nowak przyjmują, że *„informacją jest to wszystko, co można wykorzystać do bardziej sprawnego wyboru działań prowadzących do realizacji celu działania*[10]". Mówiąc o zwiększeniu sprawności działania, należy podkreślić, że mając i użytkując właściwie informację, można celowe działanie realizować lepiej bez istotnego zwiększenia nakładów środków materialnych bądź zużywanej energii.

Jest oczywiste, iż z pozyskiwaniem i użytkowaniem informacji wiąże się konieczność wprowadzenia pewnych środków materialnych i energii, z tym jednak że są one w zasadzie o wiele niższe, niż środki i energia zużywane bezpośrednio na realizację działania celowego. Innymi słowy, informacji nie można uzyskiwać za darmo, lecz koszt jej uzyskania jest z reguły niewspółmiernie niski do zysków płynących z jej uzyskania.

W literaturze przedmiotu spotyka się rozróżnienie informacji faktycznie wykorzystywanych od informacji, które dopiero po odpowiednim przetworzeniu mogą być wykorzystane. Tego typu informacje zwykło się nazywać – danymi.

Niektórzy eksperci wojskowi, kierując się kryterium przedmiotu informacji, wyodrębnili z informacji rozumianej ogólnie informację, którą człowiek lub automat stara się dostarczyć innemu człowiekowi lub automatowi. Taką, w świadomy sposób zdobytą i dostarczoną informację, nazywają oni – wiadomością.

Treścią systemu informacyjnego są wycinkowe informacje techniczne i dotyczące działania w danej dziedzinie, pochodzące z różnych jego podsystemów, dlatego też system ten musi zapewnić sprawny ich obieg, począwszy od zdobycia i przetworzenia danych, a kończąc na wykorzystaniu informacji do podejmowania decyzji. Stąd też kryteria kwalifikacji, forma i zakres systemów zdobywania informacji są determinowane przez potrzeby użytkowników informacji oraz właściwości i powiązania zachodzące między układami, jakie tworzą: człowiek–człowiek; człowiek–maszyna; maszyna–maszyna.

Zgodnie z ogólną teorią organizacji pojęcie „system" może być odniesione do dowolnej całości zorganizowanej, rozumianej jako uporządkowany – według określonego kryterium – zbiór elementów, którymi mogą być nie tylko przedmioty i rzeczy zorganizowane, ale również instytucje, a także cechy i procesy w nich przebiegające[11]. W tym rozumieniu informacje o sytuacji powietrznej oraz procesy związane z ich powstawaniem, jako określone zbiory elementów, również tworzą pewien system. Ujęcie takie ma duże znaczenie w dziedzinie analizy funkcjonowania danego systemu, wykrywanie bowiem obiektów powietrznych i ocena zagrożeń powietrznych realizują się w ramach funkcjonowania systemu wczesnego wykrywania i powiadamiania, działającego w systemie rozpoznania przeciwnika powietrznego, zasilającego system dowodzenia wojskami obrony powietrznej, jak również system wykonawczy (aktywnych środków walki).

---

[10] R. Kwećka, A. Nowak, *Budowa modelu rozpoznania wojskowego w aspekcie organizacyjnym i informacyjnym*, AON, Warszawa 1994; s.167, (rozprawa doktorska).

[11] Por. M. Rembiałkowski, *Projektowanie systemów informatycznych zarządzania*, Gdańsk 1978, s. 12.

Wynika stąd, że systemy zdobywania informacji kwalifikują się do systemów informacyjnych i są logicznym, całościowym układem (zbiorem) danych o sytuacji powietrznej (obiektach powietrznych) na podejściach do granic rejonu obrony kraju. Ponadto, dotyczą stanu i możliwości bojowych sił i środków napadu powietrznego przeciwnika, a także logistycznych i innych danych uzyskiwanych w wyniku zaistnienia zdarzeń i procesów w ramach prowadzonych działań bojowych, następnie przetwarzanych przy zastosowaniu odpowiednich metod, technik i urządzeń ułatwiających poznanie i ocenę zagrożeń i rzeczywistości sytuacji powietrznej, a także organizowanie (planowanie) działań obronnych w wyniku podejmowania decyzji na różnych szczeblach dowodzenia.

Na uwagę zasługuje to, że w ujęciu dynamicznym system zdobywania informacji może być traktowany jako zbiór procesów (faz), niezależnie od specyficznych warunków działania i potrzeb informacyjnych decydentów obrony powietrznej. Możemy wyodrębnić zbiór takich procesów, jak: zdobywania, selekcji i gromadzenia danych źródłowych; przetwarzania, analizy i syntezy informacji; formułowania wniosków oraz opracowania prognoz i przekazywania uprzedzających informacji decydentom obrony powietrznej.

Strukturę systemu zdobywania informacji w ujęciu dynamicznym, przedstawiono na rys. 3.

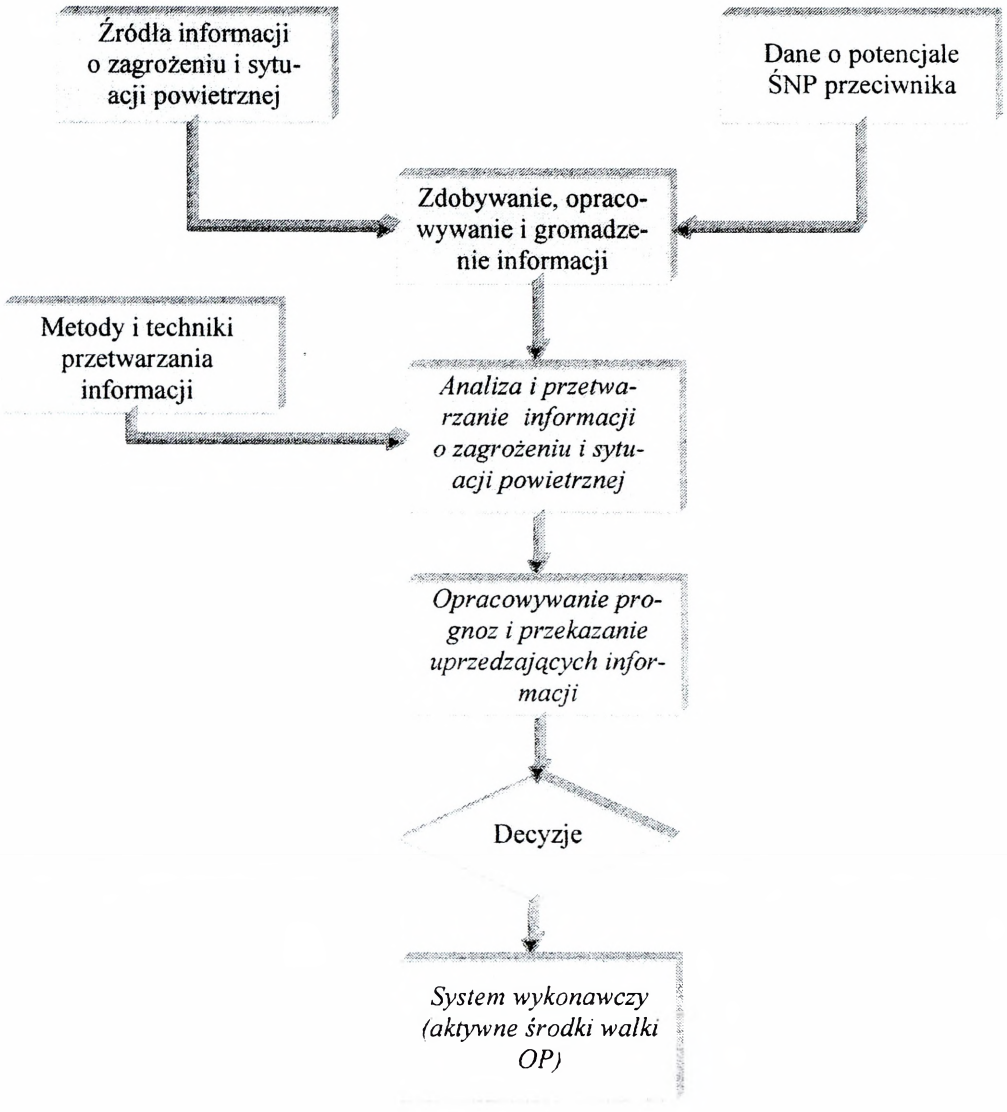
Wyróżnione na rysunku elementy (układy, podsystemy) systemu zdobywania informacji, z punktu widzenia dynamicznego zawierają obraz wzajemnego ustosunkowania się do siebie czynności składających się na pełny proces przetwarzania danych w tym systemie. Jest to typowy obraz struktury procesów przebiegających w systemie informacyjnym, w tym wypadku – systemie zdobywania informacji o sytuacji powietrznej.

Zdobywanie, opracowywanie i gromadzenie informacji obejmuje wykrywanie i śledzenie obiektów powietrznych, namierzanie pracujących źródeł radioelektronicznych, zamianę danych źródłowych na symbole (kody) lub ich uogólnianie za pomocą wskaźników zbiorczych, a następnie przekazanie ich do banku danych. Czynności te dotyczą również wyboru właściwego źródła informacji o zagrożeniu i sytuacji powietrznej oraz sposobu jej przekazania i opracowania.

Gromadzenie informacji powinno się ograniczać do minimum i odbywać według ściśle określonego programu działania, ponieważ ma ono obrazować sytuację powietrzną na podejściach do rejonu obrony kraju, mającą wpływ na efektywność dowodzenia oraz rozstrzygać kwestie: co, gdzie, kiedy i jak należy gromadzić, by zaspokoić potrzeby użytkowników informacji (systemu dowodzenia).

Analiza i przetwarzanie informacji o zagrożeniach i sytuacji powietrznej ma zasadnicze znaczenie w systemie wczesnego wykrywania i powiadamiania. Zbiór danych otrzymany (zdobyty) z odpowiednich źródeł informacji jest wykorzystywany w dowodzeniu po uprzednim uporządkowaniu według algorytmu[12].

[12] Por. M. Adamczyk, Z. Groszek, *Rozpoznanie radiolokacyjne dla potrzeb dowodzenia wojskami w systemie OP – obecnie i w przyszłości*, AON, Warszawa 1995, s. 51.



Rys. 3. Struktura systemu zdobywania informacji w ujęciu dynamicznym

Algorytm ten określa się mianem: wytyczne przetwarzania informacji, obejmuje bowiem takie czynności, jak: integracja, programowanie i kodowanie danych, przyjmowanie i przetwarzanie informacji. Analiza i przetwarzanie informacji pozwala wypracować odpowiednie wnioski podczas oceny zagrożenia i sytuacji powietrznej, a tym samym warunkuje opracowanie prognoz i wariantów działania ŚNP przeciwnika. W odniesieniu do systemu zdobywania informacji, w wyniku analizy i przetwarzania informacji staje się możliwe: ustalenie faktu rozpoczęcia przez przeciwnika powietrznego działań bojowych lub nowego ich etapu; ujawnienie

operacyjnego (taktycznego) zamiaru działań przeciwnika powietrznego; prognozowanie jego dalszych działań; zwiększenie terminowości i wiarygodności informacji.

Formułowanie wniosków i przesyłanie informacji użytkownikom jest bardzo ważnym elementem w podejmowaniu decyzji. Na odpowiednim szczeblu dowodzenia determinuje je określony zbiór informacji gromadzonych i przetwarzanych z odpowiednią częstotliwością w systemach informacyjnych. Na szczeblu operacyjnym (operacyjno-taktycznym), są potrzebne informacje uogólnione, obejmujące przestrzeń na podejściach do granicy państwa (rejonu obrony korpusu SP), charakteryzujące się dużą wiarygodnością. Informacje te powinny umożliwić: doprowadzenie wojsk w systemie obrony powietrznej do pełnej gotowości bojowej; ujawnienie zamiaru nalotu przeciwnika powietrznego; określenie kierunku skupienia głównego wysiłku obrony i utworzenie niezbędnego stosunku sił na kierunkach i rubieżach względem celów powietrznych przez racjonalny podział zadań dla systemu wykonawczego (aktywnych środków walki OP).

Charakterystyka źródeł zdobywania informacji

Zdobywanie informacji jest działaniem celowym i planowanym, wykonywanym przez osoby bezpośrednio lub pośrednio (przy wykorzystaniu sprzętu technicznego). Ponieważ posiadanie informacji zwiększa sprawność działania – i można celowe działanie wykonywać efektywniej – bez istotnego zwiększenia nakładów środków materialnych i energii, z tym jednak że są one w zasadzie o wiele niższe, niż środki i energia zużywana bezpośrednio na realizację działania celowego. Innymi słowy, koszt uzyskania informacji jest z reguły niewspółmiernie niski do zysków płynących z jej uzyskania[13].

Skuteczność i efektywność zintegrowanej OP oraz bezpieczeństwo państw NATO jest uwarunkowane posiadaną aktualną, wiarygodną informacją o przeciwniku, a w szczególności o jego działaniach powietrznych. W zintegrowanej obronie powietrznej rozpoznanie jest jego istotnym elementem, odgrywa znaczącą rolę w wykonywaniu stojących przed nim zadań. Wypełnia jedną z podstawowych funkcji, jaką jest zdobywanie informacji i informowanie decydentów aktywnych środków walki o działaniach sił powietrznych przeciwnika. Ponadto, jest najważniejszym elementem zabezpieczenia działań bojowych wszystkich szczebli dowodzenia rodzajów wojsk oraz sił zbrojnych.

Zdobyta i przekazana decydentom informacja, jest podstawą racjonalnego przygotowania sił i środków do prowadzenia walki z przeciwnikiem powietrznym w celu wykonania postawionych zadań. Zdobywanie informacji jest realizowane przez wyspecjalizowane siły i środki na każdym szczeblu. Właściwy podział źródeł zdobywania informacji można dokonać według przyjętych kryteriów, do których

[13] Por. Z. Skwarek, *Systemy wczesnego wykrywania w obronie powietrznej państw NATO*, AON, Warszawa 1998.

możemy zaliczyć potencjał rozpoznawczy[14], szczebel – na jakim jest prowadzone rozpoznanie – oraz środowisko, z którego jest prowadzone rozpoznanie.

Do scharakteryzowania źródeł zdobywania informacji o sytuacji powietrznej przyjęto ostatnie kryterium, ze względu na środowisko, z którego jest prowadzone rozpoznanie. Wyboru dokonano na podstawie analizy możliwości bojowych poszczególnych środków rozpoznania w zakresie pozyskiwania informacji o sytuacji powietrznej, wobec występujących zagrożeń ze strony ŚNP w obecnych czasach.

Kosmiczne źródła zdobywania informacji

Rozpoznanie kosmiczne należy traktować jako najważniejszy rodzaj rozpoznania zarówno w okresie pokoju, kryzysu jak i wojny. Za pomocą rozpoznania satelitarnego mogą być zdobywane prawie wszystkie informacje natury wojskowej i gospodarczej potencjalnego przeciwnika. W stosunku do realizowanych zadań bojowych oraz zapotrzebowania na informację, są modelowane orbity satelitów rozpoznawczych w celu zdobywania informacji o przeciwniku lub terenie. Najczęściej w taki sposób, aby cyklicznie, w określonych interwałach czasowych, zlokalizować i ustalić rzeczywistą sytuację militarną i radioelektroniczną na obszarach zainteresowania.

Satelita umieszczony na pewnej wysokości H nad powierzchnią ziemi, ma możliwość kontrolowania obszaru ograniczonego linią horyzontu. Obszar ten jest więc częścią powierzchni ziemi ograniczoną okręgiem.

Możliwości techniczne rozpoznania kosmicznego umożliwiają prowadzenie rozpoznania wzajemnie uzupełniającymi się technikami. W rozpoznaniu kosmicznym stosuje się satelity wyposażone w urządzenia elektroniczne (radiolokacyjne, radioelektroniczne), optyczne, fotograficzne (termiczne), które umożliwiają zdobywanie informacji o przeciwniku w każdych warunkach. Najważniejszym zadaniem rozpoznania satelitarnego jest ostrzeganie o zagrożeniu bezpieczeństwa państwa lub koalicji państw, możliwie wczesne, o ataku nieprzyjaciela za pomocą rakiet, lotnictwa, sił morskich i lądowych[15].

Zintegrowana OP NATO nie posiada systemów rozpoznania kosmicznego, ale w każdej chwili może otrzymać informację z amerykańskiego satelitarnego systemu wczesnego ostrzegania SEWS (Satellite Early Warning System). Polska jako członek NATO niewątpliwie będzie posiadała dostęp do informacji pozyskiwanej przez amerykańskie systemy satelitarne wówczas, gdy nasz system OP zakończy proces integracji z systemem OP NATO. SEWS oparty jest na satelitach umieszczonych na geostacjonarnych orbitach, znajdujących się nad Oceanem Indyjskim, Spokojnym i Atlantykiem. Ich zadaniem jest wykrywanie rakiet balistycznych już podczas startu i uprzedzenia naziemnych środków dowodzenia[16]. Dodatkowo, zintegrowana OP NATO może otrzymywać informacje rozpoznawcze poprzez Do-

[14] L. Ciborowski, *Rola i miejsce rozpoznania w systemie obronnym RP*, AON, Warszawa 1993.

[15] Por. W. Świątnicki, *Wykorzystanie systemów satelitarnych przez siły powietrzne RP*, AON, Warszawa 1999.

[16] Por. Z. Skwarek, *Systemy wczesnego wykrywania*... op. cit.

wództwo NORAD z innych satelitów, organizacyjnie podporządkowanych siłom powietrznym i marynarce wojennej USA. Źródłami informacji mogą być satelity rozpoznania radiolokacyjnego „Lacross 1" i „Lacross 2", które pracują w zakresie pasma centymetrowego oraz satelity rozpoznania radioelektronicznego „Magnum" oraz „Vortex". Satelity rozpoznania radiolokacyjnego są przeznaczone do wykrywania sygnałów emitowanych przez stacje radiolokacyjne, stacje systemów naprowadzania rakiet oraz określania ich charakterystyk. Dane uzyskiwane poddaje się obróbce w odpowiednim układzie analizującym. Celem tego działania jest niezbędne uszeregowanie informacji o obiektach i nadanie im formy umożliwiającej odległościowe przekazywanie w pożądanym czasie. Przekazywanie wyników może się odbywać w formie obrazów, które w punktach odbioru będą natychmiast odtwarzane na ekranach urządzeń zobrazowania. Jest to najsprawniejsza z możliwych form przekazu, ale nie jedyna. W uzasadnionych wypadkach może być stosowany bardziej złożony system rejestracji i wizualizacji wyników rozpoznania radiolokacyjnego, a mianowicie optyczny[17].

Natomiast satelity rozpoznania radioelektronicznego przechwytują fale elektromagnetyczne emitowane przez systemy (urządzenia) łączności, radiolokacyjne oraz radionawigacyjne. Przechwytywane fale elektromagnetyczne są źródłem wielu bezpośrednich informacji i na ich podstawie możliwe jest także określenie współrzędnych punktów, w których znajdują się rozpoznawane źródła promieniowania elektromagnetycznego lub nosiciele tych urządzeń.

Rozpoznanie kosmiczne w nowym systemie dowodzenia i kontroli NATO (ACCS) będzie wykorzystywane jako jedno z głównych źródeł zdobywania informacji o sytuacji powietrznej w czasie konfliktu i wojny. Największą korzyścią wynikającą z zastosowania tego typu środków jest możliwość prowadzenia ciągłego rozpoznania i terminowego dostarczania informacji przez RPC (RAP Production Centre) do stanowisk dowodzenia zintegrowanej OP NATO, umożliwiając planowanie działań[18]. Zadaniem rozpoznania satelitarnego w ramach zabezpieczenia informacyjnego elementów OP może być wykrycie: środków napadu powietrznego przeciwnika, rejonów dyslokacji stanowisk startowych rakiet, stanowisk dowodzenia i naprowadzania lotnictwa, systemów łączności satelitarnej oraz środków rozpoznania radiolokacyjnego i radionawigacji.

Niezaprzeczalnym dowodem na powyższe stwierdzenia jest skuteczny udział rozpoznania kosmicznego w konflikcie irackim. Od jego początku satelity rozpoznawcze przekazywały informacje w czasie rzeczywistym poprzez Centrum Kontroli i Przetwarzania Informacji Dowództwa USSC do SD sił sprzymierzonych dotyczące położenia wojsk, posterunków radiolokacyjnych, startów pocisków SCUD. Ważną rolę spełniały satelity rozpoznania radioelektronicznego umieszczone nad zachodnią częścią Oceanu Indyjskiego, które wykrywały wszystkie urządzenia emitujące fale elektromagnetyczne (radiostacje, stacje radiolokacyjne i naprowadzania rakiet). Wysoko oceniono przydatność satelitów wczesnego

[17] Por. W. Świątnicki, op. cit.
[18] Zob. ibidem.

ostrzegania typu DSP (Defense Support Program). Czujniki tych satelitów wykrywały start i określały tor lotu pocisków SCUD, a dane o nich były natychmiast przekazywane na stanowiska startowe przeciwlotniczych zestawów rakietowych Patriot. Niezawodną łączność zapewniały systemy łączności satelitarnej typu Single Channel Ground and Airborne Radio System i Tri-service Tactical Communications[19].

Powietrzne źródła zdobywania informacji

Skutecznym środkiem zwiększenia zasięgu urządzeń rozpoznania radiolokacyjnego i radioelektronicznego jest wyniesienie ich w powietrze i pokonanie tym samym podstawowego ograniczenia jakim jest krzywizna ziemi. Instalowane stacje rozpoznawcze na pokładzie samolotów wczesnego ostrzegania i naprowadzania charakteryzują się wspaniałymi wskaźnikami możliwości przestrzennych, które bezpośrednio wpływają na wydłużenie czasu reakcji aktywnych środków walki OP w stosunku do ŚNP, szczególnie na małych wysokościach. Obrona powietrzna RP nie posiada takowego systemu, ale jako członek NATO posiada możliwość pozyskiwania informacji o sytuacji powietrznej z samolotu systemu AWACS poprzez CAOC w Kalkar.

Powietrzny system wczesnego wykrywania i naprowadzania (AWACS) jest podstawowym źródłem zdobywania informacji o sytuacji powietrznej w zintegrowanej OP NATO podczas konfliktu i wojny. System ten powstał na bazie amerykańskich samolotów E-3 Sentry i jest przeznaczony do:[20]

– wykrywania i identyfikacji obiektów powietrznych oraz lokalizowania ich w całym przedziale wysokości, ze szczególnym uwzględnieniem małych wysokości;

– wykrywania, lokalizowania i identyfikowania celów nawodnych;

– wykrywania i lokalizowania naziemnych środków OP i OPL przeciwnika;

– wykrywania promieniujących pokładowych stacji radiolokacyjnych, stacji obserwacji terenu, kierowania uzbrojeniem, a także innych urządzeń radioelektronicznych emitujących energię elektromagnetyczną;

– przekazywania informacji o sytuacji powietrznej do stanowisk dowodzenia i kierowania zintegrowaną OP;

– naprowadzania własnych samolotów na obiekty powietrzne;

– kierowania działaniami lotnictwa taktycznego podczas wykonywania zadań bojowych.

Realizacja powyższych zadań przez system wczesnego wykrywania i naprowadzania umożliwia:

– stworzenie szczelnej strefy informacyjnej nad obszarem państw członkowskich NATO oraz w rejonie działań bojowych;

– znaczne zwiększenie zasięgu wykrywania obiektów powietrznych na małych i bardzo małych wysokościach;

---

[19] Por. E. Pawlak, D. Stachura-Michalski, *Współczesne rozpoznanie kosmiczne*, „Przegląd Wojsk Lotniczych i Obrony Powietrznej" 1993, nr 12.

[20] Por. Z. Skwarek, *Systemy wczesnego wykrywania*... op. cit.

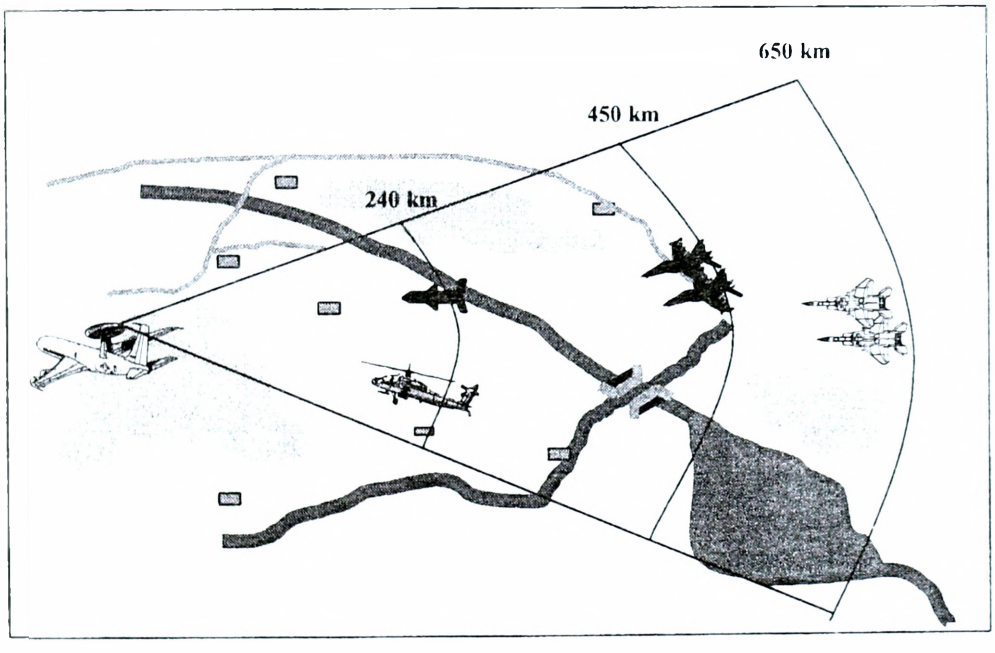
– przesunięcie możliwych rubieży wprowadzenia do walki lotnictwa myśliwskiego;

– obniżenie wymagań dotyczących utrzymywania w wysokim stopniu gotowości bojowej aktywnych środków walki w okresie kryzysu i wojny bez zmniejszenia możliwości ich oddziaływania na cele powietrzne;

– kontrolę przestrzeni powietrznej na każdym kierunku operacyjnym oraz zwiększenie żywotności naziemnego i nawodnego systemu rozpoznania pracującego w warunkach zakłóceń radioelektronicznych poprzez wymianę informacji.

Podstawowym wyposażeniem pokładowym samolotów E-3A/D oraz E-3F[21] (francuskie), przeznaczonym do zdobywania informacji, jest impulsowa stacja radiolokacyjna AN/APY-2 z cyfrowym przetwarzaniem danych oraz stacja rozpoznania radioelektronicznego typu AN/AYR-1 (E-3D posiadają stację typu LORAL1017).

Podstawowym rodzajem pracy stacji radiolokacyjnej AN/APY-2, podczas przebywania w strefie dyżurowania, jest impulsowo-dopplerowski, który pozwala na wykrywanie i śledzenie celów powietrznych na tle ziemi. Możliwości wykrywania systemu zależą od skutecznej powierzchni odbicia celu oraz odległości i wysokości lotu (rys. 4).



Źródło: Opracowanie własne na podstawie W. Marud, M. Mikołajczuk, *Planowanie działań bojowych w SP z wykorzystaniem procedur NATO. Wybrane kalkulacje taktyczne*, AON, Warszawa 1999.

Rys. 4. Możliwości wykrywania samolotu E-3A systemu AWACS.

[21] Siły zbrojne Francji nie należą do NATO, ale francuski powietrzny system wczesnego wykrywania ściśle współpracuje z siłami wczesnego wykrywania NATO.

Zadaniem stacji rozpoznania radioelektronicznego AN/AYR-1 jest pasywne rozpoznawanie celów powietrznych na podstawie przechwyconej energii elektromagnetycznej, promieniowanej przez takie urządzenia, jak: pokładowe stacje kierowania uzbrojeniem i obserwacji terenu, pokładowe urządzenia nadawczo-odbiorcze oraz system nawigacyjny. Wykrycie i przechwycenie takich źródeł promieniowania, a także ich podstawowych parametrów, tj. częstotliwości nośnej, długości i okresu powtarzania impulsów, pozwalają określić konkretny typ każdego urządzenia i przypisać go do odpowiedniego nosiciela[22].

Zautomatyzowany system przekazywania danych JTIDS (Joint Tactical Information Distribution System), przeznaczony do przesyłania informacji zakresu łączności KF i UKF, zapewnia łączność wielokanałową, utajnioną i jawną, z selektywnym wyborem abonentów naziemnych i powietrznych. JTIDS zapewnia załodze samolotu E-3A/D wymianę danych o sytuacji powietrznej z naziemnymi ośrodkami zautomatyzowanego systemu OP NATO (także z wprowadzanym systemem ACCS). Działanie tego systemu polega na automatycznym przekazywaniu informacji o wykrytych celach z pokładu samolotu z jednoczesną bardzo szybką zmianą częstotliwości nośnej, co uniemożliwia przechwycenie i zakłócenie przez przeciwnika przekazywanej informacji[23]. System ten umożliwia utrzymywanie łączności z 2000 korespondentów rozmieszczonych w strefie o promieniu 500 km (od 1995 r. zainstalowano cyfrowy system transmisji danych – Link 16)[24].

Dodatkowym źródłem informacji są samoloty rozpoznania radioelektronicznego (C-160, RF-16, Atlantic, Nimrod), które wykonują nieregularne loty wzdłuż granic państwowych. Z samolotów jest prowadzone rozpoznanie radiowe UKF, systemów radiolokacyjnych oraz sporadycznie rozpoznanie radiolokacyjne. Zasięg rozpoznania jest uwarunkowany mocą rozpoznawanych źródeł promieniowania oraz wysokością lotu samolotu rozpoznawczego. Na podstawie analizy parametrów lotów samolotów rozpoznawczych, w ocenie zagrożenia można przyjąć następujące wielkości zasięgów:

– podzakres UKF (do 100 MHz) – do 150–200 km;

– podzakres UKF (do 440 MHz) – do 400 km;

– urządzenia rozpoznania systemów radiolokacyjnych – 400 km (środków naziemnych) oraz 550 km (środków powietrznych)[25].

Nawodne źródła zdobywania informacji

Rozpoznanie przestrzeni powietrznej jest również prowadzone na akwenach morskich przez środki rozpoznania nawodnego zainstalowane na pokładach okrętów sił morskich NATO oraz jednostek narodowych państw należących do Sojuszu.

---

[22] Z. Groszek, *Narodowy system rozpoznania w obronie powietrznej RP*, AON, Warszawa 2001.

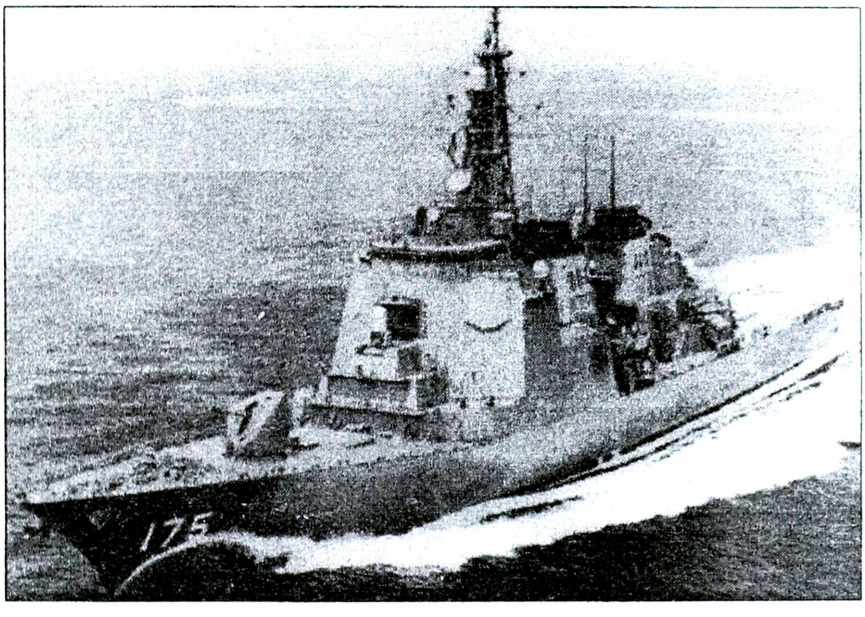
[23] W. Marud, M. Mikołajczuk, *Planowanie działań bojowych w SP z wykorzystaniem procedur NATO. Wybrane kalkulacje taktyczne*, AON, Warszawa 1999.

[24] M. Kozub, S. Szulc, *Wsparcie działań powietrznych w operacjach połączonych NATO*, „Przegląd Wojsk Lotniczych i Obrony Powietrznej" 2000, nr 8.

[25] Zob. Z. Skwarek, *Systemy wczesnego wykrywania i powiadamiania OP RP*, AON, Warszawa 2000, (rozprawa doktorska).

Warto zwrócić uwagę na fakt, że obecnie nowy okręt nie posiada klasycznego systemu obrony okrętu, lecz system obrony obszaru (np. okrętowy system obrony powietrznej AEGIS). Okręty te spełniają rolę pływających zestawów, zapewniających przeniesienie strefy OP w obszar prowadzenia operacji na odległym teatrze. Nowe okręty są przeznaczone do wypełniania różnego rodzaju misji i dlatego wyposażono je w bogaty zestaw uniwersalnych systemów uzbrojenia i elektroniki bojowej. Ich nadrzędnym zadaniem jest wczesne wykrywanie i skuteczne zwalczanie celów powietrznych, takich jak samoloty, pociski kierowane oraz rakiety balistyczne o zasięgu strategicznym i operacyjnym.

Wyposażenie radioelektroniczne okrętów jest przystosowane do jednoczesnego wykrywania i obserwacji różnych typów celów w warunkach silnych zakłóceń radioelektronicznych oraz w każdych warunkach atmosferycznych i w różnych klimatach.

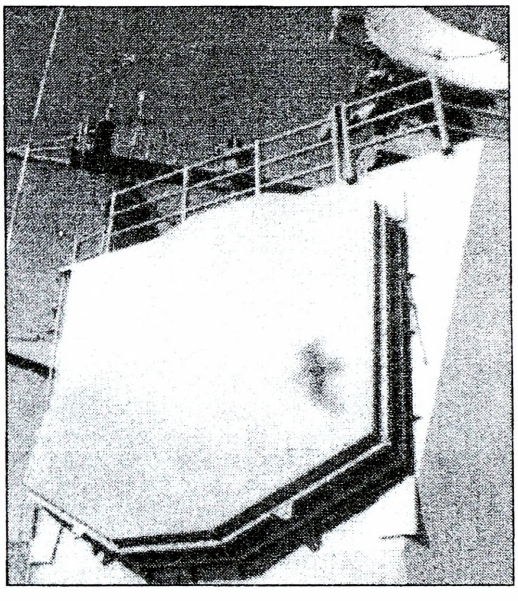


Rys. 5. Niszczyciel wyposażony w okrętowy system obrony powietrznej AEGIS

Do podstawowego wyposażenia okrętów sił morskich NATO należą stacje radiolokacyjne dalekiego zasięgu. Niewątpliwie, najsłynniejszym radarem okrętowym jest AN/SPY-1, który stanowi podstawowe źródło informacji dla systemu dowodzenia okrętu, oznaczonego symbolem AEGIS. Radar AN/SPY-1 jest radarem wielofunkcyjnym, który przeszukuje przestrzeń w pełnym sektorze 360^0 i w całej górnej półsferze w zasięgu kilkuset km, dokładnie śledzi wykryte obiekty, naprowadza własne samoloty na wykryte cele oraz naprowadza rakiety wystrzelone w kierunku zwalczanych celów. Natomiast najnowocześniejszą i powszechnie stosowaną stacją radiolokacyjną na okrętach jest SMART-L, która jest cyfrowym,

trójwspółrzędnym radarem wielowiązkowym. Została zaprojektowana w myśl nowych wymagań NATO dotyczących radiolokatorów obserwacji dużych przestrzeni.

Dzięki dużej mocy i zaawansowanej cyfrowej obróbce sygnałów, SMART-L doskonale nadaje się do wykrywania i obserwacji trudno wykrywalnych aparatów latających (obiektów wykonanych w technologii stealth – przypuszczalnie do ok. 150 km), dalekiego wykrywania rakiet balistycznych czy pocisków rakietowych innych typów. Na plus stacji SMART-L należy jednak zaliczyć to, iż udało się uzyskać wysoką dokładność obserwacji obiektów powietrznych i szybką obróbkę informacji, wymaganą szczególnie przy śledzeniu celów balistycznych. SMART-L może wykrywać cele z maksymalnej odległości 400 km oraz śledzić do 1000 obiektów powietrznych jednocześnie, na odległości do 350 km[26].



Rys. 6. Jedna z czterech anten stacji radiolokacyjnej SPY-1 okrętowego systemu walki AEGIS

Rozpoznanie radioelektroniczne z morza jest prowadzone przez specjalistyczne okręty (Oste-Alster, Oste-Oker, Oste, Viben) sił morskich państw NATO. Z pokładów okrętów rozpoznaje się źródła promieniowania elektromagnetycznego, analogicznie jak z samolotów. Zasięgi rozpoznawania poszczególnych urządzeń radioelektronicznych wynoszą:

– podzakres UKF (do 100 MHz) – do 60 km;
– podzakres UKF (do 440 MHz) – 100–150 km;

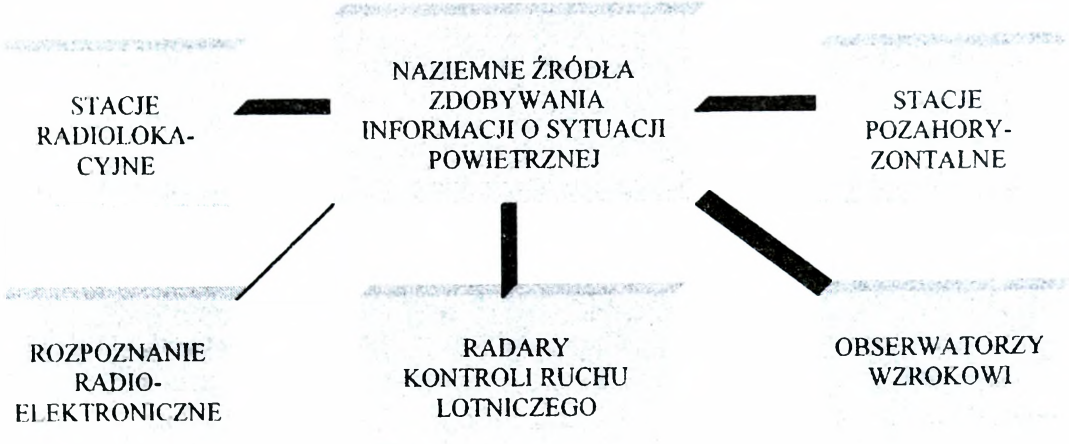
[26] Por. „Nowa Technika Wojskowa", 2000 nr 10.

– urządzenia rozpoznania systemów radiolokacyjnych – 300–400 km (środków naziemnych) oraz 500–550 km (środków powietrznych)[27].

Zdobyte informacje przez okrętowe środki rozpoznania o sytuacji powietrznej i nawodnej są przekazywane do ośrodków zbierania, analizy i oceny poszczególnych TDW i ETW przez systemy łączności Link 11. Ponadto okręty wykorzystują systemy łączności klasycznej Link 4A i satelitarnej SATCOM WRN-5. Na nowych okrętach, oprócz licznych radiostacji krótko- i długofalowych o zasięgu taktycznym, przewidziano instalację – we wszystkich flotach NATO – standardowych urządzeń łączności satelitarnej SATCOM UHF/SHF oraz łączy transmisji danych operacyjnych w czasie rzeczywistym Link 11 i Link 16 MIDS[28]. Wyposażanie okrętów w powyższe urządzenia transmisji danych świadczy o tym, że systemy zbioru i dystrybucji informacji o sytuacji powietrznej OP NATO zamierzają współpracować z poszczególnymi jednostkami nawodnymi w zakresie wymiany informacji.

Naziemne źródła zdobywania informacji

Naziemne, mobilne i stacjonarne, źródła pozyskiwania informacji (rys. 5) są powszechnie stosowane we wszystkich systemach OP. W okresie pokoju wykorzystuje się je jako podstawowe do pozyskiwania informacji o sytuacji powietrznej. Naziemny system rozpoznania zabezpiecza stanowiska dowodzenia OP w informację o sytuacji powietrznej, niezbędną do dowodzenia dyżurnymi siłami obrony powietrznej, funkcjonowania podsystemu poszukiwania i ratownictwa lotniczego, zabezpieczania procesu szkolenia lotniczego oraz uczestniczy w kontroli i nadzorze przestrzeni powietrznej[29].



Rys. 7. Naziemne źródła pozyskiwania informacji

[27] Zob. Z. Skwarek, rozprawa doktorska, op. cit.
[28] Raport, *Wojsko, technika, obronność*, 03/2000 r.
[29] Zob. Z. Skwarek, *Taktyka wojsk radiotechnicznych SP*, AON, Warszawa 2001.

Naziemne środki rozpoznania umożliwiają zorganizowanie ciągłej oceny sytuacji powietrznej na podejściach do rejonu obrony i nad obszarem kraju czy Sojuszu. Urządzenia te są stosunkowo tanie w produkcji i eksploatacji (z wyjątkiem stacji pozahoryzontalnych) w porównaniu z powietrznymi czy kosmicznymi urządzeniami pozyskiwania informacji o sytuacji powietrznej, stąd są uważane za najefektywniejsze z ekonomicznego punktu widzenia. Natomiast wadą tych źródeł są ograniczone możliwości przestrzenne, które wobec współczesnych zagrożeń ze strony ŚNP nie w każdej sytuacji taktycznej mają możliwość wykonania postawionych zadań.

a) naziemne stacje radiolokacyjne

Naziemne stacje radiolokacyjne można podzielić na wiele typów, które łączy jedna wspólna cecha – służą do ciągłej obserwacji przestrzeni powietrznej w celu wykrywania wszystkich pojawiających się w niej obiektów, śledzenia tras wybranych obiektów oraz stałego przekazywania informacji o ich wykryciu do nadrzędnych stanowisk dowodzenia. Poza tą wspólną cechą, wszystkie stacje radiolokacyjne można podzielić na wiele grup, różniących się takimi cechami, jak: zakres częstotliwości roboczej, możliwości określania parametrów obiektów powietrznych oraz przeznaczenia taktycznego.

Stacje radiolokacyjne są zasadniczym źródłem zdobywania informacji o sytuacji powietrznej w okresie pokoju, kryzysu i wojny. Powyższe stwierdzenie wynika z takich właściwości RLS, jak:

– niskie koszty eksploatacji;

– możliwość zdobywania informacji o obiektach powietrznych w każdych warunkach atmosferycznych oraz o dowolnej porze doby i roku;

– możliwość zdobywania informacji o obiektach powietrznych w warunkach stosowania zakłóceń radioelektronicznych;

– możliwość zdobywania informacji o obiektach powietrznych praktycznie w całym zakresie wysokości ich lotu;

– możliwość szybkiego wykonania manewru na zagrożone kierunki.

Charakterystykę możliwości naziemnych stacji radiolokacyjnych w dziedzinie pozyskiwania informacji przedstawiono na podstawie klasyfikacji dokonanej według możliwości określania parametrów obiektów powietrznych. Ten podział pozwoli przedstawić najważniejsze cechy trzech grup RLS odnośnie do możliwości pozyskiwania informacji o obiektach powietrznych. Scharakteryzowano współczesne stacje, które są powszechnie używane w systemie rozpoznania RP oraz ich możliwości bojowe, które są porównywalne z innymi RLS tego typu.

Stacja radiolokacyjna dwuwspółrzędna typu NUR-31 określa dwie współrzędne obiektów powietrznych (azymut i odległość) oraz automatycznie współpracuje z wysokościomierzem NUR-41, który określa trzecią współrzędną – wysokość obiektu. Stacja NUR-31 wykrywa obiekty powietrzne o skutecznej powierzchni odbicia 1 m^2 i prawdopodobieństwie 0,5 w zakresie odległości do 160 km oraz wysokości około 20 km. Antena reflektorowa o rozpiętości 10 m formuje wiązkę

o szerokości azymutalnej ok. 2°, co pozwala uzyskać dokładność określania azymutu obiektu 0,3°. W stacji zastosowano technikę kompresji impulsu, dzięki czemu uzyskano dobrą rozróżnialność w odległości – ok. 100 m [30]. W stacji zastosowano szereg układów przeciwzakłóceniowych do eliminowania zakłóceń aktywnych (LOS, TES, KLB, losowe przestrajanie automatyczne na jedną z ośmiu częstotliwości) oraz do eliminowania zakłóceń pasywnych (TES, ZRT). Stacja może śledzić trasy do 32 obiektów manewrujących i posiada wyjście umożliwiające cyfrową transmisję całej sytuacji powietrznej przez przystawkę TSS-10 do ZtSD „Dunaj" w czasie rzeczywistym.

Do następnej grupy stacji radiolokacyjnych należą wysokościomierze, które określają odległość i kąt elewacji wykrytych obiektów. Na tej podstawie wylicza się wysokość obiektu powietrznego. Współczesne wysokościomierze są automatycznie sprzęgnięte z odległościomierzem i pracują bez udziału operatora. W tym rodzaju pracy operator odległościomierza automatycznie naprowadza anteną wysokościomierza kolejno na azymuty śledzonych obiektów, który odsyła do niego zmierzoną wysokość, dowiązaną do właściwej trasy śledzonego obiektu przez odległościomierz. W efekcie, odległościomierz przesyła pełne dane wykrytego obiektu powietrznego do stanowiska dowodzenia. Przykładem tego typu wysokościomierza jest NUR-41. Antena tej stacji formuje wiązkę o szerokości 3,5° w płaszczyźnie poziomej i 0,8° w płaszczyźnie pionowej. Takie rozmiary kątowe wiązki umożliwiają określanie kąta elewacji z błędem nie większym niż 0,1°, co oznacza, że na odległości 150 km błąd pomiaru wysokości obiektu wynosi około 250 m. Ważnym parametrem wysokościomierzy jest liczba wykonywanych pomiarów wysokości na minutę. W przypadku stacji NUR-41 zajmuje to około 5 s, co pozwala wykonać 8 pomiarów wysokości na minutę przy zautomatyzowanej pacy z odległościomierzem NUR-31.

Obecnie do systemu rozpoznania wprowadza się trójwspółrzędne stacje radiolokacyjne, które mierzą azymut, odległość i jednocześnie kąt elewacji wykrytych obiektów, za pomocą którego wylicza się wysokość obiektu. Charakterystyczną stacją tego typu jest NUR-12, która określa współrzędne obiektu z dokładnością 200 m w odległości, 0,2° w azymucie i 600 m w wysokości, mierzone na odległości 150 km[31]. W stacji zastosowano szereg układów przeciwzakłóceniowych do eliminowania zakłóceń aktywnych i pasywnych. Odporność na zakłócenia zapewniają:

- antena o niskim poziomie listków bocznych;
- automatyczny dobór optymalnej częstotliwości w paśmie ok. 7%;
- praca na dwóch częstotliwościach zmiennych od impulsu do impulsu;
- kompresja impulsu;
- układy filtrów cyfrowych TES;
- filtracja podetekcyjna.

Stacja radiolokacyjna NUR-12 może jednocześnie śledzić do 120 obiektów powietrznych przy automatycznej inicjacji śledzenia nowo wykrytych obiektów.

---

[30] Zob. Z. Czekała, *Parada radarów*, Bellona, Warszawa 1999.
[31] Zob. ibidem.

Informacje o wykrytych obiektach są w sposób automatyczny przekazywane do urządzeń nadrzędnych (np. „Dunaj") z pełnym zestawem parametrów, w formacie akceptowanym przez te urządzenia. Informacje o sytuacji powietrznej mogą być przekazywane drogą radiową lub łączem światłowodowym na dużą odległość.

Naziemne stacje radiolokacyjne umożliwiają zdobywanie informacji o obiektach powietrznych znajdujących się w znacznej odległości. Maksymalne odległości wykrywania obiektów, pomijając czynniki związane z potencjałem zasięgowym (moc nadajnika, czułość odbiornika, zysk antenowy, skuteczna powierzchnia odbicia obiektu), są uwarunkowane wysokością zainstalowania anteny i wysokością lotu obiektu. Wynika to z faktu występowania krzywizny ziemi.

Przy określaniu zasięgu wykrywania stacji radiolokacyjnych na małych wysokościach, należy uwzględnić warunki terenowe. W realnych warunkach wokół miejsca rozwinięcia RLS występują różnorodne przeszkody terenowe, które tworzą kąty zakrycia i w znacznym stopniu ograniczają zasięg wykrywania. Znaczący wpływ na zasięg wykrywania nisko lecących obiektów powietrznych przez RLS ma tłumienie jej strefy wykrywania przez przeszkody terenowe. Tłumienie to jest wyrażane współczynnikiem kąta zakrycia pozycji rozwinięcia RLS, którego wartość zależy od wysokości przeszkody terenowej i jej odległości od stacji[32].

b) środki rozpoznania radioelektronicznego

Współczesne statki powietrzne są wyposażone w różnego rodzaju środki radioelektroniczne niezbędne do prowadzenia działań bojowych. Obecnie na pokładzie współczesnych samolotów znajdują się takie urządzenia radioelektroniczne, jak:

– łączności radiowej;
– stacje radiolokacyjne;
– systemy nawigacyjne;
– systemy kierowania uzbrojeniem.

Fala elektromagnetyczna emitowana przez powyższe urządzenia jest cennym źródłem informacji o ich nosicielach. W związku z powyższym, rozpoznanie radioelektroniczne ma możliwość zdobywania informacji o środkach napadu powietrznego na podstawie pracy jego środków radioelektronicznych. Proces zdobywania danych o ŚNP przez środki rozpoznania radioelektronicznego jest realizowany na podstawie wykorzystania obiektywnych zjawisk towarzyszących promieniowaniu energii elektromagnetycznej, takich jak:

– możliwość przechwytywania emisji pokładowych środków radioelektronicznych;
– możliwość ustalenia miejsca położenia tych środków;
– występowanie w przechwytywanych emisjach cech rozpoznawczych i informacji pozwalających określić przynależność i przeznaczenie pracujących środków radioelektronicznych oraz charakter działań ŚNP.

[32] Zob. Z. Skwarek, *Taktyka wojsk...* op. cit.

Rozpoznanie radioelektroniczne prowadzi się w zakresie fal radiowych krótkich i ultrakrótkich oraz mikrofalowym. Na znaczenie tego rodzaju rozpoznania wpływają takie cechy, jak:

– możliwość prowadzenia rozpoznania w dowolnych warunkach atmosferycznych, o dowolnej porze doby i roku;

– skrytość prowadzonego rozpoznania ze względu na bierny charakter pracy urządzeń rozpoznania radioelektronicznego;

– pozyskiwanie informacji bez bezpośredniej styczności z obiektem rozpoznania;

– duży zasięg rozpoznania, który w zasadzie jest ograniczony warunkami propagacji fal elektromagnetycznych.

Środki rozpoznania radioelektronicznego są wykorzystywane do zdobywania informacji o sytuacji powietrznej zarówno w czasie pokoju, jak i w czasie wojny. Zasadniczym zadaniem tego rodzaju rozpoznania w czasie pokoju jest ciągłe informowanie organów dowodzenia systemem OP o działalności szkoleniowej i bojowej oraz przygotowaniach do działań wojennych przez SP potencjalnego przeciwnika. Natomiast w czasie wojny, podstawowym zadaniem rozpoznania radioelektronicznego jest uprzedzanie stanowisk dowodzenia systemu OP o działalności ŚNP na dalekich podejściach do granicy państwa (poza strefą rozpoznania naziemnych stacji radiolokacyjnych) oraz ciągłe informowanie o działalności statków powietrznych przeciwnika w rejonie odpowiedzialności OP, głównie stosujących zakłócenia radioelektroniczne i wykonujących loty na małych wysokościach. Pododdziały rozpoznania radioelektronicznego wykonują powyższe zadania, prowadząc ciągłe:

– poszukiwanie, śledzenie i przechwytywanie relacji łączności radiowej między statkiem powietrznym a innym obiektem prowadzonymi odbiornikami radiowymi zakresu KF (EK-890) oraz UKF (ESM-500);

– namierzanie pokładowych radiostacji pracujących z zautomatyzowanymi systemami namierzania radiowego KF – „600", UKF – „ODF 051";

– poszukiwanie oraz namierzanie pracujących pokładowych systemów radiolokacyjnych, radionawigacyjnych oraz kierowania uzbrojeniem.

Współczesne środki rozpoznania radioelektronicznego charakteryzują się specyficznymi właściwościami co do pozyskiwania informacji o sytuacji powietrznej. Odbiornik radiowy ESM-500 firmy ROHDE & SCHWARZ umożliwia odbiór sygnałów w zakresie 20–1000 MHz. Może być zdalnie sterowany komputerem lub za pomocą jednego z odbiorników tego typu wchodzących w skład systemu rozpoznania. Odbiornik spełniający rolę elementu sterującego w systemie rozpoznania radiowego, może sterować maksymalnie dziesięcioma podległymi odbiornikami. Odbiornik posiada pamięć umożliwiającą zapamiętanie 999 częstotliwości, co zwiększa możliwości jego wykorzystania. Natomiast odbiorniki EK-890, tej samej firmy, umożliwiają odbiór sygnałów w zakresie częstotliwości od 10 kHz do 30 MHz, z możliwością przestrajania co 1 Hz. Sterowanie odbiornikiem może się odbywać lokalnie – za pomocą klawiatury odbiornika lub zdalnie, które obejmuje możliwości przestrajania w całym zakresie częstotliwości, z dyskretnością 1 Hz i czasem przestrajania 5 ms. W przypadku pracy zautomatyzowanego systemu

rozpoznania, zbudowanego wyłącznie z odbiorników EK-890, maksymalna ich liczba nie może przekraczać 99. Odbiornik posiada pamięć umożliwiającą zapamiętanie 999 częstotliwości.

Do lokalizacji pokładowych radiostacji wykorzystuje się namierniki radiowe ODF-051, które pracują w zakresie częstotliwości 30–1300 MHz. Szybkość przestrajania namiernika wynosi 188 MHz/s. Może być wykorzystany do namierzania źródeł emitujących sygnały o czasie trwania rzędu pojedynczych milisekund. Namiernik może dokonać do 200 namiarów na sekundę. Sterowanie parametrami namiernika odbywa się bezpośrednio przy użyciu klawiatury lub centralnie przy użyciu komputera. Natomiast namierniki z rodziny „600" firmy THOMSON, są automatycznymi namiernikami umożliwiającymi poszukiwanie i namierzanie emisji radiowych w zakresie częstotliwości 0,3–1350 MHz. Minimalny niezbędny czas trwania emisji namierzanej wynosi 0,5 ms. Szybkość przestrajania odbiornika namierzającego wynosi 1 GHz/s. Dokładność namierzania wynosi 0,5° w zakresie powyżej 30 MHz i 2° poniżej 30 MHz. Namiernik może być sterowany za pomocą komputera. Zobrazowanie wyników namierzania odbywa się na monitorze ekranowym, na którym są również przedstawiane podstawowe parametry techniczne rozpoznawanej emisji. W drugiej części ekranu są zobrazowane wyniki namierzania w układzie azymut–częstotliwość.

Rozpoznanie pokładowych systemów radiolokacyjnych umożliwia stacja BREŃ 2B, która jest przystosowana do określania namiaru na źródło emisji w dwóch płaszczyznach – poziomej i pionowej. Pomiar dwóch kątów położenia pokładowej stacji radiolokacyjnej, prowadzony z trzech lub dwóch posterunków, umożliwia ocenę przestrzennego położenia. Stacja BREŃ-2B zapewnia automatyczne i natychmiastowe wykrywanie sygnałów stacji radiolokacyjnych w zakresie częstotliwości 0,5–18 GHz (z możliwością jego rozszerzenia do 40 GHz). Stacja przeprowadza również analizę techniczną odbieranych sygnałów, która obejmuje pomiar częstotliwości nośnej, szerokości widma oraz parametrów czasowych wyselekcjonowanych sygnałów. W wyniku analizy danych pomiarowych następuje ostateczna klasyfikacja i identyfikacja wykrytych sygnałów radiolokacyjnych, a na tej podstawie określenie typu statku powietrznego i stopnia zagrożenia.

Zasięg rozpoznawania pokładowych urządzeń radioelektronicznych zależy od zakresu częstotliwości, na którym pracują, ponieważ fale radiowe zakresu KF rozchodzą się w przestrzeni jako fale powierzchniowe (przy powierzchni ziemi) i fale jonosferyczne, które docierają do odbiornika po odbiciu od jonosfery. Zasięg fal powierzchniowych jest znikomy ze względu na duże tłumienie wnoszone przez powierzchnię ziemi oraz ze względu na jej krzywiznę[33]. Natomiast dla fali jonosferycznej zasięg rozpoznania urządzeń radioelektronicznych jest bardzo duży (ok. kilkuset kilometrów), ponieważ fale krótkie odbijają się od jonosfery.

Zasady rozprzestrzeniania się fal ultrakrótkich i mikrofal stawiają warunek bezpośredniej widzialności anten urządzeń nadawczych i odbiorczych. Dlatego też

[33] Por. Z. Mordarski, *Środki rozpoznania i obezwładniania radioelektronicznego SP*, AON, Warszawa 1997.

na sposób ugrupowania środków rozpoznania radioelektronicznego tego zakresu częstotliwości zasadniczy wpływ ma prognozowana wysokość lotu rozpoznawanych ŚNP, od której zależy wielkość zasięgu rozpoznania radioelektronicznego.

c) stacje radiolokacyjne (radary) kontroli ruchu lotniczego

Szybki rozwój lotnictwa cywilnego spowodował, że obecnie zapanowanie nad tak nasilonym ruchem lotniczym w rejonie lotniska oraz na trasach dolotu jest niemożliwe bez radaru. Przelatujące samoloty dostosowują się do przepisów, które mają na celu zapewnienia bezpieczeństwa i płynności ruchu zgodnie z planem. Bez zastosowania radaru egzekwowanie porządku ruchu lotniczego byłoby niemożliwe.

W procesie kontroli ruchu lotniczego są wykorzystywane trzy główne kategorie radarów:

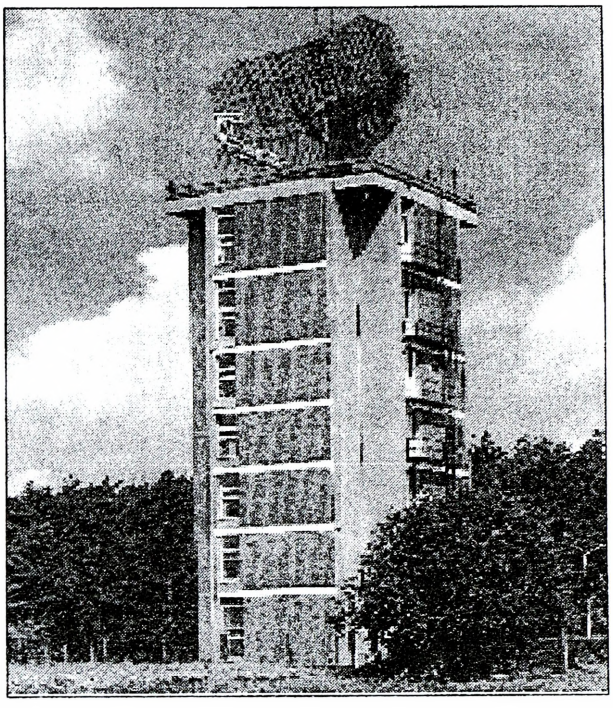
- radary kontroli tras przelotów;
- radary kontroli rejonu lotniska;
- radary kontroli lądowania.

Ze względu na możliwości tych radarów, dwa pierwsze mogą być wykorzystywane przez system rozpoznania OP jako źródło pozyskiwania informacji o sytuacji powietrznej, ponieważ charakteryzują się szczególnymi właściwościami w wykrywaniu i śledzeniu obiektów powietrznych.

Radary kontroli ruchu lotniczego pracują 24 godziny na dobę i charakteryzują się dużym wskaźnikiem bezawaryjności. Ten wynik osiągnięto przez zastosowanie struktury dwukanałowej. Zdublowanie aparatury wpłynęło na podwyższenie niezawodności sprzętu. Radary kontroli ruchu lotniczego określają współrzędne obiektu z dużą dokładnością (np. radar ASR-9 określa azymut z dokładnością $0{,}16^0$, a odległość z dokładnością 150 m). Zasięg wykrywania radarów kontroli rejonu lotniska wynosi ok. 50–110 km, natomiast radary kontroli tras przelotu od 150 do 400 km, w zależności od typu i wersji urządzenia. Radary wykorzystywane do kontroli ruchu lotniczego (np. ASR, TRAC) mogą automatycznie wykrywać i śledzić trasy do 1000 samolotów. Dane o trasach śledzonych samolotów przekazuje się do stanowisk kontrolerów ruchu lotniczego, które są wyposażone w komputerowe systemy przetwarzania danych radarowych i informacji o lotach. Do centrum kontroli ruchu lotniczego mogą być przesyłane dane z kilku radarów, z których jest tworzona ujednolicona informacja o sytuacji powietrznej. Na podstawie analizy sytuacji powietrznej i planów lotów, które są wprowadzone do systemu komputerowego, wypracowuje się sygnały alarmowe (np. o naruszeniu reżimu lotu lub w przypadku wykrycia nie zgłoszonego celu)[34].

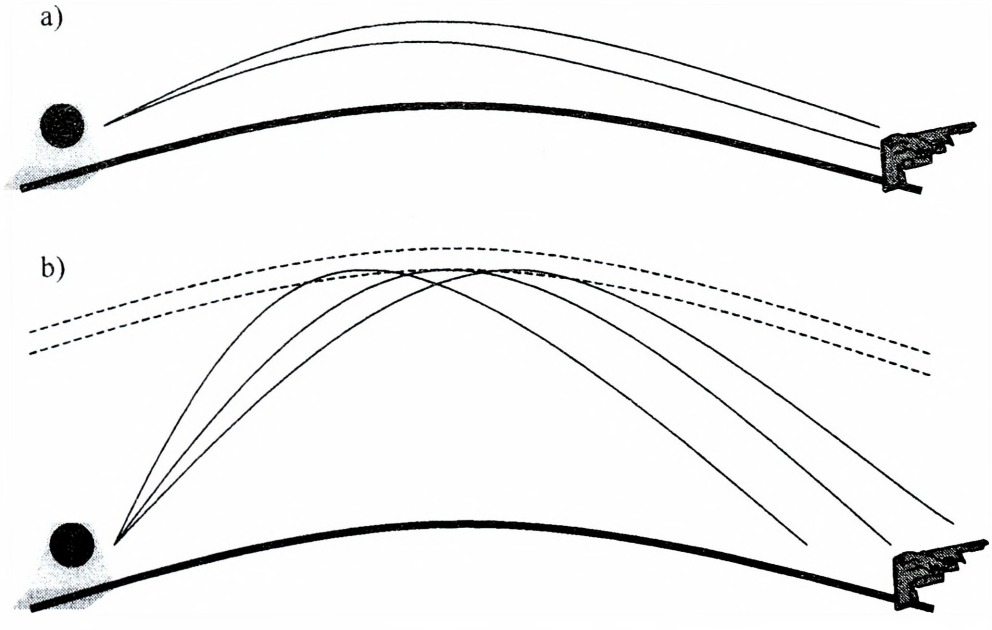
Zautomatyzowane systemy rozpoznania OP powinny posiadać możliwość odbierania ujednoliconej informacji o sytuacji powietrznej z centrum kontroli ruchu lotniczego, która może być przesyłana przez cyfrowe środki łączności.

[34] Por. Z. Czekała op. cit.



Rys. 8. Radar kontroli ruchu lotniczego AVIA CM w paśmie L

d) stacje pozahoryzontalne



Źródło: Z. Czekała, *Parada radarów*, Bellona, Warszawa 1999.

Rys. 9. Sposoby funkcjonowania radaru pozahoryzontalnego:
a) wykorzystanie ugięcia fali przyziemnej, b) wykorzystanie odbicia od jonosfery

Możliwe jest wykrywanie obiektów na znacznie większych odległościach, sięgających paru tysięcy kilometrów, ale przy wykorzystaniu fal elektromagnetycznych zakresu 3–30 MHz, czyli o długościach fali 100–10 m. Tego typu urządzenia noszą nazwę stacji pozahoryzontalnych. Wyróżnia się dwa podstawowe typy radarów pozahoryzontalnych. W pierwszym wykorzystuje się zjawisko fali przyziemnej, powstające w wyniku ugięcia drogi rozchodzenia się fali nad kulistą powierzchnią ziemi. Zjawisko to występuje na częstotliwości 3–5 MHz i umożliwia wykrywanie obiektów znajdujących się nisko nad powierzchnią ziemi na odległości 300–500 km, nieosiągalnych dla stacji klasycznych. Drugi typ stacji pozahoryzontalnych wykorzystuje zjawisko odbicia fali elektromagnetycznej od warstw jonosfery. To zjawisko występuje w zakresie częstotliwości 5–30 MHz oraz umożliwia wykrywanie obiektów na odległościach ok. 3000 km. Stacje pracujące z odbiciem fali od jonosfery nie są w stanie dokładnie określić współrzędnych obiektu, rozróżnialność zaś w określeniu pozycji wynosi 20–40 km. Można stwierdzić, że tego typu stacje zapewniają bardzo wczesne ostrzeżenie i są wykorzystywane do wczesnego wykrywania pocisków balistycznych, samolotów, okrętów itp. Jako stacje pracujące na fali dekametrowej mają cenną zaletę – wykrywają z dużym prawdopodobieństwem samoloty wykonane w technologii stealth. Stacje pozahoryzontalne posiadają także wady, takie jak sektorowe przeszukiwanie przestrzeni powietrznej, minimalną odległość wykrywania (ok. 800 km) oraz duży pobór mocy zasilającej (ok. 4 MW)[35].

Na terenie państw europejskich, należących do Sojuszu, znajduje się tylko jeden posterunek wyposażony w stację pozahoryzontalną AN/FPS-115 w Fylingdales (Wielka Brytania), która pracuje w systemie wczesnego wykrywania rakiet balistycznych (BMEWS). Posterunek ten współpracuje z zintegrowaną obroną powietrzną NATO w zakresie uprzedzania o ewentualnym ataku rakietowym na państwa Sojuszu. Stacja umożliwia wykrycie obiektów powietrznych w kierunku wschodnim z odległości około 4500 km oraz charakteryzuje się dużym prawdopodobieństwem wykrywania bardzo szybkich, nisko lecących obiektów powietrznych o małej SPO (pociski manewrujące Cruise oraz obiekty wykonane w technologii stealtch) i rakiet balistycznych na maksymalnych odległościach.

e) obserwatorzy wzrokowi

Rozpoznanie wzrokowe z użyciem przyrządów optycznych może stanowić uzupełniające źródła informacji o sytuacji powietrznej. Posterunki obserwacji wzrokowej są wystawiane w wyższych stanach gotowości bojowej w rejonie rozmieszczenia pododdziałów, oddziałów i związków taktycznych wszystkich rodzajów wojsk i sił zbrojnych. Celem tego rodzaju rozpoznania jest zwiększenie ciągłości śledzenia obiektów powietrznych nisko lecących, szczególnie obiektów wykonujących zadania poza strefą rozpoznania radiolokacyjnego i radioelektronicznego, w tzw. strefie martwej[36].

---

[35] Zob. Z. Czekała, op. cit.

[36] Zob. Z. Groszek, *Rozpoznanie w obronie powietrznej RP*, AON, Warszawa 1996.

Zasadniczym zadaniem obserwatorów wzrokowych jest wykrywanie obiektów powietrznych i natychmiastowe składanie meldunków do stanowisk dowodzenia przez techniczne środki łączności.

Konkluzje:

Zdobywanie informacji jest uznawane za jeden z najważniejszych warunków skutecznego prowadzenia działań bojowych przez aktywne środki walki OP, a systemy zdobywania informacji stały się trwałym elementem uzbrojenia wielu państw. Ich posiadanie staje się obecnie koniecznością. Nowoczesny system jest w stanie dostarczyć aktywnym środkom walki sił powietrznych informację o wymaganych parametrach. Dzięki temu mogą one prowadzić efektywną walkę ze współczesnymi powietrznymi środkami walki.

Analiza ostatnich konfliktów zbrojnych potwierdza, że powietrzne i kosmiczne systemy są jednym z najbardziej rozwijających się elementów współczesnego uzbrojenia.

Konflikt w Zatoce Perskiej spowodował dalszy wzrost zainteresowania problematyką zdobywania informacji o sytuacji powietrznej, szczególnie w zakresie wykrywania startu i określania trajektorii lotu taktycznych rakiet balistycznych.

Państwa nie mające powietrznych i kosmicznych systemów, doceniając korzyści z ich posiadania, drogą współpracy z innymi krajami, starają się uzyskać dostęp do informacji pochodzących z takich systemów.

ppłk dr inż. Gabriel Nowacki
mjr mgr inż. Wiesław Błażejczyk

Zakład Rozpoznania Wojskowego i Walki Radioelektronicznej
Instytut Dowodzenia AON

ZAGROŻENIA INFORMACYJNE W OBRONIE POWIETRZNEJ

Wprowadzenie

Jednym spośród uniwersalnych wyzwań społeczeństw świata jest bezpieczeństwo. Pomimo wielu wojen, w tym światowych, pozostało ono potrzebą globalną i jest zachowywane. Podstawowym gwarantem bezpieczeństwa narodu są jego siły zbrojne, które poprzez odpowiednie modelowanie, wdrażanie nowej myśli naukowej i technicznej są wstanie zapewniać bezpieczeństwo nawet w szybko zmieniającym się środowisku zewnętrznym.

Siły zbrojne i organy państwa mogą skutecznie realizować swoją politykę i zadania długookresowe tylko wtedy, gdy bliższe i dalsze otoczenie będzie im przyjazne oraz znane, to znaczy, gdy odpowiednie organizacje państwowe i wojskowe będą dysponowały określonymi danymi o otoczeniu.

Zmieniające się uwarunkowania prowadzenia działań bojowych na wszystkich szczeblach sił zbrojnych oraz wzrastające zagrożenie terroryzmem (w ogólnym pojęciu) i zorganizowaną przestępczością powodują, że niezbędne stało się określenie nowych zadań dla rozpoznania wojskowego NATO. Są one konieczne w procesie kształtowania polityki bezpieczeństwa, planowania obronnego i operacyjnego. Przedstawione zostały w koncepcji strategicznej Sojuszu Północnoatlantyckiego, wytycznych ministerialnych, decyzji Rady Północnoatlantyckiej oraz Komitetu Wojskowego.

Dysponowanie danymi uzyskanymi w wyniku działalności rozpoznawczej, stanowi istotny element zarządzania państwem i siłami zbrojnymi. Dane te niezbędne są także do przeciwdziałania współczesnym zagrożeniom, takim jak wymieniony już terroryzm czy zorganizowana przestępczość, ale również militarnym oraz społecznym i cywilizacyjnym. W związku z tym, każde suwerenne państwo dąży i będzie dążyć do skutecznego budowania systemu rozpoznania i przeciwdziałania rozpoznaniu ze strony potencjalnego przeciwnika, w tym organizacji przestępczych, terrorystycznych oraz przeciwdziałania określonym zagrożeniom zarówno w czasie pokoju, jak i wojny.

Od zakończenia wojny w rejonie Zatoki Perskiej zaczęto przywiązywać dużą wagę do nowych środków przemocy, których zastosowanie w czasie wojny – i nie tylko – okazuje się wysoce skuteczne z punktu widzenia osiągnięcia zwycięstwa nad przeciwnikiem. Środki te są często nazywane nieśmiercionośnym arsenałem broni. Ich przykładem mogą być paski folii z włókna węglowego, które rozproszone nad systemami energetycznymi w czasie wojny w rejonie Zatoki Perskiej spowodowały wyłączenie prądu bez niszczenia zakładów energetycznych, a tym samym unieruchomiły pracę systemu obrony powietrznej Iraku. W epoce informacji na szeroką skalę mogą być stosowane: mikroprocesory, bardzo szybkie systemy odbioru i obróbki danych, skomplikowane czujniki oraz specjalne wirusy, które zainfekowane w systemach broni potencjalnego przeciwnika spowodują ich dezorganizację i nieefektywność. Urządzenia wytwarzające impuls elektromagnetyczny[1] (wielkości walizki) są już projektowane w Laboratorium Narodowym Stanów Zjednoczonych w Los Alamos. Infradźwięki o częstotliwości 16 Hz używane przeciwko sile żywej powodują wzbudzanie wibracji w organach wewnętrznych, powstanie nudności, dolegliwości sercowych i zaburzeń równowagi. Ponadto mogą być stosowane promienniki równokierunkowe (izotropowe, w formie amunicji artyleryjskiej lub lotniczej) w celu porażenia czujników, dezorientowania pilotów czy nawet oślepienia żołnierzy. Wzrost roli nieśmiercionośnych czynników jest trendem rozwojowym, świadczącym o nowych możliwościach, jakie się otwierają przed pozazbrojnymi formami walki w działaniach wojennych. Nie można oczywiście twierdzić, że maleje znaczenie walki zbrojnej w wojnie. Jednak już dziś, a tym bardziej w przyszłości, nie musi już ona być jedynym i decydującym czynnikiem o rezultacie wojny. Narastająca zależność potencjału obronnego od ekonomiki, techniki i ideologii (w sensie świadomości społecznej, społecznych przekonań i dążeń) doprowadziła do sytuacji, w której można już mówić o przemocy ekonomicznej, naukowo-technicznej i ideologicznej. Środki, metody i formy tej przemocy bardzo się wzbogaciły, szczególnie w ostatnich dziesięcioleciach. Coraz częściej w sferze pozamilitarnych form walki szukać się będzie możliwości obrony lub ataku, uzyskania równowagi lub przewagi, a być może decydujących rozstrzygnięć. Możliwości takie zapewniają narzędzia walki informacyjnej, które stają się potencjalnym zagrożeniem dla funkcjonowania systemu obrony powietrznej.

Potencjalny przeciwnik może zadać poważne straty bez użycia tradycyjnych sposobów walki oraz narażania własnych sił i środków. Oddziałując tylko na systemy informacyjno-sterujące, przeciwnik może obezwładnić czy wręcz zniszczyć istotne elementy infrastruktury cywilnej i wojskowej. Ponadto atakujący może ukryć swoją tożsamość, a zaatakowane państwo nie będzie w stanie jednoznacznie wskazać agresora. Wynika z tego, że walka o informację staje się realnym zagro-

[1] Impuls elektromagnetyczny – impuls fal radiowych o czasie trwania rzędu tysięcznych części sekundy. Charakteryzuje się bardzo dużą amplitudą zmian natężenia pola elektrycznego i magnetycznego. Powoduje indukowanie się prądów i napięć w obwodach urządzeń elektronicznych, co jest przyczyną niszczenia niektórych elementów półprzewodnikowych na skutek przeciążeń. Zasadniczymi obiektami oddziaływania impulsu elektromagnetycznego są środki radioelektroniczne.

-żeniem dla bezpieczeństwa narodowego. Aby się przed tym uchronić, potrzebna jest wiedza o stanie otoczenia i rodzących się przesłankach zagrożeń, które z natury rzeczy będą utrzymywane przez zainteresowanego w jak największej tajemnicy. Trzeba je będzie zdobywać i stosownie do tego kształtować przestrzeń bezpieczeństwa państwa w sferze ekonomicznej, politycznej i militarnej. Są to argumenty przemawiające za potrzebą ciągłego doskonalenia i rozwijania narzędzi walki informacyjnej.

Problematyka ta jest sensu proprio dostrzegana w wielu państwach na świecie. Najwyższą jednak rangę nadano jej w Stanach Zjednoczonych. W sierpniu 1996 roku Dowództwo Szkolenia i Doktryn (TRADOC – Trainining and Doctrine Command) opublikowało *Regulamin walki sił lądowych USA*" (FM–100–6) zawierający doktrynę[2] operacji informacyjnych. Zgodnie z nią wszelkie działania wojskowe Stanów Zjednoczonych mają się opierać na koncepcji tworzenia wieloczynnikowej przewagi militarnej (multifactor military superiority). Kluczem do jej uzyskania jest przewaga informacyjna (information superiority) i technologiczna (technological superiority).

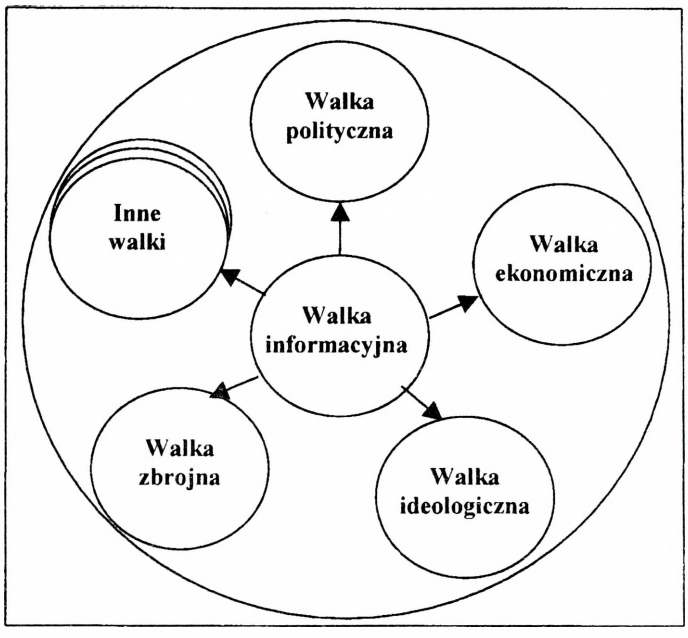
W kwietniu 1999 roku została przyjęta nowa *koncepcja strategiczna NATO*, w której podkreśla się znaczenie technologii informacyjnych na współczesnym polu walki. W związku z koncepcją Rosja opracowała nową doktrynę wojenną, w której w większym niż dotychczas zakresie podkreślono znaczenie bezpieczeństwa informacyjnego, którego jednym z zasadniczych elementów ma być prowadzenie wielopłaszczyznowej walki informacyjnej.

Prowadzone konflikty zbrojne (szczególnie wojna w rejonie Zatoki Perskiej) dowiodły, że o odniesionym sukcesie w głównej mierze decyduje walka informacyjna.

Walkę informacyjną zawsze się prowadzi wespół z innymi walkami – nigdy nie może występować w oderwaniu, bo nigdy też sama dla siebie nie może stanowić celu. Jej cel wynika zawsze z charakteru i celu walki wspieranej (rys. 1).

---

[2] Doktryna – podstawowe zasady, którymi kierują się SZ lub ich elementy w trakcie działalności zmierzającej do osiągnięcia celów państwowych. W literaturze zachodniej termin „doktryna" jest najczęściej używany w odniesieniu do zasad działania wyspecjalizowanych struktur wojskowych (doktryna SL, SP, wojsk specjalnego przeznaczenia itd.), które są zbiorami ustaleń normatywnych zawierającymi szczegółowe instrukcje określające sposób prowadzenia działań bojowych. Doktrynę można porównać do koncepcji działań. Wojska prowadzą działania w sposób określony przez doktrynę, opracowaną z uwzględnieniem ustaleń obowiązującej koncepcji strategicznej oraz możliwości bojowej wojsk.

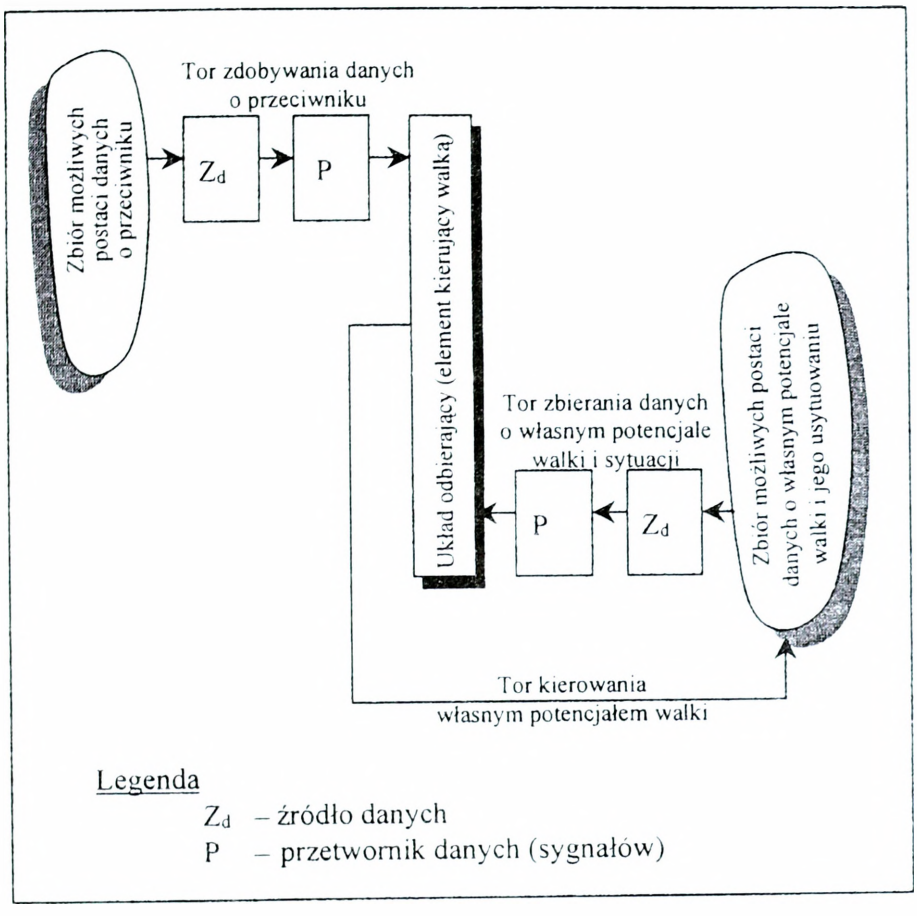


Rys. 1. Miejsce funkcjonalne walki informacyjnej w zbiorze walk

Podczas każdego rodzaju walki zawsze jest organizowany określony system informacyjno-sterujący. (Dotyczy to tak samej walki informacyjnej, jak i walk przez nią wspieranych). Jego struktura i zasady funkcjonowania mogą być różne. Jednak zawsze są dostosowywane do konkretnych potrzeb określonej walki. W swej różnorodności systemy te posiadają także pewne cechy wspólne. Każdy i zawsze przeznaczony jest do spełniania trzech podstawowych funkcji – zdobywania danych o przeciwniku, zbierania danych o własnym potencjale walki i jego sytuacji oraz kierowania własnym potencjałem walki (rys. 2).

Taka struktura systemu informacyjno-sterującego jest determinowana potrzebami decyzyjnymi. W każdym rodzaju walki odbywa się przecież dowodzenie i zarządzanie własnym potencjałem. Muszą być więc podejmowane odpowiednie decyzje. W ramach tego procesu każdy zaangażowany podmiot dąży do wypracowania takich decyzji, aby po ich wdrożeniu do realizacji pokonać swojego negatywnego kooperanta. Dąży zatem do wypracowywania decyzji możliwie najtrafniejszych w danej sytuacji. Do osiągnięcia tego niezbędna jest jednak wiedza o0stanie, usytuowaniu oraz możliwościach i zamiarach wykorzystywania narzędzi walki przez przeciwnika i o panującej u niego sytuacji. Tak samo jest niezbędna wiedza o własnym potencjale walki. Posiadanie tych danych stanowi podstawę świadomego wypracowywania poprawnych decyzji. Luki w zasobach wiedzy z tej dziedziny powodują podejmowanie decyzji ryzykownych, o nie dających się przewidywać skutkach. Nie mniej ważny od wypracowywania decyzji jest również proces jej wdrażania do realizacji. W tym względzie szczególną rolę odgrywa terminowość i skrytość wykonywania poszczególnych przedsięwzięć. Nawet najtraf-

niej podjęte decyzje nie spowodują osiągnięcia sukcesu, jeśli zostaną wdrożone nieterminowo lub wcześniej ujawnione negatywnemu kooperantowi. Przy porównywalnych potencjałach sukces może osiągnąć tylko ta strona, która zdoła szybciej i trafniej od przeciwnika wykorzystać swój potencjał do walki z nim.



Rys. 2. Funkcjonalna rola systemu informacyjno-sterującego

W kooperacji negatywnej wzajemnej, oprócz działań zasadniczych toczy się jeszcze walka o szybkość reakcji i trafność działania (walka o czas i walka o precyzję działania). W tej właśnie sferze – w walce o czas i o precyzję działania – mieści się funkcjonalna rola walki informacyjnej. Jako że przedmiotem tej walki są systemy informacyjno-sterujące, jej efekty będą się materializować w sprawności i skuteczności ich funkcjonowania. Stany te będzie odzwierciedlać:

- sprawność i skuteczność działania toru zdobywania danych o przeciwniku;
- sprawność i precyzja działania toru zbierania danych o własnym potencjale walki i panującej tam sytuacji;
- sprawność funkcjonowania organów kierowania walką;
- stopień uzyskiwanej skrytości sytuacyjnej.

Wynika z tego, że walka informacyjna tak w rozumieniu rzeczowym, jak i czynnościowym jest częściowo ulokowana wewnątrz systemu informacyjno-sterującego, a częściowo w jego otoczeniu.

W zależności od przyjętego stopnia szczegółowości system informacyjno-sterujący jednego z kooperantów negatywnych możemy traktować jako całość lub też rozpatrywać poszczególne jego podsystemy i podsystemy podsystemów. Zauważyć należy, że w systemie informacyjno-sterującym kooperanta, typu np. wojsk lądowych, można wyróżnić niezliczoną[3] ilość podsystemów informacyjno-sterujących, działających we wszystkich przestrzeniach wyróżnionych zarówno według kryterium sposobu oddziaływania, kontaktu narzędzi z przedmiotem walki informacyjnej, jak i według kryterium środowiska nośnika treści informacyjnych. Ten zbiór cząstkowych podsystemów skorelowanych organizacyjnie i funkcjonalnie, tworzy w sumie system informacyjno-sterujący strony biorącej udział w walce informacyjnej. Postulować można, że każdy system informacyjno-sterujący militarnej przestrzeni walki informacyjnej da się rozłożyć według określonego kryterium na skończoną liczbę elementarnych układów informacyjnych[4] (takich, dla których dalsza dezagregacja na podukłady przestaje być celowa).

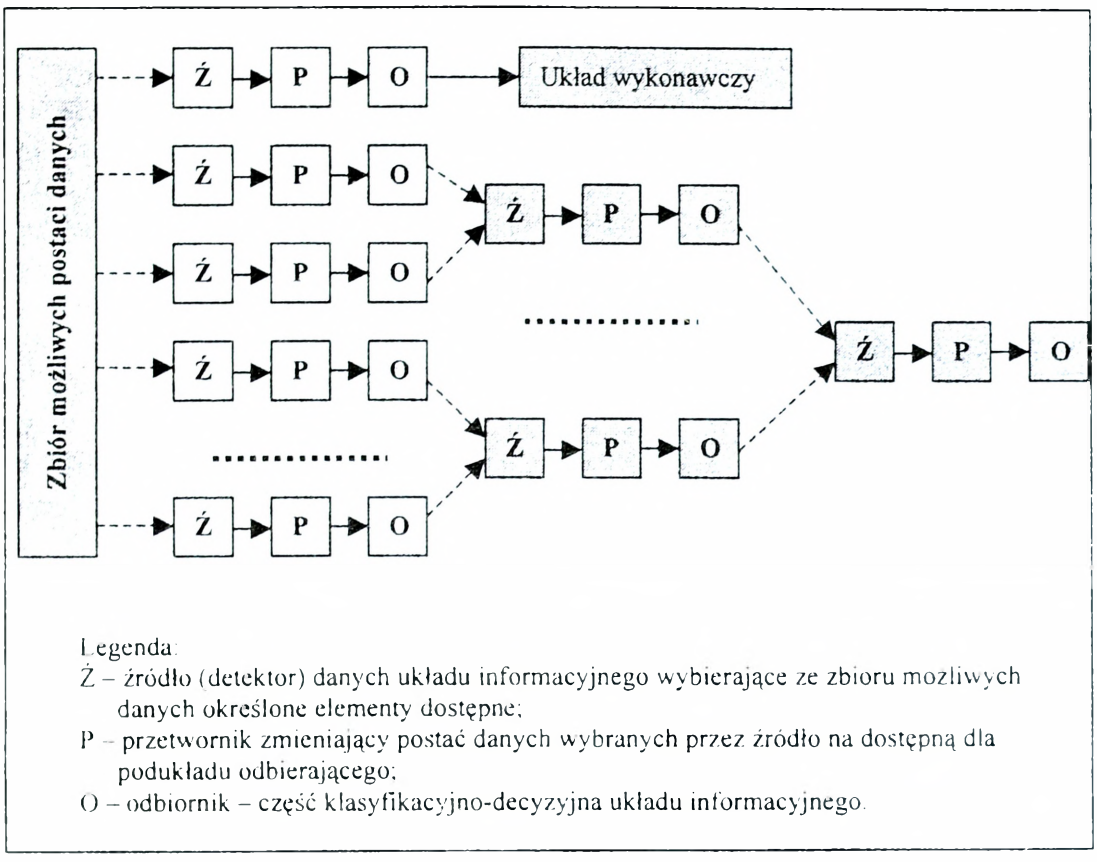
W rozumieniu opisywanej walki informacyjnej, jako wspomniany układ elementarny należy traktować układ informacyjny przystosowany do wybierania ze zbioru możliwych postaci danych jednej określonej ich postaci i przetwarzania jej na inną postać stanowiącą element zbioru możliwych postaci danych innych układów systemu informacyjno-sterującego lub też stanowiącą sygnał sterujący dla elementów wykonawczych funkcjonujących zarówno wewnątrz systemu informacyjno-sterującego, jak i należących do systemu wspieranego. Przyjmując uproszczoną strukturę układu informacyjnego w postaci: źródło–przetwornik–odbiornik, strukturę fragmentu systemu informacyjno-sterującego możemy przedstawić w postaci ukazanej na rys. 3.

Zbiór pierwotnych elementarnych układów informacyjno-sterujących (jasny kolor na rys. 3.) grupuje układy informacyjne oparte na źródłach przystosowanych do wybierania ze zbioru możliwych postaci danych treści informacyjnych należących do różnych środowisk, zapewniając w efekcie ich równoległe funkcjonowanie oraz możliwie maksymalnie multiśrodowiskowy i multispektralny nabór i przetwarzanie danych.

---

[3] Przykładowo każdy żołnierz na polu walki może być w sensie informacyjnym traktowany zarówno jako swoisty zbiór elementarnych układów informacyjnych (system informacyjny), jak też element innych systemów informacyjnych.

[4] Układ informacyjny – układ, który ma choć jedno wejście informacyjne oraz choć jedno wyjście informacyjne, a więc jest jednocześnie układem informującym i układem informowanym, *Mały słownik cybernetyczny*, Wiedza Powszechna, Warszawa 1973, s. 47.



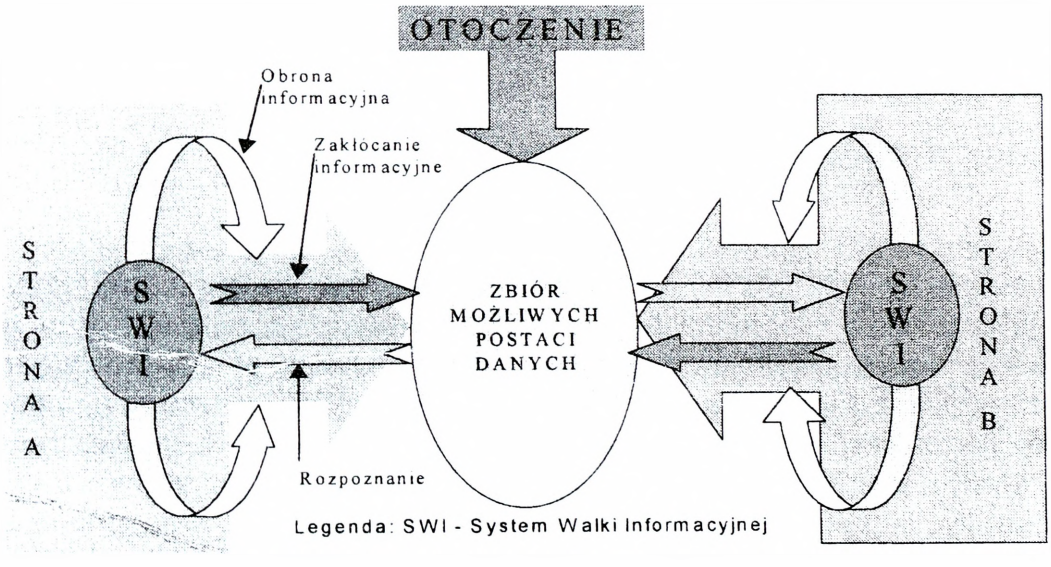
Rys. 3. Model struktury systemu informacyjno-sterującego jako zbioru uporządkowanych sekwencji elementarnych układów informacyjnych

Celem walki informacyjnej jest dążenie do stworzenia przeciwnikowi fałszywego obrazu rzeczywistości po drugiej stronie toczących się zmagań i przez to ukierunkowanie jego wysiłków na planowanie i prowadzenie działań w stosunku do nieistniejących lub nieistotnych odniesień. Innymi słowy, jest to niezmiernie złożony proces kierowania działaniami przeciwnika przez podmiot mu przeciwny i w nieznany mu sposób. Dlatego też paleta podejmowanych w tym zakresie wysiłków musi być niezmiernie spójna i precyzyjnie dobierana. Rzeczywiste plany muszą być utrzymywane w największej tajemnicy, a wprowadzanie w błąd przeciwnika musi od początku do końca sprawiać pozory realizmu reżyserowanej sytuacji. Nieprzestrzeganie tych reguł może doprowadzić do sytuacji, że własna strona zamiast reżyserem, stanie się nieświadomym narzędziem manipulacji w rękach przeciwnika i w ten sposób zostanie wyprowadzona na przegraną pozycję w każdej sferze podjętej negatywnej kooperacji.

W torze zdobywania danych o przeciwniku istota walki informacyjnej sprowadza się do tego, że jeden z jej podmiotów stara się wszelkimi sposobami zdobyć

jak najwięcej prawdziwych danych o stanie, usytuowaniu, możliwościach działania oraz planach i zamiarach przeciwnika. Stosownie do tego tworzy, na bazie dostępnych mu narzędzi, system rozpoznania dostosowany do realizacji tego zadania. Drugi z podmiotów stara się, z podobnym zaangażowaniem, czynić wszystko, aby udaremnić przeciwnikowi osiągnięcie celu, a jeśli jest to niemożliwe, to przynajmniej maksymalnie utrudnić. Stosownie do tego tworzy na bazie dostępnych mu narzędzi, system zakłócania rozpoznania i system obrony informacyjnej zbioru własnych postaci danych. W tym torze (zdobywanie danych o przeciwniku) przedmiotem walki jest zbiór możliwych postaci danych o przeciwniku.

Zbiór ten jako taki, mieści w sobie potencjał informacyjny, a dane o przeciwniku mają nieskończoną liczbę postaci. Ich chwilowo identyfikowane formy są tylko odzwierciedleniem mocy rozpoznawczej określonego systemu zdobywania danych. Zależy to, przede wszystkim od stopnia dostosowania narzędzi do realizacji zadań rozpoznawczych. Kooperanci negatywni wzajemnie dążą zatem do wcześniejszego poznania tych możliwości u swojego przeciwnika. Jeśli to osiągną, będą świadomi, do których postaci danych może być organizowany dostęp rozpoznawczy. Dlatego też, stosując odpowiednie narzędzia, każdy z nich stara się walczyć z systemem rozpoznania swojego kooperanta negatywnego przez stosowanie odpowiedniej obrony danych i zakłócanie toru ich zdobywania, tworząc w tym celu odpowiednie systemy.



Rys. 4. Model systemu walki informacyjnej

Obrona zbioru postaci danych może być realizowana różnymi sposobami i narzędziami. Jako że dotyczy obrony pewnej potencji informacyjnej, można ją nazywać *obroną informacyjną*, a użyte narzędzia – *narzędziami obrony informacyjnej*. Istota tej obrony sprowadza się do stwarzania warunków uniemożliwiających przeciwnikowi przechwytywanie danych, szczególnie zaś tych ich postaci,

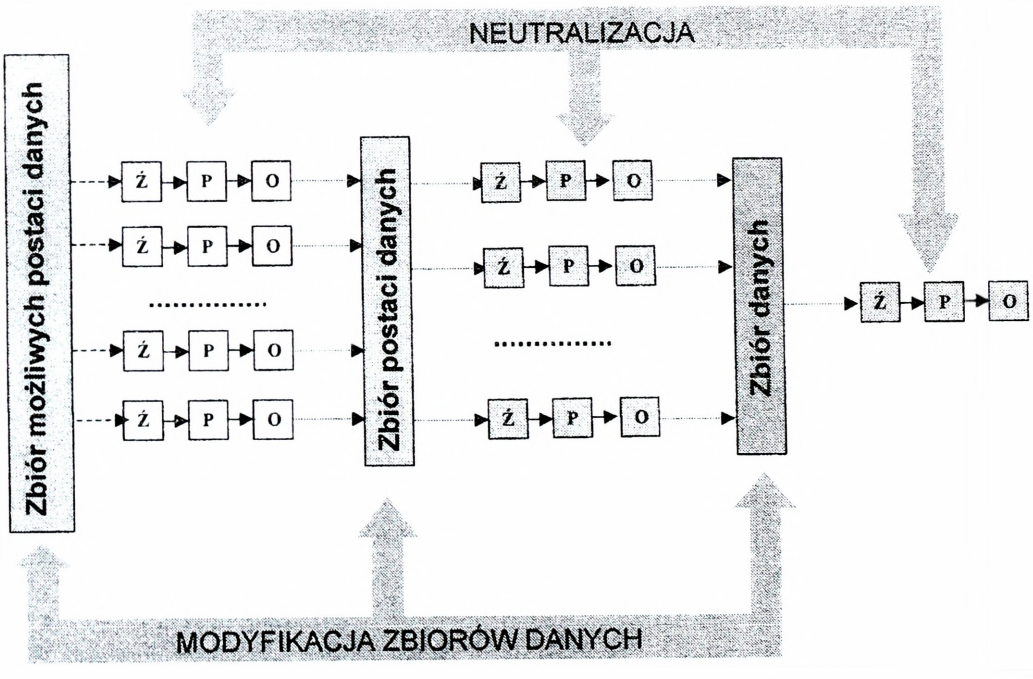
które zawierają największą potencję informacyjną o ważnych sytuacjach rzeczywistych. Nie zawsze jednak istnieje możliwość osiągnięcia tego. Nie zawsze też pewne postacie danych można ukryć. Dlatego w ramach obrony informacyjnej jest stosowane *ukrywanie danych*. Jego istota sprowadza się do stosowania takich rozwiązań, które powodują tylko zmianę wartości potencjału informacyjnego określonych postaci danych. Przykładem tego może być chociażby technika stealth, która nie tylko ukrywa określony obiekt, ale również i dezinformuje, że takiego zupełnie nie ma. Ma to też pewien związek z zakłócaniem informacyjnym, ale do tego celu przeznaczony jest głównie system zakłócania toru zdobywania danych, który (na tych samych zasadach jak poprzednio) można nazywać *systemem zakłócania informacyjnego*, a spełniane przez niego funkcje – *zakłócaniem informacyjnym*. Informacyjne zakłócanie toru zdobywania danych może być także prowadzone różnymi sposobami i przy wykorzystywaniu różnych narzędzi. Jego rola funkcjonalna jest jednak bardziej złożona niż obrony informacyjnej. System ten spełnia nie tylko jedną, ale dwie podstawowe funkcje. Chociaż służy do zwiększania entropii informacyjnej w torze zdobywania danych, to jednak funkcję tę realizuje drogą stosowania szeroko rozumianej pozoracji i drogą fizycznej destrukcji jego elementów technicznych.

W systemie informacyjno-sterującym odrębnymi przedmiotami walki informacyjnej są elementy kierujące walką i sterujące jej określonymi procesami. Przy walkach bardziej złożonych, w organach takich (centrach) szeroko stosuje się dzisiaj technikę informatyczną i różnego rodzaju urządzenia elektroniczne. Wykorzystuje się je do rejestrowania i gromadzenia danych, ich analizowania, segregowania i przechowywania oraz do wypracowywania decyzji i przekazywania tych decyzji wykonawcom. Tym samym są to najbardziej newralgiczne punkty w strukturze każdego systemu informacyjno-sterującego, zorganizowanego na potrzeby dowolnego rodzaju walki. Można nawet stwierdzić, że od sprawności ich funkcjonowania zależy sukces bądź porażka w każdym rodzaju złożonej kooperacji negatywnej wzajemnej. Dlatego też elementy te, jako przedmioty oddziaływania, są szczególnym obiektem zainteresowania walki informacyjnej. Dla strony przeciwnej są obiektami rozpoznania i zakłócania informacyjnego, dla własnej – pieczołowitej obrony informacyjnej.

Efektywność walki informacyjnej zależy od wielu czynników. W pierwszej kolejności decyduje o tym trafność doboru narzędzi i form ich wykorzystywania w procesie oddziaływania na wyselekcjonowane przedmioty walki. Inne narzędzia i formy muszą być stosowane przy wspieraniu każdego rodzaju walki – inne przy wspieraniu walki politycznej, inne przy wspieraniu walki ekonomicznej i jeszcze inne przy wspieraniu walki zbrojnej. Tak samo inne zestawy narzędziowe i inne formy oddziaływania konieczne są do stosowania w obrębie tego samego systemu informacyjno-sterującego. Ich zróżnicowanie wynika z niejednorodności strukturalnej tego systemu. Inne muszą być zastosowane w torze zdobywania danych o przeciwniku, inne w torze zbierania danych, inne w torze kierowania i jeszcze inne w stosunku do elementów kierujących (sterujących) walką. Również w wymienionych torach, jako w przedmiotach oddziaływania, problemy te nie mogą być

rozwiązywane jednakowo. Każdy z nich stanowi odrębną i właściwą tylko sobie złożoność rzeczową i czynnościową. Warunkowane jest to zawsze konkretnymi potrzebami i możliwościami organizacyjnymi konkretnych użytkowników. Przy całej złożoności walki informacyjnej można jednak wyróżnić pewne reguły, których przestrzeganie będzie sprzyjać sukcesowi. Oprócz wymienionej już kompatybilności narzędziowo-przedmiotowej, należy też pamiętać, że *walka informacyjna powinna zawsze wyprzedzać walkę wspieraną. Najpierw należy wygrać w walce informacyjnej, aby osiągnąć sukces w walce wspieranej (zasadniczej).*

Z punktu widzenia potrzeb prowadzenia walki informacyjnej, ważna jest wcześniejsza i bieżąca wiedza o przedmiotach tej walki i ich otoczeniu. Tylko taki stan informacyjny może stanowić podstawę trafnego doboru narzędzi i form walki, a co za tym idzie – przeprowadzenia skutecznego działania. Każda reakcja celowa musi być zawsze poprzedzona rozpoznaniem przedmiotu, na który będzie skierowana i warunków jego usytuowania. Jeśli określone działanie celowe, w tym wypadku walka informacyjna, składa się z szeregu równoległych, a także następujących po sobie reakcji, to każda kolejna reakcja musi być poprzedzona rozpoznaniem efektów reakcji poprzedniej, jeśli ma być trafna. Proces ten w ujęciu dynamicznym staje się jak gdyby łańcuchem składającym się z przemiennie spiętych ogniw rozpoznania i reakcji. Rozpoczyna się zawsze od tego, że każda pierwsza reakcja musi być poprzedzona rozpoznaniem przedmiotu tej reakcji.



Rys. 5. Możliwości oddziaływania na zbiory danych i elementy funkcjonalne systemu informacyjnego

Walka informacyjna i wszystkie wspierane nią walki są również działaniami celowymi. Realizowane są zawsze w aspekcie osiągnięcia konkretnych zamiarów. Dlatego związane z nimi działania, stanowią również łańcuch przeplatających się ogniw rozpoznania i reakcji. Dlatego wszystkie podstawowe formy walki informacyjnej – rozpoznanie, zakłócanie i obrona informacyjna – nie mogą być stosowane w oderwaniu od siebie i w oderwaniu od każdej walki wspieranej. Tylko ich ścisłe zespolenie jednolitymi regułami gry może sprzyjać walce wspieranej. W innym wypadku mogą tylko szkodzić. Można zatem przyjąć, że szeroko rozumiane: centralizacja, kompleksowość, spójność, wiarygodność, nieszablonowość, skrytość, terminowość, ciągłość i elastyczność – to dziewięć podstawowych zasad, które powinny być przestrzegane w każdej formie i przestrzeni prowadzonej walki informacyjnej. Zakres ich przestrzegania będzie się zawsze przekładać na trafność i szybkość reakcji podejmowanych w każdej walce wspieranej, to znaczy na dwa główne elementy, które decydują o sukcesie lub porażce każdego podmiotu funkcjonującego w kooperacji negatywnej wzajemnej (w walce).

Narzędzia walki informacyjnej zagrożeniem dla systemu obrony powietrznej

Jednym z najważniejszych czynników decydujących o powodzeniu obrony powietrznej jest szybkość uzyskiwania informacji o celach powietrznych.

„Informacja" to takie komunikaty lub dane, które zmniejszają stopień niewiedzy (entropię informacyjną) o badanym zjawisku, a tym samym umożliwiają jej rzeczywistym lub potencjalnym użytkownikom na polepszenie znajomości otoczenia i sprawniejsze przeprowadzenie celowego działania.

Przyjęcie tego podejścia oznacza, że:

– po pierwsze człowiek ma do czynienia nie z zalewem informacji, a z zalewem komunikatów (danych), z których dopiero, stawiając określone pytania, może wyłowić informacje (a więc te komunikaty lub kombinacje komunikatów, które zawierają odpowiedź na postawione pytania);

– po drugie zdolność do pozyskiwania informacji jest równoznaczna z dysponowaniem wiedzą umożliwiającą stawianie właściwych pytań i umiejętnością ich stawiania, co akcentuje aktywną rolę jednostki lub organizacji nie tylko na etapie budowy systemów informacyjnych, lecz także przy ich wykorzystywaniu;

– po trzecie informacja stanowi wartość subiektywną, której każdy człowiek lub każda organizacja nadaje swoją indywidualną wagę i indywidualną interpretację.

W radiolokacji informacja nie występuje w czystej formie, tylko w postaci sygnałów. Stacja radiolokacyjna rozpatrywana jako element systemu informacyjno-sterującego w większości przypadków jednocześnie spełnia funkcję źródła informacji i przetwornika, stanowiąc ogniwo pośrednie pomiędzy otaczającą przestrzenią i operatorem, będącym pierwotnym elementem odbierającym. Umożliwia ona

uzyskanie danych, które w wyniku obiektywnych, naturalnych ograniczeń nie są dla tego operatora dostępne.

Dla stacji radiolokacyjnej kryterium dostępności postaci danych w otaczającej przestrzeni stanowi możliwość odebrania przez jej odbiornik echa własnego (wysyłanego) sygnału sondującego, odbitego od obiektów w tej przestrzeni. Owa dostępność jest warunkowana ograniczeniami: geometrycznymi (zasięg, horyzont radiowy, miejsce zamontowania, ukształtowanie terenu itp.), technologicznymi (zakres częstotliwości, rodzaj i struktura sygnału, wydajność energetyczna, kształt charakterystyki antenowej, rozróżnialność), przeznaczeniem (wykrywanie tylko celów ruchomych, śledzenie wybranego celu, tworzenie mapy terenu itp.).

W radiolokacji zbiór możliwych danych nie jest tworzony przez rzeczywiste (istniejące) obiekty, ale przez fale elektromagnetyczne, z których część stanowią echa odbitych sygnałów sondujących. W tym wypadku pierwszy element systemu informacyjnego – stacja radiolokacyjna – bierze aktywny udział w tworzeniu zbioru dostępnych dla niego postaci danych poprzez determinowanie otaczającej przestrzeni do tworzenia własnego obrazu w dostępnej dla niego formie.

Zasadne wydaje się zatem pytanie, czy sygnał radiolokacyjny (pierwotny i odbity) jest nośnikiem informacji? Otóż należy sądzić, że w tym wypadku występuje zjawisko względności w odniesieniu do informacji. Sygnał pierwotny (sondujący) wysyłany przez stację radiolokacyjną jest, z jej punktu widzenia (jako źródła informacji), pozbawiony wartości informacyjnych ze względu na swój w pełni zdeterminowany charakter, czyli posiadaną przez system pełnię znajomości parametrów. Nośnikiem informacji jest oczywiście sygnał odbity od obiektu, stanowiący, jak wspomniano wcześniej, poszukiwany element zbioru dostępnych postaci danych dla tej stacji radiolokacyjnej. Dokładnie odwrotnie przedstawia się sytuacja z punktu widzenia stacji rozpoznania sygnałów radiolokacyjnych, dla której sygnał sondujący stanowi poszukiwany element zbioru jej dostępnych postaci danych, natomiast sygnał odbity może stanowić jedynie szkodliwy sygnał zakłócający jej pracę.

Pod pojęciem sygnału odbitego należy rozumieć tylko tę część sygnału, który obijany jest w kierunku odbiornika (odbiorników) stacji radiolokacyjnej wysyłającej sygnał. Stacja radiolokacyjna, traktowana jako element systemu informacyjnego, stanowi również swoisty przetwornik, zamieniając wybrane sygnały elektromagnetyczne na postać dostępną dla kolejnych członów systemu. W zależności od rodzaju układu odbierającego różna jest liczba koniecznych przekształceń sygnału ze źródła danych oraz jego dostępna postać końcowa, jak również sygnały te, w końcowym efekcie, mogą mieć postać sygnałów informacyjnych lub sterujących.

Aby zniszczyć samolot czy rakietę przeciwnika, obieg informacji o zagrożeniu, podjęcie decyzji i przekazanie ustaleń do poszczególnych jednostek, muszą być szybsze niż nadlatujące samoloty lub pociski. Tu nie wystarczą tradycyjne sposoby łączności. Współczesny samolot w ciągu minuty przelatuje około 20 km. Systemy OP muszą być szybsze. Pomocne w tym są komputerowe systemy dowodzenia, które po zlokalizowaniu samolotu przeciwnika podają współrzędne i rodzaj broni jaką należy go zniszczyć. Wszystkie te dane są przekazywane elementom OP, któ-

rych zadaniem będzie zniszczenie celów powietrznych. Jednym ze skuteczniejszych środków walki informacyjnej, który może sparaliżować system obrony powietrznej, jest *impuls elektromagnetyczny*. Laboratorium w Los Alamos opracowało projekt takiej bomby (wielkości walizki), która może być zrzucana przez samoloty lub pozostawiana przez dywersantów w ważnych obiektach przeznaczonych do zniszczenia. Doświadczenia pokazują, że charakter oddziaływania impulsu elektromagnetycznego zależy od długości fali. Jeśli jej długość jest większa od rozmiarów obiektu, to na obudowach urządzeń elektronicznych powstają duże prądy i napięcia, co może być przyczyną naruszenia zakładanego przepływu prądów i napięć użytkowych pracujących wewnątrz urządzeń i w rezultacie ich uszkodzenie. Długofalowy impuls elektromagnetyczny do wnętrza obudowy nie przenika. Jeśli natomiast mamy do czynienia z falami centymetrowymi i milimetrowymi, to oprócz oddziaływania pośredniego, polegającego na indukowaniu się prądów i napięć w obudowach urządzeń radioelektronicznych, następuje jeszcze oddziaływanie bezpośrednie – fale milimetrowe przenikają przez osłony, szczeliny i otwory montażowe, indukując prądy i napięcia bezpośrednio w obwodach urządzeń elektronicznych. Należy podkreślić, że im bardziej różni się zakres częstotliwości odziaływującego promieniowania od pasma częstotliwości roboczych urządzenia radioelektronicznego, tym mniejszy jest efekt skuteczności. Dla impulsów elektromagnetycznych istnieje oddzielna skala wrażliwości różnych obiektów. Gęstość promieniowania strumienia mocy, potrzebna do zniszczenia dwóch rakiet jednego typu, różniących się głowicami naprowadzającymi (radiolokacyjna i na podczerwień), mogą się różnić o rząd wielkości i więcej. Duży wpływ na efektywność impulsu elektromagnetycznego (EM) ma jego zdolność do wywołania przebić przestrzeni powietrznej. Tworząca się podczas przebicia plazma izoluje źródło i energia promieniowania jest zużywana jedynie na nagrzewanie plazmy. Wraz ze zmniejszaniem się ciśnienia (wzrostem wysokości), możliwości powodowania przebić maleją. Ograniczenia związane ze zdolnością przebijania przestrzeni powietrznej sztywno określają stosunek między wielkością źródła impulsu EM a promieniem rażenia, zgodnie z zasadą, że gęstość mocy zmniejsza się proporcjonalnie do kwadratu odległości. Dlatego też maksymalna odległość skutecznego rażenia środka elektronicznego, nie przewyższa gabarytu źródła promieniowania (dla źródła kierunkowego to długość, a dla izotropowego – promień) więcej niż tysiąc razy. Impuls elektromagnetyczny może zakłócić przelot samolotów, a także system obrony przeciwlotniczej. Obiektami rażenia w tym wypadku będą środki radiolokacyjne systemu obrony powietrznej, artylerii, naprowadzania lotnictwa i rakiet przeciwlotniczych.

Kolejnym środkiem są paski folii *włókna węglowego*. System obrony powietrznej może być zdezorganizowany przez wyłączenie sieci energetycznej potencjalnego przeciwnika. Do tego celu wykorzystuje się rakiety wypełnione paskami folii włókna węglowego. Paski te opadając na linie przesyłowe i transformatory, powodują spięcie i przepalenie wszystkich instalacji. W tym kierunku usiłowano zmodernizować pociski Tomahawk. Przerwy w zasilaniu energetycznym przez uderzenie na elektrownie lub użycie włókien węglowych na energetycznych

liniach przemysłowych, doprowadziły do przerw w pracy elektronicznych maszyn cyfrowych o przeznaczeniu militarnym i stwarzały sytuację deficytu czasu (brak czasu) wśród organów dowodzenia.

Nowe technologie pola walki obejmują wykorzystanie lasera. Promienniki równokierunkowe (izotropowe), wykorzystywane do celów wojskowych, występują w formie amunicji artyleryjskiej lub lotniczej, wytwarzającej promieniowanie elektromagnetyczne o własnościach zbliżonych do laserowego. Ich działanie polega na krótkotrwałej emisji promieniowania elektromagnetycznego w zakresie od podczerwieni do nadfioletu oraz na porażeniu czujników i oczu żołnierzy przeciwnika. Źródłem promieniowania jest plazma powstała z gazu szlachetnego. Do rozgrzania gazu i doprowadzenia go do stanu plazmy wykorzystuje się energię detonacji materiału wybuchowego w kształcie stożka wypełnionego gazem szlachetnym. Najczęściej stosowanymi gazami są neon, argon lub ksenon. „Humanitarne" działanie tego typu lasera polega na tym, że promień nie zabija, ale trwale oślepia przeciwnika. Ponadto niszczy elementy światłoczułe w przyrządach optycznych. Ślepy staje się nie tylko człowiek, ale również sprzęt.

W zakresie fal sprężystych są stosowane *generatory infradźwięków* do czasowego obezwładniania siły żywej, dzięki wytwarzaniu i emitowaniu fal akustycznych o bardzo małej częstotliwości. Działanie infradźwięków polega na wykorzystaniu zjawiska wzbudzania wibracji materiałów na skutek oddziaływania fal o długości zbliżonej do fizycznych rozmiarów opromieniowanego obiektu. Przy wystarczającej intensywności i czasie ekspozycji można spowodować wibrację i zniszczenie trwałych struktur budownictwa lądowego. Natomiast infradźwięki o częstotliwości 16 Hz, używane przeciwko sile żywej, powodują wzbudzanie wibracji w organach wewnętrznych, powstanie nudności, dolegliwości sercowych i zaburzeń równowagi. Zaletą tych rodzajów broni jest przede wszystkim łatwość przenikania przez struktury materii.

Do zagrożeń systemów informacyjnych zalicza się:

- przerwanie;
- przechwycenie;
- modyfikację;
- podrobienie.

Przerwanie ma na celu zmniejszenie stopnia lub spowodowanie utraty dyspozycyjności i polega na uniemożliwieniu używania systemu informacyjnego lub jego części.

W kontekście zagrożeń związanych z podłączeniem określonych struktur wojskowych lub cywilnych do Internetu, na szczególną uwagę zasługują takie sposoby zmniejszania stopnia dyspozycyjności, jak:

- przeciążenie systemu informacyjnego,
- działanie wirusów komputerowych.

Przeciążenie – zablokowanie działania poszczególnych elementów lub usług systemu informacyjnego czy też uniemożliwienie pracy całego systemu poprzez przesłanie ogromnej liczby danych do przetworzenia. Atakujący może wysyłać, np.: komunikaty, listy elektroniczne, żądania usług sieciowych czy połączeń mo-

demowych z takim natężeniem, że system informacyjny nie będzie w stanie obsłużyć wszystkich zleceń, w tym także zleceń rzeczywistych użytkowników. Skutkiem może być dezorganizacja pracy w takim stopniu, że normalne funkcjonowanie danej organizacji okaże się niemożliwe. Ataki przeprowadzane w ten sposób, są nazywane atakami typu odmowa usługi. Wykrycie tego programu jest bardzo trudne, gdyż został tak napisany, by po otrzymaniu określonego sygnału lub wykryciu prób jego namierzania, odinstalował się i usunął ślady swej bytności w systemie.

Typowa sieć rozproszonego ataku typu odmowa usługi składa się z: agresora, zarządcy, żołnierzy, ofiary. Agresor nie bierze udziału w samym ataku, ograniczając się jedynie do wysłania sygnału do jego rozpoczęcia do zarządcy lub zarządców. Dopiero zarządcy uruchamiają i koordynują atak, przesyłając do żołnierzy odpowiednie sygnały.

Wirus komputerowy to kawałek kodu programu, który dołącza się do istniejącego programu i zmienia go w celu dalszego rozmnażania się wirusa. Ponadto, gdy zostaną spełnione pewne warunki, wirus może zacząć działalność niszczącą dane, generując w celu odwrócenia uwagi od działalności niszczącej efekty specjalne w postaci melodyjek, rysunków itp. Wirusy mogą spowolnić działanie systemu informacyjnego lub całkowicie go unieruchomić. Korzystanie z ogromnych zasobów Internetu zwiększa zagrożenie zainfekowania wirusami komputerowymi.

Do podstawowych rodzajów wirusów zalicza się:
- wirusy rekordu startowego,
- wirusy plikowe,
- wirusy towarzyszące,
- bakterie,
- wirusy makro,
- robaki.

Przechwycenie jest atakiem mającym na celu spowodowanie utraty poufności danych. Przechwycenie może polegać na ujawnieniu danych i analizie przesyłu.

Ujawnieniu mogą podlegać dane, które później są wykorzystywane bezpośrednio lub informacje pośredniczące w uzyskaniu innych informacji. Dane wykorzystywane bezpośrednio, to np. plany działań czy dokumenty operacyjne. Natomiast przykładem informacji pośredniczących w uzyskaniu innych informacji jest plik z hasłami, który może w przyszłości pozwolić na ujawnienie innych informacji czy też naruszenie bezpieczeństwa w inny sposób, np. przez modyfikację lub podrobienie. Ujawnienie danych może się odbywać na wiele różnych sposobów. Wykorzystując Internet, najczęściej korzysta się ze:
- sniffingu;
- koni trojańskich;
- monitorowania zdalnych sesji;
- przeglądania;
- przenikania.

Analiza przesyłu – przechwycenie zaszyfrowanych danych przez osoby niepowołane nie jest równoznaczne z ich ujawnieniem. Dlatego też zamiast zajmować

się rozszyfrowaniem, bada się strukturę budowy przesyłanych komunikatów, ich długość i częstotliwość z jaką są wysyłane. Analiza przesyłu pozwala też na odkrycie lokalizacji i tożsamości komputerów wymieniających dane. Tego typu dane mogą być równie ważne, jak treść przesyłanych informacji.

Modyfikacja jest atakiem mającym na celu spowodowanie utraty integralności. Wiąże się ona z wprowadzaniem zmian dotyczących danych przez osobę, która nie posiada do tego uprawnień. Modyfikacja może oznaczać:

– dopisanie jakiejś nowej treści do oryginalnego komunikatu;
– przekształcenie treści oryginalnych komunikatów;
– kasowanie oryginalnych danych;
– celowe opóźnianie przesłania danych;
– powtarzanie transmitowanych komunikatów.

Podrobienie jest atakiem powodującym wprowadzenie w błąd odnośnie do autentyczności. Jest więc to atak na uwierzytelnianie. Podrobienie polega na wprowadzeniu do systemu informacyjnego fałszywych obiektów i wiąże się z podszywaniem, podczas którego maszyna sieciowa udaje inną maszynę. Podszywanie się pod pewien podmiot sieciowy ma na celu wprowadzenie w błąd innych komputerów na temat pochodzenia danych i skłonienie ich do przesłania pożądanych danych.

Przedmiotem zakłóceń informatycznych mogą być zarówno komputery, jak też programy i zbiory danych. Zakłócanie to może być realizowane przy wykorzystaniu różnorodnych programów złośliwych, które powodują wymazanie w krótkim czasie dużej liczby zbiorów danych, spowalniając pracę programów użytkowych. Programem złośliwym nazywa się kod wyrządzający szkody. Niektórzy również posługują się określeniem malware (zlepek – z ang. malicious software – oprogramowanie złośliwe)[5]. Do programów tych należy zliczyć: wirusy, konie trojańskie, bomby logiczne, robaki komputerowe, bakterie i króliki oraz wiele innych im podobnych. Koncepcja zastosowania *wirusów komputerowych* wprowadzonych do systemów komputerowych przeciwnika (CVW – Computer Virus Weapon) w celu zakłócenia pracy systemów dowodzenia i kierowania, po raz pierwszy została sprawdzona w czasie wojny w rejonie Zatoki Perskiej. Niektóre wirusy podejmują działania natychmiast po wprowadzeniu do systemu, a niektóre są wprowadzane w postaci zaszyfrowanej lub upakowanej. Charakteryzują się tym, że po wprowadzeniu do systemu komputerowego podejmują jedynie działania mające na celu samoreplikację i dotarcie do najistotniejszych elementów systemu. Sygnałem do podjęcia działań destrukcyjnych jest aktywacja po określonym czasie lub zaistnieniu określonych warunków w systemie. Celami dla tego rodzaju wirusów są urządzenia komputerowe pracujące w sprzęcie bojowym i zabezpieczeniu logistycznym; ich uruchamianie może nastąpić, np. za pomocą sygnału radiowego

Zdaniem Amerykanów zakłócanie informatyczne będzie jednym z najważniejszych sposobów walki informacyjnej w XXI wieku. Przekonały się o tym Stany Zjednoczone, których komputery zarówno w sferze cywilnej, jak i wojskowej są wrażliwe na atak informatyczny. Systemy komputerowe Departamentu Obrony

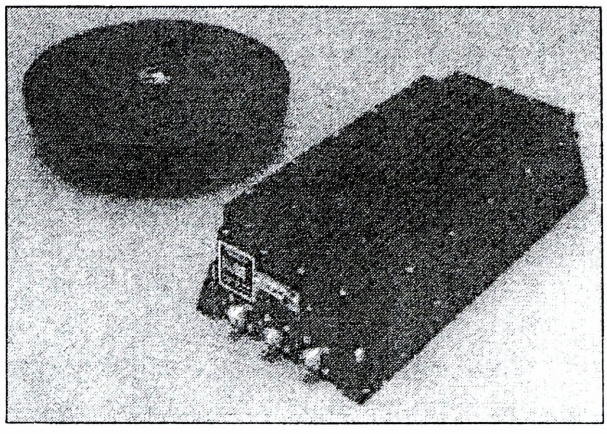
[5] S. Garfinkel, G. Spafford, *Bezpieczeństwo w Unixie i Internecie*, Warszawa 1997, s. 31.

USA stają się coraz częściej celem hackerów, którzy włamując się do komputerów Pentagonu mają dostęp do zastrzeżonych informacji. Hackerzy każdego roku dokonują około 250 tysięcy włamań, z czego 65% kończy się powodzeniem.

Jim Settle, konsultant ds. bezpieczeństwa FBI, jest przekonany, że przyszła wojna będzie polegać na blokowaniu dostępu do informacji i wprowadzaniu w błąd strony przeciwnej. W odróżnieniu od zasobów nuklearnych, środki walki informacyjnej (zakłócania informatycznego) są osiągalne niemal dla każdego. Celem tej walki będzie zarażenie wirusem programów komputerowych przeciwnika, tak aby był niezdolny do podejmowania jakichkolwiek działań. Skoro systemy obrony powietrznej większości krajów są oparte na systemach komputerowych, wystarczy zakłócić pracę tego systemu, aby przeprowadzić skuteczny atak. Wpadli na to Amerykanie podczas wojny z Irakiem. Pół roku wcześniej sprzedali do Iraku drukarki komputerowe, których odbiorcą było wojsko. Wewnątrz drukarek były zainstalowane specjalne mikronadajniki, które codziennie podawały swoją pozycję do satelity. W ten sposób można było zlokalizować obiekty systemu obrony powietrznej Iraku. Lotnictwo amerykańskie bombardowało te pozycje, na których znajdowały się drukarki.

Zarówno siły powietrzne, jak i obrona powietrzna wykorzystują na szeroką skalę system GPS. Ważnym problemem jest jego podatność na zakłócenia elektroniczne, które powstają w sposób niezamierzony (harmoniczne, listki boczne, efekty modulacji wzajemnej), w wyniku niekompatybilości różnych urządzeń elektronicznych lub też są to zamierzone sygnały celowo emitowane przez komórki walki elektronicznej. Nadajniki małych mocy potrafią zakłócić odbiorniki GPS w promieniu do 10 km. Może to mieć niekorzystny wpływ na działania wojsk, szczególnie podczas kierowania operacjami połączonymi w oddalonych obszarach. W celu ochrony przed zakłóceniami firma ERI[6] zaproponowała uzupełnienie odbiorników systemu GPS w urządzenie eliminujące zakłócenia ISU (Interference Suppresion Unit – rys. 6). Urządzenie to zapewnia ochronę własnych odbiorników, ale także może zmienić rodzaj pracy i zakłócać odbiorniki przeciwnika w tym samym czasie, kiedy własne odbiorniki odbierają sygnały z satelitów. Podatność odbiorników systemu GPS na zakłócenia stosowane przez podręczne nadajniki staje się ewidentna, co wpływa niekorzystnie na działalność wojskową (podczas kierowania operacjami w oddalonych obszarach, zapewnienia precyzji środków kierowanych) ze względu na to, że siły zbrojne wykorzystują ten system do przekazywania danych. Urządzenie ISU może być wykorzystywane do ochrony przed zakłóceniami zarówno wojskowych, jak i cywilnych naziemnych stacji końcowych pracujących w satelitarnych systemach łączności. Urządzenie ISU systemu GPS jest produkowane przez firmę elektroniczną ERI w Fairfield (New Jersey). Złożony test tego urządzenia obejmował zarówno szerokie, jak i wąskie pasmo częstotliwości przy stosowaniu kodu odbiornika: C/A i P/Y. Sił zbrojnych USA nie stać na produkcję broni przeciwradiolokacyjnej, która mogłaby niszczyć nadajniki zakłóceń małej mocy (zakłócające system GPS) i obecnie nie rozważają takiej możliwości.

[6] ERI – ang. Electro-Radiation, Incorporated, Fairfield, New Jersey.



Rys. 6. Urządzenie eliminujące zakłócenia (ISU)

Możliwości zintegrowanego systemu przeciwzakłóceniowego wynoszą: 95–100 dB tłumienności przy zakłóceniach szerokopasmowych oraz 105–110 dB tłumienności przy zakłóceniu wąskopasmowym. Urządzenie ISU nie musi być kierunkowo sterowane za pomocą dodatkowych urządzeń. To pozwala uniknąć znacznych kosztów i ograniczeń w projektowaniu. Urządzenie testowano przy stosowaniu kodów C/A i P/Y. Scenariusz testu przewidywał używanie od jednego do dwóch nadajników zakłóceń o osiągach 35–40 dB przy zakłóceniu szerokopasmowym i 45–50 dB przy zakłóceniu wąskopasmowym. Skuteczna tłumienność urządzenia przy dwu rozstawionych oddzielnie nadajnikach zakłóceń wynosi powyżej 45 dB i zależy od typu nadajnika.

Kolejnym zagrożeniem dla obrony powietrznej jest broń energii wiązkowej (Directed Energy Weapon – DEW). Energia wiązkowa (Directed Energy – DE) to skoncentrowana (skupiona) energia elektromagnetyczna wypromieniowana w celu zniszczenia lub uszkodzenia obiektu.

Działanie broni DEW polega na tym, że wygenerowany i odpowiednio uformowany strumień fal elektromagnetycznych lub cząstek elementarnych o dużej gęstości energii bezpośrednio oddziałuje na obiekt, powodując jego zniszczenie lub uszkodzenie bądź wyeliminowanie z walki.

Broń tego typu jest w stanie zniszczyć lub uszkodzić elementy uzbrojenia przeciwnika bądź obezwładnić siłę żywą. Wiązkową broń energetyczną można podzielić na trzy rodzaje:

1) broń częstotliwości radiowych (Radio Frequency Weapon);

2) broń laserową (Laser Weapon);

3) broń cząstek elementarnych (Particle Beam Weapon).

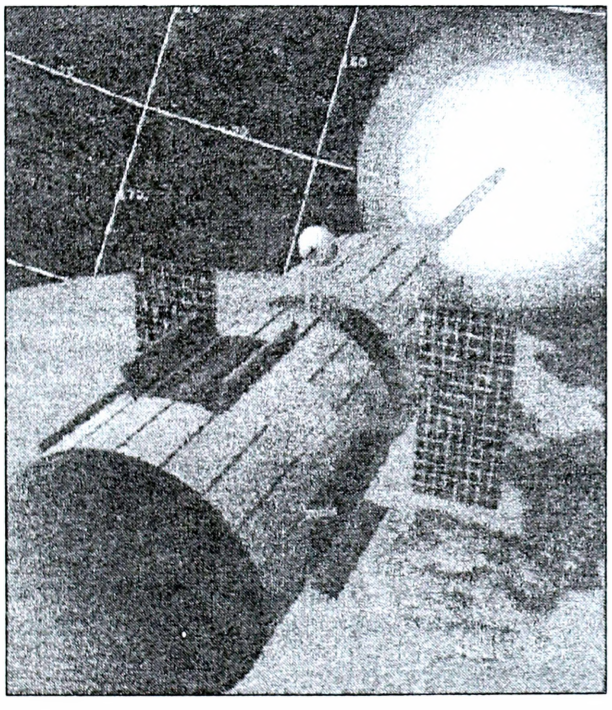
Mikrofalowe emitery HPM, najbardziej zaawansowane technicznie z grupy urządzeń częstotliwości radiowych, działają najskuteczniej, gdy ich częstotliwość emisji pokrywa się z częstotliwością pracy obiektu bądź jego układów wewnętrz-

nych. W takim wypadku efektem oddziaływania jest najczęściej zniszczenie całego obiektu bądź uszkodzenie któregoś z jego podzespołów.

Emitery typu UWB stanowią drugą grupę urządzeń, które promieniują energię w postaci sygnałów, jednak rozproszonych w wielokrotnie szerszym paśmie częstotliwości i znacznie mniejszej gęstości mocy. Energia rozproszona w szerokim paśmie nie niszczy więc elektroniki, a jedynie zakłóca jej pracę lub powoduje uszkodzenie urządzeń.

Broń laserowa małej mocy (LEL) umożliwia obezwładnienie techniki bojowej przeciwnika poprzez ich oślepienie bądź czasowe, rzadziej trwałe uszkodzenie. Wiązka laserowa tej broni wywołuje efekt termiczny wrażliwych elementów elektronicznych, urządzeń optoelektronicznych oraz czujników i sensorów środków rozpoznawczych przeciwnika. Może być także stosowana do oślepiania ludzi, chociaż takie jej użycie jest zakazane konwencją.

Broń laserowa dużej mocy (HEL) umożliwia zwalczanie celów wiązką energii znacznie bardziej skoncentrowaną, niż np. wiązka mikrofalowa emitera HPM. Efektem jej oddziaływania jest termiczne uszkodzenie lub zniszczenie celu przy gęstościach energii rzędu >10 MJ/cm^2. Czynnikiem rażącym jest przegrzanie celu bądź przepalenie gorącą plazmą wytworzoną na powierzchni rażonego celu.



Rys. 7. Zestaw nazwany skrótem ALI (Alpha–LAMP–Integration) z lustrem o średnicy 4 metrów, uruchomiony w ramach programu SBL w 1997 roku; uzyskał moc rzędu megawatów i utrzymał ją przez kilka sekund

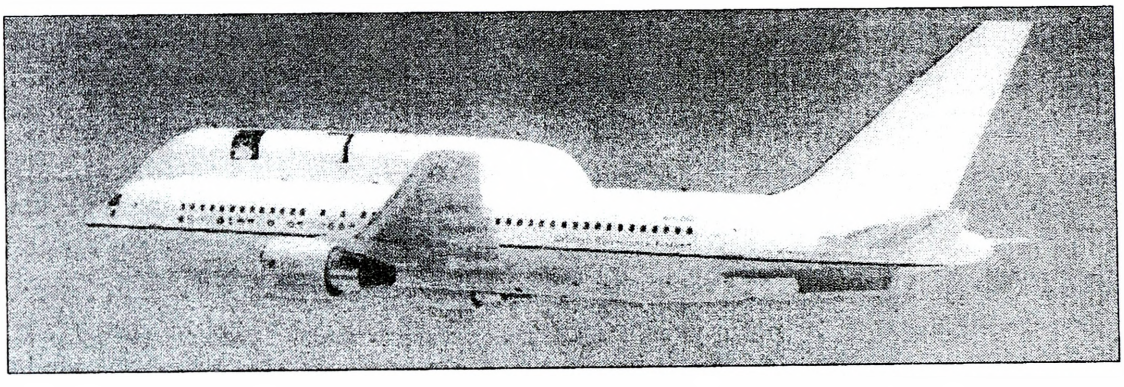
Badania nad laserami typu HEL są prowadzone w ramach trzech oddzielnych programów.

Pierwszy z nich – SBL (*Space Based Laser*) – obejmuje prace związane z budową emiterów (dział) laserowych przeznaczonych do zwalczania obiektów kosmicznych i satelitów oraz zwalczania pocisków balistycznych.

Drugi program – ABL (*AirBorne Laser*) – obejmuje budowę dział laserowych instalowanych na samolotach. Zadaniem ABL będzie zwalczanie będących w ich zasięgu (do 300 km) balistycznych pocisków rakietowych przeciwnika w fazie startu, jego samolotów oraz satelitów na niskich orbitach. Broń cząstek elementarnych PBW jest bronią wiązkową, która działa na zasadzie akceleracji cząstek elementarnych. Badania dotyczą dwóch rodzajów emiterów:

1) CBP – emitujących strumień cząstek posiadających ładunek elektryczny,

2) NBP – emitujących cząstki elementarne bez ładunku.



Rys. 8. Działo laserowe zamontowane na samolocie Boeing 767

Energia strumienia neutronów z emitera NBP jest znacznie większa od strumienia (np. elektronów) z emitera CBP i może przyjąć formę plazmy bądź kilkumilimetrowych pierścieni, niosących jednak energię porównywalną z pociskami artyleryjskimi największych kalibrów.

W związku z prowadzonymi na świecie badaniami nad tymi rodzajami broni, szczególnie w Stanach Zjednoczonych (program HAARP) oraz w Rosji (program SURRA), proponuje się interpretować termin Directed Energy jako energia kierowana, a Directed Energy Weapon jako broń energii kierowanej. W tej sytuacji, oprócz już wymienionych trzech rodzajów tej broni, podział obejmowałby również:

– broń ekstremalnie niskich częstotliwości (Extremely Low Frequency Weapon);

– broń infradźwiękową (Infrasonic Weapon);

– broń impulsową na ekstremalnie wysokich częstotliwościach – promieniowanie gamma (Extremely High Frequency Pulse Weapon – Gamma Radiation).

Wnioski

Potencjalne użycie sił zbrojnych na współczesnym polu walki każdorazowo będzie przebiegać w innych okolicznościach. Zastosowanie narzędzi walki informacyjnej spowoduje, że zwycięstwo w przyszłych działaniach będzie mógł odnieść jedynie wysoko wykwalifikowany personel, umiejący we właściwy sposób wykorzystać dane z rozpoznania i systemy precyzyjnego rażenia.

Armia, która będzie potrafiła korzystać z narzędzi walki informacyjnej, znacznie będzie się różnić od armii masowej produkcji wieku industrialnego, w jej bowiem składzie znajdą się specjaliści od walki informacyjnej. Oczywiście, będą występować znaczne różnice między strukturami wojska a korporacjami. W znaczny sposób zmienią się metody działania. Działanie armii wieku informacji będzie oparte na systemie informacyjnym, który dostarczy aktualnych danych o wojskach własnych i przeciwniku w czasie niemal rzeczywistym. Dowódcy związków operacyjnych i taktycznych będą wiedzieć, gdzie jest przeciwnik, gdzie go nie ma oraz jakie posiada siły i środki. Wiadomo, że uzyskane dane nigdy nie będą kompletne, ale będą bardziej wiarygodne oraz chronione przed rozpoznaniem przeciwnika. Zarówno dane o przeciwniku, jak i wojskach własnych zostaną doprowadzone do najniższego szczebla dowodzenia. Taka dostępność do informacji, w połączeniu z możliwościami prowadzenia działań wojennych w każdych warunkach, zarówno w dzień, jak i w nocy, pozwoli armiom wieku informacji szybciej podejmować decyzje i działać precyzyjniej i sprawniej. Szybkość i precyzja będzie wynikać z połączenia rodzajów sił zbrojnych oraz różnych specjalności i systemów wsparcia ogniowego w jednolitą całość opartą na połączonym systemie informacyjnym. System ten będzie obejmował podsystemy sił lądowych, morskich, powietrznych i infrastrukturę w kosmosie. W przyszłych działaniach wojennych, wykorzystując systemy broni precyzyjnego rażenia będzie można zaatakować cele przeciwnika oddalone o dziesiątki tysięcy kilometrów. Armia wieku informacji będzie bardziej elastyczna i uniwersalna, mniej liczna, ale bardziej skuteczna dzięki posiadaniu wykwalifikowanego personelu oraz najnowocześniejszego uzbrojenia opartego na technologiach informacyjnych. Ulegnie zmianie proces podejmowania decyzji, który będzie się opierał zarówno na inteligencji ludzkiej, jak i sztucznej.

Ten nowy model armii wywrze wpływ na wszystkie poziomy działań wojennych – strategiczny, operacyjny i taktyczny.

Wiele państw przywiązuje dużą uwagę do tej problematyki. W stanach Zjednoczonych organizuje się formacje do prowadzenia operacji informacyjnych we wszystkich rodzajach sił zbrojnych. Środki i technologie informacyjne stosowane w walce zbrojnej mogą w znaczny sposób wprowadzić w błąd przeciwnika co do posiadanych sił i prowadzonych działań, co zwiększy zdolność bojową własnych sił i zrekompensuje braki w posiadanych systemach broni.

Zastosowanie sił i środków przeznaczonych do prowadzenia operacji informacyjnych może w krótkim czasie doprowadzić nie tylko do dezorganizacji systemu obrony powietrznej, ale do całkowitego zniszczenia nowocześnie zorganizowanego

systemu całego państwa. Właśnie dlatego wysoko uprzemysłowione społeczeństwa są zmuszone zastanawiać się nad środkami ochrony własnych systemów telekomunikacyjnych i informatycznych nie tylko w aspekcie militarnym, ale także pozamilitarnym. Polityka bezpieczeństwa narodowego zyskuje więc pewien zupełnie nowy wymiar. Formy organizacji i strategii będą musiały być dopasowane do nowych zagrożeń. Siły i środki do prowadzenia operacji informacyjnych będą narażone na oddziaływanie w tym zakresie strony przeciwnej. Ponadto siły polityczne, rzekomo z mało znaczących regionów, mają dzisiaj dostęp do tego rynku technologicznego. Niezbędne środki (komputery osobiste, oprogramowanie itp.) są dostępne na całym świecie. Dlatego też siły te nie muszą już dzisiaj wydawać ogromnych sum pieniędzy na zakup systemów uzbrojenia i broni, które zresztą są objęte zakazem eksportu do tych regionów. Rozwój tej dziedziny trwać będzie w tych regionach z pewnością jeszcze dłuższy czas, dlatego już teraz muszą być poczynione wysiłki, które uodpornią własne systemy na oddziaływanie środków walki informacyjnej przeciwnika.

Doktryna Operacji Informacyjnych Stanów Zjednoczonych ma poważne implikacje dla Rosji i to zarówno w technicznym, jak i moralno-psychologicznym aspekcie. Z powodu obecnej psychologicznej niestabilności, która dotyka ten kraj, Rosjanie postrzegają operacje informacyjne z zaniepokojeniem, podejrzeniami i brakiem zaufania. Wskazują, że informacyjne bezpieczeństwo jednostki i całego społeczeństwa jest jednym z priorytetów interesu narodowego.

Armia rosyjska jest szczególnie zainteresowana wpływem operacji informacyjno-psychologicznych na swoich żołnierzy, co wynika z doktryny wojennej. Należy oczekiwać, że rosyjska armia będzie gotowa do prób wykorzystania operacji informacyjnych przeciw żołnierzom innych krajów.

Technologia informacyjna oferuje śmierć chirurgiczną niedostępną w przeszłości. Dzięki cyfrowemu zobrazowaniu sytuacji na polu walki, jednostki będą miały możliwość uzyskania potężnej mocy bojowej, jakiej do tej pory nie znano. Większej mocy bojowej nie można będzie tworzyć przez gromadzenie większej ilości danych. Ale można zwiększyć moc bojową przez wykorzystanie własnych aktywów, lecz tylko tam i w czasie, kiedy one są niezbędne do osiągnięcia celów militarnych. Dlatego zwiększenie świadomości sytuacyjnej może nastąpić na skutek zdobycia istotnych (kluczowych) informacji, co doprowadzi do wyeliminowania niepewności i podjęcia niezbędnych środków bezpieczeństwa.

Hipotetyczna wizja ewentualnych kryzysów w przyszłości wskazuje, że zwycięstwo w każdej walce, bitwie, operacji czy wojnie będzie zależeć od umiejętności dowódców i oficerów sztabu, stworzenia przewagi informacyjnej nad przeciwnikiem i mistrzowskiego jej wykorzystania do osiągnięcia celów strategicznych, operacyjnych i taktycznych z jak najmniejszymi stratami.

Koncepcja prowadzenia działań wojennych w wieku informacji ulega i będzie ulegać znacznym zmianom.

Po pierwsze nie można już traktować wojny jako walki armii jednego państwa z drugim lub grupy państw z innymi. Państwa – narody nie mają monopolu na prowadzenie wojny. Wojnę mogą prowadzić różnorodne organizacje, korporacje, grupy religijne, organizacje terrorystyczne, partyzanci, mafie narkotykowe lub inne

grupy przestępcze. Ponadto państwa zacofane w rozwoju (wieku agrarnego) mogą kupować uzbrojenie wieku informacji. Technologia tego wieku już znajduje różnorodne zastosowanie zarówno w sferze cywilnej, jak i wojskowej. Dziś trudno odróżnić wojnę od innych działań.

Po drugie rozszerza się zakres wojny. W wieku industrialnym zwycięstwo nad państwem uprzemysłowionym oznaczało zniszczenie nie tylko poważnej części jego armii, ale także pozbawienie infrastruktury, bogactw naturalnych i bazy przemysłowej. Natomiast zwycięstwo nad państwem wieku informacji wymaga czegoś więcej. Nie wystarczy zniszczenie sił zbrojnych przeciwnika i pozbawienie go fizycznych zdolności walki, ale trzeba także zniszczyć lub obezwładnić jego system informacyjny. Tę możliwość zapewniają właśnie operacje informacyjne, które mogą być prowadzone zarówno przez siły zbrojne, jak i organy pozazbrojne. Dlatego wiele państw na świecie prowadzi badania nad wykorzystaniem narzędzi walki informacyjnej.

Współczesne narzędzia walki informacyjnej wskazują, jak nigdy dotąd, na konieczność uwzględniania tej kwestii nie tylko w programach reformowania sił zbrojnych, ale również w funkcjonowaniu państwa. Potrzeba taka wynika chociażby z tego, że ich użycie jest możliwe nie tylko w okresie zagrożenia i wojny. Już w okresie pokoju mogą być podejmowane w tej dziedzinie wysiłki ukierunkowane nie tylko na zdobywanie informacji, ale również na powodowanie niepokojów, zamieszek i kryzysów rządowych, co w atmosferze ciągle trwającej globalnej konkurencji, wydaje się być bardzo realne. Nie można też wykluczyć, że w ramach tego mogą być stosowane różnego rodzaju akty terrorystyczne sterowane przez jakieś państwo. Ta forma przemocy może być prowadzona chociażby siłami służb specjalnych, o których wiadomo, że są stale, na całym świecie, doskonalone i rozwijane. Może to nawet stanowić ekwiwalent otwartych agresji, co z coraz większą intensywnością daje się obserwować już teraz. Wysiłki walki informacyjnej mogą być ukierunkowywane na podrywanie autorytetu zaatakowanego państwa na arenie międzynarodowej czy też podrywanie jego zaufania sojuszniczego. W szerokim zakresie może być włączana do tego dyplomacja, handel zagraniczny i media. Na oddziaływanie takie szczególnie są podatne sfery ekonomiczna, polityczna i społeczna. W działaniach tych mogą być również prowokowane incydenty międzypaństwowe, powodujące napięcia społeczne w stosunkach dobrosąsiedzkich. Można przypuszczać, że spośród tych, które miały już miejsce, wiele ma takie właśnie podłoże. Sądzić też można, że w przyszłości ta forma działań będzie intensyfikowana w jeszcze szybszym tempie i z większą siłą. Dlatego też trafna tu będzie stara rzymska maksyma: *si vis pacem, para bellum* (jeśli chcesz pokoju, gotuj się do wojny), z tym tylko uzupełnieniem, że do walki informacyjnej.

LITERATURA:

Brillouin. L.: *Nauka a teoria informacji*, PWN, Warszawa 1969.

Burhans W. A.: *Iraqi Air Defenses – Initial Soviet Post – Mortem*, „Journal of Electronic Defense", October 1991.

Campen A. D.: *The first Information War*, Virginia 1992.

Czermiński A., Czapiewski M.: *Organizacja procesów decyzyjnych*, Uniwersytet Gdański, Gdańsk 1995.

Fitzgerald M. C.: *Russian views on information warfare*. „Army" 1994, nr 5.

Giboney T. B.: *Chaos informacyjny*, „Military Review" 1991, nr 1.

Grier P.: *Information Warfare*, „Air Force" 1994, nr 4.

Hercman K.: *Teoria informacji na użytek szkoły*, WSiP, Olsztyn 1977.

Keramas J. G.: *Workforce Training for Global Copmpetitivenes*, AFCEA – Stockholm Symposium and Exposition, 1995.

Keuren E. V., Knighten J.: *Implications of the High – Power Microwave Weapon Threat in Electronic System Design*, IEEE International Symposium on EMC, Cherry Hill, 1991.

Kurnal J.: *Zarys teorii organizacji i zarządzania*, Warszawa 1970.

Leonhard R.: *The Art of Maneuver*, Novato 1991.

Mitiugow W.: *Fizyczne podstawy teorii informacji*, PWN, Warszawa 1980.

Neri F.: *Introduction to Electronic Defense Systems*, Artech House Inc., 1991.

Ochman J.: *Integracja w systemach informatycznych zarządzania*, PWE, Warszawa 1992.

Peterson K., Pracht U.: *Walka informacyjna*, „Soldat und Technik" 1995, nr 12.

Riccardelli R. F.: *The Information and Intelligence*, „Military Review" 1995, nr 5.

Ross J. D.: *Wojna o informację*, „Army" 1994, nr 2.

Schwartau Winn.: *Information Warfare – Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, m. wyd. 1993.

Seidler J.: *Podstawy, modele źródeł i wstępne przetwarzanie informacji*, WNT, Warszawa 1983.

Shannon C. E., Warren W.: *The Mathematical Theory of Communication*, Urbana, The University of Illinois Press 1949.

Sokołowski A.: *Ochrona informacji komputerowych*, MON, Warszawa 1987.

Starry M. D., Arneson C. W.: *Działania informacyjne*, „Military Review" 1996, nr 6.

Sullivan G. R., Dubik J. M.: *War in the Information Age*, „Military Review" 1994 nr 4.

Świątnicki W. Z.: *Bronie inteligentne*, ISBN, Warszawa 1992.

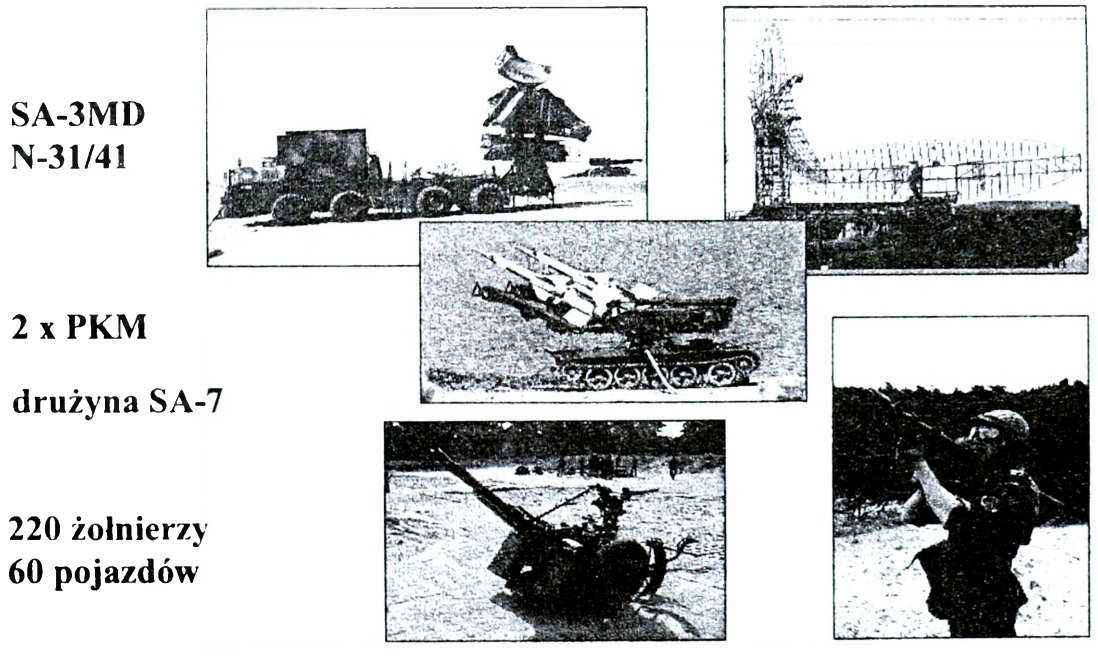
Toffler Alvin i Heidi: *Wojna i antywojna* (War and Antiwar), Warszawa 1993.

ppłk dr inż. Tomasz Jakusz

2 Korpus Obrony Powietrznej

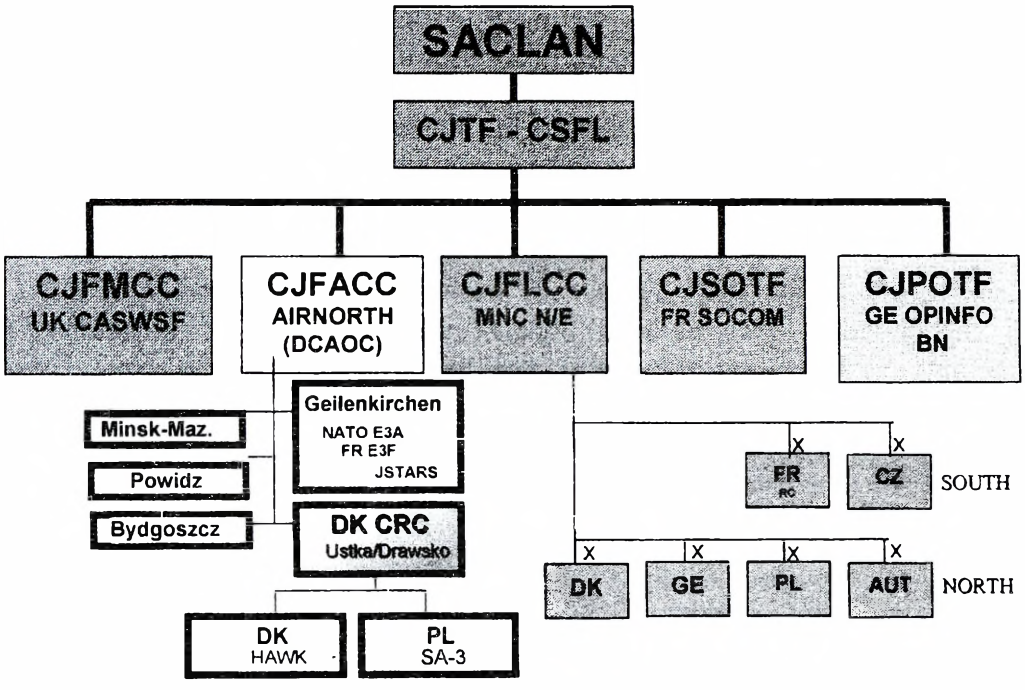
PROBLEMY INFORMACJI W WOJSKACH OBRONY PRZECIWLOTNICZEJ WLOP

Tytułem wstępu skrótowo przytoczę epizod wystąpienia zakłóceń radioelektronicznych w trakcie ćwiczenia „STRONG RESOLVE – 2002". W tym ćwiczeniu uczestniczył 60 dr OP w eksperymentalnej strukturze dywizjonu sił reagowania (rys. 1).



Rys. 1. Skład 60 dr OP

W pierwszym etapie dywizjon został przebazowany z Warszawy do Ustki, a następnie w ramach ćwiczenia wykonał manewr w rejon poligonu Drawsko Pomorskie, gdzie zadaniem sił przeciwlotniczych była osłona duńskiej Brygady Międzynarodowej, jednostki przeciwlotnicze zostały rozmieszczone w duńskim sektorze odpowiedzialności wojsk lądowych. (Struktura dowodzenia i kierowania została przedstawiona na rys. 2).



Rys. 2. Struktura dowodzenia i kierowania operacją wspierania pokoju w ćwiczeniu „STRONG RESOLVE – 2002"

Na stanowisku stacji radiolokacyjnej w rejonie Drawska Pomorskiego, wbrew wcześniejszym uzgodnieniom, zostały rozmieszczone radiolinie wojsk lądowych. W trakcie rozmów po rekonesansie stwierdzono, że rozmieszczony na tym stanowisku sprzęt nie będzie sobie wzajemnie przeszkadzał i zdecydowano w tym miejscu ustawić również polskie stacje radiolokacyjne. Po jednym dniu od osiągnięcia gotowości zgłoszono zakłócanie systemu łączności przez polską stację radiolokacyjną; zakłócenia występowały również przejściowo na stacji radiolokacyjnej. W wyniku takiej diagnozy zażądano wyłączenia tej stacji. Ponieważ zaistniała sytuacja budziła liczne wątpliwości strony polskiej, przeprowadzono badanie wpływu polskiej stacji radiolokacyjnej na system łączności radioliniowej. Nie stwierdzono żadnego wpływu, niemniej zakłócenia powtarzały się i mimo powtórzenia badań z analogicznym skutkiem, doprowadzono do wyłączenia stacji radiolokacyjnej.

Stworzyło to dla jednostki polskiej szczególnie trudną sytuację, gdyż nie otrzymała ona, mimo wcześniejszych uzgodnień, sytuacji powietrznej z CRC oraz utraciła możliwość identyfikacji celi powietrznych. Następnego dnia doprowadzono do wyłączenia z ćwiczenia polskiego dywizjonu – otrzymał RS – 0. Decyzja ta, ze względu na niekorzystne stanowisko ogniowe jednostki duńskiej, praktycznie pozbawiła ugrupowanie możliwości oddziaływania na cele nisko lecące. Podjęte energiczne działania wyjaśniające doprowadziły do powtórnego włączenia całości polskiego sprzętu, lecz strona duńska podjęła decyzję o zmianie dyslokacji radiolinii.

W chwili obecnej, z nieoficjalnych źródeł, wiadomo, że zakłócenia były wytwarzane przez amerykańskie pododdziały walki radioelektronicznej. Cel uderzenia był starannie wybrany – był nim podwójny styk pomiędzy komponentami wojsk lądowych i lotniczych oraz pomiędzy narodowościami Duńczykami i Polakami. Należy uznać, że działania pododdziałów walki radioelektronicznej dały znaczne efekty stronie przeciwnej, gdyż poza utrudnieniem łączności na pewnym kierunku osiągnięto napięcie na wyżej wspomnianych stykach, co doprowadziło do wyłączenia stacji radiolokacyjnych na około jeden dzień oraz krótkoterminowego wyeliminowania dywizjonu rakietowego, a w ostateczności do dodatkowego, niekoniecznego manewru radioliniami wojsk lądowych.

Powyższy prosty przykład ilustruje:

1. Jak starcie może być przeniesione w wymiar walki o informacje.

2. Jakie wymierne efekty w zakresie możliwości bojowych mogą być uzyskane bez fizycznego oddziaływania, co uzasadnia konieczność nowego spojrzenia na zagadnienie walki jako na proces sterowany za pomocą informacji, gdzie racjonalne jest skierowanie oddziaływania nie tylko na elementy wykonawcze – jednostki walczące – lecz również na szeroko pojmowany system informacyjny.

3. Oddziaływanie na system informacyjny nie jest ograniczone do środków informatycznych. Do tego celu mogą być wykorzystane wszystkie dostępne środki i metody walki.

Wojska obrony przeciwlotniczej są rodzajem wojsk szczególnie uzależnionym od informacji. Są to zarówno szybkozmienne informacje niezbędne do kierowania walką, jak też informacje zapewniające sprawność systemu dowodzenia i zabezpieczenia działań.

Nie wymaga uzasadnienia stwierdzenie, iż szybkość pozyskiwania, opracowania i udostępnienia informacji, w przypadku Wojsk OPL, ma szczególne znaczenie. Dlatego od lat rozwija się zautomatyzowane systemy dowodzenia, gdzie początkowo starano się wesprzeć proces kierowania walką, a obecnie coraz bardziej rozwija się systemy informatyczne wspierania dowodzenia i zabezpieczenia działań. Powstaje w ten sposób skomplikowany układ sprzętu komputerowego, oprogramowania, baz danych, łączy transmisji danych wewnętrznych i zewnętrznych względem danego podsystemu, ludzi obsługujących i wykorzystujących informacje, a także zależności służbowych i informacyjnych zachodzących między nimi. Wszystkie te elementy i relacje w czasie działań mogą się stać przedmiotem oddziaływań. W trakcie krótkiego wystąpienia nie ma możliwości przeprowadzenia

szczegółowej analizy tego zagadnienia, dlatego chciałbym podzielić się jedynie kilkoma konkluzjami:

1. Efektywność bojowa wymaga wprowadzenia do WOPL WLOP zautomatyzowanych, mobilnych systemów kierowania walką i wspierania dowodzenia oraz równie mobilnego systemu łączności. Obecnie WOPL nie dysponują takimi systemami, chociaż ostatnio się pojawił i był skutecznie wykorzystywany półautomatyczny system kierowania walką oparty na systemie ORCHIDEA, który jest rozwijany.

2. Wojna informacyjna jest faktem, a działania są przygotowywane w czasie pokoju. Możliwości rażenia – obezwładniania są znaczne i powinny być uświadamiane szerokim kręgom oficerów i decydentów.

3. Wojskowe systemy informacyjne winny zachować dużą odporność na uderzenia poprzez:

a) wprowadzenie sprawdzonego sprzętu i oprogramowania;

b) odizolowanie sprzętu i baz danych od otoczenia zewnętrznego poprzez nie korzystanie z cywilnych łączy telekomunikacyjnych i usług Internetu, wprowadzenie specyficznych dla wojska nośników danych – dyskietki, CD-ROM-y – wprowadzenie szyfrowania wiadomości w trakcie transmisji i zapisywania danych;

c) zapewnienie ochrony systemu przed zniszczeniem impulsem elektromagnetycznym lub unieruchomieniem sygnałami sterującymi z zewnątrz poprzez ekranowanie lub nadmiarowość urządzeń oraz automatyczne tworzenie kopii danych;

d) nabywanie dla wojska systemów telekomunikacyjnych o dużej odporności na zakłócenia radioelektroniczne, automatycznie utajniających przesyłane wiadomości, w tym głos, który w chwili obecnej jest podstawowym sposobem kierowania walką;

e) systemy dowodzenia i łączności powinny zapewniać dużą żywotność, między innymi poprzez tworzenie struktur sieciowych o zdolności do samoorganizacji,

f) w trakcie transmisji winno następować systematyczne potwierdzanie autentyczności nadawcy i odbiorcy w celu uniemożliwienia włączenia się elementów obcych i utrudnienia przejęcia elementów własnych.

4. W trakcie ćwiczeń sztabowych powinny być systematycznie sprawdzane:

a) kompletność baz danych;

b) sprawność obiegu informacji;

c) odporność na działania zakłócające.

Działalność ta winna oswajać z sytuacjami wojny informacyjnej, wyrabiać zaufanie do własnej wiedzy i odporności systemu.

5. Niezbędna jest skuteczna ochrona danych, zapewniająca możliwość prowadzenia działań związanych z maskowaniem i myleniem informacyjnym. Szczególne obawy budzi tu szczelność informacji w pionie głównego księgowego, który posiada dostęp do wszystkich zasobów.

6. Problemy ekonomiczne nie mogą powodować obniżenia wymagań wojskowych – zjawisko takie mogło by doprowadzić do utraty cech użyteczności w warunkach bojowych, a więc zasadności funkcjonowania w wojsku.

7. Zasadniczym przymiotem sił zbrojnych jest zdolność do fizycznego zwalczania przeciwnika. Niezmiennie jednym z najważniejszych wskaźników określających możliwości sił zbrojnych jest ilość „szabel" – systemów broni na stosownym do epoki poziomie technologicznym. Nośność i niewątpliwa słuszność idei wojny informacyjnej nie może przysłonić tej podstawowej prawdy. Pominięcie tego zasadniczego elementu i skupienie się wyłącznie na doskonaleniu struktur organizacyjnych, procesów informacyjnych i potencjału intelektualnego, może doprowadzić do sytuacji tzw. starego wilka, który słabo widzi, słyszy i czuje, ale doskonale wszystko rozumie, perfekcyjnie organizuje działania nawet przy słabych sensorach, lecz nie ma czym ugryźć.

8. Wdrażanie przyjętych rozwiązań wymaga stworzenia skutecznie działającej pętli ujemnego sprzężenia zwrotnego oraz sygnałów testujących. W przypadku wojska, w czasie pokoju, sytuacja jest szczególnie trudna, gdyż nie ma sygnału wyjściowego efektów bojowych, które by w obiektywny sposób wpływały na decyzje przełożonych różnych szczebli. Zdając sobie sprawę, że bez ujemnego sprzężenia zwrotnego żaden system nie może stabilnie pracować, wydaje się, że rozwiązanie tego problemu jest kluczem do sukcesu, w tym wprowadzania rozwiązań z przygotowujących do wojny informacyjnej.

ppłk dr Adam Halama

Adiunkt Katedry Obrony Powietrznej Wydziału Lotnictwa i OP AON

INFORMACJA O PRZECIWNIKU POWIETRZNYM

Zapewnienie odpowiedniej bazy informacyjnej jest jednym z niezbędnych warunków podjęcia przez dowódcę decyzji, rozumianej jako złożony i twórczy proces pracy umysłowej. Przy podejmowaniu decyzji obiektem poznawczym jest sytuacja bojowa, na której obraz składają się informacje w postaci spostrzeżeń, wyobrażeń i pojęć otrzymywanych z różnych źródeł.

Wśród procesów i zjawisk stanowiących obszar zainteresowania dowódców obrony przeciwlotniczej, niewątpliwie najtrudniejsze są te, które dotyczą prognozowania działań przeciwnika. Prognozowanie to jest niezbędnym elementem procesu decyzyjnego, a jego trafność warunkuje skuteczność prowadzonej następnie walki, również ze środkami napadu powietrznego (ŚNP).

W pracy zatytułowanej *Metodyka oceny przeciwnika powietrznego na szczeblu taktycznym i operacyjno-taktycznym wojsk systemu OP RP*[1] Zbigniew Groszek napisał, że do prawidłowego funkcjonowania obrony powietrznej jest niezbędny zbiór informacji (Z_I) o przeciwniku.

Zbiór ten tworzą informacje pochodzące z otoczenia (I_O) oraz źródeł systemu (I_S), które tworzą zbiór informacji źródłowych (Ij). Gdy $Ij < Z_I$, różnicę (Ip) uzupełnia organ dowodzenia danego szczebla, tak aby spełnić warunek z rys. 1.

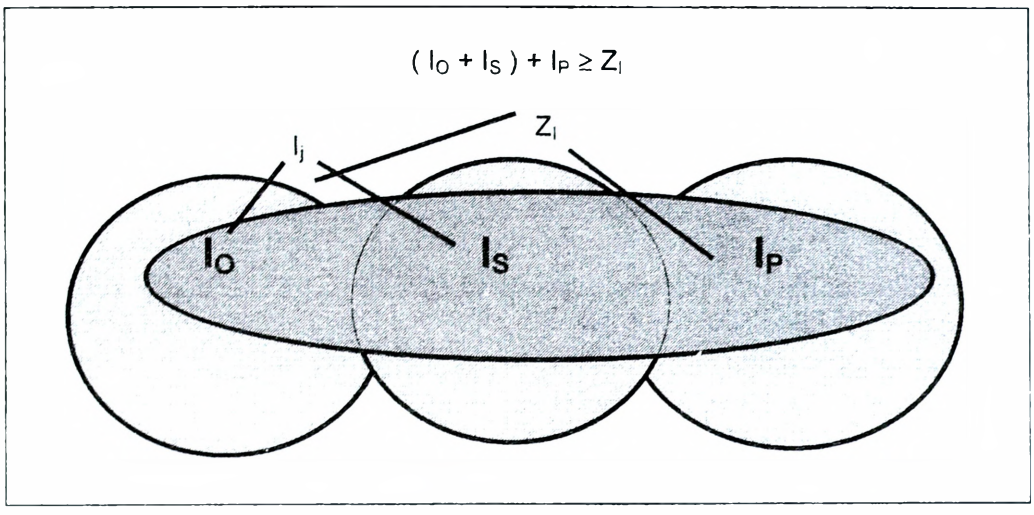
Aby wnioski z oceny przeciwnika były obarczone jak najmniejszym błędem, informacje o przeciwniku i jego działaniach muszą pochodzić z pewnych, wiarygodnych źródeł, a przede wszystkim powinny być produktem doboru właściwych metod jego oceny.

Informacja musi jednocześnie spełniać szereg wymagań[2], by skutecznie i trafnie zasilić organy dowódcze w niezbędne informacje o przeciwniku. Do najważniejszych wymagań należy zaliczyć: ciągłość prowadzonych ocen, wielośródłowość ich pochodzenia, znajomość przeciwnika powietrznego i trafność (realność) dokonanych ocen.

---

[1] Z. Groszek, *Metodyka oceny przeciwnika powietrznego na szczeblu taktycznym i operacyjno-taktycznym wojsk systemu OP RP*, AON, Warszawa 1993.

[2] Por. Z. Groszek, B. Zdrodowski, *Metodyka oceny zagrożenia wojsk lądowych uderzeniami środków napadu powietrznego,* AON, Warszawa 1994.



Rys. 1. Zakres informacji o przeciwniku

Ciągłość prowadzenia oceny przeciwnika powietrznego wiąże się z systematycznym analizowaniem napływających danych o zagrożeniu powietrznym bronionych obiektów. Nie może się ona ograniczać tylko do wybranego czasu działań, np. tylko do okresu wzrostu napięcia międzynarodowego czy powstałych sytuacji kryzysowych w określonym rejonie bądź do okresu przygotowania walki czy operacji, ale proces oceny powinien być systematyczy.

Wielośródłowość informacji o działaniach przeciwnika polega na ich gromadzeniu z wielu różnych źródeł informacyjnych. Ocenę przeciwnika powietrznego powinno się prowadzić na podstawie wiadomości i materiałów o najwyższym stopniu wiarygodności, a więc na wiadomościach wielokrotnie sprawdzonych i potwierdzonych.

Znajomość przeciwnika, szczególnie zaś jego środków napadu powietrznego, w znacznym stopniu ułatwia prowadzenie oceny i prognozowania jego działań bojowych. Dotyczy to w szczególności: wszechstronnej znajomości organizacji, składu bojowego, ugrupowania, możliwości bojowych sił powietrznych przeciwnika oraz poglądów i zasad prowadzenia operacji i walk powietrznych.

Trafność ocen osiąga się poprzez dogłębną analizę i wielowariantowść prognozowanych działań przeciwnika powietrznego. W procesie oceny i prognozowania jego działań, obiektywność zapewnia się wypracowując kilka możliwych wariantów działań przeciwnika, bazując na wariantach najbardziej prawdopodobnych w danej sytuacji operacyjno-taktycznej.

W praktycznej działalności, w końcowym etapie oceny przeciwnika powietrznego niezależnie od warunków oraz zakresu jej prowadzenia, należy posiadać wiarygodne informacje, będące jednoznacznymi odpowiedziami na pytania:

- Jaki cel zamierza osiągnąć przeciwnik powietrzny w działaniach bojowych?

• Z jakich kierunków i na których z bronionych obiektów spodziewać się skupienia wysiłku ŚNP przeciwnika?

• Jaką taktykę działania zastosują ŚNP przeciwnika?

• Jakie skutki bronionym obiektom oraz OP może przynieść oddziaływanie ŚNP?

Potrzebny zbiór informacji o przeciwniku, zapewniający podjęcie racjonalnych decyzji, powinien zawierać:

1) Informacje zawierające możliwie pełną orientację taktyczną:

a) ogólną identyfikację jednostek naziemnych nieprzyjaciela w interesującym obronę powietrzną obszarze;

b) prawdopodobny cel działania przeciwnika;

c) charakter prowadzonych działań;

d) przewidywany manewr;

e) stosowane nowe sposoby i środki walki.

2) Ocenę dotychczasowych działań przeciwnika, w tym jego ŚNP.

3) Prawdopodobny cel działania ŚNP.

4) Rolę i miejsce ŚNP w osiąganiu celu działania przeciwnika.

5) Ocenę bronionych obiektów (przypuszczalnych obiektów oddziaływania ŚNP przeciwnika).

6) Wielkość potencjału bojowego ŚNP:

a) typy i dysponowaną przez przeciwnika liczbę ŚNP w interesującym obronę powietrzną obszarze;

b) stosowane środki rażenia.

7. Taktykę walki ŚNP, często określaną mianem sposobu użycia ŚNP:

a) kierunki sprzyjające skrytemu dolotowi ŚNP do bronionych obiektów i wykonania na nie ataku;

b) trasy, wysokość lotu i czas dolotu ŚNP do obiektów uderzeń;

c) liczbę i skład grup uderzeniowych w poszczególnych falach i rzutach ŚNP oraz kolejność ich wchodzenia w rejon działań bojowych i broniony rejon; odległości i odstępy między grupami, falami i rzutami ŚNP w nalocie;

d) środki rażenia i rubieże ich odpalenia w stosunku do bronionych obiektów i przewidywanych warunków lotu ŚNP;

e) organizację dowodzenia ŚNP w nalocie;

f) sposoby naprowadzania ŚNP na obiekty uderzeń oraz elementy zabezpieczające to naprowadzanie, ich skład i prawdopodobne rejony rozmieszczenia;

g) sposoby stosowania zakłóceń radioelektronicznych, w tym prawdopodobne rejony działania samolotów specjalnych z aparaturą zakłócającą, miejsca znajdowania się i liczbę samolotów zakłócających lecących w ogólnym ugrupowaniu bojowym ŚNP w nalocie, wysokość ich lotu i czas wejścia w strefę wykrywania WRt, ewentualne rubieże lub czas rozpoczęcia stosowania zakłóceń, ich charakterystykę na przewidywanych kierunkach nalotu ŚNP (zakres, rodzaj, moc);

h) prawdopodobne rejony działania grup demonstracyjnych i pozorujących zasadnicze kierunki nalotu w składzie pilotowanych lub bezpilotowych ŚNP;

i) czas trwania nalotu i jego natężenie w bronionym obszarze.

Według procedur innych państw NATO[3] informacje o przeciwniku powietrznym obejmują dane o: bezzałogowych aparatach latających, rakietach (Cruise i balistycznych), samolotach, śmigłowcach, transporcie drogą powietrzną. Środki te rozpatrywane są, przede wszystkim z punktu widzenia:

- położenia rakiet balistycznych i baz środków napadu powietrznego;
- położenia punktów nawigacyjnych;
- zasięgu i możliwości zagrożenia powietrznego;
- możliwej wysokości (pułapu) zagrożenia powietrznego;
- zasięgu taktycznych pocisków balistycznych i innych ŚNP;
- profili lotu taktycznych pocisków balistycznych;
- taktyki lotu;
- typów i dostępności artylerii;
- elementów i taktyki artylerii, takich jak: oddalenie, szybkość i wysokość oraz dowodzenie systemem;
- technicznych zdolności lotnictwa, takich jak: zdolność działania w nocy, maksymalna i minimalna prędkość, pułap, zasięg, ładunek i możliwość tankowania paliwa w powietrzu;
- selekcji obiektów ataku;
- procedur ataków powietrznych;
- całokształtu dowodzenia;
- nawigacji.

Są one więc poszerzone o rakiety balistyczne i zawierają szczegółowe dane o rakietach typu Cruise, wynika to jednak z możliwości rozpoznawczych, szczególnie wojsk amerykańskich.

Informacja ta nie jest jednak potrzebna w pełnym zakresie na każdym szczeblu prowadzenia obrony powietrznej. Z jednej strony na wyższych szczeblach zbędna jest informacja szczegółowa o technice wykonywania uderzenia, z drugiej zaś wykonawcy zadań ogniowych zbędne są informacje typu: potencjał przeciwnika powietrznego czy rola i miejsce ŚNP w osiąganiu celu działania przeciwnika.

Uwzględniając specyfikę obrony przeciwlotniczej informacja o przeciwniku powietrznym powinna być inna w sztabach ogólnowojskowych i inna w sztabach oddziałów i samodzielnych pododdziałów przeciwlotniczych.

W sztabach ogólnowojskowych, w zespołach oceniających przeciwnika, powinien być oceniony również przeciwnik powietrzny. W rozkazach i komunikatach muszą być zawarte informacje o:

1) potencjale bojowym ŚNP (ogólna identyfikacja jednostek sił powietrznych, typy i dysponowana przez przeciwnika liczba ŚNP oraz przewidywany manewr);

2) roli i miejscu ŚNP w osiąganiu celu działania przeciwnika, w tym prawdopodobny cel działania przeciwnika powietrznego;

---

[3] W rozdziale 4 amerykańskiego regulaminu *FM 34-130. Rozpoznawcze przygotowanie pola walki dla potrzeb sztabów i jednostek specjalistycznych* opisano wymagania i zakres oceny przeciwnika na potrzeby jednostek przeciwlotniczych.

3) dotychczasowych działaniach przeciwnika, w tym jego ŚNP, szczególnie zaś stosowanych nowych sposobach i środkach walki;

4) obiektach ataku.

W sztabach oddziałów i samodzielnych pododdziałów przeciwlotniczych, oceniając przeciwnika powietrznego, należy pozyskać informacje o:

1) kierunkach dolotu do obiektów;

2) trasach, wysokości lotu i czasie dolotu ŚNP do obiektów uderzeń;

3) modelu nalotu – liczbę i skład grup w poszczególnych falach i rzutach ŚNP;

4) środkach rażenia i rubieżach ich odpalenia;

5) organizacji dowodzenia i naprowadzania ŚNP w nalocie;

6) formach walki radioelektronicznej;

7) czasie trwania nalotu i jego natężeniu w bronionym obszarze.

W niniejszym materiale zaproponowano jedno z możliwych rozwiązań, jakie według autora umożliwi zebranie posiadanej i wygenerowanie nowej informacji o przeciwniku powietrznym. Oczywiście, nie zostały tu rozwiązane wszystkie problemy związane z tematem wystąpienia; nadal nie rozwiązany pozostaje problem zakresu analizy informacji o przeciwniku powietrznym w baterii, dywizjonie i pułku przeciwlotniczym. Autor ma nadzieję, że to wystąpienie stanie się przyczynkiem do szerszej dyskusji nad problemem.

kpt. pil. mgr inż. Dariusz Sarnecki

3 Korpus Obrony Powietrznej

CECHY INFORMACJI CZYNNIKIEM SELEKCJONUJĄCYM POTRZEBY INFORMACYJNE PROCESÓW DECYZYJNYCH

Decydowanie jest współcześnie traktowane jako najistotniejszy element procesu kierowania. Efektywność procesu decyzyjnego i trafność podjętych decyzji przesądzają o skuteczności kierowania. Pogląd taki jest obecnie powszechnie uznawany przez naukowców zajmujących się problematyką zarządzania. Ilustrują go przedstawione poniżej cytaty:

– *„Na wszystkich szczeblach w organizacji ludzie muszą podejmować decyzje i rozwiązywać problemy. Zadania te są szczególnie ważną częścią pracy kierowników. [...] Podejmowanie decyzji jest, zatem istotną częścią działalności kierownika".*

– *„Kierowanie organizacją można traktować jako permanentny proces podejmowania decyzji".*

– *„Proces podejmowania decyzji jest rzeczywistym ciągiem przekształceń informacji przechodzących kolejne fazy podejmowania decyzji. Procesy informacyjne leżą u podstaw procesu decyzyjnego".*

– *„Główną funkcją kierownika jest podejmowanie decyzji. Wynagradza się go i ocenia według ich skuteczności".*

– *„Podjęcie prawidłowej decyzji, traktowanej jako jedno z naczelnych ogniw procesu zarządzania, staje się dziś przedsięwzięciem coraz bardziej skomplikowanym i wymagającym coraz częstszego uciekania się do form kolektywnych przy szerokim udziale specjalistów".*

– *„Proces zarządzania można rozpatrywać jako ciąg podejmowania decyzji kierowniczych".*

– *„Cele, zadania i decyzje traktuje się łącznie. Obejmują one całość zarządzania organizacją, z tym że decyzja stanowi tu swoisty „most" łączący realizację celów i zadań ze sferą informacji na tle skrajnej złożoności i różnorodności otaczającej nas rzeczywistości".*

Z kolei, dysponowanie odpowiednią informacją jest zasadniczym elementem wpływającym na racjonalność decyzji[1]. W każdym zatem procesie decyzyjnym występuje zapotrzebowanie na odpowiednie informacje. Aby zrozumieć istotę tych potrzeb, należy określić czym jest informacja w procesie decyzyjnym.

Samo pojęcie „informacja" należy do kategorii pojęć pierwotnych i jako takie nie jest w pełni definiowalne. Filozofowie, a w szczególności rozmaite szkoły filozoficzne, socjologowie, ekonomiści, cybernetycy definiują to pojęcie różnie [7, s. 48]. Istniejące definicje uwypuklają tylko niektóre strony informacji, w zależności od dziedziny, dla której potrzeb definicja była tworzona. Poniżej przedstawiono przykładowe definicje tego pojęcia.

– *„Informacja – jedno z podstawowych pojęć cybernetyki, prawdopodobnie nie w pełni definiowalne z uwagi na jego pierwotny, elementarny charakter* [...]".

– *„Informacja jest nazwą treści zaczerpniętych ze świata zewnętrznego w miarę tego, jak się do niego zastosujemy i jak przystosowujemy doń swoje zmysły".*

– *„Informacją jest wszelka wiadomość o procesach i stanach dowolnej natury, które mogą być odbierane przez organy zmysłowe człowieka lub przez przyrodę".*

– *„Informacja jest to związek między stanami tego samego zbioru".*

– *„Informacje są to stany wyróżnione wejść i wyjść układu".*

– *„Współcześnie informacja jest, obok energii, trzecim podstawowy elementem otaczającej nas rzeczywistości".*

W zarządzaniu informacja jest postrzegana jako **czynnik, który zwiększa wiedzę (lub zmniejsza niewiedzę) decydenta o rzeczywistości decyzyjnej**.

Stanowi pełnej wiedzy decydenta o sytuacji decyzyjnej można przypisać wartość jeden, a stanowi niewiedzy wartość zero. Wówczas to można stwierdzić, że wraz z napływem właściwych informacji wartość wiedzy będzie się zwiększać w przedziale od zera do jednego. Widoczna jest tu zależność, którą można wyrazić twierdzeniem: **stopień wiedzy zależy od ilości informacji**.

Stan idealny zostałby osiągnięty, gdyby wiedza decydenta, dotycząca interesującego go problemu, osiągnęła jeden. Nie jest to w realnych, skomplikowanych warunkach możliwe do uzyskania. Teoria informacji w jednym ze swych praw określa to zjawisko następująco: *Brak naszej wiedzy o wybranym fragmencie rzeczywistości rośnie tym szybciej, im bardziej złożony jest problem, którym się interesujemy.*

Problem możliwości dostarczenia decydentowi określonych informacji, wiąże się z problemem czasu zbierania informacji oraz kosztów ich pozyskania.

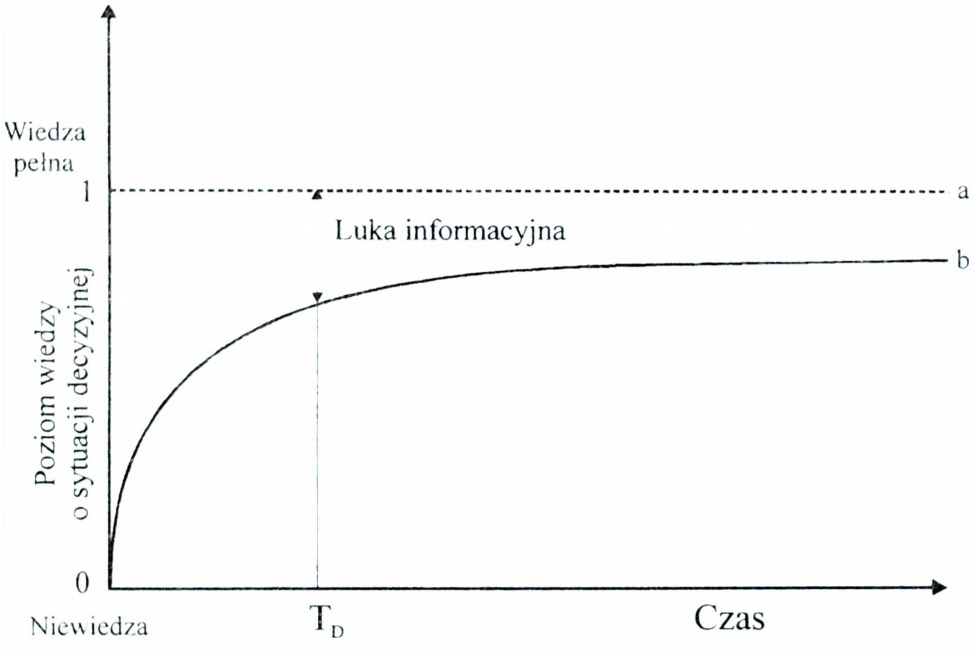
Jeżeli decydent zażąda informacji standardowych, które są rejestrowane w systemie informacyjnym, powinien je otrzymać w miarę szybko. Jeśli są one

---

[1] Należy przyjąć, że racjonalność decyzji jest zachowana, gdy jest ona świadomym, nielosowym, najlepszym w sensie metodologicznym wyborem wariantu działania. T. Kotarbiński traktuje racjonalność metodologiczną następująco: „[...] *sens metodologiczny mamy na myśli, ilekroć uznajemy za rozumne, czyli racjonalne, postępowanie danego osobnika, skoro postępuje on wedle wskazań posiadanej wiedzy, a przez posiadaną wiedzę rozumiemy tutaj ogół tych posiadanych informacji, którym zważywszy na sposób ich uzasadnienia, ów osobnik winien przypisywać prawdopodobieństwo tak, jak gdyby były prawdziwe".*

nieaktualne lub nieprecyzyjne, nie wzbogacą jego wiedzy w zadowalający sposób. W takim przypadku zażąda on uaktualnienia i sprawdzenia informacji. Zanim je otrzyma, ponownie upłynie pewien czas. Jeśli natomiast decydent potrzebowałby informacji niestandardowych, które nie są rejestrowane w systemie, to oprócz czasu, jaki zajęłoby ich przygotowanie, konieczne byłoby poniesienie z tego tytułu dodatkowych kosztów. Jeżeli uwzględnimy czynnik czasu w procesie poznania, to można stwierdzić, że **poziom wiedzy o określonej rzeczywistości wzrasta wraz z czasem poświęconym na zbieranie informacji o nim**. Im więcej czasu poświęcimy na pozyskiwanie informacji, tym więcej możemy ich uzyskać. Czas, zwłaszcza w organizacjach gospodarczych i militarnych, jest bezpośrednio związany z kosztami działania. Można więc wykazać związek między kosztem a informacją. **Koszt pozyskania informacji, wzrasta wraz z jej szczegółowością**.

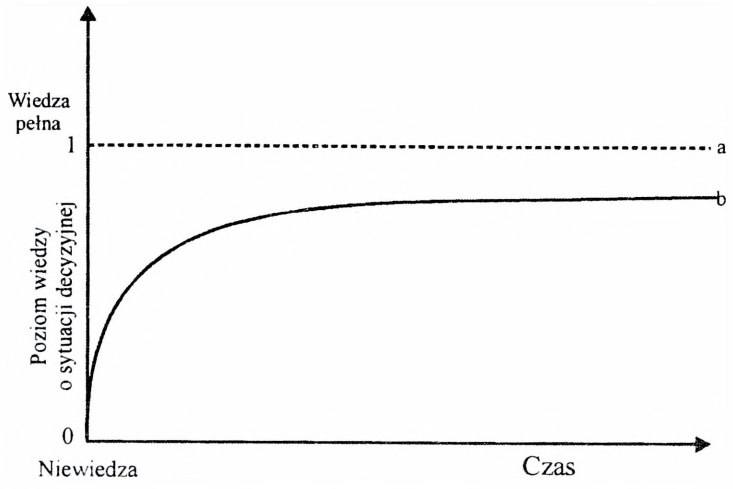
W praktyce bardzo rzadko posługujemy się informacjami pełnymi, lecz przeważnie informacjami dostępnymi, które nie zawsze pozwalają w pełni opisać interesujące nas zjawisko. Różnicę pomiędzy informacją pełną a informacją dostępną, określa się mianem **luki informacyjnej** (rys. 1).



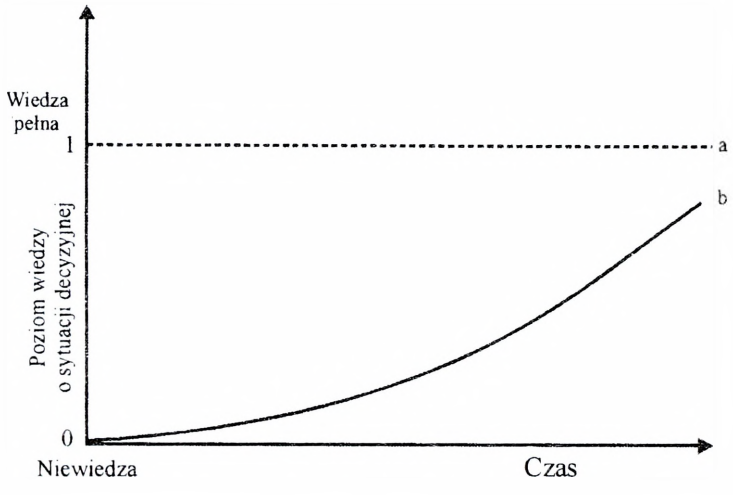
Rys. 1. Luka informacyjna w procesie podejmowania decyzji

Rysunek 1. jest pewnym uproszczeniem, gdyż przedstawia tylko jeden z wielu możliwych przebiegów krzywych opisujących przyrost wiedzy w czasie. Na rys. 2. przedstawiono trzy dalsze przykłady krzywych przyrostu wiedzy o sytuacji decyzyjnej.

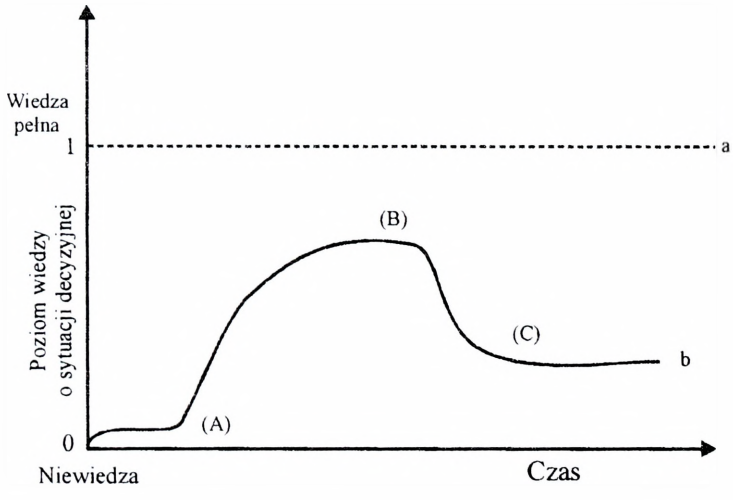
a)



b)



c)



Rys. 2. Rzeczywisty wzrost poziomu wiedzy decydenta

Rysunek 2a przedstawia sytuację, w której decydent już na początku procesu podejmowania decyzji wiedział dość dużo na temat problemu. Dostęp do pamiętanych przez siebie informacji trwał bardzo krótko, stąd też krzywa ta rośnie szybko w początkowym okresie. Rysunek 2b przedstawia odwrotną sytuację – decydent niewiele wiedział o sytuacji na początku procesu, ale w miarę jej poznawania następował gwałtowny przyrost jego wiedzy. Trzeci wariant (2c) opisuje sytuację, gdy kierownik w początkowym okresie wie bardzo mało (A), następnie jego wiedza wzrasta gwałtownie (B) na skutek przypływu informacji, po czym maleje (C) na skutek otrzymania fałszywych informacji, które zniekształcają (zmniejszają) jego wiedzę. Oczywiście, krzywa przyrostu wiedzy nie może przekroczyć osi czasu, gdyż wiedza nie może być ujemna.

Konieczność pogodzenia się ze zjawiskiem istnienia luki informacyjnej podczas podejmowania decyzji, wynika z następujących przyczyn:

1) technicznej niewykonalności zgromadzenia wszystkich informacji;

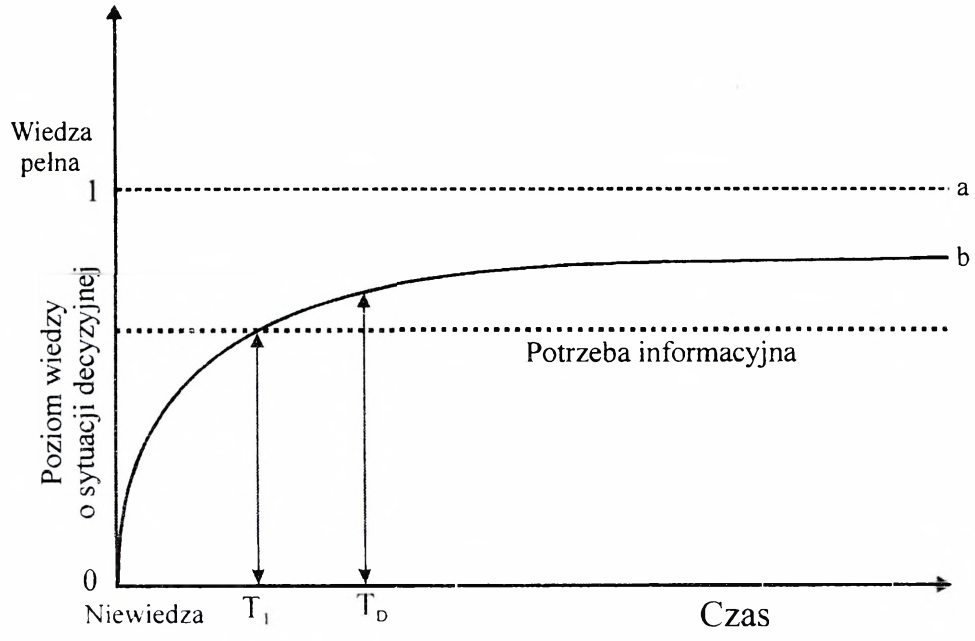
2) kosztów związanych z zebraniem wszystkich informacji, które mogą przewyższyć potencjalne korzyści;

3) wydłużenia czasu gromadzenia informacji, groźby odwlekania decyzji w czasie, szczególnie niekorzystne w dynamicznej sytuacji decyzyjnej;

4) nadmiaru i zbytniej szczegółowości informacji, której mogą przekroczyć możliwości percepcyjne decydenta.

Określając potrzeby informacyjne decydenta w konkretnym procesie decyzyjnym, należy być świadomym ograniczeń wynikających z istnienia zjawiska luki informacyjnej. Za wyznacznik poziomu potrzeb informacyjnych należy przyjąć minimalny poziom wiedzy o rzeczywistości decyzyjnej, jaki zapewni racjonalność podejmowanych decyzji. **Potrzebę informacyjną, wyraża zatem pewien poziom wiedzy o rzeczywistości decyzyjnej, który powinien posiadać decydent, tak aby podejmowane przez niego decyzje spełniały warunki racjonalności metodologicznej**. Rysunek 3. przedstawia potrzeby informacyjne jako pewien ustalony poziom wiedzy. Na prezentowanym tu przykładzie poziom ten zostaje osiągnięty po czasie T_I. Moment podjęcia decyzji powinien być $T_D \geq T_I$, co dla powyższego przykładu jest spełnione.

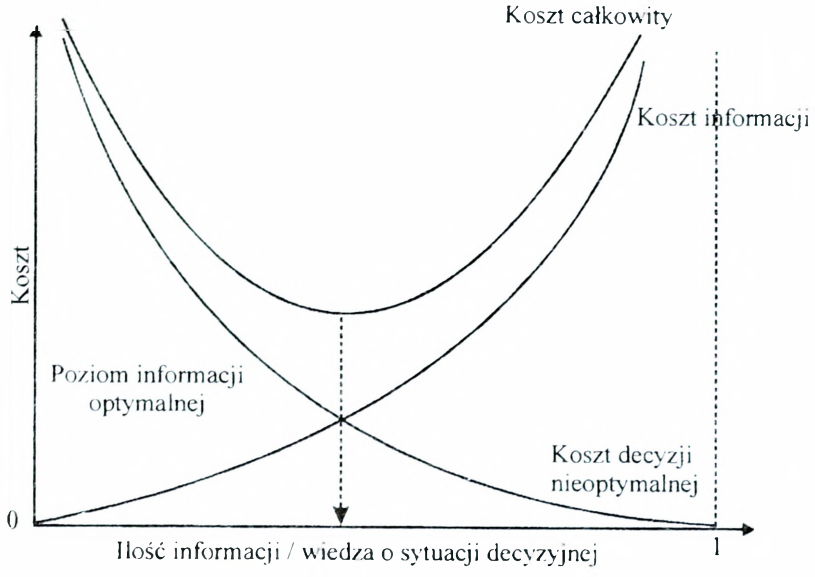
Poziom potrzeb informacyjnych powinien zostać ustalony na pewnym minimum zapewniającym racjonalność decyzji. Zagadnienie to wyjaśnia Wiesław Flakiewicz, który napisał, że *„Przede wszystkim możemy się zapytać, czy zawsze konieczne jest dążenie do poznania całego, aktualnego obszaru wiedzy o danym problemie? Czy dyrektor chcący poznać stan maszyn w fabryce musi znać fizykę ciała stałego oraz orientować się w fizyce atomu? Oczywiście nie. Chodzi tu o selekcję naszej wiedzy na tę, która jest niezbędna do poznania interesującego nas fragmentu rzeczywistości i zbędna lub nieprzydatna w danym momencie czy zakresie. [...] Selekcjonując nasze informacje i koncentrując swą uwagę na określonej jej części, również nie jesteśmy pewni, że znamy zagadnienie w sposób wystarczający, ale przynajmniej możemy ustalić pewne minimum, poniżej którego nie możemy zejść"*.



Rys. 3. Potrzeby informacyjne

Minimum to powinno być określone na poziomie zapewniającym **optymalność decyzji,** przy czym optymalność należy rozumieć jako najmniejszy stosunek kosztu informacji do jej ilości. Zagadnienie to wyjaśnił Wiesław Flakiewicz Zależność tę przedstawiono na rys. 4 następująco: *„Wraz ze wzrostem ilości informacji rośnie progresywnie (nie liniowo) koszt ich uzyskania. Z drugiej strony, najczęściej mamy do czynienia z luką informacyjną, która jest przyczyną podejmowania decyzji nieoptymalnych, a to związane jest z dodatkowym kosztem. Oczywiście wraz ze wzrostem informacji luka ta będzie się zmniejszać, a koszt decyzji nieoptymalnych maleć".*

Określenie informacji stanowiących potrzebę informacyjną za pomocą wyznaczenia poziomu informacji optymalnej jest w rzeczywistości niezmiernie skomplikowane. Wielce problematyczne jest obliczenie kosztu decyzji nieoptymalnej, gdyż w praktyce nie ma właściwego miernika. Nie można również znaleźć miernika dla kosztu informacji jako funkcji jej ilości [4, s. 66]. Metoda ta, mimo iż dotyka sedna problemu, jest rozwiązaniem czysto teoretycznym. Z tego też względu należało poszukać innego sposobu rozwiązania tej kwestii.



Źródło: Opracowanie własne na podstawie [4, s. 66].

Rys. 4. Zależność między ilością informacji i jej kosztami

Do określania potrzeb informacyjnych występujących w procesach decyzyjnych można wykorzystać cechy, jakie posiadają informacje.

Potrzeby informacyjne można potraktować jako **pewien skończony zbiór, którego elementami[2] są informacje[3]**. Jeżeli zbiór ten oznaczymy symbolem I, a jego elementy $i_1, i_2 \ldots i_n$, to możemy to zapisać:

$$I = \{i_1, i_2, \ldots i_n\}$$

Zbiór I traktuje się jako kolekcję informacji zarówno dostępnych, jak i potencjalnie możliwych do otrzymania, niezbędnych decydentowi w określonej sytuacji decyzyjnej. W zastosowaniach teorii mnogości zakłada się z reguły, że wszystkie rozważane zbiory są podzbiorami pewnego stałego zbioru, zwanego przestrzenią. Jeżeli X lub 1[4] oznacza daną przestrzeń, to mamy zatem $A \subset 1$ dla każdego z rozważanych zbiorów. Przez A' lub A^C oznaczymy zbiór elementów przestrzeni, które do A nie należą [10, s. 23], to znaczy:

$$A' = 1 - A$$

Zbiór A' nazywamy dopełnieniem (lub uzupełnieniem) zbioru A. Mamy więc:

[2] Obiekty należące do zbioru.
[3] Zarówno informacje możliwe, jak i potencjalne.
[4] Oznaczenie 1 jest celowe ze względów rachunkowych.

$$x \in A' \equiv (x \in A)' \equiv (x \notin A)$$

Dla przyjętych wcześniej oznaczeń, powyższa zależność będzie miała postać:

$$I' = 1 - I$$

Gdzie *I'* jest dopełnieniem zbioru *I*, czyli zbiorem informacji, które nie są przydatne do rozwiązania danej sytuacji decyzyjnej, a *I* reprezentuje **zbiór potrzeb informacyjnych** dla tej sytuacji.

Aby powyższe zależności mogły być użyteczne, należy wskazać sposoby wyznaczania[5] elementów, które należą do zbioru *I*. Zadanie to sprowadza się to do odpowiedzi na pytanie: Co *pozwala określić jednoznacznie elementy należące do dowolnego zbioru?* Którą dostarcza teoria zbiorów, dowodząc, że **wyliczenie wszystkich elementów zbioru określa ten zbiór jednoznacznie**. Oznacza to, że zbiór jest całkowicie określony przez elementy, które go tworzą. Sposób, w jaki te elementy są określane jest nieistotny. Nie ma różnicy, na przykład między zbiorem składającym się z elementów 2, 3, 5, 7 i zbiorem wszystkich liczb pierwszych mniejszych od 11.

Jednym z często używanych sposobów określenia zbioru jest podanie własności charakteryzującej jego elementy. Przynależność do zbioru ustala dokładnie funkcja zdaniowa[6], będąca zapisem własności przysługującej niektórym elementom dziedziny tej funkcji. Podzbiór zbioru *Z* utworzony z takich i tylko takich elementów *x*, które spełniają funkcję zdaniową *φ(x)*, tzn. mają własność *φ*, zapisuje się symbolem $\{x \in Z: \varphi(x)\}$.

Funkcja określa nam pewną procedurę lub operację, która zastosowana do *x* daje nam *y*. Zazwyczaj operacja ta da się zapisać w postaci mniej lub bardziej skomplikowanego wzoru matematycznego. Współcześnie rozumienie zapisu *f(x)* nie sugeruje, bynajmniej, istnienia jakiegoś prostego obliczenia pozwalającego otrzymać y. Operacja *f* może wymagać użycia wykresu, tabelki lub decyzji według określonych wcześniej kryteriów.

Specyficzną odmianą wykorzystania funkcji określającej przynależność elementów do zbioru, jest zastosowanie predykatu[7] *P(x)*, oznaczającego, że każdy element x zbioru ma własność P. Przykładowo zbiór R = *{czerwony, pomarańczowy, żółty, zielony, niebieski}* jest przykładem zbioru skończonego, który jest opisany przez elementy zbioru.

Predykat *P(x)* przyporządkowuje wartości prawda i fałsz elementom (jeśli element *x* ma wartość *P*, to *P(x)* jest prawdą, w przeciwnym wypadku jest fałszem). Bardzo podobnie można definiować zbiór za pomocą funkcji charakterystycznej.

---

[5] W znaczeniu mechanizmu wybierania informacji ze zbioru cech.

[6] Funkcja zdaniowa – wyrażenie zawierające zmienne wolne, które w wyniku związania tych zmiennych kwantyfikatorami lub podstawienia za nie odpowiednich nazw, stają się zdaniami.

[7] Predykat w semantyce: wyrażenie opisujące cechę wyróżnionego przedmiotu albo relację między wyróżnionymi przedmiotami; także: treść tego wyrażenia; w logice współczesnej: wyrażenie opisujące jakąś właściwość lub relację.

Definicja 1. „Funkcja $\mu_A : X \rightarrow \{1,0\}$ jest funkcją charakterystyczną zbioru A wtedy i tylko wtedy, gdy dla wszystkich x

$$\mu_A(x) = \begin{cases} 1 \text{ dla } x \in A \\ 0 \text{ dla } x \notin A \end{cases}$$

Różnica między definicją zbioru opartą na predykacie a opartą na funkcji charakterystycznej, sprowadza się do tego, że funkcja charakterystyczna zamiast wartości logicznych przyporządkowuje elementom wartości 1 i 0. Wartości te (1 i 0) określa się mianem stopni przynależności.

W takim razie elementy i zbioru I będącego potrzebami informacyjnymi, mogą zostać zapisane następująco:

$$\mu_I(i) = \begin{cases} 1 \text{ dla } i \in I \\ 0 \text{ dla } i \notin I \end{cases}$$

Dowolna informacja może być określona przez zbiór jej postaci, w przypadku informacji będącej potrzebą informacyjną, w rozumieniu zdefiniowanym powyżej, zbiór postaci nie określa jej właściwie. Z punktu widzenia decydenta i procesu decyzyjnego, postać informacji (np. czy jest ona meldunkiem pisemnym czy ustnym) jest mało ważna. Najważniejszy jest natomiast zbiór cech, jakie informacja może posiadać. Jeżeli ten zbiór oznaczymy symbolem C^I, a jego elementy $c^I_1, c^I_2, \ldots c^I_n$ to możemy to zapisać:

$$C^I = \{c^I_1, c^I_2 \ldots c^I_n$$

Istnieją różnice w klasyfikacji cech informacji pomiędzy poszczególnymi naukowcami.

Przydatność informacji w podejmowaniu decyzji należałoby określać na podstawie wartości cech, którymi są:

- istotność,
- dokładność,
- aktualność.

W związku z tym, że zbiór C^I jest trzyelementowy. Wzór (6) należy zapisać w postaci:

$$C^I = \{c^I_{ist}, c^I_{dok}, c^I_{aktu}\}$$

Każdy z elementów tego zbioru może przyjmować pewne wartości. Dla c^I_{ist} będą to prawda lub fałsz. Prawda dla informacji, która jest przydatna w danej sytuacji decyzyjnej (poprawia sprawność celowego działania) i fałsz dla informacji, która jest dla tego problemu nieistotna.

Cecha dokładności

Dokładność informacji stanowi główny wyznacznik jej jakości. Cecha ta określa, w jakim stopniu informacja odzwierciedla rzeczywistość. Wysoka wartość tej cechy oznacza dużą pewność przy podejmowaniu decyzji. Składową tej cechy będzie wiarygodność informacji, gdyż informacja nie może być wiarygodną, jeżeli nie opisuje sytuacji z wymaganą dokładnością.

Jako miarę dla tej cechy należy przyjąć **poziom jej szczegółowości**. Dokładność określana będzie zatem następująco:

– **Zupełna** – gdy informacja oddaje wiernie wszystkie detale rzeczywistości, której dotyczy;

– **Szczegółowa** – gdy informacja nie opisuje wszystkich detali występujących w rzeczywistości, ale możliwe jest na jej podstawie poznanie istotnych jej szczegółów;

– **Konturowa** – gdy obraz, jaki informacja daje zawiera główne elementy, pomijając szczegóły;

– **Powierzchowna** – gdy na podstawie informacji możemy poznać tylko pewne nie zawsze istotne elementy rzeczywistości;

– **Niewielka** – gdy na podstawie informacji możemy określić pewne obiekty, które występują w rzeczywistości;

– **Zerowa** – sytuacja równoznaczna brakowi informacji.

Cecha aktualności

Cecha ta uwzględnia wpływ czasu na zniekształcenie powstające w obrazie rzeczywistości tworzonym na podstawie posiadanej informacji. Można założyć, że wszystkie informacje o rzeczywistości, którymi dysponujemy są historyczne, czyli opisują tę rzeczywistość sprzed roku, miesiąca, godziny czy nawet ułamka sekundy. Tylko informacje będące prognozami dotyczą przyszłości, ale i one są tworzone na podstawie danych historycznych.

Wymóg aktualności należy powiązać z częstotliwością, z jaką należy uaktualniać dane. Wiąże się to z tendencją do zmian, jaką posiada dany obszar rzeczywistości. Niektóre obszary cechuje duża zmienność (rzeczywistość dynamiczna), inne pozostają niezmienione przez bardzo długi czas (rzeczywistość stacjonarna). Ważne jest zatem, aby tendencja do zmian została określona, gdyż uaktualnianie informacji częściej niż jest to konieczne, byłoby po prostu nieekonomiczne. Za miarę wartości tej cechy przyjęto wielkość tej tendencji.

Wartości, jakie się przypisuje cesze aktualności, odpowiadają tempu, w jakim opisywana przez informacje rzeczywistość się dezaktualizuje.

Wysoka – określa informacje, które odnoszą się do rzeczywistości wysoce dynamicznej, w której zmiany zachodzą bardzo szybko. Spełnienie wymogu aktualności, wymaga uaktualniania informacji w czasie rzeczywistym.

Bardzo duża – określa informacje, które się odnoszą do rzeczywistości dynamicznej, w której zmiany zachodzą szybko. Informacje takie powinny być aktualizowane bardzo często, w odstępach określanych w minutach.

Duża – dotyczy informacji, które wymagają kilku aktualizacji dziennie, odstępy między aktualizacjami określane są w godzinach.

Średnia – dotyczy informacji wymagających aktualizacji w odstępach tygodniowych.

Mała – określa informacje, które się odnoszą do rzeczywistości quasi-stacjonarnej. Konieczność aktualizacji w okresach miesięcznych.

Bardzo mała – dotyczy informacji, które raz zebrane, praktycznie nie wymagają aktualizacji.

Przykłady ilustrujące przyjęty wyżej sposób wartościowania, przedstawiono w tabeli 1.

Tabela 1

AKTUALNOŚĆ INFORMACJI – SPOSÓB OKREŚLANIA

Wielkość cechy	Przykład	Częstotliwość uaktualniania informacji
Wysoka	Informacja o położeniu ruchomego celu względem wystrzelonego pocisku podczas naprowadzania go na ten cel.	Urządzenie naprowadzające lub operator muszą otrzymywać aktualną informację o zmianach w położeniu celu tak często, jak to możliwe, bez opóźnienia.
Bardzo duża	Występuje w sytuacji, gdy planujemy atak na poruszającą się kolumnę pancerną i potrzebujemy informacji o położeniu tej kolumny.	Informacje muszą być na tyle aktualne, aby umożliwiły odnalezienie celu.
Duża	Informacje o stanie pogody.	Wystarczy uaktualniać ją kilka razy dziennie.
Średnia	Stan magazynu.	Sprawdzany jest w odstępach tygodniowych.
Mała	Informacja o poziomie wyszkolenia żołnierzy.	Uaktualniana co kilka miesięcy.
Bardzo mała	Informacja topograficzna zawarta w mapach.	Uaktualniana co kilka, kilkadziesiąt lat.

Wartości opisujące cechy dokładności i aktualności są trudne do wyrażenia liczbowego, stąd też powinny być określane werbalnie. Zastosowanie wartościowania opisowego jest tutaj jak najbardziej do przyjęcia i zastosowania. Wymaga ono jedynie potraktowania zbioru potrzeb informacyjnych jako zbioru rozmytego i zastosowania teorii zbiorów rozmytych oraz wyrosłej na jej bazie logiki rozmytej.

Zbiorów rozmytych używa się szeroko w sterowaniu do reprezentacji pojęć lingwistycznych, takich jak wysoki–niski, gruby–chudy, gorący–zimny, stary–młody itp. Przykłady pojęć w tych obszarach często są trudne do wyrażenia jednym słowem. W obszarze temperatury może to być komfortowy, a w obszarze wieku średni.

Biorąc pod uwagę sygnalizowane wcześniej ograniczenia związane z ekonomiką i racjonalnością decyzji, należy dla każdej badanej sytuacji określić pewną wartość progową, która określa minimalną wartość dla danej cechy.

Mając ustalone wartości progowe dla poszczególnych cech, wybieranie informacji potrzebnych (innymi słowy, określanie zbioru potrzeb informacyjnych dla danej sytuacji decyzyjnej), sprowadza się do sprawdzenia wartości progowych (w_P) dla wymienionych wcześniej cech informacji.

Oznacza to, że informacja i należąca do przestrzeni X wypełnia potrzebę informacyjną (czyli należy do zbioru $I = \{i_1, i_2 \ldots i_n\}$) wtedy i tylko wtedy, gdy jej cecha istotności równa się 1 (prawda) oraz jej cecha dokładności jest większa (równa) od ustalonej dla niej wartości progowej oraz jej cecha aktualności jest większa (równa) od ustalonej dla niej wartości progowej.

Jeżeli przyjmiemy następujące oznaczenia:

C^I_{ist} – cecha informacji – istotność

C^I_{dok} – cecha informacji – dokładność

W_{Pdok} – wartość progowa dla C^I_{dok}

C^I_{aktu} – cecha informacji – aktualność

W_{Paktu} – wartość progowa dla C^I_{aktu}

I – zbiór potrzeb informacyjnych

X – przestrzeń informacji

to możemy powyższe stwierdzenie zapisać:

$$I \subset X$$

$$i \in I \Leftrightarrow \left(c^I{}_{ist} = 1 \wedge c^I{}_{dok} \geq w_{Pdok} \wedge c^I{}_{aktu} \geq w_{Paktu}\right)$$

Formuła ta opisuje warunki, jakie musi spełniać informacja, aby była przydatna w procesie decyzyjnym. Pozostałe informacje zmniejszają obszar niewiedzy decydenta w zbyt małym stopniu lub wcale, z tego też względu nie mogą zaspokoić potrzeb informacyjnych procesu decyzyjnego.

LITERATURA:

Antczak S.: *Podstawy dowodzenia siłami powietrznymi*, AON, Warszawa 1997.

Driakov D., Hellendoorn H., Reinfrank M.: *Wprowadzenie do sterowania rozmytego*, WNT, Warszawa 1998.

Flakiewicz W., Wawrzyniak B.: *Zasady i metody podejmowania decyzji kierowniczych*, PWE, Warszawa 1978.

Flakiewicz W.: *Podejmowanie decyzji kierowniczych*, PWE, Warszawa 1971.

Głuszkow W.: *Wstęp do cybernetyki*, KiW, Warszawa 1967.

Greniewski H.: *Cybernetyka nie matematyczna*, PWN, Warszawa 1969

Kofler E.: *Podejmowanie decyzji przy niepełnej informacji*, Zurich, Real Publishers 1993.

Kotarbiński T.: *Traktat o dobrej robocie*, wyd. 5, PWN, Warszawa 1973.

Kowalczyk E.: *Człowiek w świecie informacji*, KiW, Warszawa 1974.

Kuratowski K.: *Wstęp do teorii mnogości i topologii*, PWN, Warszawa 1980 .

Kurnal J.: *Zarys teorii organizacji i zarządzania*, PWE, Warszawa 1969.

Mały słownik cybernetyczny, Wiedza Powszechna, Warszawa 1975.

Mazur M.: *Jakościowa teoria informacji*, WNT, Warszawa 1970.

Miller D. W., Starr M. K.: *Praktyka i teoria decyzji*, PWN, Warszawa 1971.

Sawyer W. W.: *W poszukiwaniu modelu matematycznego*, Wiedza Powszechna, Warszawa 1975.

Wiener N.: *Cybernetyka a społeczeństwo*, KiW, Warszawa 1961.

PUBLIKACJE AKADEMII OBRONY NARODOWEJ

do nabycia w Wydziale Wydawniczym AON
al. gen. A. Chruściela 103, bl. 2
00-910 Warszawa, tel./faks 681 37 52

- H. Binkowski, A. Ciupiński – **Polityka obronna i siły zbrojne partnerów Polski z Grupy Wyszehradzkiej**
- R. Bojarski – **Operacja obronna**
- R. Bojarski – **Główne problemy działań operacyjnych**
- J. Brzozowski – **Metodyka zajęć grupowych**
- A. Bujak – **Praca w terenie na szczeblach taktycznych według standardów NATO**
- M. Cieślarczyk, P. Krawczyk, Z. Korulczyk – **Poradnik metodyczny autorów prac kwalifikacyjnych**
- A. Ciupiński, R. Białoskórski – **Wczesne ostrzeganie i zapobieganie współczesnym konfliktom zbrojnym w strategii Sojuszu Północnoatlantyckiego**
- J. Czaja – **Stolica apostolska wobec integracji europejskiej**
- A. Dawidczyk – **Nowe wyzwania, zagrożenia i szanse dla bezpieczeństwa Polski u progu XXI w.**
- W. Drążczyk – **Logistyka sił powietrznych w działaniach wielonarodowych**
- **Działania (operacje) połączone.** Materiały z konferencji naukowej
- M. Gąska, A. Ciupiński – **Międzynarodowe prawo humanitarne**
- M. Gąska – **Obronność w aktach prawnych RP**
- J. Gotowała – **Lotnictwo XXI wieku**
- J. Groskrejc – **Antropologiczne i aksjologiczne aspekty edukacji oficerów**
- J. Groskrejc – **Nauczyciel w edukacji. Funkcje – kompetencje – koncepcje kształcenia**
- J. Halik – **Metodyka opracowania pracy magisterskiej I studyjnej**
- H. Herman – **Działania specjalne w wojnach i konfliktach zbrojnych po II wojnie światowej**
- M. Huzarski (red.) – **Taktyka ogólna wojsk lądowych**
- K. Jałoszyński – **Terroryzm antyizraelski**
- K. Jałoszyński – **Terroryzm czy terror kryminalny w Polsce?**
- K. Jałoszyński – **Zagrożenie terroryzmem w wybranych krajach Europy Zachodniej oraz w Stanach Zjednoczonych**
- J. Janczak – **Zakłócanie informacyjne**
- T. Jemioło – **Globalizacja. Szanse i zagrożenia**
- A. Jóźwiak, Cz. Marcinkowski – **Wybrane problemy współczesnych operacji pokojowych**
- L. Kanarski, B. Rokicki (red.) – **Teoria i praktyka przywództwa wobec wyzwań edukacyjnych**
- J. Kardas, K. Loranty – **Wybrane problemy bezpieczeństwa i obronności państwa w opiniach pracowników administracji publicznej**
- J. Kardas – **Edukacja kadr administracji publicznej na Wyższych Kursach Obronnych**
- W. Kitler (red.) – **Obrona cywilna (niemilitarna) w obronie narodowej III RP**
- W. Kitler – **Obrona narodowa w wybranych państwach demokratycznych**
- W. Kitler – **Obrona narodowa III RP. Pojęcie. Organizacja. System** (rozprawa habilitacyjna)
- Z. Klawitter – **Wybrane aspekty systemu dowodzenia brygady zmechanizowanej (pancernej) w działaniach taktycznych**
- S. Korzeniowski – **Żandarmeria wojskowa**
- M. Koziński – **Umowa offsetowa i inne formy udziału państwa w międzynarodowym obrocie gospodarczym**
- M. Kozub – **Lotnictwo w operacjach połączonych**
- M. Kozub – **Lotnictwo w bojowym poszukiwaniu i ratownictwie**
- J. Kręcikij – **Metodyka pracy sekcji dowodzenia stanowiska dowodzenia oddziału i związku taktycznego**
- S. Kunnia – **Współczesna brytyjska myśl obronno-ekonomiczna**
- R. Kwećka – **Informacja w walce zbrojnej**
- Z. Lach, J. Skrzyp, A. Łaszczuk – **Wojskowo-geograficzna charakterystyka Niemiec**

- L. Łukaszuk – **Europejskie prawo pokoju i bezpieczeństwa**
- T. Majewski – **Ankieta i wywiad w badaniach wojskowych**
- J. Marczak (red.) – **Samoorganizacja społeczeństwa na rzecz bezpieczeństwa powszechnego. Samoobrona powszechna III RP**
- Z. Maślak, K. Kozłowski, P. Krawczyk – **Podstawy użycia lotnictwa myśliwskiego**
- W. Michalak – **Dominacja z powietrza**
- J. Michniak (red.) – **Projektowanie struktury organizacyjnej dowództwa brygady zmechanizowanej (pancernej)**
- G. Nowacki – **Strategiczne siły jądrowe wybranych państw**
- E. Nowak – **Gospodarowanie zasobami majątkowymi**
- I. Nowak – **Wybrane problemy historii polskiej techniki wojskowej XX wieku. Sprzęt i środki wojsk chemicznych**
- M. Obrusiewicz – **Wielonarodowe połączone siły zadaniowe CJTF**
- J. Pawłowski, A. Ciupiński (red.) – **Umiędzynarodowiony konflikt wewnętrzny**
- J. Płaczek – **Ewolucja polskiej myśli obronno-ekonomicznej w latach 1976–2000**
- J. Płaczek (red.) – **Gospodarka obronna Polski w końcu lat dziewięćdziesiątych. Szanse i zagrożenia**
- **Prawo w stosunkach międzynarodowych. Wybór dokumentów** (praca zbiorowa)
- K. Przeworski – **Ewakuacja jako sposób ochrony ludności**
- A. Radomyski – **Zagrożenie śmigłowcowe dywizji zmechanizowanej**
- A. Rejmak – **Ratownictwo lotnicze**
- S. Sadowski – **Podstawowe zagadnienia teorii walki zbrojnej**
- P. Sienkiewicz – **5 wykładów**
- A. Skrabacz – **Kobiety w obronie narodowej Polski u progu XXI w.**
- Z. Skwarek – **Powietrzne systemy wczesnego wykrywania i powiadamiania**
- K. Słaboń – **Sytuacja jeńców wojennych w konflikcie iracko-irańskim (1980–1988)**
- J. Słowik – **Dowodzenie brygadą zmechanizowaną (pancerną) w natarciu**
- **Słownik terminów z zakresu bezpieczeństwa narodowego** (praca zbiorowa)
- **Słownik terminów z zakresu psychologii** (praca zbiorowa)
- M. Sołoducha, P. Malinowski – **Użycie artylerii w szczególnych rodzajach działań bojowych**
- H. Spustek – **Wybrane zagadnienia badań operacyjnych i modelowania liniowego**
- Z. Stachowiak – **Metodyka i metodologia pisania prac kwalifikacyjnych (licencjackich, magisterskich i podyplomowych)**
- R. Stępień (red.) – **Edukacja w wyższych szkołach wojskowych**
- M. Strzoda, N. Prusiński – **System dowodzenia. Terminologia. Część I**
- R. Szpyra – **Powietrzna sztuka operacyjna wybranych państw**
- B. Szulc, T. Majewski (red.) – **Rozwój kompetencji kierowniczych. Pomiar motywacji studentów i absolwentów AON do rozwoju kompetencji kierowniczych**
- E.A. Wesołowska, A. Szerauc (red.) – **Patriotyzm – Obronność – Bezpieczeństwo**
- J. Wołejszo, Z. Fiołna – **Dowodzenie brygadą zmechanizowaną (pancerną) w obronie**
- J. Wołejszo – **Wybrane aspekty projektowania struktury organizacyjnej zespołu dowodzenia stanowiska dowodzenia brygady zmechanizowanej**
- **Wojsko wobec polskiego października'56. Rezolucje, uchwały, listy** (wybór, wstęp i opracowanie: E. J. Nalepa)
- J. Wojtasik (red.) – **Studia z dziejów polskiej techniki wojskowej od XVI do XX wieku**
- W. Zawadzki, T. Majewski, N. Prusiński – **Informacyjne uwarunkowania procesu decyzyjnego**
- B. Zdrodowski, M. Marszałek – **Operacje pozawojenne sił powietrznych**
- J. Zieliński (red.) – **Podstawowe założenia dydaktyki sztuki operacyjnej**
- J. Zuziak – **Dzieje Instytutu Józefa Piłsudskiego w Londynie 1947–1997**

Zamówienia przyjmujemy telefonicznie lub pisemnie