AKADEMIA
OBRONY
NARODOWEJ

Ppłk dr inż. Gabriel NOWACKI

DZIAŁANIA INFORMACYJNE W OPERACJACH POŁĄCZONYCH

Rozprawa habilitacyjna

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid.
58058

Biblioteka Główna
Akademii Sztuki Wojennej
58058
09-058058-000-0

WARSZAWA 2004

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH
INSTYTUT ZARZĄDZANIA I DOWODZENIA

BIBLIOTEKA GŁÓWNA I ARCHIWUM
Nr ewid. 58058
Akademii Obrony Narodowej

Ppłk dr inż. Gabriel NOWACKI

DZIAŁANIA INFORMACYJNE W OPERACJACH POŁĄCZONYCH

Rozprawa habilitacyjna

WARSZAWA 2004

SPIS TREŚCI

WPROWADZENIE **3**

1. CHARAKTERYSTYKA OPERACJI POŁĄCZONYCH **15**

1.1. Rodzaje operacji połączonych 15
1.2. Planowanie operacji połączonych 18
1.3. Zasady tworzenia struktur wielonarodowych 23
1.4. Rola i cele działań informacyjnych w operacjach połączonych 34
1.5. Efekty poznania 35

2. GENEZA DZIAŁAŃ INFORMACYJNYCH **38**

2.1. Uwarunkowania historyczne działań informacyjnych 38
2.2. Wojna w Iraku 53
2.3. Efekty poznania 74

3. POGLĄDY NA DZIAŁANIA INFORMACYJNE WEDŁUG WYBRANYCH PAŃSTW **77**

3.1. Koncepcja działań informacyjnych NATO 77
3.2. Działania informacyjne według poglądów amerykańskich 79
3.3. Niemieckie poglądy na prowadzenie działań informacyjnych 86
3.4. Działania informacyjne według poglądów rosyjskich 91
3.5. Efekty poznania 100

4. ISTOTA DZIAŁAŃ INFORMACYJNYCH **103**

4.1. Kwestie terminologiczne i klasyfikacyjne 103
4.2. Kompleks przedsięwzięć działań informacyjnych 158
4.3. Koncepcja przewagi informacyjnej 181
4.4. Efekty poznania 199

5. PROWADZENIE DZIAŁAŃ INFORMACYJNYCH **203**

5.1. Planowanie działań informacyjnych 203
5.2. Zasady prowadzenia działań informacyjnych w operacjach połączonych 212
5.3. Efekty poznania 219

ZAKOŃCZENIE **222**

BIBLIOGRAFIA: **226**

WPROWADZENIE

„Najwyższym osiągnięciem jest pokonać wroga bez walki."

Sun Tzu

Wojny towarzyszą ludzkości od zarania dziejów. Zdaniem niektórych autorów[1] są one naturalnym stanem oraz archetypem ludzkiej egzystencji. Jednak wojny nie należy gloryfikować, co stwierdza Cyceron: „Pokój nawet niesprawiedliwy jest pożyteczniejszy niż najsprawiedliwsza wojna".

Pomimo najstraszliwszych doświadczeń, jakie wyniesiono z wojen, ludzkość nie potrafiła na przestrzeni dziejów zlikwidować ich czy obronić się przed nimi.

Jak twierdzi gen. Bolesław Balcerowicz dziś nikt już nie ma złudzeń, że wojna w XXI wieku będzie obecna, tak jak obecna była w dziejach ludzkości.

Wojna jest dla państwa sprawą najwyższej wagi, sprawą życia lub śmierci, drogą wiodącą do przetrwania lub upadku. Dlatego też należy jej poświęcić poważne studia – Sun Tzu[2].

Postęp naukowo-techniczny oraz rozwój nowych technologii informacyjnych pod koniec XX wieku spowodowały powstawanie nowych koncepcji prowadzenia wojen. Zdaniem A. i H. Tofflerów[3] sposoby prowadzenia wojen odpowiadają sposobom zdobywania dóbr materialnych. Przemiany w siłach zbrojnych są paralelą w porządku ekonomicznym przeszłości a szybko zmieniającą się naturą wojny – przy czym jeden czynnik przyśpiesza przemiany drugiego.

Wszelkie działania prowadzone zarówno w sferze wojskowej, jak też cywilnej uzależniają się od napływu aktualnych i wartościowych informacji, przekazywanych z wykorzystaniem systemów informacyjnych, w których na szeroką skalę stosuje się osiągnięcia nowych technologii.

Era społeczeństwa informacyjnego zaczyna się wtedy, gdy większa część dochodu narodowego pochodzi z działalności związanej z przetwarzaniem informacji, a nie z produkcji przemysłowej. W epoce industrialnej o znaczeniu państwa decydowała ilość

---

[1] V. D. Hanson, *Jesień wojny (An Autumn of War)*, Anchor/Vintage 2002, s. 49.
[2] Sun Tzu, *Sztuka wojny*, Warszawa, Przedświt, 1994, s. 13.
[3] A. i H. Tofflerowie, *Wojna i antywojna (War and Antiwar)*, Poznań, Wyd. Zysk i Spółka, 1996, s. 29–34. „Fala pierwsza" – społeczeństwo gospodarki rolnej z muszkietami i pikami jako uzbrojeniem; „fala druga" – ery przemysłowej, kiedy to używano czołgów i bombowców; „fala trzecia" – wieku informacji, wojownicy „wiedzy".

wytwarzanej stali i kwasu siarkowego. W cywilizacji informacyjnej już nie. To okres gospodarki wiedzy.

Technologie informacyjne stanowią wielką szansę dla rozwoju ludzkości, ale tworzą także nowe bariery i nierówności, niosą z sobą wiele zagrożeń, zarówno w sferze militarnej, jak i cywilnej. Uświadomienie sobie tego oraz wiedza na ten temat są konieczne by móc im w porę stawić czoło.

Te zmiany mają także wpływ na sposób prowadzenia wojny. Tradycyjnie wojna toczyła się o terytorium i korzyści ekonomiczne. Wojna społeczeństwa ery informacyjnej będzie toczona o zdobywanie „ludzkich umysłów"[4] lub przestrzeni właściwych dla środowiska informacyjnego.

Istotą nowej koncepcji wojennej stał się system bardziej elastyczny, dynamiczny i zdecentralizowany, oparty na wymianie informacji; system, który wykorzystuje lokalne, bezpośrednio związane z polem bitwy, zasoby informacyjne[5] i odwołuje się do decyzji znakomicie wyszkolonych, w dużym stopniu niezależnych, dowódców.

Jeśli konflikty zostaną ujęte w kategoriach trzech fal przemian, wtedy nie powiemy, że obecnie główny konflikt toczy się pomiędzy światem islamu a Zachodem, ani że jest to starcie „Zachodu z resztą świata", jak sugeruje Samuel Huntington[6]. Ani Ameryka nie chyli się ku upadkowi, jak głosi Paul Kennedy[7], ani nie stanęliśmy w obliczu „końca historii", który ogłosił Francis Fukuyama[8].

Nowoczesne społeczeństwo informacyjne wypracowuje nową zasadę w sposobie przekazywania informacji i wiedzy, zaś nowe technologie informacyjne są czynnikiem, który stwarza zapotrzebowanie na zupełnie nowe rozwiązania organizacyjne.

Kiedyś w społeczeństwach funkcjonowała zasada rozwoju siły militarnej, która miała chronić przed niewolą i służyć do zniewalania innych. Takie formuły jak rzymska: – jeśli pragniesz pokoju, szykuj się do wojny (*si vis pacem, para bellum*) lub angielska – usprawiedliwiam mój kraj, nawet gdy popełnia zbrodnie (*right or wrong, my country*) – należały do repertuaru polityki wszystkich rządów.

---

[4]Dotyczy zespołu myślowego funkcji poznawczych mózgu.

[5]Zasoby informacyjne: rzeczowe (umysłowe, materialne), narzędziowe (detektory, przetworniki, transmitery, sterowniki, rejestratory, komutatory, analizatory), infrastrukturalne (medialne, edukacyjne, naukowo-poznawcze, zarządcze, ogólnodostępnej komunikacji społecznej). L. Ciborowski, *Zasoby informacyjne jako obiekt zarządzania*. VI Międzynarodowa Konferencja Naukowa VALUE 2003. Materiały konferencyjne, Lublin, UMCS, 2003, t. I, s. 183.

[6]S. P. Huntington, *The Clash of Civilizations and the remaking of World order*, New York, Simon and Schuster, 1996, s. 31-40.

[7]P. Kennedy, *U progu XXI wieku (Preparing for the 21st Century)*, tłum. P. Konczewski, Kielce, 1994, s. 16–20.

[8]F. Fukuyama, *The Great Disruption*, New York, Free Press, 1999, s. 49–56.

W ostatnich latach ukształtowała się nowa zasada, która zakłada, iż centralne znaczenie dla wartości organizacji posiadają jej *zasoby wiedzy* (ang. knowledge assets), a nie nagromadzenie środków produkcji, obiektów budowlanych, narzędzi i materiałów. Uważa się, że to zasoby wiedzy i zdolności intelektualne decydują o możliwości dostosowywania się do zmian zewnętrznych.

Zachodzi przy tym konieczność kojarzenia dwóch pozornie sprzecznych zdolności: do elastycznego i szybkiego dostosowywania się do zmieniającej się sytuacji zewnętrznej oraz do przewidywania przyszłych warunków działania. Występuje, z jednej strony, potrzeba ciągłego obserwowania sytuacji zewnętrznej, w otoczeniu konkurencyjnym, a z drugiej, podejmowania w porę takich działań, przedsięwzięć i projektów, które dawałyby duże szanse osiągnięcia sukcesu w przyszłości.

Współczesna wojna, a w zasadzie konflikt zbrojny lokalnej społeczności, może przynieść olbrzymie skutki dla całego globu. Wymagania sojusznicze zobowiązują do przekształcenia armii, a w niej do poszerzenia kompetencji dowódców i żołnierzy, którzy poza doskonałym przygotowaniem do walki pod względem rzemiosła wojskowego, powinni posiadać kompetencje, takie jak: lingwistyczne, kulturoznawcze, prawne, administracyjne oraz psychologiczne.

Sukces operacji połączonych zależy w dużej mierze od terminowej i wiarygodnej informacji. Informacja umożliwia dowódcom podjęcie lepszej decyzji niż przeciwnik, a tym samym pozwala na odniesienie zwycięstwa na polu walki. Zdobywanie informacji (rozpoznanie) znane było już w czasach starożytnych[9]. Najstarszym z zapisów, mówiącym o roli informacji w walce zbrojnej, jest kryterium sukcesu zbrojnego sformułowane przez Sun Tzu w VI w. p.n.e.

Aktualnie informacja staje się dominującym czynnikiem, który ma wpływ zarówno na zachowanie bezpieczeństwa narodowego, jak też na sukces operacji połączonych.

Zarówno państwo, jak i jego siły zbrojne zależne są od swobodnego przepływu treści informacyjnych oraz niezawodnego funkcjonowania systemów informacyjnych. Jest to argument przemawiający za włączeniem technologii informacyjnych we wszelką działalność militarną, szczególnie w proces decyzyjny, aby osiągnąć cele polityczne i wojskowe.

---

[9]Sun Tzu w swoim traktacie pisał: „Poznaj siebie i poznaj wroga, dopiero wtedy twoje zwycięstwo nie będzie zagrożone. Poznaj warunki terenu i pogody, wtedy twoje zwycięstwo będzie całkowite". Poznanie wroga, terenu i pogody — to nic innego, jak prowadzenie kompleksowego rozpoznania, czyli zdobywania informacji. Sun Tzu, op.cit., s. 116.

Będzie to wymagało mistrzowskiego zdobywania informacji, jej wykorzystania, ochrony oraz manipulacji. Można to osiągnąć, realizując przedsięwzięcia działań informacyjnych.

Przedsięwzięcia realizowane w ich ramach (np. zdobywanie informacji, dezinformacja, bezpieczeństwo informacyjne) w znaczny sposób mogą przyczynić się do uzyskania przewagi informacyjnej, co może doprowadzić do zaniechania walki przez przeciwnika, a w razie konfrontacji będzie kartą atutową w pokonaniu go.

Wykorzystanie i ochrona własnych systemów informacyjnych oraz dezorganizacja takich systemów u strony przeciwnej stały się warunkiem *sine qua non* osiągnięcia sukcesu w operacjach połączonych oraz wszelkiej działalności w sferze cywilnej. Uzyskiwana w tym zakresie przewaga jest nie tylko gwarantem, ale wręcz warunkiem bezpiecznej egzystencji, i to nie tylko w skali pojedynczego człowieka czy instytucji, ale i w odniesieniu do państwa czy koalicji. Dlatego też zachowanie bezpieczeństwa narodowego w znacznym stopniu zależy od prowadzenia działań informacyjnych.

Ich znaczenie zostało dostrzeżone w wojnie w rejonie Zatoki Perskiej (w 1991 r.). Siły koalicji atakowały środowisko informacyjne Iraku z wykorzystaniem systemów broni precyzyjnej, o zaawansowanej technologii, systemów informacyjnych pierwszej generacji, systemów rozpoznania wielospektralnego.

Działania informacyjne prowadzone były w byłej Jugosławii, Afganistanie oraz w drugiej wojnie w Iraku (2003 r.).

Zdaniem gen. Richarda Myersa, przewodniczącego Połączonych Szefów Sztabów, wojna w Iraku to przykład nowego standardu prowadzenia działań zbrojnych, polegającego na połączeniu kompleksu przedsięwzięć działań informacyjnych z możliwościami systemu C4IEWS[10] na poziomie strategicznym.

Związane to jest z implementacją koncepcji opartej na nowych technologiach, co nazwano mianem rewolucji w sprawach wojskowych (RMA – Revolution in Military Affairs).

Zdaniem R. Szafrańskiego, pioniera tej rewolucji, działania informacyjne bazują na teorii poznania przeciwnika. Przyczyniają się do uzyskania przewagi informacyjnej, dzięki której wzrost siły bojowej jest generowany poprzez połączenie w system informacyjny sensorów, decydentów i systemów walki w celu osiągnięcia wspólnej świadomości

[10]C4IEWS (Command, Control, Communications, Computers, Intelligence, Electronic Warfare and Sensors) – system dowodzenia, kontroli, rozpoznania i walki elektronicznej.

sytuacyjnej, zwiększenia szybkości dowodzenia i skuteczności uzbrojenia, wzrostu odporności na uderzenia przeciwnika oraz zwiększenia stopnia synchronizacji działań.

Amerykanie, dzięki znakomitemu rozpoznaniu oraz technologiom informacyjnym nie tracili czasu na podejmowanie decyzji i przekazywanie meldunków. Zaistniała na polu walki sytuacja natychmiast była przedstawiana na cyfrowej mapie, a komputer proponował kilka rozwiązań. Dowódca, nawet niższego szczebla, mógł podejmować decyzje w zależności od aktualnej sytuacji. Co więcej, mógł sam koordynować swoje działania ze wsparciem udzielanym mu z powietrza lub przez artylerię.

Wojna ta w sposób szczególny ukazała, że działania informacyjne będą stosowane w przyszłości w operacjach połączonych dla osiągnięcia celów politycznych i militarnych i dlatego należy je włączyć do przyszłego instrumentarium militarnego. W tym zakresie należy dokonać identyfikacji specjalnych narzędzi i technik, które wchodzą w skład działań informacyjnych. Ponadto należy brać pod uwagę zasady dotyczące ich planowania i prowadzenia, które muszą być zrozumiałe dla decydentów i dowódców, którzy będą odpowiadać za ich realizację na potrzeby operacji połaczonych.

Środowisko działań informacyjnych to kompleks wielowymiarowy, składający się z wielu zależnych i powiązanych z sobą niezależnych działań. Te działania dość często prowadzone są jednocześnie dla osiągnięcia celów strategicznych i operacyjnych.

Na podstawie literatury przedmiotu należy sądzić, że kwalifikacje wymagane do prowadzenia działań informacyjnych powinny obejmować znajomość różnego rodzaju dyscyplin naukowych, technologii informacyjnych oraz wykorzystania we właściwym czasie specjalistów i narzędzi oddziaływania informacyjnego.

Ważna rola przypada także technologii informacyjnej, która zwiększa możliwości bojowe sił zbrojnych oraz efektywność działania różnego rodzaju agencji rządowych.

Narodowa infrastruktura informacyjna staje się najważniejsza w zakresie rozwoju i egzystencji danego państwa w świecie. Narodowe systemy informacyjne służą m.in. do zapewnienia bezpieczeństwa państwa oraz prowadzenia działalności w wielu sferach. Narody stają się całkowicie uzależnione od systemów informacyjnych. Systemy te mogą stać się celem potencjalnego ataku obcego państwa i przyczynić się do utraty państwowości, a co za tym idzie – niezależności.

Dlatego też dowódcy poszczególnych szczebli dowodzenia powinni posiadać odpowiednie kompetencje do prowadzenia pełnozakresowych działań informacyjnych.

Zadaniem struktur działań informacyjnych będzie oddziaływanie na proces podejmowania decyzji oraz systemy informacyjne. Wojskowe działania informacyjne nie

są działaniami takimi, jak: zarządzanie czy administrowanie systemami. Jest to oddziaływanie na systemy informacyjne, które obejmuje zarówno ofensywne, jak i defensywne działania skierowane na wszystkie szczeble procesu podejmowania decyzji. Dlatego też przy planowaniu operacji połączonych należy uwzględniać działania informacyjne oraz doskonalić i rozwijać ich struktury i narzędzia.

Problematyka ta jest *sensu stricto* dostrzegana w wielu państwach na świecie. Najwyższą jednak rangę nadano jej w Stanach Zjednoczonych. W sierpniu 1996 r. Dowództwo Szkolenia i Doktryn (TRADOC – Trainining and Doctrine Command) opublikowało „Doktrynę działań informacyjnych".

W związku z nową sytuacją polityczno-militarną Rosja opracowała nową doktrynę wojenną, w której w większym niż dotychczas zakresie podkreślono znaczenie bezpieczeństwa informacyjnego, którego jednym z zasadniczych elementów ma być prowadzenie wielopłaszczyznowych działań informacyjno-psychologicznych.

W kwietniu 1999 r. została przyjęta nowa „Koncepcja strategiczna NATO", w której podkreśla się znaczenie technologii informacyjnych na współczesnym polu walki. W części II, w punkcie: Wyzwania i ryzyko polityki bezpieczeństwa, stwierdza się, że państwowi i niepaństwowi przeciwnicy mogą przeciwdziałać wykorzystywanym coraz powszechniej przez sojusz systemom elektronicznym do prowadzenia działań informacyjnych. Ponadto została opracowana polityka i doktryna działań informacyjnych[11].

Polska, jako kraj członkowski NATO, zobowiązana jest przestrzegać ustalenia zawarte w powyższych dokumentach normatywnych. Udział sił zbrojnych w operacjach sojuszniczych wynika z naszych narodowych interesów, racji stanu oraz z treści „Strategii bezpieczeństwa RP" i „Strategii obronności RP". Dlatego też ogniwa systemu obronności powinny realizować zadania mające na celu ochronę i propagowanie polskich interesów na arenie międzynarodowej, informacyjne osłabienie przeciwnika oraz umacnianie morale, determinacji obronnej i wytrwałości własnego społeczeństwa w warunkach wojennych poprzez informacyjne zabezpieczenie funkcjonowania całego systemu obronności oraz informacyjne oddziaływanie zarówno na przeciwnika, jak i własne społeczeństwo. Pomimo tych aspektów obecnie w siłach zbrojnych nie opracowano odpowiedników natowskich dokumentów normatywnych dotyczących problematyki działań informacyjnych.

---

[11] NATO Military Information Operations Policy (MC-422/1, 2002), NATO Military Information Operations Doctrine (AJP-3,10, 2003).

Badania w tym obszarze problemowym prowadzone są w Akademii Obrony Narodowej. Największy dorobek naukowy ma L. Ciborowski[12], który opracował podstawy teorii walki informacyjnej, a jego prace były publikowane zarówno w kraju, jak i za granicą od 1995 roku.

R. Szpyra[13] w swojej rozprawie habilitacyjnej wprowadził termin operacje informacyjne oraz dokonał ich podziału na państwowe, militarne oraz sił powietrznych. Sam termin budzi pewne kontrowersje, ponadto wszystkie te trzy rodzaje operacji informacyjnych są prowadzone w tym samym środowisku informacyjnym[14] oraz mają te same cele (polityczne), nie wspomniano nic na temat celów militarnych. Nie dokonano podziału odpowiedzialności w tym zakresie pomiędzy agencje rządowe i siły zbrojne.

Działania informacyjne realizowane przez siły zbrojne są skomplikowane ze względu na to, że wojsko korzysta z cywilnej infrastruktury informacyjnej. Wykorzystanie tej infrastruktury, tylko dla celów wojskowych, byłoby z góry nieekonomiczne. Niesie to jednak z sobą pewne niebezpieczeństwo, atak na użytkowników cywilnych powoduje zniszczenie lub zakłócenie systemów wojskowych i *vice versa.*

Autor problematyką działań informacyjnych zajmuje się od 1996 r., opublikował na ten temat ponad 50 prac naukowych, monografii, podręczników, prac studyjnych i artykułów, z których kilka rozpowszechnionych zostało również za granicą („Aarms").

Ponadto brał udział w wielu konferencjach i sympozjach naukowych, organizowanych przez Akademię Obrony Narodowej, Wojskową Akademię Techniczną, Biuro Bezpieczeństwa Narodowego, Dowództwo Wojsk Lądowych, oraz zagranicznych – m.in. w sympozjum naukowym organizowanym przez Organizację Badań i Technologii NATO (NATO RTO) nt. „Wieloplatformowa integracja systemów wykrywania i walki na potrzeby wojsk" (USA, 2002) oraz konferencji naukowej organizowanej przez Naczelne Dowództwo Sił Sojuszniczych Europy (PSYOPS Conference, 2003), na których wygłosił referat nt. „Polskie poglądy w zakresie działań informacyjnych i działań psychologicznych".

---

[12]L. Ciborowski, *Walka informacyjna,* Toruń, A. Marszałek, 1999; Item, *Przestrzenie walki informacyjnej*, Warszawa, AON, 1997; Item, *Zarządzanie zasobami informacyjnymi w walce i operacji,* Warszawa, AON, 2002.

[13]R. Szpyra, *Operacje informacyjne państwa w operacjach sił powietrznych.* Rozprawa habilitacyjna. Warszawa, AON, 2002.

[14]Operacje informacyjne (państwa, militarne, sił powietrznych) jest to aktywność skierowana na zewnętrzne i wewnętrzne systemy informacyjnego komunikowania lub przepływającą przez nie informację, która zmierza do osiągnięcia celów politycznych.

Uwzględniając złożoną sytuację polityczno-militarną na świecie, wdrażanie nowych koncepcji prowadzenia operacji połączonych z wykorzystaniem technologii informacyjnych przez wiele państw, można stwierdzić, że jest to ważny argument dla władz państwowych oraz Sił Zbrojnych RP, przemawiający za:

— określeniem założeń doktrynalnych prowadzenia działań informacyjnych, aby osiągnąć cele dyplomatyczne i militarne, zwalczać terroryzm i akty przestępcze;

— powołaniem i doskonaleniem struktur działań informacyjnych;

— sponsorowaniem badań w zakresie działań informacyjnych.

W konkluzji powyższych rozważań należy stwierdzić, że *niniejsza rozprawa dogłębnie analizuje te problemy i ma na celu określenie istoty działań informacyjnych, zasad ich planowania i prowadzenia w ramach operacji połączonych.*

Przeprowadzona analiza i ocena literatury pozwoliły na dokonanie, w miarę wszechstronnych i wiarygodnych, uogólnień merytorycznych oraz uzyskanie odpowiedzi *na pytanie, jaka jest istota działań informacyjnych. Pozwoliły również na dokonanie syntezy występujących poglądów na działania informacyjne w wybranych państwach. Ponadto umożliwiły określenie genezy i historycznych uwarunkowań działań informacyjnych. Dzięki nim sformułowano podstawowe wymagania, w zakresie planowaia i prowadzenia działań informacyjnych w operacjach połączonych.*

Dotychczasowa wiedza, analiza literatury przedmiotu i doświadczenia wyniesione z udziału w ćwiczeniach oraz wnioski z przetłumaczonych dokumentów normatywnych pozwoliły na sformułowanie *hipotezy roboczej. Działania informacyjne to kompleks planowych przedsięwzięć polegający na wpływaniu na postawy dowódców (decydentów), degradacji nośników danych i systemów informacyjnych przeciwnika, z jednoczesną ochroną nośników danych i systemów informacyjnych wojsk własnych.*

Działania informacyjne, prowadzone w umiejętny sposób, mogą znacząco wpływać na powodzenie operacji połączonych lub prowadzić wprost do „wygaszenia" konfliktu.

Rozwój cywilizacyjny oraz postęp naukowo-techniczny powodują, że zmieniają się formy i środki działań informacyjnych. Oprócz znacznego rozwoju środków walki elektronicznej (mikroprocesory, generatory impulsu elektromagnetycznego, bomby „logiczne", wirusy komputerowe) oraz mass mediów (internet, telewizja, radio, prasa) pojawiły się nowe możliwości oddziaływania, jak chociażby broń wiązkowa (energii kierowanej), światła stroboskopowe wywołujące nudności, czy infradźwięki powodujące depresje, napięcia, strach, sztuczną wesołość, spowolnienie reakcji, dolegliwości sercowe i zaburzenia równowagi. Ponadto mogą być wykorzystywane różne techniki

psychotroniczne prowokujące subiektywne i obiektywne zachowania ludzi ulegających wpływowi sugestii lub autosugestii. Na współczesnym polu walki, w warunkach zbliżonego potencjału militarnego, podobnego wyposażenia i uzbrojenia przeciwstawnych stron, właśnie człowiek staje się czynnikiem decydującym o sukcesie lub porażce.

Prowadzenie działań informacyjnych w ramach operacji połączonych odznacza się specyfiką w zakresie struktur organizacyjno-funkcjonalnych, procesów, procedur oraz dokumentów planistycznych. Rozwiązania tego problemu powinny spełniać oczekiwania narodowe, warunki standaryzacyjne NATO, a także odpowiadać wymogom wynikającym z mnogości komponentów narodowych.

Szeroki obszar problemowy rozprawy oraz potrzeba przeprowadzenia badań wymagała przyjęcia określonej procedury badawczej, w której budowie kierowano się głównie podejściem systemowym. System[15] to wszelki skoordynowany wewnętrznie i wykazujący określoną strukturę układ elementów; rozpatrywany od zewnątrz jest całością, rozpatrywany od wewnątrz – zbiorem, do którego przynależność warunkuje związki między wszystkimi jego elementami; ogół elementów systemu w tym rozumieniu nazywa się składem, ogół zaś związków (relacji) pomiędzy elementami, które są uwarunkowane przez ich przynależność do systemu, nazywa się strukturą. Przeważnie do tej definicji przyjmuje się dodatkowo dwa aksjomaty:

— istnieje wzajemne oddziaływanie systemu i środowiska; oznacza to, że system ma wejście i wyjście;

— system ma przynajmniej jedną cechę, która wyróżnia go od innych.

O stanie systemu można wnioskować na podstawie procesów informacyjnych, których badanie umożliwia cybernetyka. Zajmuje się ona ilościową stroną informacji, co pozwala sprecyzować w ogólnym znaczeniu samo pojęcie informacji oraz logikę przetwarzania informacji. Cybernetyczne podejście do logiki wymaga koniecznie włączenia do niej nie tylko algorytmów świadomego przetwarzania informacji przez myślenie, ale także algorytmów i heurystycznego przetwarzania informacji na poziomie poznania zmysłowego, w toku przechodzenia od obrazów zmysłowych do abstrakcyjnych przedstawień, podczas intuicyjnego poszukiwania rozwiązania problemów itd.

---

[15]Pojęcie system nie ma jednoznacznego desygnatu. W niniejszej rozprawie termin ten jest używany w nawiązaniu do rozumienia holistycznego, ujmującego całość rozpatrywanego zjawiska w kontekście jego związków, tak z otoczeniem, jak i jego wewnętrzną budową. W rozwoju teorii systemów ważną rolę spełniły prace takich autorów, jak: Bertalanffy, Findeisen, Klir, Konieczny, Rappaport, Sage, Sienkiewicz, Szymański, Toffler, Weinberg.

Informacja jest nierozerwalnie związana z systemem, praktycznie zaś trzeba uwzględnić co najmniej trzy podsystemy:

— pierwszy, którego odwzorowaniem jest informacja, czyli system o którym informacja mówi, który informacja opisuje;

— drugi, w którym informacja obiega, jest gromadzona, przechowywana i przetwarzana;

— trzeci, dotyczący języka, w którym informacja jest wyrażona (język opisu).

Z powyższego wynika, że badanie informacji jako takiej, bez wymienionych systemów, byłoby błędem metodologicznym. Rozpoznanie potrzeb informacyjnych użytkownika sprowadza się do zdefiniowania systemu, którego ten użytkownik jest częścią, w jakim funkcjonuje. Liczba wiadomości[16] w danym systemie o jakimś innym systemie w skończonym przedziale czasu jest skończona, a każda wiadomość zawiera informację tylko w ramach tego systemu. Wiadomość zawierająca bogatą treść w jednym systemie może więc nie zawierać żadnej informacji, gdy znajdzie się w innym systemie.

Analiza systemowa, oprócz wspomnianych już aspektów, odgrywa także ważną rolę we wspomaganiu procesów decyzyjnych, m.in.:

— zwiększa jakość informacji,

— umożliwia prowadzenie szybkich analiz sytuacji problemowych,

— zwiększa profesjonalność podejścia do procesów planowania i podejmowania decyzji.

Rozwiązywanie problemów decyzyjnych, wynikających z potrzeb racjonalnej działalności człowieka, wymaga badań operacyjnych (ang. operational research). Rozwiązanie problemu decyzyjnego za pomocą badań operacyjnych jest procedurą składającą się z następujących etapów:

— rozpoznanie sytuacji decyzyjnej i wynikającego z niej problemu decyzyjnego,

— budowa modelu decyzyjnego,

— rozwiązanie problemu decyzyjnego (metodą badań operacyjnych lub programowania matematycznego),

— ocena poprawności i realności uzyskanych rozwiązań oraz ewentualna weryfikacja modelu decyzyjnego,

— przedstawienie rozwiązań decydentowi i ostateczne przygotowanie decyzji.

[16]Przyjęto, że „wiadomość" to specjalnie opracowana informacja na użytek konkretnego adresata (układu odbiorczego – człowieka lub urządzenia technicznego).

W rozprawie, we wszystkich etapach badań, stosowane były metody teoretyczne, takie jak: definiowanie, analiza, wnioskowanie, synteza, porównanie, analogia oraz uogólnienie.

Definiowanie było przydatne w określeniu pojęć dotyczących działań informacyjnych, przewagi informacyjnej oraz procesu decyzyjnego.

Analiza znalazła zastosowanie głównie w celu określenia uwarunkowań historycznych działań informacyjnych oraz aktualnych ustaleń i kierunków zmian w rozpatrywanym obszarze.

Syntezie poddane zostały wnioski z badań teoretycznych, które porównane były następnie z przyjętymi założeniami. Porównanie pomocne było szczególnie w wydobywaniu podobieństw i różnic w rozwiązaniach z zakresu zasad planowania działań informacyjnych w operacjach połączonych.

Równolegle z porównaniem stosowana była analogia, szczególnie we wnioskowaniu o podobieństwach występujących procesów i zjawisk.

Uogólnienie wykorzystane zostało do ujawnienia cech i zjawisk powtarzalnych, a w konsekwencji do sformułowania zasad uniwersalnych, dotyczących przebiegu procesu planowania działań informacyjnych.

Oprócz wspomnianych metod teoretycznych, w badaniach wykorzystano także modelowanie, m.in. zaproponowano modele decyzyjne oraz model uzyskiwania przewagi informacyjnej.

Po wnikliwej analizie literatury przedmiotu, na potrzeby powyższego tematu, przyjęto procedurę badawczą obejmującą pięć etapów.

W pierwszym etapie prowadzono konsultacje i dyskusje ze specjalistami wojskowymi i cywilnymi, uczestniczono w różnego rodzaju formach naukowej wymiany poglądów.

Rozumienie i dostrzeganie luk w istniejącej wiedzy dotyczącej problematyki działań informacyjnych, będącej obszarem zainteresowania autora, stworzyło sytuację problemową, rozpoczynając pierwszy etap badań naukowych.

W drugim etapie badań podjęto próby teoretycznego rozwiązania problemu poprzez analizy, porównania, analogie i dalsze studiowanie literatury. W ich trakcie pojawiła się potrzeba dokonania podziału głównego problemu naukowego na elementy ograniczone pod względem rozległości rozpatrywanych zagadnień. W tym celu wyodrębniono problemy szczegółowe.

Konsekwencją rozwiązania problemów szczegółowych było uzyskanie nowych faktów naukowych, które pozwoliły na weryfikację hipotezy roboczej.

W ramach czwartego etapu badań hipoteza została poddana weryfikacji w celu jej ostatecznego uzasadnienia i sprawdzenia. Główną problematykę badań poddano weryfikacji podczas uczestnictwa w sympozjach naukowych prowadzonych przez AON, WAT, Organizację Badań i Technologii NATO, Naczelne Dowództwo Sił Sojuszniczych Europy (SACEUR).

Piąty etap stanowiło podsumowanie wyników badań, ich uogólnienie i synteza. Przyjęto wiarygodną interpretację rozwiązania problemu badawczego, przedstawioną w pisarskim opracowaniu wyników badań i tym samym stworzono bazę do ich kontynuacji w kolejnych etapach dotyczących struktur organizacyjnych dowództw i jednostek działań informacyjnych na potrzeby Sił Zbrojnych RP oraz NATO, a także stosowanych w tym zakresie procedur i dokumentów planistycznych.

Rozprawa habilitacyjna obejmuje wprowadzenie, pięć rozdziałów oraz zakończenie.

Wprowadzenie zawiera uzasadnienie podjęcia badań, cel badań, problemy badawcze, hipotezę roboczą oraz metody badawcze.

W rozdziale pierwszym przedstawiono ogólne założenia operacji połączonych, zasady ich planowania oraz tworzenia struktur wielonarodowych.

Rozdział drugi zawiera uwarunkowania historyczne działań informacyjnych oraz przykład ich prowadzenia w wojnie w Iraku.

Rozdział trzeci obejmuje analizę i syntezę poglądów natowskich, amerykańskich, niemieckich i rosyjskich w zakresie prowadzenia działań informacyjnych.

W rozdziale czwartym przedstawiono kwestie terminologiczne i klasyfikacyjne oraz określono założenia teoretyczne działań informacyjnych. Ponadto zaproponowano koncepcję przewagi informacyjnej.

Rozdział piaty obejmuje zasady planowania i prowadzenia działań informacyjnych w operacjach połączonych.

W zakończeniu rozprawy przedstawiono ocenę stopnia realizacji zadań badawczych, propozycje dotyczące zastosowania wyników badań oraz kierunki dalszego pogłębiania i rozszerzania badań.

1. CHARAKTERYSTYKA OPERACJI POŁĄCZONYCH

1.1. Rodzaje operacji połączonych

Działania informacyjne będą prowadzone równocześnie przez więcej niż jeden rodzaj sił zbrojnych i dlatego będą kontrolowane na poziomie sił połączonych (również sojuszu, koalicji). Ze względu na powyższe celowym jest dokonanie ogólnej charakterystki operacji połączonych.

Istotą operacji połączonych jest taka synchronizacja działań rodzajów sił zbrojnych aby efekty poszczególnych komponentów jako całości były wyższe od sumarycznych efektów jednostkowych poszczególnych komponentów. W warunkach zrównoważonego środowiska, różnych kierunków działania i zróżnicowanego oddziaływania zachodzi konieczność czasowej i przestrzennej synchronizacji operacji lądowych, powietrznych i morskich.

Celem operacji połączonych w ramach artykułu 5. jest zniszczenie sił przeciwnika i załamanie jego woli kontynuowania dalszych działań. Natomiast celem operacji połączonych spoza atykułu 5. jest wymuszenie na stronach konfliktu zaprzestania działań zbrojnych, niedopuszczenie do przekształcenia się kryzysu w konflikt zbrojny poprzez nakłonienie stron do rokowań pokojowych[17].

Osiągnięcie tych celów jest możliwe gdy wszystkie komponenty prowadzą połączone zadania zgodnie z zasadami prowadzenia operacji połączonych. Głównym determinantem jest osiągnięcie celu operacji przy jak najmniejszych stratach. W tym kontekście wyróżnia się trzy główne aspekty operacji połączonych: strukturalny, fukcjonalny i personalny.

Aspekt strukturalny dotyczy działań z udziałem co najmniej dwóch rodzajów sił zbrojnych lub działań wielonarodowych z udziałem kilku państw w tym spoza NATO. Istotne jest w tym wypadku posiadanie takiej struktury dowodzenia która w zależności od sytuacji umożliwi wybór i połączenie poszczególnych komponentów.

Aspekt funkcjonalny, obejmuje zespolenie możliwości rodzajów sił zbrojnych w zakresie sprawnego działania w dążeniu do osiągnięcia zakładanego celu przy optymalnym efekcie synergicznym.

---

[17] R. Bojarski – Główne problemy działań operacyjnych AON. W-wa 2001 r.

Aspekt personalny zakłada współpracę dowódców poszczególnych komponentów i wewnętrznego przekonania o celowości prowadzenia działań połączonych. Wiąże się to z wspólnym systemem pojęć oraz dogłębną znajomością potencjalnych możliwości oraz posiadanych ograniczeń. W zależności od charakteru zadań i środowiska, w jakim mogą być one prowadzone, dowodzenie operacją przypada dowódcy który reprezentuje ten rodzaj sił zbrojnych, który w danej operacji spełnia wiodącą rolę[18].

Operacje połączone dzielą się m.in. na:

— połączone operacje narodowe – z udziałem komponentów jednego państwa (Joint Operations);

— wielonarodowe operacje połączone (Combined Joint Operations – CJO);

— sojusznicze operacje połączone (Allied Combined Joint Operations).

Połączone operacje narodowe dotyczą sił zbrojnych jednego państwa i przynajmniej dwóch komponentów reprezentujących dwa rodzaje sił zbrojnych. Obejmują one dwie płaszczyzny zadaniowe:

— szeroko rozumianą obronę państwa w celu przeciwdziałania zagrożeniom zewnętrznym i wewnętrznym;

— zobowiązania sojusznicze w ramach zadeklarowanych przedsięwzięć.

Kierowanie operacją powierza się dowódcy rodzaju sił zbrojnych, który w danej operacji będzie spełniać wiodącą rolę. Działania zgrupowań różnych rodzajów sił zbrojnych podejmowane dla osiągnięcia celu strategicznego mogą być prowadzone w czasie pokoju, kryzysu i wojny.

Wielonarodowe operacje połączone prowadzone są z udziałem wojsk państw sojuszniczych oraz partnerskich. Charakteryzują się one wysokim stopniem złożoności. Wynika to z faktu iż poszczególne komponenty mają swoją narodową tożsamość co utrudnia współpracę w zakresie podejmowanych decyzji i realizowanych zadań.

Niezależnie jednak od tego Wielonarodowe Siły Połączone (Combined Joint Task Force-CJTF) mają składać się z rozdzielonych ale nie oddzielnych sił – jak określono to na szczycie NATO w 1994r. Problemem są wyzwania logistyczne oraz standaryzacja sprzętu, jak też kompatybilność w zakresie szkolenia i procedur dowodzenia. Ważne jest wzajemne zrozumienie i współdziałanie wszystkich sił uczestniczących w operacjach wielonarodowych. Z drugiej jednak strony wielonarodowość wzbogaca tę współpracę o najbardziej wartościowe elementy poszczególnych komponentów i zwiększa możliwości

[18] M.Wiatr, M.Kozub, *Operacje połączone,* Myśl Wojskowa nr 1, Warszawa, 1999.

operacyjne. Nie bez znaczenia jest też aspekt polityczny powstania i wspólnego działania tych sił. Operacje wielonarodowe klasyfikowane są jako operacje reagowania kryzysowego oraz jako operacje spoza art. 5. traktatu waszyngtońskiego. Celem tego typu operacji, po 11 września 2001 roku i po doświadczeniach w byłej Jugosławii, jest wspólna walka z szeroko rozumianym terroryzmem na całym świecie.

Wielonarodowa operacja połączona prowadzona jest przez jednolite dowództwo i obejmuje wspólne działania różnych rodzajów sił zbrojnych, we współdziałaniu z siłami zbrojnymi innych państw. Za planowanie i prowadzenie działań odpowiada szczebel operacyjny, chociaż ich zarysy i cele powstają na szczeblu strategicznym. Dlatego wyodrębnia się dwie fazy planowania:

— planowanie kampanii (*Campaign Planning)* ma miejsce najczęściej już w okresie pokoju i realizowane jest jako planowanie wyprzedzające (*Advance Planning*), uwzględniające hipotetyczne sytuacje;

— planowanie operacji (*Operational Planning)*. W sytuacjach kryzysowych realizuje się tzw. planowanie kryzysowe (*Crisis Response Planning*), a więc dostosowanie istniejących planów do konkretnej sytuacji lub też opracowanie nowych planów od podstaw.

W celu realizacji określonych zadań siły zbrojne państw sojuszniczych i państw partnerskich organizują Wielonarodowe Połączone Siły Zadaniowe *(Combined Joint Task Forces- CJTF)*. Siły te składają się z komponentów narodowych państw – członków NATO, UE lub państw partnerskich mając w swoim składzie co najmniej dwa rodzaje sił zbrojnych. Siły te tworzone są doraźnie w celu realizacji określonych zadań i pod tym kątem dobierane jest zarówno wyposażenie, jak i struktura organizacyjna[19].

Pełne dowodzenie (Full Comand – FULLCOMD) – władza wojskowa i odpowiedzialność przełożonego za wydawanie rozkazów podwładnym. Obejmuje wszystkie aspekty działań wojskowych i administracyjnych i występuje jedynie w ramach sił narodowych.

Dowodzenie operacyjne (*Operational Command – OPCOM*) – uprawnienia dowódcy do stawiania zadań podległym dowódcom, rozwijania jednostek do działań, do zmiany ich podporządkowania oraz przekazywania części uprawnień dowodzenia. Uprawnienia te nie obejmują odpowiedzialności logistycznej i administracyjnej.

---

[19] A. Obrusiewicz, *Wielonarodowe Połączone Siły Zadaniowe CJTF*, Warszawa, AON, 2002, s. 27.

Kontrola operacyjna (*Operational Control – OPCON*) – zakres władzy przyznany dowódcy do kierowania przydzielonymi mu siłami w celu wykonania określonego zadania, ograniczony zwykle co do rodzaju, miejsca i czasu. Pozwala na kierowanie operacją, sprawowanie lub przekazanie kontroli nad przydzielonymi jednostkami bez możliwości stawiania nowych zadań dla części tych sił. Uprawnienia te nie obejmują odpowiedzialności administracyjnej ani logistycznej.

Sojusznicze operacje połączone to takie działania, w których biorą udział elementy więcej niż jednego rodzaju sił zbrojnych oraz więcej niż jednego państwa członkowskiego NATO. Klasyfikowane są jako operacje wojenne w ramach obrony kolektywnej jednego z państw NATO lub całego sojuszu oraz jako operacje reagowania kryzysowego wynikające zarówno z art. 5. traktatu waszyngtońskiego, jak i spoza tego artykułu. Prowadzone mogą być w trzech fazach:

— początkowej (*Initial)*;

— podtrzymywania *(Sustainment)*;

— przejścia *(Transition)*.

Faza początkowa trwa od decyzji Rady Północno-atlantyckiej do wprowadzenia do rejonu operacji sił głównych. W fazie tej dochodzić będzie do narastania intensywności konfliktu od wymiaru regionalnego do konfliktu na dużą skalę i w tym czasie użyte zostaną siły zdolne do przerzutu..

W fazie podtrzymywania prowadzone będą wielonarodowe działania połączone z użyciem sił głównych.

Faza przejścia to faza o niskiej intensywności konfliktu, a jednocześnie konieczności stabilizowania sytuacji.

1.2. Planowanie operacji połączonych

Proces planowania operacji połączonych obejmuje pięć, kolejno po sobie następujących faz planistycznych, w ramach, których wypracowany wynik końcowy poprzedniej fazy stanowi podstawę do rozpoczęcia następnej:

— faza I – wprowadzenie operacyjne (*ang. Initiation stage*);

— faza II – orientowanie operacyjne (*ang. Orientation stage*);

— faza III – opracowanie zamiaru działania (*ang. Concept development stage*);

— faza IV – opracowanie planu (*ang. Plan development stage*);

— faza V – weryfikacja planu (*ang. Plan review stage*).

Proces planowania działań może być prowadzony prawie równolegle na kilku szczeblach dowodzenia. Zależeć to będzie zarówno od charakteru planowanych działań, jak i od zakresu prowadzonych prac planistycznych. W takiej sytuacji dużą rolę odgrywać będzie ścisła koordynacja pomiędzy poszczególnymi dowództwami oraz poszczególnymi państwami partycypującymi w wielonarodowych siłach połączonych.

Faza I – wprowadzenie operacyjne (*ang. Initiation stage*) obejmuje następujace przedsięwzięcia:

— otrzymanie ze szczebla nadrzędnego dyrektywy wstępnej lub samodzielne rozpoczęcie planowania;

— przeprowadzenie wstępnej oceny sytuacji strategicznej w oparciu o posiadane do tej pory informacje;

— zorganizowanie specjalistycznego zespołu w ramach dowództwa, składającego się z odpowiednio przygotowanych, reprezentujących różne specjalności oficerów, którzy rozwiązywać będą problemy planistyczne, określanego jako **Grupa Planowania Działań** (*ang. Operational Planning Group – OPG*) oraz zgromadzenie niezbędnych informacji do rozpoczęcia procesu planowania.

Faza II – orientowanie operacyjne (*ang. Orientation stage*) rozpoczyna właściwy proces planowania, obejmuje a**nalizę zadania,** która może być prowadzona metodą „burzy mózgów", a która ukierunkowuje cały procesu planowania. Przeprowadza się ją w celu określenia istoty problemu, sprecyzowania rezultatów, jakie powinny być osiągnięte oraz ustalenia pożądanego stanu końcowego. Dowódca jest osobiście odpowiedzialny za prowadzenie analizy zadania. Chociaż sama analiza prowadzona jest przez wyspecjalizowany zespół dowództwa, rezultaty pracy specjalistów realizujących to zadanie muszą uzyskać aprobatę dowódcy przed rozpoczęciem kolejnych czynności procesu planowania. Można stwierdzić, iż celem prowadzenia analizy zadania jest niejako określenie „ograniczeń" sytuacji decyzyjnej, którą należy rozwiązać.

W trakcie analizy zadania powinny zostać rozpatrzone następujące problemy:

— sytuacja polityczno – militarna w obszarze odpowiedzialności, w tym prawdopodobny cel (cele) oraz możliwości stron sporu/konfliktu;

— myśl przewodnia przełożonego;

— ograniczenia w procesie planowania;

— przewidywania (założenia);

— czynniki wpływające na realizacje zadania;

— silne i słabe strony;
— środki ciężkości;
— punkty decydujące;
— zadania (*Tasks*);
— cele;
— pożądany stan końcowy;
— kryteria powodzenia.

Zadanie (*Mission*) – jest jasnym, zwięzłym stwierdzeniem określającym: **kto** będzie realizował określone działanie, **co** będzie realizował, **kiedy** to będzie realizowane, **gdzie** to będzie realizowane i **jaki jest cel** realizacji tego zadania.

Odprawa informacyjna prowadzona jest w celu przedstawienia dowódcy wniosków ze wszystkich aspektów rozważanych w trakcie analizy zadania oraz wydania wytycznych dowódcy do dalszego planowania. Odprawa ta podsumowuje informacje zawarte w otrzymanych dyrektywach i wstępnie zidentyfikowane problemy oraz pozwala dowódcy na wyciągnięcie wniosków dotyczących istoty otrzymanego zadania. Wynikiem informowania operacyjnego jest przygotowanie **wytycznych dowódcy do planowania**, które odzwierciedlają akceptację przez dowódcę wyników analizy zadania, w tym przyjmowanych przez sztab kierunków dalszej pracy.

Konsekwencją orientowania operacyjnego są **wytyczne dowódcy do planowania** – jest to formalny dokument, który może służyć jako **dyrektywa wstępna** do rozpoczęcia planowania zarówno na własnym szczeblu dowodzenia, jak i w podległych dowództwach. Wytyczne dowódcy do planowania – produkt finalny odprawy informacyjnej, poszerzone przez dowódcę o dodatkowe informacje, obejmują trzy główne grupy problemów:
— myśl przewodnią dowódcy;
— jego pogląd na pożądany stan końcowy;
— sprecyzowane zadanie własne.

Poprzez wykorzystanie wytycznych w charakterze dyrektywy wstępnej dla podwładnych, podlegli dowódcy otrzymują możliwość rozpoczęcia własnych przygotowań do przyszłych działań. Podjęte na podstawie tych informacji czynności będą następnie przydatne w trakcie trzeciej fazy planowania.

Faza III – opracowanie zamiaru działania (*ang. Concept development stage*) obejmuje następujące przedsięwzięcia:
— ocenę czynników wpływających na wykonanie zadania (analiza sytuacji);

— opracowanie wariantów działania;

— odprawę decyzyjną;

— opracowanie zamiaru działania.

Efektem tej fazy jest **zamiar działania** (ang. *Concept of Operations – CONOPS*), który jest kolejnym dokumentem wyrażającym sposób, w jaki dowódca zamierza użyć oddane mu do dyspozycji siły, czas ich użycia oraz miejsce, a także cele do osiągnięcia i pożądany stan końcowy. Zamiar działania zawiera informacje wyjaśniające jak należy zsynchronizować możliwości dostępnych sił, aby osiągnąć pożądane cele. Zanim zostanie on rozwinięty do postaci planu działania przedstawiany jest do akceptacji **w postaci formalnego dokumentu** temu szczeblowi dowodzenia, który uruchomił proces planistyczny poprzez wysłanie dyrektywy wstępnej.

Zamiar jako dokument zawiera zwykle:

— opis sytuacji;

— sprecyzowane zadanie własne;

— myśl przewodnią dowódcy;

— zarys przebiegu działań;

— potrzeby w zakresie sił;

— ogólną koncepcją wsparcia logistycznego;

— zasadnicze ustalenia w ramach organizacji dowodzenia.

Faza IV – opracowanie planu (*ang. Plan development stage*) to końcowy etap prac planistycznych, w ramach którego zostaje zatwierdzony **plan działania** (*ang. Operation Plan – OPLAN*). Jest to dokument planistyczny, przygotowywany w odpowiedzi na aktualne lub powstające zagrożenie sojuszu lub kryzys międzynarodowy, w którego rozwiązanie NATO może być zaangażowane. Plan działania opracowywany jest na podstawie założeń zawartych w dyrektywie wstępnej, może być przygotowywany na wszystkich szczeblach dowodzenia. Plan zapewnia współpracę dowódców stosownych szczebli dowodzenia z władzami cywilnymi i państwami członkowskimi sojuszu oraz innymi organizacjami międzynarodowymi i państwami uczestniczącymi w rozwiązaniu sytuacji kryzysowej. W pełni opracowany plan jest uzupełniony właściwą liczbą aneksów.

Faza V – weryfikacja planu (*ang. Plan review stage*) obejmuje dwa zasadnicze etapy: **sprawdzanie i ocenę**. W konsekwencji tych przedsięwzięć może zajść niekiedy potrzeba przeprowadzenia dodatkowej odprawy decyzyjnej.

Sprawdzanie planu pod względem zgodności z aktualnymi wymaganiami i wyzwaniami stojącymi przed sojuszem, realizowana jest dwutorowo, poprzez sprawdzanie ciągłe i okresowe.

W trakcie działań plan musi być sprawdzany, a właściwie weryfikowany w sposób ciągły, gdyż pojawiające się zmiany w sytuacji powodować będą konieczność uaktualnienia planu. Uaktualnienie takie może zostać zarządzone także przez szczebel nadrzędny. W każdym przypadku konieczna jest ocena, czy wystarczające będzie uaktualnienie planów już istniejących, czy też konieczne stanie się sporządzenie nowych. Aktualizacja koncentrowana jest głównie na nowych zagrożeniach, dyspozycyjności sił, poprawności planów alternatywnych, zmianie mandatu sił wsparcia pokoju itp. Po dokonaniu weryfikacji planu, dowódca zostaje zapoznany z wynikami tego przedsięwzięcia, łącznie z propozycjami działań, jakie powinny być podjęte w związku ze zmianami sytuacji. Istotne jest, iż każda zmiana o charakterze zasadniczym, wprowadzona do planu, wymagała będzie ponownej akceptacji przez właściwy szczebel nadrzędny.

Sprawdzanie okresowe stanowi kompleks przedsięwzięć realizowanych cyklicznie w poszczególnych dowództwach, w celu zapewnienia aktualności planów pomimo następujących zmian w sytuacji.

Ocena planu prowadzona jest na podstawie jego szczegółowego sprawdzania, także poprzez ćwiczenia i symulacje. Biorąc pod uwagę kryteria czasu i otrzymane wyniki, za najbardziej efektywne przyjmuje się stosowanie symulacji komputerowych. Jednakże nie dopuszcza się do całkowitej rezygnacji z ocen dokonywanych przez doświadczonych oficerów (oczywiście tych nie zaangażowanych bezpośrednio w przygotowanie planu). Wybór metody oceny planu podyktowany jest zawsze czynnikami czasu i dostępnością środków symulacji komputerowej w konkretnym dowództwie i określonej sytuacji.

Jeżeli ocena planu wykaże, iż wymagane są w nim zasadnicze zmiany, zaś posiadany czas jest wystarczający, proces planowania rozpoczynany jest ponownie, począwszy od fazy drugiej. Wymaga to analizy wszystkich niezbędnych czynników i w efekcie przynosi propozycje niezbędnych modyfikacji. Zmiany te zostają następnie przedstawione dowódcy w trakcie dodatkowej odprawy decyzyjnej. Jeśli natomiast czas jest ograniczony, wówczas weryfikacja może zostać skrócona i koncentrować się na ocenie zmienionej sytuacji, jej potencjalnym wpływie na istniejący plan oraz zawierać propozycje niezbędnych zmian.

Dodatkowa odprawa decyzyjna, jeżeli jest organizowana, powinna być krótka i merytoryczna. W jej trakcie należy poruszyć, co najmniej następujące problemy:

— uaktualnioną sytuację (siły stron konfliktu, siły własne);
— oddziaływanie nowej sytuacji na bieżący plan;
— potencjalne zmiany w istniejącym planie;
— ryzyko związane z dotychczasowym planem (jakie mogą być konsekwencje wprowadzenia zmian lub pozostawienia planu w dotychczasowej postaci);
— propozycje zmian.

Faza piąta kończy przebieg procesu planowania działań NATO. Szczegółowa analiza problemów rozpatrywanych w ramach weryfikacji planu prowadzi do wniosku, iż pomimo użycia do jej opisu terminy *faza* (*Stage*), przedsięwzięcia w nich występujące realizowane są w sposób ciągły, stwarzając gwarancje utrzymania aktualności już gotowych oraz przygotowywanych planów działania.

1.3. Zasady tworzenia struktur wielonarodowych

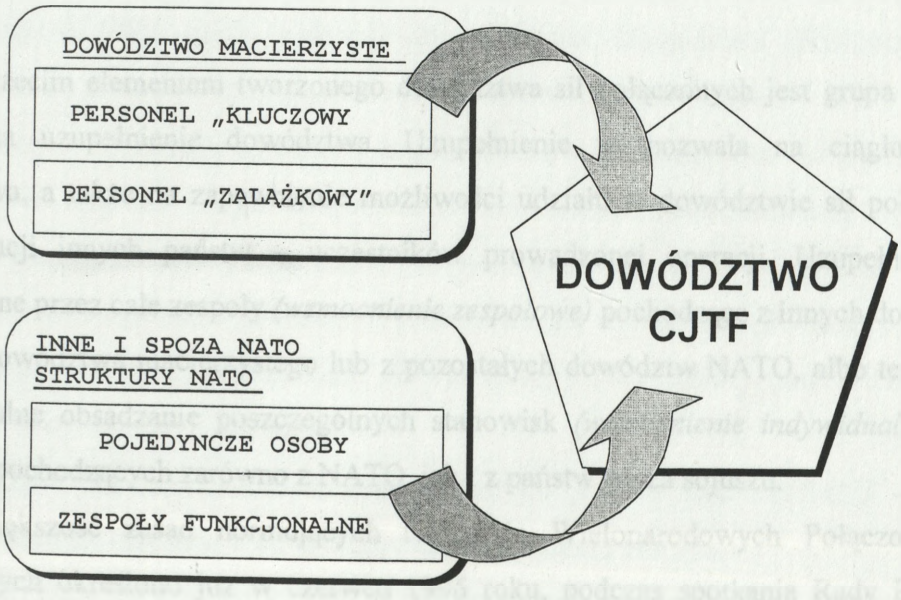
Prowadzenie działań poza obszarem NATO spowodowało, iż istniejąca struktura sojuszu nie była w stanie zapewnić sprawnego dowodzenia. Toteż ważnym elementem nowej koncepcji było założenie formowania w razie potrzeby, na czas realizacji zadań – Dowództwa Wielonarodowych Połączonych Sił Zadaniowych (*CJTF HQ*), które zdefiniowano jako: *„... mobilne (łatwe do przemieszenia i rozmieszenia) wielonarodowe, połączone dowództwo o wielkości zależnej od potrzeb, tworzone w celu dowodzenia wielonarodowymi siłami połączonymi w trakcie realizacji różnych zadań, w tym operacji wsparcia pokoju..."*

Wielonarodowe Połączone Siły Zadaniowe (WPSZ) powinny umożliwić sojuszowi wykonywanie całego spektrum zadań, wynikających zarówno ze strategii NATO, jak i wyzwań stawianych przez zmieniającą się sytuacje międzynarodową. Do zadań tych należy przede wszystkim zapewnienie możliwości obrony każdego z państw sojuszu w ramach kolektywnej samoobrony, jak i szereg innych operacji z udziałem sił NATO – ogólnie określanych jako operacje spoza artykułu 5. (ang. *Non-5 art. Operations, N5AO*).

Warunkiem niezbędnym okazała się w tej sytuacji szeroko rozumiana elastyczność koncepcji sił połączonych, wyrażona poprzez:
— swobodę doboru sił w stosunku do wyznaczonego zadania;
— wewnętrzną strukturę tworzonych sił połączonych i ich dowództwa;
— organizację dowodzenia tymi siłami.

Ze względu na założone redukcje sił oraz zmniejszanie ilości dowództw sojuszniczych, nie było możliwe utrzymywanie części personelu tylko i wyłącznie w gotowości do ewentualnych działań w ramach permanentnie funkcjonujących Wielonarodowych Połączonych Sił Zadaniowych. Toteż rozwijając koncepcję tworzenia tych sił ustalono, iż ich zalążki będą na stałe rozmieszczone w wybranych, istniejących w czasie pokoju dowództwach NATO, nazywanych ***„dowództwami macierzystymi"*** *(parent headquarters)*.

Rozpoczęte działania Komitetu Wojskowego NATO w grudniu 1996 r. (dyrektywa MC-389) przyczyniły się do opracownia „Doktryny działania dowództw wielonarodowych sił połączonych" (*CJTF HQ Doctrine*), która została opublikowana w 1997 r. Celem tego dokumentu było dostarczenie wytycznych i zasad w zakresie szkolenia i funkcjonowania dowództw wielonarodowych sił połączonych. W efekcie zostały wyznaczone trzy dowództwa macierzyste, których zadaniem stało się od tego czasu także planowanie, przygotowanie oraz szkolenie personelu niezbędnego do organizacji dowództwa tworzonego doraźnie, czyli Dowództwa Wielonarodowych Połączonych Sił Zadaniowych (DWPSZ). Obecnie w strukturach NATO wyznaczone są trzy dowództwa macierzyste. W ramach każdego z tych dowództw funkcjonują dwie grupy oficerów: grupa oficerów kluczowych i grupa oficerów zalążkowych (rys. 1.3.1).



Rys. 1.3.1. Zasada tworzenia dowództw wielonarodowych

Grupa oficerów kluczowych (ang. Key Nucleus Staff) składa się z oficerów, którzy posiadają doświadczenie w pracy w zespołach wielonarodowych i pełnią obowiązki

w dowództwie macierzystym. Grupa ta zakresem możliwości swojego działania pokrywa wszystkie najważniejsze piony funkcjonale grupy głównej dowództwa.

Oficerowie ci zajmują się wyłącznie problematyką planowania, powoływania, organizowania i rozmieszczania dowództwa wielonarodowego (DWPSZ) w oparciu o swoje struktury macierzyste. Pozwala to na płynne wprowadzenie podległych sobie pionów funkcjonalnych (od CJ-1 do CJ-9) w cykl funkcjonowania dowództwa zgodnie z procedurami obowiązującymi w NATO.

Grupa oficerów zalążkowych (ang. Nucleus Staff) – stanowi następny element tworzącego się Dowództwa Wielonarodowych Połączonych Sił Zadaniowych. W jej składzie znajduje się około 120 oficerów, wcześniej wyznaczonych i przygotowanych przez dowództwo macierzyste, doświadczonych w pracy w różnych specjalnościach i reprezentujących wszystkie niezbędne zespoły funkcjonalne dowództwa. Na co dzień wykonują oni swoje zadania w strukturze dowództwa, natomiast są dodatkowo przygotowywani do zajęcia zasadniczych stanowisk w dowództwie wielonarodowym (DWPSZ) w razie jego powołania. Zadaniem tej grupy jest zapewnienie sprawnej pracy we wszystkich zespołach funkcjonalnych stanowiska dowodzenia zgodnie z procedurami NATO. Pozwala to przede wszystkim na właściwą współpracę zarówno w ramach nowo tworzonego dowództwa, jak i z dowództwem macierzystym oraz innymi dowództwami NATO.

Trzecim elementem tworzonego dowództwa sił połączonych jest grupa oficerów, stanowiąca uzupełnienie dowództwa. Uzupełnienie to pozwala na ciągłość pracy dowództwa, a także na zapewnienie możliwości udziału w dowództwie sił połączonych reprezentacji innych państw – uczestników prowadzonej operacji. Uzupełnienie jest realizowane przez całe zespoły *(wzmocnienie zespołowe)* pochodzące z innych dowództw z regionu dowództwa macierzystego lub z pozostałych dowództw NATO, albo też poprzez indywidualne obsadzanie poszczególnych stanowisk *(wzmocnienie indywidualne)* przez oficerów pochodzących zarówno z NATO, jak i z państw spoza sojuszu.

Większość zasad normujących tworzenie Wielonarodowych Połączonych Sił Zadaniowych określono już w czerwcu 1996 roku, podczas spotkania Rady Północnoatlantyckiej w Berlinie. Zasady te pozostały praktycznie nie zmienione i pozostają do dziś aktualne. Ustalenia te stanowią m. in., że:

— nadzór polityczny nad operacjami sił połączonych będzie sprawowała Rada Północnoatlantycka;

— plany formowania dowództw wielonarodowych sił połączonych będą zatwierdzone przez Radę Północno-atlantycką;

— Naczelny Dowódca Sił Sojuszniczych Europy pełnić będzie kluczową rolę w prowadzeniu operacji wielonarodowych sił połączonych;

— kontrolę nad siłami wydzielonymi przez sojusz w czasie operacji sił połączonych sprawować będą dowódcy NATO.

Procedura uruchomienia procesu powoływania dowództw wielonarodowych inicjowana jest na najwyższym szczeblu NATO. Na wniosek Rady Północno-atlantyckiej oraz Komitetu Wojskowego przekazywana jest do dowództwa strategicznego dyrektywa. Dowództwo to z kolei przekazuje zadanie do Wielonarodowego Połączonego Zespołu Planistycznego (ang. *Combined Joint Planning Staff – CJPS*). Zespół ten znajduje się w Mons w Belgii, koordynuje swoje decyzje z Zespołem Koordynującym Zasobami oraz innymi organizacjami międzynarodowymi, które mogą być zaangażowane w rozwiązywanie sytuacji kryzysowej (np. PdP, ONZ, OBWE itd.) i ocenia, które z dowództw macierzystych powinno zostać zaangażowane do tworzenia Dowództwa Wielonarodowych Połączonych Sił Zadaniowych. Swoją sugestię zespół ten przekazuje następnie dowódcy strategicznemu, który ostatecznie wyznacza dowództwo macierzyste swoją dyrektywą. W zależności od sytuacji Wielonarodowy Połączony Zespół Planistyczny (*CJPS*), może wskazać do tworzenia Dowództwa Wielonarodowych Połączonych Sił Zadaniowych jedno z trzech dowództw macierzystych:

— Dowództwo Regionalne „Północ", znajdujące się w holenderskim mieście Brunssum (*RC North*, ang. *RC – Regional Command)*, któremu podlegają Połączone Siły Zbrojne NATO Europy Północnej (ang. *AFNORTH – Allied Forces Northern Europe)*;

— Dowództwo Regionalne „Południe", rozmieszczone w Neapolu (*RC South)*, któremu podlegają Połączone Siły Zbrojne NATO Europy Południowej (ang. *AFSOUTH – Allied Forces Southern Europe)*;

— Dowództwo Sił Uderzeniowych Floty Atlantyku (ang. *STRIKFLATLANT – Striking Fleet Atlantic)*, znajdujące się w amerykańskim mieście Norfolk.

Dwa pierwsze dowództwa macierzyste przygotowują dowództwa sił połączonych, które mając charakter **stacjonarny** i przewidziane są do rozmieszczenia na lądzie. Natomiast trzecie dowództwo, przygotowuje analogiczne dowództwo rozmieszczane na morzu, czyli mające charakter zdecydowanie **mobilny**.

Należy zauważyć, że dowództwo po wydzieleniu „grupy zalążkowej" do dowództwa sił połączonych, powinno być w stanie w dalszym ciągu spełniać rolę dowództwa regionalnego oraz wypełniać wszystkie zadania na rzecz wydzielonego przez siebie dowództwa (zgodnie z zadaniami dowództwa macierzystego). Konieczne jest więc w związku z tym zachowanie odpowiednich proporcji podziału dowództwa macierzystego. Zwykle przyjmuje się, że zalążkowa część dowództwa nie powinna być większa, niż 25% składu osobowego dowództwa macierzystego. Brakujące 75% pochodzić powinno z uzupełnienia w postaci zespołów wydzielonych przez dowództwa podległe dowództwu macierzystemu, jak i w postaci uzupełnienia indywidualnego – zgodnie z potrzebami, również spoza sił podległych dowództwu macierzystemu. Ważna w tym zakresie jest realizacja procesu uzupełniania dowództw przez całe zespoły funkcjonalne. Ma to istotne znaczenie dla skuteczności i szybkości integracji dowództwa i wprowadzania w nim procedur sojuszniczych.

Ta procedura zespołowego uzupełniania grupy zalążkowej wynika właśnie z funkcjonalnego charakteru dowództw macierzystych, które już są dowództwami sojuszniczych sił połączonych, w skład których wchodzą komponenty poszczególnych rodzajów sił zbrojnych (np. komponent lotniczy, komponent lądowy itp.). Z tego też powodu dowództwa poszczególnych komponentów są w stanie sprawnie podjąć rolę dowództw poszczególnych komponentów, również w wymiarze wielonarodowym, tzn. gdy w składzie poszczególnych komponentów znajdą się siły z państw nie należących do sojuszu.

Nową jakościowo sytuację stanowi problematyka dowodzenia w układzie koalicyjnym. Dotyczy ona sytuacji, w której zarówno w relacjach dowodzenia (podległości), jak i funkcjonalnych oraz współdziałania występują organa dowodzenia różnych, koalicyjnych armii. Analiza struktur dowództw sił wielonarodowych (*combined forces, allied forces, multinational forces*) wskazuje, że istnieją dwa zasadnicze sposoby organizacji struktury dowodzenia tego rodzaju siłami:

— sposób bezpośredni;

— dowodzenie poprzez dowódców komponentów.

Sposób bezpośredni polega na podporządkowaniu dowódców elementów różnych rodzajów sił zbrojnych, wydzielanych z różnych państw, bezpośrednio dowódcy sił połączonych. Sposób ten jest możliwy do realizacji jedynie w przypadku operacji połączonych prowadzonych relatywnie niewielkimi siłami i na małą skalę. W innym

bowiem przypadku zbyt duża rozpiętość dowodzenia spowoduje, iż skuteczne sprawowanie dowodzenia stanie się bardzo trudne, czy wręcz niemożliwe.

Znacznie skuteczniejszym i wręcz typowym sposobem wydaje się być sprawowanie dowodzenia **poprzez dowódców komponentów**, którym podporządkowane są określone siły. Sposób ten wyzwala trzy następujące możliwości zorganizowania struktury dowodzenia:

— dowodzenie poprzez dowódców komponentów narodowych;

— dowodzenie poprzez dowódców komponentów rodzajów sił zbrojnych;

— dowodzenie poprzez dowódców komponentów funkcjonalnych.

W pierwszym przypadku (dowodzenie poprzez dowódców komponentów narodowych) – dowódcy sił połączonych podporządkowuje się dowódców sił narodowych o charakterze połączonym – czyli grupujących w sobie elementy kilku rodzajów sił zbrojnych. Należy podkreślić, iż w takim przypadku dowódcy komponentów narodowych będą także dowódcami sił połączonych, a tym samym będą musieli zdecydować się na określony sposób organizacji dowodzenia.

W przypadku dowodzenia poprzez dowódców komponentów rodzajów sił zbrojnych (rys. 1.3.2), dowódca połączonych sił nadzoruje działania dowódców wielonarodowych komponentów, z których każdy reprezentuje rodzaj sił zbrojnych. Jest to najbardziej przejrzyste, najczęściej stosowane, proste i typowe rozwiązanie problemu. Oddaje również najlepiej istotę dowodzenia w wielonarodowych działaniach połączonych.

Jeżeli przyjęte zostanie rozwiązanie sprawowania dowodzenia poprzez dowódców elementów funkcjonalnych, wówczas dowódcy połączonych sił podporządkowani zostają dowódcy komponentów, którym podlegają połączone siły wielonarodowe (czyli reprezentujące kilka rodzajów sił zbrojnych z kilku państw). Mamy tu więc sytuację, w której dowódca operacji połączonej nadzoruje działania dowódców wielonarodowych sił połączonych na niższym szczeblu dowodzenia – podobnie jak w przypadku dowodzenia poprzez dowódców komponentów narodowych.

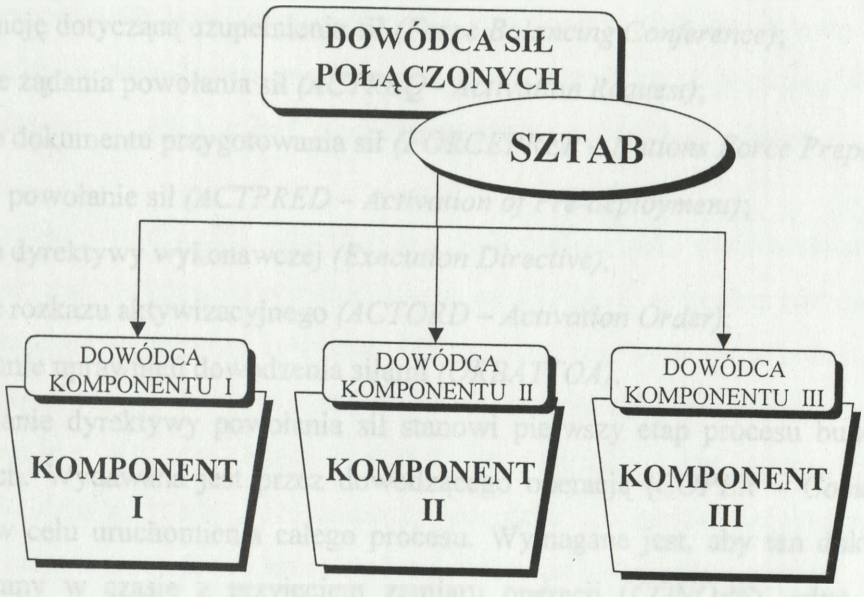
W każdym z prezentowanych rozwiązań, na pewnym szczeblu dowodzenia, wystąpi sytuacja dotycząca współdziałania lub podległości dowództw reprezentujących różne kraje, a tym samym pojawi się wiele nowych problemów, wynikających z tego rodzaju kontaktów. Do najważniejszych problemów w tym zakresie można zaliczyć:

— wymianę danych (obieg dokumentów dowodzenia) pomiędzy dowództwami w różnych relacjach;

— współdziałanie pokrewnych funkcjonalnie komórek różnych organów dowodzenia;

— formowanie mieszanych (wielonarodowych) dowództw;

— organizację służby łącznikowej.



Rys. 1.3.2. Dowodzenie siłami połączonymi poprzez dowódców komponentów

Niezależnie od przyjętego rozwiązania, osiągnięcie zdolności do dowodzenia w takim układzie może sprowadzić się do osiągnięcia w tym obszarze pełnej **interoperacyjności**, rozumianej zgodnie z obowiązującymi w NATO poglądami, jako zdolność systemów, jednostek lub sił do zapewnienia szeroko rozumianego wsparcia, korzystania ze wsparcia innych systemów, jednostek lub sił, a także zdolność do wzajemnej wymiany w tym zakresie, pozwalająca na skuteczne wspólne działanie.

To wskazuje także na potrzebę posiadania takiego systemu dowodzenia, który będzie w stanie skutecznie współpracować z systemami dowodzenia innych armii, korzystać z technicznego, informacyjnego i osobowego wsparcia z ich strony, a nawet być zdolnym do wymiany pewnych elementów.

Integralną częścią procesu zarządzania kryzysowego jest proces organizowania sił niezbędnych do zrealizowania określonych zadań wynikających z konieczności reagowania w złożonej sytuacji polityczno-militarnej. Celem tego procesu jest określenie i odpowiednie dobranie koniecznych środków militarnych do realizacji prac planistycznych i późniejszego wykonania zaplanowanych działań. Prowadzony jest tylko na szczeblu strategicznym.

Szczegółowy przebieg procesu budowania sił sojuszniczych obejmuje dziesięć przedsięwzięć:

— wydanie dyrektywy powołania (aktywacji) sił *(FAD - Forces Activation Directive)*;

— wydanie dyrektywy przygotowawczej (*ACTWARN – Activation Warning)*;

— konferencję dotyczącą budowania sił *(Force Generation Conference)*;

— konferencję dotyczącą uzupełnienia sił *(Force Balancing Conference)*;

— wysłanie żądania powołania sił *(ACTREQ - Activation Request)*;

— wydanie dokumentu przygotowania sił *(FORCEPREP – Nations Force Preparation)*;

— wstępne powołanie sił *(ACTPRED – Activation of Pre-deployment)*;

— wydanie dyrektywy wykonawczej *(Execution Directive)*;

— wydanie rozkazu aktywizacyjnego *(ACTORD – Activation Order)*;

— przekazanie uprawnień dowodzenia siłami *(ORBATTOA)*.

Wydanie dyrektywy powołania sił stanowi pierwszy etap procesu budowania sił sojuszniczych. Wydawana jest przez dowodzącego operacją (*COPER – Commander of operation*) w celu uruchomienia całego procesu. Wymagane jest, aby ten dokument był skoordynowany w czasie z przyjęciem zamiaru operacji (*CONOPS*), gdyż procedury powołania sił muszą być realizowane równolegle z konstruowaniem planu operacji (*OPLAN*). Dlatego też, zawsze gdy to jest możliwe, razem z zamiarem publikowany jest dokument określający potrzeby i wymagania w zakresie sił (*SOR - Status of Requirement*), co znacznie ułatwia przebieg narodowych procesów w państwach wydzielających swe siły, a tym samym skraca czas upływający od akceptacji zamiaru do wydania dyrektywy powołania sił.

Aby przyspieszyć prace nad określeniem sił możliwych do wydzielenia, dowodzący operacją, po wydaniu dyrektywy powołania sił, może skierować do poszczególnych państw dyrektywę przygotowawczą (*ACTWARN – Activation Warning*), zawierającą ogólny zarys planowanej operacji oraz niektóre istotne dane kluczowe. Pozwala to na określenie państwom – uczestnikom rodzajów, wielkości i zdolności bojowych sił niezbędnych do wykonania poszczególnych zadań operacji. Państwa zobowiązane są do udzielenia dowodzącemu operacją odpowiedzi w postaci nieoficjalnej oferty narodowej. Informacje te stanowią podstawę do wstępnego opracowania zestawienia sił sojuszu (*AFL – Allied Forces List*) i przygotowania konferencji dotyczącej budowania sił (*Force Generation Conference*).

Jeśli jednak dowodzący operacją uzna, że otrzymane przez niego propozycje udziału sił poszczególnych państw są w jakimkolwiek zakresie lub obszarze nie wystarczające, może on zorganizować kolejną konferencję (*Force Balancing Conference*), mającą na celu

poinformowanie państw o zaistniałych problemach. W czasie tego spotkania konieczne jest ponowne przeanalizowanie sytuacji i zwiększenie zdolności bojowych wojsk. Realizowane jest to poprzez mediacje między przedstawicielami wojskowymi, trwające do czasu osiągnięcia pożądanych rezultatów. Jeśli mediacje te nie przyniosą oczekiwanych efektów konieczne staje się zwiększenie wielkości sił wydzielanych przez poszczególne państwa albo w ostateczności, gdy i to jest z jakichkolwiek powodów niemożliwe, zmiana planu operacji.

W czasie konferencji dotyczącej budowania sił państwom-uczestnikom przedstawiana jest wstępna propozycja składu sił *(AFL)*, a następnie rozpatrywane są wszystkie szczegółowe aspekty dotyczące udziału poszczególnych sił w kolejnych fazach działań. Efektem tej analizy jest zestawienie sił dysponowanych przez sojusz *(ADL – Allied Disposition List)*, zawierające oprócz wykazu sił także takie informacje, jak czas gotowości do działań każdej uczestniczącej jednostki, ich ogólne przeznaczenie, czas i miejsce wejścia do działań oraz sposób postępowania po wykonaniu zadania.

Dokument ten jest podstawą do sporządzenia przez każde państwo uczestniczące w operacji narodowego planu przemieszczeń *(DDP - Detailed Deployment Plan)*. Plany te są podczas kolejnego spotkania koordynowane i uzgadniane z państwem-godspodarzem *(HNS – Host Nation Support)*, a następnie łączone w jeden spójny dokument – **Wielonarodowy Szczegółowy Plan Rozmieszczenia Sił** (*MNDDP – Multinational Detailed Deployment Plan*).

W końcowym etapie cyklu konferencji dowodzący siłami wysyła poszczególnym państwom-uczestnikom tzw. żądanie powołania sił *(ACTREQ – Activation Request)*, któremu towarzyszy ostateczna wersja potrzeb i wymagań w zakresie sił (*SOR – Status of Requirement*). Uczestniczące państwa proszone są o oficjalne potwierdzenie w podanym terminie wydzielenia deklarowanych sił.

W odpowiedzi na to wezwanie do dowodzącego operacją przesyłane są oficjalne potwierdzenia udziału konkretnych sił zgłoszonych wcześniej, podczas konferencji dotyczącej budowania sił. Potwierdzenia takie mają formę dokumentu przygotowania sił *(FORCEPREP – Nations Force Preparation)*. Opracowywane są one już od czasu otrzymania dyrektywy przygotowawczej (*ACTWARN – Activation Warning*). Zwykle zawierają także uwagi, określające oczekiwania państwa w zakresie użycia sił narodowych (zasady użycia, ograniczenia, wymagania wsparcia, potrzeby w zakresie dowodzenia itp.).

Po przyjęciu od wszystkich państw dokumentów przygotowania sił i zaakceptowaniu przez organy polityczne koncepcji działań, dowodzący operacją może skierować do

uczestników wstępne powołanie sił *(ACTPRED – Activation of Pre-deployment)*, pozwalające na konieczny manewr sił pierwszego rzutu do rejonu działań oraz na przygotowanie do przekazania uprawnień do dowodzenia tymi siłami.

Punktem wyjścia do rozpoczęcia operacji jest podpisanie przez organy władzy politycznej dyrektywy wykonawczej *(Execution Directive)*[20]. Podstawę tego aktu stanowi opracowany w wyniku szczegółowej analizy zamiaru operacji *(CONOPS)* i zatwierdzony plan operacji *(OPLAN)* oraz skompletowany wykaz sił sojuszu *(AFL)*. Umożliwia to wydanie przez dowodzącego operacją rozkazu aktywizacyjnego *(ACTORD – Activation Order)*, a tym samym na zainicjowanie działań poszczególnych sił w ramach postawionego zadania.

W przypadkach szczególnych, zwykle podczas ograniczenia czasowego procesu tworzenia sił, rozkaz aktywizacyjny *(ACTORD)* może być wydany przed podpisaniem dyrektywy wykonawczej *(Execution Directive)*, co może pozwolić na znacznie szybsze rozwinięcie określonych sił w rejonie działań i przystąpienie do realizacji postawionych im zadań. Sytuacja taka jest jednak wyjątkowa i wymaga każdorazowo specjalnego upoważnienia organów politycznych.

Proces uruchamiania operacji kończony jest wydaniem przez państwa (uczestników) dokumentu przekazania dowodzenia siłami *(ORBATTOA)*, który daje dowodzącemu operacją uprawnienia dowodzenia wydzielonymi siłami w zakresie dowodzenia operacyjnego (OPCOM) lub kontroli operacyjnej (OPCON).

Wielonarodowa współpraca realizowana jest w różnych formach organizacyjnych, a wielonarodowe struktury militarne organizowane być mogą zgodnie z zasadami **państwa wiodącego** (ang. *Lead Nation*), **państwa określającego ogólne ramy** (ang. *Framework Nation*) i **integracji** (ang. *Integration*).

Zasada państwa wiodącego – ***Lead Nation*** – w tej sytuacji struktura wielonarodowa kierowana jest przez przedstawicieli jednego państwa. Obowiązują przy tym zasady dowodzenia i prowadzenia działań tego właśnie państwa. Również dowództwo jest w zasadzie obsadzone przez jego przedstawicieli. Pojedyncze stanowiska w sztabie mogą być zajmowane przez reprezentantów krajów wydzielających swe kontyngenty do omawianej struktury. Jednostki innych państw podporządkowywane są tylko na okres działań.

[20] Częścią tego dokumentu są zasady użycia siły (militarnej) – *ROEAUTH*.

Zasada państwa określającego ogólne ramy – ***Framework Nation*** – w tak skonstruowanej strukturze wielonarodowej, jedno z państw odpowiedzialne jest za dowodzenie, administrację i wsparcie logistyczne. Przedstawiciele tego państwa stanowią większość pracowników dowództwa i zajmują w nim kierownicze stanowiska. Zasady dowodzenia i prowadzenia działań odpowiadają zasadom narodowym lub też – o ile zostanie to uzgodnione – procedurom NATO. Przedstawiciele państw wydzielających kontyngenty do takiej struktury zajmują stanowiska w sztabie według ustalonego klucza. Wojska podporządkowywane są tylko na okres działań i obowiązują je procedury narodowe lub ogólne procedury NATO.

Zasada integracji - ***Integration*** – w przypadku przyjęcia takiego rozwiązania tworzona jest struktura wielonarodowa z wielonarodowym sztabem, przy czym stanowiska w sztabie z reguły odpowiadają udziałowi kontyngentu danego państwa w organizowanych strukturach. Najważniejsze funkcje podlegają określonej rotacji zaś zasady dowodzenia, prowadzenia działań, a czasami również szkolenia, odpowiadają procedurom NATO lub też ustalane są przez wszystkie uczestniczące państwa. Wydzielone siły państw reprezentowanych w takiej strukturze mogą być podporządkowane wielonarodowemu dowództwu już w okresie pokoju. Zwykle jednak przekazywane są w podporządkowanie na okres działań na zasadach dowodzenia operacyjnego (ang. *Operational Command– OPCOM*) lub kontroli operacyjnej (ang. *Operational Control – OPCON*)[21]. Pomimo to pozostają w narodowej podległości służbowej i dyscyplinarnej. Ich zasady działania są zgodne z procedurami NATO lub też ustaleniami przyjętymi przez zainteresowane państwa.

Podporządkowanie części sił zbrojnych strukturom wielonarodowym nie oznacza zupełnej rezygnacji z narodowych uprawnień i odpowiedzialności. Zarówno odpowiedzialność za własnych żołnierzy, jak i odpowiedzialność wobec parlamentu i społeczeństwa pozostają w gestii narodowej. Przekazanie uprawnień dowodzenia (ang. *Transfer of Authority – TOA)* dotyczy maksymalnie poziomu dowodzenia operacyjnego. Pełne dowodzenie (*Full Command – FULLCOM*) pozostaje zastrzeżone dla dowódców narodowych.

Dowodzenie siłami połączonymi jest niewątpliwie specyficznym przypadkiem dowodzenia. Na jego kształt wpływa bowiem wiele czynników, w dużej mierze utrudniających jego przebieg i wpływających niekorzystnie na jego jakość. Konieczne jest

[21] J.Kręcikij, *Zakresy uprawnień i odpowiedzialności dowódców wobec podległych im wojsk*, Warszawa, AON, 2000.

więc generowanie nowych rozwiązań i podejmowanie kolejnych inicjatyw, mogących w wymiernym stopniu poprawić warunki, w jakich dowodzenie takimi specyficznymi siłami jest realizowane.

1.4. Rola i cele działań informacyjnych w operacjach połączonych

Działania informacyjne zajmują ważne miejsce w operacjach połączonych (również w sojuszu, koalicji), dlatego też powinny być spełnione pewne wymagania w zakresie ich planowania i prowadzenia.

Dowódca sił połaczonych prowadzi kampanię i nadzoruje także wszystkie przedsięwzięcia działań informacyjnych włącznie z procesem decyzyjnym (w całej strukturze dowodzenia). Dlatego też w jego zamiarze będzie zdefiniowany główny cel działań informacyjnych. Cel ten musi ściśle określać stan końcowy (end state).

Działania informacyjne w znacznej mierze wspierają zadania strategiczne i operacyjne, dlatego też powinny być dokładnie zintegrowane w całej strukturze dowodzenia (na wszystkich poziomach). Wszystkie elementy działań informacyjnych powinny być skoordynowane i zsynchronizowane z innymi działaniami, tak żeby nie wpływały na siebie negatywnie.

Działania informacyjne powinny być wspierane terminowymi i dokładnymi informacjami o wszystkich stronach konfliktu (o podmiotach neutralnych również), które mogą wpływać na realizację naszego zadania. Rozpoznanie, poprzez dostarczanie danych i wniosków, powinno kształtować podłoże operacyjne, wspomagając ocenę dowódcy.

Działania informacyjne powinny skupiać się na środku ciężkości przeciwnika, który jest określany w drodze szczegółowej analizy jego działań. Jednocześnie dowódca powinien zidentyfikować swój własny środek ciężkości zapewniając mu odpowiedni poziom ochrony.

Należy stosować zasadę centralnego planowania i decentralizacji wykonania na niższych poziomach działań informacyjnych (w tym definiowanie ograniczeń i zakresu działań). Jednakże dla niektórych działań wymagane będzie zcentralizowane koordynowanie – np. takich jak mylenie, kiedy wszystkie elementy sił własnych muszą ściśle trzymać się jednorodnego planu.

Potencjalna lista celów działań informacyjnych jest duża i zróżnicowana, dotyczy szerokiego zakresu wsparcia działań operacyjnych – zarówno wewnątrz jak i na zewnątrz obszaru operacji połączonych (*JOA*).

Planowanie działań informacyjnych powinno rozpocząć się z wyprzedzeniem, szczególnie tam gdzie kształtowanie opinii jest kluczem do sukcesu, ponieważ zarówno planowanie jak i wykonanie wymagają czasu, a rezultaty mogą pojawić się znacznie później. W związku z tym, wytyczne, jako część procesu planowania, muszą być określone tak szybko, jak tylko jest to możliwe.

Działania informacyjne dzielą się na ofensywne i defensywne. Defensywne wymagają znacznie więcej przygotowań, szczególnie dla systemów informacyjych, ponieważ przedsięwzięcia ochronne muszą być odpowiednio wbudowane w koncepcję operacji i tworzyć odpowiednie podłoże działań informacyjnych.

Efektywność działań informacyjnych zależna jest od ciągłej oceny skutków, krótkoterminowych i długoterminowych, wzajemnie ze sobą powiązanych działań, ukierunkowanych na osiągnięcie określonego celu. Dokonanie takiej oceny jest możliwe dzięki pozyskiwaniu informacji ze wszystkich dostępnych źródeł.

Działania informacyjne są prowadzone we wszystkich rodzajach operacji połączonych, ale środek ciężkości, prowadzący do osiągnięcia celu działań informacyjnych, będzie różny, w zależności od charakteru operacji połączonej. Kluczowym czynnikiem w prowadzeniu działań informacyjnych w operacjach połączonych będzie spójność i motywacja przeciwnika. Spójny wewnętrznie system działań przeciwnika z jego wysoką motywacją zmniejsza prawdopodobieństwo wywołania zmian w jego percepcji. W takich przypadkach środkiem ciężkości działań informacyjnych będzie prawdopodobnie dowództwo przeciwnika, struktura dowodzenia oraz proces informacyjny i nośniki informacji.

Celem działań informacyjnych jest wpływanie na podejmujących decyzje, ich percepcję oraz procedury i potencjał systemu dowodzenia. Plan działań informacyjnych musi być elastyczny i zawierać także działania korygujące, ażeby reagować na różne wydarzenia i wykorzystać nagłe zmiany w społecznych nastrojach.

Ponadto celem działań inforamcyjnych będzie ograniczenie zdolności przeciwnika w zakresie zdobywania informacji i wykorzystywania ich w procesie decyzyjnym oraz zniszczenie lub ograniczenie zdolności jego systemu dowodzenia. Wewnętrzne zakłócenia w strukturze dowodzenia przeciwnika lub podziały w wojskach, co do sensu i celowości działań, mogą kształtować środek ciężkości – działania informacyjne powinny skupić się na wykorzystywaniu tych zmian.

1.5. Efekty poznania

1. Nowe uwarunkowania geopolityczne, jakie miały miejsce pod koniec lat 90., przyjęcie nowych członków do NATO oraz nowe zagrożenia (narastanie terroryzmu) na całym świecie spowodowały nową sytuację geostrategiczną, co znalazło swoje odzwierciedlenie w nowej koncepcji strategicznej sojuszu. Konieczność ciągłego utrzymywania pokoju w różnych sytuacjach kryzysowych, jakie miały chociażby miejsce w ostatnich latach, zmusza siły zbrojne sojuszu do zachowania odpowiednio wysokiej gotowości operacyjnej i stosownie dużej mobilności wojsk celem szybkiego rozwijania się na odległych teatrach działań operacyjnych. Dlatego też w planach strategicznych sojuszu szczególną rolę odgrywają połączone operacje wielonarodowe, których podstawą jest najwyższa interoperacyjność sił połączonych, jak też poszczególnych kontyngentów narodowych, a także niektórych państw partnerskich.

2. Udział w działaniach sojuszniczych naszych sił zbrojnych podyktowany jest obroną RP lub obroną innego członka NATO. Siły Zbrojne RP mogą uczestniczyć w połączonych operacjach sojuszniczych w ramach obrony kolektywnej wynikającej z artykułu 5. traktatu waszyngtońskiego i reagowania kryzysowego poza artykułem 5. oraz konsultacji i współpracy.

3. Gwarancją powodzenia operacji połączonych jest zaangażowanie w ten proces całego potencjału obronnego państwa, zarówno militarnego, jak i pozamilitarnego. Istotną rolę w tych warunkach – oprócz działań zbrojnych – odgrywają działania informacyjne, które w znaczny sposób mogą przyczynić się do osiągnięcia założonych celów operacji połączonych.

4. Działania informacyjne mogą obejmować m.in. realizację następujących przedsięwzięć:

— destrukcyjne oddziaływanie informacyjne skierowane na struktury władzy państwowej, wojsko i ludność przeciwnika oraz jego systemy informacyjne;
— ochrona i propagowanie polskich interesów na arenie międzynarodowej;
— umacnianie morale i determinacji obronnej wojsk własnych i społeczeństwa;
— ochrona własnych systemów informacyjnych.

5. Działania informacyjne prowadzone są zrówno w czasie pokoju, kryzysu, jak i wojny we wszystkich rodzajach operacji. Swoim zasięgiem wykraczają one poza wytyczony obszar działań operacyjnych, gdyż wspierając cele militarne, adresowane będą

do szeroko rozumianego audytorium. Zasięg ich wpływu ograniczony jest jedynie możliwościami oddziaływania współczesnych środków informacyjnych.

6. W strukturach sił zbrojnych znajdują się jednostki specjalistyczne (rozpoznania, działań psychologicznych, walki elektronicznej), które mogą zostać wykorzystane do prowadzenia działań informacyjnych. Jednostki te, przeznaczone do wykonania zadań na terenie własnego kraju, mogą być wzmocnione przez siły i środki działań informacyjnych innych państw sojuszniczych biorących udział w operacji. Siły te będą pozostawać pod kontrolą operacyjną dowódcy operacji połączonej.

2. GENEZA DZIAŁAŃ INFORMACYJNYCH

2.1. Uwarunkowania historyczne działań informacyjnych

Komunikacja społeczna jest dla ludzkości procesem naturalnym i przypuszcza się, że prymitywne formy komunikowania się gatunku ludzkiego pochodzą prawdopodobnie z epoki człowieka kromaniońskiego[22]. Początkowo możliwości w tym zakresie ograniczały się do komunikowania bezpośredniego i lokalnego.

Z czasem bezpośrednie formy komunikowania stały się niewystarczające, pojawiły się zatem systemy komunikowania na odległość. W dwudziestym wieku nastąpił szybki rozwój wiedzy, który spowodował powstanie nowych technik komunikacyjnych. Do porozumiewania się na odległość wykorzystano elektryczność. Od tego czasu synonimem zwrotu „komunikacja na odległość" stała się „telekomunikacja".

Współcześnie zmierza się w stronę środków komunikacji opartych na kombinacji wszystkich elementów: tekstu, obrazu, bezpośredniej rozmowy, listu, muzyki – możliwości takie dają współczesne media – telewizja, internet.

Możliwości nowych mediów są zaskakujące. Już dzisiaj rewolucjonizują polityczne życie społeczeństw. Dla tych, którzy chcą dotrzeć do całej populacji, najbardziej przydatna jest telewizja. Korzysta z niej więcej osób niż z jakiegokolwiek innego środka przekazu. Liczba godzin oglądania telewizji przekracza liczbę godzin poświęconych innym mediom. W przeciwieństwie do radia lub materiałów drukowanych, w telewizji wydarzenia są relacjonowane i przekazywane na żywo.

Chuck de Caro[23] twierdzi, „że telewizja globalna stwarza środki pozwalające na uginanie woli narodów i wpływanie na politykę międzynarodową". Ten sposób oddziaływania określa mianem „Softwar", czyli „wrogie wykorzystanie globalnej telewizji do kształtowania woli innego narodu przez zmianę jego obrazu rzeczywistości".

Internet konkuruje z telewizją jako środek dotarcia do masowego audytorium i wpływania na opinie i decyzje. Podobnie jak audycje telewizyjne, internet także stwarza możliwości nadawania i przekazywania wydarzeń na bieżąco. Jest środkiem dającym jednostkom i małym grupom takie same możliwości wypowiedzi, jakie mają rządy i wielkie korporacje.

---

[22]Człowiek kromaniński (Homo sapiens diluvialis) – człowiek rozumny, żyjący w Europie w epoce lodowcowej (ok. 60 tys. lat temu), jego szczątki odkryto w 2 połowie XIX wieku w Crô-Magnon we Francji.
[23]Chuck de Caro – dyrektor naczelny powietrznego biura propagandy (AeroBureau Corps), satelitarnego systemu nadawania wiadomości (Strategic, Airmobile Reports – via – Satelite).

Media zajmują ważne miejsce w kształtowaniu opinii publicznej. A właśnie opinia publiczna jest ważnym czynnikiem rozwoju społeczeństwa, aktywną formą ustosunkowania się do zjawisk społecznej rzeczywistości.

Media mogą w znacznym stopniu wspierać akcje sił zbrojnych ale w niektórych sytuacjach mogą je utrudnić, a tym samym wpływać na przebieg operacji połączonych.

Skutki wyłaniających się przed ludzkością nowych możliwości – pozytywne lub negatywne – są początkiem całkowicie nowej ery, nazywanej erą informacyjną, w której informacja staje się zasobem strategicznym, a terminy, takie jak: przestrzeń, czas i cena, mogą znacznie stracić na znaczeniu.

Ta nowa era informacyjna została określona przez Tofflerów mianem „trzeciej fali". Do czasów obecnych ludzkość przeżyła dwie wielkie fale przemian, z których każda unicestwiła dawne kultury i cywilizacje, a na ich miejsce wprowadziła sposób życia, który byłby niepojęty dla ludzi, żyjących wcześniej. Pierwsza fala – rewolucja rolnicza – rozciągnęła się na tysiące lat. Druga fala, w trakcie której powstała cywilizacja przemysłowa, trwała zaledwie trzysta lat.

Społeczeństwo „trzeciej fali" jest oparte na wiedzy. Doświadczenia historyczne mówią, że „kto ma wiedzę, ten ma władzę". Istnienie społeczeństwa informacyjnego nie jest kwestią zadekretowanej decyzji, świadomego wyboru, lecz raczej pochodną wystarczająco wysokiego stopnia rozwoju gospodarki. Konkretne państwo osiąga poziom cywilizacji informacyjnej, jeśli może istnieć i rozwijać się dzięki organizacjom, których domeną działalności jest praca intelektualna.

Nowoczesne, współczesne społeczeństwo informacyjne, wspomagane przez komputerowe i telekomunikacyjne technologie dostrzega, że zastosowanie i wdrożenie nowych produktów oraz technologii znacznie zmienia standard jego życia, rodzaj komunikowania się lub sposób wykonywanej pracy. Również bardzo szybko wdrażana nowoczesna technologia wymusza na społeczeństwie ciągłe odnawianie i pogłębianie wiedzy z różnych dziedzin nauki i techniki.

Rewolucja informacyjna jest postrzegana jako kompleks procesów, realizowanych za pomocą mediów elektronicznych, prowadzących od powstania koncepcji dotyczących urządzenia spraw obywatelskich i sformułowania propozycji, aż do wcielenia tych koncepcji w życie i osiągnięcia „stadium operacyjnego". Na kompleks ten składają się działania w zakresie badań, planowania, wdrożenia, zarządzania – podejmowania decyzji, kontroli informacji, komunikacji i wielu innych.

Rewolucja informacyjna wywiera wpływ na sposób prowadzenia wojny. Nowe środki komunikacyjne zastosowane w wojnie ery informacyjnej w określonych uwarunkowaniach mogą niemal samodzielnie osiągać militarne i polityczne cele wojny, m.in. mogą prowadzić do zażegnania konfliktu, osłabienia morale wojsk przeciwnika i ludności cywilnej lub destrukcji infrastruktury informacyjnej. W krajach wysoko rozwiniętych, posiadających rozbudowaną infrastrukturę możliwe są np. blokady wojskowych systemów dowodzenia, opanowanie systemów kontroli ruchu powietrznego, czy włamania do serwerów i paraliż ważnych serwisów internetowych.

Współczesna wojna, a w zasadzie konflikt zbrojny lokalnej społeczności, może przynieść olbrzymie skutki dla całego globu. Wymagania sojusznicze zobowiązują do przekształcenia nie tylko armii, ale także szeregu kompetencji dowódców i żołnierzy, którzy poza doskonałym przygotowaniem do walki pod względem rzemiosła wojskowego, powinni posiadać kompetencje, takie jak: lingwistyczne, kulturoznawcze, prawne, administracyjne, psychologiczne i informacyjne.

D. Starry szef TRADOC (Dowództwa Szkolenia i Doktryn Sił Lądowych USA) ocenił, że Tofflerowie dokonali rzetelnej analizy przyszłości. Ich wizje zostały skonfrontowane z pomysłami strategów wojskowych.

Istotą nowej koncepcji wojennej stał się system bardziej elastyczny, dynamiczny i zdecentralizowany, oparty na wymianie informacji; system, który wykorzystuje lokalne, bezpośrednio związane z polem bitwy zasoby informacyjne i odwołuje się do decyzji znakomicie wyszkolonych, w dużym stopniu niezależnych, dowódców.

Wojnę w erze informacyjnej można prowadzić bez naruszania granic, czyli nie jest ona czynnikiem geograficznym. Można sparaliżować telekomunikację, ruch powietrzny, bankowość, produkcję elektryczności i wiele innych dziedzin o istotnym znaczeniu poprzez masową infiltrację systemów komputerowych. Pod pewnym względem ten rodzaj wojny tworzy nową równowagę sił między krajami wysoko rozwiniętymi a mniejszymi stronami konfliktu, które mogą skutecznie zaatakować przy pomocy małego gangu hackerów.

Nowe technologie informacyjne są czynnikiem, który rodzi nowe koncepcje operacji wojskowych i stwarza zapotrzebowanie na zupełnie nowe rozwiązania.

Sytuacja ta została dostrzeżona przez sojusz, który dokonał aktualizacji dotychczasowej koncepcji strategicznej, wprowadzając tzw. „Nową koncepcję strategiczną" (Alliance's New Strategie Concept). W jej ramach została opracowana

„Inicjatywa zdolności obronnych" (DCI – Defence Capabilites Initiative), przyjęta w kwietniu 1999 r. przez szefów państw i rządów krajów NATO.

Podstawowym założeniem tej inicjatywy jest natychmiastowa gotowość sił sojuszu do odparcia jakiejkolwiek agresji skierowanej przeciwko jakiemukolwiek krajowi członkowskiemu. Na europejskim obszarze odpowiedzialności operacyjnej NATO prawdopodobieństwo wystąpienia agresji militarnej na dużą skalę jest obecnie niewielkie. Znacznie większe są zagrożenia wynikające z szerokiej gamy peryferyjnych konfliktów regionalnych o małej intensywności, których źródłem są przede wszystkim:

— wojny i konflikty regionalne;
— walki na podłożu religijnym;
— kryzysy ekonomiczne i społeczne.

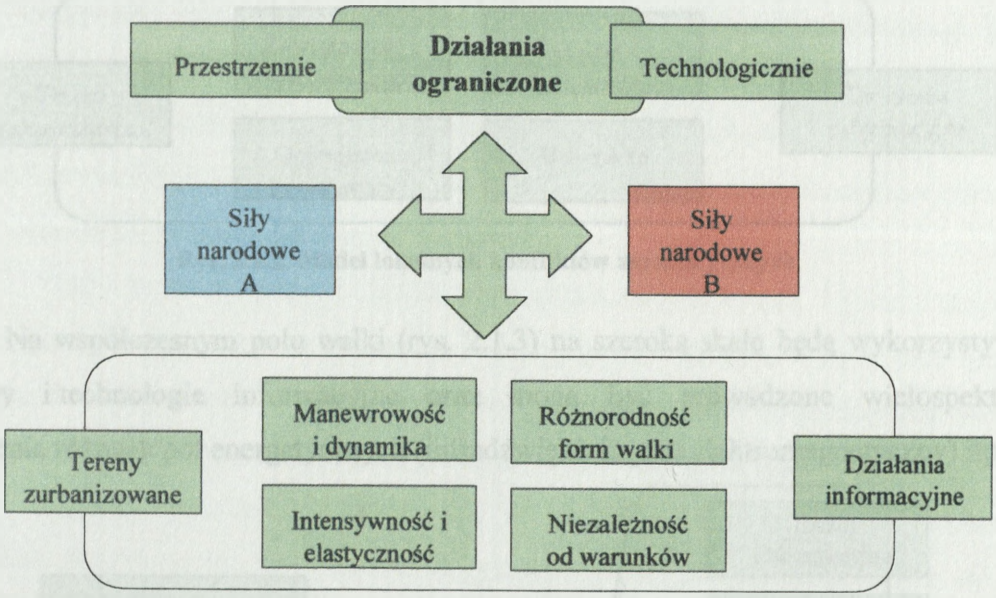
Konieczność ciągłego utrzymywania pokoju w różnych sytuacjach kryzysowych, jakie miały chociażby miejsce w ostatnich latach, zmusza sojusz do zachowania odpowiednio wysokiej gotowości operacyjnej i stosownie dużej mobilności wojsk celem szybkiego rozwijania ich na odległych teatrach działań operacyjnych. W planach strategicznych sojuszu szczególną rolę odgrywają połączone operacje wielonarodowe, których podstawą jest interoperacyjność sił połączonych, dotycząca kontyngentów narodowych oraz niektórych państw partnerskich.

W inicjatywie mówi się wprost o coraz większym zagrożeniu pokoju światowego, a tym samym bezpieczeństwa państw NATO ze strony sił (wojsk) nieregularnych (Irregular Forces). Tak organizowane siły nieregularne mogą być wyposażone w najnowszej generacji uzbrojenie, nowoczesną technologię informacyjną i mogą być odpowiednio przeszkolone do prowadzenia skutecznych akcji dywersyjno-rajdowych.

Wdrażanie i kształtowanie nowej „Inicjatywy zdolności obronnych" jest zawsze rozpatrywane w aspekcie konkretnej sytuacji polityczno-militarnej, jaka panuje w przypuszczalnym rejonie działań sił NATO. Zgodnie z założeniami „Inicjatywy zdolności obronnych", wykorzystanie sił NATO ograniczone jest w zasadzie do konfliktów lokalnych o różnej skali intensywności. Praktycznie inicjatywa ta wyklucza scenariusz wojny globalnej. Dlatego jej aplikację rozpatruje się na dwóch skrajnych modelach dotyczących odpowiednio:

— lokalnych konfliktów symetrycznych (Symmetric Conflict),
— lokalnych konfliktów asymetrycznych (Asymetric Conflict).

Konflikt *symetryczny* (rys. 2.1.1). jest definiowany jako starcie dwóch równorzędnych, regularnych armii różnych państw. Zakłada się, że są to nowoczesne, dobrze uzbrojone i wyszkolone armie, które prowadzą ograniczone działania wojenne w sąsiedztwie swoich granic. Działania te cechować będzie duża manewrowość, dynamika walki, olbrzymia elastyczność i różnorodność rodzajów wojsk i służb. Ponadto będą one prowadzone bez względu na porę dnia, warunki klimatyczne i konfigurację terenową. Ocenia się, że działania na lądzie toczyć się będą w pobliżu rejonów zurbanizowanych, co preferuje szybkie jednostki szturmowe, o lżejszym uzbrojeniu i nowoczesnym wyposażeniu. Działania informacyjne przyczyniać się będą do zwiększenia potencjału bojowego jednej ze stron, która pierwsza uzyska przewagę informacyjną nad przeciwnikiem.



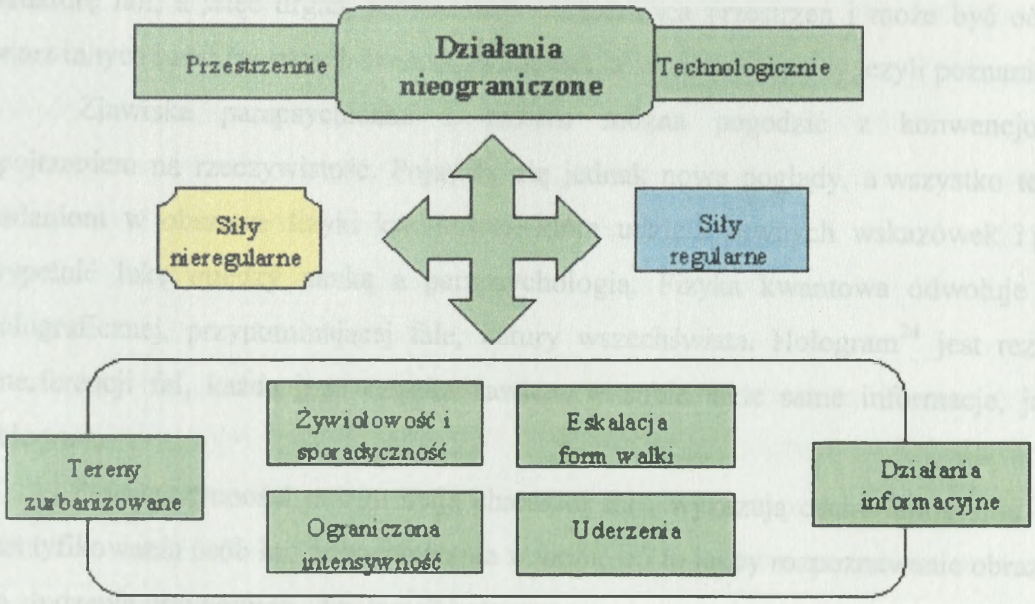
Rys. 2.1.1. Model lokalnych konfliktów symetrycznych

Drugi skrajny model reprezentuje konflikt *asymetryczny*, w którym zakłada się, że przeciwnikiem dobrze uzbrojonej, wyposażonej i wyszkolonej regularnej armii jednego państwa lub grup państw sojuszniczych będą bliżej nieokreślone siły nieregularne (rys. 2.1.2).

Siły te będą prowadzić infiltrację i destrukcję zasobów informacyjnych oraz odpowiednich sieci i systemów komputerowych przeciwnika. Obiektami informacyjnych ataków mogą być systemy dowodzenia siłami zbrojnymi, sieci i placówki finansowo-bankowe, a także ważne instytucje użyteczności publicznej takie, jak: np. policja, straż

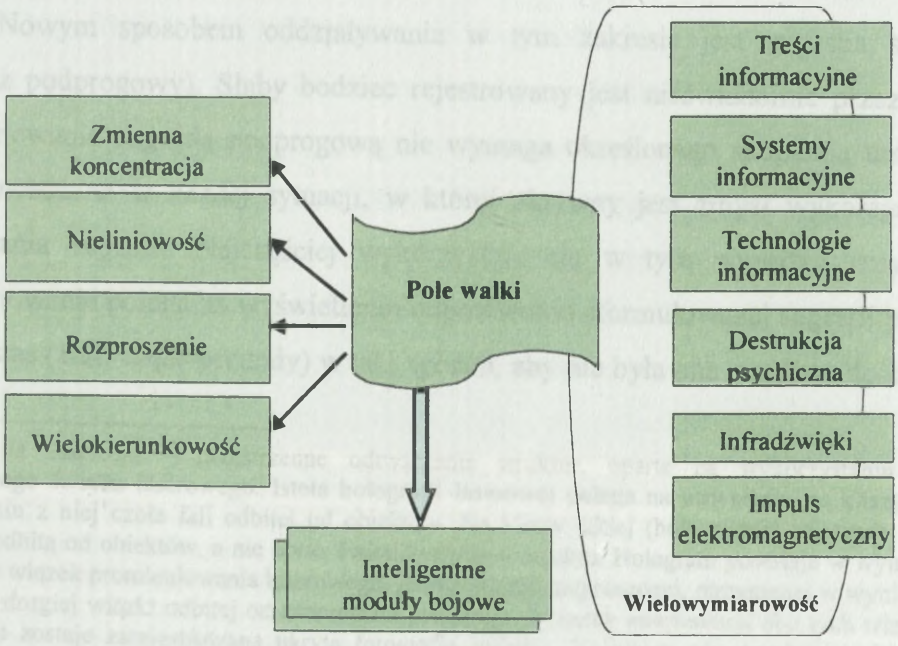
pożarna, placówki służby zdrowia, sądownictwo, prokuratura czy też systemy sterowania siecią energetyczną, kolejami państwowymi.

Jak wykazuje historia wojen, w praktyce najczęściej stosowane są mieszane warianty nieszablonowe, dalekie od czystych modeli teoretycznych. Należy się liczyć, że wojny lokalne będą zawierać komponenty obu przedstawionych powyżej modeli.



Rys. 2.1.2. Model lokalnych konfliktów asymetrycznych

Na współczesnym polu walki (rys. 2.1.3) na szeroką skalę będą wykorzystywane systemy i technologie informacyjne oraz mogą być prowadzone wielospektralne zakłócenia różnych pól energetycznych (infradźwięki, impuls elektromagnetyczny) itp.



Rys. 2.1.3. Cechy współczesnego pola walki

Nowe możliwości otwierają się przed psychotroniką i parapsychologią. Badania w tych obszarach na dużą skalę prowadzone są w Stanach Zjednoczonych i Federacji Rosyjskiej. Wielu naukowców na świecie uznaje fenomeny paranormalne za oczywiste, przyjmując istnienie w organizmach żywych pewnej formy energii, różnej od znanych postaci. Można nazwać ją bioenergią lub nieokreśloną energią biologiczną. Posiada ona strukturę fali, a więc drgań, promieniuje w otaczającą przestrzeń i może być odbierana przez innych ludzi (w sposób świadomy lub nie) jako „obraz" rzeczy, czyli poznanie.

Zjawiska parapsychiczne z trudem można pogodzić z konwencjonalnym spojrzeniem na rzeczywistość. Pojawiły się jednak nowe poglądy, a wszystko to dzięki badaniom w obszarze fizyki kwantowej, która udziela pewnych wskazówek i pomaga wypełnić lukę między nauką a parapsychologią. Fizyka kwantowa odwołuje się do holograficznej, przypominającej fale, natury wszechświata. Hologram[24] jest rezultatem interferencji fal, każda jego cząstka zawiera w sobie takie same informacje, jak cały hologram.

Pewne czynności mózgu mają charakter fal i wykazują cechy hologramu. Proces identyfikowania osób lub przywoływania wspomnień to jakby rozpoznawanie obrazów, co do złudzenia przypomina „działanie" hologramu.

Wielu badaczy widzi w zjawiskach paranormalnych skutek działania sugestii lub autosugestii, która wyzwala w naturze ludzkiej pewne energie, wywołujące niezwykłe skutki. Sugestia może wywołać nie tylko subiektywne, ale i obiektywne skutki, co prowadzi do przyjęcia przez ludzi określonych postaw czy zachowań.

Nowym sposobem oddziaływania w tym zakresie jest sugestia subliminalna (przekaz podprogowy). Słaby bodziec rejestrowany jest nieświadomie przez człowieka. Programowanie sugestią podprogową nie wymaga określonego skupienia umysłu. Może być prowadzane w każdej sytuacji, w której aktywny jest zmysł wykorzystywany do przekazania sugestii. Najczęściej wykorzystuje się w tym wypadku zmysł wzroku. Programowanie polega na wyświetleniu odpowiednio sformułowanej sugestii przez bardzo krótki czas (1/20 część sekundy) w taki sposób, aby nie była ona możliwa do świadomego

[24]Holografia laserowa – przestrzenne odtwarzanie struktur, oparte na wykorzystaniu interferencji koherentnego światła laserowego. Istota holografii laserowej polega na utrwalaniu na kliszy, a następnie odtwarzaniu z niej czoła fali odbitej od obiektów. Na kliszy takiej (hologramie) rejestruje się więc falę świetlną odbitą od obiektów, a nie obraz świetlny danego obiektu. Hologram powstaje w wyniku nałożenia się dwóch wiązek promieniowania laserowego: jednej wiązki rozproszonej, otrzymanej w wyniku odbicia od obiektu, i drugiej wiązki odbitej od zwierciadła płaskiego. Wskutek interferencji obu tych wiązek na kliszy hologramu zostaje zarejestrowana ukryta fotografia obiektu. Hologram nie przedstawia bowiem obrazu danego obiektu, lecz jedynie jest zbiorem nieregularnych prążków interferencyjnych. Odczytywanie hologramu realizowane jest również za pomocą wiązki laserowej.

zarejestrowania. Oddziaływanie takie ze względu na bardzo krótki czas trwania kodowane jest w pamięci z pominięciem świadomości. Tak powstałe engramy (ślady pamięciowe) pewnych znaków, symboli (logo) czy słów mogą być rozpoznawane później jako już znane i kojarzące się z czymś przyjemnym[25].

Skuteczność prymowania subliminalnego udowodnił w 1992 r. A. Krosnick. Badanym pokazywane były zdjęcia obcych osób. Pojawienie się każdego z nich poprzedzone zostało podprogową emisją zdjęcia wywołującego pozytywne lub negatywne emocje. Te ukierunkowujące (prymujące) zdjęcia zostały oczywiście wcześniej przetestowane. Wyniki eksperymentu pokazały jasno, że takie zestawienie spowodowało „skrzywienie" oceny osób względem grupy kontrolnej (w grupie kontrolnej zdjęcia osób prezentowane były bez wcześniejszego prymowania). Co więcej, do opisanego zjawiska doszło już po jednej ekspozycji fotografii.

Zdaniem A. Augustynka percepcja podprogowa jest faktem. Bodźce świadomie niedostrzegalne (zarówno wizualne, jak i dźwiękowe) są odbierane podświadomie, mogą to być pojedyncze słowa czy obrazy. Przekaz ten ma jednak ograniczony wpływ na człowieka. Może wzmacniać pewne podstawowe potrzeby, takie jak: głód, pragnienie czy popęd seksualny, natomiast nie wpływa na zachowanie człowieka wbrew jego chęciom, wartościom czy zasadom.

W 1993 i 1994 r. prasa amerykańska (Defense Electronics, Newsweek i Village Voice) opublikowała wiadomość, że Igor Smirnov z Moskiewskiej Akademii Medycznej zademonstrował amerykańskim służbom bezpieczeństwa i ekspertom FBI urządzenie wytwarzające dźwięk, które było w stanie „zaszczepić" myśli (perswazja subliminalna) w mózgu człowieka i w ten sposób kontrolować jego działania[26].

W Stanach Zjednoczonych przekaz subliminalny – o ile występuje – podlega ochronie wynikającej z pierwszej poprawki do konstytucji. Wspomniana poprawka gwarantuje wolność słowa i wyznania. Podczas postępowania wstępnego sędzia prowadzący sprawę, Jerry Carr Whitehead stwierdził, że komunikaty subliminalne nie spełniają przesłanek pierwszej poprawki. Odbiorca takiego przekazu nie jest go świadomy i nie może go uniknąć. Jest więc to naruszenie jego prywatności[27].

---

[25]A. Augustynek, *Reklama podprogowa; fakt czy artefakt,* Wiedza i Życie 1998, nr 7, s. 56–58. *Oddziaływanie podprogowe*, Advertising & You" 2001, nr 11, s. 1, 6–8.
[26]*Some tidbits on Mind Control and Psychic Manipulation,* Pacific Standard Time, 2/20/02.
[27]T. E. Moore, *The Judas Priest Trial*, Skeptical Inquirer, November 1996.

Mimo to badania dotyczące kontroli nad ludzkim umysłem prowadzone są w Stanach Zjednoczonych przez korporacje rządowe i siły zbrojne (HAARP[28]). Rosyjski program nosi nazwę – SURRA, pięć zestawów tej broni rozpoczęło działalność w 1976 r.

Prowadzone są również badania nad bronią ekstremalnie niskich częstotliwości (Extremely Low Frequency Weapon[29]) z zamiarem wpływania na działanie przywódców państw i dowódców wojskowych.

W programach tych chodzi m.in. o możliwość wykorzystania infradźwięków, które charakteryzują się znaczną długością fal (powyżej 21,25 m). Infradźwięki mogą powodować: wydłużenie czasu reakcji, zmniejszenie spostrzegawczości, zaburzenia równowagi. Ale również znane są efekty słuchowe, tłumaczone nieliniowością przewodzenia w obrębie ucha środkowego i wewnętrznego. Progi percepcji słuchowej infradźwięków gwałtownie wzrastają wraz ze spadkiem częstotliwości i mogą powodować: ból uszu, czasowe przesunięcie progu słuchu, zaburzenia rozumienia mowy.

Infradźwięki mogą być też odbierane przez receptory wibracji, szczególnie w mięśniach, ścięgnach i stawach oraz na skórze. Progi czucia drgań leżą około 20÷40 dB powyżej progów percepcji słuchowej. Infradźwięki mogą wywoływać drgania rezonansowe w poszczególnych tkankach i narządach organizmu, w szczególności w obrębie jamy brzusznej, klatki piersiowej i gardła.

Człowiek ma możliwość odbioru dźwięków, czyli fal sprężystych o częstotliwości w zakresie od 16 Hz do 20 kHz. Infradźwięki, chociaż niesłyszalne przez zmysł słuchu człowieka, są jednak odbierane przez mózg. Aktualnie w zakresie fal sprężystych stosowane są *generatory infradźwięków* do czasowego obezwładniania człowieka 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. Zaletą tych rodzajów broni jest przede wszystkim łatwość przenikania przez struktury materii. Obrona przed generatorami infradźwięków opiera się

---

[28]HAARP (High-frequency Active Auroral Research Project) prawdopodobnie prowadzony od 1968 roku, oficjalnie ujawniony w 1990 roku. N. Begich, J.Manning, *Angels Don't Play This Haarp, Advances in Tesla Technology*, Earthpulse Press, 1995.

[29]ELFW (Extremely Low Frequency Weapon) broń ekstremalnie niskich częstotliwości należy do broni energii kierowanej (Directed Energy Weapon) lub inaczej wiązkowej broni energetycznej. Działanie tej 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 broń: częstotliwości radiowych, laserową, cząstek elementarnych, ekstremalnie niskich częstotliwości, infradźwiękową, impulsową ekstremalnie wysokich częstotliwości (promieniowanie gamma).

na budowaniu tzw. miękkich zasłon, w celu absorpcji energii fali dźwiękowej, oraz tworzeniu tzw. pól aktywnego hałasu. Istota ich działania polega na wytworzeniu fali dźwiękowej tej samej długości, co fala atakująca, lecz odwróconej w fazie (o 180 stopni). Zasadniczym problemem w stosowaniu tej broni jest stworzenie odpowiedniego zestawu specjalistycznych głośników oraz wzmacniaczy, które wymagają m.in. bardzo wydajnych układów chłodzenia. Ponadto fale sprężyste są słabo tłumione i mogą rozchodzić się na duże odległości.

Przeprowadzone badania wskazują, że częstotliwości rzędu 6,67 Hz mogą wywoływać depresje, napięcia lub strach. Częstotliwości: 7,83 oraz 8 i 9 Hz wywołują sztuczną wesołość, podniecenie oraz beztroskę. Natomiast częstotliwości w zakresie 2–6 Hz wywołują spowolnienie reakcji oraz senność. W Polsce badania nad tym zagadnieniem od 1992 r. prowadzi prof. Stanisław Micek oraz dr Andrzej Kułak z Uniwersytetu Jagiellońskiego w Krakowie.

Podobne efekty do infradźwięków wywołują światła stroboskopowe. Stroboskopy to urządzenia wytwarzające błyski światła z określoną częstotliwością. Częstotliwość błysków jest określana za pomocą generatora żądanej częstotliwości lub w takt jakiegoś sygnału sterującego, np. pochodzącego ze sprzętu audio (miganie w takt muzyki).

Zasada działania każdego stroboskopu jest taka sama. Stroboskop zawsze składa się z palnika ksenonowego (lampy błyskowej), kondensatora gromadzącego energię oraz modułu sterującego wyładowaniami. Błysk światła powstaje na skutek rozładowania przez palnik naładowanego kondensatora. Co prawda palnik jest na stałe połączony z kondensatorem, ale napięcie zgromadzone na kondensatorze (najczęściej 300 V lub 600 V) jest za niskie, aby przebić się przez palnik. Błyski światła występują tylko wtedy, gdy pojawi się jonizujący impuls wysokiego napięcia na zewnętrznej, trzeciej, elektrodzie palnika. Impuls napięcia rzędu kilku kilowoltów wystarcza, aby zjonizować znajdujący się w palniku gaz, który zaczyna gwałtownie przewodzić i przyjmuje energię kondensatora, zamieniając ją na biało-niebieskie światło oraz ciepło.

Stroboskop podczas działania wydziela dużo ciepła. Grzeją się w zasadzie tylko 2 elementy: palnik oraz opornik mocy. O ile opornik (jeżeli jest odpowiedniej mocy) poradzi sobie z oddawaniem ciepła, to jednak palnik ma z tym problemy. Przy stroboskopach większej mocy potrzebne jest chłodzenie (np. wentylatorem). Stroboskop potrafi

generować błyski światła z częstotliwością[30] 0,5–15Hz. Energia błysków zależy od pojemności kondensatorów.

Fale mózgowe synchronizują swoją działalność ze światłami stroboskopowymi. Jeśli światło stroboskopowe pulsuje z częstotliwością 10 razy na sekundę, to podczas badania EEG można zaobserwować taką samą aktywność fal w mózgu człowieka. Przez sygnały światła pulsującego jest możliwe sterowanie falami w mózgu człowieka, np. dopasowywanie fal alfa[31] w celu dobrego zapamiętywania lub fal theta w celu głębokiego relaksu.

Ponadto prowadzone są badania nad specjalnymi wirusami, które umieszczone w systemach broni potencjalnego przeciwnika, spowodują ich dezorganizację i nieefektywność.

Urządzenia wytwarzające impuls elektromagnetyczny[32] (wielkości walizki) są już projektowane w Laboratorium Narodowym Stanów Zjednoczonych w Los Alamos. Planuje się także wykorzystanie specjalnego rodzaju mikrobów, które mogą zniszczyć układy elektroniczne i izolacyjne w komputerach.

Nowe środki przemocy (nieśmiercionośne) zastosowane w czasie wojny – i nie tylko – mogą być bardzo skuteczne z punktu widzenia osiągnięcia zwycięstwa nad przeciwnikiem. A zatem kształtuje się nowa jakość w prowadzeniu operacji, częściowo zgodna z poglądami J. Blocha (*Przyszła wojna pod względem technicznym, ekonomicznym i politycznym*, Warszawa, 1899). Jego zdaniem cel wojny mógł być osiągnięty za pomocą walki zbrojnej albo za pomocą nieorężnych form walki (dyplomatycznej, politycznej, presji propagandowej itp.). Twierdził, że w dotychczasowych rozważaniach teoretycy popełniali błąd, polegający na badaniu doświadczeń wojen minionych, bez uwzględniania zmian zachodzących współcześnie. W swojej pracy przedstawił spostrzeżenia dotyczące prowadzenia operacji. Zalecał prowadzenie rozpoznania z wykorzystaniem środków naziemnych, morskich oraz balonów i aerostatów.

Duże znaczenie przypisywał dowodzeniu na polu walki. Zapowiadał malejącą rolę naczelnego wodza, a więcej uwagi przywiązywał do szczebli operacyjnych i taktycznych.

---

[30]Częstotliwość wyraża liczbę impulsów emitowanych w czasie jednej sekundy.

[31]Rytm fal alfa (8–13 Hz) został zapisany i nazwany po raz pierwszy przez Bergera w 1929 r. Rytm fal theta składa się z fal o częstotliwości 4-7,5 Hz.

[32]Impuls elektromagnetyczny – impuls fal radiowych o czasie trwania rzędu tysięcznych części sekundy. Charakteryzuje się bardzo dużą amplitudą zmian natężenia pola elektrycznego i magnetycznego. Powoduje niszczenie niektórych elementów półprzewodnikowych na skutek przeciążeń. Zasadniczymi obiektami oddziaływania impulsu elektromagnetycznego są środki elektroniczne.

Twierdził, że nawet dowódca szczebla operacyjnego nie będzie mógł kierować samodzielnie wszystkimi elementami swych ugrupowań.

Jak przedstawiono na rysunku 2.1.3, współczesne pole walki charakteryzuje m.in. zmienna koncentracja (Variable Density), nieliniowość (Non-Linearity), rozproszenie (Dispersion), a także wielokierunkowość (Multidirectionality).

Zarówno siły regularne, jak też nieregularne działające na polu walki, będą się odznaczać większą ruchliwością, relatywnie mniejszą liczebnością, większą autonomicznością, co będzie wynikać z konieczności operowania w znacznym oddaleniu od macierzystych baz zaopatrzeniowych i braku lokalnego wsparcia. Będą to więc siły ekspedycyjne, często działające w strukturze sił połączonych (Joint Forces), grupujące jednostki wojsk lądowych, sił powietrznych i sił morskich.

Zgodnie z modułową strukturą nowoczesne siły szybkiego reagowania muszą być przygotowane do walki w różnych warunkach, z maksymalną szybkością i dużą skutecznością działań. W celu wypełnienia misji, czyli ciągłego utrzymywania inicjatywy w zakresie zdolności obronnych, niezbędne są mobilne, dobrze wyposażone i wyszkolone, wysoce autonomiczne i zwarte inteligentne moduły bojowe, składające się z doskonale wyposażonych profesjonalistów o najwyższej skuteczności i elastyczności działania.

Przeprowadzona analiza literatury przedmiotu pozwala na sformułowanie następujących tez.

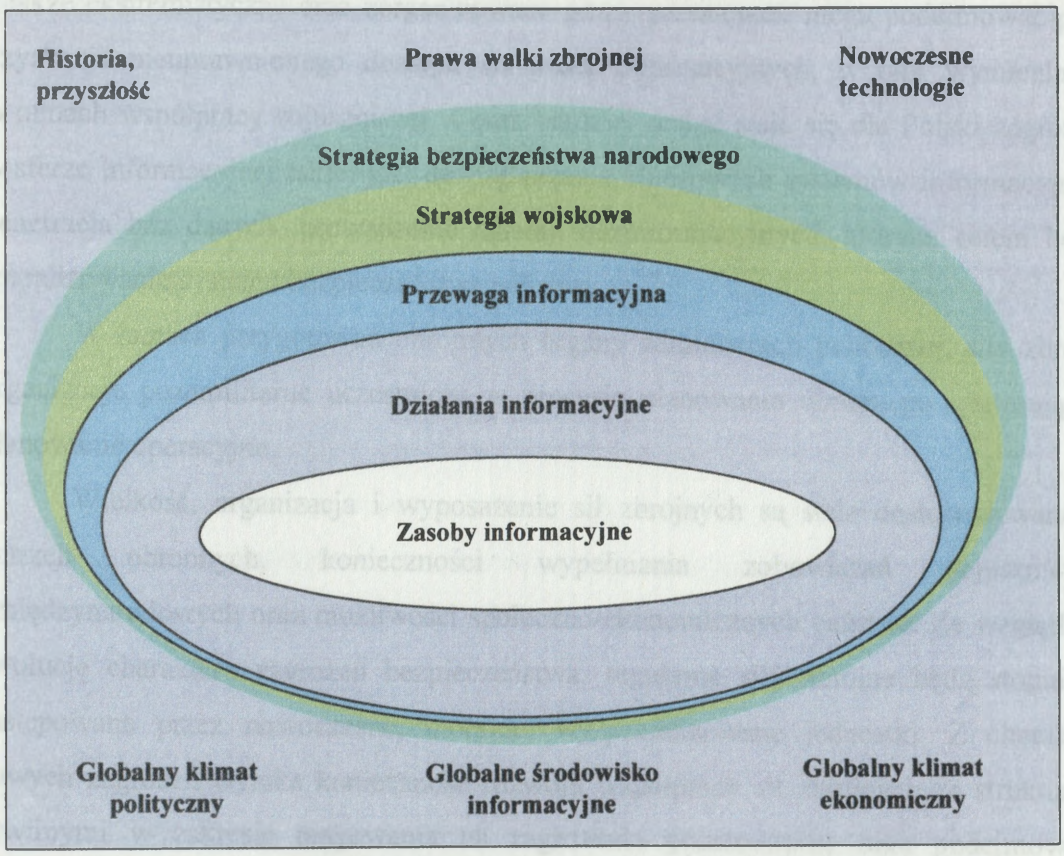
Teza 1. *W wieku informacji zapotrzebowanie na użyteczną informację staje się jednym z podstawowych zadań zarówno w sferze cywilnej, jak i militarnej. Aktualnie informacja jest traktowana jako zasób strategiczny. Stajemy się społeczeństwem „trzeciej fali", tzw. wojownikami wiedzy, co w znaczny sposób zwiększa moc bojową wojsk. To wskazuje, że informacja i technologie informacyjne powinny zostać włączone w proces decyzyjny.*

Teza 2. *Uzyskiwana w tym zakresie przewaga staje się nie tylko gwarantem, ale wręcz warunkiem bezpiecznej egzystencji i to nie tylko w skali pojedynczego człowieka czy instytucji, ale w odniesieniu do państwa czy koalicji.*

Teza 3. *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 zagrożenia w sferze informacyjnej stają się realnym zagrożeniem 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 strategię bezpieczeństwa państwa oraz strategię wojskową.

Teza 4. *Do czynników, które należy brać pod uwagę, można zaliczyć: tworzenie środowiska informacyjnego, dotychczasowy rozwój państwa (analiza wojen) i jego przyszłość, prawa walki zbrojnej, nowe technologie (w tym szczególnie informacyjne), sytuację polityczną i ekonomiczną na świecie (rys. 2.1.4).*



Rys. 2.1.4. Miejsce działań informacyjnych w strategii bezpieczeństwa narodowego

Teza 5. *Kolejnym ważnym aspektem, który należy brać pod uwagę, jest sposób uzyskania przewagi informacyjnej. Duża rola w tym zakresie przypada siłom zbrojnym oraz instytucjom narodowym. Instytucje te posiadają w swoich strukturach jednostki i organa, które mogą prowadzić działania informacyjne. Odpowiednie wykorzystanie zasobów oraz technologii informacyjnych przez te elementy może znacząco przyczynić się do uzyskania celów operacji połączonych.*

Niektóre zadania dotyczące tej problematyki zostały już sprecyzowane w „Strategii bezpieczeństwa RP" i „Strategii obronności RP". W dokumentach tych m.in. stwierdza się,

że istota zmian w środowisku bezpieczeństwa Polski polega na przesuwaniu się punktu ciężkości z zagrożeń klasycznych (inwazja zbrojna), których znaczenie się zmniejsza, na zagrożenia nietypowe, których źródłem stają się także trudne do zidentyfikowania podmioty pozapaństwowe.

Najpoważniejsze niebezpieczeństwo wśród nowych zagrożeń dla systemu międzynarodowego i bezpieczeństwa poszczególnych państw, w tym Polski, stwarza zorganizowany terroryzm międzynarodowy, aczkolwiek stopień zagrożenia terroryzmem dla poszczególnych państw jest różny. Ugrupowania terrorystyczne, obce służby specjalne, a także ekstremistyczne oraz zorganizowane grupy przestępcze mogą podejmować próby uzyskania nieuprawnionego dostępu do treści informacyjnych, w tym wymienianych w ramach współpracy sojuszniczej. Coraz bardziej realne stają się dla Polski zagrożenia w sferze informacyjnej takie, jak: dezorganizacja kluczowych systemów informacyjnych, penetracja baz danych, prowadzenie działań dezinformacyjnych, których celem będzie sparaliżowanie systemu bezpieczeństwa państwa.

W ramach przygotowań obronnych organy administracji publicznej, siły zbrojne, organizacje pozamilitarne uczestniczą w procesie planowania obronnego obejmującego planowanie operacyjne.

Wielkość, organizacja i wyposażenie sił zbrojnych są stale dostosowywane do potrzeb obronnych, konieczności wypełniania zobowiązań sojuszniczych i międzynarodowych oraz możliwości społeczno-ekonomicznych państwa. Ze względu na ewolucję charakteru zagrożeń bezpieczeństwa, regularne siły zbrojne będą stopniowo zastępowane przez nowoczesne, mobilne, wyspecjalizowane jednostki. Z charakteru nowych zagrożeń wynika konieczność rozwoju współpracy sił zbrojnych ze strukturami cywilnymi w zakresie reagowania na zagrożenia pozamilitarne oraz podejmowania operacji ratowniczych i antyterrorystycznych w kraju i poza jego granicami.

Siły Zbrojne RP służą zapewnieniu bezpieczeństwa Polski i niosą pomoc sojuszniczą zgodnie z art. 5 traktatu północnoatlantyckiego, ich celem jest także ochrona polskich interesów oraz budowa pozycji Polski w NATO i Unii Europejskiej.

Ważnym zadaniem sił zbrojnych jest zapewnienie należytej ochrony infrastruktury informacyjnej. Wyznaczone służby podejmują działania wspólnie z sojusznikami, a także producentami i dostawcami urządzeń oraz oprogramowania komputerowego, krajowymi operatorami telekomunikacyjnymi i dostawcami usług internetowych, ośrodkami badawczymi i szkoleniowymi.

Aby podejmowane działania w tej dziedzinie były skuteczne, należy w sposób priorytetowy podejść do rozwoju i wdrażania rodzimej kryptografii oraz dostosować przepisy prawa telekomunikacyjnego, które wraz z szybkim postępem technologicznym mogą się okazać niewystarczające do zapewnienia bezpieczeństwa informacyjnego.

Działania na rzecz utrzymania właściwego stanu polskiej infrastruktury informacyjnej są jednym z warunków zapewnienia odpowiedniego potencjału obronnego i bezpieczeństwa kraju, zarówno wewnętrznego, jak i zewnętrznego.

Zintensyfikowanie wysiłków na rzecz zapewnienia koniecznego potencjału informacyjno-obronnego państwa jest jednym z priorytetowych zadań w obszarze obronności, w tym w siłach zbrojnych, u progu XXI wieku.

Ogniwa informacyjne, zarówno cywilne, jak i wojskowe realizują zadania związane z ochroną i propagowaniem polskich interesów na arenie międzynarodowej, informacyjnym osłabianiem przeciwnika oraz umacnianiem morale, determinacji obronnej i wytrwałości własnego społeczeństwa.

Najistotniejsze staje się zapewnienie sprawności i bezpieczeństwa systemów dowodzenia i kierowania, zwalczanie przestępczości komputerowej wymierzonej w infrastrukturę informacyjną i przede wszystkim uzyskanie przewagi informacyjnej.

Uzyskanie przewagi informacyjnej wymagać będzie mistrzowskiego zdobywania informacji, jej wykorzystania oraz manipulowania nią. Można to uzyskać dzięki prowadzeniu działań informacyjnych. Jest to argument przemawiający za tworzeniem struktur działań informacyjnych i włączeniem ich do instrumentarium militarnego.

Docenianie znaczenia przewagi informacyjnej nie jest zjawiskiem nowym. Dowódcy na polu walki zawsze poszukiwali sposobności, aby więcej wiedzieć niż przeciwnik. Od czasów konia trojańskiego wojna wymaga rozpoznania, wprowadzania w błąd, fałszowania oraz innych elementów fikcji.

Najstarszym z zapisów, mówiącym o roli przewagi informacyjnej w walce zbrojnej, jest kryterium sukcesu zbrojnego, sformułowane przez chińskiego teoretyka i filozofa Sun Tzu w VI wieku p.n.e. W traktacie „Sztuka wojny" stwierdza on: „Poznaj siebie i poznaj wroga, dopiero wtedy twoje zwycięstwo nie będzie zagrożone. Poznaj warunki terenu i pogody, wtedy twoje zwycięstwo będzie całkowite"[33].

[33]Sun Tzu, op. cit., s. 116.

Działania wojenne prowadzone przez Aleksandra Wielkiego (336–323 p.n.e.) odznaczały się szybkością oraz bezpieczeństwem wojsk. U ich podstaw leżała dokładna znajomość przeciwnika, właściwa ocena własnych możliwości i sytuacji (rozpoznanie).

Podobne przedsięwzięcia realizował Czyngis-chan. Jego armie zawsze maszerowały w oddzielnych kolumnach. Uniemożliwiało to tym samym przeciwnikowi ustalanie planowanych miejsc ataku.

W sposób bardzo zsynchronizowany wykonywał przesunięcia swych armii w kierunkach celów, jakie zamierzał osiągnąć. Powodowało to zaskoczenie przeciwnika i to nie tylko w skali operacyjnej, ale nawet strategicznej.

Operacje „Torch", „Husky" oraz „Overlord" (opisane przez G. Pattona w książce „Wojna jak ją poznałem" w 1947 roku) miały pewne znamiona współczesnych działań informacyjnych. W operacjach tych na szeroką skalę prowadzono rozpoznanie, walkę elektroniczną, działania psychologiczne oraz dezinformację.

Pod koniec XX wieku nastąpił gwałtowny rozwój elektroniki i nowoczesnych technologii informacyjnych, które w znaczny sposób mogą wprowadzić w błąd przeciwnika, co do posiadanych sił i prowadzonych działań, zwiększając tym samym zdolność bojową wojsk własnych.

Wojna w rejonie Zatoki Perskiej w 1991 roku ukazała w sposób szczególny znaczenie technologii informacyjnej na współczesnym polu walki. W czasie tej wojny Stany Zjednoczone ujawniły nową kategorię działań, którą formalnie nazwano działaniami informacyjnymi. Dzięki realizacji przedsięwzięć z zakresu działań informacyjnych uzyskano dużą elastyczność, synchronizację i szybkość prowadzonych działań, krótki czas reakcji ogniowej i wysoką precyzję rażenia w niespotykanej do tej pory skali w historii wojskowości. Dzięki stosowaniu technologii informacyjnych, znacznie mniejsze i słabiej wyposażone siły zbrojne mogą odnieść zwycięstwo nad liczebniejszym i lepiej wyposażonym przeciwnikiem.

Działania informacyjne prowadzone były w konflikcie na Bałkanach oraz w Afganistanie.

2.2. Wojna w Iraku

Wojna w Iraku w 2003 r. – zdaniem ekspertów – była jedną z najdokładniej relacjonowanych „na żywo" w historii wojskowości. Kluczem do sukcesu były przedsięwzięcia realizowane przez struktury działań informacyjnych, których nie można było obejrzeć w telewizji.

Siły koalicji dysponowały możliwościami technologicznymi społeczeństwa informacyjnego (tzw. „trzeciej fali"), natomiast siły Iraku należy zaliczyć do „drugiej fali". Działania informacyjne prowadzone były głównie przez Stany Zjednoczone i Wielką Brytanię.

Niektóre przedsięwzięcia, dotyczące rozpoznania i wywiadu, działań psychologicznych oraz walki elektronicznej, prowadzone były także przez stronę iracką. Celem działań informacyjnych w Iraku było osłabienie morale wojsk i ludności irackiej oraz uzyskanie przewagi informacyjnej.

W trakcie wcześniejszych przygotowań prowadzono zakłócanie sieci komputerowych Iraku. Wprowadzone wirusy i bomby „logiczne" uaktywnione zostały w momencie ataku sił amerykańskich na Irak.

Przed rozpoczęciem działań zbrojnych zorganizowano 15 centrów koordynacji działań informacyjnych, które były rozmieszczone w USA, Iraku i Kuwejcie. Personel obsługujący ww. centra był zaangażowany w prowadzenie działań informacyjnych.

Według Departamentu Obrony USA w przyszłych konfliktach utrzymanie właściwego morale oraz przewagi informacyjnej stanie się ważniejsze od działań konwencjonalnych i ochrony fizycznej.

Zdaniem ekspertów USA utrzymanie przewagi informacyjnej wymagało spełnienia dwóch warunków. Po pierwsze, należało zbudować własną infrastrukturę informacyjną, a następnie ją chronić. Po drugie, trzeba było zakłócić lub zniszczyć infrastrukturę informacyjną przeciwnika.

Pentagon koordynował wszystkie przedsięwzięcia działań informacyjnych przez Centrum Działań Informacyjnych Połączonych Szefów Sztabów.

Zdaniem gen. Paula Lebrasa, dowódcy Połączonego Centrum Działań Informacyjnych USA, walka elektroniczna, działania psychologiczne, informowanie opinii publicznej, zakłócanie i obrona sieci komputerowych oraz inne przedsięwzięcia działań informacyjnych miały swoje odzwierciedlenie w planach operacyjnych, począwszy od planowania, a kończąc na wykonawstwie zadań.

Centrum wydzieliło grupę ekspertów dla Dowództwa Centralnego (Central Command) w zakresie przygotowania i prowadzenia działań informacyjnych.

Major Nigel Smith (15 Grupa Działań Psychologicznych) stwierdził, że media i struktury działań psychologicznych prowadziły działania informacyjne na poziomie strategicznym.

Zdobywanie informacji z wywiadu i rozpoznania w czasie wojny w Iraku było najistotniejszym elementem działań informacyjnychi pozwoliło koalicji na uzyskanie przewagi informacyjnej nad przeciwnikiem.

W czasie przygotowania i prowadzenia operacji „Iracka Wolność" do zdobywania informacji wykorzystywano m.in.:

— grupy rozpoznania agenturalnego oraz specjalnego;

— satelity rozpoznawcze;

— bezpilotowe aparaty latające;

— autonomiczne systemy wykrywania, śledzenia i lokalizacji celów wojsk lądowych i piechoty morskiej, współpracujące z systemem wczesnego wykrywania i ostrzegania AWACS (E3C, EP3) oraz systemem rozpoznawczo-uderzeniowym JSTARS;

— samoloty rozpoznawcze (RC-135);

— śmigłowce rozpoznawcze (OH-58 Kiowa Warrior).

CIA[34] i oddziały do zadań specjalnych odegrały rolę niezwykle istotną, choć wciąż okrytą tajemnicą. Do ich zadań należało m.in.:

— prowadzenie rozpoznania obiektów o zasadniczym znaczeniu, często strategicznym;

— likwidowanie członków kierownictwa irackiego;

— prowadzanie akcji sabotażowych, podkładanie ładunków wybuchowych;

— naprowadzanie pocisków koalicji na najważniejsze cele.

Na terytorium Iraku zostało wysłanych około 100 agentów z grupy do zadań specjalnych (Special Operations Command – SOG) Centralnej Agencji Wywiadowczej (CIA) USA. Członkowie tej grupy prawdopodobnie rozpoznawali obiekty o znaczeniu strategicznym, organizowali partyzantkę kurdyjską oraz tworzyli sieć kryjówek dla amerykańskich pilotów na wypadek ich zestrzelenia. To właśnie agenci z tej formacji dali sygnał do rozpoczęcia wojny. Dnia 19 marca rozpoznali oni miejsce narady irackich władz, prawdopodobnie z udziałem prezydenta Saddama Husajna. Amerykański prezydent George W. Bush podjął szybką decyzję o zgładzeniu dyktatora i zakończeniu kryzysu jednym uderzeniem „dekapitacyjnym".

---

[34]Centralna Agencja Wywiadowcza (CIA) – jest niezależnym źródłem wywiadu dla rządu amerykańskiego. Rdzeniem CIA jest Dyrekcja Operacyjna, składająca się z kilku tysięcy agentów. Reszta z ok. 20 tys. to pracownicy administracji, zaplecza i analitycy. CIA może angażować się w tajne operacje zgodnie z odpowiednim prawem i za zgodą prezydenta (lub wg doktryny „wiarygodnego zaprzeczenia" – w wypadku wpadki prezydent odcina się od tajnych akcji). Głównym zadaniem CIA jest zbieranie informacji o obcych wywiadach i pozyskiwanie szpiegów.

Z sił specjalnych USA działania prowadzone były przez żołnierzy takich formacji jak: „Delta Force", „Ranger", „Green Berets", „Seals".

Wielka Brytania wysłała do Iraku grupę specjalną z 22 pułku specjalnego (SAS – Special Air Services). Ze strony polskiej w rejon Zatoki Perskiej zostało wysłanych 56 komandosów GROM oraz 12 osób z grupy specjalnej płetwonurków – „Formoza".

Irackie służby wywiadowcze i specjalne zostały zlikwidowane podczas wojny w rejonie Zatoki Perskiej, a następnie odbudowane w 1995 roku. Ich liczebność przed rozpoczęciem operacji „Iracka Wolność" wynosiła ok. 32 000 osób (tab. 2.2.1).

Komitet i Służba Bezpieczeństwa Specjalnego zajmowały się osobistą ochroną dyktatora oraz osób z jego otoczenia.

Wywiad cywilny był najważniejszą agencją wywiadowczą Iraku, składał się z trzech biur (administracyjne, specjalne, polityczne) i podległych im 28 departamentów. Każdy z nich odpowiedzialny był za swoje specyficzne zadania.

Tabela 2.2.1.

Agencje wywiadu i bezpieczeństwa Iraku

Agencja	Liczebność
Komitet Bezpieczeństwa Specjalnego (Special Security Committee)	2 000
Służba Bezpieczeństwa Specjalnego (Special Security Service – Al. Amn al-Khas	5 000
Iracki Wywiad Cywilny (Iraqi Intelligence Service – Mukhabarat al Amma)	4 000
Wywiad Wojskowy (Military Intelligence – Al.-Istikhabarat)	6 000
Jednostka rozpoznania elektronicznego (Al-Haidi Project 858)	800
Wojskowa Służba Bezpieczeństwa (Military Security Service – Al. Amn)	6 000
Służba Bezpieczeństwa Ogólnego (General Security Service – Al. Amma)	8 000
Razem	**31 800**

Wywiad wojskowy (Al-Istikhabarat) posiadał w swojej strukturze:

— służbę administracyjną, odpowiedzialną za rozpoznanie wojskowe;

— służbę polityczną, odpowiedzialną za wywiad zagraniczny;

— służbę specjalną, odpowiedzialną za działania specjalne, w jej skład wchodziły:

- jednostka bezpieczeństwa, odpowiedzialna za bezpieczeństwo sił zbrojnych;
- jednostka 999, odpowiedzialna za działania specjalne na terenie kraju i za granicą (sabotaż, akcje dywersyjne, zwalczanie grup opozycyjnych i innych);

- brygada specjalna, w skład której wchodziły bataliony natychmiastowego reagowania, odpowiedzialne za ochronę Bagdadu.

Kwatera wywiadu wojskowego (Al-Istikhabarat) mieściła się w Bagdadzie, zajmowała około 300 km kwadratowych. Wywiad posiadał regionalne dowództwa w następujących miejscowościach:

— Kirkuk – odpowiedzialne za Kurdów w Iranie i północnym Iraku;

— Mosul – za Turcję i Syrię;

— Basra – kraje Zatoki Perskiej i Iran;

— Bagdad – oddzielone od dowództwa głównego, odpowiedzialne za Jordanię, Syrię, Arabię Saudyjską, Iran.

Dowództwo jednostki specjalnej 999 znajdowało się w bazie sił lądowych Salman Pak, na południowym wchodzie Bagdadu. Jednostka posiada sześć batalionów po ok. 300 żołnierzy:

— 1. batalion odpowiedzialny za rejon Zatoki Perskiej oraz Iran;

— 2. batalion odpowiedzialny za Arabię Saudyjską;

— 3. batalion odpowiedzialny za terytorium Izraela;

— 4. batalion za obszar Turcji;

— 5. batalion za operacje na morzu;

— batalion „Opozycja", był najliczniejszy i odpowiadał za terytorium Iraku.

Jednostka rozpoznania elektronicznego (Al-Hadi Project 858) była odpowiedzialna za zdobywanie, analizę i dystrybucję danych pochodzących z rozpoznania elektronicznego (ELINT). Liczyła 800 osób.

Wojskowa Służba Bezpieczeństwa sprawowała kontrolę nad siłami zbrojnymi Iraku.

Służba Bezpieczeństwa Ogólnego była tajną policją w ramach struktur Ministerstwa Spraw Wewnętrznych. Jej 8 tys. agentów kontrolowało świat kryminalny, media oraz zwalczało wszelkie przejawy działalności politycznej lub gospodarczej uznanej za zbrodniczą.

Irackie służby wywiadowcze i specjalne zostały zniszczone w czasie operacji „Iracka Wolność". Administrator Iraku Paul Bremer postanowił je odtworzyć i przyjąć ponownie do pracy funkcjonariuszy, którzy nie brali udziału w torturach i morderstwach. Głównym trzonem nowych służb mają być oficerowie wywiadu cywilnego i wojskowego.

Na szefa nowej struktury proponowany jest Wafig Samarrai, były szef wywiadu wojskowego za czasów Saddama.

Satelity rozpoznawcze nie są bronią atakującą bezpośrednio, ale nazywane są siłami wsparcia, wykorzystywanymi na potrzeby rozpoznania, śledzenia, nawigacji oraz wczesnego ostrzegania.

Na początku marca sześć wysokiej jakości satelitów fotograficznych prowadziło obserwację Iraku. Były to:

— trzy satelity typu KH-12,

— trzy satelity Lacrosse.

Satelita KH-12 (inaczej zaawansowany technologicznie KH-11) jest wyposażony w kamery optyczne oraz czujniki w zakresie podczerwieni. Ma możliwość obserwacji obszaru wielkości 180 km po lewej i po prawej stronie swojej orbity. Rozdzielczość terenowa satelity wynosi 10–15 cm w dzień – w nocy 60–90 cm.

Satelita Lacrosse jest wyposażony w radar o syntetycznej aperturze (SAR – Synthetic Aperture Radar), co umożliwia mu prowadzenie obserwacji obiektów przykrytych materiałami nieprzenikalnymi dla światła, takimi jak: liście, gleba. Rozdzielczość terenowa satelity wynosi 10 cm w każdych warunkach atmosferycznych.

Zadania w zakresie wielospektralnego rozpoznania fotograficznego realizowane były także przez satelity cywilne, typu LANDSAT, IKONOS. Satelity te fotografują i rejestrują zarówno obrazy czarno-białe o rozdzielczości 1 metra, jak i obrazy wielospektralne o rozdzielczości 4 metrów.

Satelity wsparcia obronnego (DSP - Defense Support Program) wykrywały odpalenie rakiet średniego zasięgu, samoloty lecące z włączonym dopalaczem oraz duże eksplozje. Czujniki tego satelity pracujące w zakresie podczerwieni, mogą wykrywać ciepło pochodzące z pocisków rakietowych, wystrzelonych gdziekolwiek na kuli ziemskiej. Satelity współpracują z Połączonym Taktycznym Systemem Stacji Naziemnych (JTAGS – Joint Tactical Ground Station), który ma możliwość wykrycia celów taktycznych. Stacje naziemne posiadają bezpośrednią łączność z dowódcami oraz systemami broni takimi, jak: AEGIS, Patriot.

Aktualnie system wsparcia obronnego (DSP) jest zastępowany przez system wielospektralny (SBIRS – Space-Based Infrared System), który składa się z wielofunkcyjnych satelitów umieszczonych na różnych orbitach: niskiej, wysokiej, geostacjonarnej.

Bezpilotowe aparaty latające – bal (UAV) zastosowano do prowadzenia rozpoznania, obserwacji i śledzenia zmian położenia sił przeciwnika oraz do atakowania wykrytych celów naziemnych, m.in. wykorzystywane były Predatory, które prowadziły rozpoznanie oraz samodzielnie atakowały wybrane cele za pomocą pocisków Helfire. Predator w wersji Hunter-Killer może przenosić do 14 kierowanych laserem pocisków rakietowych Hellfire lub 6 inteligentnych bomb. W niektórych sytuacjach, gdy Predatory wykryły obiekty wymagające użycia uzbrojenia o większej sile niszczącej, współrzędne wykrytych obiektów przekazywano na pokład bombowców B-1 Lancer lub B-2 Spirit. Następnie współrzędne te wprowadzono do pamięci bomb JDAM, kierowanych z wykorzystaniem systemu GPS.

Ponadto wykorzystywany był Global Hawk, który jest znacznie większy od swego taktycznego odpowiednika – Predatora, ma zasięg strategiczny. Jego prędkość przelotowa wynosi 650 km/h, teoretyczny zasięg 24 700 km, w praktyce przekracza niewiele ponad 20 000 km. Środek ten nie był projektowany na podstawie technologii stealth. Jednak duży pułap (18 500 – 19 500 m) oraz znaczny zasięg aparatury rozpoznawczej (do 200 km) umożliwiły mu bezpieczne operowanie w przestrzeni powietrznej Iraku, ze względu na mały zasięg środków obrony powietrznej. Wyposażony jest w radiolokator, który może przeszukiwać znaczne obszary, a następnie skoncentrować się na śledzeniu celów poruszających się w niewielkim sektorze (wymiary 15 – 20 km, przy pełnym zasięgu 200 km). Global Hawk ma możliwość transmisji obrazu w czasie rzeczywistym za pośrednictwem łącza satelitarnego.

Na poziomie operacyjnym i taktycznym elementy rozpoznania określane są mianem **ISTARS**[35]. Na rzecz wojsk biorących udział w operacji „Iracka Wolność" dostarczane były dane z rozpoznania elektromagnetycznego (SIGINT), czujnikowego oraz z systemu AWACS i JSTARS, z dużego obszaru w czasie niemal rzeczywistym.

Możliwości wykrywania **systemu AWACS** zależą od rodzaju celu oraz jego wysokości i prędkości. Samoloty E-3A są w stanie wykryć następujące cele:

— samoloty myśliwskie lecące na małych wysokościach, z odległości 450 km;

— samoloty myśliwsko-bombowe lecące na średnich i dużych wysokościach, z odległości 650 km,

— pociski rakietowe i śmigłowce, z odległości 240 km;

[35]ISTARS (Intelligence, Surveillance, Target Acquisition and Reconnaissance System) – system wykrywania, rozpoznania, śledzenia i identyfikacji celów.

— kutry rakietowe i torpedowe, z odległości 110 km;

— niszczyciele i krążowniki, z odległości do 400 km.

System rozpoznawczo-uderzeniowy JSTARS zastosowano do śledzenia ruchów wojsk irackich i wskazywania celów ataku. Podczas pracy w funkcji śledzenie dużego obszaru/identyfikacja celów ruchomych (WAS/MTI – Wide Area Surveillance/Moving Target Indicator) system może dozorować obszar o powierzchni 50 000 km^2, identyfikując i śledząc ruch pojazdów na tym obszarze. Praca sektorowa pozwala na dokładne rozpoznanie obszaru o powierzchni od 20 do 50 km^2. Praca z wykorzystaniem radaru o syntetycznej aperturze (SAR) pozwala na uzyskanie szczegółowego, zbliżonego do fotografii obrazu powierzchni ziemi, obiektów i wyznaczonych celów. Obrazy takie pozwalają pilotom samolotów oraz specjalistom wywiadu uzyskać najaktualniejsze informacje o sytuacji w rejonie wybranego celu.

Dzięki systemowi rozpoznawczo-uderzeniowemu (JSTARS) oraz systemowi zdalnego monitorowania pola walki (REMBASS – The Remotely Monitored Battlefield Sensor System) każdy czołg, pojazd czy żołnierz strony irackiej był na bieżąco śledzony. Dane uzyskane z tych systemów pozwoliły siłom koalicji na stałe nadzorowanie działań przeciwnika i podejmowanie odpowiednich reakcji.

Do prowadzenia rozpoznania wykorzytywane były samoloty rozpoznawcze RC-135 Rivet Joint oraz śmigłowce OH-58 Kiowa Warrior.

Na wszystkich samolotach montowany był **system pasywnego rozpoznania radiolokacyjnego AN/APR-39,** który śledził przestrzeń powietrzną wokół samolotu oraz wykrywał naziemne stacje radiolokacyjne.

Do prowadzenia **walki elektronicznej** (Electronic Warfare – EW) Stany Zjednoczone wykorzystywały samoloty typu EF-111E Raven, EC-130H Compass Call, EA-6B Prowler, śmigłowce oraz zestawy zakłócające.

Bez wątpienia najważniejszymi i najlepiej znanymi środkami walki elektronicznej były **urządzenia globalnej lokalizacji GPS**. Zarówno czołgi, ciężarówki, działa, jak i żołnierze byli wyposażeni w odbiorniki GPS. Umożliwiały one dokładną orientację oddziałom lądowym i lotnictwu, zapewniały też niespotykaną wcześniej chirurgiczną wręcz precyzję uderzeń samosterujących pocisków rakietowych i bomb, konieczną nie tylko dla skutecznego eliminowania celów, ale i dla ograniczenia do minimum strat wśród ludności cywilnej.

System zakłócania w zakresie podczerwieni AN/ALQ-144, montowany na śmigłowcach, uniemożliwiał obronie powietrznej Iraku skuteczne zwalczanie celów powietrznych.

Strona iracka prowadziła walkę elektroniczną opierając się na jednostce Al-Haidi Project 858, której kwatera znajdowała się w Al-Raszedia, 20 km na północ od Bagdadu. W tym rejonie znajdowały się także trzy stacje rozpoznania łączności radiowej (COMINT) oraz elektronicznego (ELINT). Pięć innych systemów tego typu było rozmieszczonych na całym obszarze Iraku. Obiekty te zostały zniszczone w czasie operacji „Pustynna Burza", natomiast w 1995 r. zostały odbudowane i znajdowały się w pełnej gotowości operacyjnej.

Urządzenia elektroniczne wspomnianej jednostki mogły zlokalizować nadajniki radiowe wojsk koalicji w ciągu 30 sekund oraz wykorzystywane były do monitorowania łączności wojskowej. Dane z rozpoznania elektronicznego przekazywane były do wywiadu cywilnego Mukhabarat, wywiadu wojskowego Al-Estikhabarat, wojskowej służby bezpieczeństwa oraz do systemów zakłóceń elektromagnetycznych.

Przypuszcza się, że Irak dysponował urządzeniami do zakłócania sygnałów nawigacji satelitarnej GPS. Potwierdzeniem może być wypowiedź generała sił powietrznych USA Victora Renuarta (25.03.2003 r.), który oświadczył, że samoloty amerykańskie zniszczyły sześć irackich urządzeń zakłócających sygnały nawigacji satelitarnej GPS, zakupionych prawdopodobnie od Rosjan. System GPS umożliwiał naprowadzanie bomb JDAM z dokładnością do 12 metrów. Stacje zakłóceń sygnałów nawigacji satelitarnej GPS powodowały, że dokładność wynosiła ok. 30 metrów.

Ponadto przedstawiciele Iraku oświadczyli, że dysponowali technologią, umożliwiającą zakłócanie trasy przelotu pocisków przeciwradiolokacyjnych HARM.

Zdaniem amerykańskich ekspertów Irak dysponował stacjami rozpoznania radiolokacyjnego Kolczuga. Jest to system pasywnego wykrywania i analizy impulsowych i ciągłych sygnałów, pochodzących ze źródeł promieniowania mikrofalowego, emitowanego w zakresie 0,1 – 18 GHz. Umożliwia rozpoznanie praktycznie wszystkich znanych środków radiotechnicznych, pracujących w zakresie metrowym, decymetrowym, centymetrowym i umieszczonych na statkach powietrznych, pojazdach i okrętach. Mogą to być radiolokatory nawigacyjne, wykrywania celów, komponenty systemów kierowania uzbrojeniem, interrogatory IFF, systemy kierowania ruchem powietrznym i zautomatyzowane systemy nawigacyjne. W zakresie analizowanych częstotliwości

mieszczą się kanały łączności lotniczej, satelitarnej, radioliniowej oraz transmisji danych (tzw. datalink).

Ponadto wykorzystywano szereg stacji zakłócania, np. SPN-2, SPN-4, SPN-30. Stacja SPN-2 (lub 4) może zakłócić dwa radary obserwacji bocznej lub sześć radarów naprowadzania uzbrojenia na odległość od 30 do 130 km.

Bezpieczeństwo informacyjne osiągnięto przez zapewnienie ochrony systemów informacyjnych wojsk własnych oraz zmniejszenie efektywności systemów informacyjnych strony przeciwnej. Może ono być osiągnięte przez realizację określonych przedsięwzięć oraz dzięki wykorzystaniu pasywnych lub aktywnych środków elektronicznych. Jego zadaniem jest ograniczenie zdolności prowadzenia rozpoznania przez przeciwnika.

Na potrzeby sił zbrojnych USA zorganizowany został zintegrowany system dowodzenia, kontroli, rozpoznania i walki elektronicznej – C4IEWS (Command, Control, Communications, Computers, Intelligence, Electronic Warfare and Sensors.

Na potrzeby wojsk lądowych zorganizowano globalny system dowodzenia i kontroli (The Global Command and Control System – Army). Do przekazu danych wykorzystywano m.in. satelity systemu DSCS, Milstar oraz GPS.

Uaktualnienie danych oraz ocenę aktualnej sytuacji umożliwiał system analizy danych ze wszystkich źródeł (All Source Analysis System – ASAS).

W celu zwiększenia świadomości sytuacyjnej oraz możliwości dowodzenia, a także synchronizacji wojsk wykorzystywany był zintegrowany system rozpoznawczy (Joint Intelligence and Surveillance – JISR).

Ponadto przy Centralnym Dowództwie powołano centrum oprogramowania (Software Engineering Center), które dla dowódców na niższych szczeblach dowodzenia zapewniało obraz z pola walki.

Zapotrzebowania na bezpośrednie wsparcie ogniowe realizowano na podstawie systemu – AFATIDS (The Advanced Field Artillery Tactical Integration Data System).

Zabezpieczenie logistyczne realizowano wykorzystując mobilne systemy (Sybase and Anywhere Wireless Server). Aż 64 jednostki logistyczne zostały wyposażone w te systemy, które umożliwiały zbieranie danych o pozycjach jednostek bojowych, ponadto pozwalały na realizację zaopatrzenia z baz w Kuwejcie na pole walki.

Jednostki wojskowe na froncie łączyły się bezprzewodowo z systemem monitorowania zasobów w Arlington w Virginii. Dane były wysyłane do systemu – TC-AIMS II (Transportation Coordinator's Automated Information for Movements Systems

II) poprzez bezprzewodową sieć amerykańskiego departamentu obrony, obsługiwaną przez satelitę Iridium. Dane przedstawiane były za pośrednictwem interfejsu graficznego, jednocześnie na polu walki i w Pentagonie. W ten sposób dowództwa posiadały aktualne dane na temat rozmieszczenia ludzi i sprzętu.

Wymianę danych cyfrowych umożliwiały osobiste komputery kieszonkowe PFED (Pocket-sized Forward Entry Device), produkowane w kooperacji przez firmy General Dynamics (kilkadziesiąt lat temu zaprojektowała samolot F-16) i Talla-Tech.

Płk Dobbins, dowódca 392. Grupy Ekspedycyjnej SP USA, stwierdził, że powyższe systemy zapewniły właściwy obraz sytuacji na polu walki wszystkim uczestnikom. Zbudowano sieć łączącą główne stanowiska dowodzenia oraz zapasowe stanowiska dowodzenia z wojskami biorącymi udział w operacji, które były wyposażone w 100 000 przenośnych odbiorników GPS (jeden odbiornik na dziewięciu żołnierzy wojsk lądowych lub pięciu żołnierzy piechoty).

Korpuśne i dywizyjne stanowiska dowodzenia przekazywały obraz z sytuacji pola walki dla żołnierzy wszystkich jednostek. 3000 dowódców od szczebla korpusu do szczebla drużyny miało mapy taktyczne, co umożliwiało ocenę sytuacji, określenie swojej pozycji oraz zagrożeń.

Na poziomie operacyjnym dowódcom przekazywany był ogólny obraz operacyjny (COP – Common Operating Picture), natomiast na niższych szczeblach dowodzenia sytuacyjny obraz operacyjny (CROP – Common Relevant Operating Picture). Na ich podstawie na wszystkich szczeblach podejmowano właściwe decyzje dzięki wiarygodnym i terminowym danym.

Korpus piechoty morskiej został wyposażony w szerokopasmowy system łączności troposferycznej (AN/TRC-170 Troposcatter Communications System), który umożliwiał niezawodną łączność w rejonie działań.

Radiostacje AN/PRC-112D zapewniały ratownictwo dla załóg samolotów oraz sił specjalnych.

Żołnierze amerykańscy mieli dostęp do internetu przez otwartą sieć zwaną nippernet (ang. Nonsecure Internet Protocol Network) oraz zabezpieczoną sieć (Army Knowledge Online), wykorzystywaną np. do kontaktów z rodzinami.

Na szeroką skalę wykorzystywane były telefony komórkowe. Gdy Amerykanie zniszczyli iracką infrastrukturę telekomunikacyjną, Saddam Husajn porozumiewał się ze swoimi generałami tylko za ich pomocą.

Stany Zjednoczone przed rozpoczęciem operacji „Iracka Wolność" zabezpieczyły się przed atakami na sieci komputerowe. Do ich monitorowania wykorzystano Globalny System Wczesnego Ostrzegania – GEWIS (Global Early Warning Information System). Na bieżąco z różnych sieci były wysyłane dane do centrum, co umożliwiało śledzenie stanu internetu na jednej wielkiej tablicy i lokalizację cyberataku (wirusa) w zarodku..

W Pentagonie od 1999 r. istnieje specjalna jednostka – JTFCNO (Joint Task Force on Computer Network Operations), zajmująca się atakami na sieci komputerowe.

Ponadto ochronę danych realizowano przez metodę ukrywania danych w grafice – SSIS (Spread Spectrum Image Steganography). Zdaniem ekspertów metoda ta jest znacznie lepsza od dotychczas stosowanych, nie narusza statystycznych własności obrazu oraz jest odporna na błędy.

W czasie wojny w Iraku około 1500 systemów zobrazowania termalnego zabezpieczało pojazdy korpusu piechoty morskiej, a ponad 140 – wojska lądowe. Urządzenia tego systemu zapewniały bezpieczny ruch pojazdów w różnych warunkach atmosferycznych oraz o każdej porze, zarówno w dzień, jak i w nocy.

Iracki system dowodzenia został sparaliżowany, m.in. przez **zakłócanie systemów komputerowych**, które było realizowane z wykorzystaniem różnorodnych „programów złośliwych", które powodują wymazanie w krótkim czasie dużej liczby zbiorów danych, spowalniające pracę programów użytkowych. Programem złośliwym nazywa się kod wyrządzający szkody. Niektórzy również posługują się określeniem „malware" (zlepek z ang. malicious software – oprogramowanie złośliwe)[36]. Do programów tych należy zliczyć: wirusy, konie trojańskie, bomby „logiczne", robaki komputerowe, bakterie i króliki oraz wiele im podobnych.

Inną niekonwencjonalną akcją było wysyłanie tysięcy wiadomości pocztą elektroniczną do polityków, przywódców, starszych stopniem irackich dowódców wojskowych.

Informowano ich o braku szans na wygranie wojny z USA oraz namawiano do opuszczenia prezydenta Husajna i przejścia na stronę nowego irackiego rządu formowanego pod opieką Amerykanów. Tego typu akcję (z wykorzystaniem internetu) podjęto po raz pierwszy.

[36]S. Garfinkel, G. Spafford, *Bezpieczeństwo w Unixie i Internecie*, Warszawa, 1997, s. 31.

W wojnie w Iraku obydwie strony stosowały **dezinformację**. Telewizja, radio oraz prasa przemawiały jednym głosem, wzmacniając wzajemnie przekazywane wiadomości. Sytuacja ta powodowała, że trudno było odróżnić kłamstwo od prawdy.

Nieprawdziwe były amerykańskie informacje na temat posiadania przez Irak broni masowego rażenia oraz laboratoriów chemicznych w ruchomych ciężarówkach.

Kolejną manipulacją było sugerowanie opinii publicznej związku pomiędzy Husajnem i Al-Kaidą oraz oskarżanie Saddama o zakup uranu w Nigerii.

Innym przykładem mogą być wiadomości na temat irackiego portu Umm-Kasr, gdy przed południem podano, że został zdobyty przez amerykańską piechotę morską, a po kilku godzinach okazało się, że szturmowane od pół doby miasto zostało zajęte tylko w części, wreszcie późnym wieczorem Donald Rumsfeld, amerykański sekretarz obrony poinformował, że port został całkowicie wyzwolony.

Saddam Husajn do dezinformacji opinii amerykańskiej wykorzystał jeńca (pilota) Michaela S. Speichera. Amerykanie uznali go za zaginionego w czasie wojny w Zatce Perskiej w 1991 r. Irak nie wydał Speichera w toku wymiany jeńców i oświadczył, że nic nie wie o jego losie. Przed rozpoczęciem wojny w Iraku dotarła do USA wiadomość, że Speicher żyje i może się stać – w zależności od rozwoju sytuacji – albo kartą przetargową, albo żywą tarczą. Była to spektakularna „wpadka" wielu służb amerykańskich. Mechanizm sugestywnej pogłoski o sporej skali prawdopodobieństwa stanowił narzędzie wspólne dla dezinformacji komercyjnej i wojskowej. Saddam Husajn osiągnął swój cel i przyprawił o konsternację amerykańską opinię publiczną, niezwykle wyczuloną na martyrologię jeniecką i straty wśród swoich, choćby pojedynczych żołnierzy.

Obydwie strony na bieżąco przekazywały sprzeczne wiadomości:

— w Basrze wybuchło powstanie (to według rzecznika wojsk angielskich), które premier Blair zmienił od razu na „rewoltę o ograniczonym zasięgu", potem na „manifestację";
— w wiosce irackiej odkryto maski i płaszcze przeciwgazowe. Komentator amerykański zrelacjonował, że jest to dowód, iż Irak szykował światu chemiczną zagładę;
— iracka 51. Dywizja Zmechanizowana poddała się rankiem (według amerykańskich mediów), a faktycznie Amerykanie do wieczora toczyli z nią ciężkie walki;
— po ciężkich walkach rozbito dywizję Gwardii Republikańskiej, a gdy zaczęto liczyć zabitych, to było ich tylko osiemnastu.

Wypowiedzi irackiego ministra informacji były jeszcze zabawniejsze – „Amerykanie są daleko od Bagdadu" (w chwili, gdy wkraczali na jego przedmieścia).

Dezinformację na rzecz Iraku prowadził nowozelandzki dziennikarz Peter Arnett. Został on wyrzucony z pracy przez NBC i National Geographic za wywiad udzielony irackiej telewizji, w którym wysławiał hart ducha żołnierzy Saddama i przepowiadał klęskę Ameryce. Wywiad wywołał niezadowolenie służb prasowych Pentagonu w Waszyngtonie. W 1991 roku Arnett był już oskarżony o dezinformację na rzecz Iraku za reportaż na temat bombardowania fabryki mleka w proszku dla niemowląt, którą wojskowi amerykańscy uważali za fabrykę produkującą broń bakteriologiczną.

Specjalista ds. mediów na Uniwersytecie Londyńskim, Tim Crook, stwierdził, że oprócz stosowania typowej dezinformacji popełniono także wiele skandalicznych błędów, które przyczyniały się do niezamierzonej dezinformacji opinii publicznej. Zaliczyć do nich można: niesprawdzone wiadomości o powstaniu w Basrze, oświadczenie premiera o egzekucjach brytyjskich jeńców, niepotwierdzone doniesienia o odkryciu skażeń chemicznych w Eufracie.

Działania psychologiczne prowadzone były przez obydwie walczące strony. Celem działań psychologicznych prowadzonych przez Amerykanów i Brytyjczyków było obniżenie morale wojsk irackich i ludności cywilnej. Polegały one m.in. na zachęceniu Irakijczyków do porzucania walki, kolaboracji z atakującymi i poddania się.

Według koncepcji amerykańskiej pododdziały działań psychologicznych stanowią część składową wojsk specjalnego przeznaczenia. Ogólną strategię, treści i formy działań psychologicznych sił zbrojnych Stanów Zjednoczonych określa Federalna Rada Bezpieczeństwa Narodowego, a zatwierdza prezydent.

W pionie operacyjnym szef oddziału operacyjnego (J-3) Komitetu Połączonych Szefów Sztabów koordynuje prowadzenie tych działań na poziomie połączonych dowództw oraz na rzecz związków operacyjnych i taktycznych. Każdy rodzaj sił zbrojnych ma swoje siły i środki działań psychologicznych. Jednak główny potencjał ześrodkowany jest w wojskach lądowych. Dysponują one regularnymi formacjami wchodzącymi w skład Dowództwa Działań Specjalnych Sił Lądowych USA.

Nowym elementem tej struktury jest Dowództwo Działań Psychologicznych i Spraw Cywilnych Stanów Zjednoczonych Ameryki, które zostało utworzone 27 listopada 1990 r. (The United States Army Civil Affairs and Psychological Operations Command – USACAPOC).

Dowództwo jest odpowiedzialne za nadzorowanie działań specjalnych, prowadzonych przez siły specjalne, w tym także jednostki działań psychologicznych. Jego działalność obejmuje czas pokoju, kryzysu, konfliktu lub wojny, a specyfika działania polega na wykorzystaniu aspektów tzw. mnożników siły, m.in. środków niekonwencjonalnych. Do jego zadań należy wpływanie na psychikę dowódców i wojsk, czyli wykorzystując czynniki mentalne przez perswazję, indoktrynację, propagandę, promowanie odpowiednich postaw i zachowań.

Głównym zadaniem tego dowództwa jest stworzenie sprzyjającej atmosfery do wykonywania zadań przez wojska własne, zaprzyjaźnione i neutralne oraz przeszkadzanie przeciwnikowi w jego działaniach psychologicznych.

W czasie przygotowania i prowadzenia operacji „Iracka Wolność" działalność prowadził personel 10. Batalionu Działań Psychologicznych. Jego zadaniem było demoralizowanie wojsk irackich, szczególnie Gwardii Republikańskiej oraz uzyskanie zaufania ludności cywilnej. Batalion jest jednostką rezerwową, stacjonuje w St. Louis (Missouri), podlega 7. Grupie Działań Psychologicznych w Moffett Field (Kalifornia). Strukturę batalionu stanowiły trzy kompanie (307, 308 318).

Regularną jednostką, biorącą udział w wojnie w Iraku, był 9. Batalion Działań Psychologicznych, który jest elementem 4. Grupy Działań Psychologicznych. Personel batalionu prowadził działania w bezpośrednim kontakcie z przeciwnikiem.

Udział w wojnie brała także 346. Kompania Działań Psychologicznych, stacjonująca w Columbus (Ohio).

Ze strony brytyjskiej stwierdzono udział personelu z 15. Grupy Działań Psychologicznych.

Ogółem na terenie Iraku znajdowało się około 1000 osób personelu działań psychologicznych[37].

Strategiczne działania psychologiczne prowadzone były w oparciu o telewizję i Internet. Obydwie strony (Amerykanie, Irak) rozpoczęły ich prowadzenie już w październiku 2002 r. W oddziaływaniu strony amerykańskiej motywem przewodnim była kwestia posiadania przez Irak broni biologicznej i chemicznej, a Stany Zjednoczone miały być jedyną siłą zdolną obronić tzw. wolny świat przed grożącym niebezpieczeństwem. Duży nacisk władze USA położyły na konieczność zaprowadzenia w Iraku demokracji. W oficjalnych przekazach unikano jakichkolwiek skojarzeń,

[37]Na podstawie wypowiedzi ppłk. Glenna Ayersa, dowódcy 9. Batalionu Działań Psychologicznych, stacjonującego w Fort Bragg (Północna Karolina).

pozwalających wysnuć przypuszczenie, że wojną z Irakiem jest zainteresowane amerykańskie lobby naftowe. Było to jednym z ważniejszych motywów propagandy amerykańskiej.

Ważnym zadaniem tego oddziaływania była poprawa wizerunku USA w oczach świata. W tym celu powołano specjalną, działającą przy prezydencie, komisję, w skład której weszli m.in. specjaliści od wojskowych działań psychologicznych oraz eksperci do spraw kreowania wizerunku i public relations, także z Hollywood. W ocenie zagranicznych specjalistów od spraw mediów większość amerykańskich środków masowego przekazu współpracowała z władzami państwowymi i armią. Przykładem jest telewizja Fox News, która jest powiązana z obecnymi elitami USA.

Strona iracka w adresowanej głównie do państw arabskich propagandzie starała się nadać konfliktowi charakter wojny religijnej – między chrześcijanami a światem islamu, kreując jednocześnie Saddama Husajna na jedynego obrońcę wiary.

Szczególną rolę w prowadzonych przez Irakijczyków działaniach psychologicznych odgrywała telewizja. Za jej pośrednictwem na początku wojny iracki prezydent Saddam Husajn oznajmił, że irackie wojsko nie ulegnie pod presją amerykańską i nie podda się dobrowolnie przeciwnikowi. „Lud iracki i jego siły wojskowe są przygotowane do odparcia każdego ataku, mimo że propaganda amerykańsko-brytyjska stara się złamać ich morale".

Za jej pośrednictwem zostały wyemitowane m.in. obrazy zniszczeń obiektów cywilnych powstałych w wyniku amerykańskich ataków rakietowych i lotniczych. Dlatego też priorytetowym celem dla koalicyjnych uderzeń stały się systemy nadawcze irackiej telewizji państwowej. Siedzibę irackiej TV udało się zniszczyć koalicji dopiero pod koniec marca. Nadal jednak irackie programy telewizyjne były nadawane przez satelitę. W propagandzie prowadzonej za pośrednictwem środków masowego przekazu reżim iracki bardzo często odwoływał się do gróźb. Irakijczycy grozili przeprowadzeniem zamachów terrorystycznych przeciwko państwom koalicji. Ostrzegali również, że wszystkie obce wojska, które wkroczą na terytorium Iraku, spotka śmierć ze strony gotowych na wszystko ochotników ze wszystkich państw islamskich oraz irackich sił specjalnych, tzw. fedainów Husajna.

Ważną postacią w irackich działaniach psychologicznych był minister informacji w rządzie Saddama Husajna Mohammed Said-al-Sahaf. Jego utrzymane w nieco przesadnym i kwiecistym stylu wypowiedzi mogły się wydawać dla odbiorców z kręgu kultury europejskiej nieco dziwaczne. Między innymi dlatego też w propagandzie koalicji

nadano mu deprecjonujące przezwisko „komiczny Ali". Inaczej jednak jego wystąpienia były odbierane przez Arabów. Wśród znacznej ich części cieszyły się one nawet sporym uznaniem. W kulturze arabskiej tego typu kwiecista retoryka jest bowiem czymś powszechnie przyjętym i stosowanym.

Dużą rolę w prowadzeniu działań psychologicznych odegrał internet. Jednym z nowatorskich środków oddziaływania psychologicznego wykorzystywanych przez koalicję było wysyłanie wiadomości pocztą elektroniczną, bezpośrednio do decydentów w rządzie irackim. Na początku 2003 r. w Iraku istniało jedynie 60 kawiarenek internetowych, a opłata w wysokości 25 USD za założenie jednego łącza domowego przekraczała możliwości większości Irakijczyków. Reżim iracki bardzo ostrożnie udostępniał Internet w skali całego kraju. Tak więc, o ile zwykli Irakijczycy nie mieli dostępu do sieci, miała go większość przywódców partii Baas. Koalicja wykorzystała to medium przede wszystkim po to, żeby przedstawić każdemu z nich koszty dalszego wspierania Saddama, zarówno dla wszystkich Irakijczyków, jak i dla nich samych.

Zdaniem ppłk. S. Collinsa[38] działania psychologiczne prowadzone przez Amerykanów były najskuteczniejsze na **poziomie operacyjnym i taktycznym**.

Do ich prowadzenia wykorzystywano rozgłośnie radiowe, zrzucano ulotki oraz nadawano audycje i komunikaty przez rozgłośnie elektroakustyczne – REA.

Amerykanie zrzucali ulotki przez samoloty różnych typów w specjalnych zasobnikach wykonanych z tworzywa sztucznego. W czasie przygotowania operacji „Iracka Wolność" siły sprzymierzone zrzuciły 40 milionów ulotek, a drugie tyle w czasie jej trwania. Ulotki opracowane były przez specjalne zespoły analityków, uwzględniały lokalną kulturę i język. Najskuteczniejszą metodą złamania morale jest sprawienie, by żołnierze zaczęli myśleć o sobie nie jak o części armii, ale jak o pojedynczych osobach. W tym celu wiele komunikatów na ulotkach odwoływało się do rodziny, przyjaciół: „To mógłby być twój brat. To mógłbyś być ty". Również ulotki adresowane do ludności cywilnej odwoływały się do rodziny: „Bogactwo Iraku, dobrobyt twój i twojej rodziny zależy od ropy. Jeżeli szyby naftowe zostaną zniszczone, będziecie zrujnowani. Nie pozwól na zniszczenie szybów naftowych".

Wszystkie ulotki oprócz tekstu po arabsku zawierały schematyczne, ale czytelne ilustracje. Co charakterystyczne, nie pokazywano na nich ofiar, ale dużo zniszczonego

[38]Ppłk Steven Collins jest odpowiedzialny za operacje psychologiczne (PSYOPS) w Kwaterze Głównej PSZ NATO w Europie (SHAPE) w Mons.

sprzętu wojskowego. Chodziło o to, by pokazać, że celem ataku jest sprzęt, a nie ludzie. Ulotki były również przystosowywane do aktualnych wiadomości z pola walki.

Poza akcją rozrzucania ulotek, innym środkiem oddziaływania, stosowanym w operacjach psychologicznych, intensywnie wykorzystywanym przez koalicję, było radio.

Nadając ze stałych wież transmisyjnych, a także z samolotów EC-130E Comando Solo, koalicja prowadziła podobny typ audycji jak Radio Sawa, z dużą dawką popularnej muzyki, przeplatanej wiadomościami i nielicznymi komunikatami.

Stacja obejmująca cały Irak nosiła nazwę Information Radio i rozpoczęła nadawanie audycji 18 grudnia 2002 r. na częstotliwościach: 9715 kHz i 11292 kHz. Programy nadawane były w języku arabskim, wykorzystywane były popularne piosenki irackie i libańskie oraz utwory zachodnie, jak np. utwór z filmu Titanic, „My Heart Will Go On" wykonywany przez Celine Dion. W nocy 20 marca w irackim radiu publicznym (całkowicie kontrolowanym przez reżim Husajna) spiker mówiący po arabsku oznajmił: „To dzień, na który czekaliśmy. Atak na Irak rozpoczął się". Komunikat pochodził z samolotu Comando Solo, który oprócz nadawania audycji radiowych mógł zakłócić programy oficjalnych stacji.

Lokalne stacje radiowe były także tworzone poza głównymi skupiskami ludności. Jedną z nich była radiostacja brytyjskiej 15. Grupy Działań Psychologicznych o nazwie Radio Nahrain – radio działało na przedmieściach Basry. Poza tworzeniem własnych przekaźników radiowych koalicja próbowała elektronicznie zagłuszać radiostacje irackie, aby uzyskać monopol na wiadomości udostępniane Irakijczykom za pośrednictwem tego medium.

Bardzo skuteczne były taktyczne zespoły działań psychologicznych (wyposażone w rozgłośnię elektroakustyczną – REA), które wspierały jednostki wojsk lądowych i piechoty morskiej. Przypisuje się im zasługi w przekonywaniu jednostek irackich do złożenia broni, a także w utrzymywaniu kontroli nad więźniami irackimi. Ponadto prowadziły one symulację efektów akustycznych pola walki, nadając przez głośniki odgłosy czołgów i helikopterów.

Podczas wojny w Iraku stosowano zarówno białą, szarą, jak i czarną propagandę. W wypadku białej, źródło przekazu było znane. W ramach szarej propagandy wydawany był tygodnik o nakładzie 70 000 w Bagdadzie. W ramach czarnej propagandy działało Radio Tikrit. Początkowo stacja ta budowała swoją wiarygodność, utrzymując, że kierują nią lojalni Irakijczycy w regionie Tikrit. Linia programowa stacji popierała Saddama

Husajna. Jednak w ciągu kilku tygodni ton ten się zmieniał, a stacja stawała się coraz bardziej krytyczna wobec Saddama. Podstawą czarnej propagandy jest wiara, że odbiorcy nie rozpoznają mistyfikacji i będą przekonani, iż wiadomości pochodzą z źródła, które w ich oczach jest wiarygodne.

Na sukces koalicji znaczny wpływ miało niskie morale żołnierzy irackich, którzy bardziej bali się swoich dowódców niż wojsk koalicji, ponieważ dowódca rozstrzeliwał, a przeciwnik brał do niewoli. Sam przywódca Iraku Saddam Husajn bał się swoich współpracowników, którym nie wierzył, gdyż zawsze go okłamywali.

Informowanie opinii publicznej polegało na przekazywaniu wiadomości bezpośrednio z pola walki. Wojna iracka toczyła się nie tylko na pustyni, ale przede wszystkim w mediach. Zwiększająca się liczba serwisów informacyjnych, oferowanych przez telewizje satelitarne, oraz rosnąca sieć połączeń internetowych jak nigdy dotąd utrudniała globalne wpływanie na opinie i stanowiska. Eksplozja liczby dostawców wiadomości umożliwiała odbiorcom oglądanie wiadomości, które wzmacniały ich własne uprzedzenia i zdecydowane opinie.

Ludność arabska miała możliwość weryfikacji wiadomości przekazywanych przez CNN i BBC z wiadomościami przekazywanymi przez katarską telewizję satelitarną Al-Dżazira.

Al-Dżazira starała się naśladować najlepsze zachodnie kanały informacyjne. Miała specjalnie zaprojektowane studio wojenne, prowadzący zachowywali się tak samo jak prezenterzy CNN czy BBC, na żywo łączyli się z korespondentami, relacjonowali wszystkie najważniejsze konferencje prasowe (irackie i koalicji). Emerytowani generałowie z państw arabskich na bieżąco komentowali doniesienia z frontu.

Iracka Agencja Informacyjna zdała sobie sprawę z potęgi Al-Dżaziry i posunęła się do tego, aby infiltrować tę organizację przy pomocy swoich agentów, aby programy stały się bardziej proirackie. Z kolei koalicja antyiracka starała się uniemożliwić nadawanie programów informacyjnych telewizji irackiej. W tym celu zarówno bombardowała, jak i w elektroniczny sposób zagłuszała stację, w równym – jeśli nie większym – stopniu ze względu na jej oddziaływanie poza Irakiem, jak i w obrębie kraju.

W czasie operacji „Iracka Wolność" o irackich słuchaczy walczyło ponad dwadzieścia stacji radiowych: kurdyjskie, szyickie i finansowane przez Zachód.

Amerykanie docierali do Irakijczyków na falach Radia Wolny Irak i Radia Sawa. Program Radia Wolny Irak kierowany był głównie do lokalnych elit, obejmował nadawanie wiadomości oraz analizy polityczne. Do arabskich mas docierało Radio Sawa

(Razem), kontrolowane bezpośrednio przez amerykański rząd. Program składał się głównie z zachodniej i arabskiej muzyki pop oraz serwisów informacyjnych. Słuchali ich nie tylko Irakijczycy, ale i mieszkańcy innych krajów arabskich.

Proirackie radio Głos Mudżahedinów otwarcie podburzało do rebelii przeciwko Amerykanom. Programy tego radia docierały głównie do irackich szyitów.

Na wojnę z Irakiem – obok żołnierzy – zostali wysłani dziennikarze, którzy wykorzystywali cały dostępny arsenał środków technicznych (wideotelefony, telefony satelitarne, kamery noktowizyjne) w ramach nowej formuły współpracy mediów z armią. Wymyślił ją sekretarz obrony USA Donald Rumsfeld. Przewidywała ona wcielenie ekip reporterskich do oddziałów frontowych. Jeszcze przed ich wyruszeniem do Iraku sześciuset dziennikarzy przeszło przeszkolenie wojskowe, zostali umundurowani i wyposażeni w środki zabezpieczające na polu walki: kamizelki kuloodporne, hełmy i odzież, mającą chronić ich w wypadku zastosowania broni chemicznej.

Początkowo pomysł ten oceniano jako kontrowersyjny, z obecnej perspektywy wydaje się on z kilku powodów dobrym rozwiązaniem. Po pierwsze, reporterzy, którzy deklarowali chęć działania w oddziałach, byli zmuszeni do przejścia skróconego szkolenia dla rekrutów, co pozwalało im po raz pierwszy docenić wyzwania stojące przed zwykłymi żołnierzami. Po drugie, działanie wśród żołnierzy w nieuchronny sposób prowadziło do wytworzenia się więzi pomiędzy reporterami a jednostkami, których działania mieli relacjonować. Po trzecie, taka sytuacja zapewniała reporterom bezpieczeństwo i pozwalała opinii publicznej śledzić wojnę na bieżąco.

Współpraca cywilno-wojskowa – CIMIC to całokształt współdziałania dowódców wojskowych z instytucjami cywilnymi, takimi jak: władze lokalne, organizacje rządowe i pozarządowe, społeczność lokalna czy wreszcie organizacje międzynarodowe i humanitarne.

W strukturach sił lądowych USA występują dowództwa i jednostki spraw cywilnych, które podlegają Dowództwu Działań Psychologicznych i Spraw Cywilnych Stanów Zjednoczonych (U. S. Army Civil Affairs and Psychological Operations Command (USACAPOC). Dowództwo to podlega Dowództwu Działań Specjalnych (USASOC).

Jednostką spraw cywilnych – CA (Civil Affairs), działającą już w czasie pokoju, jest 96. Batalion Spraw Cywilnych. Ponadto występują jednostki rezerwowe takie, jak: 351., 352., 353. Dowództwo Spraw Cywilnych oraz brygady i bataliony. Każda jednostka posiada specjalne zespoły ds. ochrony ludności, dowódców taktycznych i operacyjnych przed oddziaływaniem organizacji feministycznych, pomaganiu dowódcom w dotarciu do

ludności cywilnej, łączności z agencjami rządowymi, tolerancji wartości kulturalnych oraz tradycji danego narodu, odbudowie własnych wartości (prawo, ekonomia), zwalczanie feminizmu, strachu przed śmiercią i chorobą, utrwalanie poczucia niewinności, ochrona praw człowieka, zapewnienie kontynuacji edukacji dzieci i młodzieży.

Personel spraw cywilnych wspiera zadania wojsk oraz jest ogniwem łączącym siły zbrojne z organizacjami nierządowymi (Non-Governmental Organizations – NGOs) oraz prywatnymi organizacjami ochotniczymi (Private Volunteer Organizations – PVOs).

W czasie wojny w Iraku stwierdzono udział następujących dowództw i jednostek spraw cywilnych:

— 352 dowództwa CA;

— 354 brygady CA;

— 96, 422 i 432 batalionu CA.

Generał John Kern był dowódcą 352. Dowództwa Spraw Cywilnych (miejsce dyslokacji – Riverdale (Merylamd). Posiadał oficerów łącznikowych i tłumaczy, którzy ułatwiali kontakt z ludnością lokalną, przede wszystkim z miejscowymi przywódcami.

Pułkownik David Blackledge, dowódca 354. Brygady Spraw Cywilnych (Maryland), zajmował się m.in. pomocą humanitarną w rejonie Umm-Kasr (dostarczanie wody, żywności i paliwa dla miejscowej ludności) oraz odbudową infrastruktury Iraku.

96. Batalion Spraw Cywilnych (pododdział czasu „P" i „W") współpracował z ludnością iracką, udzielał pomocy przy naprawianiu mostów, wodociągów, dróg oraz w dostawie żywności i lekarstw. W czasie pokoju batalion liczy 200 osób i składa się z pięciu kompanii i grupy dowodzenia. W czasie wojny w Iraku batalion został wzmocniony 2000 żołnierzy rezerwy. W skład jednostki wchodzili specjaliści, m.in.: doktorzy medycyny, dentyści, weterynarze, elektrycy, hydraulicy, lingwiści oraz osoby przygotowane do pełnienia funkcji burmistrza miasta.

Grupa Szybkiego Reagowania z 422 Batalionu Spraw Cywilnych odkryła kryjówkę rosyjskich pocisków rakietowych „ziemia – powietrze" w Bagdadzie. Specjalista tej jednostki, dr medycyny Ashley Beaty zajmowała się badaniem kobiet i dzieci irackich.

Dowódca 432. Batalionu Spraw Cywilnych major Dan Chachakis wysoko ocenił perfekcję działania swoich 150 członków, którzy przez jeden miesiąc, w Fort Bragg (Północna Karolina), przygotowywali się do wzięcia udziału w operacji „Iracka Wolność". Ponadto jednostka zdobyła już doświadczenie w misjach w Kosowie i Bośni oraz w Zatoce Perskiej w 1991 r.

2.3. Efekty poznania

1. Rozwój cywilizacyjny oraz postęp naukowo-techniczny powoduje, że zmieniają się formy i środki prowadzenia zarówno operacji militarnych, jak i niemilitarnych. Oprócz znacznego rozwoju środków walki elektronicznej (mikroprocesory, generatory impulsu elektromagnetycznego, bomby „logiczne", wirusy komputerowe) oraz mass mediów (Internet, telewizja, radio, prasa) pojawiły się nowe możliwości oddziaływania, jak chociażby broń wiązkowa (energii kierowanej), światła stroboskopowe wywołujące nudności czy infradźwięki powodujące depresje, napięcia, strach, sztuczną wesołość, spowolnienie reakcji, dolegliwości sercowe i zaburzenia równowagi. Ponadto mogą być wykorzystane różne techniki psychotroniczne, prowokujące subiektywne i obiektywne zachowania ludzi ulegających wpływowi sugestii lub autosugestii. Na współczesnym polu walki, w warunkach podobnego potencjału militarnego, zbliżonego wyposażenia i uzbrojenia przeciwstawnych stron, właśnie człowiek staje się czynnikiem decydującym o sukcesie lub porażce.

2. Sytuacja ta powoduje, że współczesne konflikty zbrojne zmieniają swój charakter, przesuwając środek ciężkości na oddziaływanie informacyjne, które prowadzone w umiejętny sposób może wpływać na powodzenie operacji zarówno militarnych, jak i niemilitarnych lub prowadzić wprost do „wygaszenia" konfliktu.

3. W wieku informacji zapotrzebowanie na użyteczną informację staje się jednym z podstawowych zadań działalności w sferze cywilnej i militarnej. Aktualnie informacja jest traktowana jak zasób strategiczny. Takie znaczenie informacji przypisuje się m.in. ze względu na szybki rozwój technologii informacyjnych, które w znaczny sposób przyśpieszają proces komunikowania się i zdobywania wiedzy. Wzrastające znaczenie informacji, szczególnie przewagi informacyjnej, jest jednym z podstawowych czynników działalności i kompetencji w globalnym środowisku informacyjnym. Stajemy się społeczeństwem „trzeciej fali", tzw. wojownikami wiedzy, co w znaczny sposób zwiększa moc bojową wojsk. Rewolucja informacyjna wskazuje, że informacja i technologie informacyjne powinny zostać włączone w działalność militarną, szczególnie w proces decyzyjny, oraz stać się narzędziami walki, aby osiągnąć cele polityczne i wojskowe. Stąd wynika konieczność zajęcia się problematyką działań informacyjnych.

4. W czasie wojny w rejonie Zatoki Perskiej Stany Zjednoczone ujawniły nową kategorię działań, którą formalnie nazwano działaniami informacyjnymi. Jak stwierdził A. de Campen „Wiedza stała się rywalką broni i taktyki". Wojna w rejonie Zatoki Perskiej

prowadzona była w okresie przechodzenia ze społeczeństwa „drugiej fali" w społeczeństwo „trzeciej fali". W sposób szczególny wykazała znaczenie technologii informacyjnych, które w znaczny sposób przyczyniły się do zmian w zakresie prowadzenia walki zbrojnej.

5. Wojna w Iraku (2003 r.) – zdaniem generała Richarda Myersa, przewodniczącego Połączonych Szefów Sztabów – to nowy, amerykański sposób prowadzenia działań zbrojnych (nowy standard), polegający na połączeniu kompleksu przedsięwzięć działań informacyjnychz możliwościami systemu dowodzenia, rozpoznania i walki elektronicznej (C4IEWS) na poziomie strategicznym. Umożliwiło to siłom koalicji śledzenie bieżącej sytuacji operacyjnej i taktycznej, dzięki temu uzyskały one inicjatywę i mogły realizować swoje plany.

6. Prowadzenie działań informacyjnych ma związek z implementacją koncepcji opartej na nowych technologiach, co nazwano mianem rewolucji w sprawach wojskowych (Revolution in Military Affairs – RMA). Pionier rewolucji w sprawach wojskowych, pułkownik Ryszard Szafrański, stwierdził, że działania informacyjne bazują na teorii poznania przeciwnika. Bazą teoretyczną tej koncepcji jest przygotowanie i prowadzenie działań informacyjnych, które przyczyniają się do uzyskania przewagi informacyjnej, dzięki której wzrost siły bojowej jest generowany poprzez połączenie w system informacyjny sensorów, decydentów i systemów walki w celu osiągnięcia wspólnej świadomości sytuacyjnej, zwiększenia szybkości dowodzenia i skuteczności uzbrojenia, wzrostu odporności na uderzenia przeciwnika oraz zwiększenia synchronizacji działań.

7. Amerykanie, dzięki znakomitemu rozpoznaniu oraz technologii informacyjnej, nie tracili czasu na podejmowanie decyzji i przekazywanie meldunków. Zaistniała na froncie sytuacja natychmiast była przedstawiana na cyfrowej mapie, a komputer proponował kilka rozwiązań. Dowódca, nawet niższego szczebla, mógł podejmować decyzje w zależności od aktualnej sytuacji. Co więcej, mógł sam koordynować swoje działania ze wsparciem udzielanym mu z powietrza lub przez artylerię.

8. Zastosowanie sił i środków działań informacyjnych może w krótkim czasie doprowadzić 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, co jednoznacznie przemawia za tworzeniem struktur działań informacyjnych.

3. POGLĄDY NA DZIAŁANIA INFORMACYJNE WEDŁUG WYBRANYCH PAŃSTW

3.1. Koncepcja działań informacyjnych NATO

Wstępne prace związane z koncepcją sojuszu w zakresie działań informacyjnych rozpoczęto w kwietniu 1998 roku. Dokument normatywny „Polityka działań informacyjnych NATO" został przyjęty w 2002 r., natomiast „Doktryna działań informacyjnych NATO" w 2003 r.

Koncepcja działań informacyjnych integruje strategię wojskową w połączeniu z rozszerzonym spektrum działań informacyjnych, które są prowadzone po rozważeniu politycznych, dyplomatycznych i ekonomicznych możliwości członków NATO.

Działania informacyjne mogą być prowadzone na poziomie strategicznym czy operacyjnym, ale także jako pojedyncze akcje. Nie zastępują one strategii wojskowej, ale integrują tę strategię z procesem konsultacji.

Na poziomie strategicznym dla osiągnięcia celów politycznych mogą być użyte siły zbrojne w synchronizacji z mediami, środkami dyplomatycznymi, ekonomicznymi oraz psychologicznymi. Komitet Wojskowy NATO (NATO MC) przedstawia propozycje w zakresie użycia sił zbrojnych Radzie Północno-atlantyckiej (NAC) za pośrednictwem Komitetu Planowania Obronnego (Defense Planning Commitee – DPC).

Na poziomie operacyjnym siły zbrojne mogą być użyte w strefie operacji połączonych w ramach prowadzonej kampanii lub dla osiągnięcia celów strategicznych. Dowódca operacyjny odpowiedzialny jest za wykorzystanie sił zbrojnych oraz opracowanie planu operacji. Powinien także reagować na zmieniającą się sytuację i właściwie wykorzystywać możliwości bojowe elementów działań informacyjnych do skali potrzeb.

Ze względu na sposób realizacji działania informacyjne mogą być ofensywne i defensywne. Ofensywne to działania podjęte w celu oddziaływania na informacje i systemy informacyjne przeciwnika dla osiągnięcia określonych celów politycznych lub wojskowych. Prowadzenie ich opiera się na specjalnych zasadach, doktrynie i procedurach, odnoszących się do organizacji i możliwości NATO.

W ramach ofensywnych działań informacyjnych realizuje się następujące przedsięwzięcia:

— ustalenie podatności informacji, baz danych i systemów informacyjnych przeciwnika na oddziaływanie NATO;
— wykorzystanie wszystkich możliwych sposobów oddziaływania informacyjnego na słabe punkty przeciwnika;
— stworzenie mechanizmu, który pozwoli zapewnić takie prowadzenie operacji, aby osiągnąć polityczne i wojskowe zamierzenia sojuszu wobec potencjalnego przeciwnika.

Defensywne to działania podjęte w celu zabezpieczenia informacji i systemów informacyjnych wojsk własnych dla osiągnięcia określonych celów politycznych lub wojskowych.

Realizowane przedsięwzięcia w ramach działań informacyjnych w głównej mierze wpływają na decydentów, systemy informacyjne i proces informacyjny przeciwnika. Wpływ ten można uzyskać przez realizację określonego spektrum działań w czasie pokoju, kryzysu, konfliktu lub wojny, aż do czasu przywrócenia pokoju. W ramach działań informacyjnych realizowane jest jedno lub więcej następujących przedsięwzięć:
— informowanie, które wpływa na pożądane zachowanie przeciwnika (odpowiednio przygotowane treści informacyjne wywołują oczekiwane reakcje przeciwnika);
— manipulowanie informacją – polega na wprowadzeniu w błąd dowódców przeciwnika, aby podjęli decyzję na podstawie błędnych danych, w tym wypadku można stosować podstęp, walkę elektroniczną lub zakłócanie sieci komputerowych;
— pozbawienie informacji przeciwnika – realizowane jest przez bezpieczeństwo informacyjne, walkę elektroniczną oraz niszczenie obiektów pracujących w systemie ISTARS oraz C4IEWS;
— ograniczenie dopływu informacji – napływ, dystrybucja i wykorzystanie informacji mogą zostać znacznie ograniczone przez wprowadzenie przeciwnika w błąd lub znaczne opóźnienia. W tym wypadku będzie stosowana walka elektroniczna, zakłócanie sieci komputerowych oraz niszczenie obiektów infrastruktury C4IEWS;
— ograniczenie funkcjonowania dowodzenia – dowodzenie może zostać ograniczone przez prowadzenie walki elektronicznej, zakłócanie sieci komputerowych, niszczenie obiektów infrastruktury dowodzenia lub pośrednio przez wpływanie na zachowania i postawy dowódców oraz wojsk.

3.2. Działania informacyjne według poglądów amerykańskich

W sierpniu 1996 r. Dowództwo Szkolenia i Doktryn (TRADOC – Trainining and Doctrine Command) opublikowało „Regulamin walki" (FM-100-6), zawierający doktrynę działań informacyjnych.

Według tej doktryny działania informacyjne– to działania sił zbrojnych w ramach wojskowego środowiska informacyjnego (MIE), które przyczyniają się do wzmocnienia i obrony możliwości sił własnych w zakresie zdobywania, przetwarzania i przekazywania informacji w celu uzyskania przewagi w całym spektrum walki zbrojnej prowadzonej wewnątrz globalnego środowiska informacyjnego (GIE)[39], z jednoczesnym pozbawieniem takich możliwości strony przeciwnej.

Zgodnie z doktryną działań informacyjnych wszelkie działania wojskowe Stanów Zjednoczonych mają się opierać na koncepcji tworzenia wieloczynnikowej przewagi militarnej (multifactor military superiority). Kluczem jej uzyskania jest przewaga informacyjna (information superiority) i technologiczna (technological superiority).

Wszystkie dziedziny życia zarówno wojskowe, jak i cywilne są aktualnie uzależnione od infrastruktury informacyjnej. Powoduje to także powstanie nowych zagrożeń. Zdaniem Amerykanów potencjał informacyjny stał się czynnikiem tworzenia przewagi w potencjale bojowym w wybranych miejscach i określonym czasie. Działania mające na celu zakłócenie lub rażenie potencjału informacyjnego przeciwnika oraz ochronę własnych sił w tym zakresie będą stanowiły odrębny obszar funkcjonalny pola walki. Na potencjał informacyjny, jako czynnik potencjału militarnego, składają się następujące elementy:

— dane o przeciwniku (aktualne położenie, działania wojsk, zamiary strategiczne, operacyjne i taktyczne, uzbrojenie);
— wzorce doktrynalne działań, metodyka rozwiązywania problemów operacyjno-taktycznych (ocena sytuacji, podejmowanie decyzji, planowanie operacji);
— podmioty zaangażowane w procesy informacyjne (zespoły dowódczo-sztabowe, zespoły planistyczne, zespoły zajmujące się programami badawczo-rozwojowymi oraz strukturami sił zbrojnych) wraz z ich wiedzą indywidualną, stanem emocjonalnym i motywacjami;

[39]Globalne środowisko informacyjne (GIE – Global Information Environment) – to wszystkie systemy informacyjne (zarówno indywidualne, jak i połączone), media i organizacje, które zbierają, opracowują i przekazują informacje dla przedstawicielstw rządowych i wojsk. Wojskowe środowisko informacyjne (MIE – Military Information Environment) składa się z systemów informacyjnych i organizacji sił własnych i przeciwnika, które wspierają i wpływają decydująco na działania bojowe wojsk.

— infrastruktura informacyjna (systemy rozpoznania, systemy telekomunikacyjne i informatyczne) związana z bezpieczeństwem państwa.

Ponadto na potencjał informacyjny, jako czynnik potencjału militarnego, wpływ pośredni mają także:

— podmioty pozamilitarne funkcjonowania państwa (organa administarcji państwowej, instytucje naukowe, finansowe, energetyki, telekomunikacji, transportu);

— organa odpowiedzialne za programowanie rozwoju sił zbrojnych.

Na potencjał informacyjny przeciwnika można oddziaływać na wiele różnych sposobów, do których można zaliczyć:

— niszczenie danych lub ich modyfikacja (przez włamanie do infrastruktury informacyjnej przeciwnika i fizyczne zniszczenie danych lub ich zmianę);

— manipulowanie danymi (symulacja, pozoracja);

— ochrona własnych zasobów;

— prowadzenie działań psychologicznych;

— stosowanie wirusów komputerowych, bomb „logicznych", koni trojańskich, itp.

Celem działań informacyjnych jest oddziaływanie na systemy i zasoby informacyjne przeciwnika, a jednocześnie obrona własnych systemów i zasobów przed oddziaływaniem informacyjnym przeciwnika.

Zgodnie z doktryną Stanów Zjednoczonych działania informacyjne są prowadzone przez organa administracji rządowej, instytucje publiczne (media) i struktury wojskowe (stosownie do skali operacji, szczebla wykonawczego i okoliczności), których funkcje są związane z oddziaływaniem na potencjał informacyjny własny, przeciwnika, a także sojuszników czy państw neutralnych.

Nakazem doktrynalnym jest zaangażowanie w działania informacyjne wszystkich instytucji administracji rządowej, publicznych (media) i militarnych (stosownie do skali operacji, szczebla wykonawczego i okoliczności), których funkcje są związane z oddziaływaniem na potencjał informacyjny przeciwnika, potencjalnych przeciwników, państw neutralnych oraz sił własnych.

Doktryna zakłada, że działania informacyjne są prowadzone w czasie pokoju, kryzysu oraz wojny.

Na poziomie strategicznym doradcą sekretarza obrony w sprawach działań informacyjnych jest przewodniczący Komitetu Połączonych Szefów Sztabów. Odpowiada on ponadto za doktrynę, planowanie i przygotowanie działań informacyjnych, koordynację

działań w skali sił zbrojnych i w relacjach pozaresortowych, a także za wprowadzenie programów szkoleniowych i modeli symulacyjnych w uczelniach wojskowych, ćwiczeniach z wojskami oraz treningach sztabowych i grach wojennych.

Dowódcy połączonych sił oraz regionalni są odpowiedzialni za włączenie problematyki działań informacyjnych do planowania okresowego oraz planowania operacyjnego w czasie kryzysu i wojny, określenie sił i środków potrzebnych do planowania i wykonywania zadań działań informacyjnychw czasie ćwiczeń, treningów sztabowych i gier wojennych. Należy do nich także organizacja komórek sztabowych odpowiedzialnych za planowanie i koordynację działań informacyjnychna stanowiskach dowodzenia czasu „W".

Za organizowanie prac naukowo-badawczych i przedsięwzięć rozwojowych na rzecz zabezpieczenia wywiadowczego działań informacyjnychsą odpowiedzialni szefowie rodzajów wojsk i służb oraz dowództwo działań specjalnych. Spoczywa na nich również odpowiedzialność za wprowadzenie określonej problematyki do programów podległych im uczelni i ośrodków szkoleniowo-treningowych, za wspólne z Agencją Obronnych Systemów Informacyjnych (DISA) koordynowanie rozwoju i dystrybucji baz danych do planowania i prowadzenia działań informacyjnych.

Odpowiedzialność za programowanie rozwoju technologii i służb na rzecz bezpieczeństwa systemów informacyjnych (INFOSEC) i działań operacyjnych (OPSEC) ponosi Agencja Bezpieczeństwa Narodowego (NSA). Ponadto jest ona zobowiązana do bieżącego monitorowania, analizy i oceny zagrożeń własnych systemów oraz zasobów informacyjnych.

Wojskowa Agencja Wywiadowcza (DIA) jest odpowiedzialna między innymi za tworzenie baz danych i systemów informacyjnych umożliwiających uogólnianie informacji rozpoznawczych i ich przekazywanie do użytkowników. Dowódcom wyższych szczebli powinna zapewnić fachową pomoc w planowaniu i prowadzeniu działań informacyjnych. Ponadto Wojskowa Agencja Wywiadowcza we współpracy z Agencją Obronnych Systemów Informacyjnych i innymi agendami rządowymi i pozarządowymi wykonuje zadania operacyjne z zakresu ostrzegania o zagrożeniach atakiem informacyjnym.

Szczególne zadania spoczywają na centrach badawczo-szkoleniowych, do których należy opracowanie metodyk i modeli do ćwiczenia procedur działań informacyjnych.

Działania informacyjne obejmują trzy fundamentalne komponenty:

— zdobywanie informacji z rozpoznania i wywiadu;

— wykorzystanie systemów informacyjnych;

— przedsięwzięcia wojskowe w połączeniu z działalnością mediów rządowych (CA – Civil Affairs) i publicznych (PA – Public Affairs).

Aktualnie w siłach zbrojnych USA powołano struktury działań informacyjnych. Najważniejszym organem tych struktur jest Centrum Działań Informacyjnych Komitetu Połączonych Szefów Sztabów, które jest odpowiedzialne za przygotowanie i prowadzenie działań informacyjnych na potrzeby wszystkich rodzajów sił zbrojnych.

W siłach lądowych USA utworzono Centrum Działań Informacyjnych, które odpowiada za prowadzenie działań informacyjnych w wojskach lądowych na wszystkich szczeblach dowodzenia na całym świecie. Centrum podlega bezpośrednio pod dowództwo sił lądowych USA, współpracuje w zakresie działań informacyjnych z dowództwem sił powietrznych i marynarki wojennej, Centrum Działań Informacyjnych Komitetu Połączonych Szefów Sztabów oraz innymi elementami działań informacyjnych departamentu obrony oraz rządowymi. W skład centrum wchodzi:

— zespół czerwony (Red Team), który odpowiada za prowadzenie działań informacyjnych (wykorzystanie informacji, systemów informacyjnych i infrastruktury informacyjnej), na korzyść dowództwa sił lądowych USA;

— zespół reagowania na zagrożenia komputerowe (Army Computer Emergency Response Team), odpowiada za zapewnienie bezpieczeństwa systemom informacyjnym (w tym szczególnie komputerowych) wykorzystywanym na potrzeby dowództwa sił lądowych USA na całym świecie;

— zespół analizy zagrożeń i oprogramowania (Army Reprogramming and Analysis Team – Threat Analysis), który identyfikuje potencjalne zagrożenia dla systemów informacyjnych, określa zmiany w nowoczesnych technologiach informacyjnych oraz oprogramowaniu, zapewnia nowe programy komputerowe, inteligentne systemy wojskowe, sensory, procesory, wyposażenie elektroniczne dla systemów lotniczych;

— oddział zaawansowanych programów, dokonuje analizy nowoczesnych możliwości w zakresie atakowania obiektów dowodzenia przeciwnika i obrony własnych, prowadzi badania wielopłaszczyznowe (stosuje modelowanie oraz symulację komputerową) oraz monitoruje rozwój nowoczesnych technologii. Nadzoruje rozwój narzędzi działań informacyjnychw ścisłej współpracy z Dowództwem Szkolenia i Doktryn (TRADOC). Prowadzi badania nad środkami zarówno śmiercionośnymi, jak i nieśmiercionośnymi, destruktywnymi oraz niedestruktywnymi, w celu uzyskania przewagi informacyjnej w czasie operacji prowadzonych podczas pokoju, konfliktu oraz wojny;

— oddział wsparcia (Support Division), koordynuje przedsięwzięcia działań informacyjnych, szczególnie w zakresie rozpoznania, bezpieczeństwa informacyjnego, zarządzania zasobami informacyjnymi. Może także udzielić wsparcia osobowego w zakresie działań informacyjnych, jeśli jest taka potrzeba.

W siłach powietrznych Stanów Zjednoczonych funkcjonuje sześć grup działań informacyjnych.

26. Grupa Działań Informacyjnych stacjonuje w bazie sił powietrznych w Ramstein (Niemcy), rejon odpowiedzialności: Europa, Bliski Wschód oraz Afryka. Koordynuje wszystkie działania militarne na TDW. Do głównych zadań grupy należy wsparcie w zakresie rozpoznania, kryptografii, nauki i techniki dla Dowództwa SZ USA w Europie (dla komponentu wojsk lądowych, sił powietrznych oraz marynarki wojennej), Dowództwa Działań Specjalnych w Europie oraz dla NATO i innych organizacji.

67. Grupa Działań Informacyjnych stacjonuje w bazie sił powietrznych w Kelly (Teksas), rejon odpowiedzialności: terytorium USA. Realizuje zadania w zakresie wielospektralnego rozpoznania, walki elektronicznej, bezpieczeństwa systemów informacyjnych na potrzeby dowództwa narodowego, sił powietrznych, sił aeromobilnych oraz komponentu powietrznego działań specjalnych.

480. Grupa Rozpoznania stacjonuje w bazie sił powietrznych w Langley (Viktoria), zapewnia planowanie operacji oraz wsparcie w zakresie wielospektralnego rozpoznania. Ponadto odpowiada za szkolenie i przygotowanie jednostek w garnizonach.

544. Grupa Działań Informacyjnych stacjonuje w bazie sił powietrznych Peterson (Kolorado), zapewnia globalną informację z systemów kosmicznych na potrzeby agencji narodowych oraz dowództw.

690. Grupa Działań Informacyjnych stacjonuje w bazie sił powietrznych w Lackland (Teksas), odpowiada za przygotowanie i prowadzenie działań informacyjnychna potrzeby dowódców i decydentów narodowych w każdych warunkach i w różnych miejscach.

692. Grupa Działań Informacyjnych stacjonuje w bazie sił powietrznych Hickam (Hawaje), zapewnia natychmiastową dystrybucję aktualnych danych oraz wsparcie osobowe dla dowódców i agencji rządowych w rejonie Pacyfiku i Dalekiego Wschodu.

W siłach morskich występuje Departament Działań Informacyjnych, stacjonujący w Pearl Harbor.

Departament zatrudnia 60 osób personelu i składa się z trzech oddziałów:

— rozpoznania,

— obrony informacyjnej,

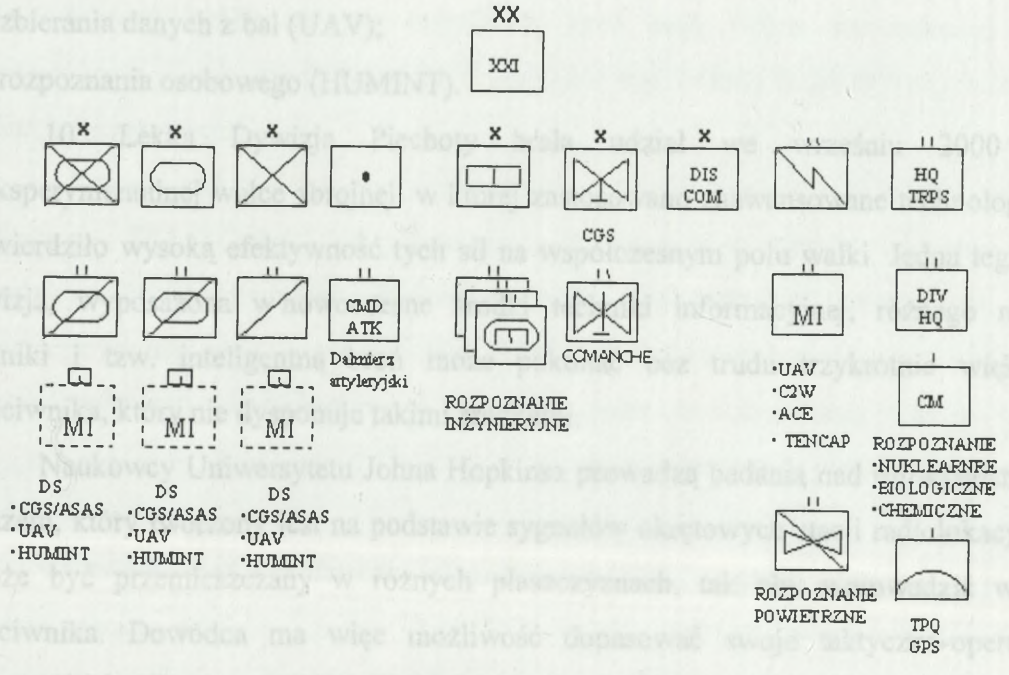
— szkolenia w zakresie działań informacyjnych.

Oddział rozpoznania (N61) prowadzi rozpoznanie elektroniczne w czasie rzeczywistym, wydziela personel do zespołu analizy rozpoznania elektronicznego na potrzeby sił morskich USA.

Oddział obrony informacyjnej (N62) chroni systemy informacyjne, które obejmują: systemy zautomatyzowane, sieci komputerowe, systemy telefoniczne, Internet, węzły łączności itp.

Oddział szkolenia (N63) odpowiada za przygotowanie personelu do prowadzenia działań informacyjnychna potrzeby Floty Atlantyckiej oraz Floty Wschodniego i Zachodniego Pacyfiku. Oddział ma do swojej dyspozycji platformę do prowadzenia symulacji.

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. Dlatego też w siłach lądowych USA dokonywana jest transformacja istniejących dywizji w dywizje XXI wieku (rys. 3.2.1).



Rys. 3.2.1. Struktura dywizji XXI wieku

W strukturze dywizji znajduje się batalion rozpoznania wojskowego, w którym występują następujące elementy:

— sekcja zbierania danych z bezpilotowych aparatów latających – bal (UAV);

— sekcja działań informacyjnych– poprzednia nazwa: sekcja walki z systemami dowodzenia i kontroli (C2W – Command and Control Warfare), zmiana nazewnictwa związana jest z szerszym zakresem działań informacyjnych);
— grupa analizy danych (ACE – Analysis and Control Element);
— sekcja oceny możliwości kraju – gospodarza (Tactical Exploitation of National Capabilities - TENCAP).

W strukturze dywizji występuje także:
— batalion rozpoznania powietrznego;
— kompania rozpoznania jądrowego, biologicznego i chemicznego (ABC);
— kompania koordynacji z systemem GPS;
— pododdziały rozpoznania inżynieryjnego.

Ponadto, jako wzmocnienie dywizji, utworzone zostaną trzy mieszane kompanie rozpoznania wojskowego o jednolitej strukturze, w każdej z nich będą występować trzy plutony (sekcje):
— zbierania danych ze wszystkich źródeł (ASAS), która ma dostęp do danych z rozpoznania satelitarnego, wyposażona jest w naziemną stację łączności satelitarnej (CGS);
— zbierania danych z bal (UAV);
— rozpoznania osobowego (HUMINT).

10. Lekka Dywizja Piechoty brała udział we wrześniu 2000 roku w eksperymentalnej walce zbrojnej, w której zastosowano zaawansowane technologie, co potwierdziło wysoką efektywność tych sił na współczesnym polu walki. Jedna tego typu dywizja, wyposażona w nowoczesne środki techniki informacyjnej, różnego rodzaju czujniki i tzw. inteligentną broń może pokonać bez trudu trzykrotnie większego przeciwnika, który nie dysponuje takimi środkami.

Naukowcy Uniwersytetu Johna Hopkinsa prowadzą badania nad trójwymiarowym obrazem, który tworzony jest na podstawie sygnałów okrętowych stacji radiolokacyjnych i może być przemieszczany w różnych płaszczyznach, tak aby wprowadzić w błąd przeciwnika. Dowódca ma więc możliwość dopasować swoje taktyczno-operacyjne planowanie do aktualnego położenia we właściwym czasie.

3.3. Niemieckie poglądy na prowadzenie działań informacyjnych

Zgodnie z niemiecką koncepcją środki masowej komunikacji mogą wywierać decydujący wpływ na przebieg i rozwiązywanie konfliktów. Ten, kto dysponuje takimi środkami, może ich użyć dla własnej korzyści, a ze szkodą dla przeciwnika. Propaganda, dezinformacja i manipulacja wiadomościami są elementami działań informacyjnych. Jeśli jedna strona będzie posiadać ograniczone możliwości w zakresie zdobywania danych oraz informowania opinii publicznej, wtedy druga będzie miała nieograniczone możliwości w zakresie prowadzenia indoktrynacji politycznej, etnicznej, religijnej oraz innego rodzaju ideologizacji. Może to prowadzić do eskalacji konfliktów wewnętrznych i międzypaństwowych oraz wpływać negatywnie na postawy dowódców i żołnierzy, którzy wykonują różnego rodzaju misje obserwacyjne, niesienia pomocy humanitarnej lub przywracania pokoju.

Dla zażegnania tego niebezpieczeństwa konieczne jest informowanie ludności cywilnej oraz wojsk własnych i sojuszniczych z wykorzystaniem własnego systemu informacyjnego. Duża rola w tym zakresie przypada strukturom działań informacyjnych, które będą wpływać na zachowanie się żołnierzy oraz ludności cywilnej i wywierać pozytywny lub negatywny wpływ na realizowane misje wojskowe. Znaczenie i możliwość wykorzystania elementów działań informacyjnychmusi być znana dowódcom wojskowym oraz decydentom. W związku z tym należy dokonać analizy różnych czynników, które mają wpływ na realizację działań informacyjnych. Analiza tych czynników i wynikające stąd wnioski mogą wpłynąć na struktury działań informacyjnych.

„Koncepcja działań informacyjnych Niemiec" (Teilkonzeption bereichsübergreifende Aufgaben – TBKA OpInfo) jest podstawowym dokumentem w zakresie planowania struktur organizacyjnych Bundeswehry. Zawiera założenia przygotowania i prowadzenia działań informacyjnych oraz zadania reprezentacyjne sił zbrojnych wobec władz cywilnych, NATO, innych państw i organizacji międzynarodowych. Koncepcja pozostaje dokumentem otwartym i będzie rozwijana stosownie do wymagań. Część zadań w tym zakresie została przedstawiona w „Białej księdze" w 1994 r.

Zadaniem struktur działań informacyjnych jest wsparcie procesu dowodzenia z wykorzystaniem środków i metod komunikowania się. Struktury działań informacyjnych są wydłużonym ramieniem dowódcy, z którego pomocą może on przekazywać wiadomości do wybranej grupy odbiorców.

Zadaniem tych struktur jest oddziaływanie na siły zbrojne, strony konfliktu lub grupy ludności wrogich państw w celu zmiany zachowań i postaw, uzyskania zaufania i wsparcia dla wypełnienia własnych zadań.

Niektóre siły działań informacyjnychwchodzą w skład sił reagowania kryzysowego i ze względu na swoje ukompletowanie i mobilność mogą być wykorzystywane w misjach poza granicami kraju.

Rozwój nowych technik informowania i ulegający coraz większemu skróceniu czas przekazywania danych poza obszarem działań militarnych oddziałuje na procesy planowania, podejmowania decyzji, przebieg i ocenę operacji wojskowych. Informacje wpływają na proces dowodzenia operacyjnego, zachowanie wojsk, opinię publiczną wewnętrzną i zagraniczną oraz na siły zbrojne i ludność na obszarze prowadzenia działań operacyjnych.

Podczas misji pokojowych wojska muszą starać się o uzyskanie akceptacji dla swoich działań stron konfliktu i ludności cywilnej. Dotyczy to zachowania bezstronności, co uzyskuje się przez przejrzyste i otwarte działanie, tak daleko posunięte, jak pozwalają na to warunki bezpieczeństwa. Stosowanie tych zasad do osiągnięcia tych celów obowiązuje wszystkich uczestników misji. Muszą oni stronom konfliktu i ludności cywilnej wyjaśniać przyczyny wkroczenia wojsk, sens i zasadność wykonywanych przedsięwzięć, pozyskiwać zrozumienie i gotowość do współpracy.

Wojska własne oraz ludność cywilna na obszarze operacji nie powinny pozostawać pod kontrolą przeciwnika i jego jednostronnym wpływem środków masowej komunikacji. Jest ważne, aby te grupy odbiorców informować zgodnie z własnym zamiarem w celu przeciwdziałania dezinformacji, pogłoskom, błędnym interpretacjom oraz ograniczeniu nieporozumień.

Celowa i zorientowana na wykonanie wojskowego zadania komunikacja z jakimkolwiek przeciwnikiem może osłabić jego morale, pomóc obniżyć straty własne i przez to służyć bezpieczeństwu własnych wojsk.

Przedsięwzięcia realizowane w ramach działań informacyjnych mogą oddziaływać jedynie wtedy, gdy ich wymowa jest zgodna z wojskowym dowodzeniem i kierowaniem operacją, a zachowanie własnych żołnierzy współgra z nimi. Wiadomości przekazane bez podania źródła mogą być tak samo szkodliwe dla wiarygodności własnych wojsk, jak nieuzasadniona reakcja na prowokację. Na te zagadnienia musi znaleźć się czas podczas szkolenia.

Także jeśli zadania realizowane w ramach działań informacyjnych różnią się od obszarów zadaniowych pracy informacyjnej Bundeswehry, cele i zawartość przekazywanych informacji musi być uzgadniana z komórkami prasowo-informacyjnymi, tak aby różnymi kanałami nie zostały podane wytypowanym grupom odbiorców niepożądane wiadomości. Zadaniem dowódcy jest

regularne i wszechstronne informowanie wojsk, przy czym ich zachowanie musi być zgodne z przewidywanymi lub prowadzonymi przedsięwzięciami.

Przedsięwzięcia działań informacyjnych wymagają dokładnego zaplanowania. Wybór celów oddziaływania i ich dokładna znajomość ma szczególne znaczenie. Do tego niezbędne są informacje z wojskowych służb informacyjnych.

Siły działań informacyjnych wykorzystują obok jawnych, także źródła wywiadowcze dotyczące sytuacji w obcych państwach. Sztab wsparcia informacji operacyjnej współpracuje ściśle z Urzędem Rozpoznania Bundeswhry.

Podczas wykonywania zadań struktury działań informacyjnych otrzymują ważne, aktualne informacje, także od jednostek nasłuchu radiowego. Wyniki wywiadu i rozpoznania przyczyniają się do selekcji celów oddziaływania i kontroli skuteczności.

W razie zapotrzebowania struktury działań informacyjnych mogą przygotować analizę sytuacji psychologicznej i prowadzić oddziaływanie z wykorzystaniem środków masowej komunikacji.

Każde zadanie z wykorzystaniem środków masowej komunikacji niesie niebezpieczeństwo nadużycia i może prowadzić do nieoczekiwanego rozwoju sytuacji. Dlatego została opracowana specjalna procedura, zezwalająca na podjęcie działań informacyjnych.

Celem procedury działania w sytuacjach szczególnych jest uzyskanie akceptacji ministerialnej o:

— celach oddziaływania informacyjnego i sposobie wykonania zadania,

— wykorzystaniu struktur działań informacyjnychi ich podporządkowaniu,

— przygotowaniu i akceptacji materiałów informacyjnych.

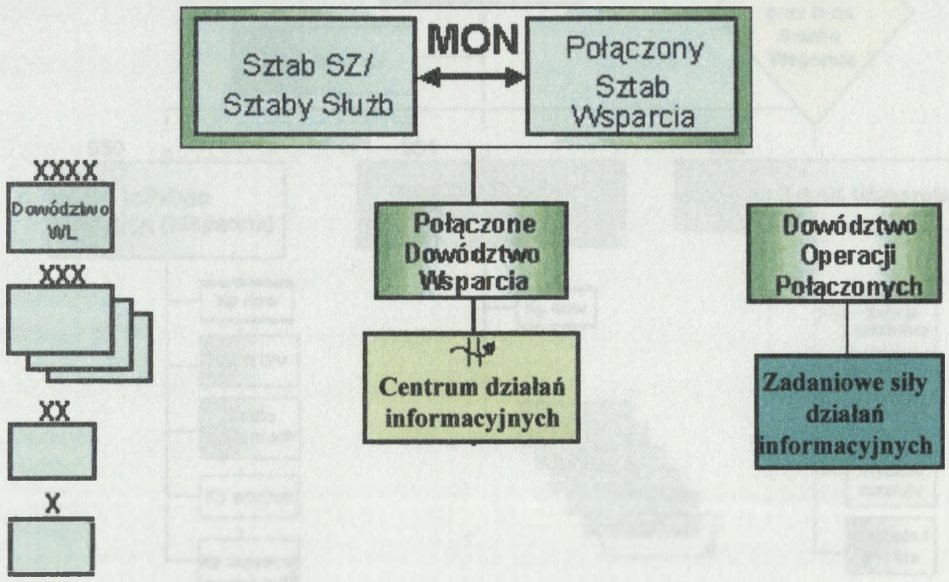
W związku z dużym zapotrzebowaniem na udział elementów działań informacyjnych Bundeswehry w misjach pokojowych, w październiku 2002 utworzono Centrum Działań Informacyjnych (rys. 3.3.1), które podlega Połączonemu Dowództwu Wsparcia.

Centrum liczy 1200 żołnierzy, składa się z 2 batalionów, sekcji wsparcia i uczestniczy w wielu operacjach prowadzonych przez sojusz, m.in. w ramach sił KFOR, SFOR, ISAF[40].

[40]KFOR (The Kosovo Force) – międzynarodowe siły w Kosowie, odpowiedzialne za utrzymanie pokoju, zostały powołane 12 czerwca 1999 r. na podstawie Rezolucji Rady Bezpieczeństwa ONZ nr 1244. W skład ich wchodzi pięć międzynarodowych brygad. SFOR (Stabilisation Force) – międzynarodowe siły stabilizacyjne w Bośni i Hercegowinie. W ich skład wchodzi trzy brygady międzynarodowe. Liczą 13 000 żołnierzy (12 900 w Bośni i Hercegowinie oraz 100 osób w Chorwacji). ISAF (International Security Assistance Force) – międzynarodowe siły bezpieczeństwa w Afganistanie.

950 batalion (951 w trakcie formowania) powstał w październiku 1989 roku na bazie 850 batalionu (Psychologische Verteidigung PSV) w Andernach.

Siły i środki 950 batalionu realizują zadania wsparcia działań i przyporządkowane są oddziałowi trzeciemu.

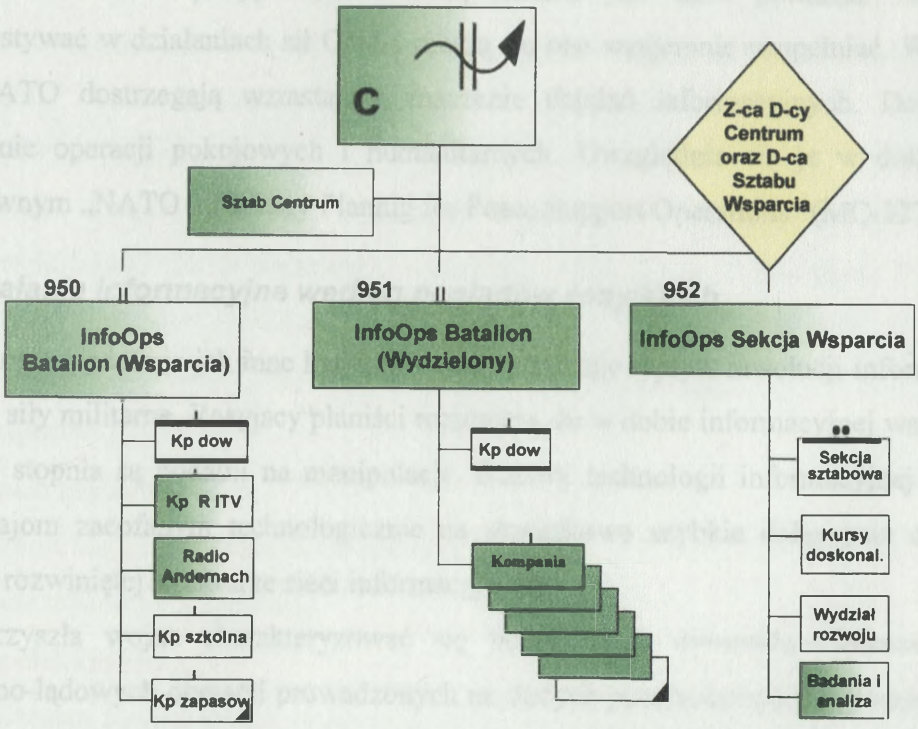


Rys. 3.3.1. Podległość struktur działań informacyjnych

Zespół specjalistów centrum informacyjnego odpowiada za proces zbierania i gromadzenia danych o prawdopodobnym obiekcie oddziaływania oraz za ich analizę pod kątem wykorzystania przy opracowywaniu audycji radiowych, elektroakustycznych i materiałów drukowanych.

Pododdziały działań informacyjnych w zupełności odpowiadają nowym zadaniom Bundeswehry. Szczególnie dotyczy to obszaru przezwyciężania kryzysu, a także udziału w akcjach humanitarnych. Użycie sił działań informacyjnychw Somalii udowodniło, jak niezbędne są one we wsparciu wojsk. Cel operacji został osiągnięty dzięki szeroko zakrojonej akcji informacyjnej. Za pomocą ulotek, plakatów, gazet i audycji elektroakustycznych ludność tego kraju była informowana o działaniach niemieckiego kontyngentu. Pluton działań informacyjnych wydawał dwujęzyczny (angielsko-somalijski) tygodnik „Irrida Nabada" („Brama Wolności"), który był bardzo ważnym pomostem porozumienia i współpracy z ludnością. Nakład pierwszego wydania tygodnika wynosił 800 egzemplarzy. W dziesiątym wydaniu wynosił już 16000 egzemplarzy. Ponadto szkolono somalijskich redaktorów w obsłudze drukarń oraz w przygotowaniu wydawnictw medycznych przeznaczonych dla ludności regionu.

Działalność pododdziałów działań informacyjnych w Somalii była udana i przeprowadzona została bez jakichkolwiek zakłóceń.



Rys. 3.3.2. Struktura Centrum Działań Informacyjnych Niemiec

Informacja w każdym społeczeństwie ma ogromne znaczenie. Dotyczy to szczególnie obszarów zróżnicowanych etnicznie. W czasie konfliktów etnicznych tworzy się tzw. chaos informacyjny, w którym manipuluje się treściami informacyjnymi, zniekształcając fakty. Jeżeli chce się uniknąć tego rodzaju sytuacji, należy przede wszystkim udzielać informacji o charakterze wyjaśniającym. Obecnie taką sytuację możemy zaobserwować w byłej Jugosławii. Tamtejsza ludność żyje pod wpływem fałszywych wiadomości, plotek i propagandy, które potęgują cierpienia ludzi. Skuteczne przeprowadzenie operacji pokojowej zależy od współpracy wszystkich uczestników misji.

Zanim jednak żołnierze ONZ wkroczą do akcji, z pomocą mediów przygotowana zostanie akcja informacyjna skierowana do stron konfliktu z wykorzystaniem takich środków, jak: ulotki, audycje radiowe czy też komunikaty elektroakustyczne. Takie działania zostały już zaakceptowane w planowaniu operacyjnym NATO.

Pododdziały działań informacyjnych oddziałują na przeciwnika i ludność cywilną poprzez odpowiednią strategię informacyjną. Przy tym muszą się wzajemnie uzupełniać, aby wiadomości wychodzące z obu źródeł nie wykluczały się wzajemnie.

Omawiane działania są dość delikatnym przedsięwzięciem politycznym, muszą one ściśle współdziałać z politycznym i wyższym dowództwem wojskowym. Stąd też odpowiedzialność za podjęte kroki w tej materii jest dość poważna. Należy je wykorzystywać w działaniach sił ONZ i muszą się one wzajemnie uzupełniać. Wszystkie kraje NATO dostrzegają wzrastające znaczenie działań informacyjnych. Dotyczy to szczególnie operacji pokojowych i humanitarnych. Uwzględnia się je w dokumencie normatywnym „NATO – Military Plannig for Peace Support Operations" (MC-327).

3.4. Działania informacyjne według poglądów rosyjskich

Rosja, podobnie jak inne kraje, poważnie analizuje wpływ rewolucji informacyjnej na swoje siły militarne. Rosyjscy planiści rozumieją, że w dobie informacyjnej wszyscy do pewnego stopnia są podatni na manipulacje. Rozwój technologii informacyjnej pozwoli wielu krajom zacofanym technologicznie na stosunkowo szybkie dołączenie do grona krajów o rozwiniętej strukturze sieci informacyjnych.

Przyszła wojna charakteryzować się będzie dużą dynamiką i intensywnością powietrzno-lądowych operacji prowadzonych na dużych przestrzeniach. Działania bojowe będą znacznie skuteczniejsze i będą prowadzone w sposób nielinearny. Łączność będzie sporadyczna, a dowodzenie trudne.

Według poglądów rosyjskich receptą na osiągnięcie powodzenia w nowoczesnych działaniach jest przede wszystkim zdobycie przewagi informacyjnej, następnie panowania w powietrzu i dopiero na końcu prowadzenie działań bojowych.

Działania informacyjne będą prowadzone w celu zdobywania informacji o przeciwniku, wykorzystania ich i tym samym zwiększenia potencjału bojowego wojsk własnych. Do zadań środków aktywnych w tym zakresie będzie należało:

— wprowadzenie wirusa do programów przeciwnika lub uszkodzenie ich w inny sposób,
— wykonanie uderzeń za pomocą broni wykorzystującej wiązkę superwysokiej częstotliwości lub pulsację elektromagnetyczną.

Do zadań środków pasywnych (obrona radioelektroniczna i maskowanie) będzie należało:

— wykorzystanie nowoczesnych rakiet przeciwradiolokacyjnych i bezpilotowych aparatów latających,
— spowodowanie zakłóceń w pracy systemów przeciwnika,
— wykorzystanie wirusa komputerowego.

Działania informacyjne mogą być prowadzone samodzielnie, bez stosowania tradycyjnych środków i sposobów walki zbrojnej:

— w czasie pokoju – może to być elektroniczne zastraszanie;

— w czasie narastania kryzysu – zmasowane (pod względem intensywności) użycie środków elektronicznych przeciwko wojskowym i cywilnym strukturom informacyjnym przeciwnika;

— w czasie trwania konfliktu zbrojnego – zmasowane użycie zarówno środków elektronicznych, jak i ogniowych przeciwko wojskowym i cywilnym strukturom informacyjnym przeciwnika.

Rosjanie za główne formy działań informacyjnych uważają:

— dezinformację,

— działania psychologiczne,

— niszczenie fizyczne systemów informacyjnych,

— ochronę tajemnicy wojskowej,

— walkę elektroniczną.

Zdaniem Rosjan strona dysponująca przewagą informacyjną będzie zawsze miała większe możliwości bojowe nawet w sytuacji, kiedy przeciwnik ma wyraźną przewgę w środkach konwencjonalnych. Z punktu widzenia efektywnego wykorzystania środków finansowych wzrost liczebny armii i sprzętu bojowego jest obecnie ślepym zaułkiem zwiększania potencjału bojowego wojsk. Wyposażenie w nowe urządzenia elektroniczne i komputerowe systemów rozpoznania, dowodzenia i kierowania środkami walki jest obecnie najszybszą metodą zwiększania mocy bojowej sił zbrojnych. Możliwości bojowe systemów rozpoznania, dowodzenia i walki elektronicznej muszą być uwzględniane we wszelkich analizach i ocenach sił ugrupowania bojowego zarówno przeciwnika, jak i własnego.

Podczas zimnej wojny niezwykle trudno było uzyskać dane na temat radzieckich struktur działań psychologicznych. Przez lata Rosjanie utrzymywali swoje archiwa, struktury sił zbrojnych i procedury operacyjne w ścisłej tajemnicy. Jedynie dzięki niedawnemu odtajnieniu danych mamy większą wiedzę na ten temat.

Od około 1992 roku Rosjanie przestali uważać za tajne informacje dotyczące istnienia i szkolenia swoich jednostek działań psychologicznych. Jednak pozyskiwanie wiadomości o tych jednostkach i ich działaniu nadal pozostaje trudne. Pewne źródła prasowe uważają, że główny zarząd wywiadu wojskowego sprawuje pieczę nad tymi

jednostkami, co może wyjaśniać trudność w uzyskaniu danych.

W czasach Związku Radzieckiego działania tego typu były określane mianem specjalnej propagandy. Obecnie teoretycy wojskowi używają terminu działania informacyjno-psychologiczne.

Działania informacyjno-psychologiczne to kompleks przedsięwzięć, obejmujących: wsparcie, przeciwdziałanie i obronę informacyjną, prowadzone według jednolitej koncepcji i planu, w celu wywalczenia i utrzymania przewagi informacyjnej nad przeciwnikiem podczas prowadzenia operacji wojskowych.

Do działań tego typy Rosjanie zaliczają także nietradycyjne sposoby, np. wstrząs i terror psychologiczny wywołany atakami artylerii i lotnictwa. Kiedy rosyjskie czołgi zaatakowały budynek parlamentu rosyjskiego w październiku 1993 roku, głównym celem ataku było wywołanie wstrząsu lub wpływu psychologicznego na osoby okupujące budynek. Kiedy w styczniu 1996 roku w mieście Pierwomajskaja Rosjanie zaatakowali czeczeńskich rebeliantów ciężkim ostrzałem artylerii i rakiet, dowódca rosyjski opisał działania jako formę działań informacyjno-psychologicznych.

Innym nietradycyjnym sposobem działań informacyjno-psychologicznych jest rosyjska koncepcja oddziaływania zwrotnego. W kontekście wojskowym może być określona jako sposób zapewnienia dowódcy wojskowemu możliwości bezpośredniego utrzymywania kontroli nad procesem podejmowania decyzji przez dowódców przeciwnika. Oddziaływanie zwrotne jest procesem manipulowania danymi tak, aby przeciwnik został zmuszony do podjęcia działań korzystnych dla drugiej strony.

Siły zbrojne (na poziomie operacyjnym) badały wartość oddziaływania zwrotnego zarówno w kontroli procesów decyzyjnych przeciwnika, jak i rozwijaniu technik „maskirowki" (oszukiwania i dezinformacji). Na początku XX wieku istniała wojskowa szkoła „maskirowki", która stała się podstawą rozwoju tej koncepcji dla przyszłych pokoleń. Szkoła została rozwiązana w 1929 roku.

Wielu rosyjskich socjologów rozumie, że siły zbrojne (po części z powodu braku treningu moralno-psychologicznego) są aktualnie bardzo podatne na ataki informacyjno-psychologiczne. W przeszłości system departamentów propagandy spełniał rolę treningu moralno-psychologicznego. Aktualnie nie istnieje niezależny aparat moralno-psychologicznego wsparcia, aby wypełnić tę lukę. Moralno-psychologiczne wsparcie jest aktualnie rozumiane jako celowy wpływ na umysły i psychikę rosyjskiego personelu wojskowego. Dowódcy na określonych szczeblach dowodzenia są odpowiedzialni za wzmacnianie psychologicznej odporności wśród personelu i formowanie ich moralnej

gotowości do działania w dowolnych warunkach. Dowódcy polowi winni skierować szczególne wysiłki na utrzymanie korelacji moralno-psychologicznych sił w równowadze.

Według rosyjskich analityków, wydarzenia lat 90. spowodowały zasadniczą zmianę militarno-politycznej sytuacji w świecie, a także politycznych, socjalno-ekonomicznych i moralno-psychologicznych stosunków wewnątrz krajów. Współczesne tendencje w rozwoju sił zbrojnych, środków i sposobów walki zmieniły się w związku z ich nowymi funkcjami w zakresie oddziaływania moralno-psychologicznego. Aktualnie istnieje rzeczywista potrzeba zrozumienia istoty i znaczenia działań moralno-psychologicznych.

Ponadto należy zapewnić bezpieczeństwo własnych wojsk przed oddziaływaniem przeciwnika w tym zakresie. Informacyjno-psychologiczne bezpieczeństwo polega na przedsięwzięciach i takim wykorzystaniu danych, aby zagwarantować stabilność psychiki i świadomości własnego personelu zarówno w czasie pokoju, jak i wojny. Mogą to być środki do zwalczania akcji psychologicznych przeciwnika, które mogłyby mieć negatywny wpływ na morale własnych sił.

Rosjanie uważają, że informacyjno-psychologiczne bezpieczeństwo jest bardzo ważne, ponieważ w ciągu ostatniego półwiecza wzrosła zdolność kształtowania świadomości, psychiki czy morale społeczeństwa, a także sił zbrojnych. Do takiego stanu rzeczy przyczyniły się znaczące osiągnięcia wielu krajów w obszarze psychologii, psychotroniki czy parapsychologii[41].

Do podstawowych założeń rosyjskiej koncepcji działań informacyjno-psychologicznych należy zaliczyć:

— analizowanie moralno-psychologicznego środowiska w Rosji na poziomie strategicznym i w obszarach, gdzie mogą być prowadzone potencjalne operacje;
— poszukiwanie, zbieranie, analizowanie i podsumowywanie informacji o przeciwniku lub potencjalnych uczestnikach konfliktu;
— przewidywanie możliwego wpływu działań informacyjnych przeciwnika na rosyjskie siły zbrojne i ludność;
— blokowanie (lub łagodzenie efektów) działań informacyjnych przeciwnika na poziomie strategicznym, używając wszelkich dostępnych środków, rodzajów uzbrojenia oraz sił

[41]Parapsychologia – nauka o zjawiskach trudnych lub niemożliwych do wyjaśnienia za pomocą znanych praw przyrody. Przedmiot zainteresowań teorii i praktyk okultystycznych. Termin wprowadzony w zakres nauki w 1889 przez M. Dessoira. Upowszechniony wraz z założeniem Laboratorium Parapsychologicznego na Uniwersytecie Dukea w Durham, w Karolinie Północnej. W 1930 badania nad parapsychologią rozpoczęli J. B. Rhine i L. Rhine. Psychotronika – interdyscyplina naukowa utworzona w 1973 na I Międzynarodowym Kongresie Badań Psychotronicznych w Pradze. Obszar jej badań mieści się na pograniczu psychologii i biofizyki.

specjalnych;

— zaopatrywanie sił działań informacyjno-psychologicznych w najnowocześniejsze środki w celu przeciwdziałania oddziaływaniu informacyjno-psychologicznemu na rosyjskie siły zbrojne i ludność;

— neutralizowanie negatywnych konsekwencji oddziaływania przeciwnika na świadomość, morale i stan ducha;

— nieustanna ochrona wojsk i ludności przed informacyjno-psychologicznym oddziaływaniem przeciwnika;

— przygotowanie sił i środków do prowadzenia działań informacyjno-psychologicznych;

— wywieranie stałego, informacyjno-psychologicznego wpływu na siły i ludność przeciwnika;

— prowadzenie nietradycyjnych działań (w tym z zakresu parapsychologii) w celu wpływania na świadomość i stan psychiczny przeciwnika;

— rozwijanie teorii działań informacyjno-psychologicznych oraz przekazywanie zaleceń i propozycji dla agencji rządowych i dowództw wojskowych.

Według poglądów rosyjskich wojskowe działania informacyjno-psychologiczne mogą być prowadzone na poziomie strategicznym, operacyjnym i taktycznym.

Na poziomie strategicznym działania są planowane i prowadzone dla osiągnięcia celów długoterminowych. Obiektem oddziaływania jest wówczas ludność cywilna, siły zbrojne i rząd atakowanego państwa. Realizacja takich działań wymaga koordynacji działań różnych struktur wojskowych i rządowych.

Na poziomie operacyjnym są one prowadzone na korzyść sił własnych, zaangażowanych w operacjach bojowych. Ich obiektem jest przede wszystkim społeczeństwo zamieszkałe na terytorium przeciwnika. Działania szczebla operacyjnego bezpośrednio lub pośrednio tworzą warunki do pokonania jego wojsk (między innymi przez podkopanie wiary w możliwość odniesienia zwycięstwa), przygotowują ludność do prowadzenia wojny na danym terytorium, stwarzają warunki do izolacji sił zbrojnych wśród ludności miejscowej oraz mają sprzyjać wciąganiu społeczeństw lokalnych do współpracy wymierzonej przeciwko strukturom administracji państwowej i samorządowej.

Na poziomie taktycznym działania są planowane i realizowane w celu osiągnięcia natychmiastowych i krótkoterminowych rezultatów, obliczonych na bezpośrednie wspomaganie jednostek bojowych wojsk własnych. Motywem przewodnim tych działań

jest wywarcie pożądanego wpływu na ludność zamieszkałą na terytorium przeciwnika i jego żołnierzy w strefie odpowiedzialności dowódcy szczebla taktycznego.

Według Rosjan warunkiem pomyślnego wyniku działań informacyjno-psychologicznych jest ciągłe wywieranie presji na przeciwnika i utrzymanie inicjatywy w zakresie wsparcia działań bojowych.

Wsparcie to oznacza system zróżnicowanych przedsięwzięć prowadzonych w ramach działań informacyjno-psychologicznych, skoordynowanych i powiązanych pod kątem celów oraz czasu i miejsca operacji zbrojnej. Działania te powinny kształtować w opinii publicznej pozytywny obraz własnej działalności wojskowej, zneutralizować lub osłabić konsekwencje negatywnego oddziaływania informacyjno-psychologicznego przeciwnika, wzmocnić postawę moralną i odporność psychologiczną własnego społeczeństwa oraz stworzyć dogodne warunki realizacji zadań przydzielonym jednostkom sił zbrojnych.

Wyścig zbrojeń wkracza obecnie w sferę oprogramowania. Im bogatszy wachlarz przydatnych programów w funkcjonowaniu autonomicznych systemów rozpoznania, podejmowania decyzji i kierowania środkami walki, tym większa możliwość skutecznego ich użycia w warunkach bojowych. Dlatego też obecnie w Rosji wprowadza się wiele zmian w tym zakresie.

Po pierwsze, wprowadzono doktrynę działań informacyjno-psychologicznych, która ma zastąpić działania propagandowo-agitacyjne byłego aparatu politycznego.

Po drugie, niektórzy teoretycy wojskowi uważają działania informacyjno-psychologiczne za niezależną formę działań militarnych, która wymaga wyspecjalizowanego personelu i ćwiczeń.

Po trzecie, jako konsekwencja powyższego, dąży się do utworzenia nowego rodzaju sił zbrojnych, dodatkowej specjalności militarnej, skierowanej na konfrontację informacyjno-psychologiczną.

Po czwarte, rosyjska kadra oficerska uświadamia sobie, że nie jest możliwe prowadzenie operacji militarnych bez informacyjno-psychologicznych działań[42].

Niektórzy rosyjscy teoretycy wojskowi uważają, że osiągnięcia technologiczne, szczególnie rozwój nowych technologii informacyjnych w Stanach Zjednoczonych, powodują, że informacyjno-psychologiczna konfrontacja staje się nieodłącznym typem działań militarnych, podobnie jak obrona i natarcie.

---

[42]G. Nowacki, *Operacje informacyjne*, Warszawa, AON, 2001, s. 59.

W rezultacie tego, w dowolnym konflikcie zbrojnym, wszelkie działania militarne będą poprzedzone działaniami informacyjno-psychologicznymi, skierowanymi przede wszystkim na świadomość, morale i psychikę ludności oraz na strukturę informacyjną przeciwnika.

Taka sytuacja wymusza niejako nadrzędność działań informacyjno-psychologicznych w stosunku do operacji militarnych i jest niezbędna do osiągnięcia końcowego sukcesu na polu walki.

Niektórzy oficerowie uważają, że siły i środki prowadzenia działań informacyjno-psychologicznych powinny być traktowane jak rodzaj broni. Niezdolność do podjęcia przeciwdziałania przyczyni się do totalnej porażki, np. jak to miało miejsce w przypadku armii irackiej w czasie wojny w rejonie Zatoki Perskiej.

Podczas drugiej operacji czeczeńskiej w latach 1999–2000 Ministerstwo Obrony Federacji Rosyjskiej nadało dużą rangę operacjom informacyjno-psychologicznym. Przyznali oni, że ten sposób oddziaływania na bojowników czeczeńskich oraz ludność zamieszkującą Czeczenię i Inguszetię może w istotny sposób wesprzeć prowadzoną operację. Do prowadzenia operacji z Głównego Zarządu ds. Pracy Wychowawczej został wydzielony specjalistyczny personel i środki. Za praktyczną realizację działań informacyjno-psychologicznych odpowiedzialny został Zarząd Rozpoznania i Walki Psychologicznej Zgrupowania Sił Federalnych na Północnym Kaukazie, który powstał na bazie Zarządu Rozpoznania Północnokaukaskiego Okręgu Wojskowego.

W strukturze zarządu utworzono oddział działań psychologicznych, składający się z grup działań psychologicznych, do których poszczególne okręgi wojskowe oraz inne ministerstwa „siłowe" wydzieliły 98 żołnierzy.

Podstawową formą prowadzenia działań psychologicznych w Czeczenii było destrukcyjne oddziaływanie na psychikę wojsk przeciwnika, głównie przez utrzymywanie poczucia stałego zagrożenia. Potęgowało to zniechęcenie i obniżanie woli walki, skutkujące w wielu przypadkach składaniem broni i przechodzeniem bojowników na stronę sił federalnych.

Istotnym elementem było również silne morale własnych wojsk oraz zapobieganie skutkom propagandy czeczeńskiej i informowanie o zamiarach wojsk.

Oddział Działań Psychologicznych opracował dwa teksty ulotek skierowanych do mieszkańców i bojowników znajdujących się na obszarze republiki, przygotował również dwie wersje programu radiowego (w języku rosyjskim i czeczeńskim), który był

skierowany do ludności zamieszkującej Północny Kaukaz. Cykl działań psychologicznych obejmował cztery etapy.

W pierwszym etapie (wrzesień – grudzień 1999 r.) do akcji psychologicznych wydzielone zostały cztery grupy działań psychologicznych. Rozrzucono ponad 2 mln ulotek (90% za pomocą bomb propagandowych z samolotów *Su-25* i pocisków artyleryjskich, pozostałe 10% przy pomocy pododdziałów wojsk wewnętrznych), nadano 78 audycji radiowych emitowanych ze śmigłowców i 270 – ze stacji naziemnych (łączny czas ich trwania wynosił ponad 24 godziny).

Analiza rozwoju sytuacji w strefie konfliktu i podjęte działania psychologiczne wykazały, że najlepsze rezultaty przynosiła bezpośrednia praca z przywódcami lokalnych społeczności i mieszkańcami poszczególnych obszarów, w której wykorzystywano wyniki prowadzonych z nimi negocjacji, retransmisje programów radiowych nadawanych z Moskwy i propagandę w postaci materiałów drukowanych.

W drugim etapie (styczeń – luty 2000 r.) rozrzucono ponad 1 mln ulotek z ultimatum wzywającym wszystkie osoby pozostające w mieście do opuszczenia Groznego oraz nadano 400 audycji o łącznym czasie trwania 16 godzin.

W trzecim etapie (marzec – maj 2000 r.) główny wysiłek skupiono na:

— rozpowszechnianiu ulotek w obszarach zabudowanych, wzdłuż dróg marszu konwojów z pomocą humanitarną oraz w miejscach wskazanych przez dowódców zgrupowań;
— nadawaniu ze śmigłowców i stacji naziemnych komunikatów skierowanych do bojowników i ludności miejscowej;
— wchodzeniu w sieci radiowe przeciwnika w celu dezinformowania go i obniżania jego morale.

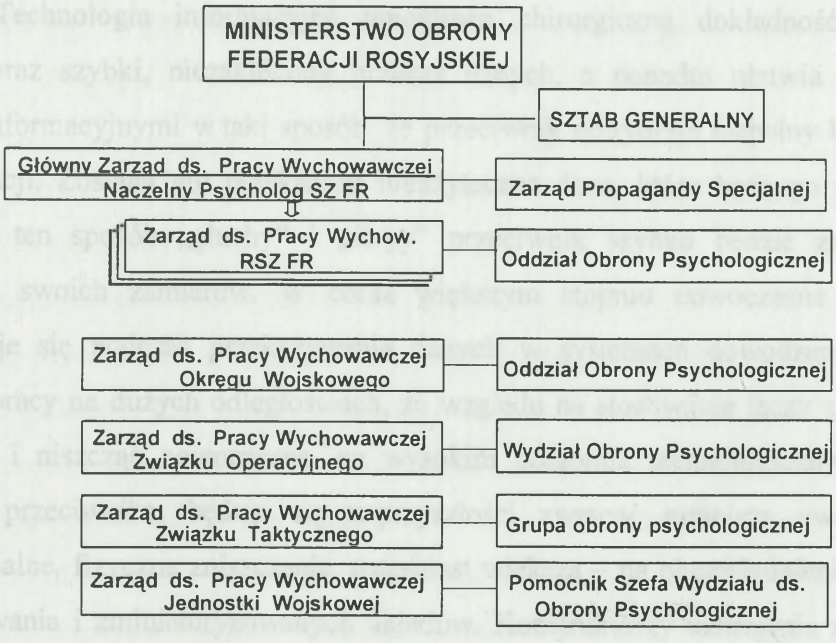
W czwartym etapie (czerwiec – lipiec 2000 r.) skoncentrowano się na pracy z mieszkańcami, liderami miejscowej ludności i duchowieństwem republiki. Rozpowszechniano prasę, ulotki i retransmitowano programy radiowe nadawane z Moskwy. W komendanturach wojskowych poszczególnych rejonów Czeczenii utworzono wydziały pracy z ludnością miejscową.

Aktualnie zadania w zakresie działań informacyjno-psychologicznych zostały przejęte przez pion oficerów wychowawczych, podporządkowany szefowi Głównego Zarządu ds. Pracy Wychowawczej Ministerstwa Obrony, któremu podlegają zarządy ds. wychowawczych rodzajów sił zbrojnych (rys. 3.4.1)[43].

[43]G. Nowacki, *Działania psychologiczne w ramach...*, s. 109.

Na poziomie rodzaju sił zbrojnych oraz okręgu wojskowego występują oddziały obrony psychologicznej, w związkach operacyjnych – wydziały obrony psychologicznej, a w związkach taktycznych – grupy obrony psychologicznej. Dodatkowo w jednostkach wojskowych utworzono etaty zastępców dowódców ds. wychowawczych, jednakże ich zadania uległy zasadniczej zmianie. Oficjalne źródła rosyjskie podkreślają, że głównym zadaniem oficerów wychowawczych jest obrona psychologiczna wojsk własnych, czemu ma sprzyjać zwiększenie zapotrzebowania rosyjskich sił zbrojnych na psychologów wojskowych.

Zgodnie z obowiązującymi w rosyjskich siłach zbrojnych ustaleniami, działanie tych pododdziałów w warunkach bojowych jest prowadzone w ścisłej koordynacji z działaniami grup specjalnych (w tym dywersyjnych), grup rozpoznawczych oraz służbami prasowymi, itp.



Rys. 3.4.1. Struktura sił działań psychologicznych SZ FR

Rosjanie przeanalizowali dokładnie doktrynę działań informacyjnych Stanów Zjednoczonych i zamierzają zrealizować następujące przedsięwzięcia:

— zapewnić zrozumienie teoretycznej koncepcji działań informacyjno-psychologicznych;

— stworzyć na bazie istniejącego aparatu działań psychologicznych i propagandy, organa działań informacyjno-psychologicznych, które mogłyby być wykorzystane zarówno w czasie pokoju, kryzysu, jak i wojny;

— włączyć struktury zaangażowane w prowadzenie działań informacyjno-psychologicznych do struktur kontrolno-decyzyjnych sił zbrojnych Rosji;

— planować i prowadzić ćwiczenia wojskowe, gry decyzyjne i treningi sztabowe z wykorzystaniem tych struktur na wszystkich szczeblach dowodzenia.

Rosjanie bardzo poważnie traktują sprawy związane z prowadzeniem działań informacyjnych, dlatego też rozpoczęli formowanie osobnej specjalności w ramach rosyjskich sił zbrojnych, rekrutujących specjalistów w sztuce zbierania i oddziaływania informacyjnego. Nieutworzenie nowej specjalności może być niebezpieczne, ponieważ, jak zauważają specjaliści, dużo gorzej jest pozostać w tyle w dziedzinie konfrontacji informacyjno-psychologicznej niż w dziedzinie cybernetyki. Nierozwiązanie problemu informacyjno-psychologicznej konfrontacji czyni niemożliwą konsolidację społeczeństwa i stabilizację sytuacji w państwie.

3.5. Efekty poznania

1. Technologia informacyjna umożliwia chirurgiczną dokładność lokalizacji obiektów oraz szybki, niezakłócony przekaz danych, a ponadto ułatwia manipulację treściami informacyjnymi w taki sposób, że przeciwnik otrzymuje niepełny lub fałszywy obraz sytuacji. Zostaną mu przekazane nieużyteczne dane, które będą go wprowadzać w błąd. W ten sposób „głuchy" i „ślepy" przeciwnik szybko będzie zmuszony do zaniechania swoich zamiarów. W coraz większym stopniu nowoczesne technologie wykorzystuje się podczas przekazywania danych w systemach dowodzenia, które są zdolne do pracy na dużych odległościach, ze względu na stosowanie łączy satelitarnych. Zwalczając i niszcząc nowoczesne, na wysokim poziomie technologicznym, systemy uzbrojenia przeciwnika, będzie się w przyszłości zwracać mniejszą uwagę na ich konwencjonalne, fizyczne zniszczenie, natomiast większą – na obezwładnienie systemów oprogramowania i zminiaturyzowanych układów. Konstruktorzy uzbrojenia zastanawiają się nad tym, aby podczas produkcji systemów broni instalować odpowiednie układy, które w określonych sytuacjach, np. przy eksporcie do innych krajów, mogłyby umożliwiać zmniejszenie ich skuteczności, np. udaremnić start rakiety, zmienić jej kurs podczas lotu lub zablokować detonator głowicy bojowej po starcie. W ten sposób pociski rakietowe nigdy nie trafiłyby do celu, ponieważ urządzenia nawigacyjne, komputery pokładowe (wypracowujące tor lotu lub zamontowane na środku przenoszenia), czujniki wszelkiego typu byłyby niezdolne do właściwego funkcjonowania.

2. Korzystając z nowych technologii, należy brać pod uwagę fakt ich zastosowania przez przeciwnika. Dlatego też trzeba rozważyć możliwości i granice osiągnięć technicznych. Zaczyna się to od zastosowania symulacji komputerowych w szkoleniu

i treningach. Zbliżone do rzeczywistości interakcyjne przedstawianie symulacji pola walki umożliwia nie tylko zaoszczędzenie środków finansowych w szkoleniu, lecz także wypróbowanie nowych scenariuszy i taktyk działania bez szkód lub strat w ludziach i sprzęcie. Dowodzący mają możliwość na podstawie istniejących danych o siłach własnych i przeciwnika, używając sztucznej inteligencji i systemów eksperckich, sprawdzić czy w konkretnym starciu zbrojnym istnieją szanse na powodzenie. Zdobycze techniki informacyjnej nabierają znaczenia w symulacjach komputerowych.

3. Sytuacja ta powoduje, że projekt struktury sił zbrojnych XXI wieku powinien uwzględniać znacznie mniejszą armię, składającą się z oddziałów (formacji) o większej manewrowości i większej skuteczności rażenia niż siły zbrojne miały w przeszłości. Dlatego też wiele państw na świecie dokonuje transformacji sił zbrojnych i tworzy struktury XXI wieku.

4. Struktury do prowadzenia działań informacyjnych zorganizowano we wszystkich rodzajach sił zbrojnych USA. 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.

5. Rosja jest szczególnie zainteresowana rozwojem i wdrażaniem środków działań informacyjno-psychologicznych przez światowe potęgi. Działania informacyjne mają poważne implikacje dla Rosji i to zarówno w technicznym, jak i moralno-psychologicznym aspekcie. Rosjanie wskazują, że informacyjne bezpieczeństwo jednostki i całego społeczeństwa jest jednym z priorytetów interesu narodowego. Armia rosyjska jest szczególnie zainteresowana wpływem działań informacyjno-psychologicznych na swoich żołnierzy – co wynika z doktryny wojennej. Należy oczekiwać, że rosyjska armia będzie gotowa do prób wykorzystania działań informacyjnych przeciw żołnierzom innych krajów.

6. Zależność wysoko uprzemysłowionych społeczeństw od systemów informacyjnych wykorzystywanych praktycznie we wszystkich płaszczyznach życia publicznego (w energetyce, w transporcie, na polu gospodarki i finansów, a także w komunikacji) i wojskowego daje potencjalnym przeciwnikom, ale także terrorystom i kryminalistom, liczne możliwości ingerencji. Na pewno w przyszłych konfliktach należy liczyć się z tym, że strona rozpoczynająca konflikt będzie paraliżować systemy informacyjne drugiej strony. Oznacza to, z jednej strony, że własne systemy muszą być przed tego rodzaju ingerencją chronione oraz, z drugiej strony, że własne siły powinny mieć możliwość zastosowania podobnych środków, aby chronić życie ludności i środki

własne. Społeczeństwo, które nie ma świadomości tego zagrożenia i nie czyni przygotowań do obrony, może zostać całkowicie zdezorganizowane za pomocą narzędzi działań informacyjnych.

4. ISTOTA DZIAŁAŃ INFORMACYJNYCH

4.1. Kwestie terminologiczne i klasyfikacyjne

W porozumiewaniu się, szczególnie językami profesjonalnymi, często są używane terminy dwuczłonowe, składające się z wyrazu podstawowego i z wyrazu dopełniającego. Łączność ich stosowania zmierza do konkretyzacji desygnatów wyrazów podstawowych.

W strukturze złożonego terminu działania informacyjne zasadniczym determinantem rzutującym na całokształt przedmiotu myślowego, jest wyraz „działania". Wyrazem dopełniającym jest natomiast ich rodzaj (charakter) określony mianem „informacyjne".

Przyjmując to za zasadę semantyczną, można dedukować, że desygnat określenia „działania informacyjne" powinien mieścić w swoim zbiorze przedmiotowym wszystkie te elementy, które są właściwe wyrazom: „działania" i „informacja".

Działania – zdaniem wielu autorów[44] – to celowe i świadome zachowania się ludzkie. T. Pszczołowski[45] twierdzi, że jeśli celowość działania zakłada świadomość i dowolność zachowania się, wystarcza określenie, że działanie jest zachowaniem się celowym

Według A. Schutza termin działanie określa ludzkie postępowanie jako bieżący proces, który jest podejmowany przez człowieka zawczasu. Trzeba mieć zamysł, koncepcję, zanim zacznie się działać. Wyróżnił także dwa podstawowe aspekty odpowiedzialności: za to co się robi (aspekt czysto subiektywny) i przed kimś (aspekt indywidualny)[46].

Z powyższych definicji wynika, że cechą definicyjną ludzkiego działania jest celowość. Jeśli zachowanie człowieka miało cel, to było działaniem, a ów człowiek był podmiotem działania. Cele może przypisywać swojemu działaniu sam podmiot (aspekt subiektywny), nad celami zachowania jakiegoś człowieka może się zastanawiać inny człowiek, czyli obserwator (aspekt obiektywny). Celem jest to, do czego dąży podmiot działania (subiektywnie i/lub obiektywnie). Środkiem zaś jest to, za pomocą czego

[44] A. Czerminski, M. Czerska, B. Nogalski, R. Rutka, *Organizacja i zarządzanie*, Gdańsk, Wydawnictwo Uniwersytetu Gdańskiego, 1994, s. 20.

[45] T. Pszczołowski, *Mała encyklopedia parakseologii i teorii organizacji.* Zakład Narodowy im. Ossolińskich, Wrocław-Warszawa-Kraków-Gdańsk, 1978, s. 56.

[46] A. Schutz, *Common-Sense and Scientific Interpretation of Human Action.* Philosophy and Phenomenological Research 14, Collected Papers III: Studies in Phenomenological Philosophy, Vienn, 1953, s. 3–47.

podmiot osiąga cel. Z tego względu można twierdzić, że środki są wtórne wobec celów (przynajmniej definicyjnie).

Działanie ma swoją historię, czyli rozpoczyna się, zmienia i kończy. Ta cecha działania wykorzystywana jest do dzielenia go na chronologicznie uporządkowane etapy, np. zidentyfikuj problem, poszukaj rozwiązania, zastosuj rozwiązanie, sprawdź czy nie popełniłaś błędu.

Najogólniej działanie można oceniać ze względu na jego efekty (stanowisko takie nazywane jest konsekwencjalizmem) lub ze względu na intencje podmiotu – intencjonalizmem. Przypisanie działaniu efektów, a podmiotowi intencji nie jest ani proste, ani łatwe.

Można argumentować, że intencjonalizm jest konsekwencjalizmem *ex ante*, czyli ocenianiem działania ze względu na efekty, jakie zamierzał osiągnąć podmiot przed jego podjęciem. Konsekwencjalizm *ex post* polega na ocenianiu działania ze względu na efekty, które zostały osiągnięte. Myślenie prawdziwie niekonsekwencjonalistyczne byłoby ocenianiem działania bez względu na zamierzone lub zrealizowane efekty.

Teorią działania zajmuje się prakseologia (praxeology) – nauka o sprawnym działaniu, formułująca zasady postępowania odnoszące się do wszelkich form świadomego i celowego działania, rozpatrywanego ze względu na kryterium sprawności. Prakseologia konstruuje i uzasadnia dyrektywy praktyczne, czyli zalecenia i przestrogi dotyczące podnoszenia sprawności i unikania niesprawności w działaniu. Prakseologia dotyczy wszelkich dziedzin ludzkiej działalności i można ją w sposób uproszczony nazwać nauką o dobrej robocie.

Prakseologia w Europie rozwinęła się w XIX wieku. Prekursorami prakseologii byli przedstawiciele różnych nauk: filozof M. Martin (1820–86), który swą naukę nazwał ponologią, filozof L. Bourdeau (1824–1900) i socjolog A. Espinas (1844–1922), którzy używali już nazwy prakseologia.

W Stanach Zjednoczonych – system prakseologii rozbudowywał L. Von Mises. (*Human Action. A Treatise on Economics,* New York, 1949).

Zdaniem L. von Misesa działanie ludzkie w odróżnieniu od automatycznej reakcji instynktownej zawiera elementy projektowania i jako takie z definicji jest racjonalne. Dlatego też stwierdził, że rzeczywisty przedmiot prakseologii, ludzkie działanie, wypływa z tych samych źródeł co ludzkie rozumowanie. Działanie i rozum są pokrewne i jednorodne, można je nawet określić jako dwa aspekty tego samego zjawiska. To, że

rozum ma możliwość wyjaśniania poprzez czyste rozumowanie istotnych cech działania, jest wynikiem tego, że samo działanie wynika z rozumu[47].

Kategorii rozumu i racjonalności L. von Mises nadaje sens pragmatyczny. Termin rozum i racjonalność odnoszą się do sądów o stosowalności i adekwatności zastosowanych procedur doboru środków służących do osiągania celów.

Jego zdaniem prakseologia odsłania racjonalność na płaszczyźnie ludzkiego działania, stosując kryterium skuteczności, natomiast ekonomia czyni to posługując się kategorią ekonomiczności.

Według L. von Misesa działanie jest to sposób w jaki człowiek reaguje na warunki otoczenia[48].

Jednak ekonomia i prakseologia nie może wyjaśnić całego fenomenu działania człowieka. Nie może też zachęcać do utrwalania i krzewienia idei rozumu, racjonalnego wyboru czy wolności. Dlatego tez, L. von Mises musi przyznać, jeśli nie racjonalnej etyce to liberalnej doktrynie politycznej funkcję mobilizującą do działań spełniających standardy racjonalności. W tym sensie liberalizm jest doktryną, która nie jest teorią lecz zastosowaniem teorii stworzonych przez prakseologię, a zwłaszcza ekonomię, dla określonych celów działania[49].

W Polsce prakseologią zajmował się T. Kotarbiński[50], który sformułował ogólną teorię skutecznego działania. W skład tej teorii wchodzą dwa zbiory tez, tj. opisowe i normatywne. Pierwsze z nich precyzują podstawowe pojęcia związane z prakseologią (np. czyn prosty, sprawca itp.), drugi zbiór tez, mówi o bezpośrednich warunkach i sposobach skutecznego działania.

Według T. Kotarbińskiego działanie to celowe, świadome i dowolne zachowanie się człowieka (jeżeli celowość zakłada świadomość i dowolność, wystarczy powiedzieć „celowe zachowanie się człowieka"). W refleksji nad działaniem używa się często pewnych charakterystycznych pojęć i schematów, mowa więc o jego:

— podmiotach (odpowiedź na pytanie kto działa?),

— obszarze, dziedzinie, sferze, kontekście,

— przedmiocie, adresatach (na co, na kogo oddziałujemy?),

— celach, motywach, zamierzeniach, intencjach,

---

[47] L. von Mises, *Ludzkie działanie. Teoria ekonomii.* [w] *Prakseologia* 3-4, 1995, s.55.
[48] Tamże, s. 115.
[49] Tamże, s.176.
[50] Kotarbiński T., *Szkice praktyczne*, Warszawa, 1913; Ibidem, *Prakseologia. Część 1*, Ossolineum, 1999; Ibidem, *Traktat o dobrej robocie*, Wrocław, 1982; Ibidem, *Medytacje o życiu godziwym*, Warszawa, 1985.

— przyczynach, uwarunkowaniach (np. te czynniki, które wpływają na przebieg działania, ale są niezależne od podmiotu),
— środkach, narzędziach, instrumentach, metodach, sposobach,
— programach, planach, strategiach, taktykach,
— normach, zasadach, regulacjach,
— efektach, skutkach, wynikach, rezultatach, wytworach,
— celowości, skuteczności, efektywności, słuszności, sprawności, ekonomiczności, korzystności, kosztowności, zyskowności, wykonalności, użyteczności, racjonalności, moralności;
— rodzajach.

Zdaniem T. Kotarbińskiego ludzkie działanie jest determinowane wieloma jeszcze czynnikami o charakterze: ekonomicznym, społeczno-kulturowym i osobistym. Każdy z tych czynników można uwzględnić w procesie decyzyjnym i to na drodze racjonalnej kalkulacji. Oczywiście można tego dokonać w stopniu na jaki pozwala sama specyfika płaszczyzny rozważań.

Według utartych schematów interpretacyjnych historii filozofii, twórczość T. Kotarbińskiego, zostaje zaliczona tradycyjnie do prakseologii. Często też jego etyka niezależna rozpatrywana jest bez prakseologicznego kontekstu.

Wydaje się, że przedsięwzięcie jedynie samodzielnego rozpatrywania pism prakseologicznych stanowi zabieg nie do końca uprawniony. Może bowiem sugerować, co jest niezgodne z intencjami T. Kotarbińskiego, że prakseologia określa właściwą, w sensie wystarczającą, płaszczyznę na której należy rozważać działania ludzkie.

Dla T. Kotarbińskiego nie było ważne tworzenie formalnej wiedzy o strukturze ludzkiego działania w oderwaniu od problematyki etycznej i felicytologicznej. Chodziło mu raczej o znalezienie recepty na mądrość życiową. Etyka w najszerszym tego słowa znaczeniu ogólna, postulowana mądrość życiowa, obejmuje (zdaniem T. Kotarbińskiego), wszystkie te działy (dotyczące: szczęścia, sumienia i sprawności). Etyka rozumiana w węższym znaczeniu pozostawia poza swoim obrębem kwestie sprawnościowe, przekazując je osobnej dyscyplinie, zwanej prakseologią, sama zaś ogranicza się do spraw szczęścia i spraw sumienia. Wreszcie etyka rozumiana w węższym znaczeniu skupia się na problemach niepokojących sumienie. Tak rozumianą etykę można nadal w tym wypadku nazywać etyką, albo etyką w najściślejszym znaczeniu. Jeśli mowa o dziale dotyczącym

szczęścia to nie ustaliła się nazwa ogólnie przyjęta dla tego działu zagadnień. Niektórzy zalecają nazywać tę dyscyplinę felicytologią[51].

Tak, więc czyn, który należy podjąć ma swój walor techniczny i organizacyjny określony kryterium skuteczności. Charakteryzują go moralne wybory dokonywane w trakcie doboru celów i środków działania. Z kolei moralne aspekty działania wyznaczają stopień dopuszczalności czynu.

W literaturze przedmiotu osoby i instytucje podejmujące działania określane są umownym terminem „sprawca". Rozróżnia się działania permutacyjne, których celem jest uzyskanie zmian obiektu oddziaływań. W ramach tej kategorii wyodrębnia się czynności konstrukcyjne i destrukcyjne. Z czynnością konstrukcyjną mamy do czynienia wtedy, gdy obiekt oddziaływań zyskuje nową cechę, a z destrukcyjną wówczas, gdy traci swoją dotychczasową cechę.

Odmienne efekty uzyskiwane są przy stosowaniu działań określanych mianem perseweracyjnych. Działania perseweracyjne charakteryzują się tym, że obiekt oddziaływań zachowuje swoje dotychczasowe cechy. W ramach tej kategorii działań wyróżniane są czynności konserwacyjne i profilaktyczne.

Czynność konserwacyjna zmierza do tego, aby obiekt oddziaływań nie utracił posiadanej cechy, a profilaktyczna do tego, aby obiekt oddziaływań nie nabył cech, których nie posiadał przed podjęciem działania.

Z punktu widzenia socjotechniki wyróżnia się trzy rodzaje postępowania: reformujące, projektujące i profilaktyczne. O tym, kiedy i jaki rodzaj postępowania powinien być wdrożony decyduje ocena aktualnego i przewidywanego stanu rzeczy, wieńcząca etap wstępnego rozpoznania.

Postępowanie reformujące rekomendowane jest, gdy dostrzega się potrzebę zmiany aktualnego stanu rzeczy, a jego negatywnie oceniane elementy są efektem uprzednich, nieskutecznych działań zaradczych.

Postępowanie projektujące podejmowane ma być w celu stworzenia takiego stanu rzeczy, który jest pożądany, a który aktualnie nie istnieje.

Natomiast *postępowanie profilaktyczne* zalecane jest przypadku, gdy przewidywany kierunek rozwoju aktualnego stanu rzeczy oceniany jest negatywnie. Postępowanie profilaktyczne ma na celu zapobieganie takim niekorzystnym stanom rzeczy, które mogą dopiero zaistnieć w przyszłości.

---

[51] T. Kotarbiński, *Medytacje o życiu godziwym*, Warszawa 1985, .s. 13.

W propozycji socjotechniki profilaktyka jest jedną z procedur ingerowania w rzeczywistość społeczną i świadomego kształtowania rozwoju tej rzeczywistości w pożądanym kierunku.

Ogólna teoria działania przyjmuje trzy podstawowe kryteria oceny działania: skuteczność, ekonomiczność, korzystność. Pierwszy walor sprawnego działania odnosi się do stopnia osiągnięcia celu, drugi do stosunku efektów użytkowych do nakładów koniecznych do ich uzyskania, trzeci do różnicy pomiędzy efektami użytkowymi a nakładami koniecznymi.

Ocena działania powinna być wielokryterialna, natomiast współczesne rozumienie efektywności to prakseologiczna ekonomiczność. Tym problemem aktualnie zajmują się nauki o organizacji i zarządzaniu. Ze względu na to, że są one ściśle związane z dorobkiem prakseologii to trzeba uznać, iż efektywność stanowi ilościową cechę działania, odzwierciedloną w relacji efektów użytkowych uzyskanych w pewnym czasie i zmierzających do zaspokojenia potrzeb odbiorcy (pośredniego i końcowego) oraz nakładów (zasobów) koniecznych do osiągnięcia tego efektu, poniesionych w pewnym czasie.

Za element wyjściowy w analizie pojęcia skuteczność należy uznać teorię prakseologii, która jako ogólna teoria sprawnego działania wyprowadza ogólne zasady, które służyć mogą albo jako kryteria ocen organizacji działań, albo jako wskazania czy wytyczne do usprawnienia organizacji działań. W literaturze przedmiotu przyjęto powszechnie, że skuteczność jest najważniejszą z trzech głównych cech charakteryzujących sprawność działania[52].

T. Kotarbiński określa jako działanie skuteczne, takie, które prowadzi do skutku zamierzonego jako cel. W tym znaczeniu skuteczność jest stopniem osiągnięcia celu albo umożliwienia lub ułatwienia jego osiągnięcia. Zdaniem J. Zieleniewskiego[53] oceną skuteczności można posługiwać się do porównywania ze sobą tylko wariantów działań stanowiących łącznie „rodzinę działań", czyli zbiór wariantów w różny sposób zmierzających do takich samych lub bardzo podobnych celów.

---

[52] Skrzypek E., *Jakość i efektywność*, Wydawnictwo Uniwersytetu Marii Curie – Skłodowskiej, Lublin 2000, s. 215.

[53] Zieleniewski, J. *Organizacja i zarządzanie*. Warszawa, PWN 1974; Ibidem, *Organizacja zespołów ludzkich*, Warszawa, PWN,1972.

Szczególną rolę skuteczności podkreśla W. Kieżun[54] pisząc, że działanie, które może być uznane za sprawne w znaczeniu ogólnym, musi być choć w minimalnym stopniu skuteczne. Bez tego inne walory sprawności nie odgrywają żadnej roli

Należy także rozróżnić dwie kategorie: skuteczność działania i skuteczność *sensu stricte*. Przez skuteczność działania rozumie się stopień realizacji celu, jakim to działanie miało się zakończyć, bez uwzględniania jego aspektów ekonomicznych. Dane działanie uważa się ze bardziej skuteczne niż inne, o ile lepiej zbliżyło ono działającego do wytkniętego celu[55].

Skuteczność określana jest jako stosunek wyrażony liczbą bezwymiarową:

$$S = W/P$$

gdzie:

S – skuteczność,

W – osiągnięty rezultat (wynik) działania,

P – założony rezultat (cel) działania.

Inne podejście do pojęcia skuteczności prezentuje P. Sienkiewicz[56] mówiąc o skuteczności systemu. Jest to taka cecha systemowa, która wyraża zdolność systemu do działania prowadzącego do skutku zmierzonego jako cel końcowy danego działania. Miernikiem tak pojmowanej skuteczności jest stopień osiągnięcia głównego celu systemu[57].

Wielkość zapotrzebowania na poszczególne zasoby oraz na działania jest istotną informacją. Wpływa bowiem na końcową efektywność działań i łańcuchów tych działań. Funkcjonowanie rachunku kosztów działań jest uwarunkowane dostępnością tych miar.

Korzystając przede wszystkim z metodologii i pojęć wypracowanych w prakseologii i teorii systemów, można określić łańcuch, układ i system działania.

Łańcuch działania $Ł$ tworzą: podmiot działania – p, pośrednik działania – q, przedmiot działania – r. Zatem jest to trójka uporządkowanych elementów:

$$Ł = < \pi, \theta, \rho > (1)$$

---

[54] Kieżun W., *Podstawy organizacji i zarządzania*, Książka i Wiedza, Warszawa 1977, s. 50.

[55] Zieleniewski J., *Efektywność badań naukowych*, PWE, Warszawa 1966, s.26; Sobolewski K., *O pojęciu skuteczności i pojęciach związanych*, op. cit., s.132.

[56] Sienkiewicz P., *Teoria efektywności systemów*, Wydawnictwo Polskiej Akademii Nauk, Warszawa 1987, s. 58.

[57] Sobolewski K., O pojęciu skuteczności i pojęciach związanych, op.cit., s.133.

Każdy łańcuch działania przedstawia działanie celowe, gdzie podmiotem działania (*p*) jest zawsze człowiek, pośrednikiem działania (*q*) są obiekty materialne zdolne do wykonywania określonych funkcji, zaś przedmiotem działania (*r*) są obiekty finalne. Obiekty finalne więc kształtowane są za pomocą pośrednika, którym kieruje podmiot działania, tj. człowiek.

Układ działania *U*, stanowi elementarny model prakseologiczny złożony z dwóch uporządkowanych elementów: stanowiska działania *w* i obiektu działania *v*, co można zapisać następująco:

$$U = < w, v > (2)$$

W układzie działania stanowisko działania w składa się z podmiotu działania (*p*), pośrednika działania (*q*), tj. $w = < p, q >$, a obiekt działania (*v*) jest przedmiotem działania (*r*), tj. $v = r$. Uwzględniając powyższe oznaczenia, zapis (2) można przedstawić następująco:

$$U = << p, q >, r > (3)$$

Uwzględniając łańcuch działania *Ł*, opisany wyrażeniem (1), i układ działania *U*, przedstawiony zależnością (3), można utworzyć jeszcze dwa dalsze elementarne układy działania, zapisując je ogólnie następująco:

$$U^* = << p, r >, q > (4)$$

$$U^{**} = < p, < q, r > > (5)$$

W teorii systemów, modele prakseologiczne typu (3) przyjęto nazywać układami obsługi, modele typu (4) – układami użytku, zaś modele typu (5) – układami kierowania (zarządzania).

System działania *Sd* kształtuje elementarny model działania złożony z następującej pary uporządkowanej:

$$Sd = < Ur, L > (6)$$

gdzie: Sd – system działania,

Ur – rodzina wyróżnionych układów działania,

L – struktura systemu.

Każdy system działania ma określony cel, którego nośnikiem jest co najmniej jeden podmiot w nim występujący. Podstawowym warunkiem sprawnego działania organizacji jest wymiana informacji pomiędzy poszczególnymi jej uczestnikami. Dlatego niezbędne jest posiadanie pewnych unikalnych umiejętności, które umożliwią jej członkom współpracę w systemie.

Po pierwsze niezbędna jest znajomość narzędzi informacyjnych wchodzących w skład globalnego systemu wykorzystywanego przez organizację. System ten musi być podłączony do internetu, który umożliwi komunikację w wymiarze światowym. Poza tym musi posiadać bazę danych umieszczoną na serwerze, do której dostęp będą mieli wszyscy uczestnicy. Interfejsem użytkownika powinien być portal korporacyjny, który może być wykorzystywany jako forum informacyjne i dyskusyjne oraz jako miejsce dostępu do pozostałych niezbędnych narzędzi informatycznych.

Po drugie bardzo ważny jest sposób prowadzenia dialogu pomiędzy uczestnikami organizacji. Niezbędne jest posiadanie umiejętności jasnego i logicznego wyrażania sądów i opinii przy wykorzystaniu mechanizmów wirtualnych. Komunikacja prowadzona w ten sposób jest dosyć specyficzna i wymaga szczególnej uwagi przy formułowaniu wypowiadanych sądów.

Po trzecie system komunikacji w organizacji musi rozwiązywać kwestie związane z prowadzeniem wymiany informacji o charakterze niespersonalizowanym. Pozwoli to przygotować partnerów do tego, że nie będą oni mogli wyciągać wniosków na temat dyskutowanych problemów na podstawie sposobu zachowania partnera, jego wyglądu zewnętrznego, mowy ciała i bodźców pozawerbalnych. Stwarza to jednak sporą trudność członkom grupy, ponieważ przekazy te są uboższe i wymagają większego wysiłku przy próbie ich interpretacji. Dlatego tak ważne jest niedopuszczenie do sytuacji, w której odbiorca skupia się na tym, co autor komunikatu miał na myśli, a nie, co tak naprawdę dana informacja wnosi do sprawy. W skrajnych sytuacjach może to, bowiem spowodować całkowitą dezorganizację pracy grupy.

Niezbędnym atrybutem każdej organizacji powinien być system informacyjny. Wcześniejsze jego zaprojektowanie pozwoli dostosować umiejętności poszczególnych członków grupy od ogólnie panującego standardu. Zagrożenia wynikające z braku odpowiednio przygotowanego systemu informacyjnego są bardzo duże. Wynikają one między innymi z tego, że komunikacja jest jedynym „naocznym świadectwem" istnienia organizacji. Poza tym przygotowanie odpowiednich procedur regulujących wymianę informacji jest niezwykle istotne z punktu widzenia skuteczności jej działania.

Podsumowując dotychczasowe rozważania należy stwierdzić, że zorganizowane działanie towarzyszy człowiekowi od chwili jego powstania, już bowiem człowiek pierwotny, posługujący się maczugą podczas polowania na dzikiego zwierza – musiał takie polowanie odpowiednio zorganizować.

Poszukiwanie przez człowieka większej sprawności działań nabrało szczególnego

znaczenia, gdy cele, które człowiek zmuszony był realizować, stawały się coraz bardziej złożone i trudne.

Aktualnie przez działania rozumie się układ intencjonalnych czynności, których celem jest przystosowanie się do otoczenia lub zmiana tego otoczenia[58]. Wszelka działalność opiera się na:

— wyznaczeniu celu działania;

— ustaleniu warunków realnych tego działania;

— wyborze środków adekwatnych zarówno do celu, jak do warunków danej rzeczywistości.

Dziś działania człowieka znacznie się skomplikowały, gdyż wdrażane są nowe złożone technologie, nowe maszyny i urządzenia, które wymagają szerszej wiedzy, umiejętności i doświadczeń.

Dlatego też L. J. Krzyżanowski twierdzi, że współcześnie terminu działań nie można odnosić tylko do człowieka, tym bardziej, że są już skonstruowane przez ludzi urządzenia techniczne, które nie tylko, że działają samoczynnie, to dokonują także wyboru sposobów działania zmierzających do osiągnięcia określonego celu.

Zdaniem L. J. Krzyżanowskiego poziomem odniesienia w tym zakresie powinny być organizacje, które są tworzone przez ludzi. W ich skład wchodzą dwa komponenty:

— bytu realnego (rzeczy),

— oddziaływania.

Istnienie (trwanie, rozwój organizacji) polega na działaniu, to zaś jest uwarunkowane przez interakcje z otoczeniem, gdyż, z jednej strony, z owych segmentów otoczenia dobierane są – stosownie do przyjętej domeny działalności organizacji – realne, aktywne lub warunkujące działanie składniki organizacji, z drugiej zaś strony, właśnie na rzecz otoczenia wytwarzane są w organizacji dobra lub świadczone usługi materialne bądź niematerialne.

Twórcami – założycielami całości zorganizowanego działania, które jest obiektem badań nauk o kierowaniu nim, są ludzie.

Tworzywem całości zorganizowanego działania jest otoczenie, które obejmuje trzy segmenty: społeczny, naturalny i sztuczny.

---

[58] R. Smolski, M. Smolski, E. H. Stadtmüller, *Słownik encyklopedyczny edukacja obywatelska*. Warszawa, Wydawnictwa Europa, 1999.

L. J Krzyżanowski do otoczenia naturalnego zalicza wytwory przyrody określone geofizycznie, biofizycznie, astrofizycznie i psychobiofizycznie.

Do otoczenia społecznego – wytwory natury o cechach socjopsychobiofizycznych, czyli ludzi.

Do otoczenia sztucznego – materialne wytwory człowieka (urządzenia techniczne oraz technologie).

Całości zorganizowanego działania, których częściami składowymi są dobrane z otoczenia społecznego, naturalnego i sztucznego konkretne, rzeczowe, zdolne do działania lub warunkujące działania komponenty zespolone wzajemnymi oddziaływaniami materialnymi, energetycznymi oraz informacyjnymi, jako kolektywne zbiory istnieją realnie, czyli rzeczywiście.

W zależności od domeny działań i sposobu, czyli technologii działania, udział osobowych, naturalnych i sztucznych rzeczowych „nośników działań" bywa w danej części zorganizowanego działania , bądź w określonych typach działań bardzo różny.

Zgodnie z koncepcją ontologiczną przez podmioty działania należy rozumieć wszelkie konkretne rzeczowe składniki bytu (osobowe, naturalne, aparaturowe), które mają zdolność do działania.

Istnienie, (trwanie i rozwój organizacji) polega na działaniu, to zaś uwarunkowane jest przez interakcje z otoczeniem społecznym, naturalnym i sztucznym.

Całości zorganizowanego działania są przedmiotem badań wielu nauk (psychologii, socjologii, nauk ekonomicznych, politycznych i prawnych, technicznych, rolniczych i innych), przy czym ich zainteresowania dotyczą sfery działalności podstawowej, czyli tego co nazywa się domeną lub domenami. Niektórzy nazywają to „funkcją genotypową:, czyli funkcją lub misją, do której realizacji określone organizacje zostały powołane.

L. J. Krzyżanowski, biorąc pod uwagę przeszłe rezultaty w działaniach wyróżnia: zamierzenie, cel i zadanie.

Zamierzenie jest to określony przedmiotowo, przyszły, pożądany stan rzeczy, którego osiągnięcie wydaje się możliwe w jakiejś bliżej nie sprecyzowanej perspektywie czasu[59].

Cel jest to określony przedmiotowo i podmiotowo, przyszły, pożądany stan rzeczy, możliwy i przewidziany do osiągnięcia w określonym przedziale czasu lub terminie.

---

[59] L. J. Krzyżanowski, *O podstawach kierowania organizacjami inaczej,* warszawa, PWN, 1999, s. 253.

Zadanie jest to wyodrębniona przedmiotowo, podmiotowo, przestrzennie, czasowo i na ogół też proceduralnie część celu przewidziana do wykonania w ustalonym okresie lub terminie, mieszczącym się w przedziale czasu przewidzianym na osiągnięcie celu.

Zdaniem L. J. Krzyżanowskiego pojęcie „działania" było niewłaściwe interpretowane. Z jednej strony odnoszono to pojęcie tylko do ludzi, z drugiej strony czynności urządzeń określano jako funkcjonowanie, podczas gdy działanie jest kategorią *par excellence* przyrodniczą w najszerszym rozumieniu terminu przyroda – fizycznym, biofizycznym i psychobiofizycznym.

T. Kotarbiński przyjął podział filozofii zgodnie z poglądami Arystotelesa na teoretyczną – ontologia i epistemologia (gneseologia) oraz praktyczną – etyka i polityka. Już w pierwszej jego pracy, *Szkice praktyczne* (1913), podobnie jak i we wszystkich późniejszych dziełach, rozprawach, esejach, aż do ostatnich, termin „praktyczne" oznacza „etyczne".

To, że przez etykę rozumiał filozofię praktyczną, wyraził *expressis verbis* w referacie na Kongresie Filozoficznym w Amsterdamie (sierpień 1948). Etyka inaczej zwana filozofią praktyczną obejmuje trzy działy: naukę o życiu szczęśliwym, naukę o praktyczności działań oraz naukę o tym, jak trzeba żyć, aby zasłużyć na miano porządnego człowieka. Jako etyk interesował się on głównie działaniem człowieka, nie negował jednak działania przyrody.

Uogólniając powyższą analizę, można określić, że „działania" to zespół zsynchronizowanych przedsięwzięć prowadzonych dla osiągnięcia zamierzonego celu (w określonej przestrzeni) z użyciem specyficznych narzędzi według ustalonych reguł.

Dalsze konkretyzowanie działań wynikać będzie z zawężania:

— przestrzeni lokalizacji celu (środowisko informacyjne);

— narzędzi użytych do ich prowadzenia (narzędzi informacyjnych);

— sposobów wykorzystywania tych narzędzi w konkretnych przedsięwzięciach.

Ważnym aspektem prowadzenia jakichkolwiek działań jest planowanie. Według J. Zieleniewskiego planowanie działań to obmyślenie środków i sposobów działania, dostosowanych zarówno do celów, jak i do warunków; albo inaczej: organizowanie toku działań[60].

[60] J. Zieleniewski, *Organizacja i zarządzanie*, Warszawa, PWN, 1975, s. 207-208.

A. Bilska i R. Flasza planowanie działań definiują jako ustalenie celów i wynikających z nich zadań oraz ustalenie środków i metod, jakimi powinny być zrealizowane[61].

Według K. Zimniewicza planowanie, jako funkcję zarządzania, można sprowadzić do określenia przyszłych relacji między warunkami i środkami działania oraz do wyznaczania celów wynikających z zachodzących relacji[62].

L. J. Krzyżanowski stwierdza, że: najistotniejszą treścią funkcji planowania jest formułowanie celów organizacji i niezbędnych do tego zasobów[63]. Natomiast zdaniem B. Kuca planowanie jest to określanie celów i sposobów ich realizacji[64]. Nawet można pokusić się o następujące porównanie: plany stanowią „mapy drogowe", według których organizacje podążają ku swoim celom.

W amerykańskiej literaturze planowanie widziane jest podobnie jak w polskiej. J. Stoner, R. Freeman i D. Gilbert uważają, że planowanie w organizacjach jest procesem ustalania celów i wybierania środków do ich osiągania[65].

Inni amerykańscy autorzy S. Robbins i D. DeCenzo[66] podają, że planowanie obejmuje definiowanie celów organizacji, określenie ogólnej strategii ich osiągania oraz opracowanie zwartej hierarchii planów służących do integracji i koordynacji działań. Stąd wynika wniosek, że dotyczy ono celów (co ma być zrobione) i środków (jak to ma być zrobione).

W niemieckiej teorii zarządzania planowanie ujmowane jest jako: myślowa antycypacja (teoretyczne przewidywanie, zakładanie przebiegu) przyszłych zdarzeń, racjonalne przygotowanie i podejmowanie decyzji zorientowanych na przyszłość oraz określających przebieg procesów w organizacji jako całości i we wszystkich jej częściach. Jest to zaprojektowanie przemyślanego, systemowego i celowego porządku, według którego powinny być realizowane przyszłe zjawiska w organizacji. Zatem zasadniczymi cechami planowania są zorientowanie na przyszłość i racjonalność[67].

Podsumowując dotychczasową analizę można uogólnić, że planowanie jest procesem ustalania celów (tego, co ma być zrobione) i wybierania sposobów, środków

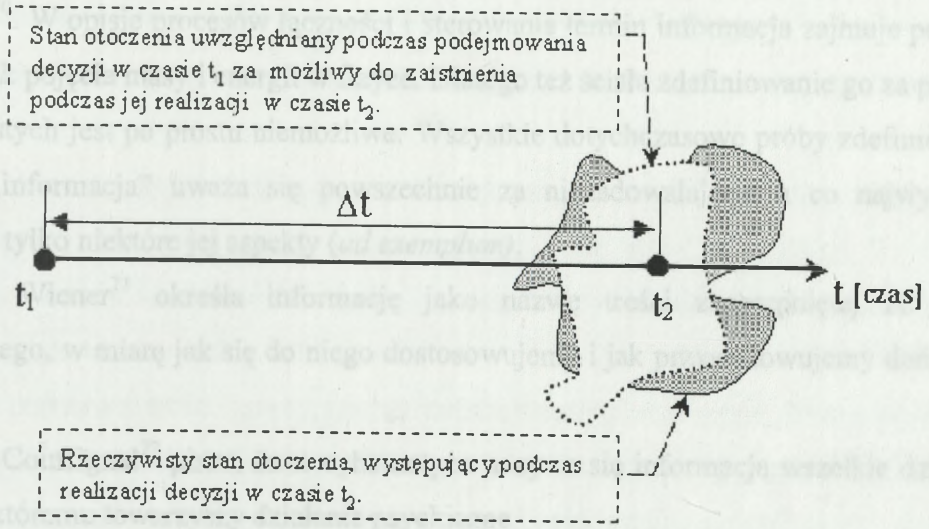
---

[61] A. Bilska, R. Flasza, *Organizacja i metody pracy społecznej w przedsiębiorstwach*, Warszawa, KiW, 1978, s. 128.
[62] K. Zimniewicz, *Nauka o organizacji i zarządzaniu*, Warszawa, PWN, 1990, s. 125.
[63] L. Krzyżanowski, *Podstawy nauk o organizacji i zarządzaniu,* Warszawa, PWN,1992, s. 211.
[64] B. Kuc, *Zarządzanie doskonałe*, Warszawa, Wyd. PTM, 2000, s. 95.
[65] J. Stoner, R. Freeman, D. Gilbert, *Kierowanie*, Warszawa, PWE, 2001, s. 263.
[66] S. Robbins, D. DeCenzo, *Podstawy zarządzania*, Warszawa, PWE, 2002, s. 131.
[67] P. Trybała, *Skuteczne kierowanie i organizowanie*, Rzeszów, FOSZE, 2001, s. 84.

osiągania tych celów (jak to ma być zrobione). Plany stanowią "mapy drogowe", według których organizacje podążają ku swoim celom.

Plany wyznaczają cele organizacji i określają najlepsze procedury ich realizacji. Ponadto plany są wytycznymi, dzięki którym: 1) organizacja uzyskuje i przydziela środki potrzebne do realizacji celów, 2) członkowie organizacji działają zgodnie z wybranymi celami i procedurami, 3) sprawdza się i mierzy postępy w realizacji celów, tak by można było podjąć działania korygujące, jeżeli postępy te są niedostateczne. Zatem planowanie nie jest jednostkowym zdarzeniem, o wyraźnym początku i końcu. Jest ono ciągłym procesem, stanowiącym odbicie zmian, zachodzących w otoczeniu każdej organizacji, i dostosowującym się do tych zmian.

Jednym z najważniejszych elementów procesu planowania działań jest podjęcie decyzji. Każda decyzja jest podejmowana w pewnym przesunięciu czasowym w stosunku do odniesienia wykonawczego. Jest wypracowywana i podejmowana w stosunku do stanu otoczenia prawdopodobnego, który w rozumieniu dosłownym zwykle nie zaistnieje (rys. 4.1.1).



Rys. 4.1.1. Zmienność otoczenia w procesie decyzyjnym

Oznacza to, że w praktyce wszelkie decyzje podejmowane są zawsze w stosunku do odniesień prospektywnych, które z natury rzeczy mogą być tylko przybliżonym odzwierciedleniem stanu rzeczywistego, który może zaistnieć w przyszłości – mogą być odzwierciedleniem tylko prawdopodobnym. Dlatego też w trakcie ich realizacji musi się odbywać ciągłe monitorowanie umożliwiające korygowanie bądź potwierdzanie kształtu i treści wcześniej stworzonego obrazu tego odniesienia. To z kolei wskazuje na potrzebę wprowadzania określonych korekt do podjętej wcześniej decyzji bądź też utwierdza

w przekonaniu o jej trafność (aktualności). Do tego jednak potrzebna jest podmiotowi (decydentowi) odpowiednia wiedza o stanie odniesienia i obiekcie oddziaływania, często utożsamiana z informacjami[68].

Ze względu na fakt, że termin informacja jest używany w wielu różnych i odmiennych znaczeniach, niezbędne będzie przeprowadzenie analizy w tym zakresie. Wieloznaczność terminu informacja prowadzi do powstania dodatkowych, nieścisłych pojęć oraz powoduje niejednoznaczność w komunikowaniu się. Dlatego też w celu określenia jednoznaczności i ścisłości języka problemu należy wyjaśnić takie terminy, jak: informacja, dane, komunikat, sygnał informacyjny, sygnał sterujący, system informacyjno-sterujący, zasoby informacyjne.

Zgodnie z *communis opinio* termin informacja zwykle utożsamiany jest z przedmiotami myślowymi odzwierciedlającymi wszelkie postacie wiadomości, wieści, nowin, rzeczy zakomunikowanych, wiedzy o zdarzeniach itp."[69].

W cybernetyce informacja stanowi jeden z podstawowych terminów, którego desygnat jest nie w pełni definiowalny z uwagi na jego pierwotny i elementarny charakter[70]. W opisie procesów łączności i sterowania termin informacja zajmuje podobną pozycję jak pojęcia masy i energii w fizyce. Dlatego też ścisłe zdefiniowanie go za pomocą pojęć prostych jest po prostu niemożliwe. Wszystkie dotychczasowe próby zdefiniowania terminu „informacja" uważa się powszechnie za niezadowalające, a co najwyżej za ukazujące tylko niektóre jej aspekty *(ad exemplum)*.

N. Wiener[71] określa informację jako nazwę treści zaczerpniętej ze świata zewnętrznego, w miarę jak się do niego dostosowujemy i jak przystosowujemy doń swoje zmysły.

N. Couffignal[72] pisze, że w cybernetyce nazywa się informacją wszelkie działanie fizyczne, któremu towarzyszy działanie psychiczne.

Według W. Głuszkowa[73], informacja to wszelkie wiadomości o procesach i stanach dowolnej natury, które mogą być odbierane przez organy zmysłowe człowieka.

---

[68]Wynika to z logiki działania celowego, a spełnianie pożądanych w tym zakresie potrzeb wiąże się ściśle z wykorzystaniem zasobów informacyjnych. Różnica pomiędzy wiedzą a informacją zostanie wyjaśniona w dalszej części procedury dowodowej.

[69]W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Warszawa, Wiedza Powszechna, 1980, s. 429.

[70]*Mały słownik cybernetyczny*, op. cit., s.155.

[71]N. Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*, New York, Hermann & Cie, The Technology Press, and John Wiley & Sons, 1948, s. 67–69.

[72]L. Couffignal, *Cybernetyka*, Paryż, 1965, s. 36.

[73]W. Głuszkow, *Wstęp do cybernetyki*, Kijów, Naukowa Dumka, 1963, s. 21–29.

Zdaniem H. Greniewskiego[74], informacja to stany wyróżnione wejść i wyjść układu.

Według C. L. Shannona[75], informacją jest to wszystko, co nie jest ani energią, ani masą, czyli zasilaniem – jest to każde rozpoznanie stanu układu, odróżnialnego od innego stanu tego układu.

J. Seidler[76] zgadza się z ogólnie panującym poglądem, że pojęcie to, ze względu na swój elementarny charakter, jest prawdopodobnie niemożliwe do zdefiniowania za pomocą określeń prostszych, tak jak nie można tego uczynić w fizyce w stosunku do masy i energii. Jest zdania, że pozytywnego rozwiązania można poszukiwać tylko wyjaśniając sens tego pojęcia. W ślad za tym formułuje wyjaśnienie, że informacją można nazywać to wszystko, co jest użytkowane do bardziej sprawnego wyboru działań prowadzących do realizacji pewnego celu. Wyjaśnia przy tym, że mówiąc o sprawności działania, należy mieć na myśli to, iż mając i użytkując właściwie informację, można realizować celowe działania lepiej, bez istotnego zwiększania czy to środków materialnych, czy zużywanej energii.

S. Koziej, interpretując walkę zbrojną, definiuje informację jako niematerialny czynnik zespalający pozostałe elementarne czynniki walki zbrojnej (ruch i rażenie) w zharmonizowaną całość starcia zbrojnego[77].

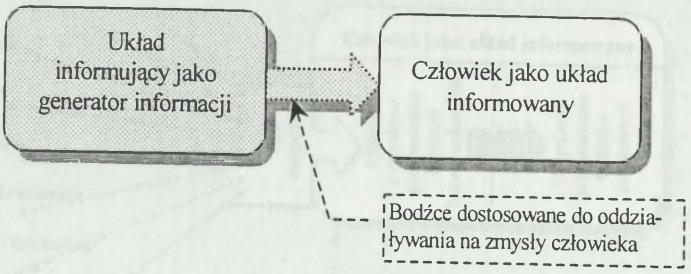
Są również i tacy, którzy, często posługując się terminem informacja, nie definiują jego desygnatu. Podejście takie można odnaleźć chociażby w książce S. Beera[78] poświęconej zastosowaniom cybernetyki jako ogólnej teorii sterowania w zarządzaniu w systemach ekonomicznych.

Na podstawie treści przytoczonych definicji należy stwierdzić, że nie wyjaśniają one jednoznacznie terminu informacja, co najwyżej ukazują tylko niektóre jej aspekty. Jednak we wszystkich, chociaż z różną mocą akcentowania, pojawiają się elementy wspólne. Są nimi: źródło informacji i układ odbierający[79] dostosowany do zmysłowego transformowania doznań i przetwarzania ich w rzeczywiste i abstrakcyjne przedmioty myślowe odzwierciedlające w jakiś sposób stany sytuacyjne otoczenia, których dotyczą.

---

[74]H. Greniewski, *Cybernetyka niematematyczna,* Warszawa, PWN, 1982, s. 43.
[75]C. E. Shannon, W. Warren, *The Mathematical Theory of Communication,* Urbana, The University of Illinois Press, 1949, s. 41-48.
[76]J. Seidler, *Nauka o informacji,* Warszawa, WNT, 1983, s. 69.
[77]S. Koziej, *Czynniki walki zbrojne,* Zeszyty naukowe nr 4, Warszawa, AON, 1993.
[78]S. Beer, *Cybernetyka a zarządzanie*, Warszawa, PWN, 1966.
[79]Pojęcie „układ odbierający" użyte zostało w rozumieniu, że jest to myślowo wyodrębniony fragment rzeczywistości, rozważany jako transformator otrzymywanych bodźców na wysyłane reakcje.

Wynika z tego, że informacja może istnieć tylko w pewnym układzie (systemie) informacyjnym[80], w którym podukład informowany (układ odbierający) stanowić będzie jednostka dostosowana do odbierania i abstrakcyjnego przetwarzania doznań zmysłowych. Taką jednostką może być tylko człowiek. Zatem *informacjami* można by nazywać tylko te doznania, które są możliwe do rejestrowania zmysłami ludzkimi, bo tylko one inspirują umysł człowieka do kojarzenia transformowanych doznań w rzeczywiste i abstrakcyjne wyobrażenia o stanie otoczenia, z którego pochodzą (rys. 4.1.2).



Rys. 4.1.2. Uproszczony schemat procesu informowania

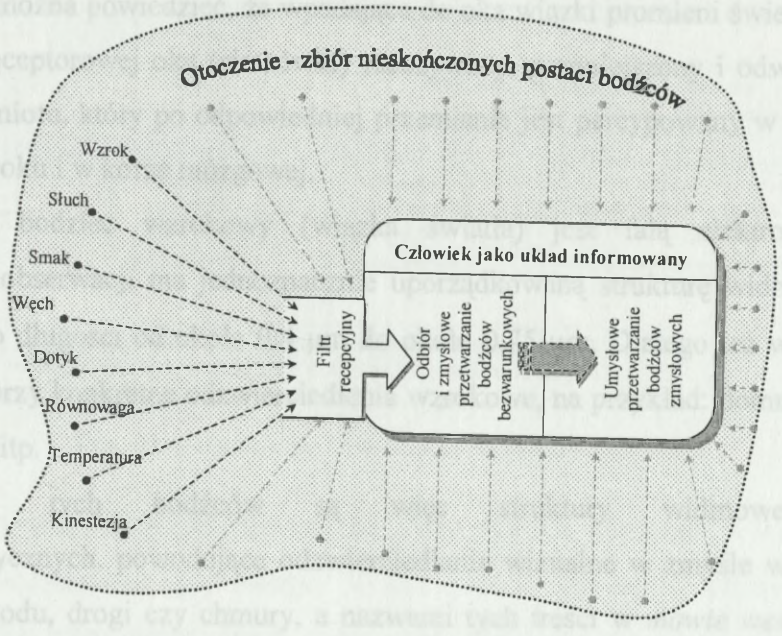
W tym miejscu można się zgodzić z Henrykiem Greniewskim[81], że informacje uzyskuje tylko człowiek. Bodziec, oddziałując na układ recepcyjny systemu zmysłowego konkretnego człowieka, powoduje wytwarzanie w jego wyobraźni przedmiotu myślowego, odzwierciedlającego obraz rzeczy materialnej lub abstrakcyjnej (przedmiotu, procesu, zjawiska, pojęcia itp.), który w jego subiektywnym przekonaniu (w jego subiektywnej świadomości) kojarzy się jakoś z tym bodźcem.

Tym samym bodziec taki mógłby być informacją, bo informuje człowieka o stanie otoczenia lub wybranych jego częściach, których dotyczy. Oznacza to, że *informacje* to tylko te doznania ludzkie, które – poprzez układ recepcyjny i system zmysłowy człowieka – inspirują umysł ludzki do pewnej wyobraźni o stanach przedmiotów, procesów, zjawisk, pojęć itp., których dotyczą. Ich istnienie jest zatem relatywnie związane z istnieniem człowieka i jego umysłu (rys 4.1.3).

[80] Pojęcie układ informacyjny użyte zostało w rozumieniu, że jest to taki układ, który ma choć jedno wejście informacyjne i choć jedno wyjście informacyjne, a więc jest jednocześnie układem informującym i układem informowanym. System informacyjno-sterujący to zespół sił i środków powiązanych z sobą funkcjonalnie i organizacyjnie, przeznaczony do zdobywania, przetwarzania, przechowywania, wykorzystania i dystrybucji danych, niezbędnych do podjęcia decyzji na wszystkich szczeblach organizacyjnych. Jego strukturę stanowią: źródła informacji, przetworniki informacji, nośniki informacji, układy odbierające oraz relacje systemowe.

[81] H. Greniewski, *Sprawy wszystkie i jeszcze inne*, Warszawa, KiW, 1970.

W kontekście powyższego wydawałoby się, że można już pokusić się o udzielenie odpowiedzi, iż *informacja jest bodźcem*. Należy się jednak zastanowić, czy można tak traktować informację.



Źródło: L. Ciborowski, Zarządzanie zasobami informacyjnymi w walce i operacji, Warszawa, AON 2002, s. 14.

Rys. 4.1.3. System informacyjny z rozwiniętym układem informowanym

W ujęciu fizjologicznym bodziec rozumiany jest jako czynnik pobudzający wyspecjalizowane narządy czuciowe, zwane receptorami, do wytwarzania stanów czynnych, wyzwalających impulsy biegnące do nerwowych ośrodków czuciowych, wywołujących określone reakcje (odruchy). Wyróżniane są *bodźce bezwarunkowe*, jako czynniki działające bezpośrednio na zmysły, i *bodźce warunkowe,* jako czynniki działające pobudzająco przez skojarzenie[82]. Można powiedzieć, że receptory, jako wyspecjalizowane narządy czuciowe, stanowią sobą układ wejściowy dla systemu poznania zmysłowego. Z ich definicji wynika, że dostosowane są do odbioru określonych sygnałów materialnych posiadających w jakiś sposób uporządkowaną strukturę wewnętrzną, odzwierciedlającą stany rzeczy i zjawisk. Formy uporządkowania tychże struktur stanowią sobą treści bodźców. Percepcyjnym[83] następstwem tego jest transformowanie tych treści (struktur) na konkretne wyobrażenia zmysłowe właściwe dla człowieka i zwierzęcia.

[82] *Encyklopedia powszechna*, Warszawa, PWN, 1973, t. 1, s. 304 i *Słownik języka polskiego,* Warszawa, PWN, 1978, t. 1, s. 183.

[83] Percepcja (spostrzeżenie) – złożony proces poznawczy, polegający na odzwierciedlaniu przez człowieka przedmiotów, zjawisk świata zewnętrznego oraz procesów zachodzących wewnątrz jego organizmu. Powstaje przez działanie na narządy zmysłowe określonych bodźców. Elementami percepcji są wrażenia zmysłowe. *Encyklopedia powszechna,* Warszawa, PWN, 1976, t. 4, s. 250.

W przypadku widzenia czynność ta sprowadza się do dostrzegania i rozróżniania przedmiotów wysyłających, odbijających lub przepuszczających światło. W następstwie tego są dostrzegane wielkości przedmiotów, ich kształty, barwy i ruch. W największym uproszczeniu można powiedzieć, że wpadające do oka wiązki promieni świetlnych tworzą w warstwie receptorowej oka (siatkówki) rzeczywisty, pomniejszony i odwrócony obraz danego przedmiotu, który po odpowiedniej przemianie jest percypowany w podkorowych ośrodkach wzroku i w korze mózgowej.

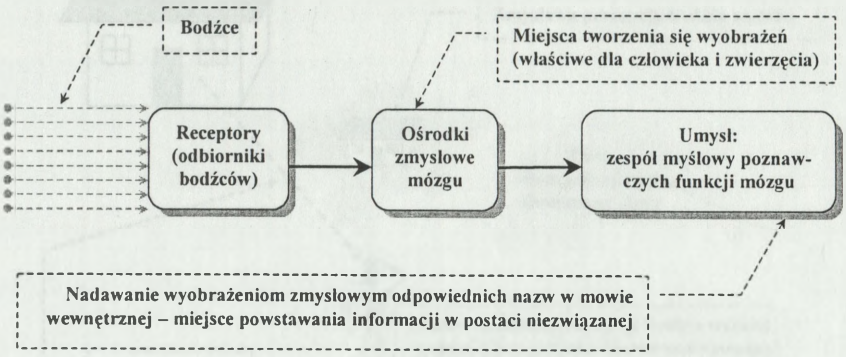
Każdy bodziec wzrokowy (wiązka światła) jest falą elektromagnetyczną. W konkretnej obserwacji ma jednoznacznie uporządkowaną strukturę widmową sygnału w paśmie fal o długości od około 0,4 μm do około 0,75 μm. Dlatego też w konkretnych sytuacjach tworzy konkretne odzwierciedlenia wzrokowe, na przykład: domu, samochodu, drogi, chmury itp.

Treścią tych bodźców są więc struktury widmowe sygnałów elektromagnetycznych, powodujące odzwierciedlanie wizualne w zmyśle wzroku obrazu domu, samochodu, drogi czy chmury, a nazwami tych treści w *mowie wewnętrznej*[84] są odpowiednio nazwy: dom, samochód, droga, chmura itp. Podobnie jest ze zmysłem słuchu. Jest to z kolei dostosowanie człowieka i zwierzęcia do odbioru fal dźwiękowych przez receptor słuchu mieszczący się w błędniku błoniastym ucha wewnętrznego. Dźwięki skupione i skierowane przez małżowinę uszną wywołują w nim drgania słupka powietrza, wprowadzając tym samym błonę bębenkową w drgania wymuszone, które po przemianie na odpowiednie impulsy nerwowe przekazywane są do podkorowych i korowych ośrodków słuchu, gdzie zachodzą procesy zmysłowej percepcji słuchowej. W następstwie tego człowiek i zwierzęta są w stanie odbierać (słyszeć) i rozróżniać zmysłowo różne brzmienia i ich barwy: mowę, muzykę itp. Umysł ludzki, jako zespół myślowy poznawczych funkcji mózgu, posiada jeszcze zdolność nadawania konkretnym brzmieniom, mieszczącym się w zakresie drgań od około 16 do 20 000 Hz, określonych nazw w *mowie wewnętrznej*, czego nie posiada zwierzę. Podobnie jest i z innymi zmysłami człowieka, gdzie zmysłowej percepcji wyobrażeniowej, bazującej na materialnych treściach odbioru recepcyjnego, towarzyszy zawsze poznanie umysłowe przypisujące poszczególnym wyobrażeniom zmysłowym określonych nazw w *mowie wewnętrznej*.

Dzieje się tak dlatego, że w poznaniu zmysłowym, właściwym dla człowieka i zwierzęcia, uwzględniane są tylko treści bodźców, bo te powodują określone procesy

[84]Mowa wewnętrzna sprowadza się do myślenia słowami (na ten temat będzie więcej w dalszej części pracy).

przemiany fizjologicznej i wynikające z tego doznania i zapamiętywanie. Na tym też opiera się tresura zwierząt. Nieuwzględniane są natomiast w niej nazwy treści. Nazwy wyobrażeń zmysłowych nadawane są tylko w umyśle ludzkim i tylko umysł ludzki jest w stanie odtwarzać na podstawie nazw określone skojarzenia zmysłowe (rys. 4.1.4).

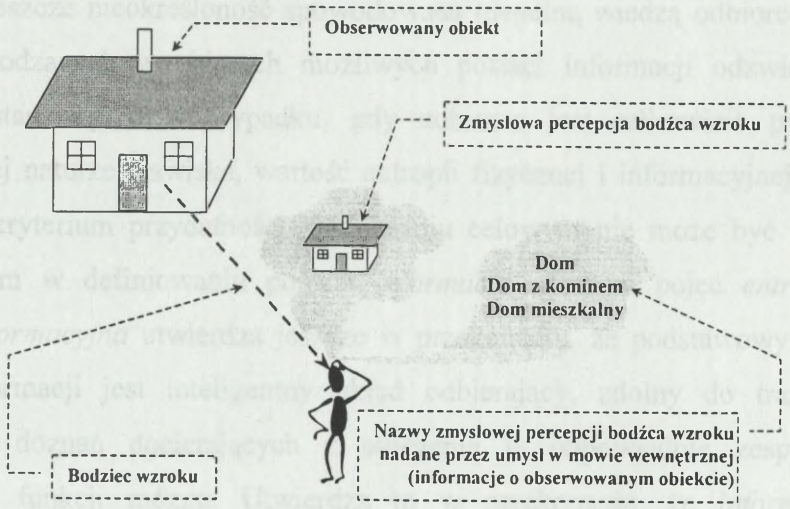


Rys. 4.1.4. Uproszczony schemat powstawania informacji

Dlatego też informacji nie można utożsamiać z bodźcem, a tylko z nazwą określonego wyobrażenia powstałego w następstwie percepcji zmysłowej bodźca. Informacjami są tylko nazwy treści przypisane umysłowo do określonych wyobrażeń zmysłowych. Bodziec jako taki jest tylko sygnałem sterującym, kształtującym poznanie zmysłowe – obraz rzeczy lub doznanie bez nadawania temu nazwy (rys. 4.1.5).

Dlatego też trzeba się zgodzić z tymi, którzy twierdzą, że *informacja* nie ma ani masy, ani energii i że jest przeznaczona tylko dla człowieka. Nie można natomiast zgodzić się, że informacja to nierozerwalny element działania celowego. Jest to prawdziwe, ale tylko w części. Posiadając określone informacje, z pewnością można jakieś działanie celowe realizować lepiej, bez istotnego zwiększania środków materialnych czy zużywanej energii. Nie można jednak tego odnosić do wszelkiej informacji, ponieważ pewne grupy informacji mogą być w jakimś działaniu celowym obojętne, a inne wręcz utrudniające jego osiągnięcie. Na przykład dla operatora nadzorującego pracę centrali automatycznej hałas wywoływany pracą wybieraków jest informacją użyteczną. Informuje go, że centrala pracuje. Ten sam hałas dla mechanika, naprawiającego jakiś element tejże centrali, jest informacją bezużyteczną. Dla osób prowadzących rozmowę w tym pomieszczeniu hałas ten jest natomiast informacją utrudniającą wymianę poglądów – zagłusza rozmowę i dekoncentruje uwagę dyskutujących. Tak samo podczas jazdy autobusem, odgłos pracy silnika będzie dla kierowcy informacją użyteczną, a dla pasażerów – bądź informacją bezużyteczną, bądź też utrudniającą realizację działania celowego, jeśli ci ostatni

zaplanowali sobie w czasie przejazdu jakąś pracę intelektualną, wymagającą koncentracji. Warkot silnika będzie rozpraszał ich uwagę.



Źródło: L. Ciborowski, Zarządzanie zasobami informacyjnymi..., s. 18.

Rys. 4.1.5. Model powstawania informacji

Nadmiar informacji jest również niepożądany w działaniu celowym, ponieważ zwiększa entropię informacyjnąo przestrzeni i materii pola operacyjnego, na którym to działanie ma być podejmowane. W języku potocznym często taki stan nazywany jest *szumem informacyjnym*. W rzeczy samej istota problemu tkwi w zwiększaniu rozbieżności pomiędzy entropią fizyczną a informacyjną. Polega to na tym, że entropia fizyczna jest funkcją aktualnego stanu fizycznego określonego obiektu materialnego przy założeniu, że stan ten jest traktowany jako zmienna losowa. W odróżnieniu od entropii informacyjnej nie uwzględnia nieokreśloności wnoszonej przez niewiedzę obserwatora, traktowanego w tym wypadku jako układ informowany. Wyznaczana jest jedynie przez statystykę stanów samego obiektu materialnego. Entropia informacyjna stanowi natomiast miarę nieokreśloności zdarzeń stanowiących źródła informacji, przy określonym stanie wiedzy o tych zjawiskach. Jest ściśle związana z ilością informacji zawartej w odebranym komunikacie[85], gdyż za miarę uzyskanej w ten sposób informacji przyjmuje się stopień zmniejszenia nieokreśloności.

[85]Komunikat to wszelki skończony zbiór stanowiący pewną porcję nazw treści bodźców. Innymi słowy komunikat to pewna porcja informacji przekazana adresatowi (do układu odbierającego) w „czystej" formie, czyli w postaci komunikatywnej dla zmysłów człowieka.

W odróżnieniu od entropii fizycznej, która jest całkowicie określona przez istniejący obiektywnie rozkład prawdopodobieństwa danego stanu, entropia informacyjna uwzględnia jeszcze nieokreśloność spowodowaną niepełną wiedzą odbiorcy o statystyce zjawisk zachodzących w zbiorach możliwych postaci informacji odzwierciedlających poznawany stan. Tylko w wypadku, gdy odbiorca jest całkowicie poinformowany o statystycznej naturze zjawiska, wartość entropii fizycznej i informacyjnej pokrywa się. Dlatego też kryterium przydatności w działaniu celowym nie może być uniwersalnym wyznacznikiem w definiowaniu pojęcia *informacja*. Analiza pojęć *entropia fizyczna* i *entropia informacyjna* utwierdza jeszcze w przekonaniu, że podstawowym warunkiem istnienia informacji jest inteligentny układ odbierający, zdolny do transformowania recepcyjnych doznań docierających z otoczenia w odpowiednie zespoły myślowe poznawczych funkcji mózgu. Utwierdza to w przekonaniu, że *informacja* istnieje w bezwzględnym związku z ludzkim umysłem. Tak jak foton nie może istnieć bez pędu, tak informacja nie może istnieć bez umysłu ludzkiego. Tylko ten zespół myślowy, poznawczych funkcji mózgu, jest dostosowany do nieskończonego transformowania doznań recepcyjnych w wyobrażenia informacyjne nazw. W kontekście powyższego można powiedzieć, że w zbiorze wszystkich definicji odnoszących się do interpretowania desygnatu pojęcia *informacja* najbardziej adekwatną jest definicja Norberta Wienera orzekająca, że informacja to nazwa treści zaczerpnięta ze świata zewnętrznego w miarę jak człowiek dostosowuje doń swoje zmysły.

Dokonując nawet pobieżnej analizy łatwo dostrzec, że oprócz określenia, że *informacja to nazwa treści*, autor wskazuje jeszcze na *otoczenie* jako jej miejsce bytu i na *zmysły ludzkie* jako narządy dostosowane do jej odbioru. Orzeka jakoby, że: po pierwsze – *informacja jako nazwa treści, jako coś niematerialnego, może istnieć w otoczeniu autonomicznie*, co w materialnej interpretacji świata zdaje się być niezrozumiałe i, po drugie, że *informacja jako nazwa treści, jako coś niematerialnego, może być odbierana przez zmysły ludzkie,* czyli przez narządy dostosowane tylko do rejestrowania i transformowania materialnych doznań, czyli treści zawartych w strukturach bodźców. Nazwy tych treści tworzone są i odbierane przez zespoły myślowe poznawczych funkcji mózgu. Układ recepcyjny człowieka rejestruje materialne treści bodźców i poprzez systemu zmysłowy transformuje je na konkretne doznania wzrokowe, słuchowe itp. Umysł ludzki, jako zespół myślowy poznawczych funkcji mózgu, nadaje dopiero tym treściom konkretne nazwy. Dlatego też *informacje jako nazwy treści* nie mogą istnieć w otoczeniu autonomicznie. Ich istnienie jest nierozerwalnie związane z istnieniem określonych

nośników, w których uporządkowane odpowiednio treści, przekazywane w formie bodźców, będą niosły z sobą nie tylko treści poznania zmysłowego, ale również i ich nazwy identyfikacyjne dla umysłu ludzkiego, czyli informacje. W związku z powyższym można sformułować **tezę 6.** *Desygnat pojęcia „informacja", w rozumieniu rzeczowym, należy utożsamiać z nazwą treści percepcji zmysłowej bodźca, a w rozumieniu czynnościowym (funkcjonalnym) – z procesem informowania.*

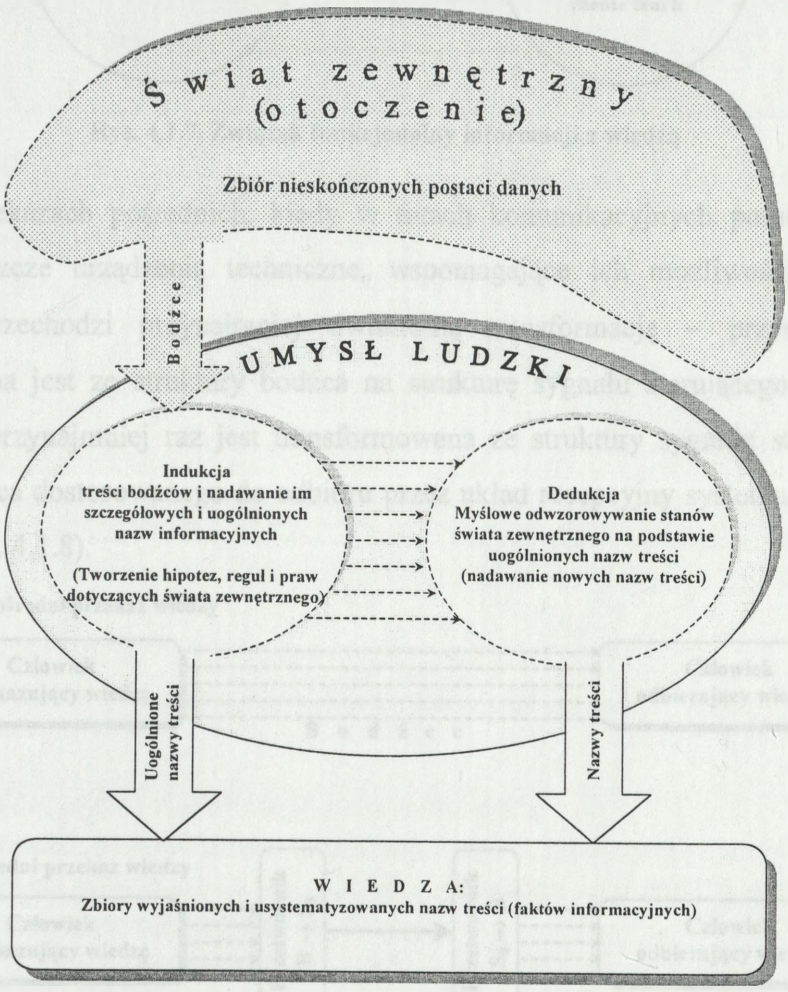
Wszelkie nazwy nadawane przez umysł ludzki, w mowie wewnętrznej człowieka, są informacjami nie tylko o świecie poznawanym zmysłowo, ale również i o świecie poznawanym umysłowo. Tworzonym nazwom przypisywane są określone przedmioty myślowe (desygnaty i denotacje) identyfikujące nie tylko rzeczy i zjawiska materialne, ale również i abstrakcyjne, będące wytworem ludzkiego umysłu. Każda nazwa kryje zatem w sobie określony potencjał informacyjny o rzeczy, której dotyczy, czyli jest informacją o tej rzeczy. W kontekście powyższego więcej wyjaśnień można uzyskać, poszukując odpowiedzi na pytanie: *do czego służy informacja?*

Najogólniej można powiedzieć, że informacja, w rozumieniu rzeczowym, służy do porozumiewania się międzyludzkiego. Tym samym stanowi podstawę do organizowania zespołowych działań ludzkich. Określone nazwy ukształtowane umysłowo w mowie wewnętrznej człowieka mogą być przekazywane na zewnątrz, jako informacje o określonych stanach, innemu człowiekowi w czterech różnych formach – oznajmującej, rozkazującej, pytającej i wykrzyknikowej. Mogą być przekazywane za pomocą różnych symboli, komunikatywnych dla drugiego człowieka. Na przykład w mowie zewnętrznej jest to zespół znaków dźwiękowych, przekładający się na umiejętność myślenia abstrakcyjnego i tworzenie pojęć poprzez bodziec słuchu.

Informacja, w rozumieniu rzeczowym, służy również do tworzenia wiedzy o otoczeniu człowieka i o nim samym. Procedurę tę w najprostszym ujęciu odzwierciedla pętla poznania indukcyjno-dedukcyjnego, w której zespoły myślowe poznawczych funkcji mózgu (umysł) spełniają rolę centralną (rys. 4.1.6).

Bodźce docierające do umysłu ludzkiego poprzez układ recepcyjny systemu zmysłowego niosą w sobie określone treści. Umysł ludzki, indukując je i poznając, nadaje im jednocześnie szczegółowe i uogólnione nazwy informacyjne w postaci określonych wyjaśnień (hipotez, reguł i praw). Zbiory tych wyjaśnień, po odpowiednim usystematyzowaniu, tworzą określoną wiedzę z różnych dziedzin, dyscyplin naukowych i specjalności, a także wiedzę o konkretnych obiektach, miejscach, zjawiskach i procesach.

Wiedza tworzona w umyśle ludzkim nie jest związana tylko z poznaniem indukcyjnym. Związana jest również z poznaniem dedukcyjnym. Istota tego procesu polega na tym, że na bazie racji indukcyjnych wyprowadzane są nowe racje dedukcyjne, które uzupełniają i rozszerzają wiedzę uzyskaną drogą indukcyjną. Te obydwie metody poznania umysłowego przeplatają się, a przewaga jednej nad drugą zależna jest tylko od skłonności umysłowych konkretnego człowieka i poznawanego przez niego obiektu.

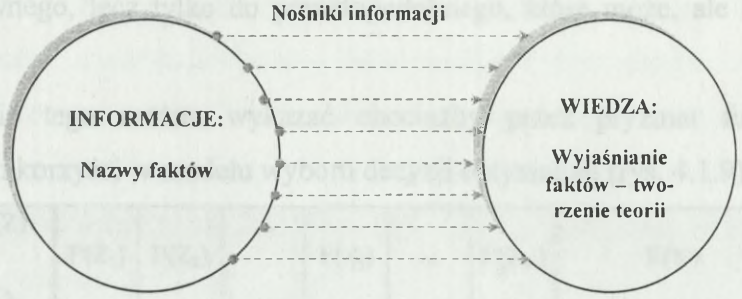


Źródło: L. Ciborowski, Zarządzanie..., s. 28.

Rys. 4.1.6. Model pętli poznania indukcyjno-dedukcyjnego

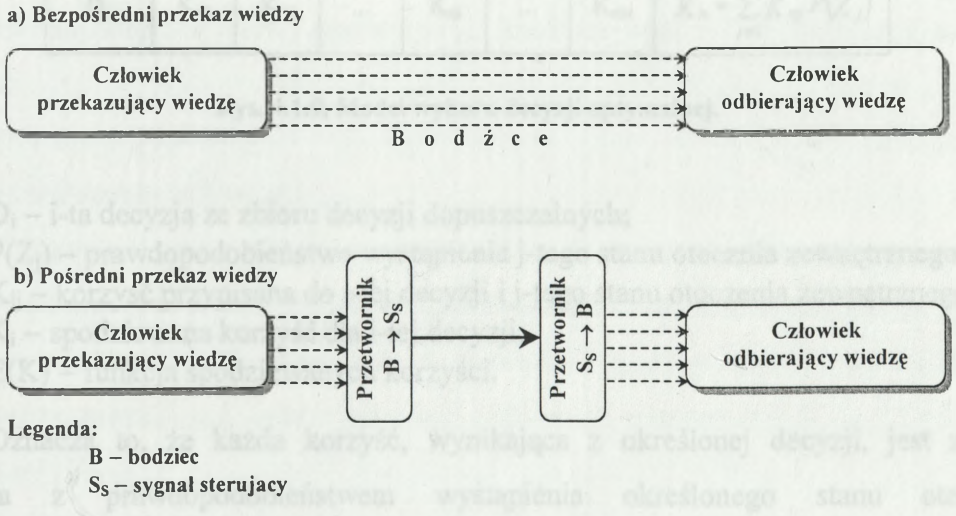
Powyższa analiza pozwala na sformułowanie **tezy 7** – *Związek funkcjonalny informacji z wiedzą polega na tym, że informacje jako nazwy określonych treści odzwierciedlają fakty. Wiedza natomiast wyjaśnia fakty i tworzy teorie. Tym samym pozwala również przewidywać stany określonych części otoczenia prospektywnego (rys. 4.1.7). Informacja i wiedza, w postaciach niezwiązanych, powstają i istnieją tylko w umyśle ludzkim. Wygenerowana natomiast na zewnątrz wiąże się automatycznie z określonymi nośnikami. W przekazie bezpośrednim „człowiek – człowiek", wiążą się*

z określonymi bodźcami (wzroku, słuchu itp.), rozpoznawalnymi przez układ recepcyjny systemu zmysłowego człowieka.



Rys. 4.1.7. Związek funkcjonalny informacji z wiedzą

W przekazach pośrednich, kiedy w torach komunikacyjnych pomiędzy ludźmi występują jeszcze urządzenia techniczne, wspomagające ich możliwości recepcyjne, wiedza ta przechodzi przynajmniej dwukrotną transformację – przynajmniej raz transformowana jest ze struktury bodźca na strukturę sygnału sterującego określonego urządzenia i przynajmniej raz jest transformowana ze struktury sygnału sterującego na strukturę bodźca dostosowanego do odbioru przez układ recepcyjny systemu zmysłowego człowieka (rys. 4.1.8).



Rys. 4.1.8. Warianty przekazu wiedzy

W procesie decyzyjnym potrzebne są zarówno wiedza, jak i informacje. Na podstawie wiedzy i informacji odwzorowywane są prospektywne stany sytuacyjne otoczenia decyzyjnego, czyli warunki i okoliczności towarzyszące realizacji postanowień decyzyjnych. Ich wcześniejsza identyfikacja zawsze sprzyja wyborowi decyzji najlepszej ze zbioru decyzji dopuszczalnych. Zależność ta, jak już wcześniej wspominano, wynika

z przesunięcia czasowego występującego pomiędzy podejmowaniem decyzji a realizacją jej postanowień. Dlatego też każda decyzja nie jest podejmowana w stosunku do odniesienia pewnego, lecz tylko do prawdopodobnego, które może, ale wcale nie musi zaistnieć.

Znaczenie tego można wykazać chociażby przez pryzmat funkcji korzyści i spodziewanych korzyści w modelu wyboru decyzji optymalnej (rys. 4.1.9)[86].

P(Z) / D	$P(Z_1)$	$P(Z_2)$	...	$P(Z_j)$	...	$P(Z_m)$	E(K)
D_1	K_{11}	K_{12}	...	K_{1j}	...	K_{1m}	$K_1 = \sum_{j=1}^{m} K_{1j} P(Z_j)$
D_2	K_{21}	K_{22}	...	K_{2j}	...	K_{2m}	$K_2 = \sum_{j=1}^{m} K_{2j} P(Z_j)$
...	...	...	...	...	...	...	...
D_i	K_{i1}	K_{i2}	...	K_{ij}	...	K_{im}	$K_i = \sum_{j=1}^{m} K_{ij} P(Z_j)$
...	...	...	...	...	...	...	...
D_n	K_{n1}	K_{n2}	...	K_{nj}	...	K_{nm}	$K_n = \sum_{j=1}^{m} K_{nj} P(Z_j)$

Rys. 4.1.9. Model wyboru decyzji optymalnej.

gdzie:

D_i – i-ta decyzja ze zbioru decyzji dopuszczalnych;
$P(Z_j)$ – prawdopodobieństwo wystąpienia j-tego stanu otocznia zewnętrznego;
K_{ij} – korzyść przypisana do i-tej decyzji i j-tego stanu otoczenia zewnętrznego;
K_i – spodziewana korzyść dla i-tej decyzji;
E(K) – funkcja spodziewanych korzyści.

Oznacza to, że każda korzyść, wynikająca z określonej decyzji, jest zawsze związana z prawdopodobieństwem wystąpienia określonego stanu otoczenia zewnętrznego, który przewidywany jest do zaistnienia w czasie realizacji określonych postanowień decyzyjnych. Funkcja spodziewanych korzyści wykazuje natomiast, że ostateczna korzyść zależna jest nie tylko od merytorycznego kształtu podjętej decyzji, ale nade wszystko z dostosowania jej do określonego odniesienia prospektywnego. Dlatego też wcześniejsza wiedza o zasadach kształtowania się określonych odniesień decyzyjnych

[86] W. Sadowski, *Decyzje i prognozy*, Warszawa, PWE, 1977, s. 87.

i bieżące informacje o ich stanie są niezbędne w podejmowaniu każdej decyzji. Posiadana wiedza pozwala na aprioryczne tworzenie modeli sytuacyjnych przyszłości.

Bieżące treści informacyjne, napływające z tych obszarów, pozwalają natomiast na ciągłe korygowanie i rozbudowywanie tych modeli i tym samym na permanentne przybliżanie ich do oryginałów. Skuteczność wykorzystywania zasobów wiedzy i zasobów informacji nie wynika tylko z faktu ich posiadania. Zależna jest także od ich alokacji. Dotyczy to zarówno zasobów wiedzy i zasobów informacji w postaciach niezwiązanych, jak i w postaciach związanych.

Ponieważ *zasoby wiedzy i zasoby informacji w postaciach niezwiązanych występują tylko w umysłach ludzkich,* można je nazywać:

a) wewnętrznymi zasobami wiedzy,

b) wewnętrznymi zasobami informacji.

Poza umysłem ludzkim, tak wiedza, jak i informacja, mogą występować tylko w postaciach związanych z nośnikami stanowiącymi bodźce komunikatywne dla zmysłu wzroku i słuchu. Jako nazwy treści elementarnych czy też zespoły tych nazw mogą być przekazywane za pomocą odpowiedniego systemu znaków graficznych, oznaczających dźwięki danego języka w mowie zewnętrznej lub za pomocą zespołu znaków dźwiękowych określonej mowy zewnętrznej. Utrwalone wraz z tymi nośnikami stanowią wówczas:

a) zewnętrzne zasoby wiedzy,

b) zewnętrzne zasoby informacji.

W kontekście powyższego można już dokonać częściowej kategoryzacji struktury zasobów informacyjnych $\{Z_{INF}\}$*, a tym samym stwierdzić* ***(teza 8)****, że w ich zbiorze mieszczą się zasoby rzeczowe* $\{Z_{RZ}\}$*, składające się z wiedzy* $\{Z_{RZw}\}$*, wiedzy wewnętrznej* $\{Z_{RZww}\}$*, wiedzy zewnętrznej* $\{Z_{RZwz}\}$*, informacji* $\{Z_{RZi}\}$*, informacji wewnętrznej* $\{Z_{RZiw}\}$ *i informacji zewnętrznej* $\{Z_{RZiz}\}$.

$$Z_{RZww} \cup Z_{RZwz} = 1^{*} \text{ zbioru } Z_{RZw}$$

oraz

$$Z_{RZiw} \cup Z_{RZiz} = 1^{*} \text{ zbioru } Z_{RZi}$$

to jednak

$$Z_{RZw} \cup Z_{RZi} \neq 1^{*} \text{ zbioru } Z_{INF}$$

Podział ten, jak już wcześniej zaznaczono, nie jest jeszcze wyczerpujący – w kontekście dobrego porządkowania zbioru nie spełnia jeszcze warunku zupełności. Wynika to z tego, że powyższy podział dotyczy tylko samej informacji i do tego tylko tej, która zaistniała i tej, która została wykorzystana do stworzenia wiedzy. W otoczeniu człowieka znajdują się zasoby nieskończonych postaci treści, które dopiero w określonych warunkach, czy przy określonym działaniu mogą się ujawniać.

Możliwości recepcyjne człowieka, mimo swej doskonałości funkcjonalnej, są jednak zbyt ograniczone pod względem zasięgu i rozpiętości postrzegania. Istniejące poza tą strefą treści realne stają się jakoby niebyłe. Niepostrzegane przez receptory zmysłów nie mogą podlegać percepcji zmysłowej i tym samym nie mogą też przyjmować nazw i tworzyć o sobie informacji. „Człowiek jednak zawsze chciał wiedzieć: jak jest? dlaczego tak jest? jak będzie? co zrobić, aby osiągnąć ten czy inny cel? czego nie należy czynić i dlaczego? Są to tylko nieliczne pytania wybrane z nieskończonej listy zapotrzebowania na informacje". Rodzi się zatem pytanie: czy można rozszerzyć dostępność poznania zmysłowego?

Postępująca politechnizacja życia stwarzała i stwarza coraz doskonalsze narzędzia użytkowe. Stwarzała i stwarza również narzędzia pokonujące bariery poznawalności zmysłowej. Sonda kosmiczna pozwoliła dotknąć powierzchni innych planet. Batyskaf wprowadził człowieka w największą głębię oceaniczną. Statki kosmiczne wyniosły go w przestrzeń międzyplanetarną – pozwoliły oglądać przestrzeń kosmiczną i poczuć treści doznań pozaziemskich.

Aparat rentgenowski czy ultrasonograf umożliwiły oglądanie wnętrza organizmów żywych, a ultraencefalograf pozwolił rejestrować fale w mózgu człowieka. Defektoskop zajrzał do wnętrza ciała stałego bez naruszania jego struktury. Radar pokonał ciemność i wydłużył zasięg widzenia. Noktowizja i termowizja umożliwiły widzenie w ciemności. Telekomunikacja pokonała w porozumiewaniu się barierę odległości.

Te i inne urządzenia, będące wytworem ludzkiego intelektu i pracy, pozwalają człowiekowi, niemalże każdego dnia, dostrzegać coraz to nowe treści pochodzące zarówno z jego bezpośredniego otoczenia, jak też z mikro – i makroświata. Stwarzają tym samym warunki do nadawania im konkretnych nazw i tworzenia w ten sposób nowych informacji. W tym miejscu można już skonstatować, że do zbioru zasobów informacyjnych należą również wszelkiego rodzaju urządzenia techniczne, rozszerzające możliwości recepcyjne człowieka, które można nazwać zasobami narzędziowymi i oznaczyć ogólnym symbolem $\{Z_N\}$.

Proces ten nie jest jednak prosty i jednorodny. Niedostępne pierwotnie bezpośredniemu poznaniu zmysłowemu treści przechodzą na swojej drodze wiele transformacji. Podawane są wyrafinowanym technicznie procedurom wykrywania, rejestracji, przetwarzania, opracowywania, gromadzenia, przechowywania i przesyłania. Dlatego też w zbiorze zasobów narzędziowych (technicznych) $\{Z_N\}$ można wyróżniać zasoby narzędziowe (techniczne) spełniające funkcje: wykrywaczy treści $\{Z_{Nw}\}$, rejestratorów treści $\{Z_{Nr}\}$, przetworników treści $\{Z_{Np}\}$, analizatorów treści $\{Z_{Na}\}$, baz treści $\{Z_{Nb}\}$ i transmiterów treści $\{Z_{Nt}\}$.

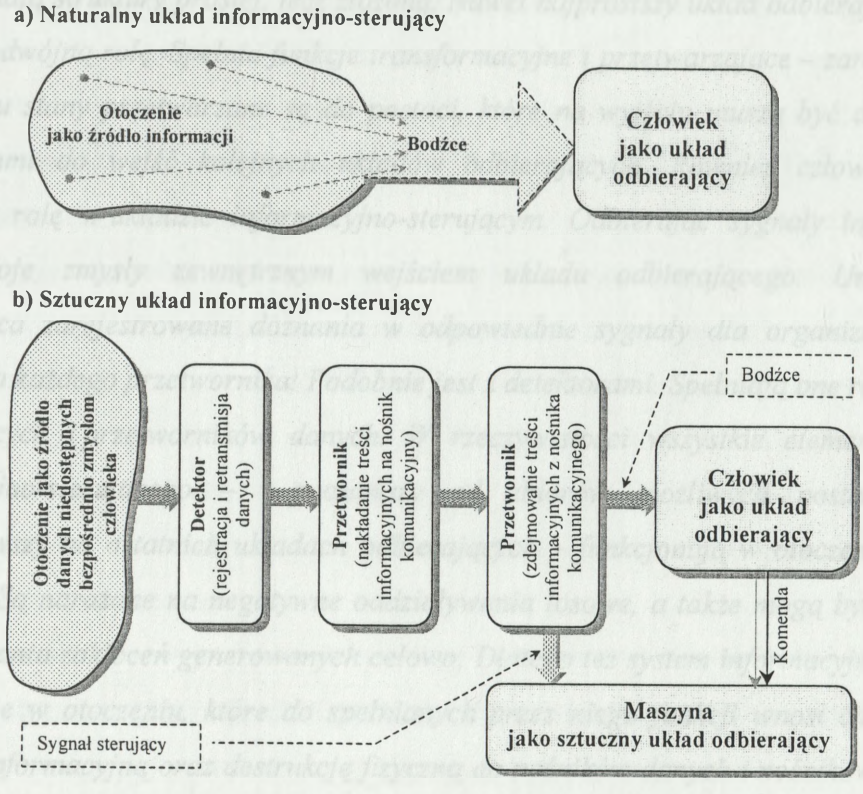
Związki informacji z umysłem ludzkim oraz informacji z treścią nie pozwalają jeszcze wyjaśnić relacji występujących w infrastrukturze informacyjnej. Powodem takiego stanu rzeczy jest fakt, że systemy informacyjne znajdujące się w otoczeniu człowieka nie mają i mieć nie mogą uniwersalnego wnętrza strukturalnego, dostosowanego funkcjonalnie do wszelkich sytuacji. Ich struktura jest zawsze następstwem konkretnych potrzeb człowieka, zespołów ludzkich, organizacji oraz możliwości technicznych i technologicznych. Wnętrze przedmiotowe infrastruktury informacyjnej stanowią nie tylko treści o rzeczach znajdujących się w bezpośrednim zasięgu poznawalności zmysłowej człowieka. Istnieją i poza nią, objawiając się różnymi treściami pod postaciami sygnałów informacyjnych i sterujących. Na swej drodze przechodzą wiele przemian, aby w ostateczności, wcześniej czy później, dotrzeć do końcowego układu odbierającego, którym zawsze jest człowiek (rys 4.1.10).

W sztucznych układach informacyjno-sterujących otoczenie to nieskończony zbiór możliwych postaci danych[87]. Dane te po zarejestrowaniu na wejściach pierwszych układów odbierających, którymi są różnego rodzaju detektory, przekazywane są na odpowiednio dobranych nośnikach, do przetworników. W tych miejscach odbywa się ich przetwarzanie na konkretne sygnały informacyjne lub sterujące[88], które kolejnymi nośnikami dostarczane są na wejścia odpowiednich układów odbierających.

Docelowe układy odbierające nie mają zwykle dostępu do danych w czystej postaci. Mają tylko dostęp do pewnych nośników sygnałów sterujących czy informacyjnych, które są już efektem spełnionej funkcji konkretnego przetwornika. Wynika to z tego, że dane w „czystej" postaci nie nadają się najczęściej ani do

[87]Dane to informacje potencjalne, które dopiero po odpowiednim opracowaniu (z wykorzystaniem odpowiedniego klucza) mogą stać się informacjami przydatnymi w działaniu celowym.
[88]Sygnał informacyjny to nośnik z danymi dostosowanymi do odbierania tylko przez układ recepcyjny człowieka. Sygnał sterujący to nośnik z danymi, które są dostosowane do rejestrowania przez układy odbierające organizmów żywych i urządzeń, z wyjątkiem zmysłów ludzkich

przetwarzania, ani do przesyłania na odległość. Dlatego konieczne jest ich przekształcanie w odpowiednie sygnały, których zasięg emisji jest znacznie większy.



Rys. 4.1.10. Elementy infrastruktury środowiska informacyjnego

Parametry tych sygnałów muszą być jednak tak modelowane, aby spełniały dwa podstawowe warunki – nie mogą zniekształcać sensu wartości podstaw źródłowych (wartości danych) i jednocześnie muszą być dostosowane parametrami do wejścia konkretnych układów odbierających. Nośnik sygnału sterującego czy informacyjnego musi mieć zawsze zachowaną postać, która będzie komunikatywna dla danego układu odbierającego.

Jeśli układem odbierającym będzie człowiek, to postać sygnału informacyjnego musi być dostosowana do możliwości recepcyjno-zmysłowych człowieka. Jeśli natomiast będzie to urządzenie techniczne, wtedy parametry energetyczne sygnału sterującego muszą być zgodne z parametrami energetycznymi wejścia tego układu. Oznacza to, że nośniki sygnałów sterujących i informacyjnych muszą mieć pewne cechy określone przez układy odbierające. Cechy te są zwykle różne od cech nośników danych. Dlatego w toku przetwarzania trzeba dokonać takich przekształceń, aby, przy zachowaniu pierwotnego sensu danych, stworzyć takie nośniki i sygnały (sterujące i informacyjne), które będą w pełni dostosowane do potrzeb spełnianych funkcji przez docelowe układy odbierające.

Teza 9. *W systemie informacyjno-sterującym, tak zbiory możliwych postaci danych, jak źródła danych, ich nośniki oraz przetworniki, nośniki sygnałów i układy odbierające nie posiadają struktury prostej, lecz złożoną. Nawet najprostszy układ odbierający spełnia zawsze podwójną rolę. Spełnia funkcje transformacyjne i przetwarzające – zarejestrowane na wejściu stany przetwarzane są do postaci, które na wyjściu muszą być dostosowane parametrami do wejść kolejnych układów odbierających. Również człowiek spełnia podwójną rolę w układzie informacyjno-sterującym. Odbierając sygnały informacyjne, czyni swoje zmysły zewnętrznym wejściem układu odbierającego. Umysł ludzki przekształca zarejestrowane doznania w odpowiednie sygnały dla organizmu, co jest typowe dla każdego przetwornika. Podobnie jest z detektorami. Spełniają one rolę układów odbierających i przetworników danych. W rzeczywistości wszystkie elementy systemu informacyjno-sterującego – począwszy od zbiorów możliwych postaci danych, a skończywszy na ostatnich układach odbierających – funkcjonują w otoczeniu ciągłych zakłóceń. Są narażane na negatywne oddziaływania losowe, a także mogą być obiektami oddziaływania zakłóceń generowanych celowo. Dlatego też system informacyjno-sterujący funkcjonuje w otoczeniu, które do spełnianych przez niego funkcji wnosi ciągle pewną entropię informacyjną oraz destrukcję fizyczną do nośników danych i nośników sygnałów, jak również do źródeł danych, przetworników i układów odbierających, a w tym i do umysłu człowieka.*

W otoczeniu istnieją dwa podstawowe rodzaje systemów informacyjno-sterujących. Pierwszą grupę tworzą systemy naturalne, a drugą – sztuczne.

Systemy naturalne stworzyła sama natura i funkcjonują poza wpływem i wolą człowieka. W szerokim rozumieniu tego słowa są również odporne na wszelkie jego oddziaływania – człowiek nie jest w stanie zmienić ani ich struktury, ani zasad funkcjonowania. Co najwyżej może je tylko obserwować i poznawać. Odpowiednio do tego może też co najwyżej dostosowywać swoją egzystencję i ewentualnie przewidywać niektóre następstwa określonego postępowania. Ingerując w prawa natury, może przewidywać konsekwencje tego. Dlatego też naturalny system informacyjno-sterujący, postrzegany w całej ogólności, należy uznawać za idealny i niezakłócalny. Każda ingerencja człowieka do panującego ładu jest wcześniej czy później wykrywana z pełną dozą naturalnej prawdy i obiektywizmu w ocenie zdarzeń i w sterowaniu następstwami. Dlatego też naturalny system informacyjno-sterujący może być poddawany co najwyżej poznawaniu.

Sztuczne systemy informacyjno-sterujące są zawsze wytworem ludzkiej działalności. W odróżnieniu od systemu naturalnego nigdy nie były, nie są i sądzić należy, że nigdy nie będą idealne. Stosowane w nich rozwiązania strukturalne i organizacyjne – hierarchiczne, funkcjonalne, informacyjne i techniczne – tworzone są zawsze tylko w aspekcie chwilowych, dających się przewidywać, potrzeb ich twórców i tylko na miarę zdobytej przez nich na ten temat wiedzy oraz fizycznych możliwości jej materializowania w konkretnych rozwiązaniach.

Zawsze wszystkie sztuczne systemy informacyjno-sterujące tworzone są przez człowieka w aspekcie spełniania konkretnych potrzeb wynikających z zamiaru jakiegoś działania celowego. Tworzone są z zamysłem poznawania lub identyfikowania zdarzeń w przestrzeni pola operacyjnego, na którego materii zamierzone jest jakieś działanie. Służą również do ustalania stanu i możliwości operacyjnych aparatu narzędziowego, przeznaczonego do realizacji tego zamierzenia, oraz monitorowania efektów podejmowanej działalności.

Realizacja każdego działania celowego odbywa się zawsze w jednym z trzech rodzajów otoczenia. Może przebiegać w zupełnym wyizolowaniu i może się odbywać w ramach współpracy lub w ramach rywalizacji.

W warunkach wyizolowania organizator i realizator działania celowego zdany jest tylko na własne siły i własną pomysłowość w osiąganiu danego celu. Nikt mu w sposób zamierzony ani nie pomaga, ani nie przeszkadza. Jest po prostu wyizolowany z otoczenia. Co najwyżej może się natknąć na pewne zdarzenia losowe, które bądź pozytywnie, bądź negatywnie wpłyną na realizację podjętego wysiłku.

W ramach współpracy organizator i realizator działania celowego wspomagany jest w swych wysiłkach działaniami innego lub innych, którzy pomagają mu osiągnąć zamierzony cel. Ten z kolei, dążąc do osiągnięcia własnego celu, wspiera działania elementów, współpracujących z nim. W tych warunkach, podobnie jak poprzednio, nikt nikomu nie przeszkadza w realizacji podjętych działań. Co najwyżej mogą wystąpić pewne zdarzenia losowe, które bądź ułatwią, bądź też utrudnią ich realizację.

Zupełnie inaczej przebiega proces działania celowego w warunkach rywalizacji (kooperacji negatywnej). Według T. Kotarbińskiego, także z punktu widzenia cybernetyki, kooperacja ta utożsamiana jest z walką.

Walka to wszelkie działania przynajmniej dwupodmiotowe (zakładając, że zespół może być podmiotem), gdzie przynajmniej jeden z podmiotów przeszkadza drugiemu[89]. W szczególnym, najzwyklejszym i najciekawszym przypadku oba podmioty nie tylko dążą obiektywnie do celów niezgodnych, lecz nadto wiedzą o tym i liczą się w budowaniu swoich planów też z działaniami strony przeciwnej.

T. Kotarbiński wyróżnił cele permutacyjne (zmieniające) i perseweracyjne (niezmieniające). W takim kontekście do walki może dojść wtedy i tylko wtedy, gdy przynajmniej jedna ze stron dążyć będzie do zmiany istniejącego stanu rzeczy.

Po pierwsze, może zaistnieć stan, w którym zarówno strona A, jak i B mogą mieć cele permutacyjne, to znaczy, że obie walczące strony pragną zmienić istniejący stan rzeczy. Obydwie strony będą więc prowadzić działania po to, by zmienić ten stan.

Po drugie, może zaistnieć stan, w którym strona A pragnie zmienić istniejący stan rzeczy, strona B zaś utrzymać go. Wówczas A atakuje, B zaś broni się.

Po trzecie, może zaistnieć stan przeciwstawny drugiemu, to znaczy, że strona B stawia sobie cele permutacyjne, zaś strona A perseweracyjne.

W walce skutecznej, niejako w uzupełnieniu teorii czynu skutecznego, zawsze jedna ze stron osiągnie cel, czyli w rezultacie zwycięży. Warunkiem zaś koniecznym do osiągnięcia celu jest uzyskanie przewagi. W wypadku działań informacyjnych będziemy mieli do czynienia z przewagą informacyjną. Istotę tej przewagi można wyrazić przez analogię z wywodzonymi w prakseologii regułami (tezami).

Teza 10. *W przewadze nie chodzi o posiadanie większych niż przeciwnik zasobów, lecz o sprawne ich wykorzystanie, a zatem o stałą możliwość wykorzystania potencjału w określonym, rozstrzygającym miejscu i czasie. Takie sprawne wykorzystanie potencjału zapewniają systemy i technologie informacyjne, które muszą być chronione przed oddziaływaniem przeciwnika.*

Teza 11. *Zwycięstwo nad przeciwnikiem będzie odnosił ten, kto potrafi wpłynąć na takie działania przeciwnika, które będą dla niego korzystne. Będzie to polegało na wprowadzaniu dowódców w błąd co do realnej sytuacji na polu walki, czyli na stwarzaniu sytuacji utrudniających przeciwnikowi podejmowanie trafnych decyzji, wykonywanie sprawnych ruchów wojskami i precyzyjnych uderzeń ogniowych, z jednoczesną obroną wojsk własnych. Innymi słowy sprowadzać się to będzie do dezorientowania przeciwnika*

[89] T. Kotarbiński, *Traktat o dobrej robocie*, Wrocław, 1982, s. 221.

co do sytuacji na polu walki, komplikowania jego warunków działania i w efekcie zmuszania go do podejmowania błędnych decyzji.

Teza 12. *Każda walka wymaga dogodnej sytuacji. Ważne dla osiągnięcia sukcesu będzie więc postawienie przeciwnika w sytuacji, w której będzie zmuszony dążyć do zmiany pozycji i sytuacji, czyli tracić część potencjału na działania przygotowawcze. W każdym wypadku do zwycięstwa przyczyni się działanie, w którym doprowadzimy do stanu przeciwstawnego oczekiwaniom strony przeciwnej, tak aby musiała ona (ta strona) odrabiać wytworzony stan rzeczy, niezgodny z jej celem.*

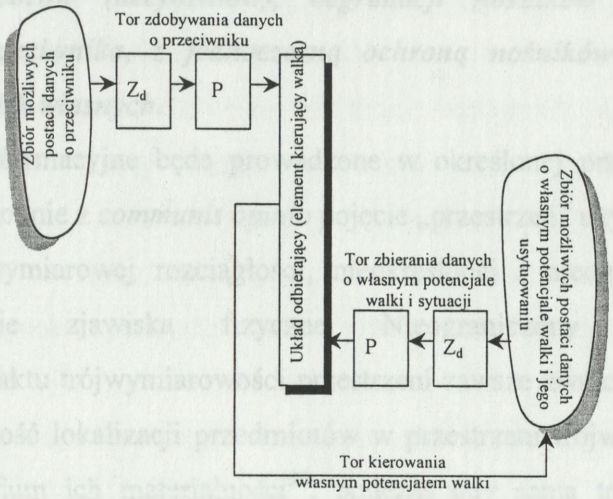
Teza 13. *Chcąc odnieść zwycięstwo, należy jak najdłużej utrzymywać swe siły w pełnej zdolności do działań. Utracenie możliwości reakcji na działania strony przeciwnej pozbawia możliwości realizacji celu. Dlatego duże znaczenie w tym zakresie będzie odgrywać rozpoznanie, które powinno dostarczyć aktualnych informacji o przeciwniku i jego działaniach.*

Teza 14. *Doświadczenia różnych wojen wskazują jednoznacznie, że groźba stanowi ważny czynnik uzyskania przewagi, a często nawet determinuje osiągnięcie zwycięstwa, zmuszając przeciwnika albo do zaniechania działań, albo do osłabienia determinacji. Dlatego też słuszne wydaje się twierdzenie, że racjonalnie i skutecznie walczy ta strona, która zamiast osiągać cel za pomocą użycia posiadanych sił i środków, osiąga go zastraszając przeciwnika groźbą ich użycia, zmuszając go zatem do zaniechania działań. Dużą rolę w tym zakresie będą miały do spełnienia działania psychologiczne oraz działania demonstracyjne.*

Teza 15. *Nie ulega wątpliwości, że najlepsze rezultaty w walce osiąga się przez nieoczekiwane działanie. Dlatego też, dla osiągnięcia celu walki, niezbędne są pewne informacje o przeciwniku, z jednej strony, a starania o to, aby strona przeciwna nie miała o nas informacji (lub miała nieprawdziwe) – z drugiej. W związku z powyższym walka odbiegająca od stereotypów, zawierająca elementy zaskoczenia przeciwnika, daje gwarancje zwycięstwa. Zaskoczenie zaś można uzyskać tylko przez rzetelną informację o stronie przeciwnej z jednoczesną dezinformacją, co do naszych czynów, sił i zamiarów. Ważną rolę do spełnienia w tym zakresie będą miały elementy walki elektronicznej.*

Teza 16. *Wszelkie konflikty, szczególnie w ostatnich latach, świadczą jednoznacznie, iż w każdej organizacji istnieją takie elementy, od których zależy jej sprawność. Jeśli przyjmie się tezę, że wszystkie sztuczne systemy informacyjno-sterujące tworzone są przez człowieka w aspekcie spełniania konkretnych potrzeb, wynikających z realizacji jakiegoś działania celowego, to można również powiedzieć, że są one*

nierozerwalnie związane z każdym działaniem celowym, realizowanym w warunkach kooperacji negatywnej wzajemnej. Systemy te mają różnorodną strukturę, jednak w zasadzie przeznaczone są do spełniania trzech podstawowych funkcji. Służą do zdobywania danych o przeciwniku, zbierania danych o sytuacji własnych sił oraz kierowania własnym potencjałem walki (rys. 4.1.11).



Legenda
Z_d – źródło danych
P – przetwornik danych (sygnałów)

Rys. 4.1.11. Rola funkcjonalna systemu informacyjno-sterującego

Taka struktura systemu informacyjno-sterującego jest determinowana potrzebami decyzyjnymi. Każdy z zaangażowanych podmiotów dąży do wypracowania takich decyzji, aby po ich wdrożeniu pokonać swojego kooperanta negatywnego. Dąży zatem do wypracowywania decyzji możliwie najtrafniejszych w danej sytuacji. Do osiągnięcia tego niezbędna jest jednak wiedza o stanie, usytuowaniu oraz możliwościach i zamiarach wykorzystywania narzędzi walki przez przeciwnika i o panującej u niego sytuacji. Tak samo niezbędna jest wiedza o własnym potencjale walki. Posiadanie tych danych stanowi podstawę do świadomego wypracowywania poprawnych decyzji. Luki w zasobach wiedzy powodują podejmowanie decyzji ryzykownych, o niedających się przewidywać skutkach. Ich niezakłócone funkcjonowanie względnie zniszczenie, uszkodzenie lub jakieś inne zdezorganizowanie przyczyniać się będzie, w sposób pośredni ale bardzo istotny, do osiągania celów głównych w konkretnych działaniach. Wyeliminowanie ich (zniszczenie, obezwładnienie) stanowi często zasadniczy czynnik determinujący powodzenie (osiągnięcie celu). Stąd też we współczesnej wojnie, nie zabijanie, nie zniszczenie masy, ale obezwładnienie systemów informacyjnych, pociągnąć może destrukcję funkcjonalną

całej organizacji. O powodzeniu wszelkich działań będzie więc decydować wyeliminowanie tych decydujących elementów w systemach przeciwnika, które stanowią o jego sprawności działania.

Realizację powyższych postulatów mogą zapewnić ***działania informacyjne***, które należy interpretować jako ***kompleks planowych przedsięwzięć polegający na wpływaniu na postawy dowódców (decydentów), degradacji nośników danych i systemów informacyjnych przeciwnika, z jednoczesną ochroną nośników danych i systemów informacyjnych wojsk własnych.***

Działania informacyjne będą prowadzone w określonej przestrzeni (środowisku informacyjnym). Zgodnie z *communis opinio* pojęcie „przestrzeń" używane jest najczęściej w rozumieniu trójwymiarowej rozciągłości, nieokreślonej i nieograniczonej, w której zachodzą wszelkie zjawiska fizyczne. Nieograniczony stopień ogólności i fundamentalność faktu trójwymiarowości przestrzeni zawsze zwracały uwagę filozofów, dla których możliwość lokalizacji przedmiotów w przestrzeni trójwymiarowej stanowiła jakże często kryterium ich materialności[90], podczas gdy sama trójwymiarowość była w istocie rzeczy niewyjaśniona. Trójwymiarowość przestrzeni przyjmowano jako aksjomat podczas tworzenia licznych teorii fizycznych, sam jednak aksjomat wymykał się wszelkim próbom uzasadnienia. *Sine ira et studio* tego typu ujęcie problemu nie może być uznane za poprawne.

Rozpatrując przestrzeń, należałoby się zastanowić nad jej wymiarem, co będzie wymagało ścisłego, matematycznego wyjaśnienia.

Pojęcie wymiaru przestrzeni ulegało ciągłej ewolucji, co doprowadziło wreszcie do współczesnego, topologicznego pojęcia wymiaru.

Jest on jedną z takich właściwości, które są zachowane dla dowolnych wzajemnie jednoznacznych i ciągłych homemograficznych przekształceń lub, inaczej, dla takich przekształceń, dla których każdemu punktowi jednego obiektu odpowiada tylko jeden punkt drugiego obiektu, a nieskończenie bliskim punktom jednego obiektu odpowiadają nieskończenie bliskie punkty drugiego. Współczesna definicja wymiaru, która jest rozwinięciem definicji Poincarego, została podana przez Ursynowa i Mengera, którzy twierdzą, że:

— zbiór pusty posiada wymiar – 1;

[90]R. Descartes, *Zasady filozofii*, Warszawa, 1960, s. 57/

— wymiar przestrzeni X jest najmniejszą całkowitą liczbą n taką, że każdy punkt $p \in X$ posiada dowolnie małe otoczenie, którego ograniczenie ma wymiar mniejszy niż n.

W topologii dowodzi się twierdzenia, że n – wymiarowa w sensie intuicyjnym przestrzeń euklidesowa posiada rzeczywiście wymiar n. Wynika z tego, że linia ma wymiar 1, powierzchnia euklidesowa – 2, a przestrzeń – 3. A więc trójwymiarowość przestrzeni jest niewątpliwie faktem fizycznym. Jako jego doświadczalne potwierdzenie przytacza się fakt posiadania objętości przez ciała przyrody, możliwość przeprowadzenia w każdym punkcie przestrzeni nie więcej niż trzech wzajemnie prostopadłych prostych, możliwość opisania dowolnego punktu przestrzeni przez trzy niezależne parametry; wreszcie możliwość osiągnięcia dowolnego punktu przestrzenie poprzez trzy prostopadłe przesunięcia. Ponadto w naszej przestrzeni można zbudować modele materialne jedynie takich obiektów geometrycznych, które należą do trójwymiarowej przestrzeni matematycznej.

Jeśli porównamy przestrzeń matematyczną (topologiczną) z rzeczywistą przestrzenią fizyczną, to można dojść do wniosku, że albo nie znajdzie się ani jednej przestrzeni, która pozwoliłaby na opisanie bez naruszenia zwykłych właściwości – wzajemnej łączności przyczynowej, albo przestrzenie takie istnieją, a wówczas, opierając się na teorii Brouwera, można pokazać, że będą to jedynie przestrzenie trójwymiarowe.

Poincar`e i jego następcy twierdzili, że jeśli zmieniłoby się radykalnie prawa fizyki, np. dopuściłoby się przyczynowe anomalie, to formalnie można by przyjąć model przestrzenny o wymiarowości różnej od 3. Jednak prawidłowości fizyczne, podstawowe fizyczne pojęcia przyczynowości nie zmieniają się w sposób dowolny, powstają one w procesie uogólnienia danych doświadczalnych i stają się ograniczonym elementem rozwijających się teorii fizycznych.

Teoria względności pokazała, że nawet metryczne właściwości przestrzeni i czasu nie mogą być rozpatrywane jako całkowicie konwencjonalne, tym bardziej odnosi się to do ich topologicznych właściwości. Można wykazać, że konwencjonalne podejście do problemu trójwymiarowości przestrzeni wynika z traktowania przestrzeni i czasu jako form postrzegania zmysłowego (jako tworów naszego umysłu) pozbawionego kantowskiego aprioryzmu: jeżeli „niedorzecznością" jest mówić o rzeczywistej przestrzeni istniejącej niezależnie od postrzegającego podmiotu, to wybór modeli przestrzenno-czasowych przez badacza podyktowany jest jedynie przez kryterium dogodności, prostoty, celowości, ekonomiki myślenia itd.

Z cybernetycznego[91] punktu widzenia desygnat przestrzeni interpretowany jest jako „zbiór dowolnych przedmiotów (liczb, stanów układu, wektorów itp.), między którymi zostały ustalone pewne relacje natury geometrycznej bądź abstrakcyjnej".

Konfrontując to z regułami stosowanymi w teorii mnogości, relacje te należy rozumieć jako cechy wyróżnialności (kryteria rozstrzygalności), które pozwalają określać czy dany element zbioru, ze względu na zachowanie warunku jednorodności, należy do tego zbioru czy też nie. Dlatego też liczba przestrzeni jest nieskończona, tak jak nieskończone są możliwości wyznaczenia relacji pomiędzy nieskończoną liczbą elementów materialnych i niematerialnych.

Co się zaś tyczy „przestrzeni działań informacyjnych", to przede wszystkim trzeba uwzględniać złożoność terminu. W jego strukturze wyrazem podstawowym jest „przestrzeń", a wyrazami dopełniającymi, konkretyzującymi desygnat całości, są pojęcia: „działania" i rodzaj tych działań, zwany „informacyjne". Dlatego też desygnat tego trójczłonowego terminu powinien zawierać w swoim zbiorze przedmiotowym wszystkie te elementy, które są właściwe pojęciom: „przestrzeń"; „działania" oraz „działania informacyjne", co można oznaczyć następująco:

{P} – zbiór elementów składających się na desygnat „przestrzeń";

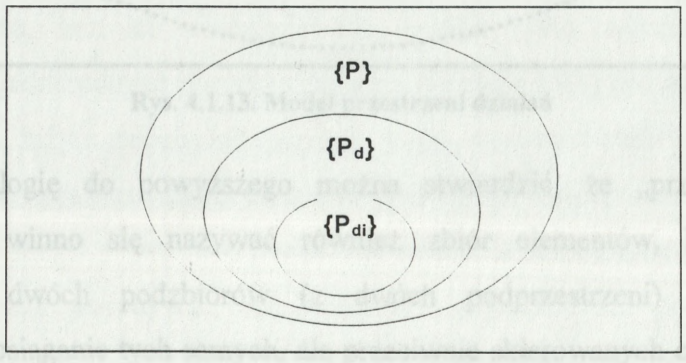
$\{P_0\}$ – zbiór elementów składających się na desygnat „przestrzeń działań";

$\{P_{oi}\}$ – zbiór elementów składających się na desygnat „przestrzeń działań informacyjnych".

Zależność semantyczną pomiędzy tymi pojęciami można wyrazić zapisem:

$$\{P_{di}\} \subset \{P_d\} \subset \{P\}$$

oraz przedstawić graficznie (rys. 4.1.12).



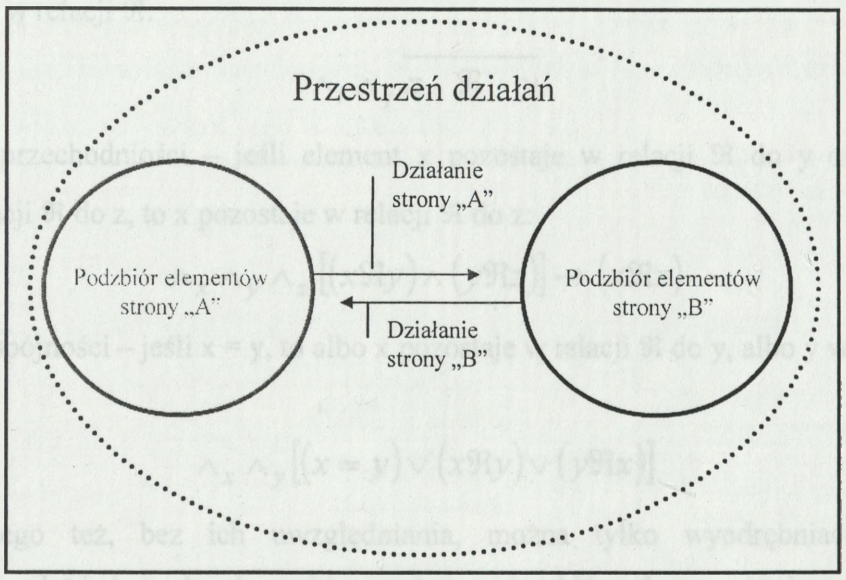
Rys. 4.1.12. Zależność semantyczna pomiędzy pojęciami: „przestrzeń", „przestrzeń działań" i „przestrzeń działań informacyjnych"

[91] *Mały słownik cybernetyczny...*, s. 251.

Podstawową cechą przedmiotu myślowego „przestrzeń" jest to, że wszystkie elementy należące do tej przestrzeni winny być zespolone wspólną relacją porządkującą, która w terminologii teorii mnogości określana jest zamiennie: bądź mianem „kryterium rozstrzygalności" bądź „cechą wyróżnialności".

Innymi słowy, „przestrzenią" można nazywać tylko taki zbiór elementów, które w granicach tego zbioru zespolone będą przynajmniej jedną i wspólną dla wszystkich relacją porządkującą, umożliwiającą wyróżnianie tego zbioru spośród innych.

Podstawą przedmiotu myślowego „przestrzeń działań" jest to, że w strukturze tej przestrzeni (w strukturze tego zbioru) muszą istnieć przynajmniej dwa podzbiory elementów, pomiędzy którymi, ze względu na funkcję celu, zachodzi kooperacja negatywna wzajemna. Oznacza to, że „przestrzenią działań" można nazywać tylko taki zbiór elementów, który składa się przynajmniej z dwóch podzbiorów (z dwóch podprzestrzeni) ukierunkowanych funkcjonalnie na osiąganie przeciwnie skierowanych celów (rys. 4.1.13).



Rys. 4.1.13. Model przestrzeni działań

Przez analogię do powyższego można stwierdzić, że „przestrzenią działań informacyjnych" winno się nazywać również zbiór elementów, który składa się przynajmniej z dwóch podzbiorów (z dwóch podprzestrzeni) ukierunkowanych funkcjonalnie na osiąganie tych samych, ale przeciwnie skierowanych celów z dodaniem, że powinny to być elementy i działania dostosowane do prowadzenia działań informacyjnych (rys. 4.1.14).

dostosowania, będą już niepodzielne. Tylko wtedy można powiedzieć, że potencjalna przestrzeń działań informacyjnychzostała uporządkowana. Aby to uczynić, należy ustalić kolejne cechy wyróżnialności i stosownie do nich dokonać klasyfikacji (podziału) jej elementów na jednorodne podprzestrzenie (podzbiory). Klasyfikacja taka powinna spełniać dwa warunki podziału zbioru pełnego, a mianowicie:

— zupełności – suma wyróżnionych podzbiorów (podprzestrzeni) tworzy zbiór pełny:

$$A_1 \cup A_2 \cup ... \cup A_n = 1^*$$

— rozłączności – iloczyn każdej pary podzbiorów (podprzestrzeni) jest zbiorem pustym:

$$\wedge_i \wedge_j \left(A_i \cap A_j\right) = 0^*$$

Nie wystarcza to jednak do rozwiązania problemu w pełnym zakresie. W praktyce zdarza się, że warunki te traktowane są nieraz jako jedyne i wystarczające. W istocie sprawy nie uwzględniają jeszcze relacji porządkujących, którymi są:

— relacja przeciwzwrotna – żaden element zbioru (podprzestrzeni) nie pozostaje do siebie samego w relacji $\Re$:

$$\wedge_i \wedge_j \overline{x \quad \Re \quad y}$$

— relacja przechodniości – jeśli element x pozostaje w relacji $\Re$ do y oraz element y w relacji $\Re$ do z, to x pozostaje w relacji $\Re$ do z:

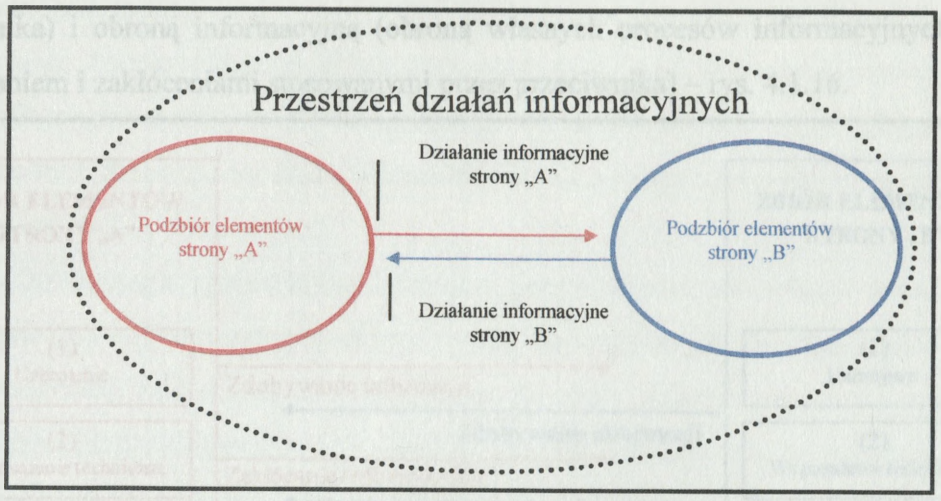
$$\wedge_x \wedge_y \wedge_z \left[\left(x \Re y\right) \wedge \left(y \Re z\right)\right] \rightarrow \left(x \Re z\right)$$

— relacja spójności – jeśli x = y, to albo x pozostaje w relacji $\Re$ do y, albo y w relacji $\Re$ do x:

$$\wedge_x \wedge_y \left[\left(x = y\right) \vee \left(x \Re y\right) \vee \left(y \Re x\right)\right]$$

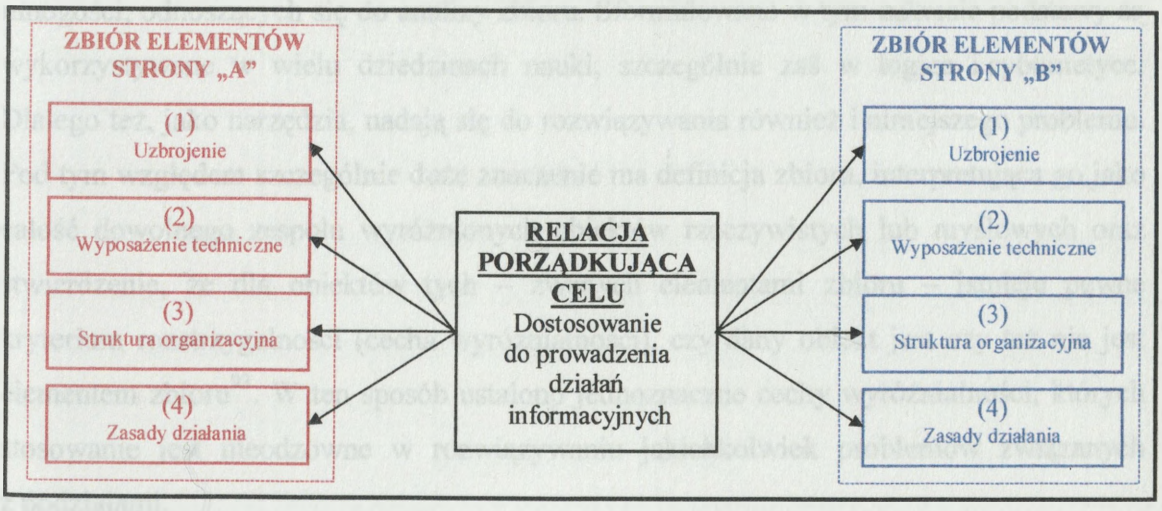
Dlatego też, bez ich uwzględniania, można tylko wyodrębniać podzbiory (podprzestrzenie) jednorodnych ze zbioru pełnego, ale zbiór pełny pozostaje nadal w stanie dużej entropii – w dużym stopniu nieuporządkowania, ponieważ zbiór jednorodny to taki, którego elementy uznaje się za identyczne w stopniu wystarczającym do danych celów.

Podziału takiego – bez uwzględniania relacji przeciwzwrotnej, przechodniości i spójności – można dokonywać, ale tylko w okolicznościach potrzeb skrótowego porozumiewania się, kiedy porozumiewające się strony doskonale wiedzą, jakie zbiory elementów kryją się pod wyróżnioną cechą. Na przykład taką cechą wyróżniającą może być konkretna jednostka organizacyjna, konkretny obszar, przestrzeń geometryczna, środowisko, element ugrupowania itp. Będzie się wtedy mówiło o walce informacyjnej



Rys. 4.1.14. Model przestrzeni działań informacyjnych

Z powyższego wynika, że podstawową strukturę[92] przestrzeni działań informacyjnych tworzą elementy, przynajmniej dwóch zbiorów, należące do przeciwnych sobie stron, które zespolone są wspólną relacją porządkującą celu ukierunkowaną na prowadzenie działań informacyjnych. Elementy te stanowią specjalnie przygotowane do tej walki: uzbrojenie, wyposażenie techniczne, system organizacyjny i system szkolenia wojsk oraz sposoby wykorzystywania tego w działaniach (rys. 4.1.15).

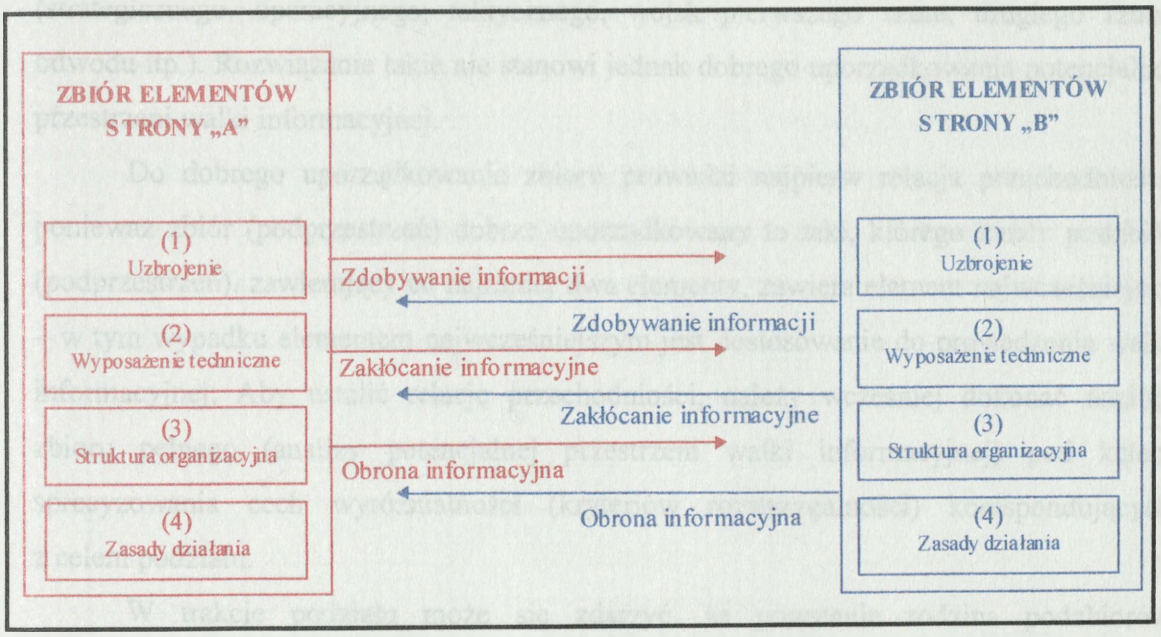


Rys. 4.1.15. Model przestrzeni działań informacyjnych

Działalność tych elementów ukierunkowana jest na realizację trzech podstawowych grup zadań, związanych ze zdobywaniem informacji o przeciwniku (prowadzeniem rozpoznania), zakłócaniem informacyjnym (zakłócaniem procesów informacyjnych

[92]Struktura to układ i wzajemne relacje elementów stanowiących całość. *Słownik języka polskiego*, Warszawa, PWN, 1981, t. 3, s. 352.

przeciwnika) i obroną informacyjną (obroną własnych procesów informacyjnych przed rozpoznaniem i zakłóceniami stosowanymi przez przeciwnika) – rys. 4.1.16.



Rys. 4.1.16. Model przestrzeni działań informacyjnych

Zasady wyznaczania przestrzeni działań informacyjnych oparto na regułach teorii mnogości, odnoszących się do analizy zbioru. Sformułowane w tym zakresie podstawy są wykorzystywane w wielu dziedzinach nauki, szczególnie zaś w logice i cybernetyce. Dlatego też, jako narzędzia, nadają się do rozwiązywania również i niniejszego problemu. Pod tym względem szczególnie duże znaczenie ma definicja zbioru, interpretująca go jako całość dowolnego zespołu wyróżnionych obiektów rzeczywistych lub myślowych oraz stwierdzenie, że dla obiektów tych – zwanych elementami zbioru – istnieje pewne kryterium rozstrzygalności (cecha wyróżnialności), czy dany obiekt jest czy też nie jest elementem zbioru[93]. W ten sposób ustalono jednoznaczne cechy wyróżnialności, których stosowanie jest nieodzowne w rozwiązywaniu jakichkolwiek problemów związanych z podziałami.

Wyznaczanie podprzestrzeni działań informacyjnych wiąże się z porządkowaniem zbioru. Proces ten powinien prowadzić do takiego rozwiązania, w którym na ostatnim poziomie podziału potencjalnej przestrzeni działań informacyjnychwszystkie jej elementy (uzbrojenie, wyposażenie techniczne, struktura organizacyjna, procedura szkolenia i zasady działania), ze względu na relację porządkującą celu, odnoszącą się do

[93]K. Kuratowski, A. Mostowski, *Teoria mnogości,* Warszawa, 1978, PWN, s. 255; .J. Słupecki, K. Hałkowska, K. Piróg-Rzepecka, *Logika i teoria mnogości*, Warszawa, PWN, 1994, s. 204; Z. Ziembiński, *Logika praktyczna*, Warszawa, PWN, 1994, s. 58.

konkretnego rodzaju sił zbrojnych, konkretnego okręgu wojskowego, związku taktycznego, konkretnego szczebla organizacyjnego czy też ugrupowania bojowego (strategicznego, operacyjnego, taktycznego, wojsk pierwszego rzutu, drugiego rzutu, odwodu itp.). Rozwiązanie takie nie stanowi jednak dobrego uporządkowania potencjalnej przestrzeni walki informacyjnej.

Do dobrego uporządkowania zbioru prowadzi najpierw relacja przechodniości, ponieważ zbiór (podprzestrzeń) dobrze uporządkowany to taki, którego każdy podzbiór (podprzestrzeń), zawierający co najmniej dwa elementy, zawiera element najwcześniejszy – w tym wypadku elementem najwcześniejszym jest dostosowanie do prowadzenia walki informacyjnej. Aby ustalić relację przechodniości, należy wcześniej dokonać analizy zbioru pełnego (analizy potencjalnej przestrzeni walki informacyjnej) pod kątem sprecyzowania cech wyróżnialności (kryteriów rozstrzygalności) korespondujących z celem podziału.

W trakcie podziału może się zdarzyć, że powstanie rodzina podzbiorów (podprzestrzeni) jednorodnych, ale ich suma nie będzie odtwarzać zbioru pełnego, który był pierwotnym przedmiotem podziału, to znaczy:

$$A_1 \cup A_2 \cup ... \cup A_n \neq 1^*$$

Może się też okazać, że na pewnym poziomie podziału, iloczyn wyróżnionych podzbiorów nie będzie zbiorem pustym:

$$\wedge_i \wedge_j \left(A_i \cap A_j\right) \neq 0^*$$

W takich wypadkach należy jeszcze raz wrócić do analizy cech wyróżnialności – ponownego ustalenia ich stopnia rozstrzygalności. Wprowadzając do tego stosowne korekty, należy dalej tak poprowadzić proces podziału, aby w ostateczności spełnione zostały te warunki, to znaczy:

$$A_1 \cup A_2 \cup ... \cup A_n = 1^*$$

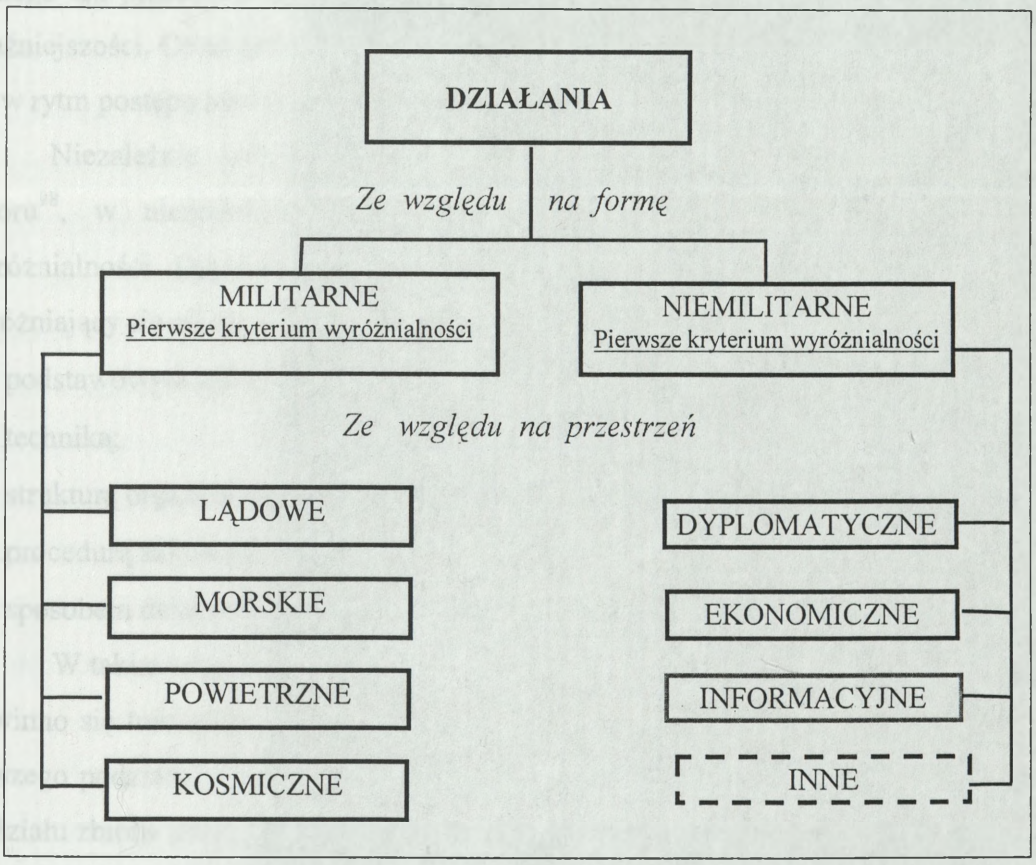
$$\wedge_i \wedge_j \left(A_i \cap A_j\right) = 0^*$$

Osiągnięcie tego będzie jednoznaczne z dobrym uporządkowaniem (podziałem) zbioru pełnego (przestrzeni działań informacyjnych).

Przestrzeń działań wyróżnia się spośród innych przestrzeni tym, że w jej zbiorze przedmiotowym (w granicach tej przestrzeni) prowadzone są działania, co najmniej dwupodmiotowe o przeciwnych celach, w których obydwa podmioty w sposób świadomy przeszkadzają sobie w osiąganiu celów.

Działania mogą być zatem prowadzone różnymi układami skoordynowanych elementów, tzn. w różnych formach[94]. Jeśli układy skoordynowanych elementów dostosowane będą do fizycznego niszczenia przeciwnika, z wykorzystaniem środków śmiercionośnych, wówczas można mówić o działaniach militarnych. Jeśli natomiast bez ich wykorzystania, wówczas można mówić o działaniach niemilitarnych.

Kolejne poziomy podziału powinny być wyznaczone przez kryterium przestrzeni (środowiska). W następstwie tego działania militarne można podzielić na: lądowe, morskie, powietrzne, kosmiczne. Natomiast w działaniach niemilitarnych można wyróżnić: dyplomatyczne, ekonomiczne, informacyjne i inne, w zależności od środowiska (rys. 4.1.17).



Rys. 4.1.17. Miejsce działań informacyjnych w kategorii „działania"

Przyjmując tak ulokowane działania informacyjneza pierwotny przedmiot podziału, można powiedzieć, że stanowi zbiór pełny $\{A_{(I)}\}$ wszelkich układów skoordynowanych elementów dostosowanych do prowadzenia tych działań i zespołów wszelkich czynników

[94]Forma to zewnętrzny kształt, postać, wygląd czegoś; *układ skoordynowanych elementów*; sposób postępowania. *Słownik języka polskiego*, Warszawa, PWN, 1979, t. 1, s. 602.

oddziałujących informacyjnie na te układy. Zatem pierwotną cechą wyróżnialności jest dostosowanie formy układu skoordynowanych elementów do prowadzenia działań w środowisku informacyjnym. Nie jest to jednak równoznaczne z interpretowaniem zbioru $\{A_{(I)}\}$ jako skończonego[95], tzn. o raz na zawsze ustalonej mocy[96] – o raz na zawsze ustalonej liczbie jego elementów materialnych i niematerialnych oraz procesów i rozwiązań funkcjonalnych. Interpretacja taka ograniczałaby podział tylko do znanych dziś elementów zbioru. Nie mogłaby być uwzględniana w nim (w tym podziale) sytuacja rozwojowa wojsk, a więc nie byłoby miejsc wolnych (miejsc zarezerwowanych) dla tych wszystkich elementów, które mogą się pojawić w przyszłości w strukturze działań informacyjnych, a które są dziś trudne, a nawet niemożliwe do dokładniejszego ustalenia. Dlatego też przestrzeń tę należy traktować jako zbiór skończony, ale tylko w aspekcie teraźniejszości. Co do przyszłości należy ją widzieć jako zbiór nieskończony[97], rozwijający się w rytm postępu naukowego i technologicznego.

Niezależnie jednak od liczby i rodzajów pojawiania się nowych elementów zbioru[98], w niezmienionej postaci powinny pozostawać podstawowe cechy jego wyróżnialności (kryteria rozstrzygalności). W dalszym ciągu będzie to potencjał odróżniający się od innych,

— podstawowym uzbrojeniem,

— techniką;

— strukturą organizacyjną;

— procedurą szkolenia;

— sposobem działania.

W takim rozumieniu wymienione cechy wyróżnialności (kryteria rozstrzygalności) powinno się traktować jako pierwotne i wystarczająco zdefiniowane do przeprowadzenia dalszego podziału, a nade wszystko do jednoznacznego sformułowania celu zasadniczego podziału zbioru $\{A_{(I)}\}$, to znaczy podziału przestrzeni działań informacyjnych.

Cel zasadniczego podziału przestrzeni działań informacyjnych, jak już zaznaczano, wynika z ogólnych cech wyróżnialności (z kryteriów rozstrzygalności) kwalifikujących elementy tego zbioru do wspólnego rodzaju wojsk. Ponadto podział zasadniczy powinien być tylko jeden. Wynika to z idei nawiązującej do założeń pierwotnych, rozstrzygających

[95]Zbiór skończony – zbiór o skończonej liczbie elementów.
[96]Moc zbioru – liczba elementów zbioru skończonego lub jego liczba kardynalna dla zbiorów skończonych i nieskończonych.
[97]Zbiór nieskończony – zbiór o nieskończonej liczbie elementów.
[98]Element zbioru – dowolnie wyróżniony obiekt rzeczywisty czy też myślowy.

w ogóle o wyróżnianiu tego rodzaju potencjału jako odrębnego zbioru pełnego w strukturze wojsk. Wszystkie inne podziały, niepodporządkowane temu, mogą być nazywane tylko uzupełniającymi lub pomocniczymi, a ich liczba jest nieograniczona. Warunkują ją zawsze występujące w danej chwili potrzeby, których granice trudne są do dokładniejszego wyznaczenia.

Z ogólnych cech wyróżnialności (z kryteriów rozstrzygalności) wynika, że celem zasadniczego podziału powinno być takie pogrupowanie (usystematyzowanie) techniki (uzbrojenia i wyposażenia) i stanów osobowych, które na kolejnych poziomach podziału prowadziłoby do coraz to większego ujednorodnienia zasad działania tych grup na polu walki i procesu ich szkolenia w okresie pokoju. Spełnienie tego warunku sprzyjać może właściwemu profilowaniu:

— wewnętrznych struktur organizacyjnych wojsk,
— wymagań profesjonalnych;
— kryteriów naboru stanu osobowego;
— procesu przygotowywania kadr i szkolenia wojsk.

Jak już stwierdzono, zasadnicze cechy wyróżnialności (kryteria rozstrzygalności) wynikają z dostosowania skoordynowanych elementów, czyli z dostosowania danych form do prowadzenia działań informacyjnych. Ulokowane są w fizycznych możliwościach podstawowej techniki (w uzbrojeniu i wyposażeniu), a mówiąc inaczej, w ich fizycznym dostosowaniu do realizacji zadań w określonych środowiskach informacyjnych. Hierarchizując je, można powiedzieć, że pierwszoplanowe są zawsze cechy wyróżnialności (kryteria rozstrzygalności), wynikające z ogólnego kształtu układu skoordynowanych elementów przygotowanych do konkretnego działania podczas realizacji celów działań informacyjnych. Kolejnymi są dopiero cechy określające środowisko działań informacyjnych, czyli zespoły czynników, które będą oddziaływać na układy skoordynowanych elementów tych działań – będą oddziaływać na konkretne formy podejmowanych działań. Innymi słowy, pierwsza cecha wyróżnialności (kryterium rozstrzygalności) winna dawać odpowiedź na pytanie: w jakiej formie odbywać się będzie realizacja celów działań informacyjnych? Druga natomiast winna odpowiadać: w jakim środowisku informacyjnym realizowane będą konkretne działania?

Pierwszą cechą wyróżnialności, wynikającą z przeznaczenia, jest dostosowanie potencjału do prowadzenia działań informacyjnych. Wszystkie elementy przystosowane do

tego tworzą zbiór pełny $\{A_{(1)}\}$, zwany przestrzenią działań informacyjnych, który ze względu na tę cechę jest zbiorem jednorodnym.

Działania informacyjne nie są jednak jednorodnym kompleksem przedsięwzięć. W jego strukturze wyraźnie wyróżniają się trzy podstawowe rodzaje działań, ukierunkowane na:

— zdobywanie informacji (prowadzenie rozpoznania),

— zakłócanie informacyjne,

— obronę informacyjną.

Dlatego też druga cecha wyróżnialności powinna umożliwiać podział potencjalnej przestrzeni działań informacyjnych na trzy podprzestrzenie (podzbiory), w których zgrupowane będą wszystkie układy skoordynowanych elementów, dostosowane do realizacji wyżej wymienionych zadań. Zatem zbiór podstawowy $\{A_{(1)}\}$ należy podzielić na:

$\{A_{(1,1)}\}$ – podzbiór układów skoordynowanych elementów, dostosowany do zdobywania informacji (podprzestrzeń rozpoznania);

$\{A_{(1,2)}\}$ – podzbiór układów skoordynowanych elementów, dostosowany do prowadzenia zakłócania informacyjnego (podprzestrzeń zakłócania informacyjnego);

$\{A_{(1,3)}\}$ – podzbiór układów skoordynowanych elementów, dostosowany do prowadzenia obrony informacyjnej (podprzestrzeń obrony informacyjnej).

Podział ten spełnia wszystkie warunki dobrego porządkowania zbioru. Jest poprawny merytorycznie, ponieważ:

— jest wewnętrznie spójny – w każdym wyróżnionym podzbiorze występuje najwcześniejszy element wyróżnialności (najwcześniejsze kryterium rozstrzygalności), który wynika z desygnatu pojęcia działania informacyjne;

— spełnia warunek zupełności – działania informacyjne, w których jeden z podmiotów przeciwdziała drugiemu, może być prowadzona tylko w formie zdobywania informacji, zakłócania i obrony informacyjnej. Zatem te trzy układy skoordynowanych elementów składają się na całość nazywaną działania informacyjne;

— spełnia warunek rozłączności – żaden element skoordynowanego układu zdobywania informacji (rozpoznania) nie spełnia ani funkcji zakłócania informacyjnego, ani funkcji obrony informacyjnej.

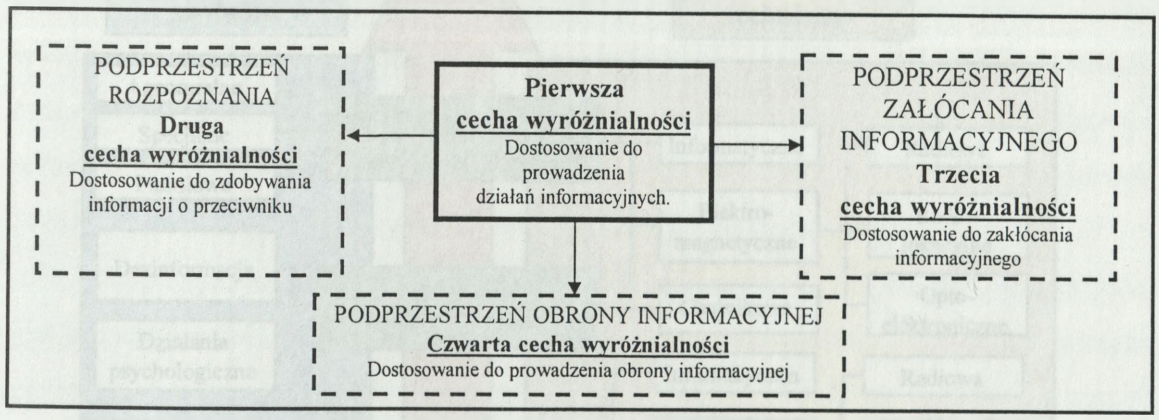
Z powyższego wynika, że w ogólnej przestrzeni działań informacyjnych, ze względu na kryterium formy, należy najpierw wyróżnić:

— przestrzeń, w której dwie przeciwstawne strony rywalizują o zdobywanie informacji (przestrzeń rozpoznania) – w przestrzeni tej rozpoznanie rywalizuje (prowadzi walkę) z zakłócaniem informacyjnym i obroną informacyjną;

— przestrzeń, w której dwie strony rywalizują o zakłócanie procesów informacyjnych przeciwnika (przestrzeń zakłócania informacyjnego) – w przestrzeni tej zakłócanie informacyjne prowadzi walkę z rozpoznaniem i obroną przeciwnika;

— przestrzeń, w której dwie strony rywalizują o obronę własnych informacji i procesów informacyjnych przed rozpoznaniem i zakłócaniem (przestrzeń obrony informacyjnej).

Można zatem powiedzieć, że ze względu na kryterium formy, działania informacyjne skupiają się na: zdobywaniu informacji (rozpoznanie), zakłócaniu i obronie informacyjnej (rys. 4.1.18).



Rys. 4.1.18. Przestrzeń działań informacyjnych

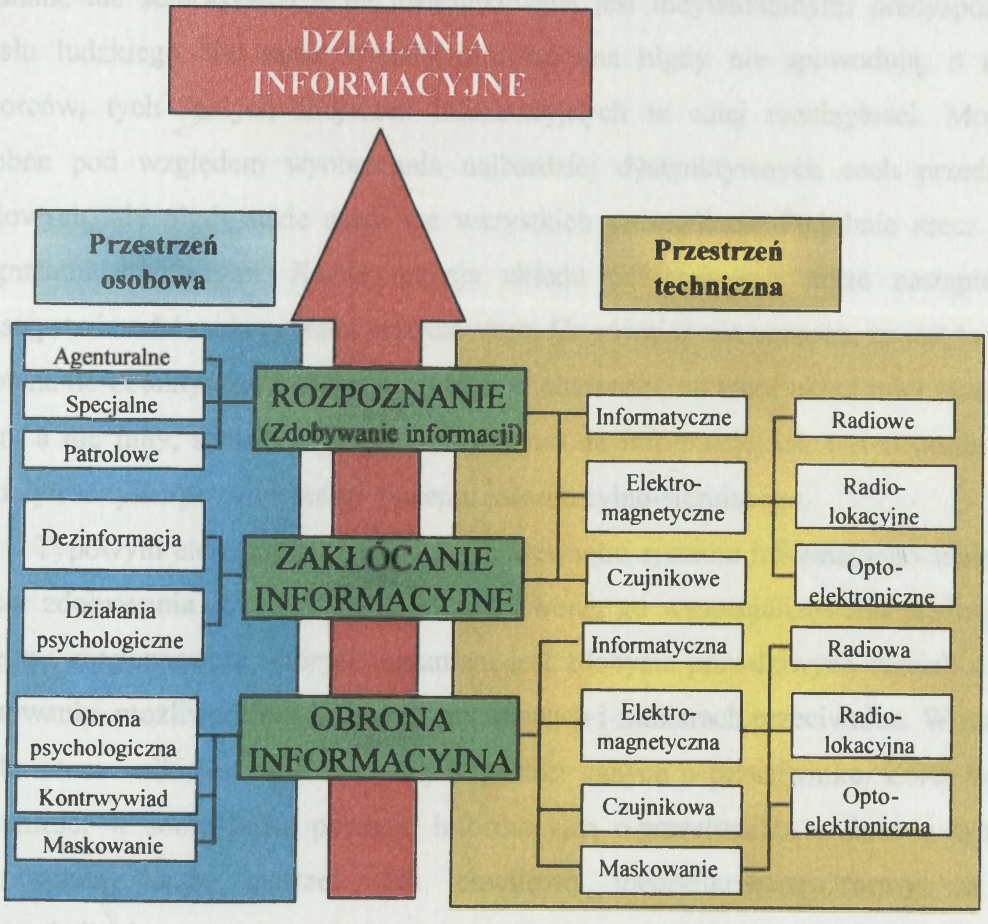
Przestrzeń działań informacyjnych to zbiór skoordynowanych elementów (przynajmniej dwóch przeciwstawnych stron), których istota, ze względu na relację porządkującą celu, skupiona jest w podprzestrzeniach: zdobywania informacji (rozpoznania), zakłócania informacyjnego i obrony informacyjnej.

Podprzestrzeń zdobywania informacji (rozpoznania) to układ skoordynowanych elementów dostosowanych do spełniania swej roli w środowisku elektromagnetycznym, akustycznym, magnetycznym i chemicznym, przez których pryzmat możliwe jest identyfikowanie aktualnego stanu pola walki.

Podprzestrzeń zakłócania informacyjnego to układ skoordynowanych elementów dostosowanych do wnoszenia entropii informacyjnej do komunikatów i powodowania destrukcji fizycznej nośników tych komunikatów i nośników danych.

Podprzestrzeń obrony informacyjnej to układ skoordynowanych elementów, których celem jest uniemożliwienie i utrudnienie zdobywania danych o fizycznej naturze aktualnego i planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania oraz uniemożliwienie i utrudnienie wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do ich nośników.

Przestrzeń osobową działań informacyjnych tworzą narzędzia i procesy dostosowane do oddziaływania w sferze środowiska informacyjnego, które jest bezpośrednio postrzegalne zmysłami ludzkimi (rys. 4.1.19).



Rys. 4.1.19. Podział przestrzeni działań informacyjnych

Przestrzeń techniczną działań informacyjnych tworzą wszelkie narzędzia i procesy dostosowane do oddziaływania w sferze środowiska informacyjnego, które jest bezpośrednio niepostrzegalne zmysłami ludzkimi.

Z powyższej klasyfikacji wynika, że przedmiotem działań informacyjnych może być umysł człowieka lub system informacyjno-sterujący i jego otoczenie. Oddziaływanie informacyjne w stosunku do człowieka jest utrudnione, ze względu na to, że na informacje,

które są niematerialne, nie można przecież oddziaływać bezpośrednio środkami materialnymi. Nie można ich bezpośrednio niszczyć. Brak jakiejkolwiek wiedzy o stanie otoczenia jest również dla człowieka informacją. Jest inspiracją dla ludzkiego umysłu do kształtowania stosownego o tym wyobrażenia (informacji). Każde wyobrażenie umysłu ludzkiego spowodowane jakimkolwiek bodźcem jest zawsze informacją prawdziwą. Nie oznacza to jednak, że stworzony w umyśle ludzkim informacyjny obraz otoczenia na podstawie recepcyjnie transformowanych sygnałów informacyjnych jest obiektywnie prawdziwym odzwierciedleniem rzeczywistości. Jest informacją prawdziwą – bo zaistniała, ale subiektywną – bo uwarunkowana jest indywidualnymi predyspozycjami umysłu ludzkiego. Te same sygnały informacyjne nigdy nie spowodują, u różnych odbiorców, tych samych skojarzeń informacyjnych w całej rozciągłości. Mogą być podobne pod względem wyobrażania najbardziej dystynktywnych cech przedmiotów myślowych, ale nigdy takie same we wszystkich szczegółach. Podobnie rzecz się ma z sygnałami sterującymi. Każda reakcja układu odbierającego może nastąpić tylko w następstwie odebrania sygnału prawdziwego. Co również nie oznacza, że jest to reakcja stosowna do obiektywnie panującej sytuacji w otoczeniu, na którą układ miał zareagować w ten, a nie inny, sposób. Dlatego też zarówno na informacje, jak i sterowanie można oddziaływać tylko przez elementy systemu informacyjno-sterującego.

Typowym elementem występującym wewnątrz systemu informacyjno-sterującego, jest tor zdobywania danych o przeciwniku. Tworzą go wyspecjalizowane profesjonalnie narzędzia rozpoznawcze, których zadaniem jest zdobycie prawdziwych danych o stanie, usytuowaniu, możliwościach działania oraz planach i zamiarach przeciwnika. W torze tym przedmiotem walki jest zbiór możliwych postaci danych o przeciwniku. Zbiór ten, jako taki, mieści w sobie pełną potencję informacyjną o przeciwniku, a dane o tym 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 oraz jakie wyobrażenia informacyjne może inspirować ta upływność przy różnych zestawieniach konfiguracyjnych. 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.

Obrona zbioru postaci danych może być realizowana różnymi sposobami i narzędziami. Istota tej obrony sprowadza się do stwarzania warunków uniemożliwiających przeciwnikowi przechwytywanie danych, szczególnie tych ich postaci, które zawierają największą potencję informacyjną o ważnych sytuacjach rzeczywistych. Nie zawsze jednak jest to możliwe. Nie zawsze też pewne postacie danych można ukryć. Dlatego w ramach obrony informacyjnej, oprócz ukrywania, stosowane jest jeszcze maskowanie danych. Jego istota sprowadza się do stosowania takich rozwiązań, które powodują tylko zmianę wartości potencjału informacyjnego określonych postaci danych. Przykładem może być chociażby technika stealth. Jej zastosowanie w lotnictwie spowodowało pomyłki operatorów radiolokatorów podczas identyfikowania wykrywanych obiektów. Zmniejszona pozornie skuteczna powierzchnia odbicia samolotu daje na wskaźniku stacji radiolokacyjnej obraz znacznie mniejszy niż w rzeczywistości. Dlatego też taka postać danej nie tylko ukrywa określoną rzeczywistość, ale również i dezinformuje.

Zakłócanie toru zdobywania danych może być prowadzone różnymi sposobami z wykorzystaniem różnych narzędzi. System zakłócania jest bardziej złożony niż obrony informacyjnej. System ten spełnia dwie podstawowe funkcje. Chociaż służy tylko 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. Procedura destrukcyjnego oddziaływania na tor zdobywania danych (system rozpoznania) realizowana jest z zamysłem uniemożliwiania przeciwnikowi wykorzystywania tych postaci danych, do których udało się mu zdobyć dostęp, mimo stosowania obrony informacyjnej. Wykorzystując różne techniki energetycznego oddziaływania można niszczyć i czasowo uniemożliwiać pracę źródłom zdobywania danych, przetwornikom danych oraz układom odbierającym. Można także zmieniać strukturę nośników danych i nośników sygnałów, niszcząc tym samym lub zniekształcając zawarty w nich potencjał informacyjny. Inny charakter mają działania pozorujące. Ich celem jest zawsze generowanie i udostępnianie przeciwnikowi zbiorów takich postaci danych, które po przetworzeniu i opracowaniu stwarzać będą obrazy sytuacyjne i zarysy rozwiązań koncepcyjnych, które z rzeczywistością nie mają nic wspólnego, względnie bardzo mało. Niezależnie jednak od tego ich zakłócająca funkcja zawsze ukierunkowana jest na jak największe dezinformowanie przeciwnika. Sposoby i narzędzia

wykorzystywane w prowadzeniu tych działań są bardzo złożone. Ich rodzajowa i ilościowa rozpiętość musi być tak dobierana, aby swoją strukturą i rolą funkcjonalną generowała do toru zdobywania danych przeciwnika takie ich postacie i w takiej liczbie, które stwarzać będą symptomy rzeczywistych działań, sytuacji i zamiarów. Dlatego też działania pozorujące muszą być synchronizowane z innymi, w tym szczególnie z obroną informacyjną i z rozpoznaną już przez przeciwnika częścią działań i planów rzeczywistych. Oderwane od siebie elementy działań pozorujących nie tylko nie wprowadzają przeciwnika w błąd, ale wręcz demaskują, że takie są prowadzone, co zamiast entropii zwiększa stan uporządkowania wiedzy o otoczeniu. Dlatego też podejmowane w tym zakresie przedsięwzięcia muszą być dostatecznie: scentralizowane, kompleksowe, spójne, wiarygodne, nieszablonowe, skryte, terminowe, ciągłe i elastyczne.

W torze zbierania danych o własnym potencjale walka ma nieco inny charakter niż w torze zdobywania danych o przeciwniku. Skupiona jest głównie na problematyce zachowywania i dezorganizowania jego sprawności funkcjonalnej. Wynika to z tego, że sukces w kooperacji negatywnej wzajemnej warunkowany jest sprawnością kierowania. Jakość tego procesu odzwierciedla się w trafności podejmowanych decyzji. Dlatego też do osiągnięcia tego nie wystarcza tylko znajomość przeciwnika. Konieczna jest jeszcze dobra znajomość chwilowych stanów własnego potencjału. Z tego też względu organy kierujące (sterujące) walką starają się wszelkimi sposobami zapewniać sobie ciągły napływ wiarygodnych i precyzyjnych danych o rzeczywistym stanie, usytuowaniu i rezultatach prowadzonej walki.

Tor zbierania danych o własnym potencjale jest przedmiotem zainteresowania organów rozpoznania i zakłócania przeciwnika. Wynika to głównie z tego, że wiedza o nim jest potrzebna przeciwnikowi przy doborze narzędzi i sposobów zakłócania. Dla przeciwnika ważne są też sygnały informacyjno-sterujące, niosące w sobie wiedzę o stanie i sytuacji potencjału walki kooperanta negatywnego – na podstawie tego można oceniać, jak w odczuciach przeciwnika zmaterializowały się skierowane przeciwko niemu określone działania negatywne. Pamiętać jednak należy, że w tej części systemu istnieją szczególnie dogodne warunki do dezinformowania przeciwnika drogą celowo dozowanej upływności informacyjnej[99]. W torze kierowania własnym potencjałem walka informacyjna skupia się głównie wokół problematyki rozpoznania i ochrony treści

[99]Upływność informacyjna to celowe lub uboczne emitowanie do otoczenia treści przez system informacyjno-sterujący. W tym przypadku chodzi o celowe emitowanie takich treści, które do systemu rozpoznawczego przeciwnika wnosić będą entropię informacyjną i tym samym powodować zakłócanie.

informacyjnych. W tym miejscu systemu informacyjno-sterującego przekazywane są najważniejsze treści o zamiarach i decyzjach użycia potencjałów walki zaangażowanych stron. Dlatego też kooperanci negatywni, z jednej strony, starają się zdobyć do niego jak największy dostęp, z drugiej zaś strony, czynią wszystko, aby w stosunku do własnego toru uniemożliwić to przeciwnikowi. Charakterystyczne przy tym jest jeszcze, że fakty uzyskanego dostępu rozpoznawczego muszą być utrzymywane w jak największej tajemnicy. Zdemaskowanie tego przez stronę przeciwną staje się dla niej podstawą do stosowania skutecznej dezinformacji. Tor kierowania potencjałem walki może być również przedmiotem zakłócania, które może spełniać tylko dwie funkcje. Działając destrukcyjnie na nierozpoznawane kanały toru kierowania potencjałem walki, może zmuszać przeciwnika do intensywniejszego wykorzystywania kanałów rozpoznawanych. Jest to działanie ukierunkowane na wymuszanie większej upływności informacyjnej. Realizowane jest jako działanie na korzyść wsparcia rozpoznania. Może być też prowadzone autonomicznie, ale tylko w newralgicznych momentach walki, gdzie masowe zakłócenia stanowić będą „zaporę" w kierowaniu potencjałem walki przeciwnika i tym samym powodować będą dezorganizację jego działań. Stosowanie natomiast ciągłego zakłócania toru kierowania potencjałem walki jest niepożądane. Uświadamia tylko przeciwnikowi, że kooperant negatywny posiadł już dostęp do tego toru i trzeba czynić wszystko, aby jak najszybciej dokonać w nim takich zmian strukturalnych i parametrycznych, które wyeliminują ten dostęp. Innymi słowy, taki sposób postępowania w procesie walki informacyjnej można nazywać działaniami demaskującymi. W tym miejscu można by powiedzieć, że tor kierowania potencjałem walki funkcjonuje w podobnym otoczeniu do toru zbierania danych o własnym potencjale walki i o sytuacji. Różnica polega tylko na przewartościowaniu roli rozpoznania i zakłócania informacyjnego. Jeśli w stosunku do pierwszego (chodzi o tor zbierania danych o własnym potencjale walki i sytuacji) zasadnicze wysiłki kooperacji negatywnej ukierunkowane były na zakłócanie treści informacyjnych, a rozpoznanie odgrywało rolę drugoplanową, to w stosunku do drugiego (chodzi o tor kierowania potencjałem walki) pierwszoplanową rolę negatywną odgrywa rozpoznanie, a drugoplanową – zakłócanie.

W systemie informacyjno-sterującym odrębnymi przedmiotami walki są elementy kierujące walką i sterujące jej określonymi procesami. W organach takich (centrach) szeroko stosuje się dzisiaj technologie informacyjne 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. Dlatego też elementy te, jako przedmioty oddziaływania, są szczególnym obiektem zainteresowania działań informacyjnych. Dla strony przeciwnej są obiektami rozpoznania i zakłócania, dla własnej – pieczołowitej obrony informacyjnej.

Nie mniej ważny od wypracowywania decyzji jest również proces jej wdrażania do realizacji. Pod tym względem szczególną rolę odgrywa terminowość i skrytość realizacji poszczególnych przedsięwzięć. Nawet najtrafniej podjęte decyzje nie spowodują osiągnięcia sukcesu, jeśli zostaną wdrożone do realizacji nieterminowo lub zostaną wcześniej ujawnione kooperantowi negatywnemu. Przy porównywalnych potencjałach sukces może osiągnąć tylko ta strona, która zdoła szybciej i trafniej od przeciwnika wykorzystać swój potencjał do walki z nim. Można więc powiedzieć, że w kooperacji negatywnej wzajemnej cała procedura planowania działań sprowadza się do wypracowywania takich decyzji o ruchu i użyciu własnego potencjału, które po wdrożeniu do realizacji spowodują takie usytuowanie narzędzi walki, które będzie sprzyjać najlepszemu ich wykorzystaniu i tym samym osiąganiu zwycięstwa nad przeciwnikiem. Można więc powiedzieć, że kooperujące negatywnie strony dążą w istocie do tego samego z tą tylko różnicą, że podejmowane wysiłki posiadają przeciwnie skierowane zwroty.

Można zatem powiedzieć, że 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 (przestrzeni) – w walce o czas i precyzję działania – mieści się funkcjonalna rola działań informacyjnych. Jako że ich przedmiotem są systemy informacyjno-sterujące, ich efekty będą się materializować w sprawności i skuteczności funkcjonowania tych systemów.

Efektywność działań informacyjnych zależy od wielu czynników. Jednym z najważniejszych jest trafność doboru narzędzi i form ich wykorzystywania w procesie oddziaływania na systemy informacyjno-sterujące. Ich zróżnicowanie wynika z niejednorodności strukturalnej tych systemów. 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 i 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.

Jak już wspominano, struktury działań informacyjnych mają przedstawić przeciwnikowi fałszywy obraz rzeczywistości w przestrzeni planowanej przez niego operacji i przez to ukierunkować jego wysiłki na planowanie i prowadzenie działań w stosunku do nieistniejących lub nieistotnych dla sukcesu odniesień. Realizuje się to po to, aby zasadnicze narzędzia walki przeciwnika znalazły się w takim usytuowaniu, jakiego życzy sobie jego kooperant negatywny. Osiągnięcie tego, w sposób nieświadomy dla przeciwnika, jest przedsięwzięciem niezmiernie trudnym i złożonym. Wiąże się przede wszystkim ze spójnością dozowanej mu specjalnie upływności informacyjnej, której szczegóły, w całej swej masie, muszą się składać na jednolicie logiczny obraz. Każdy przeciwnik zwykle zdaje sobie sprawę, że działająca negatywnie strona czynić będzie takie wysiłki. Dlatego też każdą zdobytą postać danej będzie się starał wielokrotnie sprawdzać, gruntownie analizować i potwierdzać w innym obszarze. Stwierdzone w tym zakresie rozbieżności mogą się stać dla niego sygnałem, że takie właśnie wysiłki są czynione przez jego przeciwnika i tym samym mogą doprowadzić do ich zniweczenia. Z tego też względu wszystkie przedsięwzięcia działań informacyjnychpowinny być prowadzone kompleksowo i jednolicie. Każdy organ niższego szczebla powinien realizować tylko te przedsięwzięcia, które zostały mu nakazane przez przełożonego. Wszelka inicjatywa w tym zakresie, ze strony podwładnych, jest niepożądana i może być niezmiernie szkodliwa. W wyjątkowych sytuacjach może być uwzględniana, ale tylko za zgodą organu nadrzędnego. Jest to bezwzględnie zhierarchizowany system kierowania. Niższy szczebel, nie znając rzeczywistych zamiarów i planów, może zdemaskować i tym samym zniweczyć całość przedsięwzięcia, podejmując określone działania z własnej inicjatywy. Z analizy faktów wynika, że nigdy w historii nie zdarzyło się, aby tego typu przedsięwzięcia – podjęte z inicjatywy niższych szczebli kierowania i bez zgody organu centralnego – były skuteczne. Zawsze były demaskowane, a jeśli nawet nie, to i tak przynosiły odwrotne do zamierzonych rezultaty.

Z punktu widzenia potrzeb prowadzenia działań informacyjnych ważna jest wcześniejsza i bieżąca wiedza o przedmiotach tej walki i ich otoczeniu. Tylko taki stan informacyjny może stanowić podstawę do 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 działania celowe, składają 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.

4.2. Kompleks przedsięwzięć działań informacyjnych

W związku z nowymi zagrożeniami na świecie (terroryzm), zakres działań informacyjnych ulega poszerzeniu, będą one prowadzone nie tylko w środowisku wojskowym (MIE), ale także w globalnym środowisku informacyjnym (GIE), w czasie pokoju, kryzysu, konfliktu lub wojny.

Zdaniem Ch. Glazea, (Komitet Połączonych Szefów Sztabów USA) oraz przedstawicieli NATO działania informacyjne mogą jeszcze obejmować: obronę psychologiczną, działania specjalne, atak komputerowy itp.

Na podstawie analizy literatury przedmiotu, dokumentów normatywnych NATO oraz możliwości naszych sił zbrojnych[100], zaproponowano kompleks przedsięwzięć działań informacyjnych, który obejmuje:

— zdobywanie informacji z rozpoznania i wywiadu,
— fizyczne niszczenie systemów informacyjnych,
— walkę elektroniczną (Electronic Warfare),
— bezpieczeństwo informacyjne,
— dezinformację,
— działania psychologiczne (PSYOPS),
— zakłócanie informatyczne,
— maskowanie,
— informowanie opinii publicznej (działalność mediów),
— współpracę cywilno-wojskową.

[100]Udział naszych sił zbrojnych w działaniach sojuszniczych podyktowany jest obroną RP lub obroną innego członka NATO (w ramach obrony kolektywnej wynikającej z artykułu 5 traktatu waszyngtońskiego i reagowania kryzysowego poza artykułem 5 oraz konsultacji i współpracy). Siły Zbrojne RP posiadają obecnie żołnierzy szkolonych w różnorodnych specjalnościach, wliczając w to grupę działań psychologicznych, jednostki specjalne oraz rozpoznania i walki elektronicznej, jednak niewielu żołnierzy ma przygotowanie dające im podstawy do szerszego, całościowego objęcia wszystkich działań realizowanych w ramach działań informacyjnych. Działalność polskich elementów, które mogą być wykorzystane do prowadzenia działań informacyjnych, szczególnie 4 GDP, musi się opierać na procedurach zawartych w dokumentach normatywnych NATO.

Rys. 4.2.1. Kompleks przedsięwzięć działań informacyjnych

Zdobywanie informacji z rozpoznania i wywiadu jest najistotniejszym elementem działań informacyjnych. Przedmiotem rozpoznania jest zbiór możliwych postaci danych o przeciwniku, jego otoczeniu oraz zamiarach i planach działania. Do podmiotów rozpoznania można zaliczyć wszystkich uczestników tego procesu, w tym całe zespoły ludzi, sztaby, organy rozpoznawcze występujące na poszczególnych szczeblach struktury organizacyjnej wojsk, które, zajmując się rozpoznaniem, prowadzą działania informacyjne.

Już od najdawniejszych czasów odpowiednio wczesne uzyskiwanie informacji o miejscu pobytu przeciwnika, jego ugrupowaniu i zamiarach było bardzo ważnym elementem, niezbędnym do podejmowania decyzji, zwłaszcza dla tych dowódców, którzy wiedzieli jak je wykorzystać. Dlatego też każdy dowódca musi zachowywać gotowość do prowadzenia rozpoznania i gromadzenia informacji o przeciwniku.

Znaczenie rozpoznania stale wzrasta, zwłaszcza w warunkach postępującego zwiększania siły uderzeniowej i ruchliwości wojsk oraz zwiększania ich możliwości działania na dużych przestrzeniach. Efektywne wykorzystanie systemów konwencjonalnych o dużej precyzji rażenia, a także innych współczesnych środków walki, w pełni uzależnione jest od posiadania dokładnych danych o siłach przeciwnika.

Wzrastające znaczenie rozpoznania wymusza z kolei rozwój środków i konieczność doskonalenia sposobów jego prowadzenia. Dowodem na to może być fakt, że obecnie –

dzięki osiągnięciom w dziedzinie radioelektroniki i informatyki – istnieją już realne możliwości rozpoznania dowolnego rejonu na kuli ziemskiej.

Proces zdobywania, gromadzenia, przetwarzania i dystrybucji danych i komunikatów powinien być realizowany i doskonalony już w czasie pokoju. W procesie zdobywania danych o siłach i środkach przeciwnika powinny być wykorzystane na szeroką skalę środki informatyczne, które – jak powszechnie wiadomo – umożliwiają tworzenie komputerowych baz danych. W bazach tych powinny być zawarte zbiory umożliwiające: tworzenie dowolnych kompilacji informacyjnych (także w wypadku sytuacji krytycznych), tworzenie prostego „dialogu" z bazą danych w systemie konwersacyjnym (tzn. pytanie – odpowiedź), graficzne zobrazowanie sytuacyjne przeciwnika oraz komputerowe przetwarzanie i dystrybucję w czasie zbliżonym do rzeczywistego.

Istotną rolę w przygotowaniu baz danych o przeciwniku ma przyjęcie odpowiednich kryteriów podziału informacji o jego siłach i środkach, tj. określenie odpowiednich struktur tej informacji.

Złożoność procesów współczesnego pola walki powoduje, że decydenci żądają coraz większej ilości informacji, o coraz szerszym zasięgu tematycznym. Wszystkie informacje dotyczące potencjalnego przeciwnika, jego sił zbrojnych, polityki, ekonomiki, infrastruktury, demografii, nastrojów oraz terenu, warunków hydrologicznych i meteorologicznych, wykorzystywane przez rozpoznanie, noszą nazwę informacji rozpoznawczych. Ważną rolę w procesie ich gromadzenia oraz przetwarzania stanowią bazy danych o siłach i środkach przeciwnika.

Dane wprowadzane do baz danych o siłach i środkach przeciwnika powinny być usystematyzowane oraz zgromadzone w niezależnych zbiorach.

Z uwagi na sytuację polityczno-militarną RP można wyróżnić trzy wzajemnie uzupełniające się zbiory danych o siłach i środkach przeciwnika:

— zbiór okresu pokoju,

— zbiór okresu zagrożenia wojennego,

— zbiór okresu wojny (początkowego okresu wojny).

Baza danych o siłach i środkach potencjalnego przeciwnika powinna być zbudowana już w okresie pokoju. Szczególną uwagę należy zwrócić na te państwa, z którymi kraj nasz nie zawarł sojuszy obronnych. Informacje powinny być gromadzone i weryfikowane na bieżąco.

Dane o siłach i środkach przeciwnika zdobywane są w wyniku prowadzonych działań rozpoznawczych przez etatowe, odpowiednio wyszkolone i wyposażone oddziały

i pododdziały rozpoznawcze, a także doraźnie – przez wydzielone siły i środki z pododdziałów ogólnowojskowych oraz innych rodzajów wojsk na różnych szczeblach dowodzenia (strategicznym, operacyjnym i taktycznym). Podział ten powinien mieć również odzwierciedlenie w strukturze bazy danych o siłach i środkach przeciwnika.

Zdobywanie danych o przeciwniku determinowane jest potrzebami odtwarzania obrazu jego aktualnego stanu i przyszłych zachowań w czasie rzeczywistym lub maksymalnie zbliżonym do rzeczywistego. Dlatego też prowadzenie rozpoznania widziane jest przez pryzmat konstrukcji urządzeń dostosowanych technologicznie do automatycznego, ciągłego, wielofunkcyjnego[101] i wielospektralnego[102] postrzegania zjawisk w materialnej przestrzeni przeciwnika, co umożliwiają urządzenia elektroniczne.

Biorąc pod uwagę pierwszą cechę wyróżnialności, czyli formę, rozpoznanie będzie odzwierciedlać zespół skoordynowanych elementów, który dostosowany jest do zdobywania danych o przeciwniku. Elementami tymi są:

— źródła informacji;
— nośniki informacji;
— układy odbierające.

Podstawowymi elementami w strukturze przestrzeni zdobywania informacji są źródła informacji, które wybierają ze zbioru możliwych postaci danych o przeciwniku tylko te, które są im fizycznie dostępne.

Ze względu na formę dostępu informacyjnego, można wyróżnić:

— rozpoznanie osobowe (wg terminologii NATO – HUMINT– Human Intelligence),
— rozpoznanie nieosobowe (techniczne).

Przestrzeń rozpoznania osobowego tworzy człowiek i wszelkie narzędzia przystosowane do zdobywania danych w postaciach bezpośrednio odbieranych przez układ recepcyjny człowieka. Bezpośrednie ludzkie doznania zmysłowe stanowią podstawowe sygnały informacyjne w identyfikowaniu stanu otoczenia. Pomiędzy zbiorem możliwych postaci danych o otoczeniu i ludzkimi zmysłami nie mogą występować żadne przetworniki zmieniające ich postać.

---

[101] Przyjęto, że postrzeganie wielofunkcyjne to dostosowanie do zbierania informacji w różnych technikach – w różnych przestrzeniach informacyjnych.

[102] Postrzeganie wielospektralne to dostosowanie do jednoczesnego zbierania informacji w kilku różnych zakresach widma elektromagnetycznego.

Oznacza to, że jest dopuszczalne stosowanie urządzeń wspomagających zasięg i czułość doznań zmysłowych, ponieważ te nie zmieniają postaci danych, a czynią je tylko bardziej wyrazistymi. Innymi słowy, określony sygnał informacyjny o przeciwniku dociera do człowieka (zwiadowcy) prowadzącego rozpoznanie w formie bezpośrednio dla niego zrozumiałej. Mogą to być dane zawarte w paśmie promieniowania widzialnego, drgań akustycznych, jak również informacje odbierane dotykowo, smakowo i przez powonienie. Należy w tym wypadku wykluczyć transformowanie na ludzkie doznania danych z obszarów pozazmysłowego poznania i tych, które po detekcji przetwarzane są na sygnały spoza tego poznania. Dlatego też człowiek nie może być pewien, czy poza zasięgiem jego doznań nie dokonano jakiejś deformacji postaci danej, stanowiącej sygnał informacyjny.

Rozpoznanie osobowe jest jednym z najstarszych rodzajów rozpoznania. Do jego prowadzenia można wykorzystywać przedstawicielstwa dyplomatyczne oraz pododdziały wojskowe. Praktycznie przedstawicielstwa dyplomatyczne mogą prowadzić je na szczeblu strategicznym, natomiast pozostałe organa tylko na szczeblu taktycznym. Rozpoznanie osobowe prowadzi zatem człowiek. Jego bezpośredni kontakt ze zbiorami różnych postaci danych o przeciwniku może być zapewniony przez:

— ściśle zakonspirowane działania wywiadowcze;
— fizyczne penetrowanie obszaru drogą patrolowania;
— fizyczne penetrowanie obszaru drogą specjalnie przygotowanych działań.

W zaiązku z tym przestrzeń rozpoznania osobowego należy dzielić na podprzestrzenie:

— rozpoznania agenturalnego;
— rozpoznania patrolowego;
— rozpoznania specjalnego.

Przestrzeń rozpoznania technicznego (nieosobowego) tworzy zespół skoordynowanych źródeł rozpoznania, dostosowany do zdobywania danych w postaciach bezpośrednio nieodbieranych przez układ recepcyjny człowieka. W przestrzeni tej występują przetworniki informacji przekształcające jej pierwotnie przechwyconą postać w postać odbieraną przez układ recepcyjny człowieka. Urządzenia te są zawsze dostosowywane konstrukcyjnie do rejestrowania określonych efektów, charakterystycznych dla danego środowiska (np. elektromagnetycznego, chemicznego). Przez pryzmat rejestrowanych stanów jest identyfikowana sytuacja panująca w ich otoczeniu. Identyfikacji tej dokonuje ostatecznie człowiek, jako najważniejszy element

układu decyzyjnego. Rejestrowane przez przetworniki wartości pomiarowe nie stanowią jednak dla człowieka form bezpośrednio komunikatywnych. Znajdują się poza jego możliwościami postrzegania zmysłowego. Dlatego też muszą być przetwarzane, według odpowiednich algorytmów, do postaci zrozumiałych dla człowieka. Klasycznym tego przykładem może być telewizja, gdzie odbierany na wejściu sygnał elektromagnetyczny – nieodbierany bezpośrednio przez człowieka – przetwarzany jest w torze wizyjnym na konkretny obraz, a w torze fonicznym – na konkretny głos, które człowiek jest już w stanie odbierać. Innymi słowy, rozpoznanie nieosobowe ma na celu zdobywanie i przetwarzanie tych postaci danych o przeciwniku, których nośnikami są fale elektromagnetyczne oraz inne efekty uboczne towarzyszące działaniom bojowym. Postęp naukowo-techniczny pozwolił już na konstruowanie wielu takich urządzeń. Między innymi opracowano całą rodzinę urządzeń dostosowanych do rejestrowania określonych efektów, charakterystycznych dla danego środowiska – elektromagnetycznego, akustycznego, magnetycznego, elektrycznego, chemicznego.

Biorąc pod uwagę powyższe kryterium – środowisko nośników danych – rozpoznanie techniczne można podzielić na:

— *rozpoznanie elektromagnetyczne* (według terminologii natowskiej SIGINT – Signal Intelligence, zdobywanie danych na podstawie emisji elektromagnetycznej obcych systemów elektronicznych);

— *rozpoznanie czujnikowe* (zdobywanie danych na podstawie identyfikowania przeróżnych stanów w środowisku akustycznym, elektrycznym, magnetycznym i chemicznym);

— *rozpoznanie informatyczne* (dane w systemach komputerowych).

Rozpoznanie elektromagnetyczne charakteryzuje się długościami fal zawartymi w przedziale od 0,5 pm do 1 km. W widmie elektromagnetycznym wykorzystywane są głównie fale radiowe, mikrofale i promieniowanie widzialne. Biorąc to pod uwagę, należy jeszcze w przestrzeni rozpoznania elektromagnetycznego wyróżnić podprzestrzenie:

— rozpoznania radiowego;

— rozpoznania radiolokacyjnego;

— rozpoznania optoelektronicznego.

Rozpoznanie czujnikowe może zdobywać oraz przetwarzać dane o przeciwniku, których nośnikami są fale sprężyste (infradźwięki, ultradźwięki) oraz wszelkiego rodzaju

uboczne efekty towarzyszące działaniom bojowym, na przykład: akustyczne, sejsmiczne, magnetyczne, chemiczne, zapachowe itp.

Rozpoznanie informatyczne powinno być natomiast prowadzone z uwagi na masowy rozwój sieci informatycznych, które są bogatymi źródłami danych o siłach i środkach przeciwnika.

Współczesny system rozpoznania wojskowego SZ RP powinien być w pełni zintegrowany i zautomatyzowany. Jego strukturą podstawową powinny tworzyć:

— podsystem stacjonarny,

— podsystemy mobilne.

W czasie pokoju powinien funkcjonować stacjonarny podsystemem rozpoznania wojskowego. W takim ujęciu zintegrowany stacjonarny podsystem rozpoznania mógłby już dziś funkcjonować w oparciu o potencjał: rozpoznania agenturalnego oraz rozpoznania radiowego i radiolokacyjnego (pasywnego i aktywnego) dalekiego zasięgu. W przyszłości można byłoby uzupełnić go powietrznymi elementami dopplerowskiego rozpoznania radiolokacyjnego, jak również wyniesionymi ponad ziemię, w pasie nadgranicznym, elementami horyzontowego rozpoznania radiowego i dopplerowskiego rozpoznania radiolokacyjnego. Przy odpowiednim skonfigurowaniu sieci i właściwie dobranej trasie lotu, rozpoznanie radioelektroniczne mogłoby nieprzerwanie i dość dokładnie śledzić sytuację do 500 km wzdłuż granicy państwowej.

Mobilne podsystemy rozpoznawcze związków operacyjnych, taktycznych oraz oddziałów i pododdziałów powinny funkcjonować w okresie zagrożenia i wojny. Powinny dostarczać dowódcom dane o wojskach przeciwnika i o jego zamiarach, m.in. przez wykrywanie, identyfikację i lokalizację elementów ugrupowania.

Współczesne pole walki stawia przed rozpoznaniem zadania, do których można zaliczyć:

— rozszerzenie przechwytywanego pasma częstotliwości oraz zwiększenie dokładności namierzania, co pozwoli na efektywniejsze zwalczanie obiektów przeciwnika;

— szersze wykorzystanie zdalnie sterowanych aparatów latających;

— stosowanie bardziej złożonych układów „sztucznej inteligencji" w centralnych ogniwach systemu, w celu przyspieszenia konwersji danych do postaci pozwalającej na ocenę sytuacji;

— posiadanie szybko rozwijanych zestawów antenowych;

— integrację urządzeń rozpoznania radioelektronicznego z czujnikami różnych typów.

Na współczesnym polu walki coraz większego znaczenia nabierają satelity rozpoznawcze. Rozpoznanie satelitarne jest obecnie warunkiem *sine qua non* w zakresie zdobywania precyzyjnych i terminowych danych, bez których niemożliwe jest przygotowanie i prowadzenie współczesnych operacji połączonych[103].

Rozwinięte technicznie kraje są już niemal całkowicie uzależnione od przestrzeni kosmicznej, w której znajdują się urządzenia wykrywające i ustalające położenie samolotów, okrętów, czołgów czy innych obiektów (o wielkości 10 cm). Uderzenie w te systemy oznacza nie tylko oślepienie armii, ale też paraliż całych krajów. Wojsko intensywnie pracuje nad urządzeniami, które niszczyłyby wrogie satelity rozpoznawcze i chroniły własne. Systemy rozpoznania satelitarnego są zintegrowane z systemami wojsk lądowych, sił powietrznych i marynarki wojennej oraz systemami wykorzystywanymi przez agencje cywilne.

Fizyczne niszczenie infrastruktury informacyjnej przeciwnika jest prowadzone z dwóch powodów. Po pierwsze, jego celem jest demonstracja przeciwnikowi woli walki i możliwości bojowych wojsk własnych. Po drugie, w znaczny sposób ogranicza ono możliwości dowodzenia przeciwnika przez zniszczenie kluczowych obiektów w jego infrastrukturze informacyjnej. Plan niszczenia obiektów musi być ściśle skoordynowany z planem ochrony systemów informacyjnych.

Fizyczne niszczenie może być realizowane przez: użycie systemów broni precyzyjnej, bezpośrednie wsparcie lotnicze albo też przeniknięcie małej grupy specjalnej w celu zneutralizowania ważnego obiektu w systemie dowodzenia.

W wojnie w Iraku (2003 r.) w ramach fizycznego niszczenia prowadzona była kampania ***„Szok i przerażenie"*** (ang. „Shock and awe"), która miała skłonić przywódców Iraku do kapitulacji oraz sparaliżować irackie siły zbrojne i skłaniać irackich żołnierzy do poddania się.

Przewodniczący Kolegium Szefów Sztabów gen. Richard Myers powiedział, że celem kampanii było kilkaset obiektów rządowych oraz *stricte* wojskowych, do których można zaliczyć: centra łączności, dowodzenia, rozpoznania, punkty obrony przeciwlotniczej. W ramach tej kampanii wykorzystano pociski samosterujące Cruise i Tomahowk. Wystrzeliwane pociski Tomahowk zostały znacznie unowocześnione. Ich podstawową zaletą bojową jest skrytość działania, osiągana dzięki lotowi na minimalnej

[103]Szerszy zakres tej problematyki można znaleźć w pracy G. Nowackiego, *Rozpoznanie satelitarne USA i Federacji Rosyjskiej*, Warszawa, AON, 2002.

wysokości po zaprogramowanej trasie, maksymalnie wykorzystującej walory maskujące terenu.

Niektóre obiekty atakowane były z wykorzystaniem bomb typu JDAM (kierowane za pomocą systemu GPS), które były zrzucane z samolotów B-1, B-2, B-52 oraz innych. Większość przeprowadzanych tym razem ataków powietrznych stanowiły uderzenia z użyciem precyzyjnych środków rażenia na ściśle wyselekcjonowane cele. Taka taktyka minimalizowała przypadkowe zniszczenia i straty, szczególnie wśród ludności cywilnej.

W ramach pierwszej fazy tej kampanii do atakowania siedziby Saddama użyto bomb lotniczych naprowadzanych laserowo GBU-28A („Niszczyciel bunkrów" – Bunker Buster) o zwiększonej sile przebicia.

Zdaniem ekspertów amerykańskich w latach 1990–1991, w pierwszej wojnie w Zatoce Perskiej, odsetek amunicji precyzyjnej w stosunku do ogółem użytej wynosił 7%, w Kosowie – 35, w Afganistanie – 50, natomiast w Iraku – 68 procent.

Walka elektroniczna *(Electronic Warfare – EW)* to przedsięwzięcia związane z zapewnieniem dostępu do spektrum elektromagnetycznego dla wojsk własnych i pozbawienia takich możliwości strony przeciwnej. Obejmuje ona:

— rozpoznanie elektroniczne (ESM — Electronic Support Measures),

— zakłócanie elektroniczne (ECM — Electronic Countermeasures),

— obronę elektroniczną (EPM — Electronic Protection Measures).

W działaniach informacyjnych walka elektroniczna może być prowadzona w formie:

— ataku elektronicznego (EA – Electronic Attack),

— obrony elektronicznej (EP – Electronic Protection),

— wsparcia elektronicznego (ES – Electronic Support).

Atak elektroniczny polega na pozbawieniu przeciwnika dostępu do spektrum elektromagnetycznego, aby nie mógł zdobywać danych z rozpoznania, dowodzić i kierować swoimi wojskami.

Obrona elektroniczna polega na zapewnieniu dostępu do spektrum elektromagnetycznego dla własnych sił zbrojnych.

Wsparcie elektroniczne polega na zdobywaniu danych z rozpoznania elektronicznego i dokładnej ocenie sytuacji w strefie działań.

Walka elektroniczna w ofensywnych działaniach informacyjnych. Wsparcie elektroniczne zapewnia informację bojową w czasie rzeczywistym, wymaganą do

zlokalizowania i identyfikacji obiektów dowodzenia, systemów wczesnego wykrywania oraz rozpoznawczo-uderzeniowych przeciwnika. W ramach wsparcia prowadzone jest rozpoznanie elektromagnetyczne (SIGINT).

Atak elektroniczny ma obezwładnić ww. obiekty przeciwnika. Może to być realizowane za pomocą zakłócania elektromagnetycznego (Electromagnetic Jamming), broni energii kierunkowej (DE – Direction Energy) lub pocisków przeciw-radiolokacyjnych (ARMS – Antiradiation Missiles).

Obrona elektroniczna ma zapewnić dostęp do spektrum elektromagnetycznego dla sił własnych. Ponadto ma zapewnić takie wykorzystanie energii elektromagnetycznej przez siły własne zgodnie z wykazem zakazanych częstotliwości (JFRL – Joint Restricted Frequency List), aby uniknąć zakłóceń wzajemnych.

Walka elektroniczna w defensywnych działaniach informacyjnych. Wsparcie elektroniczne może być wykorzystane do monitorowania zbliżającego się ataku przeciwnika na obiekty dowodzenia oraz jako forma bezpieczeństwa elektromagnetycznego do identyfikacji źródeł informacji, z których przeciwnik uzyskuje kluczowe wiadomości nt. systemów dowdzenia.

Walka elektroniczna jest jednym z filarów działań informacyjnych. Wnosi wiele do oceny sytuacji i procesu podejmowania decyzji. Stosowana jest również do dezintegracji systemu dowodzenia przeciwnika, jak również rozpoznania i systemów kierowania uzbrojeniem. Ponadto w sposób zasadniczy wpływa na utrzymanie ciągłości dowodzenia, rozpoznania i kierowania uzbrojeniem wojsk własnych poprzez zastosowanie obrony elektronicznej.

Użycie struktur walki elektronicznej w operacjach połączonych wymaga ścisłej koordynacji i współpracy pomiędzy komórkami: operacyjną, rozpoznania i łączności. Dlatego też dowódcy wszystkich szczebli dowodzenia są wspomagani przez specjalistów walki elektronicznej, stanowiących obsadę Komórki Koordynacji Walki Elektronicznej – *KKWE* (ang. *Electronic Warfiare Coordination Center – EWCC*).

Komórka (KKWE) przeznaczona jest do kierowania całokształtem przedsięwzięć z zakresu walki elektronicznej, prowadzonych w strefie działań operacyjnych. Stanowi ona integralną część sztabu i odpowiada za planowanie użycia wszystkich organicznych, przydzielonych i współdziałających sił i środków walki elektronicznej.

W działaniach sojuszniczych i koalicyjnych personel komórki (KKWE) powinien składać się z przedstawicieli wszystkich narodowości i zapewnić wsparcie elektroniczne wszystkim zasadniczym elementom ugrupowania.

Pomimo tego, że wyłącznie narodowe dowództwa kierują swoimi jednostkami walki elektronicznej, jednostki te uczestniczą w procesie wymiany danych w układzie sojuszniczym. Dzięki temu dane są przekazywane do komórek analizy danych w celu wykonania dogłębnych analiz, zestawień i rozpowszechnienia oraz do organów dowodzenia, w celu stworzenia warunków do reagowania na zagrożenia oraz zachowania ciągłości dowodzenia.

W działaniach sojuszniczych zasady wymiany informacji powinny być zawarte w odpowiednich aneksach planów operacyjnych (i innych), stałych procedurach operacyjnych (SOP) i publikacjach sojuszniczych. Wspólne procedury walki elektronicznej, jako rezultat procesu planistycznego powinny uwzględniać:

— przegląd danych rozpoznawczych dotyczących wojsk własnych i przeciwnika, które mogą podlegać wymianie;
— tryb prowadzenia wymiany danych w czasie pokoju, kryzysu lub wojny;
— prowadzenie ćwiczeń w czasie pokoju mających na celu usprawnienie wymiany danych;
— znajomość struktur walki elektronicznej sił sojuszniczych (koalicyjnych);
— ustanowienie punktów kontaktowych z sąsiadującymi sojuszniczymi jednostkami walki elektronicznej oraz z wyższym i podległymi dowództwami dla ustalenia celów działania i zasad współdziałania;
— wymianę zespołów łącznikowych wyposażonych w odpowiednie środki łączności;
— przygotowanie i sprawdzenie planów operacyjnych pod kątem wymiany informacji o wojskach własnych i przeciwnika;
— przygotowanie procedur łączności według dokumentu STANAG 5048;
— zapewnienie bezpieczeństwa i żywotności systemom łączności.

Bezpieczeństwo informacyjne polega na zapewnieniu ochrony dla systemów informacyjnych wojsk własnych oraz zmniejszeniu efektywności systemów informacyjnych strony przeciwnej. Może ono być osiągnięte przez realizację określonych przedsięwzięć oraz za pomocą pasywnych lub aktywnych środków elektronicznych. Jego zadaniem jest ograniczenie zdolności prowadzenia rozpoznania przez przeciwnika.

Infrastruktura informacyjna tworzy środowisko, które jest tak zorganizowane pod względem operacyjnym, proceduralnym i technicznym, aby możliwe było tworzenie wirtualnych ogniw połączonych z elementami działań bojowych w miarę aktualnych potrzeb, zgodnych z planami prowadzenia operacji lub doraźnymi decyzjami dowódców

właściwych szczebli. Obejmuje jednolitą sieć dowodzenia wojskami i sterowania środkami walki. Jej funkcje polegają na przyjmowaniu danych źródłowych od sensorów lub użytkowników, dystrybucji danych do określonych użytkowników, zapewnieniu bezpieczeństwa informacyjnego i przetwarzaniu danych według integralnych harmonogramów lub dyspozycji użytkowników.

Potencjalni przeciwnicy będą chcieli wykorzystać niedoskonałości jakościowe urządzeń funkcjonujących w systemach informacyjnych, aby pozbawić wojska drugiej strony technologicznej dominacji na polu walki. Rozwój środków w zakresie technologii informacyjnych, dostępnych na rynku powoduje, że środowisko informacyjne, w którym znajdują się wojska własne, ulega całkowitej zmianie. Należy dysponować takimi środkami na polu walki, aby zachować nienaruszalność własnych systemów informacyjnych i nie dopuścić do uzyskania przewagi informacyjnej przez przeciwnika.

Właściwe funkcjonowanie własnych systemów informacyjnych (Information Systems – IS) daje dowódcom i sztabom możliwość kontrolowania aktualnej sytuacji na polu walki, synchronizacji działań oraz integracji z systemami walki (Battlefield Operation Systems – BOSs). Zapewniają one:

— koordynację działań wojsk lądowych z siłami powietrznymi i marynarką wojenną;

— niezbędne dane dla nowoczesnych systemów broni;

— ścisłą kontrolę prowadzonych działań oraz ich skuteczność;

— synchronizację różnego typu operacji zarówno na tyłach, jak i wysuniętych rubieżach w jedną połączoną operację.

Systemy te zbierają, analizują, wykorzystują i przekazują dane dla sił prowadzących operacje połączone. Jakkolwiek olbrzymie są możliwości automatyzacji transmisji danych, to jednak ludzie są najważniejsi, bo to oni decydują o wartości informacji. Integracja systemów informacyjnych odbywa się w płaszczyźnie zarówno pionowej, jak i poziomej.

W architekturze pola walki zarówno systemy wojskowe, jak i cywilne odgrywają ważną rolę.

Do różnorodnych sposobów ochrony własnych systemów informacyjnych dołączone zostają przedsięwzięcia przeciwdziałania środkami rozpoznania, zapewniające skrytość zamiaru działań, obezwładnienia radioelektronicznego, ogniowego oddziaływania i in.

Plan bezpieczeństwa informacyjnego musi być skoordynowany z najwyższym szczeblem dowodzenia, zaangażowanym w operację połączoną. Dane, dotyczące najważniejszych przedsięwzięć w zakresie bezpieczeństwa informacyjnego, powinny być udostępnione dowódcy operacji i kluczowym członkom jego sztabu. Zasada ta powinna obowiązywać również względem bezpośrednio podległych dowódców, którzy realizują własne przedsięwzięcia bezpieczeństwa, tak aby skoordynować wszystkie przedsięwzięcia w ramach jednolitego planu.

Bezpieczeństwo informacyjne musi odnieść się do wszystkich aspektów operacji. Powinno ono obejmować również takie zagadnienia, jak: synchronizację w czasie, łączność i przemieszczanie wszystkich elementów systemu informacyjnego.

Jedną z funkcji bezpieczeństwa informacyjnego jest kontrolowanie i analizowanie poziomu bezpieczeństwa programów komputerowych oraz procedur wymiany danych.

Oceny wrażliwych punktów w systemie informacyjnym przeciwnika i podatności na atak muszą być wykonane przed lub podczas planowania. Należy je ciągle uaktualniać w miarę rozwoju sytuacji, aby uprzedzać nowe zagrożenia. Przedsięwzięcia bezpieczeństwa informacyjnego powinny być realizowane ze znacznym wyprzedzeniem, a nie dopiero po zaistniałej sytuacji.

Prawidłowa ocena możliwości sytemu rozpoznania zarówno przeciwnika, jak i wojsk własnych jest niezbędna do zastosowania właściwych, co do zagrożeń, środków bezpieczeństwa. Działania podjęte dla przeciwdziałania zawyżonemu potencjałowi przeciwnika mogą odciągnąć środki potrzebne do innych działań.

Przedsięwzięcia bezpieczeństwa informacyjnego, o ile to możliwe, powinny wydawać się przeciwnikowi częścią normalnej operacji. Ponadto plan bezpieczeństwa informacyjnego musi być elastyczny – dostosowany do reagowania na zmiany sytuacji i ciągle uaktualniany w celu doboru środków przeciwdziałania do zaistniałej sytuacji.

Dezinformacja – to działania prowadzone w celu zmylenia przeciwnika co do zdolności bojowej, rzeczywistego położenia sił i ich stanu, zamiaru działania, kierunków i charakteru przyszłej operacji. Innymi słowy, działania te mają spowodować, aby dowódca przeciwnika niewłaściwie ocenił sytuację na polu walki i podjął błędną decyzję[104]. Czasami realizowane przedsięwzięcia mogą wprowadzać niepewność wśród dowódców przeciwnika podczas krytycznych warunków działania i powodować, że przeciwnik nie będzie podejmował żadnych działań.

---

[104]Podstęp jest dozwolony przez międzynarodowe prawo wojenne pod warunkiem nienaruszenia ogólnych zasad prowadzenia wojny oraz umów wojskowych zawartych z nieprzyjacielem.

Celem tych przedsięwzięć jest:

— powodowanie, aby przeciwnik podejmował działania, które w istocie będą dla niego niekorzystne;

— prowokowanie przeciwnika do ujawniania stanu liczebnego, gotowości i zdolności bojowej oraz aktualnego położenia i zamiarów działania;

— przeciążenie grup analizy danych przeciwnika nadmiarem bezwartościowych danych;

— prowokowanie przeciwnika do stosowania określonych wzorców zdarzeń, które powodować będą małą skuteczność jego działalności;

— powodowanie utraty mocy bojowej przeciwnika na skutek występowania opóźnień lub podejmowania niewłaściwych działań.

Aby działania takie odniosły pożądany skutek, należy spowodować stan, w którym przeciwnik:

— nie zauważy przedsięwzięć wprowadzających go w błąd (mylących);

— oceni działania mylące – po analizie – jako prawdziwe;

— podejmie działania przeciwko pozorowanym celom i sytuacjom.

Działania dezinformujące prowadzone są na poziomie strategicznym, operacyjnym i taktycznym.

Na poziomie strategicznym dezinformacja realizowana jest w celu wprowadzenia przeciwnika w błąd, co do czasu, miejsca, potencjału i zamiaru działania. Przedsięwzięcia dezinformujące na ty poziomie w operacjach połączonych mogą być planowane na poziomie narodowym lub teatru działań.

Na poziomie operacyjnym dezinformacja obejmuje przedsięwzięcia i środki wprowadzające w błąd przeciwnika w zakresie sposobu prowadzenia operacji. Część przedsięwzięć moż się znaleźć także w „Strategicznym planie dezinformacji".

Na poziomie taktycznym dezinformacja obejmuje całość przedsięwzięć i środków, mających na celu wprowadzić przeciwnika w błąd na lądzie, morzu oraz w powietrzu.

Planowanie działań dezinformujących wymaga głębokiej znajomości kultury, polityki, doktryny oraz procesu decyzyjnego przeciwnika. Dezinmformacja jest zależna od dokładnego i wiarygodnego rozpoznania, śledzenia, a także od ścisłej współpracy z kontrwywiadem. Działania dezinformujące muszą być planowane od góry w dół oraz skoordynowane z działaniami rzeczywistymi. Ze względu na bezpieczeństwo działań tylko wybrana grupa wyższych dowódców może wiedzieć, które akcje są dezinformujące.

Sukces działań dezinformujących zależy od wysokiego stopnia koordynacji i współdziałania pomiędzy sztabami (w tym sztabami rodzajów wojsk) w planowaniu, wykonaniu i monitorowaniu planu dezinformacji. Brak koordynacji w opracowaniu planu dezinformacji może spowodować niebezpieczne zamieszanie w wojskach własnych i może ujawnić przeciwnikowi cel działania.

Obiektami zainteresowania dezinformacji są ludzie i ich reakcje (dowódca i sztab). Wszystkie środki potrzebne do wsparcia i monitorowania dezinformacji muszą być gruntownie przygotowane włącznie z kalkulacjami, co do spodziewanych reakcji celów oddziaływania.

Elastyczność jest wymagana do umiejętnego wykorzystywania reakcji przeciwnika, zarówno przewidywalnych jak i nieprzewidywalnych w celu uzyskania przewagi.

Koordynacja czasowa w przypadku dezinformacji jest decydująca. Przeciwnikowi należy dać wystarczająco dużo czasu na przyjęcie, zrozumienie informacji oraz podjęcie reakcji, lecz nie tak dużo, żeby mógł przeprowadzić gruntowną analizę. Plan dezinformacji powinien być tak koordynowany, aby przynieść przeciwnikowi maksymalne szkody w decydującym momencie działań.

Działania psychologiczne (PSYOPS – Psychological Operations) prowadzone w ramach działań informacyjnych dają szczególne możliwości wpływania na decydentów (przywódców, liderów, dowódców) oraz ludność cywilną przez wykorzystanie środków masowego komunikowania.

Głównym zadaniem działań psychologicznych jest osłabienie morale wojsk przeciwnika, a tym samym obniżenie jego zdolności bojowej i przez to wsparcie działań bojowych wojsk własnych.

Powodzenie zadania głównego zależy od wykonania na wszystkich szczeblach organizacyjnych szeregu zadań szczegółowych, zarówno w czasie pokoju, jak i w czasie wojny.

Do zadań realizowanych w czasie pokoju należą:

— pozyskiwanie i gromadzenie danych o siłach zbrojnych państw obcych i na ich bazie rozpoznawanie morale wojsk;
— prowadzenie prac studyjno-analitycznych w zakresie charakterystyki społeczno-demograficznej innych państw;
— poznawanie struktur działań psychologicznych innych państw oraz studiowanie ich doświadczeń;

— doskonalenie form i metod działania własnych pododdziałów działań psychologicznych;
— aktualizowanie danych o zasobach miejscowych (ośrodki RTV, punkty poligraficzne) pod kątem ich wykorzystania w ramach doraźnych świadczeń rzeczowych;
— systematyczne utrzymywanie rezerw osobowych w gotowości do prowadzenia działań psychologicznych.

Zadania realizowane w czasie kryzysu lub wojny są między innymi następujące:
— kształtowanie i eksponowanie niekorzystnej dla przeciwnika sytuacji psychologicznej do prowadzenia działań bojowych;
— oddziaływanie nękające sferę psychiczną i system nerwowy żołnierzy przeciwnika oraz zakłócające rytm psychicznych i fizycznych czynności organizmu;
— potęgowanie zniechęcenia, poczucia stałego zagrożenia, wywołujących u żołnierzy przeciwnika stany beznadziejności, apatii i defetyzmu, osłabiające tym samym ich wolę walki;
— podrywanie zaufania do kierownictwa cywilnego i wojskowego oraz podważanie wiary w skuteczność prowadzonej wojny i możliwość osiągnięcia zwycięstwa;
— stymulowanie niezadowolenia wśród żołnierzy oraz osłabienie spoistości poszczególnych grup armii przeciwnika poprzez uwypuklanie sprzeczności i antagonizmów na tle narodowościowym, rasowym, politycznym, ekonomicznym i wyznaniowym;
— nakłanianie do zaniechania walki, wywoływanie zjawiska symulacji i osłabienia dyscypliny;
— umacnianie wpływu grup opozycyjnych w społeczeństwie przeciwnika;
— wspieranie działań bojowych wojsk własnych, poprzez oddziaływanie na zachowanie się ludności przeciwnika w rejonie walk.

Działania psychologiczne (PSYOPS) w działaniach wojennych zakładają osiągnięcie następujących celów:
— załamanie morale oraz zdolności bojowej wojsk przeciwnika;
— uodpornienie wojsk własnych i ludności, będącej w obszarze działań, na oddziaływanie informacyjno – psychologiczne sił i środków przeciwnika;
— współudział w skutecznym maskowaniu wojsk własnych.

Działania psychologiczne muszą być skoordynowane z innymi elementami działań informacyjnych. Sztab działań psychologicznych powinien uczestniczyć we wszystkich

fazach procesu operacyjnego, poczynając od badań i analiz, poprzez ocenę, aż do fazy wykonawczej. Sztab działań psychologicznych może uczestniczyć w ochronie własnych informacji i systemów informacyjnych przez analizowanie działań psychologicznych przeciwnika. Na tej bazie może zostać określona myśl przewodnia przeciwdziałania. Działania psychologiczne mogą podnosić ogólną efektywność walki i zostać użyte do prowadzenia dezinformacji.

Działania psychologiczne (PSYOPS) są ściśle związane z innymi elementami działań informacyjnych (tab. 4.2.2), które muszą być brane pod uwagę podczas prowadzenia kampanii w celu osiągnięcia maksymalnego efektu operacyjnego lub zabezpieczenia wojskowych działań sojuszniczych.

Tabela 4.2.2.

Relacje pomiędzy operacjami informacyjnymi a działaniami psychologicznymi

Działania informacyjne	**Działania psychologiczne**
Strategia wojskowa	Doktryna
Wpływanie na podejmujących decyzje Koordynacja obszarów	Wpływanie na zachowania, nastawienie sił zbrojnych oraz ludności cywilnej przeciwnika
Ustalanie podatności treści informacyjnych Proces informacyjny, systemy C2 i CIS	Ocena sytuacji psychologicznej (obiektów oddziaływania, skuteczności oraz podatności)
Zapewnienie doradztwa w zakresie ochrony danych, procesów i systemów informacyjnych NATO	Osłabienie woli walki przeciwnika, obniżenie morale oraz ograniczenie zdolności bojowej przeciwnika, rozwijanie kooperacji, osiąganie poparcia niezaangażowanych stron

Struktury (elementy) działań psychologicznych są odbiorcami danych rozpoznawczych. Wymaga to ciągłej współpracy z innymi organizacjami rozpoznawczymi i wywiadowczymi w zakresie kompleksowej oceny sytuacji i potencjalnych obiektów oddziaływania oraz analizy efektywności przyjętej linii kampanii psychologicznej. Dane dostarczane od tych instytucji mogą okazać się bezcenne dla osiągnięcia sukcesów w działaniach psychologicznych.

Programy działań psychologicznych wymagają ciągłej i właściwej transmisji danych. W jednostkach działań psychologicznych muszą zachodzić ściśle określone i dokładne procesy zbierania, gromadzenia i przetwarzania danych. Komórki planistyczne działań psychologicznych muszą przedstawić formalne dokumenty w zakresie potrzeb rozpoznawczych do określonych komórek wojskowych i cywilnych. Oficerowie komórek rozpoznawczych, działający na rzecz działań psychologicznych mogą również zażądać wsparcia od innych instytucji spoza wojska. Oficer rozpoznania jednostki działań

psychologicznych musi dokładnie zidentyfikować, zlokalizować i oszacować możliwości tych instytucji.

Na wstępie należy przeprowadzić analizę danych rozpoznawczych. Personel działań psychologicznych przeprowadza procesy analizy w sposób ciągły, oceniając rejon działań i odzwierciedlając jego prawdziwy charakter. Proces ten stanowi modyfikację procedur stosowanych w czasie informacyjnego przygotowania pola walki (IPB). Polega na analizie warunków atmosferycznych i terenowych, ocenie obiektu oddziaływania oraz analizie wszystkich dostępnych danych.

Podczas analizy wpływu pogody na techniczne środki działań psychologicznych, szczególną uwagę zwraca się na: kierunek wiatru, jego prędkość oraz zmianę warunków atmosferycznych, które mogą mieć znaczny wpływ na prowadzone działania, wybór odpowiednich środków (w tym także mediów) oraz technik rozpowszechniania materiałów propagandowych.

Analiza terenu skupia się na jego ukształtowaniu, co będzie miało wpływ na rozprzestrzenianie materiałów psychologicznych. Góry, doliny, systemy rzeczne wpływają bezpośrednio na program prowadzonych działań.

Ocena obiektu oddziaływania obejmuje właściwości demograficzne, socjologiczne, kulturowe, polityczne, religijne oraz historyczne ludności zamieszkującej na terenie prowadzonych operacji. Wszystkie siły specjalne (SOF – Special Operations Force) prowadzą podobne analizy w czasie przygotowań do działań. Jednostki te powinny koordynować ocenę ludności. Taka koordynacja daje wartościowe rezultaty i zwiększa szansę na osiągnięcie sukcesu w operacjach militarnych.

Ocena audytorium jest podstawową częścią procesu analizy działań psychologicznych. W tej fazie personel działań psychologicznych analizuje również realną wartość swojej propagandy i rozważa techniki przeciwdziałania wrogiej propagandzie.

Końcowym elementem procesu analizy w działaniach psychologicznych jest zestawienie wszystkich danych i wniosków w jeden bank danych przeznaczony dla planistów działań psychologicznych. Faza ta zależy w głównej mierze od ilości danych i przykładowych rozwiązań opracowanych podczas analiz. Procesy analiz działań psychologicznych są zorientowane na człowieka, jako obiekt oddziaływania. Przykładowe rozwiązania i wzorce prowadzenia działań psychologicznych powstają po przeanalizowaniu całego spektrum danych i są uzależnione od przewidywanych rezultatów akcji prowadzonych przez siły własne, przeciwne i niezaangażowane.

Obiekty oddziaływań klasyfikuje się według określonego kryterium ważności, dzieląc je na: obiekty najwyższej wagi (HVT), obiekty wymagające wysokich nakładów i zaangażowania (HPTS).

Koordynacja przedsięwzięć działań psychologicznych w operacjach połączonych powinna się wyrażać w jednolitej polityce narodowej i sojuszniczej. Brak konsekwencji pomiędzy tematami realizowanymi przez różne agencje lub na różnych poziomach mogą dyskredytować operację i niszczyć wysiłki sprzymierzonych sił wojskowych. W celu uniknięcia takiej sytuacji istotna jest staranna koordynacja działań psychologicznych.

Działania psychologiczne, jeżeli prowadzone są w odpowiednio i w odpowiednim czasie, znacząco wzmocnią lub, jeżeli jest to konieczne, zminimalizują wymiar operacji. Z drugiej strony, jeżeli nie są przeprowadzone w odpowiednim czasie, mogą okazać się nieefektywne lub nawet wzmocnić pozycję przeciwnika.

Działania psychologiczne, bardziej niż inne, wymagają skoordynowanego, wysokiego szczebla planowania i aprobaty. Podstawowym wymogiem jest, aby plany działań psychologicznych były zatwierdzone na możliwie najwyższym szczeblu politycznym i militarnym. Scentralizowane planowanie powinno skupiać się na szczeblu dowództwa regionalnego i opierać się na wytycznych Rady Północno-atlantyckiej i dowódcy strategicznego. Wymóg aprobaty wysokiego szczebla ogranicza w pewnym stopniu swobodę działania dowódców na szczeblu operacyjnym i taktycznym, ale jest to ograniczenie niezbędne.

Wysiłki działań psychologicznych powinny być zintegrowane z zamiarem dowódcy sił połączonych. Dowódca szczebla strategicznego może przydzielić siły działań psychologicznych dowódcy operacyjnemu lub dowódcy komponentu (RSZ) do wsparcia wykonania określonego zadania. Zazwyczaj połączone siły działań psychologicznych będą tworzone jako element wyższego dowództwa na teatrze działań. Istotne jest, żeby wszystkie materiały działań psychologicznych (tj. scenariusze radiowe i materiały drukowane) używały zgodnych informacji, tematów i symboli wymagających jednorazowego procesu akceptacji dla wszystkich rodzajów działań psychologicznych.

Zakłócanie informatyczne jest realizowane za pomocą różnorodnych „programów złośliwych", które powodują wymazanie w krótkim czasie dużej liczby zbiorów danych, spowalniające pracę programów użytkowych. Programem złośliwym nazywa się kod

wyrządzający szkody. Niektórzy również posługują się określeniem *malware* (zlepek z ang. *malicious software* – oprogramowanie złośliwe)[105].

Do programów tych należy zliczyć: wirusy, konie trojańskie, bomby „logiczne", robaki komputerowe, bakterie i króliki oraz wiele 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 uaktywniają się natychmiast po wprowadzeniu do systemu, a niektóre wprowadzone są 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 zajściu 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.

Konie trojańskie otrzymały swoją nazwę ze względu na analogię ze znanym mitem greckim. Są one podprogramami, które (wmontowane np. w oryginalne programy użytkowe, jak gry, arkusze kalkulacyjne czy edytory) mogą na określony sygnał lub komendę wymazywać bazy danych, formatować dyski itp. Użytkownik może na przykład myśleć, że program jest grą. W czasie, gdy program wyświetla komunikat o tym, że aktualizuje bazy danych, bądź zada pytanie w stylu „jaki wybierasz poziom zaawansowania?", program może w tym czasie faktycznie usuwać pliki, formatować dysk czy w inny sposób modyfikować wiadomości.

Bomby „logiczne" są zazwyczaj podkładane w programach przez informatyków, którzy mają legalny dostęp do systemu. Impulsem wyzwalającym „wybuch bomby" może być obecność określonych plików, określony dzień tygodnia czy jakiś użytkownik uruchamiający aplikację. Odpalona bomba „logiczna" może zniszczyć lub zniekształcić dane, spowodować zatrzymanie pracy komputera lub w inny sposób zniszczyć system. Bomby mają podobne działanie jak konie trojańskie, mogą np. uniemożliwiać korzystanie z zakupionego oprogramowania z chwilą utraty ważności licencji użytkownika.

[105] S. Garfinkel, G. Spafford, *Bezpieczeństwo w Unixie i Internecie*, Warszawa ,1997, s. 31.

Robaki komputerowe to programy, które mogą działać samodzielnie, a których zadaniem jest podróżowanie z komputera na komputer za pośrednictwem połączeń sieciowych. Może mieć miejsce taka sytuacja, gdzie wiele części jednego robaka będzie działać w różnych komputerach. Same robaki nie zmieniają innych programów, ale mogą przenosić kod, który to robi. Wypełniają pamięć komputera taką ilością zupełnie przypadkowo generowanych danych, że prowadzi to do istotnego spowolnienia pracy komputera lub wręcz do jego zatrzymania.

Bakterie, zwane również *królikami*, to programy, które nie uszkadzają plików wprost. Ich jedynym zadaniem jest rozmnażanie. Typowy program – bakteria lub program – królik może nie robić nic innego niż dzielić się na dwie kopie i uruchamiać je w środowisku wielozadaniowym. Może też tworzyć dwa nowe pliki, z których każdy jest kopią programu wyjściowego. Oba nowe programy będą się następnie dalej mnożyły, tworząc kolejne „potomstwo". Bakterie reprodukują się wykładniczo i zajmują ogromną ilość pamięci, przestrzeni dyskowej i innych zasobów, przez co użytkownik nie może z nich dalej korzystać.

Maskowanie stanowi zespół przedsięwzięć i czynności mających na celu ukrywanie istotnych zamiarów i działań dotyczących bezpieczeństwa państwa oraz eliminowanie czynników, które mogą zdemaskować (ujawnić) strategicznie ważne przedsięwzięcia obronne. Maskowanie może być prowadzone na trzech poziomach: strategicznym, operacyjnym oraz taktycznym.

Maskowanie strategiczne to wprowadzenie w błąd najwyższych organów kierowania i dowodzenia przeciwnika odnośnie do aktualnego stanu przygotowań państwa i prowadzenia działań militarnych.

Maskowanie operacyjne jest częścią maskowania strategicznego i obejmuje skoordynowane działania mające na celu wprowadzenie w błąd przeciwnika, co do przedsięwzięć, istnienia ważnych obiektów, w tym systemów kierowania i dowodzenia w okresie ich przygotowania do prowadzenia operacji (lądowych, powietrznych, morskich, kosmicznych). Realizowane jest we wszystkich rodzajach sił zbrojnych.

Maskowanie taktyczne to całokształt przedsięwzięć zmierzających do ukrycia lub zmiany wyglądu zewnętrznego pojedynczych i zespołowych obiektów, urządzeń, uzbrojenia i sprzętu wojskowego za pomocą środków i materiałów maskujących w trakcie przygotowania i prowadzenia działań bojowych.

Informowanie opinii publicznej polega na przekazywaniu wiadomości prawdziwych przez media rządowe i publiczne.

Media rządowe spełniają integralną rolę w operacjach informacyjnych w globalnym środowisku informacyjnym (GIE). Zarówno w czasie pokoju, jak i konfliktu czy wojny, wzmacniają one działania bojowe wojsk przez podnoszenie morale własnych wojsk oraz mają wpływ na uzyskanie przewagi informacyjnej.

Media publiczne (o zasięgu światowym) odgrywają dużą rolę w kształtowaniu opinii publicznej. Krytykują one cele operacji militarnych przeciwnika, działania sił zbrojnych oraz obiekty ataku. Mają znaczący wpływ na politykę, strategię, podejmowanie decyzji i planowanie działań bojowych, a tym samym przyczyniają się do odniesienia sukcesu w prowadzonych działaniach. W czasie rzeczywistym (realnym) są w stanie przekazać najnowsze informacje dla dowódców, władz oraz szerokiej rzeszy odbiorców (audytorium).

Na poziomie militarnym (sojuszu, koalicji, państwa) media przekazują wiadomości o działaniach i osiągnięciach sojuszu (koalicji, państwa) przy jednoczesnej ochronie przed wyjawieniem wiadomości ważnych dla przeciwnika. Informowanie opinii publicznej (rodzaj środka przekazu, temat, forma, zakres, czas emisji) powinno być skoordynowane z innymi przedsięwzięciami działań informacyjnych, a szczególnie z działaniami psychologicznymi, żeby zapewnić konsekwentną realizację zamierzonych celów.

Działalność mediów Amerykanie zaczęli doceniać dopiero od wojny w rejonie Zatoki Perskiej. Nowoczesna technologia przekazu wiadomości spowodowała, że media odegrały jedną z ważniejszych ról, dając moralne wsparcie.

Artur Lubow napisał w „The New Republic", że w nowoczesnej wojnie reporterzy muszą mieć zezwolenie na przebywanie na linii frontu i muszą być poddani cenzurze. Obustronny brak zaufania jest elementem podziału na żołnierzy i dziennikarzy w czasie działań wojennych. To powinno być obustronne porozumienie — konsensus. Media stały się ważnym instrumentem w operacjach informacyjnych. Technologia satelitarna, umożliwiająca reporterom natychmiastowy przekaz informacji o prowadzonych działaniach wojennych, może spowodować, że obiektywni reporterzy mogą stać się nieświadomymi obserwatorami, przekazującymi wiadomości w krzywym zwierciadle. Technologia satelitarna pozwala reporterom uwolnić się od cenzury wojskowej i wpływać na odczucia odbiorców w czasie relacjonowania wizerunków (obrazów) zdarzeń w sposób, w jaki oni uważają za stosowny.

Współpraca cywilno-wojskowa (CIMIC) to całokształt działania dowódców wojskowych z instytucjami cywilnymi, takimi jak: władze lokalne, organizacje rządowe

i pozarządowe, społeczność lokalna czy wreszcie organizacje międzynarodowe i humanitarne.

Do zasadniczych zadań komórek CIMIC należy zapewnienie efektywnej współpracy między dowódcą odpowiedzialnym za prowadzoną operację a wszystkimi komponentami lokalnego społeczeństwa dla osiągnięcia celu operacji. Współpraca ta obejmuje nie tylko kwestie operacyjne, lecz i administracyjne, humanitarne, prawne, ekologiczne czy religijne. Współpraca ta jest domeną komórek CIMIC (skrót od angielskiej nazwy Civil-Military Cooperation), istniejących na wszystkich szczeblach zintegrowanej struktury dowodzenia NATO.

CIMIC ma za zadanie kreować pozytywny stosunek miejscowej ludności do wielonarodowych sił wojskowych we współdziałaniu z innymi komórkami sztabów i wyspecjalizowanymi jednostkami.

Jedną z fundamentalnych zasad działania CIMIC jest zachowanie neutralności. Bezstronność jest bezwzględnym warunkiem akceptacji przez lokalną społeczność, nie zawsze przychylnie nastawioną do sił stacjonujących na obcym terenie.

Doświadczenia natowskie w byłej Jugosławii wyraźnie wskazują na konieczność precyzyjnego określenia najistotniejszych problemów do rozwiązania – oczywiście w odczuciu miejscowej ludności. Wojsko ma dbać o aspekty militarne, wspomagając działania ludności tylko w niezbędnym zakresie. Nowa metodologia, jasno rozgraniczając obszary odpowiedzialności obu stron, umożliwi łatwiejsze przechodzenie od początkowej fazy militarnej do finałowego etapu przejęcia pełnej kontroli nad operacją przez społeczność lokalną.

Dokumentem normatywnym NATO w zakresie CIMIC jest „Polityka współpracy cywilno-wojskowej" – MC-411/1 (NATO Military Policy on Civil-Military Co-operation) opracowana w 2002 r., aktualnie przygotowywana jest doktryna CIMIC.

W drugim dokumencie zostanie określony charakter, zakres i cel CIMIC oraz zasady wielostronnej współpracy.

W ramach przygotowań do nowej doktryny NATO zaleciło tworzenie regionalnych grup CIMIC. Powstają dwie: północna (do niej należy Polska) – mocno zaawansowana oraz południowa - w początkowej fazie organizowania. W pierwszej grupie liderami są Niemcy i Holendrzy.

Zakłada się, iż kraje podlegające pod Dowództwo Regionalne Północ (Regoinal Command NORTH) będą mogły korzystać ze wspólnych zasobów (pododdziałów wsparcia CIMIC) oraz z narodowych ekspertów.

Współpraca cywilno-wojskowa będzie wymagała wsparcia ze strony środków działań psychologicznych do komunikowania się z ludnością cywilną (uchodźcy i bezdomni). Dodatkowo struktury działań psychologicznych i CIMIC mogą prowadzić wzajemną wymianę danych w celu rozwijania planów i oceny efektywności podejmowanych działań. Akcje CIMIC mogą wspierać działania psychologiczne, jeśli występują jako potwierdzenie wiadomości przekazywanych przez elementy wsparcia psychologicznego (korpuśne, dywizyjne, brygadowe).

4.3. Koncepcja przewagi informacyjnej

Motywem przewodnim tego podrozdziału jest ukazanie koncepcji przewagi informacyjnej, osiąganej dzięki operacjom informacyjnym, z uwzględnieniem procesu decyzyjnego oraz technologii informacyjnej. Przewaga informacyjna jest kamieniem węgielnym, dzięki któremu dowódcy i decydenci podejmują właściwą decyzję. Technologia informacyjna daje możliwości szybkiego zdobywania danych, ich przechowywania, manipulowania nimi oraz ich dystrybucji.

Rozwiązaniem przyjętych założeń było wykonanie modeli kognitywnych (po lewej stronie model wprowadzający do badań, po prawej model wykonany przez program „Inspirationâ 5.0"[106] – rys. 4.3.1).

Przedsięwzięcia realizowane w ramach działań informacyjnych (np. walka elektroniczna, działania psychologiczne, bezpieczeństwo informacyjne) w znaczny sposób przyczyniają się do uzyskania przewagi informacyjnej, a tym samym do odniesienia sukcesu w walce. Z powyższych założeń wynika, że przewaga informacyjna jest logicznym następstwem skutecznego prowadzenia działań informacyjnych.

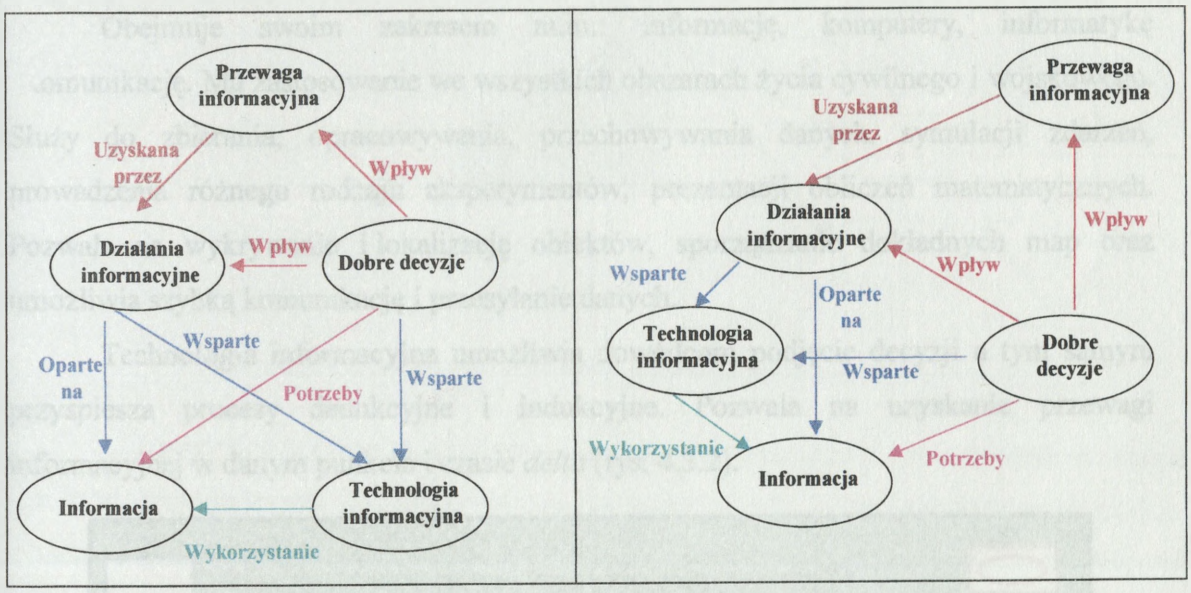
Przewagę informacyjną można porównać do przewagi w powietrzu. Zdaniem specjalistów sił powietrznych USA jest to taki stopień przewagi w sferze informacyjnej, który pozwala własnym wojskom podejmować decyzje, prowadzić operacje oraz reagować na zmieniającą się sytuację na polu walki, podczas gdy pozbawia takich samych możliwości stronę przeciwną. Inne źródło traktuje przewagę informacyjną jako dokładną znajomość (wiedzę) nt. struktur wojskowych potencjalnego przeciwnika, jego potencjału ekonomicznego, kultury i celów politycznych[107].

---

[106]S. M. Clements, *The one with the Most Information Wins? The Quest for Information Superiority),* Air Force Institute of Technology, Ohio, 1997, s. 13.

[107]N. B. Hutcherson, *Command and Control Warfare: Putting Another Tool in the War-Fighter's Data Base.* Maxwell AFB AL: Air University Press, September, 1994, s. 11.

W „Regulaminie wojsk lądowych" (FM-100-6 Information Operations) przewagę informacyjną zdefiniowano jako stopień przewagi, który umożliwia podmiotowi oddziaływań wykorzystać systemy informacyjne i uzyskać przewagę operacyjną w konflikcie lub kontrolę nad sytuacja operacyjną w krótkiej wojnie, pozbawiając takich możliwości stronę przeciwną.



Rys. 4.3.1. Modele kognitywne koncepcji badań

W dokumencie „Joint Vision 2010", przewagę informacyjną określono jako możliwość w zakresie zdobywania, przechowywania, wykorzystania i dystrybucji danych, z jednoczesnym pozbawieniem takich możliwości strony przeciwnej.

Do działań, które przyczyniają się do uzyskania przewagi informacyjnej, należy zaliczyć:

— tworzenie informacyjnej przestrzeni pola walki, tzw. infosfery;

— zdobywanie danych i ich dystrybucja;

— ochrona infosfery,

— atakowanie infosfery przeciwnika, jego systemów informacyjnych.

Tworzenie i ochrona infosfery, to dwa priorytetowe działania w zakresie uzyskiwania lub utraty przewagi informacyjnej.

Infrastruktura informacyjna zapewnia podwaliny, które pozwalają dowódcy uzyskać przewagę w infosferze na polu walki i w jego otoczeniu.

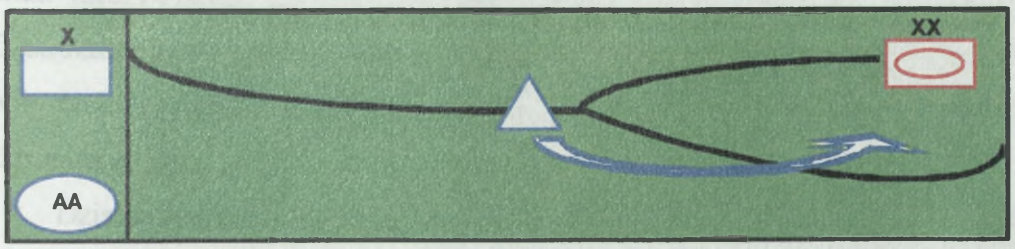
Ta infrastruktura zapewnia dowódcom napływ bieżących danych, zwiększa świadomość sytuacyjną oraz umożliwia łączność. Ochrona infosfery powinna być realizowana na poziomie strategicznym, operacyjnym i taktycznym.

Tworzenie i ochrona infosfery na tych poziomach zależne są w dużej mierze od właściwego wykorzystania technologii informacyjnej.

Technologia informacyjna (TI) to zespół środków (czyli urządzeń, takich jak: komputery i sieci komputerowe) i narzędzi (w tym oprogramowanie), a także inne technologie, które służą wszechstronnemu posługiwaniu się informacją.

Obejmuje swoim zakresem m.in.: informację, komputery, informatykę i komunikację. Ma zastosowanie we wszystkich obszarach życia cywilnego i wojskowego. Służy do zbierania, opracowywania, przechowywania danych, symulacji zdarzeń, prowadzenia różnego rodzaju eksperymentów, prezentacji obliczeń matematycznych. Pozwala na wykrywanie i lokalizację obiektów, sporządzanie dokładnych map oraz umożliwia szybką komunikację i przesyłanie danych.

Technologia informacyjna umożliwia dowódcom podjęcie decyzji a tym samym przyspiesza procesy dedukcyjne i indukcyjne. Pozwala na uzyskanie przewagi informacyjnej w danym punkcie i czasie *delta* (rys. 4.3.2).



Rys. 4.3.2. Punkt Δ - punkt uzyskania przewagi informacyjnej

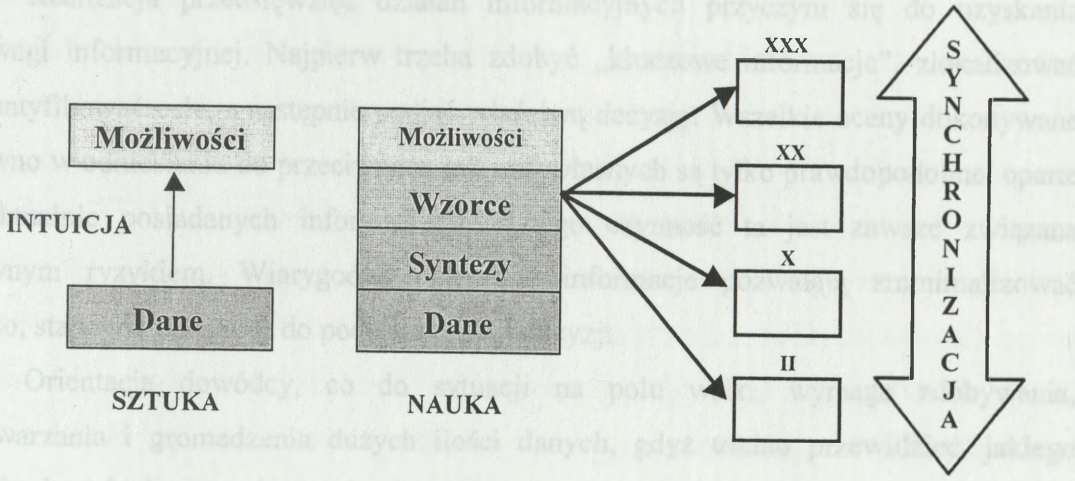
Dzięki zastosowaniu technologii informacyjnych każdy dowódca może uzyskać przewagę w zobrazowaniu sytuacji pola walki. Ta sama technologia pozwala na zobrazowanie wybranych elementów pola walki zarówno w pionie, jak i poziomie struktury dowodzenia, co umożliwia synchronizację planowania i prowadzenia działań (rys. 4.3.3).

Technologia informacyjna jest związana z infrastrukturą informacyjną, dlatego budując ją, należy się skupić na trzech płaszczyznach:

— standaryzacji przekazywanych danych, która decyduje o otwartości systemów informacyjnych;

— uwarunkowaniach techniczno-organizacyjnych wymiany danych, tj. rozwoju technologii informacyjnych i ich dostępności;

— zabezpieczaniu przekazywanych danych przed dostępem osób nieupoważnionych i zagwarantowania ich wiarygodności.



Rys. 4.3.3. Synchronizacja działań na podstawie przekazywanych danych

Infrastruktura informacyjna powinna zapewnić bezpieczny obieg danych w czasie niemal rzeczywistym, co przyczyni się do wzmocnienia potencjału bojowego wojsk. Infrastrukturę powinny tworzyć systemy sensorowe (np. systemy zdobywania informacji źródłowych, systemy dowodzenia wojskami oraz systemy sterowania urządzeniami elektronicznymi).

Działania wymagane do tworzenia strategicznej infrastruktury informacyjnej są kompleksowe. Ważną rolę w tym zakresie odgrywa planowanie systemów informacyjnych oraz zarządzanie nimi, niemniej jednak należy brać pod uwagę adaptowanie systemów do zmieniających się warunków pola walki oraz wdrażanie nowych technologii. Technologia informacyjna musi być całkowicie wykorzystana we wszystkich obszarach, ale także musi łatwo się przystosowywać do zmieniających się potrzeb.

Na poziomie operacyjnym uzyskanie przewagi informacyjnej jest warunkiem wstępnym do prowadzenia działań, podobnie jak posiadanie panowania w powietrzu.

Na poziomie taktycznym przewagę informacyjną można określić jako zmienną warunkową, pozwalającą na wykorzystanie sprzyjających okoliczności na polu walki i uchwycenie inicjatywy. Proces uzyskiwania przewagi informacyjnej na tym poziomie musi przebiegać w całym zakresie czasowym działań bojowych, począwszy od planowania użycia sił zbrojnych, poprzez zobrazowanie pola walki, a kończąc na walce rozstrzygającej.

Armie, które będą dążyć do odniesienia zwycięstwa przez prowadzenie działań informacyjnych, mogą bardzo szybko stracić moc bojową i być stroną przegraną, jeśli

napływ danych z pola walki zostanie zakłócony. Nowoczesna broń inteligentna jest bezużyteczna, jeśli nie przekaże się danych za pomocą systemów informacyjnych.

Realizacja przedsięwzięć działań informacyjnych przyczyni się do uzyskania przewagi informacyjnej. Najpierw trzeba zdobyć „kluczowe informacje", zlokalizować i zidentyfikować cele, a następnie podjąć właściwą decyzję. Wszelkie oceny dokonywane zarówno w odniesieniu do przeciwnika, jak i sił własnych są tylko prawdopodobne, oparte na aktualnie posiadanych informacjach, dlatego czynność ta jest zawsze związana z pewnym ryzykiem. Wiarygodne i aktualne informacje pozwalają zminimalizować ryzyko, stanowią podstawę do podjęcia trafnej decyzji.

Orientacja dowódcy, co do sytuacji na polu walki, wymaga zdobywania, przetwarzania i gromadzenia dużych ilości danych, gdyż trudno przewidzieć, jakiego rodzaju dane będą potrzebne w konkretnej sytuacji, w wykonywanym zadaniu bojowym lub przewidywanych zdarzeniach.

Działania wojenne w istocie rzeczy są walką z czasem. Cykl podejmowania decyzji musi przebiegać szybciej niż u przeciwnika, jeśli zamierza się osiągnąć nad nim przewagę, która zakłóci spójność jego działań.

Podjęcie szybkiej i właściwej decyzji na współczesnym polu walki zależy przede wszystkim od technologii informacyjnej, która umożliwia:

— przekazywanie danych z rozpoznania w czasie niemal rzeczywistym do rodzajów wojsk i służb,
— obserwację pola walki w czasie planowania działań,
— zobrazowanie sytuacji w trzech wymiarach z wielu kierunków;
— uchwycenie inicjatywy i osiągnięcie uniwersalnych korzyści.

J. Kurnal pisze, że podejmowanie decyzji polega na akcie świadomego wyboru jednego z rozpoznanych i dostępnych wariantów działania[108].

Prakseologia rozpatruje decyzję z punktu widzenia sprawności, wprowadza zasady działań racjonalnych. Na tle tych działań rozpatruje znaczenie i związki zachodzące między takimi pojęciami, jak: cel, dzieło, działanie, sprawca, oszczędność, marnotrawstwo, skutek itp.

Matematyczne podejście polega na poszukiwaniu optymalnej decyzji, a więc odpowiadającej rzeczywistym warunkom[109]. Za pomocą teorii matematycznej badane są

[108] J. Kurnal, *Zarys teorii organizacji i zarządzania*, Warszawa, 1970, s. 31.
[109] A. Czermiński, M. Czapiewski, *Organizacja procesów decyzyjnych*, Gdańsk, Wydawnictwo Uniwersytetu Gdańskiego, 1995, s. 13.

związki zachodzące między konkretnymi prawdopodobieństwami zdarzeń, prób losowych oraz zbiorów zdarzeń. Decydent stara się wybrać taką decyzję (optymalną), która prowadzi do możliwie małych strat.

Z punktu widzenia psychologii właściwa decyzja zależy od człowieka, który w sposób bezpośredni lub pośredni będzie ją podejmował. Nader ważną cechą są predyspozycje decydenta, umiejętność rozróżnienia złożoności i nowości problemu decyzyjnego[110]. Na zachowanie decydenta mają wpływ takie cechy, jak: wykształcenie, kwalifikacje, percepcja, pamięć, intuicja, temperament, emocjonalność, aspiracje, poziom lęku. W procesie podejmowania decyzji, szczególnie na polu walki, pojawia się pewne ryzyko. Jak wynika z doświadczeń wojennych, uzasadnionemu podejmowaniu ryzyka podczas działań bojowych często towarzyszą elementy niepewności, wśród których można wyróżnić:

— brak informacji o aktualnym położeniu wojsk własnych i przeciwnika;
— niekompletną, mało wiarygodną oraz szybko zmieniającą się informację.

Podejmowanie decyzji w takich warunkach można określić zależnością:

$$dr = f(kw, wn)$$

gdzie:

dr – podejmowanie decyzji ryzykownej,
kw – konieczność wyboru,
wn – warunki niepewności.

Niejednokrotnie w sytuacjach ekstremalnych konieczne jest podjęcie decyzji (dokonanie określonego wyboru) w sposób intuicyjny lub na podstawie zdobytej wiedzy i doświadczenia. Taki sposób podejścia można odnieść do właściwości, która uznawana jest za subiektywną użyteczność wyników wyboru. Inną właściwość wyboru w sytuacji ryzykownej stanowi szansa uzyskania atrakcyjnego wyniku, którą charakteryzują cztery zasadnicze parametry:

— prawdopodobieństwo sukcesu;
— wielkość (użyteczność) sukcesu;
— prawdopodobieństwo niepowodzenia;
— wielkość porażki, niekorzystnego wyniku działania.

Ryzyko podejmowania decyzji ma charakter wieloaspektowego wyboru działania, dlatego błędem jest sprowadzenie go do określenia jedynie skutków podjętej decyzji

[110] J. Kozielecki, *Psychologiczna teoria decyzji*, Warszawa, 1977, s. 19.

(najczęściej wyboru tzw. mniejszego zła). Sytuacje ryzykowne wymuszają tworzenie alternatywnych rozwiązań, które zazwyczaj pojawiają się w trakcie dynamicznych działań bojowych. Dlatego uważa się, że tego rodzaju sytuacje wymagają od decydentów przede wszystkim odpowiednich predyspozycji intelektualnych i cech psychofizycznych. Predyspozycje intelektualne, w szerokim rozumieniu tego słowa, niezbędne są do opracowywania wariantów rozwiązań, natomiast cechy psychofizyczne związane są z odpornością na stres. Skutki ryzyka mogą być pozytywne lub negatywne. Pozytywne polegają na pobudzaniu do czynności, do podejmowania decyzji innowacyjnych, niestandardowych, wspomaganiu tym samym sprawności intelektualnej i kreatywności, pobudzaniu wyobraźni, pogłębianiu intuicji, zwiększaniu hartu ducha, silnej woli, odwagi i doświadczenia oraz odpowiedzialności za skutki działania w nietypowych, ekstremalnych czy szczególnie złożonych sytuacjach. Często skutkiem przewlekłych sytuacji ryzykownych jest występowanie długotrwałych napięć psychicznych, które mogą być przyczyną powstania stresu. Uwarunkowania współczesnego pola walki sprzyjają powstawaniu stresu, a tym samym znacznie ograniczają podejmowanie racjonalnych decyzji. Wielu psychologów uważa, że sytuacje trudne są przyczyną występowania bezpośrednich, a także odległych skutków stresu, czego przebieg można przedstawić zarówno w aspekcie biologicznym, jak i psychologicznym.

Decyzję można rozpatrywać w zależności wynikowej i czynnościowej. W sensie wynikowym decyzja rozumiana jest jako akt wyboru celu lub sposobu działania, pożądanego z punktu widzenia systemu, w ramach którego wybór ten jest dokonywany, przy czym aktowi wyboru są stawiane określone wymagania. W tym wypadku istotą decyzji jest skupienie uwagi na rezultacie określonego ciągu zdarzeń lub czynności, doprowadzających do aktu wyboru przyszłego działania.

W sensie czynnościowym decyzja rozumiana jest jako szczególna aktywność ludzi, wyrażająca się w poszukiwaniu takich rozwiązań pojawiających się problemów, które mogą zapewnić realizację zamierzonych celów systemu. Istotą takiego wyjaśnienia pojęcia decyzji jest koncentracja na czynnościach, które składają się na tę szczególną aktywność ludzi, a których efektem ma być rozwiązanie pojawiających się na tle realizacji zadań systemu – problemów decyzyjnych.

Aspekt informacyjny decyzji, na którym skoncentrowano się w dysertacji, jest poruszany przez W. Flakiewicza[111]. Traktuje on decyzję jako proces transformacji

[111] W. Flakiewicz, *Podejmowanie decyzji kierowniczych*, Warszawa, 1983, s. 23.

przekształcającej sytuację decyzyjną w zbiór wariantów, z których wybrany traktowany jest jako decyzja ostateczna.

Z powyższego wynika, że decyzja jest wolnym, nielosowym i świadomym wyborem jednego z wariantów – z możliwych wariantów w danym momencie.

Proces informacyjno – decyzyjny można przedstawić w postaci relacji:

$$W = T_1 \{B\}$$

$$D = T_2 \{W\}$$

gdzie:

B – zbiór informacji bazowych;

W – zbiór wariantów dopuszczalnych decyzji;

D – decyzja ostateczna (stanowiąca podstawę działań wykonawczych);

T_1, T_2 – transformacja.

Stąd wynika:

$$D = T_2 [T_1 \{B\}]$$

Zgodnie z powyższym można stwierdzić, że:

— w procesie decyzyjnym występują dwie różne transformacje;

— w wyniku działania transformacji T_1, traktowanej jako operator na informacjach bazowych, otrzymuje się tzw. dopuszczalne warianty decyzji ostatecznej;

— w wyniku działania transformacji T_2 jest dokonywany wybór jednego z wariantów. Wyboru tego dokonuje podmiot decyzyjny, uznając dany wariant za decyzję ostateczną.

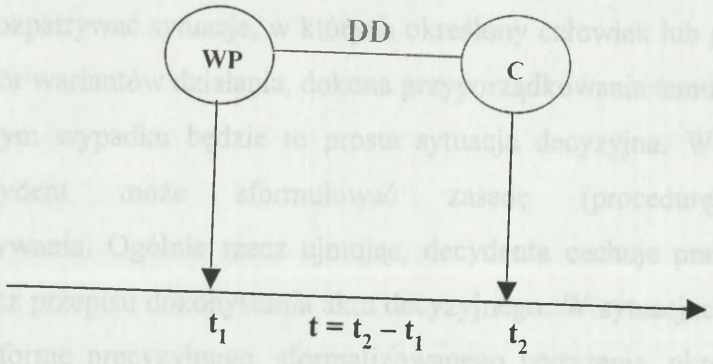
Ciąg czynności wykonywanych przez ludzi, najczęściej pozostających w otoczeniu podmiotu decydującego, związany z przygotowaniem wariantów decyzji dopuszczalnych, też wymaga podejmowania decyzji, z tym że są one podrzędne w stosunku do decyzji ostatecznej, związanej z pełnym rozstrzygnięciem określonego problemu. Stąd też ustalenia zbioru W dokonuje się na podstawie tego drugiego typu decyzji, zwanego dalej „wewnętrznym". Można stwierdzić, że system informacyjno – decyzyjny ma budowę hierarchiczną, wielostopniową. Na szczycie tej hierarchii znajduje się decyzja ostateczna, która rozkłada się na decyzje wewnętrzne, również wielostopniowe, np. jeśli na poziomie G podejmuje się decyzję ostateczną, to na poziomie G_1 ustala się, które z wariantów uznaje się za dopuszczalne, a na poziomie G_2 ustala się warianty decyzji dopuszczalnych w danych warunkach itd. Dokonując dalej tej dekompozycji, dochodzi się do momentu, w którym pracownik, przygotowując pewne materiały cząstkowe, sam dokonuje wyboru

zarówno „wewnętrznego", jak i „ostatecznego" w postaci gotowego materiału, który np. przekazuje swemu zwierzchnikowi.

Z powyższej analizy wynika, że podstawową właściwością każdej decyzji jest wybór (alternatywa). Bez możliwości alternatywy nie można mówić o decyzjach.

Drugą cechą każdej decyzji jest uznanie jej za informację sprawczą, tj. taką, która nakazuje człowiekowi lub ludziom przystąpić do określonego działania. Nakaz ten może mieć różny stopień obligatoryjności, od zlecenia, jako formy najsłabszej, do rozkazu, czyli najsilniejszej formy decyzji.

W każdym świadomym działaniu człowieka (rys. 4.3.4), niezależnie od tego, czego konkretnie dotyczy, muszą być uwzględnione cztery główne składniki:



Rys. 4.3.4. Warunki działania człowieka

1) określenie warunków początkowych (WP) działania, tzn. warunków, w jakich przystępuje się do działania. Wymaga to odpowiednich danych, tzw. danych początkowych;
2) ustalenie celu działania (C). Wymaga to już znacznie głębszego i bardziej wszechstronnego przetworzenia posiadanych danych, które mogą się okazać niedostateczne i mogą wymagać uzupełnienia;
3) wybór dojścia do celu (DD). Składnik ten odgrywa podwójną rolę:
   — weryfikatora możliwości realizacji celu,
   — precyzującego sposób jego osiągnięcia,
4) określenie ΔT, czyli czasu potrzebnego do realizacji celu. Należy podkreślić, że ΔT, zwane „horyzontem czasowym" decyzji, może w pewnych warunkach przekreślić działanie. Może to nastąpić wtedy, gdy cel będzie nie do zrealizowania w czasie ΔT, mimo że dysponuje się środkami lub gdy cel jest realny, ale w ΔT nie można zdobyć takich środków, które będą mogły wyznaczyć pożądaną DD.

Z powyższych rozważań wynika, że decyzja to wygenerowanie (utworzenie) pewnej informacji o charakterze sprawczym, w wyniku wyboru alternatyw dopuszczalnych, związanych z oceną WP, C, DD oraz ΔT, opracowanych na podstawie posiadanych danych bazowych.

Realizacja aktu decyzyjnego wymaga spełnienia pewnych warunków, np. jeśli dany zbiór możliwych alternatyw decyzyjnych X zawiera co najmniej dwie alternatywy x_1 i x_2, gdzie:

$$x_1 \cup x_2 = 1^* = X$$

$$x_1 \cap x_2 = 0^*$$

to akt decyzyjny będzie polegał na wyborze ze zbioru X jednego elementu tego zbioru. Zatem można rozpatrywać sytuacje, w których określony człowiek lub grupa ludzi, mając wyróżniony zbiór wariantów działania, dokona przyporządkowania temu zbiorowi jednego z działań. W tym wypadku będzie to prosta sytuacja decyzyjna. W sytuacji bardziej złożonej decydent może sformułować zasadę (procedurę) dokonywania przyporządkowywania. Ogólnie rzecz ujmując, decydenta cechuje prawo do kreowania zasady czy wręcz przepisu dokonywania aktu decyzyjnego. W sytuacjach, gdy przepis ten można ująć w formę precyzyjnego, sformalizowanego wyrażenia, określa on po prostu funkcję, zgodnie z którą zbiorowi X zostaje przyporządkowany jego element. Funkcję tę nazywa się funkcją decyzyjną, a wskazany przez nią element – decyzją. W tym wypadku powinny być spełnione następujące postulaty:

1. Każdy element zbioru X powinien być opisany przez wszystkie, mogące interesować decydenta, właściwości.
2. Każde dwa elementy zbioru X powinny być różne.
3. Zbiór X powinien obejmować wszystkie elementy, mogące interesować decydenta.
4. Ani zbiór X, ani jego elementy nie powinny zmieniać swych właściwości.

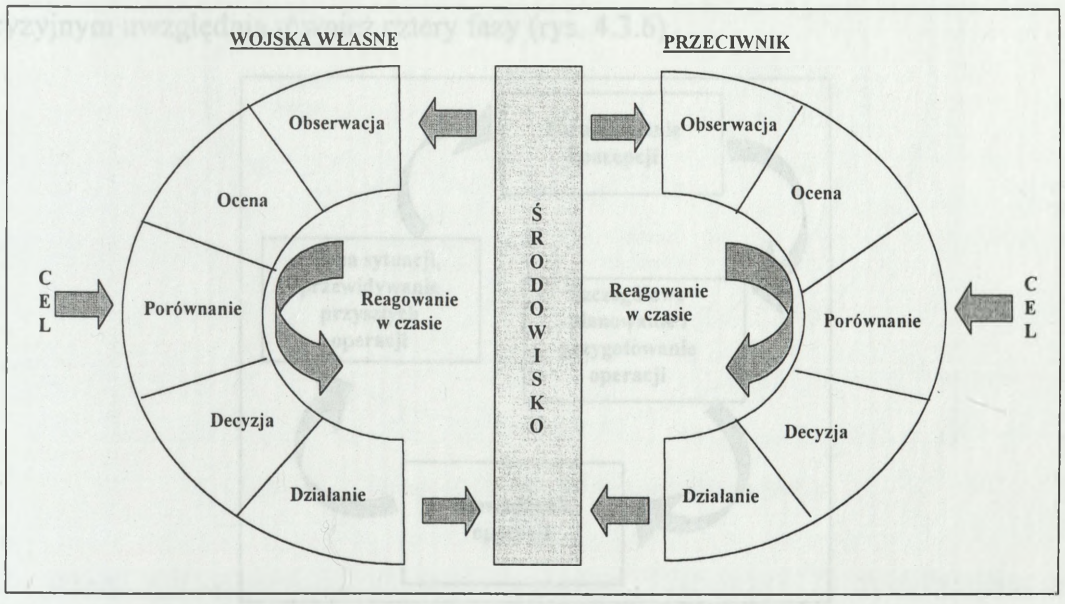
Funkcja decyzyjna powinna być tak skonstruowana, aby istniała możliwość porównywania dowolnych elementów, przy czym porównywalność musi być zupełna i przechodnia. Celem powyższego jest uzyskanie maksimum informacji o zbiorze możliwych wariantów działania. Gdy zbiór wariantów działania X jest określony precyzyjnie, istota problemu decyzyjnego przenosi się na zasady kreowania funkcji decyzyjnych. Zgodnie z przyjętą interpretacją, funkcję decyzyjną tworzy decydent.

Jest oczywiste, że żaden decydent nie działa w izolacji i dlatego akt tworzenia pewnej funkcji decyzyjnej podlega pewnym ogólnym prawidłowościom.

Jeżeli w problemie decyzyjnym znane są wszystkie niezbędne informacje o zbiorze wariantów działania X oraz istnieje funkcja decyzyjna, pozwalająca porównać każde dwa elementy tego zbioru i wskazać jednoznacznie element, który jest decyzją, to mówi się, że podjęcie decyzji nastąpiło w warunkach pewności lub, inaczej, w warunkach pełnej informacji. Natomiast jeśli nie posiada się pełnej informacji o problemie decyzyjnym, wtedy można stwierdzić, że podjęcie decyzji nastąpiło w warunkach ryzyka. Dlatego też w celu sprawnego i trafnego podejmowania decyzji należy utworzyć odpowiednie zbiory informacji, które muszą być uporządkowane, przygotowane i aktualizowane. Wymaga to budowy systemu informacyjno – sterującego. Należy w tym wypadku określić:

— sposób zdobywania informacji – co? kiedy? jak?
— sposób ich aktualizowania – co? kiedy? jak?
— sposób utrzymywania informacji – na jakich nośnikach? w jakiej ich organizacji?
— sposób przetwarzania informacji – na podstawie jakich procedur i algorytmów?, przy wykorzystaniu jakich technik i technologii?
— sposób przekazywania informacji – jakie? komu? kiedy? w jaki sposób?

Na polu walki cykl decyzyjny ma charakter dwustronny (rys. 4.3.5).



Rys. 4.3.5. Dwustronny cykl decyzyjny

Jak twierdzi C. Coe i T. J. Dockery[112], w takim cyklu należy brać pod uwagę dwa aspekty:

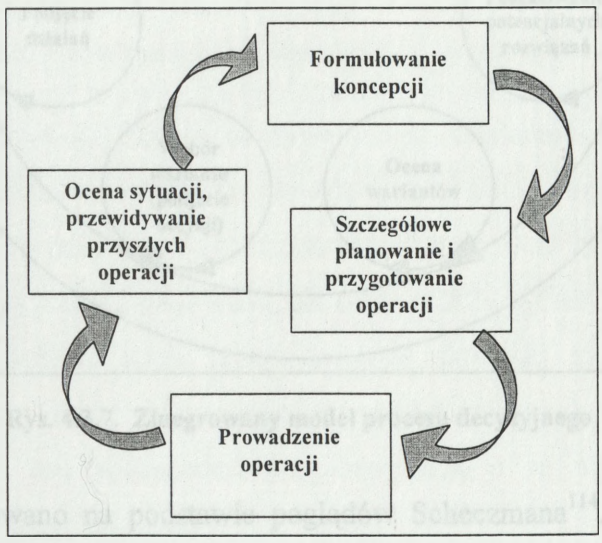
[112]C. Coe, J. T. J. Dockery, *JCS Initiatives in C2 Analysis and Simulation.* [w:} *Science of Command and Control: Coping with Uncertainty*, red. Stuart E. Johnson and Alexander H. Levis, Washington, International Press, 1988, s. 43.

— po pierwsze, przeciwnik reaguje na zmieniającą się sytuację i podejmuje decyzję;
— po drugie, środowisko (otoczenie), w którym prowadzone są mediacje pomiędzy obydwiema stronami. Chociaż wewnętrzne środowisko jest specyficzne dla strony podejmującej decyzje, to zewnętrzne środowisko może być takie samo dal obydwu stron.

Jeśli jedna strona uzyska kontrolę nad zewnętrznym środowiskiem, uzyska przewagę informacyjną, będzie mogła zastosować efekt „fikcji" w stosunku do drugiej strony. Bieżąca i użyteczna informacja może zredukować ten efekt dla wojsk własnych oraz przyczynić się do manipulacji danymi w stosunku do przeciwnika.

W procesie decyzyjnym można wyróżnić cztery fazy:
— *obserwacja* – zdobywanie danych w otoczeniu;
— *orientacja* – tworzenie mentalnego modelu (szkicu) zdarzeń, które zachodzą w otoczeniu i mogą mieć wpływ na decyzję;
— *decyzja* – podjęcie decyzji (wybór właściwego wariantu);
— *działanie* – implementacja decyzji.

Podobnie do tego zagadnienia podchodzi D. L. Rota[113], który w procesie decyzyjnym uwzględnia również cztery fazy (rys. 4.3.6).



Rys. 4.3.6. Czterofazowy proces decyzyjny

Proces decyzyjny w tym wypadku obejmuje:
— tworzenie obrazu pola walki i ogłoszenie zamiaru,
— planowanie i przygotowanie operacji,

[113]D. L. Rota, *Combat Decision Making in Operations Other Than War,* Military Review, March-April 1996, s. 24–28.

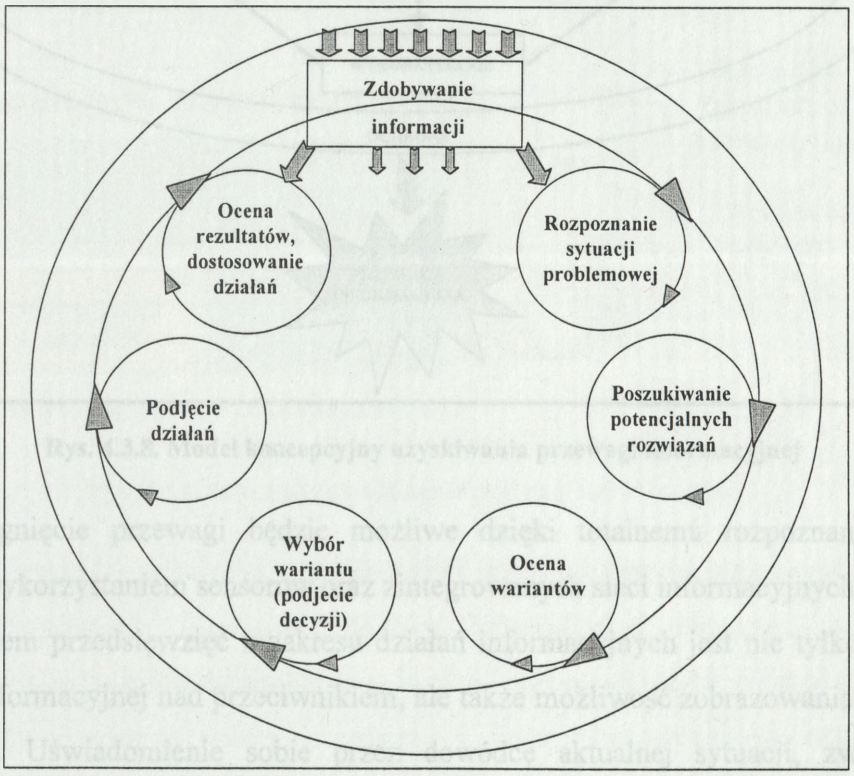
— prowadzenie operacji,

— ocena bieżąca sytuacji (przygotowanie przyszłych operacji).

Informacja jest czynnikiem podstawowym w fazie pierwszej, ponieważ, aby ogłosić zamiar działań dowódca musi posiadać aktualną ocenę sytuacji pola walki.

Chociaż informacje potrzebne do prowadzenia działań wojennych lub pokojowych mogą się znacznie różnić między sobą, przedsięwzięcia związane ze zdobyciem istotnych informacji są takie same. Analiza danych i ich dystrybucja są niezbędne do planowania, przygotowania i prowadzenia wszelkich operacji.

Na podstawie analizy literatury przedmiotu stworzono zintegrowany model procesu decyzyjnego (rys. 4.3.7), zawierający wspomniane wcześniej fazy działań.



Rys. 4.3.7. Zinegrowany model procesu decyzyjnego

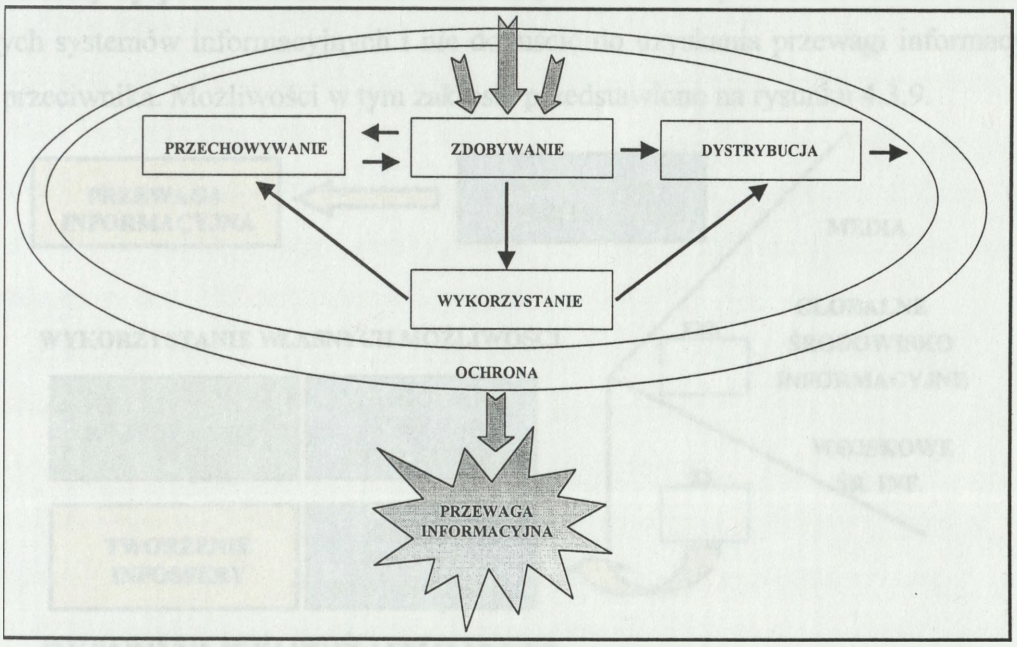
Model opracowano na podstawie poglądów Scheczmana[114], uwzględniając przy tym środowisko pola walki. Zdobywanie informacji jest procesem ciągłym, musi być brane pod uwagę w każdej fazie działań.

Ponadto fazy w procesie decyzyjnym należy traktować jako kompleks przedsięwzięć w kontekście przygotowania operacji i osiągania celów.

[114]G. M. Schechtman, *Manipulating The OODA Loop: The Overlooked Role Of Information Resource Management In Information Warfare,* Wright-Patterson School of Logistics and Acquisition Management, Air Force Institute of Technology, 1996, s. 16–18.

Elementem wejściowym w procesie uzyskiwania przewagi informacyjnej jest oczywiście informacja.

W celu uzyskania przewagi informacyjnej należy podjąć cztery działania: zdobywanie, przetwarzanie, dystrybucja i wykorzystanie danych (rys. 4.3.8). Działania te są podstawowe w powyższym procesie oraz są integralną częścią szerszego kompleksu przedsięwzięć realizowanych w ramach działań informacyjnych.



Rys. 4.3.8. Model koncepcyjny uzyskiwania przewagi informacyjnej

Osiągnięcie przewagi będzie możliwe dzięki totalnemu rozpoznaniu obszaru operacji z wykorzystaniem sensorów oraz zintegrowanych sieci informacyjnych.

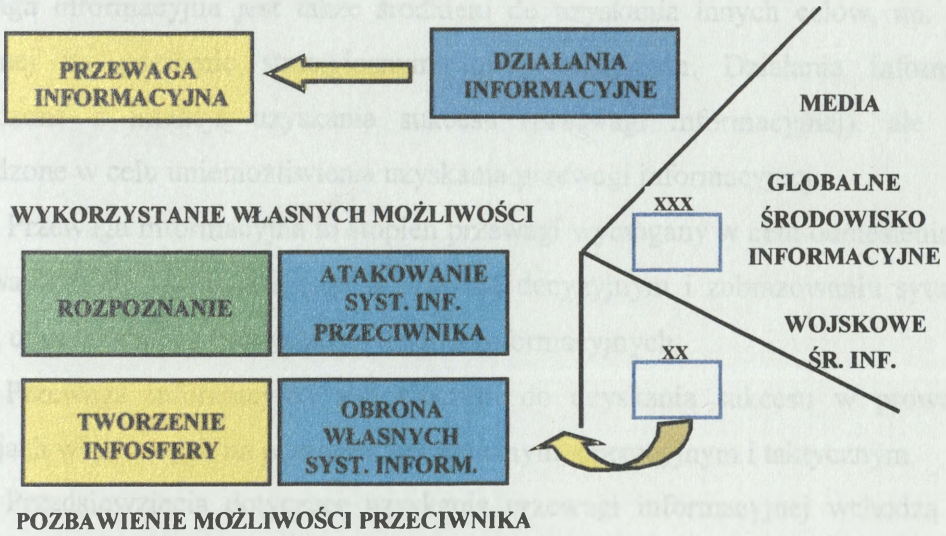
Sensem przedsięwzięć z zakresu działań informacyjnych jest nie tylko uzyskanie przewagi informacyjnej nad przeciwnikiem, ale także możliwość zobrazowania sytuacji na polu walki. Uświadomienie sobie przez dowódcę aktualnej sytuacji, związanej ze środowiskiem i przeciwnikiem oraz możliwości obserwacji zmian w kontekście potrzeb i sytuacji, umożliwia mu wiarygodne prognozowanie, a w efekcie podejmowanie właściwych decyzji w trakcie działań.

Aby działania informacyjne w operacjach połączonych przyczyniły się do uzyskania sukcesu, proces planowania należy rozpocząć z dużym wyprzedzeniem. Całość działań musi być zsynchronizowana, czyli plan rozpoznania musi się wiązać z planem rażenia elektronicznego i ogniowego oraz planem manewru. Potencjalni przeciwnicy będą chcieli wykorzystać niedoskonałości jakościowe urządzeń funkcjonujących w systemach

informacyjnych, aby pozbawić wojska drugiej strony technologicznej dominacji na polu walki.

Rozwój środków w zakresie technologii informacyjnych, dostępnych na rynku spowoduje, że środowisko informacyjne, w którym będą się znajdować wojska własne ulegnie całkowitej zmianie w potencjalnych, przyszłych konfliktach.

Należy dysponować takimi środkami na polu walki, aby zachować nienaruszalność własnych systemów informacyjnych i nie dopuścić do uzyskania przewagi informacyjnej przez przeciwnika. Możliwości w tym zakresie przedstawiono na rysunku 4.3.9.



Rys. 4.3.9. Schemat - uzyskiwanie przewagi informacyjnej

Jak z powyższego wynika, do najbardziej istotnych przedsięwzięć w tym zakresie zalicza się rozpoznanie, tworzenie infosfery (informacyjnej przestrzeni pola walki), atakowanie systemów informacyjnych przeciwnika i obronę własnych systemów.

Obiekty sensorowe, centra dowodzenia i obiekty bezpośredniego oddziaływania bojowego powinny być w takim stopniu poddane rygorom interoperacyjnej standaryzacji, aby można było tworzyć jednolitą infrastrukturę wymiany danych, wirtualne systemy zadaniowe bez względu na lokalizację geograficzną obiektów, ich przynależność „branżową" (rodzaje wojsk i służb) czy specyfikę technicznej implementacji (stacjonarne lub mobilne, na pokładzie obiektów latających czy też pojazdów lądowych). Ważną rolę pod tym względem odgrywają środki rozmieszczone w przestrzenia kosmicznej (np. satelity rozpoznawcze oraz pracujące w ramach systemu GPS).

Infrastruktura informacyjna tworzy środowisko, które jest tak zorganizowane pod względem operacyjnym, proceduralnym i technicznym, aby możliwe było tworzenie wirtualnych ogniw połączonych z elementami działań bojowych w miarę aktualnych

potrzeb, zgodnych z planami prowadzenia operacji lub doraźnymi decyzjami dowódców właściwych szczebli. Obejmuje jednolitą sieć dowodzenia wojskami i sterowania środkami walki. Jej funkcje polegają na przyjmowaniu informacji źródłowych od sensorów lub użytkowników, dystrybucji danych do określonych użytkowników, zapewnieniu bezpieczeństwa informacyjnego i przetwarzaniu według integralnych harmonogramów lub dyspozycji użytkowników.

Podsumowując dotychczasową analizę, należy stwierdzić, że przewaga informacyjna jest celem, który uzyskujemy przez prowadzenie działań informacyjnych. Przewaga informacyjna jest także środkiem do uzyskania innych celów, np. przewagi militarnej na poziomie strategicznym lub operacyjnym. Działania informacyjnesą prowadzone z intencją uzyskania sukcesu (przewagi informacyjnej), ale także są prowadzone w celu uniemożliwienia uzyskania przewagi informacyjnej.

Przewaga informacyjna to stopień przewagi wymagany w celu odniesienia sukcesu w prowadzonych działaniach (np. w procesie decyzyjnym i zobrazowaniu sytuacji pola walki), uzyskana przez prowadzenie działań informacyjnych.

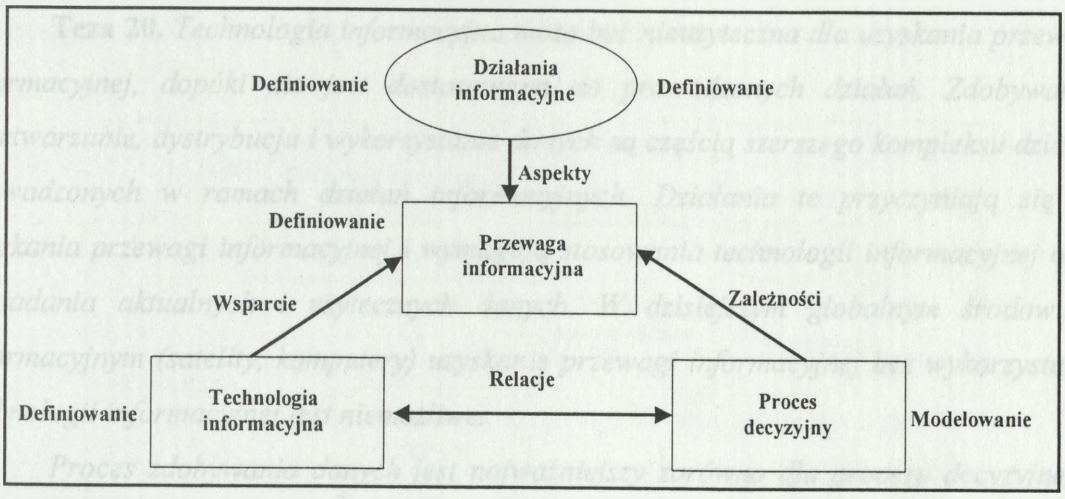
Przewaga informacyjna jest kluczem do uzyskania sukcesu w prowadzonych operacjach wojskowych na poziomie strategicznym, operacyjnym i taktycznym.

Przedsięwzięcia dotyczące uzyskania przewagi informacyjnej wchodzą w skład szerszego kompleksu działań właściwych dla działań informacyjnych. Przedsięwzięcia w ramach działań informacyjnych obejmują m.in. tworzenie infosfery, zarządzanie systemami i zasobami informacyjnymi oraz akcje prowadzone w ramach walki informacyjnej. Wszelkie działania w tym zakresie są wspomagane przez technologię informacyjną.

Zdobywanie danych (rozpoznanie) nie jest nową koncepcją, jak już wcześniej stwierdzono, znane było w czasach starożytnych, oczywiście możliwości te były znacznie mniejsze w porównaniu ze współczesnymi (satelity, komputery, nowoczesna technologia informacyjna). Dlatego też, zanim dojdzie do działań zbrojnych (fizycznego niszczenia), najpierw należy sparaliżować systemy informacyjne przeciwnika, inteligentne systemy broni. Oczywiście nieocenione usługi również w tym zakresie daje technologia informacyjna, która pozwala przeprowadzić bardziej precyzyjny i zsynchronizowany atak.

Na podstawie przeprowadzonych badań dotyczących koncepcji przewagi informacyjnej (rys. 4.3.10) można sformułować następujące tezy:

Teza 17. *Przewaga informacyjna może być osiągnięta przez następujące przedsięwzięcia: zdobywanie, przetwarzanie, dystrybucję i wykorzystanie danych, które należy prowadzić w sposób bardziej efektywny niż przeciwnik.*



Rys. 4.3.10. Schemat badań dotyczących koncepcji przewagi informacyjnej

Teza 18. *Zdobywanie użytecznych informacji jest „kluczowym" czynnikiem uzyskania przewagi informacyjnej. Dlatego zarówno źródła zdobywania danych, jak i realizowane przedsięwzięcia muszą odpowiadać światowym standardom, w innym wypadku mogą wystąpić przeszkody w uzyskaniu przewagi informacyjnej. Dlatego też należy prowadzić badania dotyczące nowych technologii informacyjnych i wdrażać w życie nowe sposoby. Ponadto tylko użyteczne dane powinny być odbierane i przekazywane, gdyż niepożądane dane (nieprawdziwe) mogą opóźnić proces decyzyjny oraz przyczynić się do niewykonania misji. Zdobywanie użytecznych danych jest ważne nie tylko dla uzyskania przewagi informacyjnej, ale także dla procesu decyzyjnego.*

Teza 19. *W trakcie analizy przewagi informacyjnej z perspektywy użyteczności (osiąganych celów) zauważono, że przewaga informacyjna i proces decyzyjny są ściśle z sobą powiązane. Możliwość opóźnienia przekazu danych u przeciwnika, obrazujących położenie strategiczne, zwiększa skuteczność wpływu na podejmowanie przez niego decyzji* [115]*. Informacja jest ważnym elementem w procesie decyzyjnym, natomiast technologia znacznie przyśpiesza cykl decyzyjny, jeśli oczywiście wykorzystywana ona jest w ramach prowadzenia działań informacyjnych, których rezultaty wspomagają proces decyzyjny*

[115] D. J. Dishong, *On Studying the Effect of Information Warfare on C2 Decision Making*, Naval Postgraduate School, 1994. Przeprowadził eksperyment, do którego wykorzystał program symulacji komputerowej nazwany „Tactical Tic-Tac-Toe". Eksperyment udowodnił, że opóźnienie w tworzeniu obrazu pola walki na poziomie taktycznym u przeciwnika, zwiększa możliwość odniesienia sukcesu w walce oraz w znaczny sposób zmniejsza straty własne.

w operacjach militarnych. Ważną rolę odgrywa tu bieżąca i użyteczna informacja, gdy napływ bieżących danych zostanie zakłócony, proces decyzyjny może zakończyć się fiaskiem.

Teza 20. *Technologia informacyjna może być nieużyteczna dla uzyskania przewagi informacyjnej, dopóki nie jest dostosowana do prowadzonych działań. Zdobywanie, przetwarzanie, dystrybucja i wykorzystanie danych są częścią szerszego kompleksu działań prowadzonych w ramach działań informacyjnych. Działania te przyczyniają się do uzyskania przewagi informacyjnej i wymagają stosowania technologii informacyjnej oraz posiadania aktualnych i użytecznych danych. W dzisiejszym globalnym środowisku informacyjnym (satelity, komputery) uzyskanie przewagi informacyjnej bez wykorzystania technologii informacyjnej jest niemożliwe.*

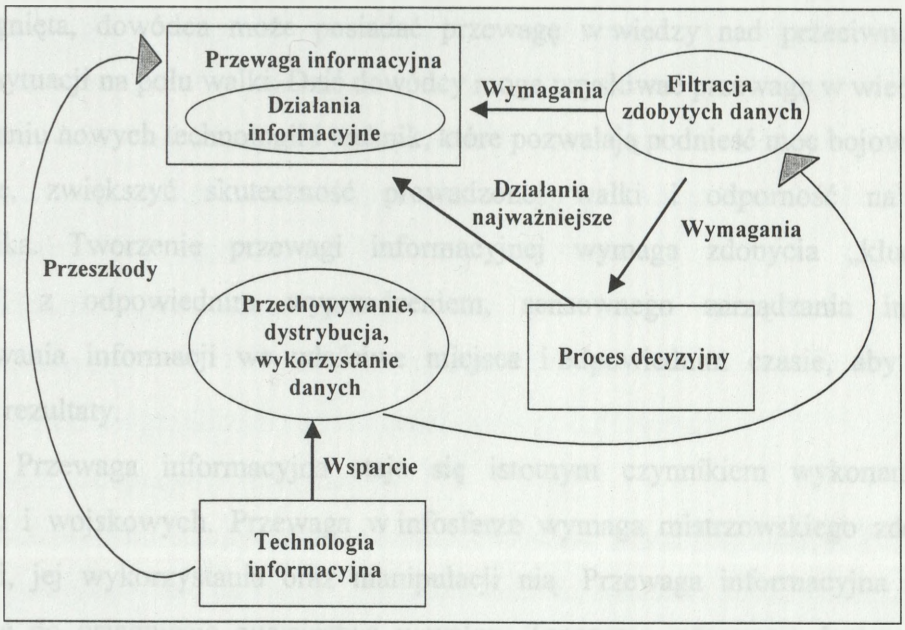
Proces zdobywania danych jest najważniejszy zarówno dla procesu decyzyjnego, jak i uzyskiwania przewagi informacyjnej. Technologia informacyjna może powodować przeciążenie systemów informacyjnych przeciwnika, a tym samym opóźnić decyzję lub uniemożliwić jej podjęcie. Może także znacznie ograniczyć możliwości przeciwnika w zakresie zdobywania danych, co uniemożliwi mu uzyskanie przewagi informacyjnej. Powszechnym zastosowaniem dzisiejszej technologii informacyjnej jest trójwymiarowy obraz pola walki.

Teza 21. *Uzyskanie przewagi informacyjnej wymaga zastosowania technologii informacyjnej, która zapewnia łączność, umożliwia zdobywanie użytecznych danych, ich przetwarzanie, przekazywanie i wykorzystanie. Najważniejszym działaniem jest zdobywanie danych, które musi być zorganizowane wyprzedzająco już w czasie pokoju i prowadzone w sposób ciągły, nawet po zakończeniu działań militarnych lub niemilitarnych.*

Podsumowując dotychczasową analizę, należy stwierdzić, że działania informacyjne przyczyniają się w znaczny sposób do uzyskania przewagi informacyjnej (rys. 4.3.11).

Najistotniejsze w uzyskiwaniu przewagi informacyjnej staje się posiadanie informacji o przeciwniku. Informacja, jako zasób, powinna być tak wykorzystywana, aby możliwe było określenie jej wartości. Wcześniej jednak, zanim zostanie wykorzystana, musi być zdobyta i przekształcona w użyteczną formę przekazu. Może pochodzić od człowieka, być przekazywana przez system informacyjny lub pochodzić z innych źródeł. Jeśli nie jest wykorzystywana natychmiast, może być magazynowana, aż do czasu transmisji. Wykorzystanie informacji obejmuje wiele różnego rodzaju działań

prowadzonych w ramach działań informacyjnych. Działania takie, jak: opóźnienie informacyjne, degradacja treści informacyjnych przeciwnika, manipulowanie danymi, atakowanie jego systemów informacyjnych oraz możliwość terminowego wykorzystania informacji w planowaniu lub procesie decyzyjnym, wpływają wartość informacji i rezultat końcowy.



Rys. 4.3.11. Model uzyskiwania przewagi informacyjnej

Zdobywanie danych ma najistotniejsze znaczenie zarówno dla przewagi informacyjnej, jak i podejmowania decyzji, dlatego wymaga wielu środków ostrożności, aby upewnić się, że otrzymuje się istotne i prawdziwe informacje. Należy brać pod uwagę dane techniczne, wykorzystanie stanowisk analizy technicznej danych, szczególnie w planowaniu strategicznym. Dlatego też wymaga to zastosowania odpowiednich technologii informacyjnych, począwszy od zdobycia danych, ich przechowywania w odpowiednim formacie, aż do pożądanego wykorzystania.

4.4. Efekty poznania

1. Działania informacyjne to kompleks planowych przedsięwzięć polegający na wpływaniu na postawy dowódców (decydentów), degradacji nośników danych i systemów informacyjnych przeciwnika, z jednoczesną ochroną nośników danych i systemów informacyjnych wojsk własnych.

2. Działania informacyjne przyczyniają się do uzyskania przewagi informacyjnej nad przeciwnikiem. Przewaga ta jest określana jako stopień dominacji informacyjnej,

pozwalający użyć systemy informacyjne i ich możliwości tak, aby uzyskać zaskoczenie, kontrolować sytuację w konflikcie lub krótkich działaniach wojennych, z jednoczesnym pozbawieniem takich możliwości strony przeciwnej. Osiągnięcie przewagi informacyjnej pozwala na wzmocnienie i ochronę własnych systemów informacyjnych i operacji wojsk oraz na obniżenie możliwości informacyjnych przeciwnika. Jeśli przewaga informacyjna jest osiągnięta, dowódca może posiadać przewagę w wiedzy nad przeciwnikiem lub kontrolę sytuacji na polu walki. Dziś dowódcy mogą uzyskiwać przewagę w wiedzy dzięki zastosowaniu nowych technologii i technik, które pozwalają podnieść moc bojową, przejąć inicjatywę, zwiększyć skuteczność prowadzonej walki i odporność na systemy przeciwnika. Tworzenie przewagi informacyjnej wymaga zdobycia „kluczowych" informacji z odpowiednim wyprzedzeniem, sensownego zarządzania informacją, przekazywania informacji we właściwe miejsca i odpowiednim czasie, aby osiągnąć pożądane rezultaty.

3. Przewaga informacyjna staje się istotnym czynnikiem wykonania zadań cywilnych i wojskowych. Przewaga w infosferze wymaga mistrzowskiego zdobywania informacji, jej wykorzystania oraz manipulacji nią. Przewaga informacyjna może się przyczynić do osiągnięcia zwycięstwa w walce. Znaczenie informacji dostrzegane jest przede wszystkim w procesie decyzyjnym. Zrozumienie relacji pomiędzy informacją a procesem decyzyjnym jest ważnym elementem uzyskiwania przewagi informacyjnej. Jeśli dowódca ma możliwość podjęcia natychmiastowej, lepszej decyzji niż przeciwnik, to z pewnością odniesie zwycięstwo nad przeciwnikiem na polu walki. Rozwój technologii informacyjnych jest kolejnym czynnikiem, który należy brać pod uwagę. Technologia informacyjna w znaczny sposób usprawnia proces dystrybucji danych, możliwości komunikacyjnych, co w efekcie sprowadza się do podjęcia właściwej decyzji. Technologia informacyjna daje możliwości szybkiego zdobywania danych, ich przechowywania, manipulowania nimi oraz ich dystrybucji. Przewaga informacyjna jest kamieniem węgielnym umożliwiającym dowódcom i decydentom podjęcie właściwej decyzji. Przedsięwzięcia realizowane w ramach działań informacyjnych(np. walka elektroniczna, działania psychologiczne, bezpieczeństwo informacyjne) w znaczny sposób przyczyniają się do uzyskania przewagi informacyjnej, a tym samym do odniesienia sukcesu w walce zbrojnej oraz operacjach innych niż wojna.

4. Działania informacyjneprowadzone zarówno w ramach operacji militarnych, jak i niemilitarnych stanowią nowy i specyficzny dla polskiej sztuki wojennej rodzaj działań. Przygotowanie i prowadzenie działań informacyjnychodznacza się specyfiką w zakresie

struktur organizacyjno–funkcjonalnych, procesów, procedur oraz dokumentów planistycznych. Rozwiązania tego problemu powinny zaspokajać potrzeby narodowe, wymagania standaryzacyjne NATO oraz odpowiadać wymogom wynikającym z mnogości komponentów narodowych.

5. Przedsięwzięcia prowadzone w ramach działań informacyjnych mają zastosowanie we wszystkich możliwych scenariuszach wojennych w obszarze dowodzenia, wsparcia i planowania walki. Znajomość zamiarów i możliwości przeciwnika, dokładnej dyslokacji jego sił oraz przypuszczalnych obiektów ataku, a także dyslokacji własnych sił są nieodzowne do skutecznego prowadzenia walki. Najistotniejsze przeto w tej dziedzinie staje się:

— pozyskiwanie danych o przeciwniku;

— analiza danych;

— niezwłoczne ich przekazanie do zainteresowanych odbiorców;

— niezawodność (prawdziwość) danych.

Duży problem stanowi analiza i opracowywanie zebranych danych. Powinny być zebrane i posegregowane na ważne i potrzebne oraz na nieważne. Idealnym rozwiązaniem byłoby przekazywanie zainteresowanym odbiorcom tylko tych danych, które są im potrzebne. Przez stworzenie sieci połączeń, możliwie największej liczby odbiorców, powstaje możliwość optymalnej współpracy pomiędzy różnymi rodzajami sił zbrojnych lub strukturami wielonarodowymi.

6. W przyszłości może dojść do sytuacji, że siły zbrojne bardziej będą skupiać swoje wysiłki na zdobywaniu danych i procesie decyzyjnym w celu uzyskania przewagi informacyjnej, niż na działalności militarnej, jaką jest atak lub obrona. Dlatego też należy lepiej zarządzać zdobywaniem danych, właściwie wykorzystać zasoby informacyjne, stosować technologię informacyjną w celu monitoringu informacji i upewnienia się, że przekazywane są użyteczne informacje.

7. Technologia informacyjna przyczynia się w znacznym stopniu do uzyskania przewagi informacyjnej, ale tylko wtedy, jeśli ma odpowiednie cechy charakterystyczne. Ponadto technologię informacyjną należy rozpatrywać z ogólnego punktu widzenia, a nie z punktu wsparcia (wzmocnienia) przewagi informacyjnej, gdyż faktycznie może ona być przeszkodą w jej uzyskaniu. Wykorzystanie cech charakterystycznych technologii informacyjnej musi być odpowiednio zaplanowane, aby uzyskać przewagę informacyjną, a tym samym odnieść zwycięstwo w walce. Kiedy użyteczna i bieżąca informacja jest

zdobyta, wtedy należy podejmować kolejne działania. Technologia informacyjna powinna być włączona w proces zdobywania danych, ich przetwarzania i przekazywania oraz do zapewnienia łączności.

8. Siły zbrojne powinny kontynuować badania nad technologią informacyjną i jej cechami charakterystycznymi, przede wszystkim nad jej możliwościami w zakresie zdobywania danych, ich przetwarzania i przekazywania oraz łączności. Ponadto należy zwrócić uwagę, że są to najistotniejsze działania przyczyniające się do uzyskania przewagi informacyjnej. Technologię informacyjną należy stosować w procesie planowania strategicznego oraz zarządzaniu zasobami informacyjnymi aby upewnić się, że użyteczna informacja jest zdobywana, przetwarzana i przekazywana.

9. Teza 17 identyfikuje specyficzne działania w celu uzyskania przewagi informacyjnej. Natomiast tezy 18 i 19 sugerują, które z tych działań są najważniejsze. Teza 20 wskazuje, że technologia informacyjna może być przeszkodą w uzyskaniu przewagi informacyjnej, natomiast teza 21 odzwierciedla cechy charakterystyczne technologii informacyjnej, niezbędne do uzyskania przewagi informacyjnej. Teza 21 jest oparta na badaniach wojskowych nad aktualnymi trendami rozwojowymi technologii informacyjnej. Ta propozycja może być stosowana zarówno w stosunku do wsparcia tezy 18, jak również do potwierdzenia konkluzji, że wysiłki militarne idą we właściwym kierunku, aby uzyskać przewagę informacyjną.

5. PROWADZENIE DZIAŁAŃ INFORMACYJNYCH

5.1. Planowanie działań informacyjnych

Na podstawie literatury przedmiotu badań sporządzono schemat planowania działań informacyjnych (rys. 5.1.1), który obejmuje następujące fazy:

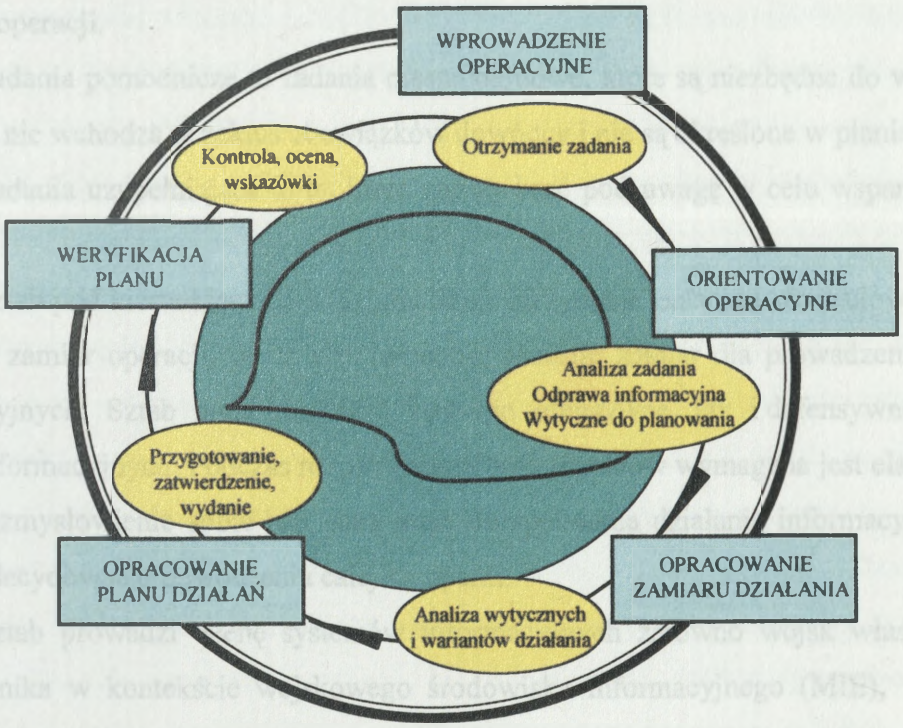
— faza I – wprowadzenie operacyjne;

— faza II – orientowanie operacyjne;

— faza III – zamiar działań;

— faza IV – opracowanie planu;

— faza V – weryfikacja planu.



Rys. 5.1.1. Schemat planowania działań informacyjnych

Faza I – wprowadzenie operacyjne. Celem pierwszej fazy planowania jest formalne rozpoczęcie procesu planowania działań informacyjnych, który w operacjach połączonych stanowi najwcześniejsze stadium planowania operacyjnego. Rozpoczyna się zazwyczaj po otrzymaniu zadania (wytycznych) ze sztabu nadrzędnego lub własnej inicjatywy danego szczebla dowodzenia. Wytyczne do planowania powinny zawierać następujące informacje:

— koncepcję strategicznego planu wspierania działań informacyjnych;

— zamiar działań informacyjnych;
— szczegółowe zadania działań informacyjnych;
— ograniczenia metod działań informacyjnych.

Faza II – orientowanie operacyjne. Dowódca po otrzymaniu zdania dokonuje analizy zadania razem ze swoim sztabem, w celu udzielenia odpowiedzi na pytanie, jakie zadania działań informacyjnych powinny być wykonane, aby osiągnąć zakładane cele operacji.

Zadania należy pogrupować w poszczególne bloki (główne, pomocnicze, uzupełniające), aby określić jaką rolę działania informacyjne mogą odegrać w realizacji celów operacji.

Zadania główne to te, które zamierza wykonać dowódca, i które są określone w planie operacji.

Zadania pomocnicze to zadania niestandardowe, które są niezbędne do wykonania misji, ale nie wchodzą w zakres obowiązków dowódcy i nie są określone w planie operacji.

Zadania uzupełniające to te, które należy brać pod uwagę w celu wsparcia celów operacji.

Sztab pod kierunkiem CJ-3/G-3 analizuje otrzymane zadanie i sformułowany przez dowódcę zamiar operacji, po to aby następnie określić zamiar dla prowadzenia działań informacyjnych. Sztab musi rozważyć zarówno ofensywne, jak i defensywne aspekty działań nformacyjnych. Podczas rozpatrywania tych aspektów wymagana jest elastyczność i pełne uzmysłowienie sobie roli, jaką mają do spełnienia działania informacyjne, które mogą zadecydować o powodzeniu całej kampanii.

Sztab prowadzi ocenę systemów informacyjnych zarówno wojsk własnych, jak i przeciwnika w kontekście wojskowego środowiska informacyjnego (MIE), w którym będzie działał dowódca określonego szczebla dowodzenia. Celem tej analizy jest identyfikacja pojedynczych elementów, węzłów łączności i powiązań między nimi. Każdy system, pomimo różnych celów przeznaczenia, specyficznych technologii i technik, analizuje, gromadzi i przekazuje dane w celu wsparcia procesu decyzyjnego. Najpierw należy przeanalizować architekturę funkcjonalną systemu. Następnie należy dopasować architekturę fizyczną do różnych obszarów funkcjonalnych. Rezultatem powinno być określenie architektury statycznej, a następnie dynamicznej systemu.

Dlatego też należy dokonać analizy architektury informacyjnej systemu oraz protokółów i metod transmisji danych. To jest aspekt dynamiczny planisty informacyjnego

ponieważ pozwala mu określić ważny element (węzeł) w systemie, który odgrywa „kluczową" rolę w procesie decyzyjnym przeciwnika.

Kiedy to jest wykonane, planista ma ustalony stan dynamiczny systemu. Przez analizę architektury dynamicznej rozpoznaje kluczowe węzły i połączenia w systemie, których zniszczenie lub obrona może mieć decydujące znaczenie dla jego funkcjonowania.

Sztab formułuje również wymagania i określa warunki niezbędne do uzyskania przewagi informacyjnej. Osoby funkcyjne uwzględniają w swoich kalkulacjach również możliwości cywilnych systemów informacyjnych, mających strefy swojego oddziaływania poza kontrolą wojska, a które mogą mieć wpływ na operację, na przykład lokalne lub regionalne sieci łączności, stacje radiowe, telewizyjne, sieci komputerowe i media informacyjne. Analiza ta prowadzi do stworzenia listy ważnych węzłów i słabych stron zarówno po stronie własnej, jak i przeciwnika, które będą później wykorzystywane w planowaniu i prowadzeniu ofensywnych i defensywnych działań informacyjnych.

Analiza prowadzona pod kątem działań ofensywnych polega na określeniu kluczowych obiektów w systemach informacyjnych przeciwnika, do których m.in. należą ważne węzły łączności stanowisk dowodzenia. Następnie identyfikuje się te obiekty pod kątem ich eliminacji, określając m.in. ich słabe strony.

Ważną rolę zarówno w ofensywnych, jak i defensywnych działaniach informacyjnych odgrywa rozpoznanie i wywiad, dostarczając „kluczowych" danych o strukturach i dyslokacji sił zbrojnych przeciwnika, jego środkach ataku i możliwościach bojowych. Działania defensywne skupiają się na ochronie ważnych obiektów występujących w systemach informacyjnych, po to aby ochronić je przed oddziaływaniem przeciwnika. W tym aspekcie należy także brać pod uwagę walkę elektroniczną oraz ochronę własnych systemów i wojsk. W rezultacie tej analizy sporządza się listę kluczowych, wrażliwych obiektów i procesów, które muszą być objęte ochroną.

Po ukończeniu analizy zadania powinna być sporządzona pełna ocena środowiska działań informacyjnych, zaczynajaca się od rozważań czynników wpływajacych na misję, poprzez identyfikację poszczególnych celi działań informacyjnych, punktów kluczowych, zadań, aż do ustalenia kierunków rozwoju sytuacji.

Głównym celem tej fazy jest określenie prawdopodobnego działania przeciwnika oraz metody wpływania na te działania. Wszystkie systemy informacyjne powinny być poznane i szczegółowo opisane, a w szczególności zaś ich wartość, zasady użycia, proces przepływu danych i słabe strony tego procesu.

W oparciu o taki opis można zidentyfikować ogólne cele działań informacyjnych, które pomogą w osiągnięciu celów operacji połączonych.

Faza III – opracowanie zamiaru działań informacyjnych. Obowiązkiem dowódcy jest sformułowanie zamiaru (koncepcji) działań informacyjnych. CJ-3/G-3 dokonuje przeglądu swoich ustaleń odnośnie potencjalnych celów dla działań ofensywnych i defensywnych. W fazie tej następuje ustalenie celów i wybór narzędzi.

Ustalenie celów. Cele polityczne powinny być zrozumiałe i przemianowane na logiczne cele wojskowe. Już Clausewitz zauważył, że cel polityczny jest nadrzędny, wojna jest środkiem uzyskania, a środki nie powinny nigdy być brane pod uwagę w izolacji od celów.

Oczywiście cele należy ustalać w zależności od sytuacji. Dlatego też komórki planistyczne muszą dokonać analizy celów politycznych, przemianować je na cele militarne, a następnie na cele informacyjne. To pozwala udzielić odpowiedzi na pytanie: dlaczego prowadzi się działania informacyjne – co się chce osiągnąć? Udzielenie odpowiedzi na to pytanie pozwala planiście określić pożądany stan końcowy (end state).

Jasne zrozumienie celów i pożądanego stanu końcowego pozwala planiście przejść do identyfikacji kluczowych węzłów (w systemie informacyjnym przeciwnika), których zniszczenie pozwoli na wyeliminowanie systemu informacyjnego przeciwnika, a tym samym przyczyni się do wykonania zadania bojowego (osiągnięcia celów wojskowych i politycznych).

Komórki CJ-2/G-2) i CJ-3/G-3 identyfikują kluczowe obiekty (różnego rodzaju węzły łączności, systemy broni) i możliwe zagrożenie z ich strony. Te obiekty i systemy broni oraz funkcje ich zagrożeń są wyszczególnione według kategorii ważności na podstawie ich największej mocy bojowej i stopnia zagrożenia dla naszych jednostek.

Największe zagrożenie, pierwszej kategorii ważności, przyjmuje się dla elementów rozpoznawczych przeciwnika. Oczekuje się, że od elementów rozpoznawczych zależne są (przez przekazywanie poufnych danych) działania innych jednostek i systemów broni. Jeśli sukcesywnie będzie się zakłócać działania tych elementów, zostanie opóźniony przekaz danych, a tym samym atak systemów broni. Zakłócanie opóźni czas reakcji ogniowej przeciwnika, co jest jednoznaczne z opóźnieniem ataku na nasze siły.

Zagrożenie ogniem artylerii należy do kolejnej kategorii ważności. Zakłóca się sieć kierowania ogniem artylerii pomiędzy dowództwem, posterunkiem obserwacyjnym a bateriami ogniowymi. Dowódca dywizji może także dążyć do zniszczenia artylerii przeciwnika. W tym wypadku elementy rozpoznania elektronicznego mogą być

wykorzystane do lokalizacji tych obiektów (celów) dla bezpośredniego wsparcia lotniczego.

Zagrożenie WE przeciwnika należy do trzeciej kategorii ważności. Podczas atakowania przeciwnika możliwość użycia własnych radiostacji staje się bardzo ważna. Aby zapewnić wykorzystanie tych środków radiowych, należy zlokalizować stacje zakłóceń przeciwnika za pomocą własnych namierników. Po zlokalizowaniu należy je niszczyć za pomocą artylerii lub bezpośredniego wsparcia lotniczego.

Jednostki manewrowe należą do czwartej kategorii ważności od czasu, kiedy specjalne jednostki przeciwnika pojawią się na pozycjach obronnych.

Bezpośrednie wsparcie lotnicze należy do tej samej kategorii zagrożeń, ponieważ przeciwnik zwykle nie reaguje, dopóki nie ustali naszych punktów ataku. Kiedy atak się rozpocznie, bezpośrednie wsparcie lotnicze przeciwnika staje się większym zagrożeniem i może wtedy otrzymać wyższy priorytet.

Artyleria przeciwlotnicza znajduje się na ostatnim miejscu w kolejności zagrożeń, ponieważ nasz atak może nie wymagać wsparcia powietrznego. Konieczne jest jednak utrzymanie w gotowości elementów rozpoznania elektronicznego do wykrywania i lokalizacji SRL przeciwnika w strefie działań bojowych. Jeśli nasz atak przeciąga się, możemy wykorzystać bezpośrednie wsparcie lotnicze dla osiągnięcia przewagi. Bezpośrednie wsparcie lotnicze prowadzi się w celu obezwładnienia stacji radiolokacyjnych przeciwnika (zlokalizowanych przez elementy rozpoznania elektronicznego), podczas gdy nasze stacje zakłóceń zakłócają jego radiostacje. W etapie tym należy zidentyfikować wszystkie siły i środki informacyjne przeciwnika wykorzystywane w systemach dowodzenia i sterowania bronią oraz ich funkcje zagrożeń.

Określenie środków ciężkości w systemie przeciwnika pozwala na realizację następnej fazy, jaką jest wybór odpowiednich narzędzi.

Wybór narzędzi. Planista musi wybrać odpowiednie narzędzia działań informacyjnych na podstawie kilku kryteriów. Pierwszym z nich jest dostępność. Jest oczywiste, że nie każde narzędzie z arsenału działań informacyjnych będzie dostępne do wykorzystania na każdym poziomie działań. Narzędzia wykorzystywane na poziomie strategicznym czy operacyjnym nie będą nadawać się do wykorzystania na poziomie taktycznym. Ponadto należy brać pod uwagę tylko te narzędzia, które znajdują się w dyspozycji.

Kolejnym kryterium, które należy brać pod uwagę, jest zamierzony efekt, jaki planista chce osiągnąć przez wykorzystanie narzędzi. Należy wykorzystać pełny zakres

możliwości narzędzi, tak aby zniszczyć czy zneutralizować kluczowe obiekty przeciwnika lub wprowadzić go w błąd. To spowoduje, że nie będzie on w stanie podejmować reakcji na nasze działania. Oczywiście nie wolno angażować 100% posiadanych narzędzi, gdyż w wypadku ich zniszczenia znaleźlibyśmy się w pułapce bez wyjścia. Narzędzia należy wykorzystywać przez dłuższy lub krótszy okres, w zależności od sytuacji. Oczywiście dłuższe stosowanie narzędzi powoduje wzrost kosztów. Dlatego należy planować takie wykorzystanie narzędzi, aby koszty i ryzyko ich zniszczenia były jak najmniejsze. Pozytywnym przykładem mogą być wirusy komputerowe czy pociski przeciwradiolokacyjne, które neutralizują urządzenia nie niszcząc ich całkowicie.

Elementy systemu informacyjnego, zidentyfikowane przez nas jako środki ciężkości, mogą również zostać zidentyfikowane przez potencjalnego przeciwnika. Rezultatem powyższego może być ich ochrona, czyli zmniejszenie podatności na atak. Planista musi wybrać takie narzędzia, które pokrzyżują plany przeciwnikowi i będą oddziaływać na obiekt bez żadnego ryzyka.

Komórka CJ-3/G-3 określa możliwości bojowe dla struktur działań informacyjnych pod kątem ich najlepszego wykorzystania w prowadzonej kampanii i pełnej ich synchronizacji z ogólnym zamiarem operacji. Synchronizacja w aspektach: wewnętrznym – pomiędzy przedsięwzięciami wchodzącymi w kompleks działań informacyjnych, a zewnętrznym – przez wszystkie operacyjne systemy pola walki (BOSs – Battlefield Operating Systems) – jest konieczna dla osiągnięcia rozstrzygających rezultatów działań zarówno ofensywnych, jak i defensywnych. Znaczenie właściwej synchronizacji polega na skupieniu wysiłków w całym zakresie własnych możliwości dla osiągnięcia maksymalnych efektów w decydującym punkcie, czasie i przestrzeni.

Następnie wykonuje się listę celów działań informacyjnych i przyporządkowuje się im zadania.

W liście należy określić metody i techniki działań informacyjnych, które przyczynią się do wykonania zadań głównych, pomocniczych i uzupełniających.

Lista celów powinna uwzględniać obiekty oddziaływania informacyjnego (grupa osób, element systemu informacyjnego). Następnie należy określić czas oddziaływania rozpoczęcie, zakończenie itp.).

Aby to wykonać należy określić metody i techniki działań informacyjnych według kryteriów:

— możliwość osiągnięcia celów operacji;

— przychylność opinii;

— skuteczność;
— podatność przeciwnika na oddziaływanie.

Analiza **możliwości osiągnięcia celów operacji** obejmuje ocenę:
— zdolności bojowych środków działań informacyjnych w wykonaniu celów operacji;
— prawdopodobieństwa osiągnięcia sukcesu przez zastosowanie środków działań informacyjnych.

Stopnie możliwości osiągnięcia celów opracji:
— niski – działania informacyjne nie przyczynią się do osiągnięcia lub wsparcia celów operacji;
— średni – działania informacyjne mogą przyczynić się do osiągnięcia lub wsparcia celów operacji;
— wysoki – działania informacyjne definitywnie przyczynią się do osiągnięcia lub wsparcia celów operacji.

Przychylność opinii obejmuje trzy aspekty:
— polityczny – sytuacja polityczna jest sprzyjająca na zastosowanie działań informacyjnych;
— prawny – z punktu prawnego istnieje przychylność na zastosowanie środków działań informacyjnych;
— kulturalny – kultura (religia) nie powodują ograniczeń w zastosowaniu działań informacyjnych.

Stopnie przychylności:
— niski – ograniczenia uniemożliwiają zastosowanie sił i środków działań informacyjnych;
— średni – ograniczenia dopuszczają na zastosowanie sił i środków działań informacyjnych;
— wysoki – występują preferencje (brak ograniczeń) dla zastosowania sił i środków działań informacyjnych.

Skuteczność to efektywne użycie sił i środków działań informacyjnych w osiągnięciu zakładanych celów operacji.

Obejmuje następujące aspekty:
— techniczny – metody i techniki działań informacyjnych wojsk własnych będą skuteczne w stosunku do przeciwnika;

— przestrzenny –siły i środki działań informacyjnych pozwolą na wykorzystanie zasobów informacyjnych własnych systemów i pozbawią takich możliwości stronę przeciwną;
— czasowy – siły i środki działań informacyjnych zostaną wykorzystane precyzyjnie we właściwym czasie.

Stopnie skuteczności:

— niski – użycie sił i środków działań informacyjnych będzie nieskuteczne;
— średni – użycie sił i środków działań informacyjnych może być skuteczne;
— wysoki – użycie sił i środków działań informacyjnych będzie z pewnością skuteczne.

Podatność przeciwnika to jego słabe strony na oddziaływanie sił i środków działań informacyjnych.

Przy określaniu podatności należy dokonać analizy celów głównych i szczegółowych oraz wziąć pod uwagę, które działania przeciwnika będą podatne na oddziaływanie informacyjne naszych wojsk.

Są dwa sposoby postępowania, które pozwalają na ocenę podatności przeciwnika. Pierwszy zależy od planistów działań informacyjnych wojsk własnych. Planiści znają cele działań informacyjnych wojsk własnych i wiedzą,do których działań przeciwnika należy zastosować metody i techniki działań informacyjnych aby osiągnąć zakładane rezultaty i wyeliminować z walki kluczowe elementy systemów informacyjnych przeciwnika.

W drugim przypadku należy brać pod uwagę sytuację, że planiści przeciwnika przewidzą działania informacyjne naszych wojsk i podejmą niezbędne kroki, aby pokrzyżować plany. W tym wypadku planiści powinni udzielić odpowiedzi na pytanie, jakie działania może przewidzieć przeciwnik, jeśli zamierza pokrzyżować sukces działań informacyjnych naszych wojsk.

Stopnie podatności:

— niski – podatność przeciwnika na działania informacyjne jest ograniczona;
— średni – podatność przeciwnika na działania informacyjne jest umiarkowana;
— wysoki – przeciwnik jest ekstremalnie podatny na działania informacyjne.

Zrozumienie zasady działań informacyjnych przeciwnika, określenie celów szczegółowych, zidentyfikowanie środków ciężkości i wybór narzędzi są elementami świadczącymi o zrealizowaniu tej fazy planowania.

Faza IV – opracowanie planu. W trakcie tej fazy zamiar działań informacyjnych ulega skonkretyzowaniu. Dowódca i sztab muszą uwzględnić w planie operacji następujące specyficzne zadania:

— prowadzenie ofensywnych i defensywnych działań informacyjnych, zarówno z perspektywy wojsk własnych, jak i przeciwnika;
— określenie potrzeb w stosunku do zdobywania danych z rozpoznania i wywiadu;
— ustalenie wymagań w stosunku do wsparcia działań przez systemy informacyjne;
— ustalenie synchronizacji wszystkich elementów działań informacyjnych (linie czasowe, odpowiedzialność, poszczególne fazy działania i pożądane rezultaty).

Zadania dla struktur działań informacyjnych powinny znaleźć się w rozkazie operacyjnym, który oprócz zamiaru operacji zawiera wskazówki w zakresie koordynacji. Dodatkowe szczegóły zawarte są w oddzielnych aneksach.

Dodatkowo planiści muszą mieć świadomość, że przeciwnik, oddziałując informacyjnie, będzie prawdopodobnie atakował również infrastrukturę cywilną. Inne ośrodki oddziaływania występujące w środowisku informacyjnym, takie jak: media, organizacje rządowe i pozarządowe mogą mieć również bezpośredni wpływ na sukces misji. Zagrożenie takimi akcjami może powodować nie tylko skutki rzeczywiste, ale także psychologiczne.

Faza V – weryfikacja planu. W tej fazie planista musi porównać zaplanowane efekty stanu końcowego systemu ze stanem aktualnym. Mamy tu do czynienia z dwoma typami sprzężenia zwrotnego, które pozwalają planiście na dostosowanie wysiłków w razie konieczności.

Pierwszy z nich polega na porównaniu efektów (dotyczących atakowania lub ochrony własnych elementów) z efektami pożądanymi ustalonymi w fazie trzeciej. Jeśli efekty realne są zgodne z pożądanymi, można przejść do kolejnych działań. Jeśli efekty aktualne nie są zgodne z pożądanymi (oczekiwanymi), planista powinien określić ponownie czy efekt będzie wystarczający, jeśli nie to należy wziąć pod uwagę ponowne atakowanie systemu informacyjnego przeciwnika. Musi także ocenić, dlaczego efekt aktualny różni się od zaplanowanego, czy narzędzia zostały właściwie wykorzystane oraz czy podatność obiektu na oddziaływanie została właściwie oceniona.

Drugi typ sprzężenia dotyczy ciągłego porównywania efektów oddziaływania na systemy informacyjne przeciwnika, jako całości, z pożądanym stanem końcowym ustalonym w fazie drugiej. To zapewnia planiście możliwość kontroli postępów w zakresie osiągania celów prowadzonej kampanii. To pomaga udzielić odpowiedzi na pytanie: kiedy zakończyć prowadzoną kampanię i skierować zasoby gdzie indziej. To może być także

wskazówka, która umożliwi zrekonstruowanie modelu systemu informacyjnego i zrewidowanie wyboru środków ciężkości.

5.2. Zasady prowadzenia działań informacyjnych w operacjach połączonych

Zakres i stopień zaangażowania narodowych sił i środków działań informacyjnych określony jest postanowieniami konstytucji, „Strategii bezpieczeństwa RP", „Strategii obronności RP" oraz „Polityczno-strategicznej dyrektywy obronnej".

Szczegółowy zakres zasad działań informacyjnych w ramach sojuszniczych planów operacyjnych określają następujące dokumenty normatywne:

— „Polityka NATO w zakresie działań informacyjnych" (MC-422/1 NATO Information Operations Policy) - 2002;

— „Doktryna NATO w zakresie działań informacyjnych" (AJP-3,10 NATO Information Operations Doctrine) - 2003;

Na poziomie narodowym, Rada Ministrów RP powinna określać ogólne cele, kierunki i wytyczne prowadzonych działań informacyjnych, na podstawie zaakceptowanych przez parlament głównych założeń polityki zagranicznej i obronnej państwa.

Zakres odpowiedzialności Rady Ministrów RP za działania informacyjne na poziomie strategicznym obejmuje:

— określenie celów i pożądanych efektów działań informacyjnych;

— koordynowanie narodowych działań informacyjnych z przedsięwzięciami realizowanymi w ramach operacji sojuszniczej;

— kierowanie działaniami informacyjnymi, realizowanymi w ramach strategicznych działań informacyjnych, siłami i środkami wyspecjalizowanych jednostek Sił Zbrojnych RP.

Zakres odpowiedzialności Ministerstwa Obrony Narodowej obejmuje:

— przedstawianie Radzie Ministrów RP propozycji w zakresie prowadzenia działań informacyjnych z zamiarem osiągnięcia narodowych i wojskowych celów operacji;

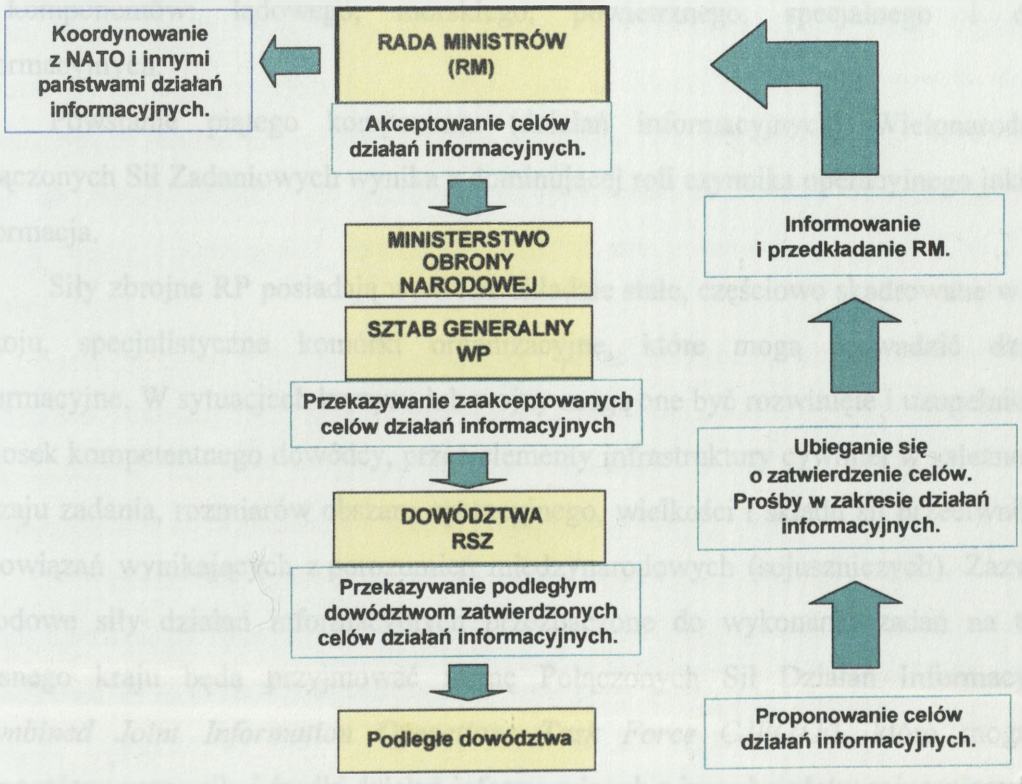
— planowanie działań informacyjnych na poziomie strategicznym,

— opracowanie doktryny i koncepcji prowadzenia działań informacyjnych;

— aktualizowanie planów działań informacyjnych i kierowanie ich realizacją zgodnie z interesem narodowym i zobowiązaniami sojuszniczymi;

— wytyczanie kierunków rozwoju organizacyjnego i technicznego organów działań informacyjnych w SZ RP;
— współpracę ze sztabami NATO, w tym udział w pracach grupy roboczej NATO ds. działań informacyjnych.
— współpracę z organami układu pozamilitarnego odpowiedzialnymi za prowadzenie działań informacyjnych;
— monitorowanie stanu przygotowania środków działań informacyjnych układu pozamilitarnego do funkcjonowania w narodowym lub sojuszniczym systemie obronnym
— określenie założeń do prac badawczo-rozwojowych oraz wdrożeniowych w zakresie działań informacyjnych.

Organem kordynującym i planistycznym wojskowych działań informacyjnych jest Ministerstwo Obrony Narodowej. W ramach swoich kompetncji współpracuje z innymi instytucjami i agendami rządowymi, jak również – poprzez swoich przedstawicieli w sztabach sojuszu – z odpowiednimi jego strukturami.



Rys. 5.2.1. Narodowy system zatwierdzania działań informacyjnych

Dowódcy poszczególnych rodzajów sił zbrojnych odpowiadają za:
— planowanie działań informacyjnych na szczeblu operacyjnym i taktycznym;

— wytyczanie kiernków działania podległych dowództw w zakresie działań informacyjnych;

— utrzymywanie gotowości wyspecjalizowanych jednostek przeznaczonych do działań informacyjnych;

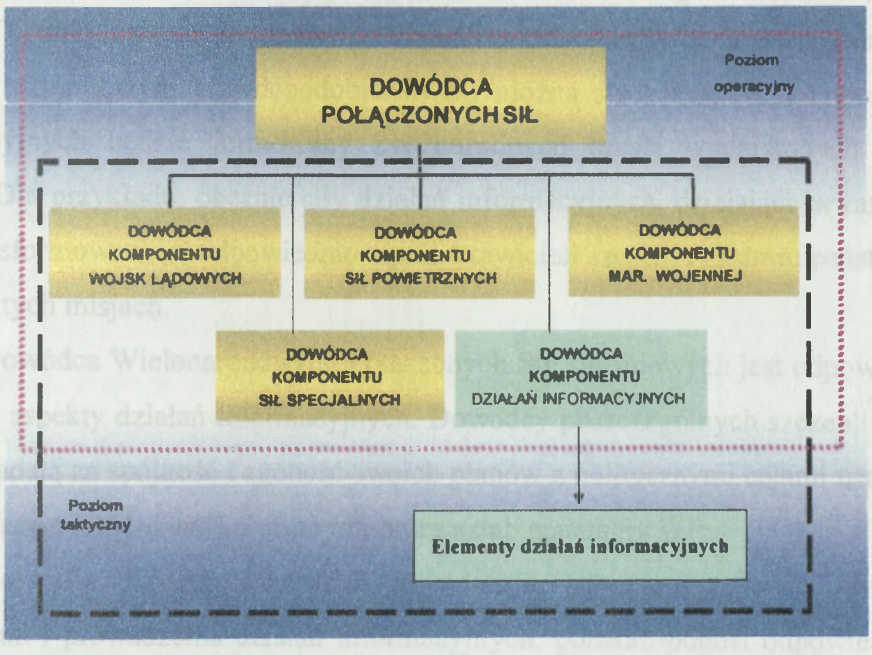
— planowanie i oranizowanie przedsięwzięć szkoleniowych w i artykułowanymi przez zakresie wykorzystania sił i środków działań informacyjnych w operacjach połączonych;

— współpracę i wymianę doświadczeń z dowództwami NATO oraz jednostkami działań informacyjnych państw członkowskich NATO.

W celu realizacji operacji połączonej powołuje się ***Wielonarodowe Połączone Siły Zadaniowe***, których skład obejmuje co najmniej dwa państwa i co najmniej dwa rodzaje sił zbrojnych przeznaczone do działania na połączonym obszarze operacyjnym, ale w różnych środowiskach i na różnych kierunkach. Skład, struktura, obsada i wyposażenie oraz podporządkowanie tych sił uzależnione są od określonego celu strategicznego. Zgodnie z najnowszymi wymogami sztuki operacyjnej a dalej dyrektywami NATO składają się one z komponentów: lądowego, morskiego, powietrznego, specjalnego i działań informacyjnych.

Powstanie piątego komponentu (działań informacyjnych) Wielonarodowych Połączonych Sił Zadaniowych wynika z dominującej roli czynnika operacyjnego jakim jest informacja.

Siły zbrojne RP posiadają w swoim składzie stałe, częściowo skadrowane w czasie pokoju, specjalistyczne komórki organizacyjne, które mogą prowadzić działania informacyjne. W sytuacjach kryzysu lub wojny mogą one być rozwinięte i uzupełnione, na wniosek kompetentnego dowódcy, przez elementy infrastruktury cywilnej w zależności od rodzaju zadania, rozmiarów obszaru operacyjnego, wielkości i składu sił przeciwnika lub zobowiązań wynikających z porozumień międzynarodowych (sojuszniczych). Zazwyczaj narodowe siły działań informacyjnych przeznaczone do wykonania zadań na terenie własnego kraju będą przyjmować formę Połączonych Sił Działań Informacyjnych *(Combined Joint Information Operations Task Force CJPOTF)*, które mogą być wzmocnione przez siły i środki działań informacyjnych z innych państw sojuszniczych.



Rys. 5.2.2. Struktura Połączonych Sił Zadaniowych (z elementami działań informacyjnych

Wielonarodowe Połączone Dowództwo Działań Informacyjnych (WPDDI) odpowiada za wszystkie aspekty działań informacyjnych podczas operacyjnego wspierania Połączonych Sił Zadaniowych NATO. Dowódca wielonarodowego komponentu działań informacyjnych będzie pełnił rolę doradcy dowódcy ogólnowojskowego i jednocześnie będzie on odpowiedzialny za planowanie i prowadzenie działań informacyjnch, jak również będzie koordynował wysiłek podległych mu jednostek – elementów działań informacyjnych.

Wielonarodowe Połączone Dowództwo Działań Informacyjnych będzie formowane z sił działań informacyjnych państw, których wojska biorą udział w operacji. W jego skład mogą wchodzić zarówno żołnierze państw członków NATO, jak również i państw niezrzeszonych w tej organizacji – w ramach partnerstwa dla pokoju – PfP.

O ile ostateczny podział zadań dla dowództwa (WPDDI) będzie uzależniony od rodzaju operacji, jej geograficznego zasięgu i wielkości audytorium, na które będzie się oddziaływać, to struktura przedstawiona w niniejszej pracy odnosi się do minimalnych wymagań, koniecznych, aby skutecznie wspierać siły operacyjne na poziomie teatru działań. Struktura tego dowództwa ma charakter modularny, co ma umożliwić szybkie jego zorganizowanie i przystosowanie do wymagań danej operacji.

Obecnie tylko dwa państwa z grupy członków NATO – Stany Zjednoczone i Niemcy – są w stanie przyjąć na siebie rolę państwa wiodącego („Framework nation")

w zakresie prowadzenia działań informacyjnych. Stąd mało prawdopodobnym jest, aby siły NATO otrzymały do prowadzenia działań informacyjnych komponent jednonarodowy. Dlatego też, z dużym prawdopodobieństwem można stwierdzić, że komponent działań informacyjnych będzie formowany z różnorodnych części wydzielonych przez kilka krajów. Dla przykładu, obecnie siły działań informacyjnych, działające w ramach KFOR i SFOR, sformowane są odpowiednio z przedstawicieli sześciu i siedmiu państw biorących udział w tych misjach.

Dowódca Wielonarodowych Połączonych Sił Zadaniowych jest odpowiedzialny za militarne aspekty działań informacyjnych. Dowódcy poszczególnych szczebli dowodzenia odpowoiadają za spójność i zgoność swoich planów z politycznymi celami ustanowionymi przez państwo (RM) i artykułowanymi przez sztab generalny WP.

Dowódca każdego szczebla dowodzenia powinien zapewnić wytyczne do planowania i prowadzenia działań informacyjnych, ponadto ponosi odpowiedzialność za angażowanie posiadanych zasobów w osiągnięciu celów tych działań.

Szef sztabu powinien być odpowiedzialny za zapewnienie, iż wszystkie ustanowione przez dowodzącego operacją połączoną cele działań informacyjnych są implementowane przez poszczególne dowództwa.

Wyznaczony oficer (ds. działań informacyjnych) powinien przewodniczyć w planowaniu, koordynacji i prowadzeniu działań informacyjnych.

Zakres odpowiedzialności oficera sztabu ds. działań informacyjnych powinien obejmować:

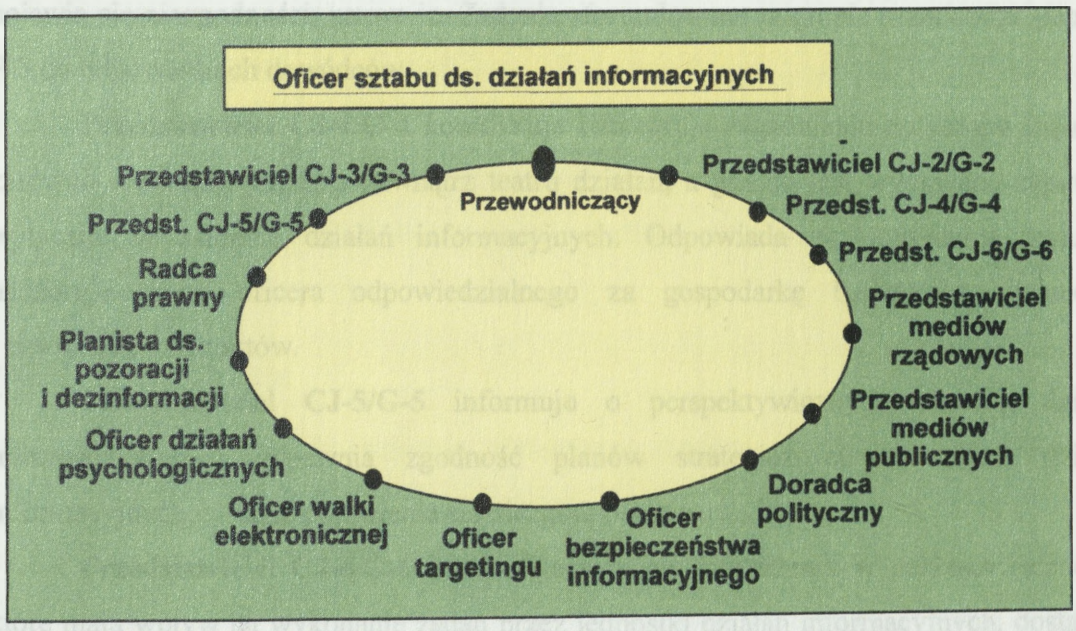
— planowanie i prowadzenie działań informacyjnych;
— koordynowanie działań informacyjnych w ramach wszystkich komponentów należących do Grupy Koordynacyjnej Działań Informacyjnych;
— koordynowanie przedsięwzięć realizowanych w ramach narodowych i sojuszniczych działań informacyjnych;
— ustanawianie w imieniu dowódcy (szefa sztabu) priorytetów działań informacyjnych;
— koordynowanie wykorzystania zasobów informacyjnych;
— rekomendowanie zadań dla poszczególnych komórek działań informacyjnych;
— nadzorowanie procesu selekcji celów działań informacyjnych;
— ustanowienie zasad użycia broni (ROE) w ramach Grupy Koordynacyjnej działań Informacyjnych.

Działania informacyjne postrzegane będą przez odbiorców (audytorium) jako wyraz polityki narodowej i sojuszniczej. Wszelkie niespójności w tym zakresie pomiędzy różnymi agencjami i instytucjami na różnych poziomach mogą dyskredytować dane działanie i zniweczyć narodowe lub sojusznicze cele operacji. Aby temu zapobiec, powołuje się Grupę Koordynacyjną Działań Informacyjnych.

Grupa Koordynacyjna Działań Informacyjnych jest odpowiedzialna za tworzenie i rozpowszechnianie wytycznych w zakresie prowadzenia działań informacyjnych oraz za kierowanie i koordynowanie działalności służącej osiągnięciu pożądanych przez dowódcę efektów.

Koordynacja ta powinna obejmować poszczególne przedsięwzięcia działań informacyjnych, ustalanie priorytetów, włącznie z określeniem obiektów ataku.

Grupie powinien przewodniczyć oficer ds. działań informacyjnych. Grupa składa się z przedstawicieli wszystkich komórek sztabu, komponentów i wspierających agencji (rys. 5.2.3).



Rys. 5.2.3. Grupa Koordynacyjna Działań Informacyjnych

Grupa jest organem wykonawczym i dlatego istotnym jest, aby reprezentanci poszczególnych komórek mieli uprawnienia do zajmowania określonego stanowiska w sprawie i podejmowania decyzji w imieniu organów, które reprezentują.

Członkostwo grupy nie jest stałe i zależy od misji i roli, jaką mają spełnić działania informacyjne w osiągnięciu celów dowódcy.

Indywidualne zakresy odpowiedzialności powinny przedstawiać się następująco.

Doradca polityczny (DPO) powinien doradzać grupie w zakresie politycznych implikacji proponowanych planów działań informacyjnych. W razie potrzeby zapewnia polityczne wytyczne oraz koordynuje cele polityczne ze swoimi odpowiednikami wyższego szczebla.

Radca prawny powinien doradzać grupie w zakresie prawnych aspektów planów działań informacyjnych, zapewniając zgodność działań z prawem międzynarodowym. Gdy jest to wymagane uczestniczy w koordynacji między agencjami i w negocjacjach.

Przedstawiciel informowania opinii publicznej powinien doradzać w zakresie spraw związanych z mediami. Koordynuje i usuwa różne konflikty. Jest to instytucja niezależna, dlatego reprezentant tego obszaru nie może wykonywać poleceń grupy.

Przedstawiciel CJ-2/G-2/ monitoruje sytuację, planuje, koordynuje i kieruje działaniami rozpoznania i przeciwrozpoznania, określa wymagania z zakresu rozpoznania.

Przedstawiciel CJ-3/G-3 (oficer działań informacyjnych) informuje o bieżącej sytuacji i zapewnia zgodność przedsięwzięć z celami działań informacyjnych, a gdy pojawią się niezgodności, usuwa je. Zadania sformułowane w grupie przechodzą poprzez P-3 do odpowiednich dowódców.

Przedstawiciel CJ-4/G-4 koordynuje i integruje zagadnienia dotyczące logistyki zarówno wewnątrz jak i na zewnątrz teatru działań, a gdy to jest wymagane zapewnia wytyczne w zakresie działań informacyjnych. Odpowiada za utrzymanie techniki, nadzoruje pracę oficera odpowiedzialnego za gospodarkę budżetową, finansową i zawieranie kontraktów.

Przedstawiciel CJ-5/G-5 informuje o perspektywicznych planach działań informacyjnych i zapewnia zgodność planów strategicznych z celami działań informacyjnych, w razie pojawienia się niezgodności, usuwa je.

Przedstawiciel CJ-6/G-6 monitoruje sytuację i zdarzenia w zakresie łączności, które mają wpływ na wykonanie zadań przez jednostki działań informacyjnych, dostarcza danych z zakresu łączności niezbędnych w procesie planowania operacyjnego. Umożliwia dostęp do systemów informacyjnych, organizuje koordynację planistów systemów informacyjnych, ponadto koordynuje współpracę z P-3 dla zminimalizowania wpływu działań informacyjnych na własne systemy.

Przedstawiciel komórki ustalania celów do uderzeń (targetingu) reprezentuje swoją komórkę i powinien zapewnić, że ustalanie celów uderzeń jest spójne z celami działań informacyjnych.

Przedstawiciel sił specjalnych reprezentuje wojska specjalne i koordynuje ich użycie w działaniach informacyjnych w obszarze odpowiedzialności.

Oficerowie łącznikowi dowództw RSZ powinni być ogniwami łączącymi grupę koordynacyjną z połączonymi komponentami RSZ, zapewniają wiedzę ekspercką i przepływ danych. Specyficzne wymagania komponentów RSZ w zakresie wsparcia informacyjnego powinny także trafiać za ich pośrednictwe do grupy koordynacyjnej.

Przedstawiciel działań psychologicznych integruje i koordynuje prowadzenie działań psychologicznych w ramach całościowego planu działań informacyjnych.

Przedstawiciel walki elektronicznej powinien koordynować całokształt działalności w zakresie walki elektronicznej. Ściśle współpracuje z P-6 dla uniknięcia konfliktów w ramach wykorzystania fal elektromagnetycznych. Rozwiązuje konflikty dotyczące częstotliwości zastrzeżonych i prowadzenia zakłóceń elektronicznych.

Przedstawiciel maskowania i dezinformacji powinien koordynować działania dowództw poszczególnych szczebli lub dowództw połączonych sił w zakresie planowania dezinformacji i maskowania.

Przedstawiciel bezpieczeństwa informacyjnego powinien koordynować wszystkie przedsięwzięcia dotyczące ochrony własnych systemów informacyjnych.

Przedstawiciel współpracy cywilno-wojskowej (CIMIC) powinien zapewnić spójność zadań w zakresie CIMIC w obszarze odpowiedzialności. Nie otrzymuje jednak zadań od grupy koordynacyjnej.

5.3. Efekty poznania

1. Zaproponowany schemat planowania działań informacyjnych może być przydatny w praktyce. W trakcie jego realizacji szczególna uwaga powinna być zwrócona na dogłębną analizę punktów „kluczowych", zarówno wojsk własnych, jak i przeciwnika. Atakowanie tych punktów (elementów) może spowodować wyeliminowanie systemu informacyjnego przeciwnika. Środki działań informacyjnych dają możliwość sprawowania kontroli nad szybkością procesu decyzyjnego zarówno przeciwnika, jak i wojsk własnych. Członkowie struktur działań informacyjnych powinni znać priorytety przeciwnika, jego cele, kulturę i wartości moralne. Jeżeli działania informacyjne są prowadzone ze znacznym wyprzedzeniem oraz skutecznie, mogą zapobiec konfliktom lub zredukować straty wojsk własnych.

2. Przedsięwzięcia realizowane w ramach działań informacyjnych powinny być zintegrowane z działaniami bojowymi. W celu stworzenia integralnego planu operacji

należy podejmować różnorodne działania, mające na celu wyciągnięcie jak największych korzyści i uzyskania koordynacji działań między siłami zbrojnymi a różnymi agencjami rządowymi i pozarządowymi. Szczególna rola w tym zakresie przypada rozpoznaniu i wywiadowi, które dają dowódcy narzędzie autentycznego postrzegania pola walki i reagowania na działania przeciwnika. Z pomocą struktur działań informacyjnych zwiększa się zasięg wariantów zapobiegawczych, które wykraczają poza tradycyjne metody , a tym samym stają się integralnym komponentem sił zbrojnych.

3. Ocena słabych stron w systemach informacyjnych identyfikuje niedociągnięcia własnych systemów informacyjnych. Wysiłek komórek CJ-3/G-3 oraz CJ-2/G-2 powinien się koncentrować na zapewnieniu wsparcia dla jednostek bojowych ze strony struktur działań informacyjnych. Komórki te otrzymują dane od różnorodnych elementów, wliczając w to siły specjalne, struktury przeciwrozpoznawcze i kontrwywiad (CI – Counterintelligence) oraz inne źródła wywiadowcze wewnątrz danego kraju. Dowódca określa „kluczowe" dane skupiając się także na ochronie wojsk własnych.

4. Opracowanie zamiaru działań informacyjnych powinno być realizowane według nastepujacych zasad:

— cele ofensywnych i defensywnych działań informacyjnych powinny być jasno ustalone i jednocześnie powinny wspierać cele militarne przedstawione w zarzadzeniu wstepnym. Cele te powinny być opisane w taki sposób, aby nie wymagały określonych działń ze strony podległych dowództw lub ich lementów funkcjonalnych. Na tym etapie powinna być zidentyfikowana metoda mierzenia skuteczności prowadzonych działań;

— wybór specyficznych zdolności działań informacyjnych dla działań skierowanych na przeciwnika musi być adekwatny do sytuacji i spójny z celami zawartymi w planie. Cele te powinny być zgodne z prawem krajowym i międzynarodowym oraz zdefiniowanymi dla danej operacji zasadami użycia broni (ROE);

— działania informacyjne wpierające cele operacji połączonych mogą być prowadzone przez struktury spoza RP. Działania tych sił lub agencji muszą być dokładnie koordynowane, integrowane, a ponadto należy zadbać, aby nie powodowały konfliktów z innymi aspektami i elementami operacji.

5. W działaniach informacyjnych prowadzonych w układzie narodowym można wyróżnić działania o charakterze ogólnonarodowym (z wykorzystaniem sił i środków znajdujących się w bezpośredniej lub pośredniej dyspozycji państwa) oraz militarnym

(z użyciem wyspecjalizowanych jednostek Sił Zbrojnych RP), za których wykorzystanie odpowiedzialność ponoszą dowódcy określonych szczebli.

6. Rada Ministrów RP na poziomie narodowym, powinna określać ogólne cele, kierunki i przedsięwzięcia działań informacyjnych, na podstawie zaakceptowanych przez parlament głównych założeń polityki zagranicznej i obronnej państwa,

7. Za planowanie i prowadzenie działań informacyjnych w siłach zbrojnych na poziomie strategicznym i operacyjnym odpowiedzialność powinien ponosić Sztab Generalny Wojska Polskiego oraz dowództwa rodzajów sił zbrojnych.

ZAKOŃCZENIE

Treści przedstawione w rozprawie stanowią wynik kilkuletnich badań nad problematyką działań informacyjnych. W procedurze poznawczej wykorzystywane były metody badań dostosowane do poznawania zjawisk złożonych. Podejście systemowe pozwoliło na uzyskanie nowych efektów poznawczych, do których można zaliczyć:

- przedstawienie uwarunkowań historycznych działań informacyjnych oraz określenie ich genezy;
- rozstrzygnięcie kwestii terminologicznych i klasyfikacyjnych działań informacyjnych;
- określenie istoty działań informacyjnych;
- przedstawienie koncepcji uzyskiwania przewagi informacyjnej;
- określenie zasad planowania i prowadzenia działań informacyjnych w operacjach połączonych.

Przeprowadzone, w ramach rozprawy, badania potwierdzają, że rozwój cywilizacyjny oraz postęp naukowo-techniczny powoduje, że zmieniają się formy i środki walki. Oprócz znacznego rozwoju środków elektronicznych (mikroprocesory, generatory impulsu elektromagnetycznego, bomby „logiczne", wirusy komputerowe) oraz mass mediów (Internet, telewizja, radio, prasa) pojawiły się nowe możliwości oddziaływania, jak chociażby broń wiązkowa (energii kierowanej), światła stroboskopowe wywołujące nudności czy infradźwięki powodujące depresje, napięcia, strach, sztuczną wesołość, spowolnienie reakcji, dolegliwości sercowe i zaburzenia równowagi. Ponadto mogą być wykorzystane różne techniki psychotroniczne, które wywołują subiektywne i obiektywne zachowania ludzi pod wpływem sugestii lub autosugestii.

Sytuacja ta powoduje, że współczesne konflikty zbrojne zmieniają swój konwencjonalny charakter, przesuwając środek ciężkości na oddziaływanie informacyjne, które prowadzone w umiejętny sposób może znacząco wpływać na powodzenie operacji połączonych.

W wieku informacji zapotrzebowanie na użyteczną informację staje się jednym z najważniejszych zadań działalności w sferze cywilnej i militarnej. Aktualnie informacja jest traktowana jako zasób strategiczny. Takie znaczenie informacji przypisuje się m.in. ze względu na szybki rozwój technologii informacyjnych (metod), które w znaczny sposób przyśpieszają proces komunikowania się i zdobywania wiedzy. Technologia informacyjna oferuje chirurgiczną dokładność lokalizacji obiektów, która nie była dostępna w przeszłości. Dzięki cyfrowemu zobrazowaniu sytuacji na polu walki jednostki będą

miały możliwość uzyskania znacznie większej mocy bojowej. Większej mocy bojowej nie można będzie tworzyć przez gromadzenie większej ilości danych. Ale można zwiększyć moc bojową przez wykorzystanie własnych sił i środków działań informacyjnych, ale tylko tam i w czasie, w którym są one niezbędne do osiągnięcia celów militarnych. Dlatego też zwiększenie świadomości sytuacyjnej może nastąpić na skutek zdobycia istotnych („kluczowych") informacji, co doprowadzi do wyeliminowania niepewności i podjęcia niezbędnych środków bezpieczeństwa. Ta rewolucja informacyjna wskazuje, że informacja i technologie informacyjne powinny zostać włączone we wszelką działalność militarną, szczególnie w proces decyzyjny oraz powinny stać się narzędziami walki, aby osiągnąć cele polityczne i wojskowe.

Rewolucja informacyjna oraz nowe zagrożenia (narastanie terroryzmu) na całym świecie spowodowały nową sytuację geostrategiczną, co znalazło swoje odzwierciedlenie w nowej koncepcji strategicznej sojuszu. Konieczność ciągłego utrzymywania pokoju w różnych sytuacjach kryzysowych zmusza siły zbrojne sojuszu do zachowania odpowiednio wysokiej gotowości operacyjnej i stosownie dużej mobilności wojsk celem szybkiego rozwijania się na odległych teatrach działań operacyjnych. Dlatego też w planach strategicznych sojuszu szczególną rolę odgrywają połączone operacje wielonarodowe, których podstawą jest najwyższa interoperacyjność sił połączonych, jak też poszczególnych kontyngentów narodowych, a także niektórych państw partnerskich.

Gwarancją powodzenia operacji połączonych jest zaangażowanie w ten proces całego potencjału obronnego, zarówno militarnego, jak i pozamilitarnego. Istotną rolę w tych warunkach – oprócz działań zbrojnych – odgrywają działania informacyjne, które w znaczny sposób mogą przyczynić się do osiagnięcia założonych celów operacji połączonych.

Dlatego też wiele krajów na świecie opracowuje koncepcje działań informacyjnych oraz tworzy struktury do ich realizacji.

Struktury działań informacyjnych zorganizowano we wszystkich rodzajach sił zbrojnych USA. Zastosowanie sił i środków przeznaczonych do prowadzenia działań informacyjnych może w krótkim czasie doprowadzić do całkowitego zniszczenia nowocześnie zorganizowanego systemu całego państwa. Właśnie dlatego wysoko uprzemysłowione społeczeństwa są zmuszone zastanawiać się nad środkami ochrony własnych systemów informacyjnych, 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 działań informacyjnych będą narażone na oddziaływanie strony przeciwnej. Ponadto siły polityczne z rzekomo 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 objęte są zakazem eksportu do tych regionów. Rozwój w tej dziedzinie 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.

Rosja jest szczególnie zainteresowana rozwojem i wdrażaniem środków działań informacyjno-psychologicznych przez światowe potęgi. Działania informacyjne niosą poważne implikacje dla Rosji i to zarówno w technicznym, jak i moralno-psychologicznym aspekcie. Rosjanie wskazują, że informacyjne bezpieczeństwo jednostki i całego społeczeństwa jest jednym z priorytetów interesu narodowego.

Armia rosyjska jest szczególnie zainteresowana wpływem działań informacyjno-psychologicznych na swoich żołnierzy – co wynika z doktryny wojennej. Należy oczekiwać, że rosyjska armia będzie gotowa do prób wykorzystania działań informacyjnych przeciw żołnierzom innych krajów.

Przyszłe pole walki będzie cechować się wysoką skutecznością rażenia broni, dużą manewrowością i wymagać będzie dotrzymania kroku nowoczesnym armiom w tym zakresie. Siły lądowe będą mniej liczebne, ponadto będą miały większą mocą bojową z powodu technologii informacyjnych, podnoszących walory stosowanej broni i taktyki. Obecnie systemy broni umieszcza się na tym, co w języku wojskowym nazywa się nośnikiem lub za pomocą nośników systemy te się dostarcza. Nośnikiem może być rakieta, samolot, statek czy nawet ciężarówka. Okazuje się, że tani, prymitywny technicznie nośnik, którym posługują się biedne, małe kraje, może transportować „inteligentne" wytwory zaawansowanych technologii – broń wyposażoną w odpowiednie oprogramowanie. „Głupie" bomby często mogą powiększyć swój iloraz inteligencji dzięki wprowadzeniu nowoczesnych komponentów zależnych od programu ich konstruowania lub funkcjonowania. Projekt struktury sił zbrojnych XXI wieku musi więc uwzględniać znacznie mniejszą armię, składającą się z oddziałów (formacji) o większej manewrowości i większej skuteczności rażenia niż siły zbrojne posiadały w przeszłości.

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 wieku informacji znajduje już 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 bogactw naturalnych i bazy przemysłowej. Natomiast zwycięstwo nad państwem wieku informacji wymaga pozbawienia go możliwości wykorzystania jego systemów informacyjnych. Tę możliwość zapewniają właśnie działania informacyjne, które mogą być prowadzone zarówno przez siły zbrojne, jak i organa niemilitarne.

Na podstawie literatury przedmiotu badań należy sądzić, że w przyszłych konfliktach zbrojnych dążenie do uzyskania przewagi informacyjnej nad przeciwnikiem przez prowadzenie działań informacyjnychmoże stać się regułą postępowania.

Rozprawa nie pretenduje do tego, by była postrzegana jako całościowe opracowanie teorii działań informacyjnych, lecz stanowi jej podstawę i może służyć za punkt wyjścia do opracowania koncepcji działań informacyjnych oraz szczegółowych zasad ich przygotowania i prowadzenia.

Siły Zbrojne RP mają obecnie żołnierzy szkolonych w różnorodnych specjalnościach, wliczając w to grupę działań psychologicznych, jednostki specjalne oraz rozpoznania i walki elektronicznej, jednak niewielu żołnierzy ma przygotowanie dające im podstawy do szerszego, całościowego objęcia wszystkich działań realizowanych w ramach działań informacyjnych. Szkolenie w tym zakresie może spowodować, że każdy stanie się fachowcem w kilku aspektach przedsięwzięć z zakresu działań informacyjnych. Niemniej jednak przygotowanie dowódców i żołnierzy do umiejętnego prowadzenia działań informacyjnych będzie wymagało czasu i nakładów finansowych.

BIBLIOGRAFIA:

1. Biela A., *Informacja a decyzja*", Warszawa, PWN, 1976.
2. Balcerowicz B., *Pokój i nie-pokój*, Warszawa, Bellona, 2002.
3. Beer S., *Cybernetyka a zarządzanie,* Warszawa, 1986.
4. Berg A. I., *Informacja i cybernetyka*, Warszawa, WNT, 1970.
5. Bertalanfy von L., *Ogólna Teoria Systemów*, Warszawa, PWN, 1984.
6. Biela A., *Informacja a decyzja*, Warszawa, PWN,1976.
7. Bielecki R., *Pustynna Burza*, Warszawa, Bellona, 1991.
8. Bielski, M. *Organizacja; istota, struktury, procesy*. Wydawnictwo Uniwersytetu Łódzkiego, Łódź 1992.
9. Bilska A., Flasza R., *Organizacja i metody pracy społecznej w przedsiębiorstwach*, KiW, Warszawa, 1978.
10. Bojarski R., *Główne problemy działań operacyjnych*, Warszawa, AON, 2001.
11. Boucher J., *Broń pancerna w wojnie,* Warszawa, MON, 1958.
12. Brillouin. L., *Nauka a teoria informacji*, Warszawa, PWN, 1969.
13. Buczkowski L., Metody pracy kierowniczej, Warszawa, PWE,1977.
14. Buhler C., Allen M., *Introduction to humanistic psychology,* Cole Monterey, Brooks, 1972.
15. Campen A. D., *The first Information War,* Virginia, 1992.
16. Cenin M., *Psychologia wojskowa: teoria i praktyka*, Warszawa, 1998.
17. Chlewiński Z., *Dojrzałość: osobowość, sumienie, religijność,* Poznań, Wydawnictwo „W drodze", 1991.
18. Ciborowski L., *Walka informacyjna,* Toruń, Adam Marszałek, 1999.
19. Ciborowski L., *Zasoby informacyjne jako obiekt zarządzania*. VI Międzynarodowa Konferencja Naukowa VALUE 2003. Materiały konferencyjne, Lublin, UMCS, 2003.
20. Ciborowski L., *Zarządzanie zasobami informacyjnymi w walce i operacji,* Warszawa, AON, 2002.
21. Ciborowski L., *Przestrzenie walki informacyjnej,* Warszawa, AON, 1997.
22. Ciganik M., *Systemy informacyjne w nauce, technice i ekonomice*, Warszawa, PWE, 1984.
23. Clements S. M., *The one with the Most Information Wins? The Quest for Information Superiority,* Ohio, Air Force Institute of Technology, 1997.

24. Clausewitz C., *O wojnie,* Lublin, Test, 1995.
25. Coase, R.H. *The Firm, The Market, and The Law*. Chicago, University of Chicago Press, 1990
26. Coe C, Dockery T. J., *Initiatives in C2 Analysis and Simulation*, [w:] *Science of Command and Control: Coping with Uncertainty,* red. Stuart E. Johnson, Alexander. H. Levis, Washington, International Press, 1988.
27. Cooper J., *Dominant Battlespace Awareness and Future Warfare,*[w:] *Dominant Battlespace Knowledge: The Winning Edge,* red. E. S. Johnson, M. C. Libicki, Washington, National Defense University Press, 1995.
28. Couffignal L., *Cybernetyka*, Paryż, 1965.
29. Czarnawska M., *Jak się bronić przed indoktrynacją,* Warszawa, 1997.
30. Czerminski A., Czapiewski M., *Organizacja procesów decyzyjnych,* Gdańsk, Uniwersytet Gdański, 1995.
31. Denzin N. K., Lincoln Y., *Handbook of Qualitative Research,* Thousand Oaks, SAGE Publications, 1994.
32. Dobek-Ostrowska B., J. Fras, B. Ociepka, *Teoria i praktyka propagandy,* Wrocław, Wydawnictwo Uniwersytetu Wrocławskiego, 1997.
33. Dockery J. T., *The Use of Fuzzy Sets in the Analysis of Military Command*, [w:] *Decision Information*, red. E. Ch. P. Tsokos, R. M. Thrall, New York, Academic Press, 1990.
34. Donald R., White J., *A Handbook Series on Elektromagnetic Interference and Copmpatibility,* Maryland, Germantown, 1973.
35. Douhet G., *Panowanie w powietrzu*, Warszawa, MON, 1965.
36. Drucker P., *Menedżer skuteczny,* Kraków, Wydawnictwo Czytelnik, 1994.
37. Dudek Z. T., Sosnowski J., *Organizacja przesyłania informacji w systemach cyfrowych,* Warszawa, PWN, 1981.
38. DudzińskiJ., Knap R., *Handel zagraniczny*, Szczecin, Zachodniopomorska Szkoła Businessu, 1996.
39. Erikson E. H., *Identity and Crisis,* New York, Norton, 1968.
40. Findeisen W., *Analiza systemowa - podstawy metodologiczne,* Warszawa, PWN, 1985.
41. Flakiewicz W., *Podejmowanie decyzji kierowniczych*, Warszawa,1983.
42. Fogleman R., *Information Operations: The Fifth Dimension of Warfare,* Washington, National Defence University Press, 1995.

43. Franta H., Salonia G., *Comunicazione interpersonale,* Roma, LAS, 1981.
44. Fukuyama F., *The Great Disruption,* New York, Free Press, 1999.
45. Ghyczy T., Oetinger B., Bassford C., *Clausewitz o strategii*, Warszawa, PWE, 2002.
46. Globan-Klas T., *Media i komunikowanie masowe. Teorie i analizy działania prasy, radia, telewizji i Internetu,* Warszawa, PWN, 1999.
47. Głuszkow W., *Wstęp do cybernetyki,* Kijów, Naukowa Dumka, 1963.
48. Green G. H., Cotter C., *Nie pozwól sobą manipulować,* Warszawa, 1997.
49. Greenfield K. R., *Command Decisions,* Washington, Center of Military History, 1990.
50. Greniewski H., *Cybernetyka niematematyczna,* Warszawa, PWN, 1982.
51. Greniewski H., *Sprawy wszystkie i jeszcze inne,* Warszawa, KiW, 1970.
52. Hanson V. D., *The Soul of Battle,* New York, Free Press 1999.
53. Hanson V. D., *An Autumn of War,* Anchor, Vintage, 2002.
54. Harrington, H. J. Esseling, E.K. Van Nimwegen, H. *Business Process Improvement Workbook. Documentation, Analysis, Design and Management of Business Process Improvement.* McGraw-Hill, 1997.
55. Huntington S., *The Clash of Civilizations and the remaking of World order,* New York, Simon and Schuster, 1996.
56. Heminger A., *Information Engineering,* Patterson, School of Logistics and Acquisition Management, Air Force Institute of Technology, 1997.
57. Hercman K., *Teoria informacji na użytek szkoły,* Olsztyn, Wydawnictwa Szkolne i Pedagogiczne, 1977.
58. Honey, *Jak radzić sobie lepiej z ludźmi,* Warszawa, 1997.
59. Hutcherson N. B., *Command and Control Warfare: Putting Another Tool in the War-Fighter's Data Base,* Maxwell, Air University Press, 1994.
60. Jacyniak A., Płużek Z., *Świat ludzkich kryzysów,* Kraków, WAM, 1996.
61. Jouvenel B., *Apres la Defaite,* Paryż, 1940.
62. Kagan D., *On the Origins of War and the Preservation of Peace*, New York, 1995.
63. Kaczmarek W., *Kierunki rozwoju sztuki operacyjnej w aspekcie teorii prognozy,* Warszawa, AON, 2000.
64. Kaczmarek W., *Prognoza możliwych zagrożeń o charakterze militarnym i niemilitarnym determinujących potrzeby w zakresie wojsk OT*, Warszawa, AON, 2002.
65. Kaczmarek W., Ścibiorek Z., *Przyszła wojna - jaka?*, Warszawa, BUWiK, 1995.

66. Kaczmarek W., Ścibiorek Z., *Przyszłe pole walki,* Warszawa, AON, 1995.
67. Kamiński S., *Nauka i metoda. Pojęcie nauki i klasyfikacja nauk,* Lublin, TN KUL, 1992.
68. Kanarski L., Gawliczek P., *Przywództwo w armiach NATO,* Warszawa, AON, 2002.
69. Kaplan, R. S. Norton, D. P. *Strategiczna karta wyników.* PWN, Warszawa 2001
70. Kępka Z., *Propaganda i agitacja na polu walki,* Warszawa, 1973.
71. Kałużyński S., *Imperium mongolskie,* Warszawa, 1970.
72. Kennedy P., *U progu XXI wieku (Preparing for the 21st Century),* tłum. P. Konczewski, Kielce, 1994.
73. Keramas J. G, *Workforce Training for Global Copmpetitivenes,* AFCEA Symposium and Exposition, Stockholm, 1995.
74. Keuren E. V., Knighten J., *Implications of the High – Power Microwave Weapon Threat in Electronic System Design,* IEEE Intern. Symp, Cherry Hill, 1991.
75. Kieżun W., *Podstawy organizacji i zarządzania,* Książka i Wiedza, Warszawa 1977
76. Killen H. B., *Transmisja cyfrowa w systemach światłowodowych i satelitarnych,* Warszawa, KiŁ, 1992.
77. Kirschner., *Manipulować - ale jak ?,* Warszawa, 1994.
78. Klein G. S., *Psychoanalytic theory: An exploration of essentials,* New York, International Univ. Press, 1976.
79. Klir G. J., *Ogólna Teoria Systemów,* Warszawa, PWN, 1972.
80. Knetki J., *Operacje połączone,* Warszawa, AON, 1997.
81. Kobyliński W., *Podstawy organizacji i kierowania w oświacie,* Radom, MCNEMT 1994.
82. Konieczny J., *Inżynieria Systemów Działania,* Warszawa, WNT, 1983.
83. Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych,* Warszawa, Wiedza Powszechna, 1980.
84. Kopp C. A., *Doctrine for the Use of Electromagnetic Pulse Bombs,* Fairbairn, Air Power Studies Centre, 1993.
85. Kosieradzka A., Lis S., *Produktywność. Metody analizy, oceny i tworzenia programów poprawy,* Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2000.
86. Kotarbiński T., *Elementy teorii poznania, logiki formalnej i metodologii nauk,* Ossolineum, 1961.
87. Kotarbiński T., *Prakseologia. Część 1,* Ossolineum, 1999.

88. Kotarbiński. T., *Traktat o dobrej robocie,* Wrocław ,1982.
89. Koziej St., *Teoria sztuki wojennej,* Warszawa, AON, 1993.
90. Kozielecki J., *Koncepcja transgresyjna człowieka*, Warszawa, PWN, 1987.
91. Kozielecki J., *Koncepcje psychologiczne człowieka,* Warszawa, Wydawnictwo „Żak", 1997.
92. Kozielecki J., *Psychologiczna teoria decyzji*, Warszawa, 1977.
93. Kriesel M. E., *Psychological Operations: A Strategic View, Essajs on Strategy,* Washington, National Defence University Press, 1985.
94. Krzyżanowski, L. *O podstawach kierowania inaczej*. Warszawa, PWN, 1999.
95. Krzyżanowski L., *Podstawy nauk o organizacji i zarządzaniu.* Warszawa, PWN, 1992.
96. Kuc B., *Zarządzanie doskonałe*, Warszawa, Wyd. PTM, 2000.
97. Kuratowski K., Mostowski A., *Teoria mnogości,* Warszawa, PWN, 1978.
98. Kurnal J., *Zarys teorii organizacji i zarządzania*, Warszawa, 1970.
99. Kwećka R., Nowak A., *Budowa modelu systemu rozpoznania wojskowego w aspekcie organizacyjnym i informacyjnym,* Warszawa, AON, 1994.
100. Landauer T. K., *The Trouble With Computers: Usefulness, Usability, and Productivity,* Cambridge, MIT Press, 1995.
101. Libicki M., *What Is Information Warfare?,* Washington, ACIS Paper, 1995.
102. Link D. M., *Information Dominance,* Washington, 1995.
103. Ludendorff E., *Wojna totalna,* Warszawa, 1959.
104. Lynch J. P., *The Global Correlation Engine (GCE): A Brief Description,* Washington,1997.
105. Maliszewski W., *Oddziaływanie psychologiczne w operacji obronnej,* Warszawa, AON, 1998.
106. Manganelli R. L., Klein M. M., *Reengineering*. Warszawa, PWE,1998.
107. Markiewicz L., *Ultradźwięki i infradźwięki,* Warszawa, PWN, 1979.
108. Maslow A.H., *Motivation and personality,* New York, Harper,1954.
109. Matwiejczuk R., *Efektywność – próba interpretacji*, Przegląd Organizacji 11/2000.
110. Mazur M., *Cybernetyka i charakter,* Warszawa, PIW, 1976.
111. Mazur M., *Jakościowa teoria informacji*, Warszawa, 1970.
112. Mazurek J., *Informacja – propaganda – opinia publiczna*, Warszawa, 1974.
113. Mazurek :J., *Informacja społeczna i propaganda,* Warszawa, 1979.
114. Mazurek J., *Z teorii propagandy socjalistycznej*, Warszawa,1974.

115. Mead G. H., *Mind, self and society,* Chicago, Univ. of Chicago Press, 1934.
116. Miles M. B., Huberman M. A., *Qualitative Data Analysis: An Expanded Sourcebook,* Thousand Oaks, SAGE Publications, 1994.
117. Miller J.A. Pniewski K. Polakowski M. *Zarządzanie kosztami działań.* WIG-Press, Warszawa 2000.
118. Mitiugow W., *Fizyczne podstawy teorii informacji,* Warszawa, PWN, 1980.
119. Morris M., *Air Force Material Command Science and Technology: Analysis of Information Needs and Capabilities,* Wright-Patterson, 1997.
120. Mossor S., *Sztuka wojenna w warunkach nowoczesnej wojny,* Warszawa, 1986.
121. Murphy E., Bender G. C., Schaefer L. J., Shepard M. M., Williamson Ch. W., *Information Operations: Wisdom Warfare For 2025,* Washington, 1996.
122. Myers M. D., *Qualitative Research in Information Systems, Qualitative Research Methods,* Washington, 1997.
123. Neri F., *Introduction to Electronic Defense Systems,* Artech House, 1991.
124. Nowacki G, *Działania psychologiczne w działaniach sojuszniczych,* Warszawa, AON, 2003.
125. Nowacki G., *Działania psychologiczne w ramach operacji informacyjnych wojsk lądowych,* Warszawa, AON, 2001.
126. Nowacki G., *Militaryzacja kosmosu,* Warszawa, AON, 2003.
127. Nowacki G., *Działania informacyjne,* Warszawa, AON, 2001.
128. Nowacki G., *Organizacja i prowadzenie działań psychologicznych w wybranych państwach,* Toruń, Adam Marszałek, 2004.
129. Nowacki G., *Rozpoznanie satelitarne USA i Federacji Rosyjskiej,* Warszawa, AON, 2002.
130. Nowacki G., *Walka informacyjna – próba kategoryzacji,* Warszawa, AON, 1999.
131. Nowacki G., *Współczesne poglądy na prowadzenie walki informacyjnej,* Warszawa, AON, 2001.
132. Obrusiewicz M. A., *Wielonarodowe połączone siły zadaniowe CJTF,* Warszawa, AON, 2002.
133. Ochman J., *Integracja w systemach informatycznych zarządzania,* Warszawa, PWE, 1992.
134. Parsons T., *The position of identity in the general theory of action,* [w:] *The self in social interaction,* red. Gordon C, Gergen K., New York ,Wiley, 1968.
135. Patton G., *Wojna jak ją poznałem,* Waszyngton, 1947.

136. Pierce J. R., *Symbole, sygnały i szumy,* Warszawa, PWN, 1967.
137. Picq A., *Studium o walce,* Warszawa, 1927.
138. Player, S. Lacerda, R. Arthur Andersen's Global Lessons in Activity-Based Management. John Wiley & Sons, New York 1999.
139. Podkowski A., *Działania psychologiczne, specjalne i niekonwencjonalne. Wybrane aspekty współzależności,* Warszawa, AON, 2002.
140. Podkowski A., *Obiektywne i subiektywne uwarunkowania skuteczności oddziaływania psychologicznego w walce*, Warszawa, AON, 2001.
141. Ponsonby A., *Fałszerstwa czasu wojny,* Londyn, 1923.
142. Popper K. R., *Logika odkrycia naukowego,* Warszawa, PWN, 1977.
143. Pyka I., Pyka J, Sobczak – Woźniak B., *Elementy ekonomii i ekonomiki przedsiębiorstwa w gospodarce rynkowej*, Stowarzyszenie Księgowych w Polsce, Warszawa 1997.
144. Rappaport A., *General Systems Theory*, Cambridge, Abacus Press, 1986.
145. Reykowski J., *Metodologiczne problemy psychologii współczesnej*, Warszawa, PWN, 1964.
146. Reykowski J., *Motywacja, postawy prospołeczne a osobowość,* Warszawa, PWN, 1980.
147. Reykowski J., *Osobowość a społeczne zachowanie się ludzi,* Warszawa, 1976.
148. Robbins S., DeCenzo D., *Podstawy zarządzania*, Warszawa, PWE, 2002.
149. Rotkiewicz W., *Kompatybilność elektromagnetyczna w radiotechnice,* Warszawa, Wyd. KiŁ, 1978.
150. Sage A. P., *Systems Management – for information technology and software engineering,* New York, John Wiley & Sons, 1995.
151. Shannon C. E., Warren W., *The Mathematical Theory of Communication,* Urbana, The University of Illinois Press, 1949.
152. Schwartau Winn., *Information Warfare – Cyberterrorism: Protecting Your Personal Security in the Electronic Age,* Emeryville, Publishers Group West, 1993.
153. Schechtman G. M., *Manipulating The OODA Loop: The Overlooked Role Of Information Resource Management In Information Warfare,* Wright-Patterson, School of Logistics and Acquisition Management, Air Force Institute of Technology, 1996.
154. Seidler J., *Podstawy, modele źródeł i wstępne przetwarzanie informacji,* Warszawa, WNT, 1983r.

155. Seidler. J., *Nauka o informacji,* Warszawa, WNT, 1983.
156. Sienkiewicz P., *Podstawy teorii systemów,* Warszawa, AON, 1993.
157. Sienkiewicz P., *Systemy kierowania*, Warszawa, Wiedza Powszechna, 1989.
158. Sienkiewicz P., *Zastosowanie techniki komputerowej w dowodzeniu wojskami: opracowanie modeli matematycznych; nowe tendencje w modelowaniu walki,* Warszawa, AON, 1994.
159. Sipkin R., *Race to the Swift,*. London, 1985.
160. Sink S., *Productivity Management Planning, Measurement and Evaluation, Control and Improvement*, New York, John Willey and Sons, 1985.
161. Skinner B.F:, *Science and human behavior*, New York, Mac-Millan, 1953.
162. Skrzypek E., *Jakość i efektywność*, Wydawnictwo Uniwersytetu Marii Curie – Skłodowskiej, Lublin 2000.
163. Smołalski A., *Elementy teorii organizacji dla pedagogów*, Wrocław, Wyd. Uniwersytetu Wrocławskiego, 1979.
164. Słupecki J., Hałkowska K., Piróg-Rzepecka K., *Logika i teoria mnogości*, Warszawa, PWN, 1994,
165. Smyksy B., *Psychologiczna charakterystyka walki zbrojnej*, Warszawa, 1987.
166. Sobolewski K., *O pojęciu skuteczności i pojęciach związanych*, Wydawnictwo Politechniki Koszalińskiej, Koszalin 1998.
167. Sokołowski A., *Ochrona informacji komputerowych*, Warszawa, MON, 1987.
168. Stoner J., Freeman R., Gilbert D., *Kierowanie*, Warszawa, PWE, 2001.
169. Strasburger D., *Zasady sztuki wojennej (od XI wieku do 1871 roku)*, Warszawa, Bellona, 1996.
170. Sun Tzu, *Sztuka wojny*, Warszawa, Wyd. Przedświt, 1994.
171. Szaniawski K., *Pragmatyczna wartość informacji,* [w:] *Problemy psychologii matematycznej,* red. J. Kozielecki, Warszawa, PWN, 1971.
172. Szulc B., *Walka zbrojna w kontekście ogólnej teorii walki i teorii konfliktów*", Warszawa, AON, 1996.
173. Szymański J. M., *Życie Systemów,* Warszawa, Wiedza Powszechna, 1991.
174. Ścibiorek Z., *Wpływ nowych środków walki na działania bojowe wojsk lądowych,* Warszawa, AON, 1993.
175. Świątnicki W. Z., *Bronie inteligentne,* Warszawa, 1992.
176. Terelak J., *Podstawy psychologii,* Warszawa, 1994.
177. Thomson O., *Historia Propagandy,* Warszawa, KiW, 2001.

178. Tiemnikow F. E., Afonin W. A., Dmitrijew W. I., *Podstawy techniki informacyjnej,* Warszawa, WNT, 1974.
179. Toffler A. i H., *Budowa Nowej Cywilizacji – Polityka Trzeciej Fali,* Poznań, Wyd. Zysk i Ska, 1996.
180. Toffler A. i H., *War and Anti War: Survival at the Dawn of the Twenty-First Century,* Boston, Little Brown, 1993.
181. Trybała P., *Skuteczne kierowanie i organizowanie*, Rzeszów, FOSZE, 2001.
182. Twardowski K., *Wybór pism psychologicznych i pedagogicznych,* Warszawa, 1992.
183. Watson J. B., *Behawioryzm oraz psychologia jak ją widzi behawiorysta*, Warszawa, PWN, 1990.
184. Weinberg G. M., *Myślenie Systemowe*, Warszawa, PWN, 1980.
185. Wiatr M., *Działania operacyjne,* Warszawa, AON, 1995.
186. Wiatr M., *Między strategią a taktyką,* Toruń, Adam Marszałek, 1999.
187. Wiatr M., R. Kwećka., *Sztuka wojenna lat dziewięćdziesiątych,* Warszawa, AON, 1997.
188. Wiener N., *Cybernetics or Control and Communication in the Animal and the Machine,* New York, The Technology Press, John Wiley & Sons, 1948.
189. Witkowski T., *Psychomanipulacje,* Warszwa, 2000.
190. Wołkogonow D., *Wojna psychologiczna,* Warszawa, 1986.
191. Wrzosek M., *Przykłady dokumentów rozpoznawczych według poglądów wybranych państw NATO*, Warszawa, AON, 1997.
192. Wyss D., *Psychoanalytic Schools from the Beginning to the Present,* New York, Jason Aronson, 1973.
193. Wyszczelski L., *Historia myśli wojskowej,* Warszawa, Bellona, 2000.
194. Zieleniewski, J. *Organizacja i zarządzanie*. Warszawa, PWN 1974.
195. Zieleniewski J., *Organizacja zespołów ludzkich*, Warszawa, PWN,1972.
196. Zieliński J., *Podstawowe założenia dydaktyki sztuki operacyjnej,* Warszawa, AON, 2002.
197. Zieliński J., *Podstawowe założenia operacji połączonych*, Warszawa, AON, 2000.
198. Zieliński J., *Rozpoznanie i ocena nieprzyjaciela w działaniach bojowych,* Warszawa, AON, 1993.
199. Zieliński J., *Sztuka operacyjna w nowych uwarunkowaniach,* Warszawa, AON, 2000.
200. Zieliński J., *Zarys Teorii sztuki operacyjnej wojsk lądowych Rzeczypospolitej Polskiej,* Toruń, Adam Marszałek, 1998.

201. Ziembiński Z., *Logika praktyczna*, Warszawa, PWN, 1994.
202. Zimniewicz K., *Nauka o organizacji i zarządzaniu*, Warszawa, PWN, 1990.

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Akademii Obrony Narodowej
Nr ewid. 58058