AKADEMIA
OBRONY NARODOWEJ

AON 5295/2001

Ppłk dr inż. Gabriel NOWACKI

WSPÓŁCZESNE POGLĄDY NA PROWADZENIE WALKI INFORMACYJNEJ

WARSZAWA 2001

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH

KATEDRA ROZPOZNANIA WOJSKOWEGO I ARMII OBCYCH

AON 5295/2001

Ppłk dr inż. Gabriel Nowacki

WSPÓŁCZESNE POGLĄDY NA PROWADZENIE WALKI INFORMACYJNEJ

STUDIUM TEORETYCZNE

WARSZAWA **2001**

Powielenie i oprawa:
Akademia Obrony Narodowej – Wydział Wydawniczy
Zam. nr 275/2001

WPROWADZENIE

Współcześnie pojawiły się zupełnie nowe „środki" przemocy, których zastosowanie w czasie wojny - i nie tylko - okazuje się wysoce skuteczne z punktu widzenia osiągnięcia zwycięstwa nad przeciwnikiem. Środki te nazywane są często "nieśmiercionośnym" arsenałem broni. Ich przykładem mogą być paski folii z włókna węglowego, które rozproszone nad systemami energetycznymi powodują wyłączenie prądu bez niszczenia zakładów energetycznych, czy chociażby światła stroboskopowe przyprawiające o mdłości niesforne tłumy. W epoce informacji, w której na szeroką skalę wykorzystane są mikroprocesory, bardzo szybkie systemy odbioru i obróbki danych oraz skomplikowane czujniki, prowadzone są prace nad specjalnymi wirusami, które "umieszczone" w systemach broni potencjalnego przeciwnika, spowodują ich dezorganizację i nieefektywność. Urządzenia wytwarzające impuls elektromagnetyczny[1] (wielkości walizki) są już projektowane w Laboratorium Narodowym Stanów Zjednoczonych w Los Alamos. Planuje się także wykorzystanie specjalnego rodzaju mikrobów, które mogą zniszczyć układy elektroniczne i izolacyjne w komputerach. Infradźwięki o częstotliwości 16 Hz używane przeciwko sile żywej powodują wzbudzanie wibracji w organach wewnętrznych, powstanie nudności, dolegliwości sercowych i zaburzeń równowagi. Zaletą tych rodzajów broni jest przede wszystkim łatwość przenikania przez struktury materii. Promienniki równokierunkowe lub izotropowe występujące w formie amunicji artyleryjskiej lub lotniczej, wytwarzają promieniowanie elektromagnetyczne o własnościach zbliżonych do laserowego. Ich działanie polega na krótkotrwałej emisji promieniowania elektromagnetycznego w zakresie od podczerwieni do nadfioletu w celu porażenia czujników, dezorientowania pilotów, czy nawet oślepienia żołnierzy. Wzrost roli czynników nieśmiercionośnych na współczesnym polu walki jest trendem rozwojowym, świadczącym o nowych możliwościach, jakie otwierają się przed pozazbrojnymi formami walki w działaniach wojennych. Nie można oczywiście twierdzić, że maleje znaczenie walki zbrojnej w wojnie. Jednakże już dziś - tym bardziej w przyszłości, nie musi już ona być jedynym i decydującym o rezultacie wojny czynnikiem. Narastająca zależność potencjału obronnego od ekonomiki, techniki i ideologii (w sensie świadomości

[1] Impuls elektromagnetyczny - impuls fal radiowych o czasie trwania rzędu tysięcznych części sekundy. Charakteryzuje się bardzo dużą amplitudą zmian natężenia pola elektrycznego i magnetycznego. Powoduje on zaindukowanie się prądów i napięć w obwodach urządzeń elektronicznych, co jest przyczyną niszczenia niektórych elementów półprzewodnikowych na skutek przeciążeń. Zasadniczymi obiektami oddziaływania impulsu elektromagnetycznego są środki radioelektroniczne. Należy podkreślić, że im bardziej różni się zakres częstotliwości oddziałującego promieniowania od pasma częstotliwości roboczych urządzenia radioelektronicznego, tym mniejszy jest efekt skuteczności.

społecznej, społecznych przekonań i dążeń) doprowadziła do sytuacji, w której można już mówić o przemocy ekonomicznej, naukowo - technicznej i ideologicznej. Środki, metody i formy tej przemocy bardzo się wzbogaciły, szczególnie w ostatnich dziesięcioleciach. Coraz częściej w sferze pozamilitarnych form walki szukać się będzie możliwości obrony lub ataku, uzyskania równowagi lub przewagi i być może decydujących rozstrzygnięć. Taką możliwość daje walka informacyjna, która warunkuje osiąganie powodzenia w prowadzonych działaniach zbrojnych. Jej znaczenie dostrzegali i dostrzegają wszyscy teoretycy, począwszy od Sun Tzu[2] (VI w.p.n.e.), poprzez generałów epoki napoleońskiej, aż do współczesnych dowódców i historyków. Jednak tylko niektórzy z nich nazywali ją bezpośrednio w ten sposób: „walka informacyjna". Najczęściej , np. w stosunku do działań w podprzestrzeni zdobywania informacji, używano określeń: „poznaj siebie i poznaj wroga", „poznaj warunki terenu i pogody" (Sun Tzu w traktacie: Sztuka wojny). W stosunku do podprzestrzeni zakłócania informacyjnego: „oszukuj przeciwnika", „zastosuj fortel", zaś w stosunku do podprzestrzeni obrony informacyjnej: „bądź czujny", „zaskocz przeciwnika, będąc silny tam, gdzie on się tego nie spodziewa".

Zastosowanie technik walki informacyjnej nadaje nową jakość współczesnym działaniom zbrojnym. Doświadczenia ostatnich konfliktów, a przede wszystkim rozwój zastosowań techniki komputerowej skłaniają do traktowania organów walki informacyjnej jako odrębnego rodzaju wojsk, funkcjonującego pod jednolitym dowództwem i posiadającego odpowiednio wyspecjalizowane ośrodki szkoleniowe.

Wojsko mocno wkroczyło w epokę technologii informacyjnych. Dostęp do nich ma obecnie bardzo istotne znaczenie. „Informacja" jest niezbędnym czynnikiem warunkującym skuteczne funkcjonowanie wszystkich szczebli dowodzenia, choć dla każdego z nich odrębne są kryteria jej doboru i wymagania w zakresie szczegółowości. Szczebel strategiczny wymaga wiadomości określanych jako ogólne, większa szczegółowość potrzebna jest do planowania operacyjnego i taktycznego zaś największa precyzja do realizacji procesów wykonawczych. Każdy z tych szczebli dowodzenia chcąc zachować swoją żywotność nie może ograniczać się jedynie do działań w podprzestrzeni zdobywania informacji, ale także musi prowadzić obronę informacyjną i zakłócanie systemów informacyjnych przeciwnika.

Walka informacyjna, przybierając różne formy, realizowana była od najdawniejszych czasów. W różny sposób na przestrzeni wieków radzono sobie z problemami integralnie związanymi z prowadzeniem tej walki, problemami bliskimi nam i dziś, jak np. skracanie

---

[2] Sun Tzu w traktacie Sztuka wojny (str. 8) pisał: „Poznaj siebie i poznaj wroga, dopiero wtedy twoje zwycięstwo nie będzie zagrożone. Poznaj warunki terenu i pogody, wtedy twoje zwycięstwo będzie całkowite".

czasu obiegu informacji (terminowość), wiarygodność, itp. Wyniki walki informacyjnej w decydujący sposób wpływały na rezultaty bezpośrednich zmagań na polach bitew, kiedy to zapadające w konfrontacji zbrojnej rozstrzygnięcia były w istocie jedynie konsekwencją przegranej, bądź wygranej walki w przestrzeni informacyjnej. Były realizacją tego co zostało już wcześniej wyreżyserowane przez stronę, która z tej poprzedzającej bezpośrednią walkę konfrontacji wyszła zwycięsko.

Nowoczesna technika, najnowsze systemy elektroniczne - nie stworzyły nowego wymiaru walki. Nadały mu jedynie dostrzegalną w ostrzejszych zarysach nową jakość.

Problem sprawnego funkcjonowania systemów informacyjnych i prowadzenia walki informacyjnej, we wszystkich jej wymiarach, wciąż czeka na odpowiadające wzrastającym potrzebom rozwiązania. Jej wartość praktyczna unaoczniła się szczególnie w czasie konfliktu w rejonie Zatoki Perskiej.

Aktualnie na temat walki informacyjnej mówi się coraz częściej i więcej nie tylko na Zachodzie, ale i na Wschodzie[3]. Według opinii admirała Wiliama Owens'a, byłego przewodniczącego Kolegium Szefów Sztabów USA, Pentagon ma szeroko zakrojone plany zrewolucjonizowania pola bitwy za pomocą techniki informacyjnej, tak jak zrewolucjonizowały je czołgi podczas pierwszej i bomba atomowa podczas drugiej wojny światowej. W 1993r. w waszyngtońskim Uniwersytecie Obrony Narodowej (National Defense University) otwarta została *Szkoła Strategii i Walki Informacyjnej* (School of Information Warfare and Strategy). W ten sposób najwyższa uczelnia wojskowa Stanów Zjednoczonych (Uniwersytet Obrony Narodowej - „uczelnia generałów") dołączyła strukturalnie i programowo do grona licznych już komórek organizacyjnych Pentagonu i innych sztabów, które zajmują się problematyką „walki informacyjnej".

Mimo wzrastającego zainteresowania tematyką walki informacyjnej na świecie oraz pojawiających się coraz liczniejszych publikacji nawiązujących do tej problematyki, wciąż nie jest ona dostatecznie dostrzegana, naświetlana i interpretowana w naszych siłach zbrojnych, a także w środowisku cywilnym. Uwzględniając *ex professo* wyżej wymienione powody oraz wzrost zainteresowania tym tematem, można stwierdzić, że jest to problem:

---

[3] *Poglądy rosyjskich specjalistów na przyszłą wojnę - "Military Review" nr 7/94.* Przyszły teatr wojny charakteryzować będzie duża dynamika i intensywność powietrzno-lądowych operacji prowadzonych na dużych przestrzeniach. Działania taktyczne będą znacznie skuteczniejsze i będą prowadzone w sposób nielinearny, a linia teatru zniknie. Łączność będzie sporadyczna, a dowodzenie trudne. Walka informacyjna będzie najważniejszym elementem.

— przyszłościowy, ale ulokowany w przestrzeni jeszcze niewystarczająco zdefiniowanej — zarówno pod względem syntaktycznym, semantycznym, pragmatycznym, jak i strukturalnym;

— mający genezę, która jest lokowana nie zawsze we właściwym przedziale czasowym;

— charakteryzujący się bardzo konkretnymi związkami z walką zbrojną, które do tej pory nie zostały wyraźnie sprecyzowane.

Niedawne konflikty zbrojne (szczególnie wojna w rejonie Zatoki Perskiej) dowiodły, że o odniesionym sukcesie decyduje w głównej mierze walka informacyjna. Poprzedza ona każde starcie zbrojne i trwa nieprzerwanie nawet po jego zakończeniu. Z analizy zgromadzonych faktów można wyciągnąć hipotetyczny wniosek, że *nie jest możliwe odniesienie zwycięstwa w walce zbrojnej bez wcześniejszego sukcesu w walce informacyjnej.*

Na podstawie literatury (głównie zagranicznej) należy sądzić, że w przyszłych konfliktach zbrojnych dążenie do uzyskania przewagi informacyjnej, a tym samym uzyskania zaskoczenia przeciwnika, może stać się regułą postępowania.

Wynika więc z tego, że temat opracowania jest w dalszym ciągu jak najbardziej aktualny. Pozwolił na dokonanie wielu rozstrzygnięć, które do dziś są tematem licznych dyskusji i sporów. Należy mieć jednak świadomość, że obszar do prowadzenia badań naukowych w zakresie tej problematyki jest ogromny i przekracza możliwości realizacyjne jednego wykonawcy.

1. POLSKIE POGLĄDY NA PROWADZENIE WALKI INFORMACYJNEJ

1.1. Pojęcie walki informacyjnej

W porozumiewaniu się, szczególnie językami profesjonalnymi, często są używane pojęcia dwuczłonowe, składające się z wyrazu podstawowego i z wyrazu dopełniającego. Łączność ich stosowania ukierunkowywana jest zawsze na większą konkretyzację desygnatów wyrazów podstawowych.

W strukturze pojęcia „walka informacyjna" zasadniczym determinantem rzutującym na całokształt przedmiotu myślowego, jest wyraz „walka". Wyrazem dopełniającym jest natomiast jej rodzaj (charakter) określony mianem „informacyjna".

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

Ad vocem pojęcia „walka" problem został już rozwiązany. Według prof. Tadeusza Kotarbińskiego interpretowana jest jako: „wszelkie działania przynajmniej dwupodmiotowe (przy założeniu, że zespół może być podmiotem), gdzie jeden przynajmniej z podmiotów przeszkadza drugiemu. W poszczególnym, 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. Dlatego też przypadek wzajemnego obiektywnego i świadomego zarazem przeszkadzania, uważany jest za najciekawszy, iż wtedy obie strony zmuszają się wzajemnie w sposób osobliwie intensywny do pokonywania trudności, a więc pośrednio — do usprawniania techniki działań. Tego typu walka występuje w sporach politycznych, konkurencji handlowej i przemysłowej oraz w grze szachowej"[4].

Walka — zarówno w ujęciu T. Kotarbińskiego, jak i z punktu widzenia cybernetyki — utożsamiana jest z kooperacją negatywną wzajemną. Są to wszelkie działania zbiorowe, w których biorą udział przynajmniej dwa układy, przy czym jeden z nich przeszkadza drugiemu. Układy te dążą do celów niezgodnych, o czym wzajemnie wiedzą, planując zaś swoje postępowanie uwzględniają przeszkadzające działanie strony przeciwnej. Partnera uczestniczącego w walce nazywa się przeciwnikiem. Między układami „A" i „B" zachodzi kooperacja negatywna wzajemna ze względu na określony cel dla „A" i na określone działanie „B" wtedy i tylko wtedy, gdy „B" swym działaniem przeszkadza „A" osiągnąć cel.

---

[4]T. Kotarbiński: *Traktat o dobrej robocie,* Wrocław 1982, s.221.

Przy kooperacji negatywnej wzajemnej nie tylko „B" przeszkadza „A", lecz i odwrotnie"[5]. W rozumieniu szczegółowym „walka" łączona jest zawsze z desygnatem określającym jej rodzaj, to znaczy przestrzeń, w której ulokowany jest cel kooperacji negatywnej. Mówi się wtedy o walce:

— ekonomicznej — jeśli jej cel ulokowany jest w przestrzeni ekonomicznej;

— politycznej — jeśli jej cel ulokowany jest w przestrzeni politycznej;

— ideologicznej — jeśli jej cel ulokowany jest w przestrzeni ideologicznej;

— sportowej — jeśli jej cel ulokowany jest w przestrzeni sportowej, itp.

Rozumiejąc walkę jako szczególny rodzaj działania, dalsze jej konkretyzowanie wynikać będzie z zawężania:

— przestrzeni lokalizacji celu;

— narzędzi użytych do jej prowadzenia;

— i sposobów wykorzystywania tych narzędzi w konkretnych działaniach.

Będzie się wówczas mówić o walce ekonomicznej o strefę wpływów lub walce politycznej o tę strefę. Konkretyzując dalej, może to być walka o rynki zbytu, gdzie narzędziami będą konkretne surowce, czy też produkty, a sposobami prowadzenia walki — działania ukierunkowane na uzyskiwanie konkurencyjnej atrakcyjności jakościowej czy też nabywczej składanych ofert.

Konstatując, można już w tym miejscu stwierdzić(przez analogię), że tę samą regułę konkretyzacji należy stosować do wszystkich rodzajów walki, a tym samym do walki informacyjnej. Przed tym jednak należy jednoznacznie:

— zdefiniować samo pojęcie „informacja";

— ustalić jej cechy charakterystyczne;

— ustalić możliwe do wykonywania operacje „na informacji" (z informacją).

1.2. Interpretacja pojęcia informacja

Zgodnie z *communis opinio* pojęcie „informacja" oznacza wiadomość, wieść, nowinę, rzecz zakomunikowaną; miarę wiedzy o jakimś zdarzeniu[6]. „Informacja" jest jednym z podstawowych pojęć w naukach teoretycznych i stosowanych. Trudno wskazać taki obszar zjawisk przyrodniczych lub taką gałąź techniki, w której nie mielibyśmy do czynienia

---

[5] *Mały słownik cybernetyczny,* op. cit., s.195.

[6] Kopaliński: *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Wiedza Powszechna, Warszawa 1980, s.429.

z przenoszeniem i przetwarzaniem danych w procesach fizycznych. „Informacja" to obiekt, który w postaci zakodowanej może być:

— przechowywany na nośniku danych (taśma magnetyczna, pamięć rdzeniowa komputera, dysk magnetyczny, taśma perforowana, kartka papieru itp.);

— przesyłany na określonym nośniku (np. głosem, falą elektromagnetyczną, prądem elektrycznym);

— przetwarzany i użyty do sterowania (np. komputerem steruje program będący zakodowaną informacją).[7]

Stanisław Koziej określa „informację" jako niematerialny czynnik zespalający pozostałe elementarne czynniki walki zbrojnej (ruch, rażenie) w zharmonizowaną całość starcia zbrojnego.[8]

W cybernetyce „informacja" stanowi jedno z podstawowych pojęć, którego desygnat jest nie w pełni definiowalny z uwagi na jego pierwotny i elementarny charakter[9]. W opisie procesów łączności i sterowania pojęcie 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 pojęcia informacja uważa się powszechnie za niezadowalające, a co najwyżej za ukazujące tylko niektóre aspekty informacji — *ad exemplum*:

- ✓ N. Wiener określa informację jako „nazwę treści zaczerpniętej ze świata zewnętrznego, w miarę jak się do niego dostosowujemy i jak przystosowujemy doń swoje zmysły. Proces otrzymywania i wykorzystywania informacji jest procesem naszego dostosowywania się do różnych ewentualności środowiska zewnętrznego oraz naszego czynnego życia w tym środowisku". „[...] Informacja jest informacją, a nie masą ani energią";
- ✓ N. Couffignal pisze, że „w cybernetyce nazywa się informacją wszelkie działanie fizyczne, któremu towarzyszy działanie psychiczne".
- ✓ Według W. Głuszkowa, informacja to „wszelkie wiadomości o procesach i stanach dowolnej natury, które mogą być odbierane przez organy zmysłowe człowieka".
- ✓ Według H. Greniewskiego, informacja to „stany wyróżnione wejść i wyjść układu".
- ✓ Według C. L. Shannona, „informacją jest to wszystko, co nie jest ani energią, ani masą, czyli jest zasilaniem — jest to każde rozpoznanie stanu układu, odróżnialnego od innego stanu tego układu".

---

[7] *Encyklopedia powszechna*, t. 2, op. cit., s.281.
[8] St. Koziej: Czynniki walki zbrojnej. W: *„Zeszyty Naukowe"* 4/93, AON, s.57 - 62.
[9] *Mały słownik cybernetyczny*, op. cit., s.155.

Z treści przytoczonych definicji wynika, że „informacją" jest nie tylko wiadomość, znak, zezwolenie, nakaz lub zakaz, ale — w najogólniejszym sensie — rozróżnialny przez odbiorcę stan układu. W takiej interpretacji „informacją" nie jest na przykład promieniowanie wysyłane przez określone źródło, jest zaś nią rozpoznanie stanu tego promieniowania, czyli stwierdzenie, czy ono występuje, czy nie występuje, czy ma taką a taką długość fali, lub czy składa się z takiego a takiego rodzaju emitowanych cząsteczek. Promieniowanie to może być również nośnikiem informacji o stanie źródła promieniowania, na przykład o realizowaniu programu radiowego przez rozgłośnię czy o procesach przebiegających we wnętrzu gwiazdy.

Źródłem nieporozumień i rozbieżności dotyczących interpretacji pojęcia „informacja" bywa najczęściej fakt, iż jest ono używane w cybernetyce w dwóch, nieco odmiennych znaczeniach — jako odbicie przez odbiorcę[10] stanów wyróżnionych układu będącego nadawcą[11] oraz jako miara zorganizowania układu.

W znaczeniu pierwszym mówi się o „informacji" jedynie w odniesieniu do układu, na który „informacja" działa przez wejścia zewnętrzne oraz wejścia wewnętrzne, czyli jest przez ten układ odbierana. W tym rozumieniu „informacja" jest interpretowana jako odbicie obiektywnych stanów samego układu informacyjnego oraz pewnych wyróżnionych stanów jego otoczenia. W tym znaczeniu ma ona charakter relatywny i stąd bywa czasem nazywana informacją względną.

W znaczeniu drugim „informacja" związana jest z interpretacją pojęcia entropia.

Podsumowując należy stwierdzić, że w cybernetyce pojęcie „informacji" nie zostało określone w sposób zadowalający. Wprawdzie N. Wiener wyraźnie wskazał, że nie należy utożsamiać informacji ani z masą, ani z energią, nie określił jednak dokładnie, czym jest informacja.

Twórca teorii informacji, C. E. Shannon, zdawał sobie sprawę, że jego aksjomatyka obejmuje tylko jeden, mianowicie ilościowy aspekt „informacji" i dlatego też zupełnie świadomie nazwał swoją teorię „matematyczną". Przedmiotem analizy Shannona był układ przesyłania informacji (rys. 1.2.1). Składał się on z pięciu elementów:

— źródła informacji;

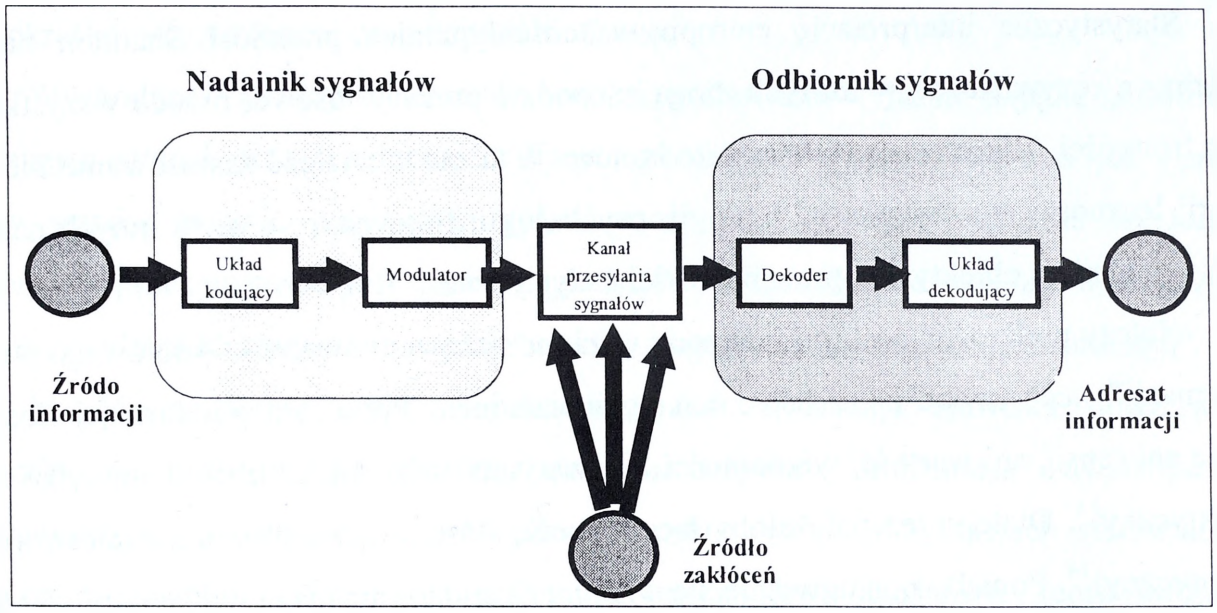
— nadajnika sygnałów, który zwykle zmienia kształt komunikatu lub koduje go;

---

[10]Odbiorca informacji to każdy obiekt rozważany wyłącznie jako układ informacyjny (człowiek, inna istota żywa jak i określone urządzenie techniczne. *Mały słownik cybernetyczny*, op. cit., s. 285.

[11]Nadawca informacji to każdy obiekt rozważany wyłącznie jako układ informujący, gdy mówi się o emitowanych informacjach, ich przesyłaniu i zamierzonym odbiorze. *Mały słownik cybernetyczny*, op. cit., s. 270.

— kanału przesyłania sygnałów, w którym komunikat jest przekazywany i który może wprowadzić szum;



Rys. 1.2.1. Model przesyłania wiadomości analizowany przez C.E. Shannona[12]

— odbiornika, w którym odbywa się odwrotne przekształcenie komunikatu adresata lub odbiorcy sygnałów;

— adresata informacji.

Według Shannona „informację" można określić miarą takiej ilości nieokreśloności, jaka znika po odebraniu komunikatu. Znaczenia „informacji" zawartej w komunikacie nie bierze się pod uwagę. Jednostką miary „informacji" jest bit. Jeden bit „informacji" — to taka jej ilość, jaka jest niezbędna do dokonania wyboru między dwiema jednakowo prawdopodobnymi, wzajemnie wykluczającymi się możliwościami. Im większy jest stopień nieokreśloności jednakowo prawdopodobnych stanów systemu, tym więcej potrzeba „informacji", by sprowadzić go do określoności. Jeżeli np. wiadomo, że oczekiwany gość ma przylecieć jednym z ośmiu lotów odbywających się z określonego miejsca odlotu do miejsca przeznaczenia, to oczywiście liczba jednakowo prawdopodobnych stanów systemu wynosi 8. Liczba możliwych stanów („tak" lub „nie") rozwiązywanych przez postawienie kolejnego pytania — 2, minimalna liczba pytań, którymi można określić stan systemu — 3 (to znaczy, że trzeba postawić trzy odpowiednio sformułowane pytania, z których każde rozwiązuje jedną alternatywę, aby otrzymać określoną informację o samolocie, którym przylatuje oczekiwany gość). W tym wypadku zatem do określenia systemu potrzebne są trzy bity „informacji". W czasie badań (np. w trakcie przeprowadzania doświadczeń) określane obiekty mają różne prawdopodobieństwa. Dlatego też zadanie polega na optymalnym wyborze najkrótszej drogi

[12] Opracowano na podstawie *„The Mathematical Theory of Communication"* The University of Illinois Press, Urbana 1949. C. E. Shannon.

prowadzącej do znalezienia pożądanej odpowiedzi na postawione pytanie metodą przyjmowania stanów systemu o największym prawdopodobieństwie.

Statystyczną interpretację entropii w termodynamice przeniósł Shannon na inne dziedziny rzeczywistości, w których mogą zachodzić procesy losowe, przede wszystkim na teorię łączności. Wkrótce okazało się, że koncepcja ta może znaleźć zastosowanie nie tylko w teorii łączności, ale również w biologii, psychologii, lingwistyce i wielu innych naukach, w których istnieją obiektywne prawidłowości statystyczne.

Należy podkreślić zasługi Shannona w zapoczątkowaniu technik ilościowego pomiaru „informacji", lecz trzeba pamiętać o ich ograniczeniach. Procedura pomiaru jej ilości nie ujmuje ani sensu, ani wartości wiadomości, ani wariancji zdarzeń. Obejmuje ona tylko aspekt syntaktyczny[13]. Dlatego też należałoby łączyć teorię ilościową z teorią wartościową (aspekt semantyczny)[14]. Ponadto posługiwanie się wzorem Shannona wymaga dokładnego określenia zbioru zdarzeń badanego zjawiska oraz wyznaczenia prawdopodobieństwa zajścia każdego z tych zdarzeń. Wymagania te nie zawsze mogą być spełnione, co również ogranicza możliwość stosowania tej teorii. Nic więc dziwnego, że z powodu tych ograniczeń niektórzy autorzy odnoszą się sceptycznie do propozycji Shannona.

W dyskusjach nad sposobem rozumienia „informacji" celowe jest rozróżnienie pomiędzy aspektem syntaktycznym, semantycznym i pragmatycznym[15].

Próbę rozwinięcia aspektu semantycznego podjął M. Mazur[16], w tzw. jakościowej teorii informacji. Przeprowadził on typologię procesów informowania, w której uwzględnił kryteria semantyczne („informowanie" oraz „dezinformowanie"). Stwierdza on, że „[...] chociaż istnieje już teoria informacji nie można się z niej dowiedzieć ani co to jest „informacja", ani nawet jaka jest ilość „informacji", w zwykłych najczęściej w praktyce spotykanych zdaniach". Wprawdzie rozpatruje się ilościową stronę „informacji", jednakże niedostatecznie wyjaśniona pozostaje jej strona treściowa. W publikacjach *in status quo* przede wszystkim i prawie wyłącznie rozpatrywano „informację" w aspekcie jej przekazywania w łączności, systemie komunikacji.

---

[13]Przez aspekt syntaktyczny informacji należy rozumieć relacje pomiędzy sygnałami niosącymi wiadomość, w której zawarta jest informacja, oraz pomiędzy sygnałami a kanałem komunikacyjnym.
[14]Aspekt semantyczny obejmuje relacje pomiędzy sygnałem a niesioną przez niego wiadomością.
[15]Aspekt pragmatyczny informacji dotyczy z kolei relacji pomiędzy niesioną przez sygnał wiadomością a jej nadawcą lub odbiorcą.
[16]M. Mazur M: *„Jakościowa teoria informacji"*, Warszawa 1970, s. 47.

Z tego powodu zwracano uwagę na zagadnienia relacji między źródłem — nadajnikiem i odbiornikiem informacji oraz na zagadnienia kwantyfikowanego jej ujęcia: ilość, określoność, złożoność prawdopodobieństwo.

Wychodząc z analizy systemów łączności, próbowano wyjaśnić pojęcie „informacji", wyróżniając sygnał oraz wiadomość. W tym kontekście sygnał określano jako przejaw zmiany stanów materii, przy czym sygnał może, ale nie musi zawierać wiadomości. Wiadomość przekazywana jest przez sygnały. W zależności od wiedzy lub niewiedzy odbiorcy wiadomości stają się mniej lub bardziej zrozumiałe i okazują się „informacją".

M. Mazur podjął próbę wyjaśnienia nader złożonego zjawiska przez analizę elementów układu sterowania. Wszystko co bywa nazywane „informacją" zawsze powstaje w sytuacjach, w których dąży się do jakiegoś celu, a więc w sytuacjach sterowania, co prowadzi do bardziej trafnego rozwiązania w postaci tzw. jakościowej teorii informacji. Rozważania nad uogólnionym torem sterowniczym ze źródłem i odbiornikiem oddziaływania prowadzą do definicji komunikatu jako stanu fizycznego, różniącego się w określony sposób od innego stanu fizycznego w torze sterowniczym. Warto tutaj zwrócić uwagę na analogię lub zbieżność definicji komunikatu i przytoczonego poprzednio sygnału. M. Mazur przyjmuje termin „informacja" dla oznaczenia „transformacji jednego komunikatu asocjacji informacyjnej w drugi komunikat tej asocjacji", co odbiega od potocznego i powszechnego rozumienia tego terminu.

Z przeprowadzonej analizy wynika, że w semantycznym ujęciu zakłada się celowy charakter „informacji" do wykorzystania w określonym układzie nadawcy (nadajnika) i odbiorcy (odbiornika). Aby treść „informacji" była zrozumiała odbiorca musi dysponować nagromadzonym zasobem — zapisem wiedzy w danej dziedzinie w postaci np. słownika, encyklopedii, zbioru modeli i symboli. Zasób taki często nazywany jest umownie tezaurusem[17]*. Treść — sens „informacji" ma więc charakter względny, odnieść ją można tylko do określonego nadawcy i odbiorcy dysponujących odpowiednim tezaurusem. Nowa, istotna treść „informacyjna", przyjęta przez odbiorcę, uzupełnia dysponowany przez niego tezaurus i odpowiednio zmienia jego skład i strukturę. Jakościowa teoria informacji, tak samo jak i ilościowa teoria informacji pomija aspekt pragmatyczny.*

Jeśli jednak bada się proces informacyjny w takim układzie komunikacyjnym, w którym człowiek pełni funkcję układu odbiorczego, to należy uwzględnić także

[17]Tezaurus – słownik stosowany w systemach automatycznego porządkowania, magazynowania i wyszukiwania informacji, zawierający listę słów kluczowych, charakteryzujących treść dokumentów. *Leksykon techniczny*, op. cit., s. 559.

pragmatyczny aspekt „informacji". Jeżeli bowiem badacz interesujący się zachowaniem podmiotu jako układu odbiorczego nie weźmie pod uwagę relacji pragmatycznej: podmiot — wiadomość zakodowana w sygnale, nie będzie mógł ani zadowalająco opisać, ani wyjaśnić tego zachowania.

Niezależnie od efektywności prób definiowania tego pojęcia wydaje się, iż desygnat pojęcia „informacja" pozostaje zawsze w relacji do jakiejś sytuacji decyzyjnej. Np. „informacja" o sytuacji na polu walki jest związana z problemem decyzyjnym dowódcy wojskowego, a „informacja" o stanie organizmu dotyczy decyzji podejmowanej przez chirurga. Takie ścisłe przyporządkowanie „informacji" o stanie rzeczy — określonej decyzji jest łatwe do przeprowadzenia w takich warunkach, w których decydent na bieżąco uzyskuje dane ułatwiające mu podjęcie decyzji. Nasuwa się jednak pytanie: Czy nie można by podać przykładów, w których „informacja" nie pozostaje w żadnym związku z sytuacją decyzyjną? Jako przykłady takich sytuacji można wymienić: sytuację ucznia, kursanta, studenta itp., w której podmiot uzyskuje szereg wiadomości zawierających informację nie związaną z żadną sytuacją decyzyjną. *De facto* żadna z wymienionych osób nie znajduje się aktualnie w sytuacji decyzyjnej, lecz nikt chyba nie ma wątpliwości, że nauka szkolna, kurs czy studia przygotowują właśnie potencjalnych decydentów.

Powyższe fakty wskazują, że desygnat pojęcia „informacja" pozostaje zawsze w ścisłym związku z pewną aktualną bądź potencjalną sytuacją decyzyjną. Funkcją „informacji" jest więc zawsze zmniejszenie nieokreśloności sytuacji decyzyjnej.

Istnienie ścisłej relacji między czynnością informacyjną a sytuacją decyzyjną wskazuje jeszcze bardziej dobitnie na konieczność pragmatycznego ujęcia „informacji", ponieważ interpretacja taka wymaga postawienia problemu użyteczności „informacji" dla decydenta w określonej sytuacji. Koncepcję pragmatyczną przedstawił K. Szaniawski, definiując wartość „informacji" ze względu na problem decyzji. Autor ten rozumie wykorzystywanie danych w sytuacji decyzyjnej jako funkcję decyzji przyporządkowującą każdej wiadomości określone działanie. Wartość „informacji" definiuje jako najwyższą wartość liczbową kosztu „informacji" połączonej z takim działaniem, określonym przez funkcję decyzji, którego użyteczność w sensie jakiegoś kryterium, przy danym koszcie, jest nie mniejsza od użyteczności każdego działania nie wyznaczonego przez tę funkcję[18]. Z uwagi na swój ogólny charakter propozycja K. Szaniawskiego może stanowić model dla interpretacji pragmatycznej wartości „informacji" w każdej sytuacji decyzyjnej.

---

[18]K. Szaniawski: *Pragmatyczna wartość informacji.* W: *„Problemy psychologii matematycznej"* pod red. J. Kozieleckiego, PWN, Warszawa 1971, s. 303 – 324.

In status quo i pro futuro w systemach informacyjnych człowiek pozostanie niezastąpiony. Od niego zależy cały zespół decyzji wyznaczających przebieg czynności informacyjnej. Podejmowanie decyzji w sytuacjach ze źródłem informacji zawodnej można rozumieć jako model często stosowanej w nauce indukcji statystycznej, natomiast podejmowanie decyzji w sytuacjach ze źródłem informacji niezawodnej — jako model wnioskowania niezawodnego.

Na tle przedstawionych poglądów można przyjąć wniosek, że przedmiotem myślowym (desygnatem) pojęcia „informacja" są bodźce, które poprzez system recepcyjny inspirują umysł człowieka do tworzenia wyobrażeń o stanie otoczenia, z którego pochodzą. Oznacza to tym samym, iż:

Istnienie „informacji" jest nierozerwalnie związane z umysłem ludzkim — tak jak foton nie może istnieć bez pędu, tak informacja nie może istnieć bez umysłu ludzkiego. Wszystko inne powodujące jakieś reakcje — tak w organizmach żywych, jak i w urządzeniach — należy nazywać sygnałami sterującymi.

„Informacja" jest szczególną formą sygnału sterującego. Jej szczególność wynika z tego, że sygnał sterujący jest odbierany przez receptory i tą drogą doprowadzany do umysłu człowieka, gdzie wytwarzane jest wyobrażenie o stanie otoczenia, z którego pochodzi — informacja jest sygnałem sterującym ludzką wyobraźnią. Dlatego też tę formę sygnału sterującego można nazywać sygnałem informacyjnym.

Wyobrażenie o stanie otoczenia, kształtowane na podstawie odebranego recepcyjnie bodźca, wiąże się z posiadaniem wcześniejszej wiedzy o możliwych stanach otoczenia i ujawniających je efektach. Umysł ludzki musi być wcześniej jakby zaprogramowany na kojarzenie określonych bodźców z daną sytuacją.

1.3. Cechy informacji charakterystyczne dla walki informacyjnej

Z założenia, że „informacja" jest czymś, co służy do bardziej sprawnego wyboru działań ukierunkowanych na osiągnięcie określonych celów, wynika jej charakter względny. Oznacza to, że dana „informacja" może być dla jednego celowego działania użyteczna, dla innego bezużyteczna, a jeszcze dla innego wręcz utrudniająca realizację działania celowego. Na przykład dla operatora nadzorującego pracę centrali automatycznej hałas wywoływany pracą wybieraków będzie „informacją" o pracy centrali. Ten sam hałas dla mechanika, naprawiającego jakiś element tejże centrali, będzie „informacją" zupełnie bezużyteczną, a dla

pracowników wymieniających tam poglądy na temat rozwiązania jakiegoś problemu hałas ten będzie „informacją" utrudniającą realizację działania celowego.

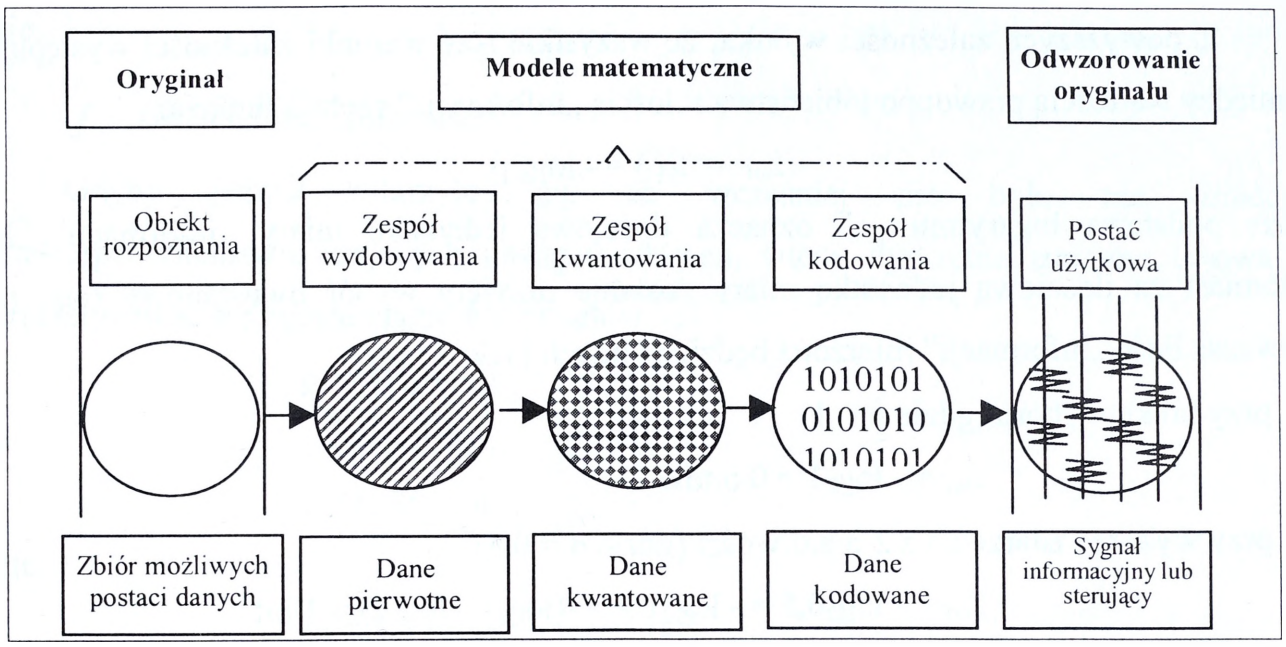
Związek „informacji" z celowością działania powoduje względność wskazującą na potencjalny i rzeczywisty jej charakter — nie wszystkie docierające „informacje" nadają się do wspomagania celowego działania w takiej postaci w jakiej zostały odebrane. Użytecznymi mogą się stać dopiero po odpowiednim przetworzeniu.

Na przykład w telekomunikacji zarejestrowanie parametrów modulacji sygnału nośnego nie spowoduje, że jego odbiorca będzie wiedział, jakie treści logiczne niesie ta „informacja". Dowie się o tym dopiero wówczas kiedy zarejestrowane parametry modulacji zostaną skonfrontowane z regułą modulacji w układzie przetwarzającym, to znaczy z uzależnieniem stanów sygnału nośnego od sygnału modulującego, który niesie w sobie „informację" logiczną dla odbiorcy. Są one „informacjami potencjalnymi" dla odbiorcy i często w literaturze przedmiotu określane są mianem „danych", które można dwojako rozumieć. Z jednej strony można je traktować jako odpowiednią postać sygnałów przeznaczonych do przetworzenia w urządzeniach; z drugiej — jako namiastkę „informacji" przekształconą w zmaterializowaną postać nadającą się do przetwarzania w urządzeniach. Jeśli natomiast człowiek stara się dostarczyć „informację" w sposób świadomy lub zaprogramowany, innemu człowiekowi, wtedy o takiej „informacji" można mówić, że jest ona „wiadomością".

Traktując „dane" i „wiadomości" jako synonimy „informacji" i uwzględniając niuanse powodów wyróżniania tych pojęć, można powiedzieć, że w większości wypadków „informacja" w czystej formie nie jest bezpośrednio dostępna. „Informacja" o określonym obiekcie rzeczywistości jest kategorią abstrakcyjną, myślową, i dlatego jako przetwarzane tworzywo procesu informacyjnego może występować, ale tylko w procesach przebiegających bezpośrednio w świadomości ludzkiej. Jeśli natomiast w procesie informacyjnym uczestniczą takie wspomagające urządzenia, jak: sztuczne receptory, tezaurusy, analizujące komputery itd., tworzywo informacyjne musi przybrać odpowiednią zmaterializowaną postać zróżnicowanych stanów na materialnym nośniku, który ogólnie nazywany jest „sygnałem" (rys.1.3.1). Na przykład jeżeli „informacja" jest przekazywana w postaci modulowanej fali elektromagnetycznej, to jej wykorzystanie po przekazaniu będzie możliwe dopiero po oddzieleniu „informacji" od fali nośnej, czego dokonuje aparatura odbiorcza z demodulatorem.

Przyjmując, że „informacja" zawarta jest w sygnale, należy uwzględniać to, że tylko niektóre cechy należą do „informacji" a inne, wpływające na jego postać, nie należą do niej

i zależą od innych czynników. Wynika więc z tego, że różnice pomiędzy „informacją" a niosącym ją sygnałem są w dużej mierze umowne, to znaczy względne.



Rys.1.3.1. Model formowania sygnału

Kolejną cechą „informacji" jest jej miara ilościowa nazywana entropią[19]. Miara ta jest nierozerwalnie związana z prawdopodobieństwem zdarzenia, czyli interpretowana jest jako:

$$I_{inf} = f(p)$$

gdzie:

I_{inf} - ilość informacji;

p - wartość prawdopodobieństwa.

Pomiędzy ilością informacji i wartością prawdopodobieństwa zachodzą trzy następujące zależności:

1) $$p_1 < p_2 \Rightarrow f(p_1) > f(p_2)$$

Oznacza to, że im większe jest prawdopodobieństwo zdarzenia, tym mniej „informacji" przynosi wiadomość, że dane zdarzenie zaszło.

2) $$p = 1 \Rightarrow f(p) = 0$$

Oznacza to, że wiadomość o zdarzeniu pewnym równa jest 0, a zatem nie niesie w sobie żadnej informacji (o zdarzeniu pewnym wiemy już wcześniej że takie zajdzie)

3) $$p = p_1 p_2 \Rightarrow f(p_1 p_2) = f(p_1) + f(p_2)$$

[19]Słowo „entropia" po raz pierwszy użyte zostało przez Clausiusa w 1876r. Później tym samym słowem nazwano funkcję opisującą stan układu termodynamicznego i jego zmiany. Jest to miara nieokreśloności i stopnia nieuporządkowania sytuacji, elementów lub stanów znajdujących się w pewnym zbiorze przeliczalnym, które traktowane są przy określaniu ich możliwej wartości jako zmienne losowe. Entropię danej zmiennej losowej można obliczyć znając charakterystyki probabilistyczne tej zmiennej.

Co oznacza, że informacja o iloczynie zdarzeń jest równa sumie informacji o poszczególnych zdarzeniach.

Z powyższych zależności wynika, że wszystkie trzy warunki zależności występujące pomiędzy wartością prawdopodobieństwa i ilością „informacji" spełnia funkcja:

$$I_{inf} = f(p) = - \log_a p$$

gdzie podstawa logarytmu „a" oznacza ilościową jednostkę miary „informacji". Jeśli natomiast za ilościową jednostkę miary zostanie przyjęty wybór dwustanowy (tak, nie), wówczas ilość „informacji" mierzona będzie w bitach i tak:

- przy braku wyboru (gdzie p = 1)

$$I_{inf} = - \log_2 1 = 0 \text{ bitów}$$

- przy wyborze zdarzenia z 2 możliwości (gdzie p = 0,5)

$$I_{inf} = - \log_2 0{,}5 = - \log_2 1/2 = -(\log_2 1 - \log_2 2) = 1 \text{ bit}$$

- przy wyborze zdarzenia z 8 możliwości (gdzie p = 0,125)

$$I_{inf} = - \log_2 0{,}125 = - \log_2 1/8 = -(\log_2 1 - \log_2 8) = 3 \text{ bity}$$

- przy wyborze zdarzenia z 2^n możliwości (gdzie $p = 1/2^n$)

$$I_{inf} = - \log_2 1/2^n = -(\log_2 1 - \log_2 2^n) = -(\log_2 1 - n \log_2 2) = n \text{ bitów}$$

Przytoczone wyżej zasady ustalania ilości „informacji" w danym komunikacie są właściwe, ale tylko w sytuacji kiedy każde zdarzenie zachodzi z takim samym prawdopodobieństwem. To znaczy kiedy rozkład dyskretnej zmiennej losowej X_d charakteryzuje się ciągiem rozkładów:

$$p_i = P(X_d = x_i)$$

dla:

$$p_1(x_1) = p_2(x_2) = \ldots = p_n(x_n)$$

co w praktyce oznacza, że wcześniej nic nie było wiadomo o mających nastąpić zdarzeniach - wiadomo było tylko, że „n" takich zdarzeń nastąpi.

W praktyce jednak jest tak najczęściej, że pewnych zdarzeń oczekuje się z mniejszym, a innych z większym prawdopodobieństwem to znaczy, że wcześniej już coś o nich wiadomo. Wówczas rozkład dyskretnej zmiennej losowej X_d charakteryzować się będzie ciągiem rozkładów:

$$p_i = P(X_d = x_i)$$

dla:

$$i = 1; 2; \ldots ;n$$

W takiej sytuacji mówi się o średniej ilości informacji, a wartość tę oblicza się z zależności:

$$\bar{I} = -\sum_{i=1}^{n} p_i \log_a p_i$$

gdzie:

$\bar{I}$ - średnia ilość „informacji".

Gdyby jednak zdarzyło się, że wcześniej nie było nic wiadomo o prawdopodobieństwie mających nastąpić zdarzeń, wtedy dyskretna zmienna losowa X_d charakteryzować się będzie ciągiem rozkładów:

$$p_i = \{X_d = x_i\}$$

dla:

$$i = 1; 2; ...; n$$

gdzie;

$$p_1(x_1) = p_2(x_2) = ... = p_n(x_n)$$

co w odniesieniu do przytoczonego przykładu przyjmie wartości:

$$p_1(x_1) = 0{,}25; \quad p_2(x_2) = 0{,}25; \quad p_3(x_3) = 0{,}25; \quad p_4(x_4) = 0{,}25;$$

a średnia ilość „informacji" $\bar{I}$ wyniesie:

$$\bar{I} = -\sum_{i=1}^{4} p_i \log_2 p_i =$$

$$= -(0{,}25\log_2 0{,}25 + 0{,}25\log_2 0{,}25 + 0{,}25\log_2 0{,}25 + 0{,}25\log_2 0{,}25) = 2bity$$

Z porównania powyższych przykładów wynika, że średnia ilość „informacji" zależna jest zawsze od wartości prawdopodobieństw, które zostały przypisane zdarzeniom elementarnym występującym podczas realizacji zmiennej losowej X_d. Z zależności tej wynika, że średnia ilość „informacji" osiąga zawsze największą wartość przy realizacji zdarzeń równo-prawdopodobnych, czyli w sytuacji, kiedy dane zjawisko (proces), na które składa się „n" realizacji zmiennej losowej X_d nie zostało wcześniej poznane.

W teorii ogólnej średnia ilość „informacji" określana jest mianem entropii. Oznaczana jest symbolem „H" i zapisywana równaniem:

- dla rozkładu dyskretnego:

$$H(X_d) = -\sum_{i=1}^{n} p_i \log_a p_i$$

gdzie:

X_d - dyskretna zmienna losowa;

p_i - prawdopodobieństwo i-tej realizacji dyskretnej zmiennej losowej X_d;

a - jednostkowa miara ilości „informacji".

- dla rozkładu ciągłego:

$$H(X_c) = -\int_{-\infty}^{\infty} f(x)\log_a f(x)dx + C$$

gdzie:

X_c — ciągła zmienna losowa;

f(x) — gęstość prawdopodobieństwa realizacji ciągłej zmiennej losowej X_c;

a — jednostkowa miara ilości informacji;

C — stała określająca początek liczenia entropii ciągłej zmiennej losowej X_c.

Tak w pierwszym, jak i w drugim wypadku, entropia rozkładu zmiennej losowej (tak ciągłej X_c, jak i dyskretnej X_d) stanowi zawsze miarę nieokreśloności i stopnia nieuporządkowania:

— sytuacji;

— elementów;

— względnie stanów;

które znajdują się w pewnym zbiorze przeliczalnym i traktowane są, przy określaniu ich możliwej wartości, jako realizacje zmiennej losowej, tak ciągłej X_c, jak i dyskretnej X_d.

Z powyższego wynika więc, że entropię zmiennej losowej można obliczać tylko wówczas, kiedy są znane charakterystyki probabilistyczne tej zmiennej. Entropia zmiennej losowej jest tym większa, przy ustalonym zakresie zmienności, im bardziej rozkład prawdopodobieństwa zmiennej losowej jest zbliżony do rozkładu równomiernego. Dla zbioru niezależnych zmiennych losowych entropia jest sumą entropii jego podzbiorów. Entropia jest równa zeru tylko dla zmiennej losowej, której zbiór wartości jest równy jedności.

Z punktu widzenia uwarunkowań walki informacyjnej, ogólna interpretacja entropii nie wystarcza jeszcze do właściwego naświetlenia problemu. W tym względzie szczególnie istotną rolę odgrywa „entropia fizyczna" i „entropia informacyjna".

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 się w niej nieokreśloności wnoszonej przez niewiedzę obserwatora, lecz 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, gdyż za miarę uzyskanej tą drogą przez odbiorcę „informacji" przyjmuje się stopień zmniejszenia nieokreśloności. W odróżnieniu od entropii fizycznej, która jest całkowicie określana przez istniejący obiektywnie rozkład prawdopodobieństwa danego stanu, entropia informacyjna uwzględnia jeszcze i nieokreśloność spowodowaną niepełną wiedzą odbiorcy o statystyce zjawisk zachodzących w źródle informacji. Tylko w wypadku, gdy odbiorca jest całkowicie poinformowany o statystycznej naturze zjawiska, wartość entropii fizycznej i informacyjnej pokrywają się.

Wszelkie działania podejmowane w ramach walki informacyjnej ukierunkowane są na manipulowanie wartością entropii informacyjnej. Rozpoznanie ukierunkowane na jej zmniejszanie (dąży do równania jej z wartością entropii fizycznej), a zakłócanie i obrona informacyjna dążą do jej maksymalnego zwiększania.

W aspekcie powyższego szczególną rolę odgrywa wartość użytkowa informacji, na którą wpływ ma szereg czynników. Dotychczasowe próby przedstawienia wartości użytkowej informacji jako wielkości skalarnej nie doprowadziły do wyniku, który znalazłby szersze zastosowanie praktyczne. W związku z powyższym proponuje się traktować wartość użytkową informacji jako wielkość wektorową. Za czynniki decydujące o jej wartości użytkowej zawartej w określonym komunikacie należy uznać: aktualność, relewantność, kompletność, przyswajalność i wiarygodność.

Aktualność informacji określana jest jako monotonicznie nierosnąca funkcja opóźnienia, z jakim informacja może być dostarczona odbiorcy. Opóźnienie θ powinno być liczone od chwili, w której zaistniał fakt przez tę informację odzwierciedlony. Jeśli oznaczyć symbolem θ_0 opóźnienie normatywne, dopuszczalne dla danego typu komunikatów, to współczynnik aktualności informacji zawartej w komunikacie można w najprostszym przypadku wyrazić zależnością:

$$k_a = \frac{\theta_0 - \theta}{\theta_0} = 1 - \frac{\theta}{\theta_0}, \quad \text{gdzie:} \quad \theta_0 > 0$$

Relewantność informacji wyraża jej zgodność z potrzebą użytkownika wyrażoną w pytaniu skierowanym do systemu. Jeśli komunikat zawiera I jednostek informacyjnych (bitów, słów itp.), a „informacja" istotna dla użytkownika zawarta jest tylko w I_r jednostkach informacyjnych, przy czym $I_r \leq I$, to współczynnik relewantności informacji zawartej w komunikacie można wyrazić wzorem:

$$k_{\mathrm{r}} = \frac{I_{\mathrm{r}}}{I}$$

Kompletność informacji wyraża stosunek ilości relewantnej, realnie otrzymanej przez użytkownika w dostarczonym mu komunikacie, do ilości informacji relewantnej, jaką teoretycznie (w sytuacji idealnej) mógłby on uzyskać wykorzystując w pełni wydajność informacyjną źródła informacji.

Współczynnik kompletności informacji I_0 można wyrazić wzorem:

$$k_{\mathrm{k}} = \frac{I_{\mathrm{r}}}{I_0},$$

przy czym $I_0 \geq I_{\mathrm{r}}$.

Przyswajalność informacji jest cechą wyrażającą jej przydatność do bezpośredniego wykorzystania przez użytkownika w podejmowaniu decyzji lub w następnej fazie przetwarzania. Przyswajalność jest zatem tym mniejsza, im większy jest przewidywany nakład środków (czasu, kosztów itp.), jakie użytkownik musi ponieść dodatkowo, ażeby informację dostarczoną mu w komunikacie uzyskać w pożądanej postaci. Oznaczając ów dodatkowy nakład środków symbolem N, a symbolem N_0 - pewien ustalony dla danego typu komunikatu nakład dopuszczalny, możemy określić współczynnik przyswajalności wzorem:

$$k_{\mathrm{p}} = \frac{N_0 - N}{N_0} = 1 - \frac{N}{N_0}, \quad \text{gdzie:} \quad N_0 > 0$$

Wiarygodność informacji jest cechą wyrażającą jej zgodność z opisywanym przez nią stanem obiektu. Może ona być wyrażona jako monotonicznie nierosnąca funkcja błędu, z jakim informacja odzwierciedla rzeczywisty stan obiektu. Oznaczając ten błąd symbolem δ, a symbolem δ_0 jego wartość dopuszczalną, możemy w następujący sposób określić współczynnik wiarygodności informacji:

$$k_{\mathrm{w}} = \frac{\delta_0 - \delta}{\delta_0} = 1 - \frac{\delta}{\delta_0}, \quad \text{gdzie:} \quad \delta > 0$$

Za informację niewiarygodną uznajemy zatem taką, dla której:

$$\delta > \delta_0 \quad \text{lub} \quad k_{\mathrm{w}} < 0.$$

Przez wartość użytkową informacji zawartej w komunikacie będziemy rozumieli wektor o składowych opisanych wzorami *ut supra*:

$$\mathbf{V} = [k_{\mathrm{a}}, k_{\mathrm{r}}, k_{\mathrm{k}}, k_{\mathrm{p}}, k_{\mathrm{w}}]$$

Sposób określania poszczególnych składowych wektora implikuje zasady obliczania wartości użytkowej informacji w toku jej przetwarzania. Każda operacja wykonywana na

komunikatach pociąga bowiem za sobą: wzrost opóźnienia, zmianę procentowej zawartości informacji relewantnej, zmianę formy komunikatu, zmianę błędu opisu rzeczywistości itd., dając tym samym podstawę do obliczenia składowych wektora **V**.

W procesie walki informacyjnej należy uwzględniać, iż:

- *użytkowymi postaciami „informacji" są różnego rodzaju sygnały informacyjne i sygnały sterujące, które można nazwać produktem procesu opracowywania i przetwarzania danych na odcinku: źródło informacji — układ odbierający;*
- *użytkową postać informacji stanowią komunikaty. Komunikaty przekazywane są na różnych nośnikach — w postaci sygnałów informacyjnych lub sterujących — które pod względem parametrycznym muszą być kompatybilne z fizycznymi możliwościami rejestracyjnymi występującymi na wejściu układów odbierających;*
- *oryginał odwzorowywany na podstawie sygnałów informacyjnych i sterujących jest zawsze odzwierciedleniem wartości entropii informacyjnej, która zwykle jest większa od wartości entropii fizycznej;*
- *wartość entropii informacyjnej determinowana jest: zakresem dostępności źródeł informacji do możliwych postaci danych odzwierciedlających rzeczywisty obiekt rozpoznania, doskonałością procesu przetwarzania i opracowywania danych oraz doskonałością kompilowania uzyskiwanych w ten sposób treści w komunikaty stanowiące sygnały informacyjne i sterujące dla docelowych układów odbierających, aktualnością, relewantnością, kompletnością, przyswajalnością;*
- *zdobywanie, przetwarzanie, opracowywanie, przekazywanie i wykorzystywanie danych odbywa się w systemie informacyjno-sterującym, którego strukturę tworzą: źródła informacji, przetworniki informacji, układy odbierające, nośniki informacji, relacje systemowe;*
- *„informacja" jest prawdziwa, co nie oznacza, że każda „informacja" jest obiektywnym odzwierciedleniem poznawanego oryginału (całości lub jego części). Jej prawdziwość wynika z faktu dotarcia do układu odbierającego. Używanie pojęcia „informacja nieprawdziwa" jest następstwem uproszczonego postrzegania problemu. Wynika z tego, że układ odbierający nie zawsze jest świadom czego rzeczywistym odzwierciedleniem jest odebrany sygnał informacyjny lub sterujący czy też określona postać danej. Powodowane jest to przypisywaniem określonych postaci danych innym obiektom rozpoznania niż tym z których rzeczywiście pochodzą;*
- *w procesie walki informacyjnej na „informacje" nie można oddziaływać bezpośrednio. Można to czynić poprzez system informacyjno-sterujący i poprzez zbiory możliwych*

postaci danych, które w swej masie stanowią obiekty rozpoznania. Nie można zatem używać pojęć „zakłócanie informacji" i „obrona informacji". Należy używać określeń — „zakłócanie informacyjne" i „obrona informacyjna";

- *szeroko rozumiane maskowanie, pozorowanie i ukrywanie możliwych postaci danych, stanowiących obiekty rozpoznania, powoduje wnoszenie entropii informacyjnej do systemu informacyjno — sterującego ukierunkowanego na rozpoznawanie tych obiektów.*

1.4. Struktura walki informacyjnej i rola funkcjonalna jej elementów

Badanie układów komunikacyjnych wymaga stosowania analizy strukturalnej w celu opisania różnorodnych zjawisk za pomocą jednorodnych narzędzi (to znaczy w celu wytropienia homologii formalnych pośród przekazów, kodów, kontekstów komunikacyjnych w jakich one funkcjonują — jednym słowem pośród aparatów retorycznych i ideologii). Funkcją metody strukturalnej jest właśnie umożliwienie rozłożenia różnych poziomów komunikacyjnych na szeregi równoległe, jednorodne. Jest to zatem funkcja operacyjna, służąca uogólnieniu wywodu. Strukturę układu komunikacji należy ustalić tam, gdzie zachodzi komunikacja w warunkach minimalnych, czyli na poziomie, na którym przepływ „informacji" odbywa się między dwoma urządzeniami mechanicznymi — i to nie dlatego, że bardziej złożone zjawiska komunikacji dają się sprowadzić do przepływu sygnału z jednej maszyny do drugiej, lecz dlatego, że pożytecznie jest zdefiniować stosunek komunikacyjny w jego zasadniczej dynamice tam, gdzie występuje on ze szczególną oczywistością i prostotą, sugerując nam budowę wzorcowego modelu. Dopiero gdy zdoła się ustalić ten model (strukturę komunikacji), zdolny do funkcjonowania również na poziomach o większej złożoności (chociażby kosztem rozmaitych zróżnicowań i komplikacji), będzie można omawiać wszystkie zjawiska w aspekcie komunikacji. Jeśli na przykład nadawca chce przekazać odbiorcy jakąś „informację", wtedy uaktywnia pewien aparat nadawczy, zdolny do wysłania sygnału (np. sygnału elektrycznego). Sygnał ten wędruję pewnym kanałem (po przewodzie elektrycznym, na falach radiowych itp.) i zostaje odebrany przez aparat odbiorczy. Odbiornik ten ujmuje sygnał w określoną formę, stanowiącą komunikat skierowany do adresata. Adresatem tym może być drugi aparat, odpowiednio poinstruowany, który odbierając komunikat zaczyna korygować sytuację wyjściową. W ten sposób powstaje łańcuch komunikacyjny: źródłem informacji jest tu nadawca komunikatu, który, ustaliwszy pewien zespół wydarzeń przeznaczonych do zakomunikowania, przesyła je do przekaźnika, a ten przetwarza je w sygnały fizyczne, wędrujące kanałem i przyjmowane przez odbiornik przetwarzający je na komunikat, który adresat odbierze.

Z powyższego wynika, że proces informacyjny nie jest możliwy poza układami materialnymi i bez określonych przemian energetycznych. Informacja wymaga obecności nośnika materialnego i materialnego charakteru przekazu. Przekaz „informacji" przez linię komunikacyjną ma sens tylko wtedy, gdy linia ta jest częścią układu informacyjno-sterującego, w którym owa informacja wyodrębnia się i służy realizacji określonych celów. „Informacja" więc związana jest ściśle z określonym układem informacyjno-sterującym.

Jeśli „informację" traktuje się w sposób relatywny, jako działanie na zewnętrzne i wewnętrzne wejścia układu odbierającego, to wówczas można stwierdzić, że: ***„informacja"** bez układu odbierającego nie może nigdy zaistnieć. Warunkiem istnienia „informacji" jest istnienie układu odbierającego, a istnienie układu odbierającego jest relatywnie związane z istnieniem „informacji" oddziałującej na zewnętrzne i wewnętrzne wejścia tego układu. „Informacja" nie jest więc czymś samym w sobie. Zostaje nią dopiero wówczas, kiedy sygnał niosący jej treść zostanie zarejestrowany na zewnętrznym lub wewnętrznym wejściu układu odbierającego.*

Relatywność „informacji" nie kończy się tylko na jej związku z układem odbierającym. Każda „informacja: związana jest jeszcze ze źródłem informacji i jej nośnikiem. Jeśli uwzględni się przy tym porządkującą regułę przechodniości, to można zapisać, że:

zapisać, że:

$$Z_i \,\Re\, I \wedge I \,\Re\, N_i \wedge N_i \,\Re\, U_o \rightarrow Z_i \,\Re\, U_o$$

gdzie:

$\Re$ — relacja

I — informacja;

Z_i — źródło informacji;

N_i — nośnik informacji;

U_o — układ odbierający.

Z powyższego wynika, że na „informację" nie można oddziaływać bezpośrednio w procesie walki informacyjnej. Można to czynić ale tylko poprzez system informacyjno-sterujący.

W walce zbrojnej systemy informacyjno-sterujące przeznaczone są do rozpoznania przeciwnika oraz do dowodzenia i kierowania własnym potencjałem walki. Każda z zaangażowanych stron dąży do tego aby jej system funkcjonował lepiej od systemu przeciwnika. Efekty tego wyznaczane są osiąganą skutecznością rozpoznania i sprawnością przebiegu procesów informacyjnych. Ujawniająca się w tym zakresie konkurencyjność

ukierunkowana jest na wzajemne negowanie dążeń — posiada wszystkie znamiona charakterystyczne dla kooperacji negatywnej wzajemnej — czyli jest walką ukierunkowaną na osiąganie przewagi informacyjnej, co można nazywać w skrócie walką informacyjną.

Postrzegając walkę informacyjną w kategoriach Brydgmanowskich, można ją potraktować jako pewną „procedurę operacyjną", posiadającą określoną strukturę. Za jej elementy można uznać:

W aspekcie czynnościowym (w aspekcie sprzężeń):

— sprzężenie rozpoznawcze;

— sprzężenie zakłócające;

— sprzężenie obronne.

W aspekcie rzeczowym:

— podukład rozpoznania;

— podukład zakłócania informacyjnego;

— podukład obrony informacyjnej;

Podukład rozpoznania tworzą źródła zdobywania danych i ich sprzężenia. Źródła te przeznaczone są do wybierania ze zbiorów danych o przeciwniku jak najwięcej takich danych, których posiadanie pozwala identyfikować jego stan aktualny i zamiary działania. Do tego podukładu (podukładu rozpoznania) są przeciwnie skierowane: podukład obrony informacyjnej przeciwnika i podukład jego zakłócania informacyjnego.

Podukład zakłócania informacyjnego przeznaczony jest do wnoszenia entropii informacyjnej do systemu informacyjno-sterującego przeciwnika i destrukcji fizycznej do jego nośników, przetworników i układów odbierających. Zakłócanie to możne być prowadzone różnymi sposobami. Najbardziej efektywnie można to jednak czynić poprzez stosowanie odpowiedniej upływności specjalnie zdeformowanych zbiorów własnych postaci danych, z których podukład rozpoznania przeciwnika czerpie zasilanie informacyjne. Dlatego też do podukładu zakłócania informacyjnego jednej strony przeciwnie skierowany jest podukład rozpoznania i podukład obrony informacyjnej strony drugiej.

Podukład obrony informacyjnej przeznaczony jest do obrony tych postaci danych, które demaskują własny stan rzeczywisty i zamiary dalszego działania. Do niego przeciwnie skierowany jest podukład zakłócania informacyjnego i podukład rozpoznania kooperanta negatywnego.

Z powyższego wynika, że w procesie walki informacyjnej każdemu podukładowi jednej strony przeciwstawione są dwa podukłady strony drugiej (mac. 1.4.1). Polega to na tym, że:

Mac. 1.4.1. Funkcjonalne powiązania walki informacyjnej

	Działanie A_1	Działanie A_2	Działanie A_3	Działanie A_4
Działanie B_1	Obrona informac. / Zdobywanie informacji			
Działanie B_2		Zdobywanie informac. / Obrona informacyjna		
Działanie B_3			Obrona informac. / Zakłócanie informacyjne	
Działanie B_4				Zakłócanie informac. / Obrona informacyjna

— prowadzący rozpoznanie musi się liczyć z przeciwdziałaniem podukładów zakłócania i obrony informacyjnej;

— prowadzący zakłócanie informacyjne musi się liczyć z przeciwdziałaniem podukładów rozpoznania i obrony informacyjnej;

— prowadzący obronę informacyjną musi się liczyć z przeciwdziałaniem podukładów rozpoznania i zakłócania informacyjnego przeciwnika.

Traktując zatem walkę informacyjną jako układ o wysokim stopniu komplikacji i oznaczając przez:

— R_A — podukład rozpoznania strony „A";

— R_B — podukład rozpoznania strony „B";

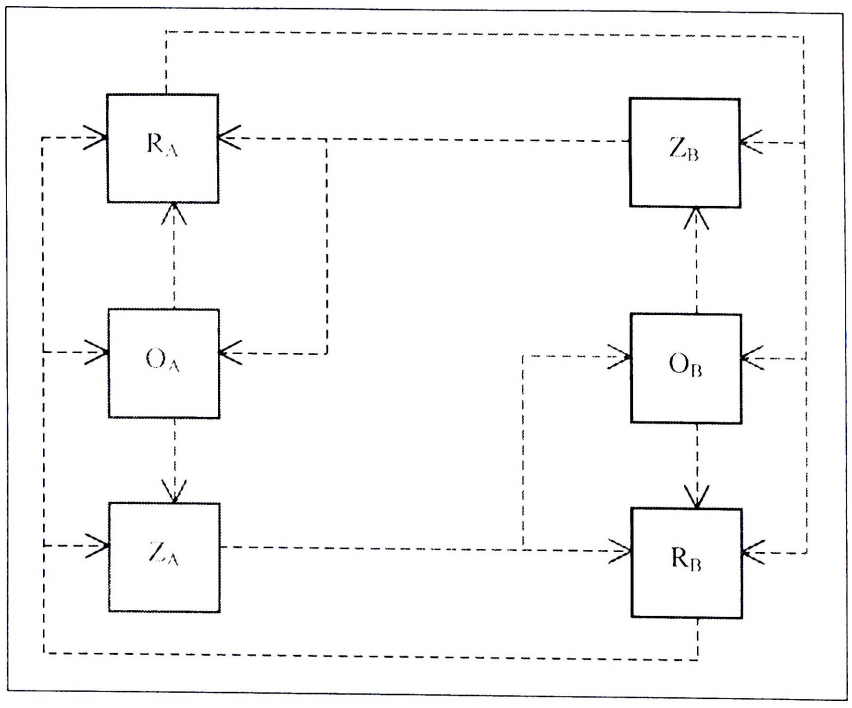
— O_A — podukład obrony informacyjnej strony „A";

— O_B — podukład obrony informacyjnej strony „B";

— Z_A — podukład zakłócania informacyjnego strony „A";

— Z_B — podukład zakłócania informacyjnego strony „B";

jej model strukturalny można wyrazić następującym schematem blokowym (rys. 1.4.1).



Rys. 1.4.1. Model struktury walki informacyjnej

Model struktury walki informacyjnej odzwierciedla następująca matryca sprzężeń:

	R_A	Z_A	O_A	R_B	Z_B	O_B
R_A	0	0	0	1	1	1
Z_A	0	0	0	1	0	1
O_A	1	1	0	0	0	0
R_B	1	1	1	0	0	0
Z_B	1	0	1	0	0	0
O_B	0	0	0	1	1	0

co oznacza, że jest to:

$$\left[\begin{array}{l}\{R_A, Z_A, O_A, R_B, Z_B, O_B\} \wedge \\ \left\{\begin{array}{l} R_A R_B, R_A Z_B, R_A O_B, Z_A R_B, Z_A O_B, O_A R_A, O_A Z_A, \\ R_B R_A, R_B Z_A, R_B O_A, Z_B R_A, Z_B O_A, O_B R_B, O_B Z_B \end{array}\right\} \end{array}\right]$$

W walce informacyjnej poszczególne podukłady przeznaczone są do spełniania następujących ról funkcjonalnych:

- *podukłady rozpoznania (R_A i R_B) — do zdobywania wszelkich postaci danych o stanie, otoczeniu i zamiarach działania przeciwnika;*
- *podukłady zakłócania informacyjnego (Z_A i Z_B) — do wnoszenia entropii informacyjnej i destrukcji fizycznej do systemu informacyjno-sterującego przeciwnika;*
- *podukłady obrony informacyjnej (O_A i O_B) — do obrony zbioru własnych postaci danych i obrony własnego systemu informacyjno —sterującego.*

Walka informacyjna jest kooperacją negatywną wzajemną realizowaną w sferze rozpoznania (zdobywania informacji), zakłócania informacyjnego i obrony informacyjnej, gdzie każdemu działaniu jednego podukładu tej walki jest przyporządkowane działanie antagonistyczne dwóch pozostałych podukładów strony przeciwnej.

Istota walki informacyjnej sprowadza się do stwarzania sytuacji utrudniających przeciwnikowi podejmowanie trafnych decyzji, wykonywanie sprawnych ruchów wojskami i precyzyjnych uderzeń ogniowych, przy jednoczesnej obronie przed tym samym wojsk własnych. Innymi słowy, ukierunkowana jest na dezorientowanie przeciwnika co do sytuacji na polu walki, komplikowanie jego warunków działania i w efekcie zmuszanie go do podejmowania błędnych decyzji.

1.5. Przestrzeń walki informacyjnej

Pojęcie „przestrzeń walki informacyjnej" powinno zawierać w swoim zbiorze przedmiotowym wszystkie te elementy, które są właściwe wyrazom: „przestrzeń"; „walka" oraz „walka informacyjna", co można oznaczyć następująco:

— $\{P\}$ — zbiór elementów składających się na desygnat „przestrzeń";

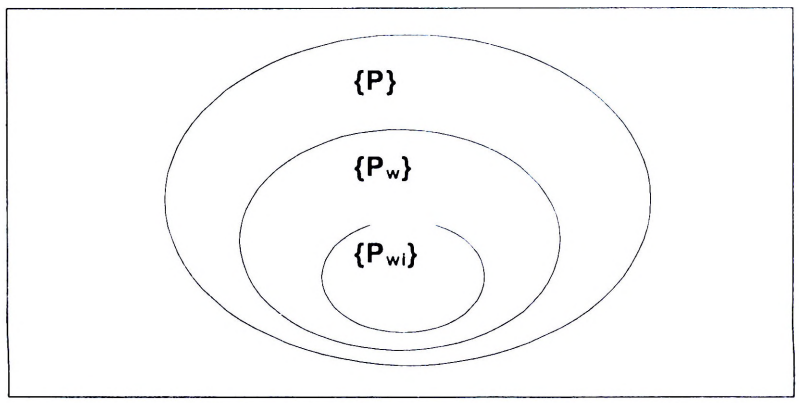
— $\{P_w\}$ — zbiór elementów składających się na desygnat „przestrzeń walki";

— $\{P_{wi}\}$ — zbiór elementów składających się na desygnat „przestrzeń walki informacyjnej".

Zależność semantyczną pomiędzy tymi pojęciami można wyrazić zapisem:

$$\{P_{wi}\} \subset \{P_w\} \subset \{P\}$$

oraz przedstawić graficznie (rys. 1.5.1).



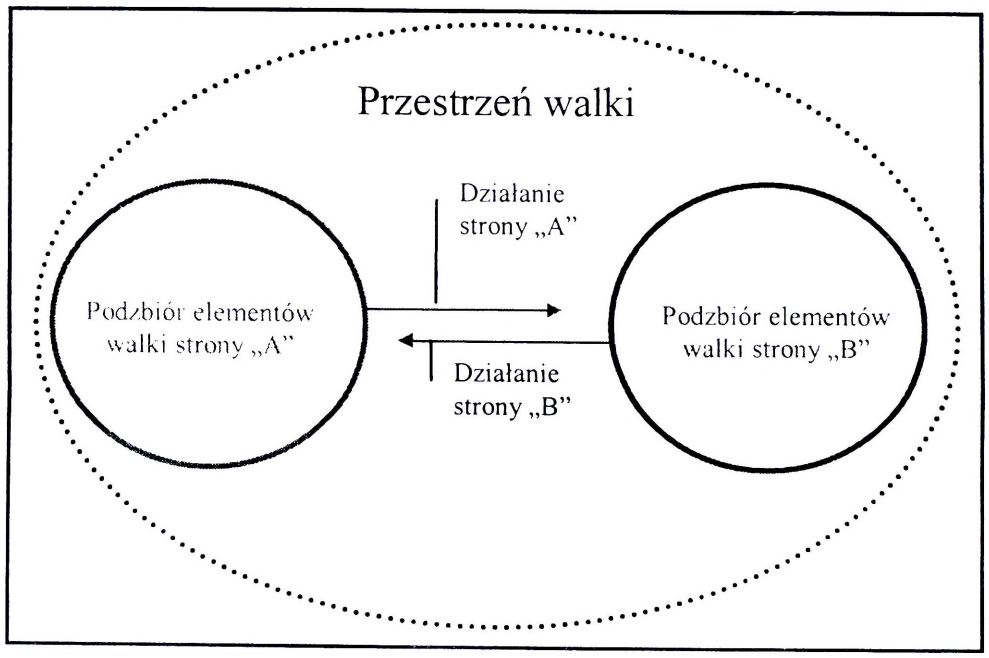
Rys. 1.5.1. Zależność semantyczna pomiędzy pojęciami: „przestrzeń", „przestrzeń walki" i „przestrzeń walki informacyjnej"

Oznacza to, że zbiór określony mianem „przestrzeń walki informacyjnej" i wyróżniony symbolem $\{P_{wi}\}$ powinien zawierać w swoim zbiorze pojęciowym podstawowe elementy przedmiotu myślowego „przestrzeń" $\{P\}$ i przedmiotu myślowego „przestrzeń walki" $\{P_w\}$.

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 walki" 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 walki" można nazywać tylko taki zbiór elementów, który składa się przynajmniej z dwóch podzbiorów (z dwóch podprzestrzeni) ukierunkowanych funkcjonalnie na osiąganie przeciwnie skierowanych celów (rys. 1.5.2).



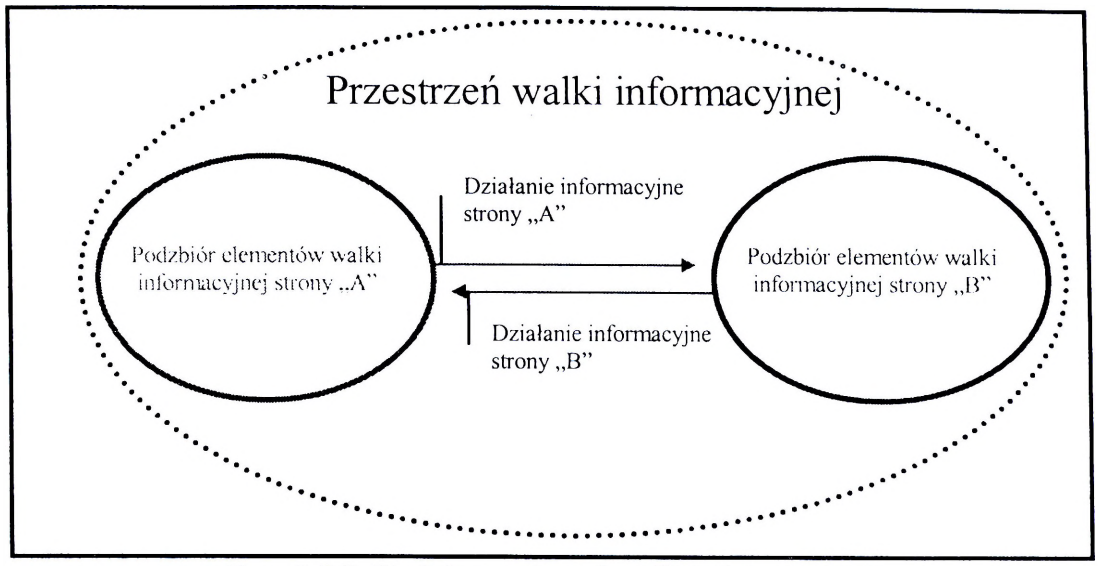
Rys. 1.5.2. Model przestrzeni walki

Przez analogię do powyższego, można stwierdzić, że „przestrzenią walki informacyjnej" 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 walki informacyjnej (rys. 1.5.3).

Z tego wynika, że podstawową strukturę[20] przestrzeni walki informacyjnej tworzą elementy, przynajmniej dwóch zbiorów, należące do przeciwnych sobie stron, które zespolone są wspólną relacją porządkującą celu ukierunkowaną na prowadzenie walki informacyjnej. Elementy te stanowią specjalnie przygotowane do tej walki: uzbrojenie, wyposażenie

[20]Struktura to układ i wzajemne relacje elementów stanowiących całość. *Słownik języka polskiego*, t 3, PWN, Warszawa 1981r., s. 352.

techniczne, system organizacyjny i system szkolenia wojsk oraz sposoby wykorzystywania tego w działaniach.



Rys. 1.5.3. Model przestrzeni walki informacyjnej

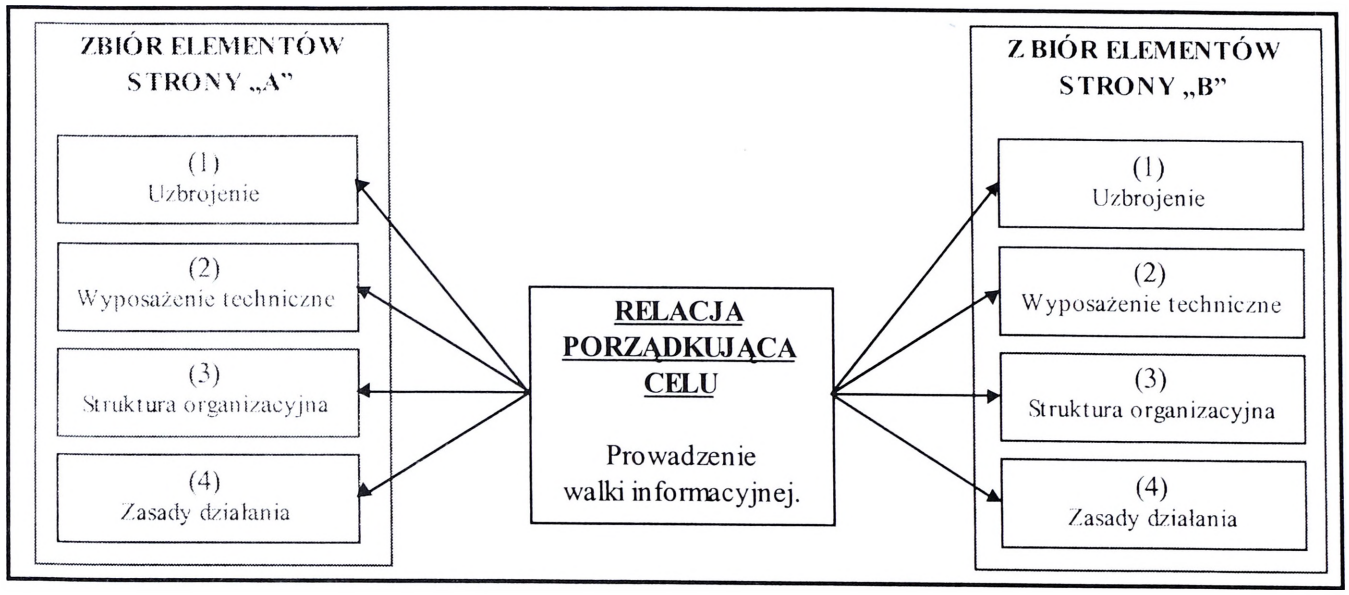
Tak zdefiniowaną przestrzeń walki informacyjnej, przy bardziej precyzyjnej konkretyzacji, winno się traktować jako przestrzeń „potencjalną" (rys. 1.5.4).

Rys. 1.5.4. Model potencjalnej przestrzeni walki informacyjnej

Wyróżnione elementy zespolone są tylko relacją porządkującą, której celem jest dostosowanie elementów do prowadzenia walki informacyjnej. Nie oznacza to jednak, że walka taka będzie kiedykolwiek prowadzona — może być prowadzona ale nie musi. Innymi słowy, w przestrzeni tej zawarty jest tylko pewien potencjał, który dopiero w konkretnym działaniu będzie się mógł wyzwalać jako określona siła tej walki. Wówczas spowoduje przekształcenie przestrzeni „potencjalnej" w „czynną" przestrzeń walki informacyjnej.

W czynnej przestrzeni walki informacyjnej relacja porządkująca celu integrować będzie elementy zbioru nie przez pryzmat dostosowania ich do prowadzenia walki informacyjnej ale przez pryzmat czynnej realizacji zadań. Dlatego też w zbiorach elementów

tej przestrzeni nie będą występowały procedury szkolenia wojsk, które funkcjonalnie związane są nie z prowadzeniem walki informacyjnej, ale tylko z przygotowywaniem elementów do uczestniczenia w tej walce (rys.1.5.5). Innymi słowy,



Rys. 1.5.5. Model czynnej przestrzeni walki informacyjnej

czynna przestrzeń walki informacyjnej różni się od przestrzeni biernej tylko tym, że zawiera elementy nie w stanie statycznym (w gotowości do prowadzenia tej walki), ale w stanie dynamicznym. Ich działalność ukierunkowana jest na realizację trzech podstawowych grup zadań związanych ze zdobywaniem informacji o przeciwniku (prowadzeniem rozpoznania), zakłócaniem informacyjnym (zakłócaniem procesów informacyjnych przeciwnika) i obroną informacyjną (obroną własnych procesów informacyjnych przed rozpoznaniem i zakłóceniami stosowanymi przez przeciwnika) — rys. 1.5.6.

Dlatego też, zarówno w potencjalnej, jak i w czynnej przestrzeni walki informacyjnej można wyróżnić po trzy podprzestrzenie, które z relacjami porządkującymi celów tworzą najbardziej ogólną strukturę przestrzeni walki informacyjnej. Elementami tymi są:

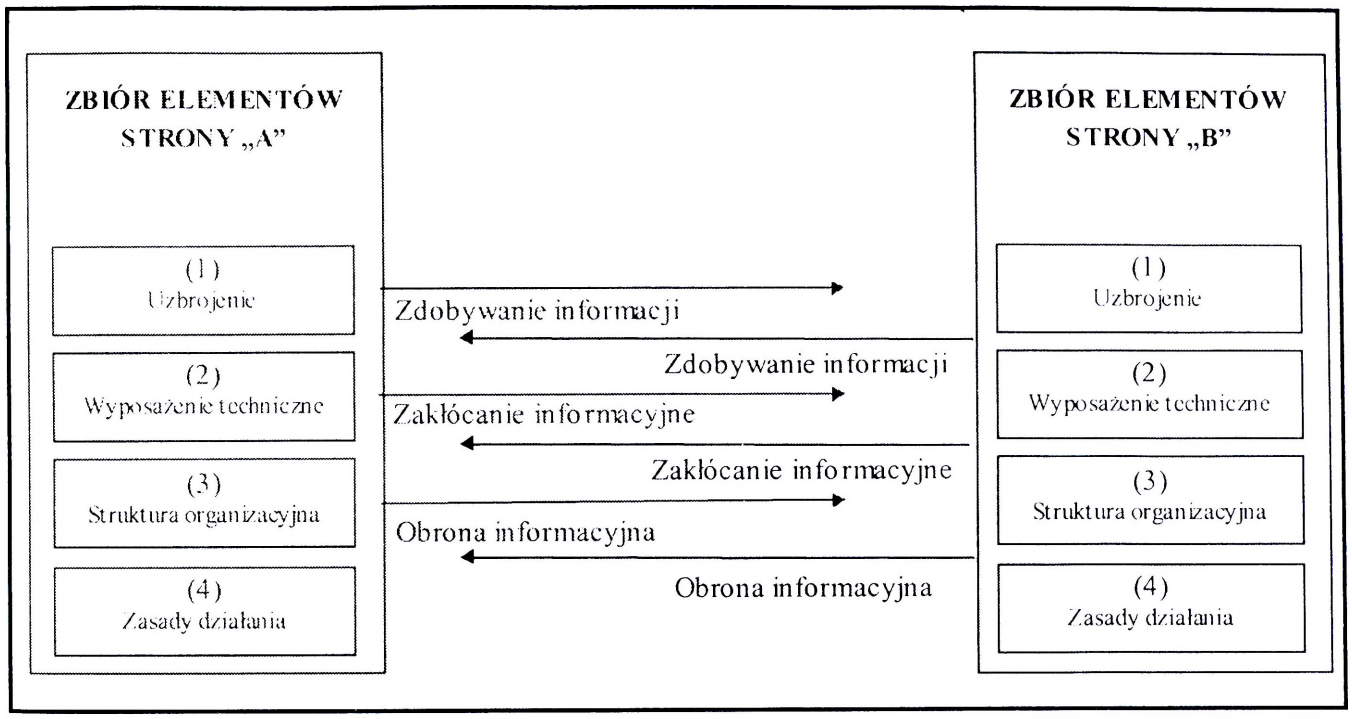
— *podprzestrzeń rozpoznania (zdobywania informacji o przeciwniku);*

— *podprzestrzeń zakłócania informacyjnego;*

— *podprzestrzeń obrony informacyjnej;*

— *ogólna relacja porządkująca celu uwzględniająca dostosowanie elementów przestrzeni potencjalnej do prowadzenia walki informacyjnej lub uwzględniająca prowadzenie walki informacyjnej — w wypadku przestrzeni czynnej;*

— *relacje celu porządkujące elementy podprzestrzeni: rozpoznania, zakłócania i obrony informacyjnej.*



Rys. 1.5.6. Model czynnej przestrzeni walki informacyjnej w stanie dynamicznym

Zasady wyznaczania przestrzeni walki informacyjnej można oprzeć 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. W tym względzie szczególnie duże znaczenie odgrywa 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[21]. W ten sposób ustalono jednoznaczne cechy wyróżnialności, których stosowanie jest nieodzowne przy rozwiązywaniu jakichkolwiek problemów związanych z podziałami.

Elementy podstaw do wyznaczania przestrzeni walki informacyjnej można również znaleźć w obowiązujących zasadach wydzielania rodzajów wojsk. Mówi się tam[22], że rodzajem wojsk powinno się nazywać taki zbiór elementów (oddziałów, pododdziałów i innych komórek organizacyjnych), które odróżniają się od innych specyfiką podstawowego:

1) uzbrojenia;

2) wyposażenia technicznego;

3) systemu organizacyjnego;

4) szkolenia;

---

[21] 204. K. Kuratowski, A. Mostowski: *„Teoria mnogości”*. PWN, Warszawa 1978, s.255.J. Słupecki, K. Hałkowska, K. Piróg – Rzepecka: *„Logika i teoria mnogości”*, PWN, Warszawa 1994, s.204.
Z. Ziembiński: „Logika praktyczna”. PWN, Warszaw 1994, s.58.

[22] Leksykon wiedzy wojskowej, wyd. MON, Warszawa 1979, s. 369.

5) sposobu działania na polu walki.

Można więc powiedzieć, że każdy rodzaj wojsk jest zbiorem elementów wyróżnionych ze względu na cechy szczególne zawarte w uzbrojeniu i wyposażeniu technicznym oraz w szczególnym dla tych wojsk systemie organizacyjnym i szkoleniowym, jak również w szczególnych sposobach ich działania na polu walki.

Pojęcie „walka informacyjna" nie jest oficjalnie wyróżniane w polskiej terminologii wojskowej. Potencjał dostosowany do jej prowadzenia nie jest też traktowany jako odrębny rodzaj wojsk. Nie ulega jednak wątpliwości, że taki występuje w strukturze sił zbrojnych. Istnieją przecież pododdziały, oddziały i komórki organizacyjne, które odróżniają się od innych specyfiką:

1) uzbrojenia;
2) wyposażenia technicznego;
3) struktur organizacyjnych;
4) procedur szkolenia;
5) zasad działania na polu walki.

Potencjał ten, ze względu na to kryterium wyróżnialności (cechę rozstrzygalności) stanowi zbiór pięciu jednorodnych elementów. Według obowiązujących normatywów wojskowych posiada on wszystkie cechy charakterystyczne predestynujące do nazwania go rodzajem wojsk, który dostosowany jest do prowadzenia walki informacyjnej. Zbiór tych elementów można też traktować jako potencjalną przestrzeń walki informacyjnej, ponieważ zawiera elementy, które ze względu na relację porządkującą celu są jednorodne — są dostosowane do prowadzenia walki informacyjnej.

Potencjalna przestrzeń walki informacyjnej, jak już zaznaczano wcześniej, nie jest tożsama z przestrzenią walki informacyjnej. Ta pierwsza zawiera w sobie tylko elementy, które decydują o możliwościach prowadzenia walki informacyjnej — zawiera w sobie tylko pewien potencjał, który dopiero w konkretnym działaniu może zmaterializować się jako określona siła walki. Ta druga natomiast — przestrzeń walki informacyjnej — zawiera w sobie elementy walki dynamicznej ukierunkowanej na: zdobywanie informacji, zakłócanie informacyjne i obronę informacyjną. Innymi słowy, w potencjalnej przestrzeni walki informacyjnej nie funkcjonują jeszcze mechanizmy kooperacji negatywnej wzajemnej, natomiast w przestrzeni walki informacyjnej mechanizmy te funkcjonują.

Wyznaczanie podprzestrzeni walki informacyjnej wiąże się z porządkowaniem zbioru. Proces ten powinien prowadzić do takiego rozwiązania, w którym na ostatnim poziomie

podziału potencjalnej przestrzeni walki informacyjnej wszystkie jej elementy (uzbrojenie, wyposażenie techniczne, struktura organizacyjna, procedura szkolenia i zasady działania), ze względu na relację porządkującą celu odnoszącą się do dostosowania, będą już niepodzielne. Tylko wtedy można powiedzieć, że potencjalna przestrzeń walki informacyjnej została uporządkowana do końca. 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 $\mathcal{R}$:

$$\wedge_i \wedge_j \overline{x \quad \Re \quad y}$$

— relacja przechodniości — jeśli element x pozostaje w relacji $\mathcal{R}$ do y oraz element y w relacji $\mathcal{R}$ do z, to x pozostaje w relacji $\mathcal{R}$ 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 $\mathcal{R}$ do y, albo y w relacji $\mathcal{R}$ 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 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 w pierwszej kolejności 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 równoznaczne z dobrym uporządkowaniem (podziałem) zbioru pełnego (potencjalnej przestrzeni walki informacyjnej).

Przestrzeń walki 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.

Walka może być zatem prowadzona różnymi układami skoordynowanych elementów, tzn. w różnych formach[23]*. Jeśli układy skoordynowanych elementów dostosowane będą do fizycznego niszczenia przeciwnika, wówczas można mówić, że walka prowadzona jest w formie zbrojnej. Jeśli natomiast nie, wówczas można mówić, że walka prowadzona jest w formie niezbrojnej. Z powyższego wynika więc, że pierwszy podział przestrzeni walki powinien być dokonany w oparciu o rozstrzygalność wynikającą z kryterium formy, tzn. w oparciu o identyfikowanie dostosowania układu skoordynowanych elementów.*

Zatem, ze względu na kryterium formy, przestrzeń walki należy dzielić na przestrzeń walki zbrojnej i przestrzeń walki niezbrojnej.

Kolejne poziomy podziału powinny być wyznaczone przez kryterium środowiska W następstwie tego można wyróżniać:

1. W przestrzeni walki zbrojnej:

— przestrzeń walki lądowej;

— przestrzeń walki powietrznej;

— przestrzeń walki morskiej.

2. W przestrzeni walki niezbrojnej:

— przestrzeń walki politycznej;

— przestrzeń walki ekonomicznej;

— przestrzeń walki ideologicznej itp.

Z powyższych analiz wynika, że walka informacyjna ze względu na kryterium formy i środowiska mieści się w przestrzeni walki niezbrojnej (rys. 1.5.7).

Przyjmując tak ulokowaną walkę informacyjną za pierwotny przedmiot podziału, można powiedzieć, że stanowi zbiór pełny $\{A_{(1)}\}$ wszelkich układów skoordynowanych elementów dostosowanych do prowadzenia tej walki i zespołów wszelkich czynników oddziałujących informacyjnie na te układy.

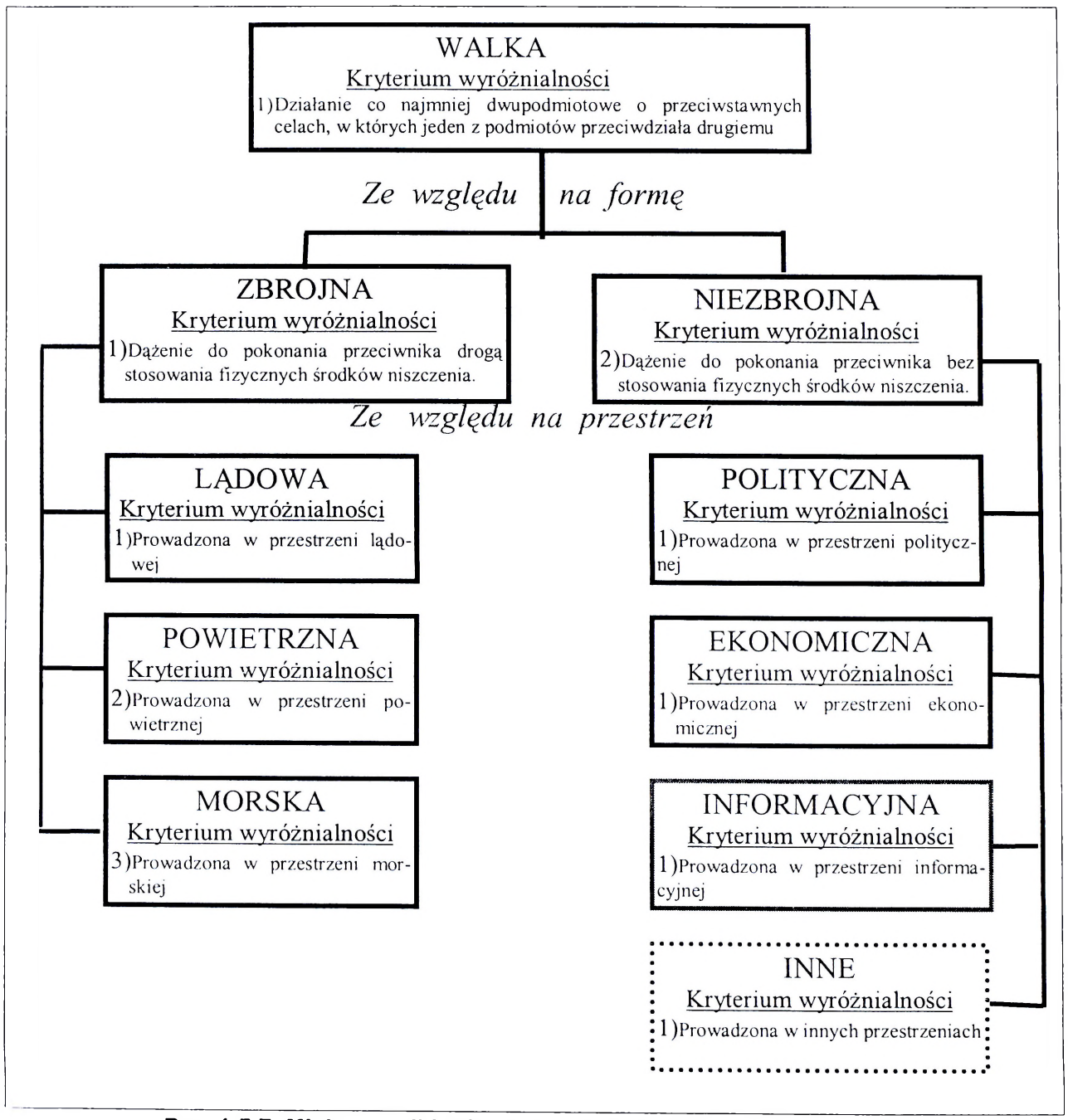
Zatem pierwotną cechą wyróżnialności jest dostosowanie formy układu skoordynowanych elementów do prowadzenia walki w środowisku informacyjnym. Nie jest to jednak równoznaczne z interpretowaniem zbioru $\{A_{(1)}\}$ jako skończonego[24], tzn. o raz na

---

[23]Forma to zewnętrzny kształt, postać, wygląd czego; *układ skoordynowanych elementów*; sposób postępowania. Słownik języka polskiego, t 1, PWN, Warszawa 1979, s. 602.

[24]Zbiór skończony – zbiór o skończonej liczbie elementów.

zawsze ustalonej mocy[25]— 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



Rys. 1.5.7. Miejsce walki informacyjnej w ogólnej przestrzeni walki

w składzie walki informacyjnej, a które są dziś trudne, a nawet niemożliwe do dokładniejszego ustalenia. Dlatego też przestrzeń tę należy traktować jako zbiór skończony,

[25]Moc zbioru – liczba elementów zbioru skończonego lub jego liczba kardynalna dla zbiorów skończonych i nieskończonych.

ale tylko w aspekcie teraźniejszości. Co do przyszłości należy ją widzieć jako zbiór nieskończony[26], rozwijający się w rytm postępu naukowego i technologicznego.

Niezależnie jednak od liczby i rodzajów pojawiania się nowych elementów zbioru[27], *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 $\{A_{(1)}\}$, *to znaczy podziału przestrzeni walki informacyjnej.*

Cel zasadniczego podziału przestrzeni walki informacyjnej, 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 w ogóle o wyróżnianiu tego rodzaju potencjału jako odrębnego zbioru pełnego w strukturze w wojsk. Wszystkie inne podziały, nie podporządkowane 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;*

---

[26]Zbiór nieskończony – zbiór o nieskończonej liczbie elementów.
[27]Element zbioru – dowolnie wyróżniony obiekt rzeczywisty czy też myślowy.

— *kryteriów naboru stanu osobowego;*

— *procesu przygotowywania kadr i szkolenia wojsk.*

Jak już stwierdzono dotychczas, zasadnicze cechy wyróżnialności (kryteria rozstrzygalności) wynikają z dostosowania skoordynowanych elementów, czyli z dostosowania danych form do prowadzenia walki informacyjnej. 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 walki informacyjnej (wynikające z ogólnego kształtu, który określa formę konkretnego działania w walce informacyjnej). Kolejnymi są dopiero cechy określające środowisko walki informacyjnej, czyli zespoły czynników, które będą oddziaływać na układy skoordynowanych elementów tej walki – będą oddziaływać na konkretne formy podejmowanych działań. Innymi słowy pierwsza cecha wyróżnialności (kryterium rozstrzygalności) winna dawać odpowiedź na pytanie: *W jakiej formie działań odbywać się będzie realizacja celów walki informacyjnej?* Druga natomiast winna odpowiadać: *W jakim środowisku informacyjnym realizowane będą konkretne działania?*

Pierwszą cechą wyróżnialności, wynikającą z przeznaczenia, jest dostosowanie potencjału do prowadzenia walki informacyjnej. Wszystkie elementy przystosowane do tego tworzą zbiór pełny $\{A_{(1)}\}$, zwany przestrzenią walki informacyjnej, który ze względu na tę cechę jest zbiorem jednorodnym.

Walka informacyjna, tak jak i walka zbrojna, nie jest przedsięwzięciem jednorodnym. W jej 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 walki informacyjnej na trzy podprzestrzenie (podzbiory), w których zgrupowane będą wszystkie układy skoordynowanych elementów dostosowane do realizacji wyżej wymienionych zadań. Zatem zbiór podstawowy $\{A_{(1)}\}$ w pierwszej kolejności 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 „walka informacyjna";

— spełnia warunek „zupełności" — walka informacyjna, jako dwupodmiotowa kooperacja negatywna wzajemna, w której 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 „walką informacyjną";

— spełnia warunek „rozłączności" — żaden element skoordynowanego układu zdobywania informacji (rozpoznania) nie spełnia ani funkcji zakłócania informacyjnego, ani funkcji obrony informacyjnej.

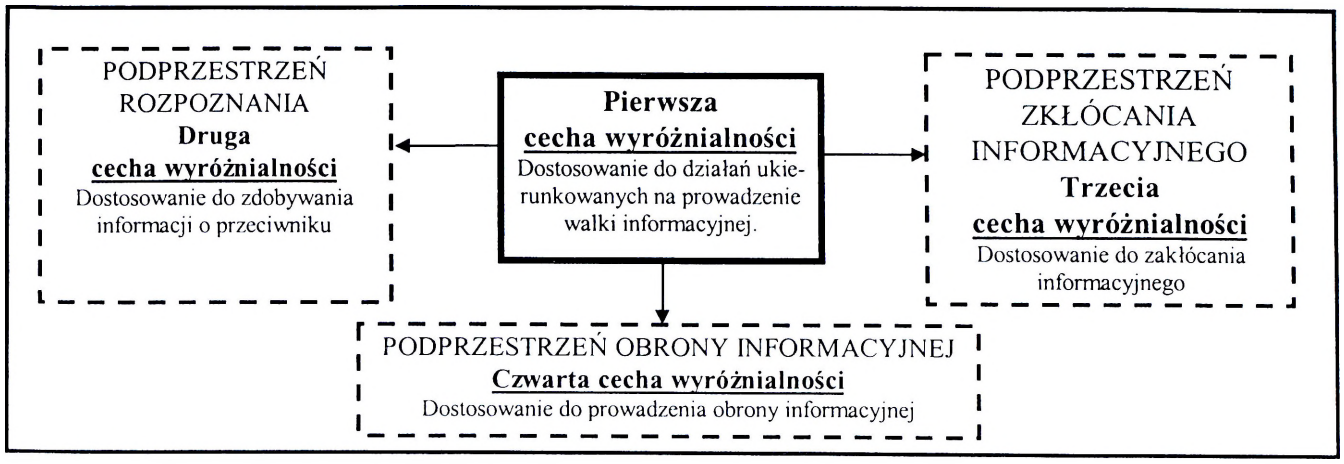
Z powyższego wynika, że w ogólnej przestrzeni walki informacyjnej, ze względu na kryterium formy, należy najpierw wyróżnić:

— przestrzeń, w której walka się toczy o zdobywanie informacji o przeciwniku (przestrzeń rozpoznania) — w przestrzeni tej rozpoznanie kooperuje negatywnie wzajemnie (prowadzi walkę) z zakłócaniem informacyjnym i obroną informacyjną;

— przestrzeń, w której walka toczy się o zakłócanie procesów informacyjnych przeciwnika (przestrzeń zakłócania informacyjnego) — w przestrzeni tej zakłócanie informacyjne kooperuje negatywnie wzajemnie (prowadzi walkę) z rozpoznaniem i obroną przeciwnika;

— przestrzeń, w której walka toczy się o obronę własnych informacji i procesów informacyjnych przed rozpoznaniem i zakłócaniem stosowanym przez przeciwnika (przestrzeń obrony informacyjnej).

Można zatem powiedzieć, że ze względu na kryterium formy walka informacyjna dzieli się na: rozpoznanie, zakłócanie i obronę informacyjną (rys. 1.5.8).



Rys. 1.5.8. Przestrzeń walki informacyjnej po pierwszym podziale na rodzaje walki informacyjnej

1.5.1. Przestrzeń zdobywania informacji (rozpoznania)

Rozpoznanie wojskowe jest immanentnym elementem systemu informacyjno-sterującego i ma już utrwalone miejsce w naszych siłach zbrojnych. Jego przedmiotem 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 walkę informacyjną.

Już od najdawniejszych czasów odpowiednio wczesne uzyskiwanie danych 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. Tego rodzaju informacje są trudne do zdobycia: nie są z pewnością dojrzałymi owocami do zerwania z drzewa; najczęściej muszą być wyrwane przeciwnikowi. W każdej sytuacji są one niezbędne do pokonania przeciwnika i osiągnięcia zwycięstwa. Dlatego też każdy dowódca musi zachowywać gotowość do prowadzenia rozpoznania i gromadzenia informacji o przeciwniku.

Wśród specjalistów wojskowych państw NATO dominuje pogląd, że walka zbrojna zawsze wymuszała, a w przyszłości będzie także narzucać, konieczność uzyskiwania precyzyjnych, wiarygodnych i aktualnych informacji o przeciwniku (o jego możliwościach, zamiarach i działaniach), terenie itd., bez których posiadania niemożliwe byłoby skuteczne kierowanie działalnością wojsk. Potrzeba zdobywania tych informacji stała się głównym stymulatorem wyróżnienia odrębnej specjalności w działalności wojsk, jaką jest rozpoznanie.

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.

Dotychczas osiągnięcia technologiczne wykorzystywane były przede wszystkim w celu zwiększenia siły uderzeniowej wojsk i środków rażenia. Obecnie dzięki zautomatyzowanym systemom dowodzenia i kierowania środkami walki (bazującymi na ciągłym i szybkim dostępie dowództw i sztabów do aktualnych informacji), osiągnięcia technologiczne wykorzystuje się w celu skoordynowania i uelastycznienia działań zbrojnych. Teoretycy wojskowi przewidują, że przyszła wojna może przebiegać według scenariuszy podobnych do dzisiejszych wojennych filmów fantastycznych. Jest prawdopodobne, że przywódcy zwaśnionych stron będą prowadzić wirtualne wojny zanim zdecydują się w ogóle na podjęcie jakichkolwiek działań. Niektórzy futuryści w swoich przewidywaniach idą jeszcze dalej. Zakładają, że państwa będą toczyły symulowane wojny zamiast faktycznych bitew, a wojna będzie *grą wideo* bez konieczności zadawania bólu ludziom.

W takiej sytuacji słuszna wydaje się teza, że „informacja" stanie się czynnikiem kluczowym na przyszłym polu walki. Aby zwyciężyć należy wygrać walkę informacyjną. Bez względu na charakter przyszłej wojny, szybkie i sprawne zdobywanie (pozyskiwanie) dokładnych informacji o przeciwniku będzie w decydujący sposób wpływało na jej przebieg oraz rezultat.

Współczesna walka zbrojna dostarcza ogromnych ilości danych o przeciwniku, których zdobywaniem, opracowywaniem oraz szeroko pojętą dystrybucją zajmują się wyspecjalizowane komórki sztabowe wraz z podległymi im organami rozpoznawczymi. Tworzą one część systemu informacyjno-sterującego wojsk, w którym zarówno źródła informacji, jak i układy odbierające dostosowane są nie tylko do spełniania swej roli w przestrzeni widma elektromagnetycznego. Dostosowywane są również do funkcjonowania w przestrzeni fal sprężystych, efektów magnetycznych i efektów chemicznych, przez pryzmat czego również możliwe jest identyfikowanie stanu aktualnego pola walki.

Celem pozyskiwania danych nie jest to, aby wszystko było wiadome, lecz to, aby wiedzieć wystarczająco dużo, a przede wszystkim więcej niż przeciwnik. Przy czym często wystarczy, aby istotne informacje uzyskiwać wcześniej od innych. Niekiedy mówi się o tzw.

„wyprzedzeniu informacyjnym", które jest najczęściej równoznaczne z *posiadaniem przewagi czasowej,* natomiast rzadko oznacza nadwyżkę danych.

Z tych też względów proces zdobywania danych powinien być wyjątkowo starannie organizowany. W procesie tym należy kierować się następującymi zasadami:

— *dane powinny być zdobywane przez źródła charakteryzujące się wysokim stopniem wiarygodności;*

— *powinny być przekazane w ciągu określonego granicznego czasu, a docelowo — w czasie rzeczywistym;*

— *zdobywanie danych powinno być starannie zaplanowane i organizowane z możliwie dużym wyprzedzeniem czasowym;*

— *dystrybucja danych i komunikatów musi być tak zorganizowana, aby do użytkowników dotarły ich wiarygodne postacie, we właściwym czasie i miejscu;*

— *powinno się prowadzić redukcję i kompresję danych w celu dopasowania ich ilości do potrzeb odpowiednich szczebli dowodzenia i sprawności ich systemów przetwarzania, a także zapobieganie tworzeniu się tzw. „wąskich gardeł" przy przekazywaniu. Należy jednak mieć na uwadze, by ilość danych nie była w żadnym wypadku „obcinana" automatycznie oraz dostosowywana do możliwości (pojemności) środków ich przekazywania i przetwarzania.*

Analizując właściwości danych i wymagania stawiane przy ich pozyskiwaniu z wojskowego punku widzenia można zauważyć, że:

- Bardzo często występuje tendencja do tego, aby wiedzieć możliwie dużo lub w ogóle wszystko wiedzieć. W związku z tym w wojskowych systemach wymiany danych i komunikatów często w obiegu występuje znacznie więcej ich postaci niż jest to potrzebne. W praktyce należy taką tendencję ograniczać, ponieważ może doprowadzić do wywołania takiego napływu danych, iż zostanie zablokowany proces decyzyjny — istota tego zagrożenia wynika z reguł teorii masowej obsługi.
- Najczęściej występuje brak tych danych, które są w określonej chwili potrzebne. Aby się tego ustrzec, w planie zdobywania informacji należy uwzględniać nie tylko siły i środki, lecz również obszar (względnie odległości), potrzeby czasowe oraz wydajność systemów dystrybucji deanych.
- W systemie informacyjnym znajduje się nadmiar danych, których jednak w pewnej chwili nie można wykorzystać. Z reguły wynika to z braku czasu na ich opracowanie i przekazanie.

- Wiele posiadanych danych dezaktualizuje się, zanim zostaną przez kogokolwiek wykorzystane.

Z przedstawionych rozważań wynika, że 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.

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.

Budując bazy danych o siłach i środkach przeciwnika należy mieć na uwadze, iż ich przepływ do różnych szczebli dowodzenia, komórek sztabowych, organów rodzajów wojsk i osób funkcyjnych winien być ujęty w sprawnie działający system informacyjno — sterujący, organizowany i koordynowany przez szczebel nadrzędny.

Orientacja dowódcy, co do sytuacji na polu walki, wymaga zdobywania, przetwarzania i gromadzenia dużych ilości danych, gdyż trudno przewidzieć, jakiego rodzaju ich postacie będą potrzebne w konkretnej sytuacji, wykonywanym zadaniu bojowym lub przewidywaniu zdarzeń. Dlatego też rozpoznanie na przyszłym polu walki będzie odgrywać ważną rolę, jest zawsze bowiem procesem pierwotnym w stosunku do zakłócania i obrony informacyjnej.

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[28] i wielospektralnego[29] 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, które można nazywać bezpośrednim (wg terminologii natowskiej HUMINT — Human Intelligence);

— rozpoznanie nieosobowe (można je nazywać technicznym lub pośrednim ze względu na to, że jest realizowane głównie przy wykorzystaniu urządzeń technicznych).

Przestrzeń rozpoznania osobowego (bezpośredniego) 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. 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

---

[28]Przyjęto, że postrzeganie wielofunkcyjne to dostosowanie do zbierania informacji w różnych technikach – w różnych przestrzeniach informacyjnych.

[29]Postrzeganie wielospektralne to dostosowanie do jednoczesnego zbierania informacji w kilku różnych zakresach widma elektromagnetycznego.

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.

A zatem przestrzeń rozpoznania bezpośredniego należy dzielić na podprzestrzenie:

— rozpoznania agenturalnego;

— rozpoznania patrolowego;

— rozpoznania specjalnego.

Rozpoznanie agenturalne jest przystosowane do zdobywania i przetwarzania informacji o przeciwniku drogą ściśle zakonspirowanych działań wywiadowczych. Pozyskiwane przez rozpoznanie agenturalne informacje o siłach i środkach przeciwnika mają bardzo dużą wartość rozpoznawczą. Są to z reguły informacje o znaczeniu strategicznym i mogą dotyczyć m.in.:

— możliwości wybuchu wojny i jej charakteru;

— terminów osiągania pełnej gotowości bojowej wojsk potencjalnego przeciwnika;

— dokładnych współrzędnych rejonów rozmieszczenia wojsk przeciwnika oraz jego środków ogniowych (stanowisk startowych rakiet operacyjno-taktycznych, lotnisk, magazynów amunicji, itp.);

— funkcjonowania systemów dowodzenia, węzłów łączności oraz zabezpieczenia bojowego i logistycznego działań;

— przedsięwzięć mobilizacyjnych oraz przerzutu wojsk z innych terytoriów (regionów);

— stanu lotnictwa taktycznego;

— rozbudowy infrastruktury oraz nowych obiektów;

— sytuacji ekonomicznej oraz stopnia zaangażowania gospodarki narodowej dla celów wojennych;

— nastrojów w społeczeństwie oraz poziomu dyscypliny w siłach zbrojnych.

Rozpoznanie specjalne ma na celu prowadzenie działań rozpoznawczych siłami niewielkich grup lub pododdziałów na terenie zajmowanym przez przeciwnika i zdobywanie o nim danych. Grupy specjalne działają zwykle na tych obszarach przeciwnika, które nie są pokryte innymi rodzajami rozpoznania. Doświadczenia wojen lokalnych wskazują na wzrost znaczenia tego rozpoznania. Głębokość usytuowania obszarów rozpoznania specjalnego może być różna, ale zawsze warunkowana jest możliwościami przerzutu (przenikania) i przetrwania elementów rozpoznawczych. Siły i środki rozpoznania specjalnego mogą pozyskiwać bądź potwierdzać dane zdobyte przy pomocy innych źródeł, bez względu na warunki (pogodę, porę roku, doby, itp.) i stopień zamaskowania obiektów. Są one w stanie określić rodzaj, charakter, stan i gotowość bojową przeciwnika, a nade wszystko określić dokładne współrzędne wykrywanych obiektów. W konkretnej sytuacji pola walki pozyskiwane przez rozpoznanie specjalne informacje o siłach i środkach przeciwnika mogą dotyczyć:

— ważnych środków ogniowych przeciwnika, ich systemów kierowania, składów i punktów amunicji specjalnej oraz symptomów świadczących o przygotowaniu do ich użycia;
— składu i rozmieszczenia systemów dowodzenia i węzłów łączności,
— rozmieszczenia środków rozpoznania radioelektronicznego, powiadamiania i naprowadzania;
— urządzeń i obiektów obrony przeciwlotniczej i przeciwrakietowej;
— rejonów ześrodkowania wojsk oraz kierunków ich przegrupowania;
— rozmieszczenia lotnisk, lądowisk, portów, baz morskich, obiektów obrony wybrzeża oraz urządzeń zabezpieczających ich funkcjonowanie;
— danych o obiektach komunikacyjnych oraz systemach logistycznego zabezpieczenia wojsk;
— danych o systemach zapór inżynieryjnych, szerokich przeszkodach wodnych, stanie urządzeń hydrotechnicznych, itp.;
— form i zasad oddziaływania propagandowego i psychologicznego w stosunku do wojsk i ludności cywilnej.

Rozpoznanie patrolowe może zdobywać dane o przeciwniku drogą fizycznej (optycznej i akustycznej) penetracji terenu (obszaru) zajmowanego przez przeciwnika. Rozpoznanie patrolowe prowadzą nie tylko etatowe siły i środki, ale i inne rodzaje wojsk, stosownie do potrzeb oraz posiadanych możliwości.

Przestrzeń rozpoznania technicznego (pośredniego) 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 (tab. 1.5.1.1).

Biorąc pod uwagę powyższe kryterium (środowisko nośników danych) i treści zawarte w tab. 1.5.1.1. przestrzeń rozpoznania pośredniego można podzielić na:

— podprzestrzeń rozpoznania elektromagnetycznego (wg NATO SIGINT — Signal Intelligence, zdobywanie danych na podstawie emisji elektromagnetycznej obcych systemów elektronicznych);

— podprzestrzeń rozpoznania czujnikowego (zdobywanie danych na podstawie identyfikowania przeróżnych stanów w środowisku akustycznym, elektrycznym, magnetycznym i chemicznym);

— podprzestrzeń rozpoznania informatycznego (dane w systemach komputerowych).

Tab. 1.5.1.1.

Parametry / Środowisko	Częstotliwość (Hz)	Długość fali	Otrzymane dane	Urządzenie rozpoznawcze
γ	$10^{21} \div 3x10^{19}$	0,5 ÷ 10 pm	Ilość impulsów w postaci	Scyntylator
X	$3x10^{19} \div 3x10^{16}$	10 pm ÷ 10 nm	numerycznej lub graficznej	Scyntylator, materiały światłocz.
UV	$3x10^{16} \div 8x10^{14}$	10nm ÷380nm	Wykres, zdjęcia lub zobrazowanie	Fotopowielacze, materiały światłocz.
W	$8x10^{14} \div 4x10^{14}$	380nm ÷760nm	Zdjęcia, obraz TV, krzywe spektralne	Fotopowielacze, materiały światłocz.
IR	$4x10^{14} \div 5x10^{11}$	760nm ÷600μm	Zdjęcia do 1,2 μm obraz TV, sygn. elektr.	Do 1,2 μm – materiały fotograficz. z lin. Wyb.
Mikrofale	$5x10^{11} \div 6x10^{8}$	600μm ÷50 cm	Sygnał, wykres, zobrazowanie	Stacje radiolokacyjne
Fale radiowe	$6x10^{8} \div 3x10^{5}$	50 cm ÷ 1 km	Sygnał radiowy, zobrazowanie	Odbiorniki, namierniki radiowe
Akustyczne	$10x10^{8}$	33 m. ÷ 3,3 m	Wykresy, sygnały elektryczne	Rejestratory drgań mechanicznych
Elektryczne	-	-	Wykresy, sygnały elektryczne	Wskaźniki prądowe – rejestratory
Magnetyczne	-	-	Wykresy, sygnały	Rejestratory natężenia pola magnetycznego
Chemiczne	-	-	Wykresy, zdjęcia, zobrazowania,	Analizator, fotoelementy, spektrofotometry

Powyższy podział jest właściwy, obejmuje bowiem całą przestrzeń, w której można zdobywać dane o przeciwniku, i tak:

— rozpoznanie elektromagnetyczne charakteryzuje się długościami fal zawartymi w przedziale od 0,5pm do 1 km. Przy takiej kategoryzacji można w nim wyróżniać wszystkie znane dziś techniki zdobywania danych w tej przestrzeni;

— rozpoznanie czujnikowe może zdobywać oraz przetwarzać dane o przeciwniku, których nośnikami są fale sprężyste (infradźwięki[30], ultradźwięki[31]) oraz wszelkiego rodzaju uboczne efekty towarzyszące działaniom bojowym, na przykład: akustyczne, sejsmiczne, magnetyczne, chemiczne, zapachowe itp.;

— rozpoznanie informatyczne[32] powinno być natomiast prowadzone z uwagi na masowy rozwój sieci informatycznych, które są bogatymi źródłami danych o siłach i środkach przeciwnika.

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;

---

[30]Infradźwięki – fale sprężyste o częstotliwościach mniejszych niż 16 Hz, w więc leżące poniżej zakresu ludzkiej słyszalności. Fale te są słabo tłumione i dlatego rozprzestrzeniają się na duże odległości od źródła. Mogą być wykorzystane do rejestracji efektów sejsmicznych oraz eksplozji na polu walki.

[31]Ultradźwięki – drgania i fale sprężyste o częstotliwościach większych iż 20 kHz, a więc leżące powyżej zakresu ludzkiej słyszalności. Mogą być wykorzystane do rejestracji efektów akustycznych (odgłosów) pola walki.

[32]W USA jest jednym z elementów walki informacyjnej.

— rozpoznania radiolokacyjnego;

— rozpoznania optoelektronicznego.

Rozpoznanie radiowe ma na celu zdobywanie danych o przeciwniku, których nośnikami są fale elektromagnetyczne wykorzystywane przez radiostacje KF — UKF, środki łączności satelitarnej, radioliniowej i innej.

Rozpoznanie radiolokacyjne[33] jest prowadzone za pomocą stacji radiolokacyjnych, które służą do wykrywania powietrznych, naziemnych i nawodnych celów ruchomych i nieruchomych. Określają ich bieżące współrzędne, kierunek oraz prędkość ruchu na podstawie zdobytych i przetworzonych informacji o przeciwniku, których nośnikami są fale elektromagnetyczne. Współczesne rozpoznanie radiolokacyjne obejmuje: systemy rozpoznania obszaru powietrznego, systemy nadzorowania pola walki, systemy kierowania ogniem, systemy obrony przeciwlotniczej, systemy rozpoznania powierzchni ziemi SLAR i in. Prowadzone jest przez samoloty rozpoznawcze wyposażone w stacje radiolokacyjne obserwacji bocznej oraz naziemne, brzegowe, okrętowe stacje radiolokacyjne w różnych zakresach częstotliwości. Dane pozyskiwane przez te urządzenia w kontekście budowy baz danych powinny dotyczyć:

— radiolokacyjnych obrazów odpowiednich sektorów przestrzeni powietrznej, terenu (lądu) oraz akwenów morskich,

— tras przelotu samolotów oraz miejsc rozmieszczenia celów ruchomych (czołgów, transporterów opancerzonych, samochodów, pododdziałów oraz pojedynczych żołnierzy w warunkach braku widoczności (noc, mgła, opady atmosferyczne, zadymienie, kurz) itp.,

— współrzędnych tych celów.

Rozpoznanie optoelektroniczne ma na celu zdobywanie oraz przetwarzanie tych informacji o przeciwniku, których nośnikami są fale elektromagnetyczne pasma optycznego[34]. Do pracy w tym paśmie skonstruowano całą rodzinę urządzeń optoelektronicznych[35], pozwalających na prowadzenie rozpoznania w ultrafiolecie, w zakresie promieniowania widzialnego oraz w zakresie bliskiej, średniej, dalekiej i skrajnej podczerwieni.

---

[33]Pasywne, jeżeli stacje radiolokacyjne przechwytują fale elektromagnetyczne, same zaś nie promieniują energii. Aktywne, jeżeli są dostosowane do zdobywania i przetwarzania tylko tych informacji, których postacie stanowią skuteczne powierzchnie odbicia własnej energii elektromagnetycznej od różnych obiektów przeciwnika.

[34]Pasmo optyczne (zakres optyczny) widma elektromagnetycznego stanowią promieniowania: ultrafioletowe (długość fali: 0,01 – 0,38μm), widzialne (długość fali: 0,38 – 0,76μm) i podczerwone (długość fali: 0,76 – 1000μm).

[35]Optoelektronika – to dział elektroniki, którego przedmiotem jest łączne wykorzystanie optycznego i elektrycznego sposobu przetwarzania i przekazywania sygnałów. Podstawą optoelektroniki są fizyczne procesy warunkujące przetwarzanie sygnałów elektrycznych na optyczne i sygnałów optycznych na elektryczne oraz procesy wytwarzania, przesyłania, przetwarzania i magazynowania informacji niesionych przez światło.

Wykorzystywane są tutaj wszelkiego rodzaju urządzenia: telewizyjne[36], termowizyjne[37], noktowizyjne[38] oraz laserowe[39]. Budując komputerowe bazy danych o siłach i środkach przeciwnika należy mieć na uwadze, że informacje pozyskiwane w wyniku rozpoznania optoelektronicznego mają charakter obrazowy. Mogą zatem być szeroko wykorzystywane do monitorowania pola walki, a w tym funkcjonowania sił i środków przeciwnika.

Rozpoznanie czujnikowe dostosowane jest do postrzegania materii pola walki przez pryzmat fal sprężystych oraz w zakresie efektów magnetycznych i chemicznych środowiska. Konstruowane urządzenia pracują z szerokim zastosowaniem elektronicznej przemiany rejestrowanych efektów. Dane o siłach i środkach przeciwnika pozyskiwane w wyniku prowadzonego rozpoznania czujnikowego mogą dotyczyć:

— nadzorowania aktywności przeciwnika w wybranych rejonach, w których rozmieszczone zostały odpowiednie czujniki;

— nadzorowania natężenia ruchu i poziomu aktywności przeciwnika wzdłuż wybranych tras;

— nadzorowania aktywności przeciwnika w rejonach rozmieszczenia własnych zapór i pól minowych;

— nadzorowania aktywności przeciwnika w rejonach przepraw rzecznych, mostów i brodów;

— nadzorowania rejonów zaplanowanych jako strefy lądowania lub zrzutu własnych wojsk desantowo — szturmowych;

— rejestracji zmian w funkcjonowaniu wybranych elementów ugrupowania przeciwnika, ich stanowisk dowodzenia, punktów zaopatrywania, itp.;

— wskazywania celów.

---

[36]Telewizja to dział telekomunikacji zajmujący się przekazywaniem na odległość, za pomocą elektrycznego kanału łączności, obrazów ruchomych wraz z towarzyszącym dźwiękiem. W celu przetworzenia obrazu optycznego na sygnał elektryczny wykorzystuje się zjawisko fotoelektryczne, natomiast dla odwrotnego przetworzenia wykorzystuje się zjawisko katodoluminescencji.

[37]Termowizja – to postrzeganie obrazów w widmie promieniowania podczerwonego (aktualnie wykorzystywane są tylko dwa pasma tego widma: 3 – 5μm i 10 – 13μm). Termowizja, w istocie wykorzystywanego zjawiska, podobna jest do noktowizji pasywnej. Różnica polega tylko na tym, że termowizja posiada jeszcze urządzenie skanujące zamieniające obraz widziany w podczerwieni na ciąg impulsów elektrycznych (noktowizor pasywny z urządzeniem skanującym można nazywać termowizorem).

[38]Noktowizja to dziedzina zastosowań techniki optoelektronicznej umożliwiającej widzenie w widmie promieniowania o długości 0,76 – 1000μm. Zakres ten podzielono na podczerwień bliską 0,76 – 1,5μm, średnią 1,5 5,6μm i daleką 5,6 – 1000μm – w dolnym paśmie podczerwieni dalekiej wyróżniany jest również zakres zwany podczerwienią skrajną). Obserwacja różnych obiektów w podczerwieni może być realizowana przez wykorzystywanie ich promieniowania własnego (wszystkie ciała, których temperatura jest wyższa od zera bezwzględnego, wysyłają własne niekoherentne promieniowanie podczerwone) lub odbitego. W związku z tym przyrządy noktowizyjne dzieli się na pasywne i aktywne.

[39]Laser – to optyczny generator kwantowy lub generator światła spójnego, czy też źródło monochromatycznych fal elektromagnetycznych w zakresie optycznym (promieniowanie monochromatyczne to promieniowanie elektromagnetyczne o ustalonej długości fali). Nazwa lasera została utworzona z liter początkowych słów: Light Amplification by Stimulated Emission of Radiation (wzmacniacz światła z wymuszoną emisją promieniowania).

Rozpoznanie to jest perspektywiczne, szczególnie na szczeblach taktycznych. Umożliwia bowiem pozyskiwanie danych z najbardziej niedostępnych stref [40] w czasie zbliżonym do rzeczywistego.

Rozpoznanie informatyczne ma możliwości stosunkowo łatwego pozyskiwania danych. Poza tym nie wymaga ani skomplikowanych urządzeń ani też specjalistycznego przygotowania załóg. Przykładem w tym zakresie mogą być międzynarodowi piraci komputerowi (ang. *hackers*), którzy bez większych przeszkód włamują się do odpowiednio zabezpieczonych systemów komputerowych m in. Pentagonu. Nie trzeba zatem być wielkim i bogatym, aby skutecznie prowadzić rozpoznanie informatyczne. *Przebogate i niezmiernie wartościowe dane dla rozpoznania ulokowane są również w promieniowaniu komputerowym.* Te nowe stosunkowo źródła są jeszcze mało dostępne dla organów rozpoznawczych naszych sił zbrojnych. Należy jednak uczynić wszystko, aby barierę tę jak najszybciej pokonać od strony technologicznej i organizacyjnej.

Budując bazy danych o przeciwniku, należy mieć na uwadze, że podejmowanie trafnych decyzji na polu walki zawsze wymuszało, a w przyszłości będzie także narzucać, konieczność pozyskiwania precyzyjnych, wiarygodnych oraz aktualnych danych. Potrzeba taka stała się głównym stymulatorem postępu w dziedzinie rozpoznania wojskowego.

Współczesny system rozpoznania wojskowego SZ RP powinien być w pełni zintegrowany i zautomatyzowany. Jego strukturą podstawową powinny tworzyć:

— *podsystem stacjonarny;*

— *i podsystemy mobilne.*

W okresie 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.

---

[40] W przyszłości mogą być wysyłane w powietrze lub rozmieszczane na lądzie tysiące maleńkich czujników. Miniaturowe czujniki zapachu mogą nawet wyczuć przeciwnika, bowiem unoszące się w powietrzu biosensory będą mogły śledzić żołnierzy na podstawie ich oddechów lub potu.

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. Mobilne podsystemy powinny:

— *dostarczać dane w odpowiednim czasie i zakresie, zależnie od szczebla, dla którego są przeznaczone;*

— *czerpać dane z innych systemów rozpoznania;*

— *określać przeznaczenie bojowe różnych obiektów i identyfikować cele;*

— *stanowić bazę do prowadzenia WRE przez gromadzenie danych niezbędnych do zakłócania i mylenia.*

Współczesne pole walki stawia przed rozpoznaniem nowe 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 mniejszych, szybko rozwijanych zestawów antenowych;*

— *integrację urządzeń rozpoznania radioelektronicznego z czujnikami różnych typów.*

W skład mobilnych podsystemów powinny wchodzić następujące środki:

— *bezzałogowe samoloty rozpoznawcze (BSR) dalekiego, średniego i bliskiego zasięgu, dostosowane do zdobywania informacji w technice telewizyjnej i termowizyjnej, z automatyczną transmisją danych;*

— *stacje radiolokacyjne kierowania ogniem;*

— *polowe radiolokacyjne stacje wykrywania;*

— *akustyczne stacje wykrywania;*

— *kamery termowizyjne z wysięgnikami;*

— *wystrzeliwane zestawy rozpoznania czujnikowego;*

— *śmigłowcowe zestawy rozpoznania radioelektronicznego;*

— *patrolowe elementy rozpoznania osobowego.*

Podsystemy mobilne powinny mieć stworzone warunki do wieloprzestrzennego i terminowego penetrowania stosownych stref odpowiedzialności i zainteresowania wojsk oraz dostarczania do komputerowych baz danych wiarygodnej i terminowej informacji o siłach i środkach przeciwnika. W bazach tych powinny być zawarte zbiory umożliwiające:

— *tworzenie dowolnych kompilacji danych w sytuacjach nieprzewidywanych;*

— *tworzenie prostego „dialogu" z bazą danych w systemie konwersacyjnym (tzn. pytanie — odpowiedź);*

— *graficzne obrazowanie sytuacji;*

— *komputerowe przetwarzanie i dystrybucję informacji w czasie zbliżonym do rzeczywistego.*

1.5.2. Przestrzeń zakłócania informacyjnego

Na polu walki zakłócanie prowadzi się w celu obniżenia efektywności funkcjonalnej systemu informacyjno-sterującego przeciwnika. Szczególne znaczenie w tym zakresie ma niedopuszczenie do wykorzystania przez niego spektrum elektromagnetycznego. Efektem zakłócania jest natomiast utrudnienie zdobywania i przekazywania informacji.

Zakłócanie informacyjne to wszelkie oddziaływanie na otoczenie (obszar zdobywania informacji — rejestratory danych, sygnały będące nośnikami informacji, zbiory danych, programy, biblioteki itp.), które doprowadza do zaniku pożądanych danych lub ich deformacji i przez to wpływa negatywnie na inne procesy pola walki.

System zakłócania informacyjnego spełnia jak gdyby dwie funkcje. Jedną z nich jest szeroko rozumiana pozoracja, wprowadzanie w błąd przeciwnika. Jej celem jest udostępnienie przeciwnikowi takich postaci danych, które po przetworzeniu będą przedstawiać sytuację nierealną, nie mającą nic wspólnego z rzeczywistością. Drugą funkcją jest fizyczna destrukcja danych.

Stosując różne techniki można niszczyć lub uniemożliwić pracę źródłom zdobywania danych, przetwornikom danych i sygnałów oraz układom odbierającym. Można też zmieniać strukturę nośników danych i sygnałów. Innymi słowy, obydwa te sposoby zwiększają stan nieuporządkowania wiedzy o położeniu wojsk, a tym samym zwiększają entropię informacyjną. Jest to proces zróżnicowany zarówno w zakresie obszarów oddziaływania, jak i metod postępowania. W walce zbrojnej proces zakłócania informacyjnego powinien obejmować czas przygotowania się do walki i okres jej prowadzenia. Czas przygotowania się do walki jest stosunkowo długi i charakteryzuje się niewielką dynamiką procesów informacyjnych. Okres walki cechuje się natomiast dynamiką znacznie większą, a zatem zakłócanie informacyjne musi zachowywać podobne proporcje.

Pożądanym rezultatem zakłócania informacyjnego jest maksymalne ograniczenie napływu danych prawdziwych i powodowanie przez to zniekształcenia obrazu pola walki. Ten fałszywy obraz pola walki ma bezpośrednie przełożenie na podejmowanie decyzji oraz działanie środków ogniowych, wykonanie manewru, zaopatrzenie materiałowo - techniczne itp. Zakłócanie informacyjne musi więc uwzględniać sam proces informacyjny, który jest w stosunku do zakłócania pierwotnym.

Procesy informacyjne są bardzo skomplikowane, a ich zakłócanie może być spowodowane nie tylko przez działalność celowo zorganizowaną, ale może również wynikać z niedoskonałości poszczególnych układów. Zakłócanie celowe może być dokonywane w każdym ogniwie procesu informacyjnego, stosownie do potrzeb i możliwości technicznych zakłócania oraz obszaru jego oddziaływania. Najpierw jednak należy zdobyć, odpowiednio wcześnie, informacje o potencjalnym przeciwniku, terenie i panujących tam warunkach. Na polu walki i w jego otoczeniu obiekty podlegające rozpoznaniu mogą zostać zamaskowane i wtedy dla czujników pozornie nie będzie obiektów, które są przez nie wyszukiwane. Ponadto mogą zostać ustawione obiekty fałszywe, które wysyłają identyczne sygnały bodźcowe jak prawdziwe. To może spowodować, że do systemów logicznych (w tym dowódców i sztabów) napłyną dane niepełne i podejmowane na ich podstawie decyzje mogą być błędne.

W warunkach walki zbrojnej potok danych jest przetwarzany przez pojedyncze układy logiczne, takie jak: mózg człowieka, komputer oraz przez układy złożone, jak sztaby i zespoły analityczne. Przy wykorzystywaniu sztucznych układów logicznych, istotny wpływ na ich funkcjonowanie mają programy, według których pracują. W wypadku czynnika ludzkiego — sprawność psychofizyczna.

Zakłócanie informacyjne może być prowadzone przy stosowaniu odpowiedniej techniki i metod postępowania. Najbardziej uniwersalne są środki niszczenia, jednak nie wszystko można niszczyć mając na uwadze realia pola walki. Nie bez znaczenia są także koszty, które powinny być minimalizowane stosownie do osiąganych rezultatów. Warunki te dyktują potrzebę posiadania środków maskowania, pozorowania, obezwładniania elektromagnetycznego (aktywnego i pasywnego), środków umożliwiających ingerencję w systemy komputerowe i banki danych, jak również ludzi przygotowanych do realizacji tych zadań. Ilość oraz proporcje tych środków należy dostosować do realiów pola walki. Metody przygotowania działań w zakresie zakłócania informacyjnego oraz metody użycia sił i środków należy sprowadzać i rozwijać stosownie do zmian zachodzących w sprzęcie

i metodach związanych z procesami informacyjno-sterującymi występującymi w walce zbrojnej.

Wojskowi zawsze próbowali uzyskać potrzebne dane i dzięki nim oddziaływali na przeciwnika aby efektywnie wykorzystać swoje siły zbrojne. Realizowano to dwoma sposobami. Pierwszy z nich polegał na bezpośrednim oddziaływaniu na układ recepcyjny człowieka, co można nazwać *zakłócaniem osobowym (bezpośrednim)*. Drugi sposób był realizowany przez oddziaływanie na urządzenia techniczne, pośrednicząc w przekazywaniu i przetwarzaniu danych, co można nazwać zakłócaniem technicznym (pośrednim).

Bezpośrednie (osobowe) zakłócanie informacyjne to zespół przedsięwzięć polegających na zdobywaniu wiadomości o przeciwniku i rozpowszechnianiu odpowiednich danych w jego wojskach w celu oddziaływania na jego morale (postawy, zachowania) i intencje, aby podjął niekorzystną dla siebie decyzję. Zakłócanie to można podzielić na:

— wprowadzanie w błąd (pozorowanie);

— działania psychologiczne;

Wprowadzanie w błąd to działania prowadzone w celu zmylenia przeciwnika co do zdolności bojowej, morale i intencji sił własnych. Innymi słowy, mają one spowodować, aby dowódca przeciwnika niewłaściwie ocenił sytuację na polu walki i podjął błędną decyzję. Czasami mogą one wprowadzać niepewność wśród dowódców przeciwnika podczas krytycznych warunków działania i powodować, że przeciwnik nie będzie podejmował żadnych działań. Celem wprowadzania w błąd 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 spowodować 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 zauważył przedsięwzięć wprowadzających go w błąd (mylących);

— oceni działania mylące — po analizie — jako prawdziwe;

— podejmie działania przeciwko pozorowanym celom i sytuacjom.

Efekty tego rodzaju zakłócania można zobrazować w postaci błędnego koła, w którym prowadzone jest rozpoznanie nieistniejącego (nierealnego) przeciwnika;

— istnieje zła orientacja w sytuacji na polu walki;

— podejmowane są niewłaściwe (błędne) decyzje;

— prowadzone działania są korzystne dla przeciwnika.

Działania psychologiczne to zespół przedsięwzięć polegających na zdobywaniu danych o przeciwniku i rozpowszechnianiu odpowiednich wiadomości w jego wojskach w celu oddziaływania na postawy i zachowania żołnierzy oraz ludności cywilnej strony przeciwnej. Nazywane są często działaniami propagandowo — psychologicznymi ze względu na środki realizacji (słowo, dźwięk, obraz, gest, ruch czy światło).

Rola działań psychologicznych w walce zbrojnej polega na:

— kształtowaniu niekorzystnej sytuacji politycznej i militarnej do prowadzenia działań bojowych przez przeciwnika;

— stwarzaniu warunków mających wpływ na pomyślny przebieg działań bojowych wojsk własnych;

— bezpośrednim wspieraniu działań bojowych wojsk własnych w szczególnie sprzyjających sytuacjach.

Działania psychologiczne 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.

Jak wykazują doświadczenia z minionych konfliktów zbrojnych, szczególnie wojny w Zatoce Perskiej, działania psychologiczne realizowane ex professo i expedite wydają się być niezmiernie humanitarnym środkiem walki, umożliwiającym osiąganie celów politycznych i militarnych przy niewielkich kosztach rzeczowych i ludzkich. In abstracto oddziaływanie to można porównać do wysoce efektywnych systemów precyzyjnego rażenia.

Z dotychczasowej analizy wynika, że człowiek w dalszym ciągu będzie odgrywał dominującą rolę w walce zbrojnej. W czasie ewentualnego konfliktu zbrojnego, bez względu na jego zakres, szczególnego znaczenia nabiera czynnik psychiczny zarówno wśród uczestników walki, jak i ludności cywilnej. W warunkach dużej dynamiki działań, dążeń

walczących stron do przejęcia inicjatywy, przy nagłych zmianach sytuacji i występowaniu niespodziewanych bodźców wzrokowych i słuchowych, ogromne obciążenie psychiczne i fizyczne żołnierzy będzie zjawiskiem powszechnym. Na przestrzeni dziejów stan psychiki oraz świadomość żołnierzy nigdy nie były obojętne dla wodzów i dowódców.

Pośrednie (techniczne) zakłócanie informacyjne to zespół przedsięwzięć organizacyjnych, wzajemnie powiązanych pod względem celu, czasu i miejsca, umożliwiających skuteczny sposób dezorganizacji pracy i działania różnorodnych środków i systemów przeciwnika. Są to urządzenia dostosowane konstrukcyjnie do rejestrowania stanu określonych efektów, charakterystycznych dla danego środowiska (elektromagnetycznego, akustycznego, magnetycznego, elektrycznego i chemicznego). Realizowane przedsięwzięcia w tym zakresie mogą w znacznym stopniu ograniczyć zakres i możliwości wykorzystania tych urządzeń, a ponadto — mimo że nie powodują bezpośrednich materialnych zniszczeń — w wielu sytuacjach są przyczyną znacznych i często bezpowrotnych strat w ludziach i sprzęcie bojowym przeciwnika.

Ze względu na środowisko (kryterium rozstrzygalności) zakłócanie techniczne można podzielić na:

— *elektromagnetyczne;*

— *czujnikowe;*

— *informatyczne.*

Zakłócanie elektromagnetyczne (electromagnetic jamming) ma na celu zakłócanie tych informacji o przeciwniku, których nośnikami są fale elektromagnetyczne (wraz z informacją w nich zawartą) wypromieniowane przez źródła przeciwnika.

Ze względu na wykorzystywane pasma częstotliwości z zakresu spektrum elektromagnetycznego można wyróżnić:

— *zakłócanie radiowe;*

— *zakłócanie radiolokacyjne;*

— *zakłócanie optoelektroniczne.*

Zakłócenia radiowe to niepożądane fale elektromagnetyczne lub zaburzenia natury elektromagnetycznej wpływające ujemnie na odbiór radiowy przez zniekształcenie sygnałów użytecznych. Dotyczą one radiostacji KF i UKF, środków łączności satelitarnej, radioliniowej i innej.

Zakłócenia radiolokacyjne to niepożądane sygnały, zniekształcające lub zakłócające sygnały użyteczne, stanowiące nośniki informacji w systemach radiolokacyjnych. Ze względu

na sposób powstawania dzielą się na celowe i niezorganizowane (przypadkowe). Zakłócenia celowe wytwarza się za pomocą specjalnych środków i urządzeń technicznych, zaś przypadkowe powstają wskutek odbicia energii elektromagnetycznej od obiektów terenowych (miejscowych), chmur, kropli deszczu lub wskutek promieniowania słonecznego, kosmicznego i z urządzeń przemysłowych. Zalicza się do nich także zakłócenia w postaci szumów własnych odbiornika i zakłócenia wzajemne urządzeń radiotechnicznych, pracujących na zbliżonych częstotliwościach.

Zakłócenia organizowane wytwarza się w celu zmniejszenia efektywności lub całkowitego sparaliżowania pracy systemów radiolokacyjnych. Ze względu na sposób wytwarzania dzieli się je na aktywne i pasywne. Do wytwarzania aktywnych służą z reguły stacje zakłóceń radiolokacyjnych.

Zakłócenia pasywne są wytwarzane w celu wywołania silnych odbić elektromagnetycznych wysłanych przez stacje radiolokacyjne. Służą do tego sztuczne lub rzeczywiste obiekty (dipole i igiełki zakłócające, reflektory rogowe i pułapki radiolokacyjne). Ze względu na szerokość widma i sposób promieniowania energii elektromagnetycznej dzieli się je na: zaporowe, przestrajanie w częstotliwości (quasi — zaporowe), wąskopasmowe, ciągłe i impulsowe. Zakłócenia zaporowe mają widmo częstotliwości wielokrotnie przekraczające pasmo przenoszenia odbiornika. Pozwalają one na jednoczesne zakłócenie wielu stacji radiolokacyjnych pracujących na różnych częstotliwościach. Zakłócenia wąskopasmowe wytwarzane są w wąskim paśmie częstotliwości; są one zwykle skuteczniejsze od zakłóceń zaporowych, ponieważ *de facto* wykorzystuje się ich całą energię, ale w tym wypadku niezbędna jest znajomość dokładnej wartości częstotliwości nośnej stacji radiolokacyjnej. Zakłócenia impulsowe mogą być odzewowe (jednokrotne lub wielokrotne) albo niezależne (nie odzewowe). Ze względu na sposób oddziaływania na zakłócane urządzenia rozróżnia się zakłócenia maskujące i imitujące (dezinformujące). Do pierwszej grupy zalicza się zakłócenia, które utrudniają lub uniemożliwiają wykrycie i obróbkę sygnału użytecznego. Zakłócenia imitujące wprowadzają do zakłócanego systemu nieprawdziwe dane, za ich pomocą można wytworzyć na ekranie wskaźnika stacji radiolokacyjnej zobrazowanie celu na takim azymucie i odległości, gdzie nie ma celów rzeczywistych. Ważnym parametrem zakłóceń jest sposób modulacji sygnału zakłócającego. Obecnie stosuje się zakłócenia z modulacją amplitudy, częstotliwości lub fazy albo najczęściej z modulacją kombinowaną (amplitudowo - fazową, amplitudowo - częstotliwościową itp.).

Zakłócanie optoelektroniczne służy do zakłócania pracy lub niszczenia aparatury rozpoznania pola walki oraz naprowadzania pocisków na cel. Działanie tej broni opiera się na

emisji promieniowania elektromagnetycznego o długości fali i natężeniu wiązki zdolnej do (najczęściej czasowego) zakłócania pracy czujników lub porażenia wzroku żołnierza obsługującego broń.

Do tej grupy należą:

— broń laserowa małej mocy;

— promienniki kierunkowe;

— generatory promieniowania mikrofalowego dużej mocy.

Broń laserowa małej mocy może być stosowana we wszystkich rodzajach sił zbrojnych. W siłach lądowych może występować jako środek przenośny (zestawy indywidualne lub podwieszane pod karabinkiem) lub przewoźny.

W laserach małej mocy wykorzystuje się promieniowanie o różnej długości fali, co zwiększa skuteczność jego działania. Najczęściej stosowane jest promieniowanie ultrafioletowe, czerwone, niebieskie i żółte.

Urządzenia impulsowego promieniowania laserowego są również stosowane do wytwarzania plazmy i fali uderzeniowej, służących do niszczenia czujników i porażenia załóg wozów bojowych. Wykorzystuje się zjawisko ablacji, zachodzące w wypadku uderzenia promienia laserowego w atakowaną powierzchnię oraz tworzenie fali uderzeniowej i powstawanie odłamków z materiału pancerza. Plazma może uszkodzić czujniki, układy kontrolno — pomiarowe i obserwacyjne.

Broń tego typu może być wykorzystana do obezwładniania lekko opancerzonych oraz lekkich wozów bojowych.

Promienniki równokierunkowe lub izotropowe wykorzystywane do celów wojskowych występują w formie amunicji artyleryjskiej lub lotniczej, wytwarzającej promieniowanie elektromagnetyczne o własnościach zbliżonych do laserowego. Ich działanie polega na krótkotrwałej emisji promieniowania elektromagnetycznego w zakresie od podczerwieni do nadfioletu oraz na porażeniu czujników i oczu żołnierzy przeciwnika. Źródłem promieniowania jest plazma powstała z gazu szlachetnego. Do rozgrzania gazu i doprowadzenia go do stanu plazmy wykorzystuje się energię detonacji materiału wybuchowego w kształcie stożka wypełnionego gazem szlachetnym. Najczęściej stosowanymi gazami są: neon, argon lub ksenon.

Promienniki kierunkowe, w odróżnieniu od równokierunkowych, są dodatkowo wyposażone w urządzenia ukierunkowujące strumień promieniowania. Pod względem konstrukcyjnym różnią się też umiejscowieniem ładunku wybuchowego. Charakteryzują się

one większą sprawnością i mniejszym prawdopodobieństwem przypadkowego porażenia celów własnych.

Generatory promieniowania mikrofalowego dużej mocy wykorzystywane są do zakłócania łączności radioliniowej oraz do niszczenia układów elektronicznych samolotów, śmigłowców, pocisków rakietowych, jak również satelitów bojowych i telekomunikacyjnych. Efektem działania tego promieniowania może być zapalenie lub topnienie atakowanych celów, dzięki zjawisku zamiany w napromieniowanym materiale energii promieniowania mikrofalowego w energię cieplną. Może ono być również wykorzystywane do atakowania celów chronionych przez metalowe osłony, takie jak np. klatki Faraday`a.

Zakłócanie czujnikowe polega na obezwładnianiu poszczególnych detektorów lub uniemożliwianiu ich pracy drogą dostarczania energii zakłócającej odpowiadającej parametrami sygnałom bodźcowym, charakterystycznym dla danego środowiska — akustycznego, magnetycznego, elektrycznego, chemicznego.

W zakresie fal sprężystych stosowane są *generatory infradźwięków* do czasowego obezwładniania siły żywej dzięki wytwarzaniu i emitowaniu fal akustycznych o bardzo małej częstotliwości.

Działanie infradźwięków polega na wykorzystaniu zjawiska wzbudzania wibracji materiałów na skutek oddziaływania fal o długości zbliżonej do fizycznych rozmiarów opromieniowanego obiektu. Przy wystarczającej intensywności i czasie ekspozycji można spowodować wibrację i zniszczenie trwałych struktur budownictwa lądowego. Natomiast infradźwięki o częstotliwości 16 Hz używane przeciwko sile żywej powodują wzbudzanie wibracji w organach wewnętrznych, powstanie nudności, dolegliwości sercowych i zaburzeń równowagi. Zaletą tych rodzajów broni jest przede wszystkim łatwość przenikania przez struktury materii.

W zakresie środowiska magnetycznego wykorzystuje się *generatory impulsów elektromagnetycznych* bardzo dużej mocy, które wytwarzają bardzo wysokie pole magnetyczne, które indukuje prąd elektryczny we wszelkiego rodzaju urządzeniach elektronicznych, co jest przyczyną niszczenia niektórych elementów półprzewodnikowych na skutek przeciążeń. Obecnie generatory tego typu mogą być instalowane w pociskach rakietowych, bombach lotniczych i sztucznych satelitach.

W zakresie środowiska elektrycznego wykorzystuje się *środki do uszkadzania linii energetycznych* (EPDM - Electronical Power Distribution Munition). Jest to amunicja zawierająca bardzo lekkie włókna węglowe przewodzące prąd elektryczny, oplątujące linie

przesyłowe oraz stacje rozdzielcze i wywołujące spięcie. Podczas stosowania w Iraku wykazały one wysoką skuteczność. Wywołane awarie powtarzały się przez dłuższy czas.

Chemiczne środki wykorzystuje się np. do uszkadzania elektrowni wodnych. Dodane do wody powodują wzrost jej lepkości, a jeśli są to nici polimerowe, to owijają się wokół turbin i powodują niszczenie układów elektrowni.

Poza tym mogą być wykorzystywane *bakterie o dużej aktywności,* które są zdolne do niszczenia urządzeń wykonanych z tworzyw sztucznych, betonu i metali. Ich przedostanie się do stacji uzdatniania wody może również stanowić duże zagrożenie dla ludzi i środowiska.

Zakłócanie pracy czujników jest procesem skomplikowanym ze względu na dużą ilość i różnorodność tego typu środków na polu walki oraz ich odporność na oddziaływanie przeciwnika.

Przedmiotem *zakłóceń informatycznych* mogą być komputery, jak też programy i zbiory danych. Zakłócanie to może być realizowane przy wykorzystaniu różnorodnych „programów złośliwych", które powodują wymazanie w krótkim czasie dużej liczby zbiorów danych, spowalniające pracę programów użytkowych. Programem złośliwym nazywa się kod wyrządzający szkody. Niektórzy również posługują się określeniem *malware* (zlepek z ang. *malicious software* - oprogramowanie złośliwe)[41]. 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" podejmują działania 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.

---

[41] S. Garfinkel, G. Spafford: *„Bezpieczeństwo w Unixie i Internecie"*, Warszawa 1997, s. 31.

"Konie trojańskie" otrzymały swoją nazwę ze względu na analogię ze znanym mitem greckim. Są one podprogramami, które (wmontowane np. w oryginalne programy użytkowe, np. 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, pewien 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.

"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 one 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 czasu procesora, pamięci, przestrzeni dyskowej i innych zasobów, przez co użytkownik nie może z nich dalej korzystać.

Według poglądów Stanów Zjednoczonych zakłócanie informatyczne będzie jednym z najważniejszych sposobów walki informacyjnej. Systemy komputerowe Departamentu Obrony USA stają się coraz częściej celem „hackerów", którzy włamując się do komputerów Pentagonu mają dostęp do informacji zastrzeżonych. Hackerzy dokonują każdego roku około

250 tysięcy włamań, z czego 65% kończy się powodzeniem. Departament Obrony Stanów Zjednoczonych przeprowadził badania, w ramach których przeprowadzono 8932 próby penetracji na systemy komputerowe. 88% prób penetracji powiodło się. Tylko 320 włamań zostało wykrytych, a 22 zostały zgłoszone przez system.

W procesie zakłócania informacyjnego niezwykle istotnym czynnikiem jest czas. Zakłócanie, aby spełniało zadania powinno w aspekcie czasu reakcji ciągle wyprzedzać funkcjonowanie procesów informacyjnych. Sprowadza się to do tego, że maskowanie i pozoracja w obszarze zbierania danych powinny zostać wykonane przed penetracją tego obszaru przez czujniki rozpoznawcze. Zakłócanie czujników należy realizować od chwili rozpoczęcia przez nie pracy. Sygnały w środkach transmisji danych należy zakłócać przed dotarciem do adresata. Niszczenie powinno być realizowane zaraz po wykryciu obiektu pracującego w systemie informacyjnym. Takie warunki czasowe zakłócania są trudne do zrealizowania, dlatego należy dążyć do posiadania sprzętu umożliwiającego takie zachowanie. Natomiast proces zakłócania należy rozłożyć w czasie w taki sposób, aby u przeciwnika występowały różne stany, m.in. takie jak: zanik informacji, opóźnienie lub brak zakłóceń, co w konsekwencji prowadzi do dezorganizacji procesów informacyjnych przy mniejszych reżimach czasu reakcji.

Skuteczność zakłócania jest uwarunkowana wieloma czynnikami, do których, miedzy innymi, należy zaliczyć:

- *posiadanie wiedzy o stanie i funkcjonowaniu procesów informacyjnych u przeciwnika, o wykorzystywanej przez niego technice, metodach zdobywania i gromadzenia informacji, o dowodzeniu itp. Wiedza ta jest niezbędna głównie po to, aby móc przygotować od strony technicznej, metodologicznej i organizacyjnej proces zakłócania.*
- *dysponowanie środkami rozpoznania (w tym głównie środkami rozpoznania elektromagnetycznego), które będą zdobywały dane o funkcjonowaniu systemów informacyjnych przeciwnika, ich stanie oraz przebiegu procesów informacyjnych, w czasie niezbędnym na uruchomienie procesów zakłócających. Bez zdobycia informacji o pracy tych systemów i środków nie można podejmować przemyślanych i skutecznych zadań zakłócających. Pewne działania profilaktyczne można podejmować na podstawie wiedzy zgromadzonej w bankach danych.*
- *wyznaczenie i przygotowanie określonych organów, odpowiedzialnych za przygotowanie i prowadzenie całego procesu zakłócania. Związana jest z tym cała procedura przygotowania sztabów i wojsk do prowadzenia walki informacyjnej.*

— *dysponowanie siłami i środkami technicznymi oraz materiałowymi, stosownie do stawianych przed zakłócaniem zadań. Możliwości techniczne tych środków powinny umożliwić wykonanie zadań, a zatem nie powinny odbiegać jakością od środków przeciwnika.*

System informacyjny przeciwnika, który podlega zakłócaniu zmienia się poprzez wypadanie i niesprawność poszczególnych ogniw oraz poprzez dokonanie wewnętrznych zmian uodparniających go na oddziaływanie środków zakłócających. Wraz z tym zmieniają się warunki działania wszystkich środków pola walki. Jest to proces dynamiczny przebiegający z różnym natężeniem w poszczególnych systemach. Procesowi temu powinny odpowiadać działania zakłócające poszukujące optymalnych i skutecznych środków i metod postępowania. W takim działaniu należy unikać szablonów, wykorzystywać teren, istniejące warunki taktyczne i operacyjne. Należy dążyć do uzyskania zaskoczenia w każdym obszarze i skali działania. Procesy informacyjne są nieodzowne w prowadzeniu walki zbrojnej, a zatem zakłócanie ich u przeciwnika prowadzi do obniżenia efektywności jego działań. Zakłócanie informacyjne może być realizowane w wielu punktach, dlatego powinno być postrzegane jako jeden obszar działania, jednolicie planowany pod kątem sposobu rozegrania walki przez dowódcę. Realizatorami zadań są wszyscy uczestnicy walki zbrojnej. Procesy informacyjne, we współczesnej walce zbrojnej, w zdecydowanej większości są realizowane za pomocą środków elektronicznych, zatem spektrum elektromagnetyczne należy uznać za najważniejsze w procesie ich zakłócania.

1.5.3. Przestrzeń obrony informacyjnej

Problem obrony informacyjnej istniał zawsze. Każda istotna zmiana w technologii zapisu i przesyłania danych stwarzała nowe problemy związane z ich ochroną. Przed wynalezieniem pisma ochrona danych sprowadzała się do dyskrecji osób, którym dane te były powierzane. Wprowadzenie pisma umożliwiło ich zapis, lecz stworzyło nowe problemy, takie jak: ochrona fizyczna tekstów, na których zapisana jest treść oraz konieczność stosowania kryptografii. Rozwój maszyn cyfrowych i telekomunikacji, przyczyniając się do wprowadzenia nowych technologii zapisu, przesyłania i przetwarzania danych, stworzył także nowe problemy ich ochrony.

W Polsce powoli dojrzewa sytuacja, w której wszelkie postacie danych: naukowych, technicznych, politycznych, gospodarczych, prawnych, administracyjnych, organizacyjnych itp., mających jakąkolwiek wartość społeczną lub mogących mieć w przyszłości znaczenie dla społeczeństwa i rozwoju jego gospodarki lub kultury, należy traktować jako wspólne

ogólnonarodowe dobro podlegające ochronie prawnej oraz obligujące do jego racjonalnego wykorzystania[42]. Nie ma istotnych powodów, aby z prawnego punktu widzenia traktować je pod tym względem inaczej niż traktuje się dziś surowce naturalne, przyrodę, zasoby wodne i atmosferę.

Przynależność Polski do NATO wymagała dostosowania prawnych ram ochrony danych do tamtejszych standardów, przede wszystkim do tzw. minimalnych wymagań w zakresie ich bezpieczeństwa, określonych w dokumencie C — M/55/15. Sejm RP uchwalił nową ustawę „O ochronie informacji tajnych". Polski projekt nawiązuje do wymagań NATO i wprowadza ujednolicone klauzule tajności: „ściśle tajne" (Top Secret), „tajne" (Secret), „poufne" (Confidential), „do użytku wewnętrznego" (Restricted). Ustawa nadaje charakter ponadresortowy problemowi ochrony informacji tajnych. Powołuje też zupełnie nowy organ — Komitet Ochrony Informacji Tajnych, kierowany przez premiera, który może powierzyć kierowanie pracami komitetu ministrowi spraw wewnętrznych i administracji. Zgodnie z tym projektem wszystkie instytucje, w których są wytwarzane, przetwarzane, przekazywane lub przechowywane tajne dane muszą mieć swoich pełnomocników ochrony, kierujących wyspecjalizowaną komórką organizacyjną, zwaną pionem ochrony. Ponadto o nadawaniu klauzuli tajności ma decydować sam autor dokumentu. Pomimo wprowadzanych przepisów o ochronie informacji, w dalszym ciągu w Polsce występuje problem braku dostatecznej świadomości społecznej skutków, jakie może powodować niewłaściwe gospodarowanie danymi, zwłaszcza zaś brak troski o ich zabezpieczenie.

Problem ochrony danych nabiera coraz większej wagi w związku z rozwojem informatyki i z rosnącą automatyzacją procesu ich przetwarzania. Rzecz polega na zmianach jakościowych i ilościowych, jakie następują w procesach ich gromadzenia, przetwarzania i dystrybucji.

Systemy informacyjno — sterujące funkcjonują zarówno w środowisku cywilnym, jak i wojskowym, a niektóre z nich mają zasięg międzynarodowy (np. Internet), co powoduje, że wiele osób oraz organizacji ma dostęp do danych i może je wykorzystać według własnego uznania.

Walka o zdobycie i wykorzystanie danych rozpoczęła się już dawno temu, kiedy jedna grupa ludzi próbowała uzyskać przewagę nad drugą. Zdobywanie, wykorzystanie i ochrona

---

[42]Kulikowski J. L.: *Organizacyjne i techniczne aspekty ochrony danych w systemach informatycznych*. W: *„Prawne problemy systemów informatycznych"*, materiały z konferencji naukowej, Wrocław 1976.

danych może mieć miejsce na arenie ekonomicznej, politycznej lub militarnej. Odpowiednie wykorzystanie danych o przeciwniku może spowodować podjęcie uzasadnionej decyzji na polu walki, a tym samym zwiększyć zdolność bojową wojsk własnych oraz ochronić własne środki.

W trakcie prowadzenia obrony informacyjnej należałoby najpierw zdobyć kluczową (newralgiczną) wiedzę o przeciwniku oraz mieć orientację w sytuacji wojsk własnych. Następnie powinno się ustalić urządzenia elektroniczne w systemach rozpoznawczych przeciwnika, które mogą być wykorzystane do rozpoznania pola walki oraz przekazywania danych. Należy wybrać środki i podjąć działania, które zredukują w odpowiedni sposób podatność sił własnych na oddziaływanie przeciwnika.

Przedsięwzięcia z zakresu obrony informacyjnej mają charakter pasywny. Są ukierunkowane przede wszystkim na uzyskanie możliwie dużych korzyści czasowych, ponieważ jest prawie niemożliwe długotrwałe wiązanie informacji wyłącznie z określonymi osobami lub miejscami. Podczas prowadzenia obrony informacyjnej należy uwzględniać między innymi następujące sytuacje:

— zdobyte dane mogą być nieprawdziwe lub nieaktualne;
— wiadomość musi być utrzymana w tajemnicy przed przeciwnikiem;
— określone dane mogą spowodować niepewność, obawę lub lęk;
— duży strumień danych może spowodować, że ich przetworzenie w pożądanym czasie będzie niemożliwe lub znacznie utrudnione.

Powyższe, a także inne przyczyny muszą być uwzględnione w wojskowych systemach informacyjno-sterujących oraz w działalności dowódców. Jednakże w praktyce należy liczyć się z możliwością wystąpienia tzw. konieczności wyższego rzędu, które spowodują, że zasady obrony informacyjnej nie zawsze będą w pełni przestrzegane. Np., ze względów politycznych może zaistnieć potrzeba ujawnienia w określonych sytuacjach tajemnic wojskowych bądź utrzymywane w tajemnicy dane będą ujawnione przez określone działanie dowódców i wojsk.

Efektem obrony informacyjnej jest wywołanie niepewności u przeciwnika. Niepewna sytuacja informacyjna i nieprawdziwe dane prowadzą do strat czasu, absorbują siły i wyczerpują przeciwnika. Dlatego też obrona informacyjna musi stanowić element planowania informacyjnego organizowanego przez dowódców wojskowych.

Obrona informacyjna może być realizowana różnymi sposobami i narzędziami. Jej istota powinna dotyczyć stwarzania sytuacji uniemożliwiających przeciwnikowi

przechwytywanie danych, szczególnie tych postaci, które zawierają największą potencję informacyjną o ważnych sytuacjach rzeczywistych.

Obrona informacyjna może być realizowana zarówno w stosunku do stanów osobowych, jak i urządzeń technicznych, czyli w środowisku osobowym i nieosobowym. Uznając powyższe za kryterium rozstrzygalności, można wyróżnić:

— *bezpośrednią (osobową) obronę informacyjną;*

— *pośrednią(techniczną) obronę informacyjną.*

Bezpośrednia (osobowa) obrona informacyjna powinna być ściśle zsynchronizowana z zakłócaniem informacyjnym i skupiać się na:

— niedopuszczaniu do sytuacji, w której człowiek traci wolę walki i poddaje się depresji;

— realizacji przedsięwzięć w celu zapobiegania obcej działalności wywiadowczej (akcjom sabotażowym, dywersyjnym itp.);

— ukrywaniu wojsk własnych w zakresie poznawania zmysłowego, ze szczególnym zwróceniem uwagi na te elementy, których ujawnienie może szkodzić w osiąganiu zakładanych celów.

A zatem w zakresie osobowej obrony informacyjnej można wyróżnić:

— *obronę psychologiczną;*

— *kontrwywiad wojskowy;*

— *ukrywanie.*

Obrona psychologiczna polega na utrzymywaniu wysokiego morale i dobrego stanu psychicznego wojsk własnych. Należy podejmować takie przedsięwzięcia, aby wojska własne nie były podatne na informacje przeciwnika. Innymi słowy, jej realizacja powinna polegać na niedopuszczeniu do niedoboru lub nadmiaru danych. Zarówno niedobór jak i nadmiar wpływają źle na psychikę człowieka, powodując niepokój, lęk, niepewność podejmowania decyzji. Sygnały informacyjne odgrywają zasadniczą rolę w orientacji człowieka w środowisku. Innymi słowy, dowódca znający aktualną sytuację będzie miał świadomość rzeczywistości pola walki. Jego orientacja co do sytuacji będzie polegała na czynnym poszukiwaniu i wykorzystaniu różnych zmian w środowisku pola walki, jako nośników sygnałów informacyjnych. Posiadanie aktualnej wiedzy będzie zatem w znaczny sposób wpływać na dobry stan psychiczny dowódcy oraz na zmniejszenie ryzyka podejmowania błędnych decyzji.

Niedobór (ograniczenie dopływu) danych powoduje, że człowiek nie zaspokaja swoich potrzeb poznawczych. Otoczenie traci wtedy dla niego znaczenie. Konieczność

odbioru i przetwarzania bardzo dużej liczby danych, jak również ich niedobór może zakłócić czynności człowieka i wywołać takie negatywne skutki, jak napięcie, lęk, zmęczenie. Postęp współczesnej cywilizacji oparty na zdobywaniu, gromadzeniu i wykorzystaniu danych wydaje się być hamowany ich nadmiarem z powodu ograniczonych możliwości percepcji człowieka. Zasadniczą rolę w tej działalności odgrywają czynniki osobowe, między innymi możliwości percepcyjne człowieka (pamięć), jego stan psychiczny, umiejętności, zdolności, doświadczenie, potrzeby. Stawianie zbyt wysokich wymagań może powodować zakłócenia obiektywne (nieosiągnięcie zakładanego celu) lub subiektywne (obniżenie zdolności działania, znużenie, nerwice).

Maksymalna ilość danych, jaką otrzymuje układ (człowiek) ze wszystkich receptorów organizmu wynosi 10^9 bit/sek., a uświadomionych zostaje tylko 10^2 bit/sek. W cybernetyce ilość informacji oznacza ciąg sygnałów przekazywanych od nadajnika do odbiornika, nagromadzonych w kanale łączności, którego najważniejszą charakterystyką jest pojemność, czyli zdolność przepustowa, wyrażona właśnie w ilości bitów na sekundę. Sprawność funkcjonowania układu człowiek — maszyna cyfrowa zależy od szybkości przepływu danych od maszyny do człowieka. Szybkość ta nie może przewyższać zdolności przepustowej „wejścia sensorycznego" człowieka. Podobnie szybkość wprowadzania rozkazów (poleceń) do maszyny nie może być wyższa, niż zdolność przepustowa „wyjścia motorycznego" człowieka. W wypadku przeciążenia informacyjnego, które powstaje po przekroczeniu „zdolności przepustowej" zmysłów i układu nerwowego człowieka, trudno jest jednoznacznie odpowiedzieć na pytanie, ile danych człowiek może spostrzec, zrozumieć i wykorzystać w określonym czasie. Zależy to od wielu czynników, takich jak: odbiór sygnałów za pośrednictwem narządów zmysłowych, czas potrzebny na podejmowanie decyzji.

W żadnym wypadku nie można pominąć psychiki człowieka w walce zbrojnej. Stresy wywołane walką i przygotowanie fizyczne, moralne uzasadnienia oraz psychika działania grupowego są to czynniki, które w określonym stopniu wpływają na wymierne wielkości dotyczące gotowości bojowej i wymiarów prowadzenia działań lub przynajmniej powodują, że efekt działania będzie niemożliwy do skalkulowania. Człowiek, jego psychika i motywacje stanowią łącznie wartość, której nigdy nie można zlekceważyć. Dzięki właściwym motywacjom działania człowiek może zdobyć lub utracić czas i przestrzeń. Motywacje mogą być potęgowane przez odpowiednią sytuację informacyjną i właściwe wykorzystanie spektrum elektromagnetycznego. Człowiek jest więc czynnikiem (przy zrównoważonym bilansie sił i uwarunkowań ramowych) decydującym o sukcesie w walce zbrojnej.

Kontrwywiad wojskowy to działalność zmierzająca do zwalczania szpiegostwa, akcji dywersyjnych i sabotażowych, mająca na celu ochronę tajemnicy wojskowej przed penetracją obcego wywiadu.

Już Sun Tsu dostrzegał celowość prowadzenia takich działań. Zalecał, aby dane pochodzące z wywiadu traktować priorytetowo i chronić, ponieważ w przypadku jeśli armia zostanie pozbawiona tajnych agentów, wszelkie działania zbrojne nie mają najmniejszego sensu. *„Wyróżnia się pięć rodzajów tajnych agentów (narodowi, wewnętrzni, podwójni, straceni*[43] *oraz powracający). Jeśli tych pięć typów zatrudnionych agentów pracuje w koordynacji, to nazywani są oni doskonałą siecią i znajdują się pod szczególną opieką władcy. Dlatego też tylko oświecony władca oraz zacny generał są w stanie użyć najinteligentniejszych ludzi jako agentów, a z nimi z pewnością mogą dokonać wielkich rzeczy. Tajne plany i operacje są zasadnicze dla działań wojennych, bez nich armia nie może zrobić żadnego sensownego ruchu. Armia pozbawiona agentów jest doprawdy jak człowiek ślepy i głuchy"*[44].

Ukrywanie to utrudnianie przeciwnikowi dostrzeżenia pozycji obronnych przez wizualne dostosowanie ich do otoczenia[45]. Ukrywanie ma na celu uczynienie obiektu niewidzialnym. W aspekcie zjawisk psychofizycznych polega ono na dążeniu do uniemożliwienia podmiotom rozpoznania dokonania aktu przedstawienia sobie ukrytych przedmiotów. Istnieją dwa podstawowe sposoby osiągania tego celu.

Pierwszy, polegający na fizycznym odizolowaniu maskowanego obiektu przed środkami rozpoznania przeciwnika. Taki sposób ukrycia charakteryzuje jedną z dwu form ukrywania – *zakrywanie*. Sposób ten pozbawia przeciwnika możliwości spostrzeżenia przedmiotu rozpoznania. Tym samym nie może zaistnieć akt bezpośredniego przedstawienia go sobie. W umyśle prowadzącego rozpoznanie nie powstaje żaden model przedmiotu rzeczywistego lub co najwyżej mocno zniekształcony. Na podstawie takiego przedstawienia podmiot rozpoznania wydaje niewłaściwy sąd o rzeczywistym przedmiocie rozpoznania.

Druga forma ukrywania – *kamuflaż* polega na obniżeniu kontrastu obiektu poniżej wartości progowej. Powoduje to, najogólniej rzecz biorąc, zlanie się kształtów, barw ukrywanego przedmiotu z barwą, dominującymi kształtami i energią tła. Efekt kamuflażu jest taki, że obserwator widzi przedmiot rozpoznania, ale go nie postrzega. Oczywiście jest to daleko idące uproszczenie kamuflażu. Podłożem psychofizycznym kamuflażu jest

---

[43] Agent stracony to taki, który przesyła nieprawdziwe informacje.
[44] Sun Tsu, op. cit., s. 40 i 46.
[45] Słownik wyrazów obcych, op. cit., s.457.

niedoskonałość zmysłów człowieka, która prowadzi do tego, że sposób, w jaki człowiek przedstawia sobie przedmioty, a wskutek tego i sposób, w jaki o nich sądzi, jest nieuchronnie zależny od jego organizacji; organizacja ta może być tego rodzaju, iż człowiek dzięki niej wydaje więcej mylnych aniżeli prawdziwych sądów.[46] Swoją niedoskonałą organizację człowiek poprawia stosując różnorodne urządzenia techniczne, dzięki którym stosunkowo łatwo radzi sobie z kamuflażem. Lornetka obniża wartość krytycznego progu kontrastu, kamera termowizyjna pozwala spostrzec różnice temperatur obiektu i tła, a jednoczesna obserwacja wielo-spektralna komplikuje kamuflaż do potęgi równej liczbie pasm spektrum obserwacji. Jednak mimo tych wszelkich utrudnień, ukrywanie (zarówno zakrywanie, jak i też kamuflaż) odgrywa nadal dużą rolę z uwagi na fakt, że dotyczy ono bezpośrednio rzeczywistego przedmiotu rozpoznania.

W wyposażeniu współczesnych armii znajduje się wiele środków przeznaczonych do ukrywania żołnierzy, do środków tych można zaliczyć:

— ubiory maskujące letnie i zimowe (np. mundur polowy z naniesionym wzorem drobnego kamuflażu);

— siatki maskujące typu peleryny i narzuty;

— pasty i kremy do nakładania na odsłonięte części ciała.

Pośrednia (techniczna) obrona informacyjna to zespół przedsięwzięć polegających na niedopuszczeniu do zakłócenia i rozpoznania środków i urządzeń wojsk własnych dostosowanych do rejestrowania określonych efektów, charakterystycznych dla danego środowiska — elektromagnetycznego, akustycznego, magnetycznego, elektrycznego, chemicznego.

Ze względu na środowisko (kryterium rozstrzygalności) techniczną obronę informacyjną można podzielić na:

— *obronę elektromagnetyczną (SIGSEC – Signal Security);*

— *obronę czujnikową;*

— *obronę informatyczną;*

— *maskowanie.*

Obrona elektromagnetyczna polega na niedopuszczeniu do zakłócenia i rozpoznania środków wykorzystujących fale elektromagnetyczne jako nośniki danych. Innymi słowy, polega na zapewnieniu dostępu do spektrum elektromagnetycznego. Istotnym wskaźnikiem

---

[46]K. Twardowski: *„Wybór pism psychologicznych i pedagogicznych"*. Wydawnictwa Szkolne i Pedagogiczne, Warszawa, 1992, s. 159.

skuteczności tej obrony jest stopień zapewnienia stabilnej pracy systemów łączności wojsk własnych, których bazę materialną stanowią w przeważającej części bezprzewodowe środki łączności, tj. radiostacje, stacje radioliniowe, satelitarne; Jak powszechnie wiadomo, są one cennymi dla strony przeciwnej i łatwo dostępnymi źródłami danych, a ich porażenie ogniowe lub obezwładnienie elektromagnetyczne grozi zerwaniem dowodzenia w najbardziej krytycznych momentach walki. Ponadto nie mniej ważna jest ochrona wszelkiego rodzaju czujników i urządzeń rozpoznawczych przed zakłóceniami elektromagnetycznymi (radiowymi, radiolokacyjnymi, optoelektronicznymi) i innymi oraz przed porażeniem ogniowym.

Ze względu na wykorzystywane pasma częstotliwości z zakresu spektrum elektromagnetycznego można wyróżnić:

— *obronę radiową (COMSEC – Communication Security);*

— *obronę radiolokacyjną (aktywną – RSEC – Radiation Security, pasywną – ELSEC – Electronic Security);*

— *obronę optoelektroniczną (OPTSEC – Optical Security).*

Obrona radiolokacyjna polegała na osłonie własnych środków radiolokacyjnych, wykorzystujących fale elektromagnetyczne jako nośniki informacji przed rozpoznaniem i zakłócaniem przeciwnika. Może ona sprowadzać się do zmiany potencjału informacyjnego określonych postaci sygnałów. Przykładem tego może być technika *stealth*. Zmniejszona skuteczna powierzchnia odbicia celu powietrznego daje na wskaźniku stacji radiolokacyjnej obraz znacznie mniejszy niż w rzeczywistości.

Obrona optoelektroniczna skupia się na stosowaniu osłon i filtrów szerokopasmowych na urządzenia, które pracujące w tym zakresie promieniowania elektromagnetycznego. Ponadto maluje się wozy bojowe specjalnymi farbami. W czasie obserwacji celu w podczerwieni powstaje złudzenie polegające na zlaniu się widma podczerwieni obserwowanego celu z widmem tła. Środki metamorficzne powodują zmianę koloru pod wpływem warunków zewnętrznych (temperatury, natężenia oświetlenia). Obrona przed generatorami promieniowania mikrofalowego dużej mocy polega na uodpornieniu i izolowaniu układów, aby nie powstawała w nich energia cieplna. Ponadto stosuje się flary emitujące promieniowanie cieplne, które mają na celu zmylenie pocisków naprowadzanych na źródło ciepła. Mogą one być wystrzeliwane ze specjalnie skonstruowanych zasobników. Flary charakteryzują się zdolnością prawie natychmiastowego uzyskiwania szczytowego poziomu energii promieniowania podczerwonego, a czas ich palenia wynosi z reguły 4 sekundy. Są one najbardziej skuteczne, gdy realistycznie naśladują ślad cieplny samolotu

i gdy się używa wraz z systemami ostrzegania o zbliżaniu pocisku, zwłaszcza gdy są odpalane ze znanego rejonu zagrożenia.

Obrona czujnikowa polega na ochronie przed rozpoznaniem i zakłócaniem własnych detektorów, które wykorzystują energię odpowiadającą parametrami sygnałom bodźcowym, charakterystycznym dla środowiska — akustycznego, magnetycznego, elektrycznego, chemicznego. Np. obrona przed generatorami infradźwięków opiera się 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 180^0). Zasadniczym problemem w stosowaniu tej broni jest stworzenie odpowiedniego zestawu specjalistycznych głośników oraz wzmacniaczy, które wymagają m.in. bardzo wydajnych układów chłodzenia.

Obrona informatyczna obejmuje ochronę przed "wirusami", "koniem trojańskim", "bombami logicznymi", "robakami" i "bakteriami".

Ochrona przed "wirusami" polega na tym aby nie dopuszczać do ładowania systemu z dyskietek niewiadomego pochodzenia. Należy pamiętać o tym, aby w stacji dysków podczas uruchamiania nie było żadnej dyskietki (wszystkie płyty główne mają obecnie funkcję, która umożliwia wybranie pierwszego dysku, z którego ma się uruchamiać system; dzięki tej funkcji nawet pozostawiona w stacji dyskietka z wirusem przestaje być groźna). Wirus zarażonego komputera można usunąć uruchamiając system z czystej, nie zawirusowanej dyskietki i zastępując zainfekowany sektor startowy czystym.

Najlepszą metodą unikania *"konia trojańskiego"* jest nieuruchamianie żadnego programu ani skryptu, dopóki się nie przeczyta dokładnie całego pliku. Do czytania pliku należy stosować program czy edytor, który wyświetla kody sterujące w sposób widoczny. Nie należy również uruchamiać programu, którego czytanie nie wyjaśnia wszystkich pojawiających się wątpliwości.

Ochrona przed "złośliwymi bombami" polega na nie instalowaniu oprogramowania bez wcześniejszego dokładnego przetestowania i przeanalizowania kodu źródłowego. Należy przeprowadzać regularne archiwizacje, aby w razie wystąpienia problemów można było powrócić do stanu sprzed awarii.

Metodą *obrony przed "robakami"* jest regularne sprawdzanie integralności ważnych plików, nowego oprogramowania, zwłaszcza z nieznanych lub słabo znanych źródeł. Innymi słowy, jeśli komputer jest zabezpieczony przed nieautoryzowanym dostępem, powinien być odporny na każdego robaka. Jeśli robak znajduje się już w systemie, zerwanie połączeń

sieciowych może nie dopuścić do jego dalszego rozprzestrzeniania oraz przesyłania prywatnych danych na zewnątrz sieci lokalnej.

Ochrona przed "bakteriami" i "królikami" polega na zachowaniu szczególnej ostrożności w stosunku do importowanych programów zarówno w postaci kodów źródłowych, jak i w postaci skompilowanej z nieznanych źródeł.

Maskowanie techniczne zmienia się wraz z rozwojem środków walki i rażenia. W okresie pierwszej wojny światowej problem maskowania dotyczył przede wszystkim strefy frontu. W czasie drugiej wojny światowej maskowaniem obejmowano nie tylko wojska, lecz także ludność i terytorium za frontem walczących ugrupowań. Stosowano wówczas maskowanie strategiczne, operacyjne i taktyczne[47].

Współcześnie znaczenie maskowania wzrosło. Jest to spowodowane pojawieniem się nowych środków rozpoznania oraz broni precyzyjnej, umożliwiającej trafienie małych celów ze znacznych odległości (systemy rozpoznawczo — uderzeniowe). Przykładem może być wojna w rejonie Zatoki Perskiej (1991), w której maskowanie było jednym z najważniejszych elementów. Wojska koalicji antyirackiej stosowały malowanie deformujące sprzętu bojowego (kamuflaż pustynny), pokrycia maskujące (siatki stosowane przede wszystkim do maskowania artylerii i czołgów na stanowiskach ogniowych). Wojska irackie natomiast z powodzeniem stosowały makiety czołgów, dział i wyrzutni rakietowych.

Należy zaznaczyć, że maskowanie na współczesnym polu walki realizowane jest w szerokim zakresie widma promieniowania elektromagnetycznego, to jest od ultrafioletu do pasma mikrofalowego. Występuje ono zarówno w obronie radiowej, radiolokacyjnej jak i optoelektronicznej.

1.6. Geneza walki informacyjnej

Na walkę zbrojną mają wpływ czynniki obiektywne i subiektywne. Czynniki obiektywne mają charakter ogólny. Do nich należy zaliczyć prawa walki zbrojnej, które są trwałe w czasie. Niezależne są też od woli i świadomości ludzkiej. W całej swej ogólności eksponują zależności unaoczniające, że sukces w tej walce może osiągnąć tylko silniejszy. Na tle tego formułowane są zasady sztuki wojennej[48], które już w konkretnych uwarunkowaniach materialnych definiują zasadnicze zależności dochodzenia do sukcesu bojowego. Czynniki subiektywne są natomiast związane z potrzebami oraz możliwościami podmiotu, jego wiedzą,

---

[47] J. Garstka: Techniczne środki maskowania. W: „Myśl wojskowa", 1/96, s.69.

[48] Sztuka wojenna to system wiedzy o wojnie - o prawach i prawidłowościach wojny o zasadach i sposobach przygotowania i prowadzenia działań wojennych o różnej skali. B. Szulc: „Walka zbrojna w kontekście ogólnej teorii walki i teorii konfliktów", AON, Warszawa 1996, s.25.

wolą i świadomością. Przesądzają zatem o intelektualnej i praktycznej działalności człowieka. Do nich należy zaliczyć procedury przygotowania i rozgrywania walki zbrojnej, które rzutują na jej rezultat. Z tej przyczyny odnotowywane są w historii fakty materialnie nieuzasadnionych klęsk i materialnie nieuzasadnionych wygranych. Amerykański historyk Dupuy w książce "Liczby, prognozy i wojna" przedstawia wynik badań 42 bitew (od Austerlitz do Wzgórz Synaj). Wynik tych badań to stwierdzenie, że tylko 18 zwycięstw (43%) odniesiono dzięki przewadze liczebnej, a 24 zwycięstwa (57%) odniesiono siłami mniejszymi liczebnie. Prof. K. Nożko z kolei dodaje, że spośród 25 historycznych bitew, stoczonych przez polskie siły zbrojne (od 1102 do 1920r.), aż w 23 przypadkach (92%) odniesiono zwycięstwo nad większym liczebnie przeciwnikiem („Problemy i zasady sztuki operacyjnej", s.193). Potocznie tłumaczy się to nieudolnością bądź geniuszem dowódców.

Analizując powyższe fakty, można dostrzec, że konkretne efekty były następstwem sukcesu bądź klęski w prowadzonej wcześniej walce, którą dziś można nazwać „walką informacyjną". W taki sposób można zatem tłumaczyć tak zarówno geniusz, jak i nieudolność dowódców.

Najstarszym z zapisów, mówiącym o roli walki 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:

„Jeśli wiem, że moje oddziały mogą uderzyć na wroga, lecz nie wiem, czy wróg jest przygotowany do odparcia, to szansa przegranej i wygranej jest jak jeden do jednego. Tak samo, jeśli wiem, że wróg nie jest przygotowany na atak, lecz nie wiem czy moje oddziały są gotowe do uderzenia, szansa zwycięstwa i porażki jest jak jeden do jednego. Jeśli wiem, że moje oddziały mogą uderzyć i wróg nie jest przygotowany na atak, lecz nie rozpoznałem dobrze ułożenia terenu bitwy, szansa zwycięstwa i porażki jest jak jeden do jednego. Dlatego też twierdzę: Poznaj siebie i poznaj wroga, dopiero wtedy twoje zwycięstwo nie będzie zagrożone. Poznaj warunki terenu i pogody, wtedy twoje zwycięstwo będzie całkowite".[49]

Z powyższego wynika, że już sześć wieków p.n.e. problem walki informacyjnej, aczkolwiek tak formalnie nie nazywanej, dostrzegany był z pełną ostrością merytoryczną, bo przecież:

— *poznanie wroga, terenu i pogody — to nic innego, jak prowadzenie kompleksowego rozpoznania - czyli zdobywanie informacji;*

---

[49]Sun Tzu: *Sztuka wojny.* Wydawnictwo Przedświt, Warszawa 1994, s.116.

— *poznanie siebie — wiążę się z niezakłóconym funkcjonowaniem własnego systemu informacyjnego, co jest tożsame z obroną informacyjną;*
— *wnoszenie natomiast przez przeciwnika entropii informacyjnej do komunikatów o powyższym staje się tożsame z zakłócaniem informacyjnym, co już wynika z podtekstu przytoczonego zapisu.*

Elementy te znacznie uwidoczniły się w roku 490 p.n.e. w bitwie pod Maratonem. W odwecie za wspieranie przez Greków powstańczych miast w Azji Mniejszej, znajdujących się pod perskim panowaniem, Dariusz wysłał armię pod wodzą Datusa i Artafernesa z zadaniem ujarzmienia Aten. Armia perska liczyła 20 tys. żołnierzy, natomiast po przeciwnej stronie było 9000 Ateńczyków i 1000 Platejczyków. Persowie mieli więc dwukrotną przewagę nad przeciwnikiem. Grecy pod wodzą Militiadesa, zdając sobie z tego sprawę, starali się wprowadzić przeciwnika w błąd. W tym celu przeprowadzili dokładne rozpoznanie, co pozwoliło im na wybór i zajęcie dogodnej pozycji do prowadzenia walki. Militiades ukrył swoje wojska na wzgórzach Agrieliki i w ten sposób zagrodził Persom obydwie drogi, jakie prowadziły do Aten. Ponadto nie mogli się oni bezpiecznie załadować na okręty, gdyż również groziło to klęską. W rezultacie podjętych przedsięwzięć Grecy uzyskali zaskoczenie, które przyczyniło się do odniesienia zwycięstwa. Straty Persów wynosiły 6400 zabitych, podczas gdy straty greckie tylko 200 zabitych i 1000 rannych[50].

Zastosowane przez Militiadesa elementy walki informacyjnej przyczyniły się do osiągnięcia zwycięstwa przez Greków. Wydawać by się mogło, że Grecy nie zrobili niczego nadzwyczajnego, poza dokładnym rozpoznaniem i obroną informacyjną. Ale dzięki realizacji tych przedsięwzięć Militiades niejako „zaprogramował" działanie przeciwnika do trzech możliwych sytuacji:
— *pójście drogą przez wąwóz i bitwa z Grekami zajmującymi dogodną i umocnioną pozycję;*
— *pójście drogą nad morzem i narażenie się na atak ze skrzydła;*
— *ładowanie na okręty i narażenie się na atak z tyłu.*

Przez zwykłe zajęcie i utrzymanie dogodnej pozycji Militiades ograniczył zbiór możliwych decyzji przeciwnika do trzech wariantów, które były korzystne dla Greków. Pozbawił przeciwnika swobody działania i zmusił go do stoczenia bitwy w niekorzystnych dla niego warunkach, co w efekcie przyczyniło się do odniesienia zwycięstwa nad dwukrotnie liczniejszym przeciwnikiem.

---

[50]D. Strasburger: *„Zasady sztuki wojennej"*. Wydawnictwo Bellona, Warszawa 1996, s.17.

W bardzo szerokim zakresie elementy walki informacyjnej wykorzystywał Czyngis-chan. Potwierdzeniem tego może być sposób prowadzenia przez niego kampanii przeciwko państwu Chorezmu, w latach 1218 - 1223[51]. Podbił on północne Chiny, Koreę, Mandżurię, kraje azjatyckie i południową Syberię. Podlegli mu wodzowie — Dżebe i Subudej — podbili kraje zakaukaskie. Szach Chorezmijski Muchammed Ala ed — Din, dysponował regularną armią dwa razy większą niż wszystkie wojska Czyngis-chana, które liczyły w przybliżeniu 150 do 200 tysięcy żołnierzy. Hordy Mongołów znane jako „RAND"[52], znacznie mniej liczebne, systematycznie pokonywały przeważające siły przeciwnika. Mongolscy dowódcy ciągle prowadzili intensywne rozpoznanie przeciwnika, terenu i warunków atmosferycznych. Stosując maskowanie (obronę informacyjną) i pozorowanie (zakłócanie informacyjne), często unikali walki po to, by innym razem zaatakować tam gdzie chcieli i tam gdzie się tego nie spodziewał przeciwnik. Wykorzystując szybkich łączników na koniach, utrzymywali cały czas łączność pomiędzy dowódcami i wielkim Chanem, co potwierdzać może ich dbałość o niezakłócone funkcjonowanie własnego procesu informacyjnego. Bacząc na obronę informacyjną, wojska Czyngis-chana maszerowały zawsze w oddzielnych kolumnach. Uniemożliwiało to tym samym przeciwnikowi ustalanie planowanych miejsc ataku. Utrzymywanie w tajemnicy rejonów koncentracji wojsk, unikanie walki bez wcześniejszego przygotowania oraz duża ostrożność Czyngis-chana, który w sposób bardzo zsynchronizowany wykonywał przesunięcia swych armii w kierunkach celów, jakie zamierzał osiągnąć, jak również prowadzenie dezinformacji wśród wojsk i ludności cywilnej jest tożsame z obroną informacyjną i zakłócaniem informacyjnym.

Analizując poszczególne epizody kampanii, wyraźnie dostrzega się, że sukcesy bojowe Czyngis-chana uwarunkowane były wcześniejszym powodzeniem uzyskanym w prowadzonej przez niego walce informacyjnej. Prowadził rozpoznanie przeciwnika i terenu, co przyczyniało się do tego, że dokładnie wiedział o jego położeniu, zamiarach i rejonie, w jakim chce walczyć. Utrzymywał w tajemnicy rejony koncentracji wojsk, co jest równoznaczne z obroną informacyjną. Stosował dezinformację wśród wojsk przeciwnika i ludności cywilnej (zakłócanie informacyjne).W następstwie tego często wprowadzał w błąd przeciwnika i w ten sposób uzyskiwał nad nim przewagę. Dlatego też ogólna liczebność wojsk nie odgrywała decydującej roli w kampanii.

---

[51]S. Kałużyński: *„Imperium mongolskie"*, Warszawa 1970, s.76 - 82.
[52]P. Grier: *Information Warfare w:* „Air Force", 4/1994, s.34 - 37. Aktualnie nazwę „Rand Corps" przyjęła grupa fachowców zajmująca się walką informacyjną.

Elementy walki informacyjnej stosował również król polski Władysław Jagiełło w czasie przygotowywania i prowadzenia bitwy pod Grunwaldem. Bitwa ta, stoczona 15 lipca 1410 roku przez połączone siły Królestwa Polskiego i Wielkiego Księcia Litewskiego z wojskami Zakonu Krzyżackiego, należy do najważniejszych wydarzeń w średniowiecznych dziejach Europy Środkowo — Wschodniej.[53] Brak jest dokładnych danych co do liczebności wojsk biorących udział w bitwie. Według danych przedstawionych przez Dominika Strasburgera armia polsko-litewska liczyła około 31 500 zbrojnych żołnierzy, natomiast wojska krzyżackie miały ponad 27 000 rycerzy.[54] Zygmunt Ryniewicz podaje, że wojska prowadzone przez Jagiełłę liczyły 27 000 żołnierzy (14 000 jazdy polskiej, 10 000 Litwinów i Rusinów oraz 3000 Tatarów), natomiast wielki mistrz Ulryk von Jungingen 3000 jazdy pozostawił nad Wisłą, a z 11 000 rycerzy zagrodził drogę Jagielle pod Grunwaldem.[55]

Wojska sprzymierzonych były liczniejsze od wojsk Zakonu, jednak ich uzbrojenie i wyposażenie znacznie ustępowało sile Krzyżaków. Jagiełło zdając sobie sprawę z tego, zamierzał zmusić Zakon do stoczenia walnej bitwy w otwartym polu, a więc w warunkach przewagi polsko-litewskiej. Zaplanował marsz na Malbork, aby sprowokować Krzyżaków do wystąpienia całością sił. Chciał uniknąć oblegania licznych i silnych zamków krzyżackich. W Brześciu w grudniu 1409 roku, zapadły ważne decyzje strategiczne, które zaważyły na przebiegu kampanii w 1410 roku. Dotyczyły one przede wszystkim: skupienia większości sił na wybranym, ograniczonym teatrze działań wojennych, zamiaru wymuszenia na przeciwniku walnej bitwy przez marsz zagrażający jego stolicy, zbudowania na Wiśle (pod Czerwińskiem) mostu na łodziach. Aby dokonać bezpiecznej przeprawy przez Wisłę, Jagiełło wprowadził w błąd przeciwnika wykorzystując wydzielone oddziały, które niepokoiły pogranicze krzyżackie od strony Nowej Marchii, Kujaw i Żmudzi, aby odwrócić jego uwagę od głównego przedsięwzięcia. Powyższe działania można utożsamić z zakłócaniem informacyjnym.

Jagiełło w czasie bitwy sam kierował swoimi wojskami za pomocą gońców, którzy przenosili rozkazy i meldunki nawet na bardzo znaczne odległości. Istotną rolę odgrywały sygnały optyczne (w tym umowne znaki dawane ruchem chorągwi) oraz akustyczne, na które oprócz dźwięku trąb i bębnów składały się okrzyki i hasła rozpoznawcze. Prawo używania sygnałów miał tylko trębacz królewski. Na pierwszy dźwięk trąby wojsko wstawało i zbroiło się, na drugi odgłos trąby — siodłało konie, na trzeci — ruszało w drogę. Przed bitwą Jagiełło

---

[53] A. Nadolski: *„Grunwald 1410"*. Wydawnictwo Bellona, Warszawa 1993, s.101-133.
[54] D. Strasburger: *„Zasady sztuki wojennej (od XI wieku do 1871 roku)"*. Skrypt AON, s.23.
[55] Z. Ryniewicz: *„Bitwy świata. Leksykon"*. Wiedza Powszechna, Warszawa 1995, s.217.

ukrył swoje wojska w gęstwinie lasów. W czasie bitwy grunwaldzkiej hasło rozpoznawcze brzmiało: „Kraków" — „Wilno". Ten rodzaj przedsięwzięć równoznaczny jest z ochroną informacyjną.

Polski król prowadził również rozpoznanie terenu i przeciwnika, wykorzystując do tego tzw. podjazdy. Podczas planowanej przeprawy przez Drwęcę, zwiadu dokonał najpierw podjazd, który zaskoczył przeciwnika, zajmując mu 50 koni. Dzięki podjazdowi dokładnie ustalono: rejony wojsk krzyżackich, bezpieczne miejsce na rozbicie obozu dla wojsk własnych, drogi przemarszu oraz punkty zaopatrzenia w żywność, wodę i drzewo. Ujawnienie obecności Krzyżaków i ufortyfikowania przeprawy nad Drwęcą spowodowało zmianę decyzji co do kontynuowania zamierzonego wcześniej marszu. Zdecydowano się na obejście rzeki u jej źródeł, a następnie kontynuowanie marszu na Malbork. Było to wielkim zaskoczeniem dla Zakonu, który początkowo ocenił to przedsięwzięcie jako ucieczkę. 15 lipca wojska sprzymierzonych zatrzymały się nad jeziorem Łubień. Zwiad doniósł o ruchach wojsk krzyżackich. Jagiełło przeprowadził rozpoznanie terenu i nakazał uchwycić zalesiony, pofałdowany teren, na zachód od jeziora. Powstał w ten sposób przesłaniający ekran, który mógł zapewnić czas i należyte ukrycie sił sprzymierzonych. Do spotkania z Krzyżakami doszło dzięki właściwej pracy oddziałów rozpoznawczych i ubezpieczeń operujących na bezpośrednim przedpolu Krzyżaków. Powyższa działalność równoznaczna jest ze zdobywaniem informacji.

Konstatując, można stwierdzić, że w prowadzonej kampanii polski król stosował elementy walki informacyjnej. Prowadząc działania pozorne i dezinformację, sprowokował przeciwnika do wystąpienia całością sił w celu stoczenia walnej bitwy. Ponadto podczas samej bitwy wykorzystał słońce do oślepienia wojsk krzyżackich, co utrudniło dokładne obserwowanie wojsk. Działania te można utożsamiać z zakłócaniem informacyjnym, ponieważ wnosiły do dowództwa krzyżackiego coraz bardziej nieuporządkowaną wiedzę o rzeczywistym otoczeniu, czyli innymi słowy zwiększały entropię informacyjną. Poprzez właściwe wykorzystanie informacji z rozpoznania uniknął strat podczas planowanej przeprawy przez Drwęcę oraz zajął dogodne miejsce do prowadzenia bitwy. Obronę informacyjną realizował przez ukrywanie swoich wojsk w gęstwinie lasów oraz stosowanie sygnałów umownych.

Dość wymownym przykładem skuteczności stosowania walki informacyjnej może być bitwa pod Kircholmem, prowadzona przez hetmana Karola Chodkiewicza 27 września 1605 roku. Siły polskie liczyły 4150 żołnierzy (3110 jazdy, 1040 piechoty oraz 7 dział), natomiast siły szwedzkie były znacznie większe, liczyły 10725 żołnierzy (2425 rajtarów, 8300 piechoty

oraz 11 dział).[56] Ogólna przewaga Szwedów była więc 2,5 krotna. Sukces Chodkiewicza polegał na tym, że zdołał wprowadzić przeciwnika w błąd, stosując bardzo skutecznie elementy obrony informacyjnej i zakłócania informacyjnego. Rozpoczął bitwę atakiem harcowników, a następnie upozorował ich ucieczkę. Wówczas natarł cały pierwszy rzut szwedzki, oddalając się o 1 km od drugiego rzutu. Zosatał ostrzelany i rozbity kontratakiem Woyny i rajtarii kurlandzkiej zanim drugi rzut przyszedł z pomocą. Chodkiewicz przywiązywał również wielką wagę do rozpoznania terenu i przeciwnika, czyli zdobywania informacji, co przyniosło efekt w końcowej fazie bitwy. Po rozbiciu pierwszego rzutu Szwedów i uzyskaniu przewagi na lewym skrzydle, Chodkiewicz postanowił właśnie na tym kierunku wykonać główne uderzenie, aby odrzucić Szwedów od Dźwiny i drogi prowadzącej do Rygi, zamykając im w ten sposób drogę odwrotu. Powodem podjęcia takiej decyzji były dane z rozpoznania. Jak wiadomo, bitwa zakończyła się bezładną ucieczką Szwedów, a ich straty wyniosły 8 tysięcy zabitych. Karol IX uciekł z jedną chorągwią rajtarów. Polacy stracili natomiast zaledwie 500 żołnierzy.

Z powyższego wynika, że polski hetman wprowadził wroga w błąd przez pozorację ucieczki, co można utożsamiać z zakłócaniem informacyjnym. W rezultacie tego Szwedzi dokonali złej oceny rzeczywistości, podjęli błędną decyzję i znaleźli się w niekorzystnej sytuacji. Chodkiewicz w ten sposób uzyskał przewagę nad przeciwnikiem już w początkowym etapie bitwy. Wykorzystując właściwie dane z rozpoznania okrążył przeciwnika i zamknął mu całkowicie drogę odwrotu. W wyniku zastosowania elementów walki informacyjnej przez stronę polską Szwedzi mający 2,5 krotną przewagę w bitwie, ponieśli całkowitą klęskę.

Także Napoleon stosował elementy walki informacyjnej. We wrześniu 1805 roku rozpoczął przemarsz wojsk z Francji do Europy Środkowej. Przegrupowanie realizował w ścisłej tajemnicy, w wyniku czego błyskawicznie przeprawił wojska przez Ren i dotarł do południowych Niemiec. Korzystając z zaskoczenia, okrążył 20.10.1805r. wojska austriackie pod Ulm, które liczyły 60 tysięcy żołnierzy i zmusił je do kapitulacji niemalże bez wystrzału. Punktem kulminacyjnym kampanii była bitwa pod Austerlitz, która miała miejsce 2 grudnia 1805 r. Stosunek sił przed bitwą kształtował się następująco: armia rosyjsko – austriacka liczyła 95 000 żołnierzy, a francuska 75 000[57]. Napoleon, licząc się ze wzmocnieniem sił sprzymierzonych, chciał jak najszybciej stoczyć z nimi bitwę. Przeprowadził dokładne rozpoznanie przeciwnika i terenu. Z oceny sytuacji wynikało, że przeciwnik zajął dogodne

---

[56] Z. Ryniewicz, op. cit., s.281.

[57] D. Strasburger: *„Zasady sztuki wojennej w kampaniach i bitwach od starożytności do wojny francusko – pruskiej 1870 – 1871"*. Bellona, Warszawa 1996, s. 85.

pozycje pod Ołomuńcem. Napoleon starał się wprowadzić przeciwnika w błąd. W tym celu, stwarzając pozory słabości, zasugerował sprzymierzonym niechęć do stoczenia bitwy. Car Aleksander i cesarz Józef uwierzyli, że Francuzi nie są przygotowani do bitwy, dlatego też rozpoczęli przemarsz w kierunku Austerlitz. Ich awangarda odrzuciła osłonowe jednostki kawalerii francuskiej, które zgodnie z zaleceniem nie stawiały oporu. Gdy Napoleon poprosił o zawieszenie broni, dowodzący wojskami sprzymierzonych uwierzyli, że przeciwnik nie jest przygotowany do bitwy i podjęli decyzję o rozpoczęciu ataku. Napoleon, prowadząc walkę informacyjną, z pozorowanej postawy obronnej przeszedł na czele swych wojsk do rozstrzygającego natarcia, zaskakując całkowicie przeciwnika. Zapewnił, przy pomocy minimalnych sił, uwikłanie go w walkę na każdym kierunku. Nad Goldbachem 10 000 żołnierzy przeciwstawił 42 000 Rosjan; na trakcie ołomunieckim 10 000 ludzi Lannesa i 7000 Murata przeciwstawił co najmniej 18 000 wojsk Bagratina i Liechtensteina, a bateriami ufortyfikowanego Santonu zabezpieczył obszar wyjściowy do przeciwnatarcia. Stosując elementy walki informacyjnej Napoleon spowodował, że bitwa prowadzona była w warunkach korzystnych dla niego. Sprowokował przeciwnika, który z dogodnych pozycji przegrupował się do rejonu nierozpoznanego, źle ocenił sytuację i wykonał uderzenie na niewłaściwym kierunku. Ponadto wykorzystał czynnik czasu na umocnienie się w wybranym terenie i dokładne przygotowanie bitwy. Straty sprzymierzonych wynosiły 27 000 zabitych i rannych. Straty Francuzów 1300 zabitych i 7000 rannych. Bitwa ta wzbudziła taki podziw, że często uznawana jest za najpiękniejszą i za przykład do naśladowania.

Patrząc na ten fakt pobieżnie można sądzić, że powodem klęski wojsk sprzymierzonych i warunkiem sukcesu wojsk napoleońskich było zaskoczenie. W rzeczywistości zaskoczenie było tylko ogniwem pośrednim pomiędzy napoleońskim sukcesem osiągniętym wcześniej w walce informacyjnej i sukcesem końcowym osiągniętym w walce zbrojnej. To właśnie skutecznie prowadzone działania pozorujące (zakłócanie informacyjne), maskowanie działań (obrona informacyjna), doskonałe rozpoznanie (zdobywanie informacji o przeciwniku), doprowadziły do uzyskania zaskoczenia, które już bezpośrednio przyczyniło się do sukcesu zbrojnego.

Walka informacyjna, chociaż tak formalnie nie nazywana, prowadzona była już od czasów najdawniejszych. Do pierwszej połowy XIX wieku realizowana ona była tylko w przestrzeni osobowej. Przestrzeń tę tworzył człowiek i wszelkie narzędzia wspomagające zasięg i czułość doznań zmysłowych. W zakresie rozpoznania człowiek posługiwał się głównie lunetą. Zakłócanie informacyjne polegało na wprowadzaniu w błąd przeciwnika

przez prowadzenie działań pozornych i dezinformacji. Obronę informacyjną realizowano przez ukrywanie wojsk oraz stosowanie sygnałów umownych za pomocą trąb lub chorągwi.

Odkrycia naukowe w pierwszej połowie XIX w. spowodowały, że walka informacyjna zaczęła być realizowana zarówno w przestrzeni osobowej, jak i technicznej. Pierwszym faktem w tym zakresie było wynalezienie telegrafu przez S. F. B. Morse`a w 1838 r. I opracowanie do niego alfabetu w 1840 r. Kolejnym była praca teoretyczna J. C .Maxwella (1831 — 1879), w której światło widzialne zostało uznane za falę elektromagnetyczną, co przyczyniło się do opracowania podstaw elektroniki. Następnie H. R. Hertz w latach 1887 — 1888 potwierdził przewidywania teoretyczne Maxwella, wytwarzając fale elektromagnetyczne o długości 1 m. W 1896 r. G. Marconi zbudował pierwszą radiostację, uzyskując po raz pierwszy w historii bezprzewodowe połączenie radiowe poprzez Zatokę Biskajską.

Podobne prace w tym zakresie (nadajnik i odbiornik radiowy) prowadził Rosjanin A. S. Popow. Na początku XX wieku po raz pierwszy zastosował on odbiornik radiowy do prowadzenia rozpoznania w celu poszukiwania okrętów na pełnym morzu. 8 marca 1904 r. admirał Makarow sprecyzował pierwsze zadania dla rozpoznania radiowego w czasie wojny rosyjsko — japońskiej[58].

Niemcy swój ośrodek rozpoznania radiowego (nasłuch i deszyfraż) zorganizowali w 1907 r. na wyspie Helgoland. Brytyjczycy i Francuzi rozwinęli rozpoznanie radiowe w latach 1912 — 1914.

Przykładem walki informacyjnej, realizowanej zarówno w przestrzeni osobowej jak i technicznej była bitwa pod Tangą, we wschodniej Afryce w 1914 roku, pomiędzy wojskami brytyjskimi i niemieckimi.[59] Na dowódcę brytyjskich sił ekspedycyjnych, liczących 8000 żołnierzy, został wyznaczony generał Aitken. W skład sił wchodzili żołnierze z północnego Lancasteru, Gurkowie oraz oddziały hinduskie z Armii Indyjskiej. Anglicy nie stosowali elementów zdobywania informacji oraz nie prowadzili obrony informacyjnej. Niemcy mieli bardzo dużo danych o zbliżaniu się Anglików. Na skrzyniach z zaopatrzeniem dla sił brytyjskich umieszczono nalepki z adresem „Hinduskie Siły Ekspedycyjne >>B<<, Mombasa, Afryka Wschodnia, natomiast prasa brytyjska i wschodnioafrykańska donosiła o zbliżaniu się armii. Depesze radiowe, między okrętami konwoju a Mombasą, przesyłano otwartym tekstem.

---

[58]H. Piekarski: *„Walka radioelektroniczna"*. Wydawnictwo MON, Warszawa 1980, s.19.
[59]G. Regan, op. cit., s.4-6.

Okręty brytyjskie płynęły bardzo blisko brzegów Afryki, były z lądu doskonale widoczne. Nie przeprowadzono rozpoznania portu ani też rejonu wyładunku. Dokonywano również rozminowania portu, który w ogóle nie był zaminowany. Oddziały brytyjskie zostały wysadzone na brzegu w odległości 1,5 km na południe od portu. Było to jedno z najgorszych miejsc, utrudnieniem był las drzew mangrowych pełen pijawek i węży wodnych, gdzie szalały moskity i muchy tse — tse. Wszystkie oddziały brytyjskie zeszły na ląd dopiero po 48 godzinach, co pozwoliło Niemcom na przygotowanie się do odparcia ataku. Stosunek sił wynosił 8:1 dla Brytyjczyków. Brytyjczycy nie przeprowadzili rozpoznania, nie wiedzieli więc gdzie znajdują się pozycje niemieckie i jakie są siły przeciwnika. Dlatego też nie zastosowano ogniowego przygotowania ataku z własnych okrętów. Niemcy okopali się mocno, wzmacniając linię obrony zasiekami z drutu kolczastego. Pomiędzy stanowiskami zorganizowano łączność telefoniczną. Karabiny maszynowe ustawiono w równych odstępach wzdłuż umocnień. Atak Brytyjczyków na pozycje niemieckie zakończył się fiaskiem. Ogólne straty wyniosły 800 zabitych, 500 rannych i 250 zaginionych. Straty niemieckie wyniosły: 15 zabitych i rannych Europejczyków oraz 54 Askarów.

Oceniając fakty należy stwierdzić, że Brytyjczycy ponieśli klęskę pomimo przewagi liczebnej w skali 8:1. Byli tak pewni swego zwycięstwa, że nie prowadzili obrony informacyjnej. Wszystkie informacje przesyłane były tekstem jawnym. Okręty płynęły w bliskiej odległości od brzegu i zostały dokładnie rozpoznane. Spowodowało to, że Niemcy już dużo wcześniej zostali uprzedzeni o mającym nastąpić ataku i mieli dużo czasu na doskonałe przygotowanie obrony. Ponadto nie przeprowadzono rozpoznania przeciwnika i terenu, w wyniku czego rozmieszczono wojska w bardzo niedogodnym rejonie. Niemcy odnieśli pełne zwycięstwo, a na dodatek przejęli cały sprzęt, który Anglicy zostawili na plaży po natychmiastowej ewakuacji

Elementy walki informacyjnej stosowano w bitwie warszawskiej w 1920 roku. Zaliczana ona jest do największych starć zbrojnych w dziejach oręża polskiego. Decydowała ona nie tylko o wyniku prowadzonej wojny, ale o losach narodu polskiego, który dopiero co odzyskał niepodległość. Bitwa ta ma także wymiar europejski, jako że strategiczne cele Rosji Radzieckiej wybiegały znacznie poza militarne rozgraniczenie Polski. Bolszewicy uznali bowiem, że są na tyle silni, by przystąpić do rewolucji światowej. Strona polska przygotowywała i prowadziła bitwę w niezwykle trudnym położeniu operacyjnym. Po porażkach na Ukrainie i Białorusi Wojsko Polskie nieprzerwanie cofało się na całym froncie

wschodnim. Planowano przeprowadzić operację obronną oraz, wykorzystując błędy w ugrupowaniu przeciwnika, przejść do operacji zaczepnej.[60]

Dowódca Frontu Płn — Zach., M. Tuchaczewski rozpoczął 4 lipca 1920 roku ofensywę w kierunku Warszawy, mając 105 000 żołnierzy i 595 dział.[61] Liczebność wojsk rosyjskich pod koniec operacji wzrosła do około 140 000 — 160 000. Polskie siły liczyły 69 000 żołnierzy. Bitwa warszawska trwała od 13 do 20 sierpnia i składała się z trzech faz:

— obrony przedmieścia warszawskiego i linii Wisły, Wkry i częściowo Narwii (13 — 15 sierpnia);
— ofensywy znad Wieprza i wypierania przez polską 5 armię przeciwnika za Narew (16 — 18 sierpnia);
— pościgu oraz próby osaczenia i rozbicia 4 armii rosyjskiej (19 — 25 sierpnia).

Straty polskie w bitwie wyniosły: 4500 zabitych, 22 000 rannych, 10 000 zaginionych. Natomiast straty rosyjskie oceniane są na około 25 000 zabitych, 66 0000 jeńców i około 30 000 internowanych w Prusach Wschodnich.

Szef sztabu generalnego WP gen. Rozwadowski nakazał stosować zasady maskowania (element ochrony informacyjnej) przez ukrywanie stanowisk środków ogniowych i artylerii oraz używanie tych środków tylko w okresach przełomowych.

Generał Sikorski, dowódca 5 armii, wprowadzał w błąd przeciwnika (element walki informacyjnej) co do własnych posunięć. Skierował grupę składającą się z 8 samochodów pancernych, która prowadziła dywersję na tyłach przeciwnika. Ponadto nad Wieprzem wyznaczono do specjalnych zadań grupę uderzeniowa, która, jak się później okazało, odegrała decydującą rolę w bitwie.

Konstatując można stwierdzić, że strona polska lepiej potrafiła zastosować elementy walki informacyjnej. Posiadała aktualne dane z rozpoznania, wykorzystując do tego celu między innymi lotnictwo. Strona rosyjska nie posiadała wiarygodnych danych o przeciwniku. Tuchaczewski dowodził wojskami z Mińska, nie posiadał dostatecznych środków łączności i dlatego miał słabą orientację w dynamice prowadzonej walki. Z dwudniowym opóźnieniem dowiadywał się o wydarzeniach na froncie. Strona polska prowadziła także działania wprowadzające w błąd przeciwnika (zakłócanie informacyjne). W wyniku tego niespodzianką dla wojsk rosyjskich było pojawienie się nad Wkrą 5 armii polskiej oraz koncentracja nad Wieprzem polskiej grupy uderzeniowej. Ponadto ukrywano wojska i sprzęt, co jest tożsame

---

[60] L. Wyszczelski: *„Warszawa 1920"*. Wydawnictwo Bellona, Warszawa 1995.
[61] Z. Ryniewicz, op. cit., s.588.

z obroną informacyjną.

Podsumowując dotychczasową analizę literatury przedmiotu badań, można stwierdzić, że *od drugiej połowy XIX wieku nastąpiło przeniesienie części walki informacyjnej z przestrzeni osobowej do technicznej. Jednak do końca I wojny światowej, w aspekcie technicznym realizowana ona była głównie w przestrzeni zdobywania informacji. Do urządzeń rozpoznawczych, wykorzystywanych w tym czasie należy zaliczyć: telegraf, telefon i odbiornik radiowy. Do technicznego zakłócania informacyjnego nie przywiązywano jeszcze większej wagi, co związane było z brakiem odpowiednich stacji zakłócających. W 1917 r. Niemcy próbowali stosować zakłócenia radiowe lotnictwa francuskiego i brytyjskiego (głównie meldunki przekazywane z samolotów rozpoznawczych). Jednak w większym stopniu dezorganizowały one łączność radiową niemieckiego lotnictwa aniżeli lotnictwa przeciwnika.*

Przygotowanie i wykonanie operacji „Overlord" we Francji, w 1944 roku, dało możliwość przeprowadzenia klasycznych studiów nad walką informacyjną. Operacja „Overlord" opierała się na wprowadzeniu w błąd przeciwnika, co polegało na podawaniu Niemcom fałszywych danych, że inwazja nastąpi w Norwegii i w rejonie Pas de Calais we Francji, w Grecji, we Włoszech i w rejonie Zatoki Biskajskiej. Dwie aplikacyjne armie: 1A amerykańska dowodzona przez generała Georga S. Pattona i 4A brytyjska, wyposażone w makiety samolotów, okrętów desantowych, czołgów oraz radiostacje i zabezpieczenie logistyczne prowadziły pozorne szkolenie w Dover. Ponad 20 oficerów brytyjskich spędziło miesiące w Szkocji wymieniając fałszywe komunikaty radiowe dla brytyjskiej armii, stacjonującej w Szkocji i zamierzającej zaatakować Norwegię w połowie lipca[62]. Aby operacja „Overlord" była bardziej wiarygodna, miesięcznie wytwarzano ponad 250 000 zdjęć rozpoznawczych. Aplikacyjne rozpoznanie brzegowe rozpoczęło się na D—150, na podstawie analizy szczegółowych map terenu w skali 1:50 000, które opracowywano jako modele dla taktycznych planistów (analiza terenu w państwach NATO jest elementem informacyjnego przygotowania pola walki — IPB). Powołano amerykańsko — brytyjski Zarząd Rozpoznania i Zakłócania. Jego zadaniem było zabezpieczenie łączności własnych sił i zakłócanie środków łączności i radarów niemieckich, szczególnie samolotów rozpoznawczych Luftwaffe, które mogły wykryć i zniszczyć okręty przepływające przez kanał La Manche. W tym celu wykorzystywano brytyjskie morskie i powietrzne stacje zakłóceń, takie jak: „Ground Cigar", „Aspirin", „Grover" i „Tuba". Brytyjskie siły powietrzne RAF zrzucały paski folii metalowej wzdłuż kanału La Manche, aby symulować ruch okrętów w kierunku Pas de Calais we

[62]R. F. Riccardelli: *The Information and Intelligence*. W: *„Military Review"*, 5/95, s.83.

Francji. Do naprowadzania samolotów wykorzystywano system Oboe. Zasada pracy tego systemu polegała na współdziałaniu samolotu z dwiema stacjami naziemnymi, zwanymi „kot" i „mysz". Zadaniem stacji „kot" było utrzymywanie samolotu na określonej trasie, dokładnie na kierunku celu. Ze stacji „mysz", robiono pomiary odległości i prędkości przelotu. Samolot prowadzony przez Oboe musiał przebyć ostatni odcinek trasy na określonej, stałej wysokości, gdyż inaczej dane odbierane przez stację „mysz" byłyby niedokładne. Do działań wykorzystano samoloty De Havilland Mosquito, które dzięki znacznej prędkości i pułapowi były trudnym obiektem ataku dla przeciwnika, a jednocześnie ich drewniana konstrukcja praktycznie uniemożliwiała wykrycie za pomocą radaru.

Aby upewnić się, że Niemcy odbierają fałszywe komunikaty, sprzymierzeni rozkodowywali przechwycone szyfrowane komunikaty „Ultra"[63]. Hitlerowcy, opierając się na opiniach swych najwybitniejszych matematyków, uważali to stale udoskonalane urządzenie do przekazywania przez radio najtańszych rozkazów, raportów i innej korespondencji za absolutnie pewne i nierozwiązywalne. Nawet jeśli jakiś egzemplarz maszyny wpadłby w ręce przeciwnika, to zmieniana codziennie pozycja wyjściowa i klucz — inny dla każdej depeszy — teoretycznie uniemożliwiały odczytanie zakodowanej informacji. A jednak dzięki polsko — francuskim wysiłkom tajemnica „Enigmy" została teoretycznie i praktycznie rozwiązana i to na kilka lat przed wojną. Starszy oficer brytyjskiego wywiadu lotnictwa F. W. Winterbotham[64], który kierował zespołem kryptologów, po raz pierwszy w piśmiennictwie historycznym przedstawił ogrom informacji o przeciwniku, jakie ze źródła „Ultra" czerpały naczelne dowództwa i sztaby sojusznicze w czasie II wojny światowej. Rozszyfrowywane meldunki niemieckie „Ultra" ujawniły, że Niemcy spodziewali się głównego uderzenia w rejonie Pas de Calais.

Alianci obawiali się, że Niemcy mogą rozpoznać te działania jako fałszywe. Aby mieć pewność, że zdjęcia lotnicze robione przez Niemców nie przyczynią się do rozpoznania, że sprzęt znajdujący się w rejonach ćwiczeń, to tylko makiety, siły koalicji zmusiły niemieckie samoloty rozpoznawcze do lotów na wysokości powyżej 33 000 stóp (9900 m.). Na podstawie zdjęć wykonanych z tej wysokości Niemcy nie mogli rozróżnić rzeczywistego sprzętu od makiet pozorujących obiekty wojskowe.

---

[63] „Ultra" (inaczej „Enigma") - nazwa elektrycznej maszyny szyfrującej, którą - począwszy od 1926/1927 roku aż do załamania hitlerowskiej IIIRzeszy - posługiwały się z pewnymi modyfikacjami, zarówno niemieckie wojska lądowe (Heer), marynarka (Kriegsmarine) i lotnictwo (Luftwaffe), jak też centralne instytucje policji - SS i SD. Władysław Kozaczuk: *„Wojna w eterze"*, Warszawa 1977, s.40.

[64] F. W. Winterbotham: *„The Ultra Secret"*, Londyn 1974.

Meldunki wysyłane przez najbardziej zaufanych agentów niemieckich (szpiegów niemieckich) w Wielkiej Brytanii były pisane przez agentów koalicji. Dzięki programowi „podwójny system łączności" („Double-Cross System"), większość niemieckich szpiegów stała się podwójnymi agentami, a ich meldunki do Niemiec przekazywane były umiejętnie przez brytyjskie i amerykańskie służby wywiadowcze. Więcej niż 2000 żołnierzy z korpusu ochrony zapewniało bezpieczeństwo w obszarach, na których znajdowały się poczty. Całość korespondencji dyplomatycznej wychodzącej z W. Brytanii, z wyjątkiem amerykańskiej i rosyjskiej, była sprawdzana.

Brytyjskie dowództwo potrzebowało jednak ostatecznego argumentu, który przekonałby Niemców, że inwazja nastąpi w rejonie Pas de Calais. Należało znaleźć człowieka o niepodważalnym autorytecie, który mógłby potwierdzić te dane. Sytuacja była sprzyjająca, ponieważ generał Hans Cramer, ostatni dowódca Afrika Korps, przebywał w obozie w Anglii. Ze względu na stan zdrowia wyrażono zgodę na przewiezienie go do Niemiec. Wcześniej jednak generał odbył podróż z południowej Walii do Londynu. Była to dziwna podróż, przebiegała okrężną trasą, prowadzącą przez okolice Portsmouth, gdzie stacjonowały jednostki 21. Grupy Armii. Generał obserwował maszerujące oddziały żołnierzy, sznury ciężarówek, zmierzające w kierunku portów, ale nie mógł dostrzec żadnej tablicy z nazwą miasta, ponieważ zostały usunięte wcześniej, gdy Anglia szykowała się do odparcia inwazji niemieckiej. Gdzieniegdzie natomiast ustawiono fałszywe tablice, które sugerowały, że znajduje się w rejonie Dover. Po drodze zjadł obiad z generałem Pattonem i dowódcami kilku dywizji. 23 maja 1944 r. Cramer dotarł do Niemiec i został natychmiast przyjęty przez Kurta Zeitzlera, szefa sztabu, któremu zrelacjonował całą sytuację. Został doradcą generała Geyra von Schweppenburga. Jego wrażenia, jakie odniósł w Anglii, wpłynęły na decyzje ludzi odpowiedzialnych za przygotowanie wojsk niemieckich do odparcia inwazji.

6 czerwca 1944 rozpoczęła się główna faza operacji w Normandii. Po ciężkim bombardowaniu lotniczym i ostrzale z 107 okrętów wojennych nastąpił desant wojsk sprzymierzonych. Feldmarszałek von Rundstedt skierował do walki z desantem dwie dywizje pancerne, jednak nie był pewny, czy właściwie ocenia sytuację, gdyż był przekonany, że inwazja nastąpi w innym rejonie. Starał się powiadomić o sytuacji kwaterę Hitlera. Meldunek jednak odebrał generał Jodl, który wydał rozkaz natychmiastowego zatrzymania czołgów.

W tym samym czasie z Madrytu napłynęła depesza od generała Ericha Kuhlenthala, który donosił, że operacja normandzka jest manewrem odwracającym uwagę Niemców, aby

ściągnąć rezerwy w rejon przyczółków i przeprowadzić decydujące uderzenie w innym miejscu.

Hitler w końcu dowiedział się o zaistniałej sytuacji. Po naradzie z najwyższymi dowódcami ocenił operację w Normandii jako wprowadzającą w błąd. Dlatego też nakazał utrzymać 15 armię w rejonie Pas de Calais i wzmocnić pozycje obronne.

Do 12 czerwca na ląd wysadzono 326 500 żołnierzy z 54 185 pojazdami. Ze względu na zastosowane elementy walki informacyjnej uzyskano zaskoczenie przeciwnika. Dlatego też straty wojsk sprzymierzonych były małe i wyniosły 3%.

Operacja „Overlord" była klasycznym przykładem zastosowania wszystkich elementów walki informacyjnej, realizowanej zarówno w przestrzeni osobowej jak i technicznej. Na szeroką skalę prowadzono działania pozorne, dezinformację i mylenie, co można utożsamiać z zakłócaniem informacyjnym. Pozorowano naloty lotnictwa na Pas de Calais z wykorzystaniem dipoli odbijających oraz ruch okrętów za pomocą pasków folii metalowej. Czołgi i samochody pozorowano za pomocą makiet. W rejonach pozorowanej dyslokacji wojsk zmuszano rozpoznawcze samoloty niemieckie do wykonywania lotów na dużych wysokościach, co uniemożliwiało identyfikowanie rzeczywistej sytuacji. Wykorzystując podwójnych agentów przekazywano meldunki do Rzeszy, które były zgodne z kreowaną sytuacją. Prowadzono zdobywanie danych o przeciwniku i terenie. Wykorzystując urządzenia elektroniczne rozpoznano dyslokację posterunków radiolokacyjnych wchodzących w skład systemu wykrywania celów powietrznych i nawodnych. Zastosowane elementy walki informacyjnej wprowadziły w błąd dowódców niemieckich, którzy uwierzyli, że Pas de Calais było głównym obiektem inwazji. Uwierzyli także, że alianci mieli 89 dywizji przygotowanych do inwazji oraz wystarczającą liczbę okrętów desantowych dla 20 dywizji. W rzeczywistości było tylko 39 dywizji i wystarczająca liczba okrętów dla pięciu dywizji.

Od drugiej wojny światowej (operacja Overlord 1944 r.) techniczna walka informacyjna była prowadzona już w trzech przestrzeniach: zdobywania informacji, zakłócania i obrony informacyjnej. Wysiłek rozpoznania skupiano głównie na zdobywaniu danych w relacjach łączności radiowej oraz na lokalizacji środków radiowych i radiolokacyjnych. W tym celu wykorzystywano urządzenia naziemne oraz okręty i samoloty rozpoznawcze. Zakłócaniem i obroną informacyjną objęto środki radiowe i radiolokacyjne (system łączności radiowej dowodzenia, współdziałania i kierowania ogniem artylerii, system naprowadzania i radionawigacji lotnictwa). W prowadzonej walce jedną z głównych ról zaczęło odgrywać środowisko elektromagnetyczne. W związku z tym, że z jego zakresu

wykorzystywano głównie fale radiowe, prowadzoną walkę zaczęto nazywać walką w eterze (radiową), radioelektroniczną lub elektroniczną.

Wojna w Zatoce Perskiej ukazała w sposób szczególny znaczenie technologii informacyjnej na współczesnym polu walki.

Generał Powell, wypowiadając się na temat tej wojny stwierdził: „Polowy system rozpoznawczy stwarzał o wiele większe możliwości niż istniejące potrzeby w tym zakresie w czasie tej wojny. Komputery osobiste zwielokrotniły jeszcze te możliwości". Istotnym czynnikiem w tej operacji było pozyskiwanie informacji i jej analiza, co pozwalało na korzystny wybór celów do zniszczenia. Taka działalność doprowadziła do tego, że Saddam Hussein w pierwszych dniach wojny stał się ślepym, głuchym i niemym wodzem. Zakłócanie informacyjne prowadzone przez koalicję doprowadziło do tego, że Saddam nie był w stanie śledzić położenia ani wojsk własnych, ani koalicji.

Podczas całej fazy przygotowawczej i w trakcie trwania działań wojennych planiści koalicji zasypywani byli ogromną ilością informacji. Wielkości te obrazuje wyciąg z jednego dnia pracy:[65]

— 700 000 rozmów telefonicznych;

— 152 000 przesłanych faksów i tekstów dalekopisowych;

— 35 000 wykrytych i wykorzystanych częstotliwości pracy środków łączności.

Te ogromne możliwości zabezpieczała ogromna sieć łączności na bazie systemu „TRI—TAC". Satelity były jednym z najważniejszych czynników, umożliwiających siłom lądowym USA szybkie i bezkolizyjne przegrupowanie wojsk przy ograniczonym wykorzystaniu sieci łączności taktycznej w rejonie działań. Oprócz systemu łączności satelitarnej „FLEETSATCOM", wykorzystywane były systemy „DSCS—II" i „DSCS—III". W ciągu jednego miesiąca liczba terminali naziemnych pracujących w paśmie od 3 do 30 GHz zwiększyła się z czterech do 49, a w końcowym etapie wynosiła 141. Uruchomiono satelity NATO i rozwinięto 11 linii łączności dalekosiężnej T-1. Ogółem stan wykorzystania poszczególnych systemów wynosił:

— DSCS — 75%;

— NATO — 5%;

— satelity cywilne — 20%.

W lutym 1991 rozwinięto 35 troposferycznych linii radioliniowych i mikrofalowych. Na teatrze działań znajdowało się 20 central telegraficznych i 60 central telefonicznych

---

[65] A. D. Campen: *„The first Information War"*, Virginia 1992, s.22.

systemu „TRI-TAC". Ponadto wykorzystywano system „PTARMINGAN" i „RITA". Siły morskie w głównej mierze wykorzystywały system „TACSAT". Liczba użytkowników komutacyjnego systemu informacji cyfrowej „CUDIX" i sieci radiowej SM została potrojona. Na mocy porozumienia z Wielką Brytanią wykorzystywano system „SKYNET". Doświadczalnie zestawiono łącze zakresu fal milimetrowych „EHF SATCOM" dla zabezpieczenia utajnionej łączności pomiędzy Kolegium Połączonych Szefów Sztabów a Dowództwem PSZ NATO Europy Środkowej. Rozwinięto sieci „AUTOVON" i „AUTODIN". System abonentów ruchomych „MSE" zabezpieczał łączność w rejonie działań bojowych poprzez system „TRI-TAC".

„Pustynna Burza" była pierwszą główną operacją militarną prowadzoną w erze mikroprocesorów. Naczelne dowództwo, dowództwa sił zbrojnych (rodzajów służb) i oddziałów były połączone w sieć komputerową, która zabezpieczała planowanie złożonych operacji, sporządzanie dokumentów, mobilizację, rozwijanie i przegrupowanie sił zbrojnych. System planowania i prowadzenia połączonych operacji „JOPES" oparty był na komputerach Honywell. Połączenie między adresatami zabezpieczały:

— sieć transmisji danych utajnionych „DSNET2";

— sieć transmisji danych jawnych.

Informacje z rozpoznania przesyłane były dwoma sposobami. Jednym z nich było wykorzystanie systemu „TRI—TAC", wyposażonego w telefony utajnione typu „STU—III" i „KY—68". W tym wypadku informacje przekazywano od szczebla dowództw sił zbrojnych do szczebla pododdziałów. Drugim sposobem było bezpośrednie przekazywanie (droga radiową) aktualnych informacji z banku danych do skrzydeł i eskadr oraz korespondentów naziemnych.

„Wojna w Zatoce Perskiej była wojną, podczas której uncja krzemu w komputerze przynosiła większe efekty niż tona uranu"[66]. Pod względem ważności wiedza staje się rywalką broni i taktyki z chwilą, gdy damy wiarę teorii, że wroga można rzucić na kolana, niszcząc lub uszkadzając środki służące dowodzeniu i kontroli. Jednym ze wskaźników rosnącego znaczenia wiedzy w sposobie prowadzenia wojen jest komputeryzacja. Dosłownie każdy aspekt wojny jest dziś zautomatyzowany, wymaga warunków do przenoszenia znacznej liczby danych w wielu różnych postaciach. Pod koniec Pustynnej Burzy w strefie wojny funkcjonowało ponad trzy tysiące komputerów, połączonych z komputerem znajdującym się w Stanach Zjednoczonych. Na ekranach telewizyjnych odbiorcy widzieli samoloty, działa

[66] A. Campen, op. cit., s. 11.

i czołgi, lecz nie widzieli nieuchwytnego przepływu informacji, danych i wiedzy, dziś nieodzownych dla wykonania najzwyklejszych funkcji wojskowych. Nad Zatoką Perską unosiła się najpotężniejsza broń informacyjna — aparatura systemu AWACS i J—STARS. System AWACS (Airborne Warning and Control System) wykrywał każdy wrogi samolot lub rakietę, przekazując dane do myśliwców w celu naprowadzenia ich na cel oraz do urządzeń naziemnych. Odpowiednikiem tego systemu, wykrywającym obiekty naziemne, był J—STARS (Joint Surveillance and Target Attack Radar System) — połączony radarowy system rozpoznania i ataku. Miał on pomagać w wykryciu, rozerwaniu i zniszczeniu przegrupowujących się oddziałów sił lądowych wroga. Dwa samoloty systemu J—STARS wykonały 49 lotów, zidentyfikowały ponad 1000 celów (włączając w to konwoje, czołgi, samochody ciężarowe, wozy bojowe piechoty i działa) oraz nadzorowały 750 myśliwców. Jak mówi generał Thomas S. Swalm z SP USA, siły powietrzne kierowane przez ten system w dziewięćdziesięciu procentach znajdowały cel za pierwszym razem. W tym samym czasie, w którym siły koalicyjne były zajęte zbieraniem, analizowaniem i rozdzielaniem informacji, prowadziły one także przedsięwzięcia związane z niszczeniem informacji i łączności przeciwnika. Najwcześniejsze ataki sił koalicji kierowane były na emitery mikrofalowe, centrale telefoniczne, stacje przekaźnikowe, węzły światłowodów, mosty, po których przebiegały koncentryczne kable komunikacyjne. Oprócz stosowania systemów precyzyjnego rażenia, zrzucane były paski folii metalowej. Prowadziło to albo do przerwania pracy tych urządzeń, albo zmuszało dowództwo irackie do użycia anachronicznych systemów, umożliwiających podsłuch, który dostarczał wartościowych informacji wywiadowczych. Te właśnie ataki, sprzężone z uderzeniami bezpośrednio wymierzonymi w polityczne ośrodki dowodzenia Saddama, zmierzały do zniszczenia lub izolowania irackiego dowództwa, odcięcia go od oddziałów pozostających na froncie. Zadanie polegało na rozerwaniu mózgu i układu nerwowego sił zbrojnych Iraku. Jeśli jakaś część tej wojny miała charakter operacji chirurgicznej, była to, jeśli można tak powiedzieć, operacja chirurgiczna mózgu.

Jak konkluduje Alan D. Campen, wojna w rejonie Zatoki Perskiej, w porównaniu z analizowanymi poprzednio, miała inny charakter. Wynik jej ukazał wyższość zastosowania wiedzy (informacji) nad działaniem systemów broni i ilością stanu osobowego. Należy o tym mówić, dlatego że historia mogłaby przeoczyć lub obniżyć wartość kluczowej roli odegranej przez systemy informacyjne i ludzi, którzy je zbudowali. Te bezcenne aktywa mogłyby zostać nie zauważone i stracone bezpowrotnie, gdyż bez wyjaśnienia nie zostałyby należycie zrozumiane.

Szef Sztabu SZ USA nazwał operację „Pustynna Burza" wojną wiedzy („knowledge war"). Systemy broni, które doprowadziły do dewastacji infrastruktury i machiny wojennej Iraku były rozmieszczone w rejonie i wokół Zatoki Perskiej. Systemy wsparcia, zabezpieczające „broń inteligentną", były rozmieszczone na całym świecie (wokół Ziemi), w przestrzeni kosmicznej.

Jak twierdzi były przewodniczący komitetu badania przestrzeni kosmicznej, Ralph W. Shrader, „nigdy przedtem zapotrzebowanie na błyskawiczny przekaz informacji nie było tak pilną potrzebą jak w tej wojnie". Siły zbrojne z wielu krajów działały razem przez wykorzystanie różnego rodzaju systemów łączności o zasięgu i złożoności nieznanej dotąd w historii wojskowości.

Iracki system dowodzenia i kontroli był pierwszym celem ataku w czasie operacji „Pustynna Burza". Irak stał się pierwszą w historii ofiarą walki, którą dziś Departament Obrony USA nazywa walką informacyjną. Jej ważnym aspektem są różnice informacyjne. Irak rozpoczął swoją inwazję na Kuwejt przy wykorzystaniu systemu OP budowanego na bazie sprzętu z różnych krajów, takich jak: Niemcy, Francja i Rosja.

Według Williama A. Burhansa[67], główne cele Iraku były osłaniane przez rosyjskie pociski typu: SA—2, SA—6 „Kwadrat", SA—8 „Osa", podczas gdy jednostki sił zbrojnych przez: SZU—23—4 „Szyłka", SA—3 „Strzała 10" i przenośne zestawy SA—14 „Strzała 3".

Panowanie w powietrzu (pierwszy istotny czynnik walki powietrzno — lądowej) zostało osiągnięte w momencie rozpoczęcia ataku powietrznego i było utrzymywane cały czas w trakcie trwania wojny poprzez:

— powtarzanie ataków powietrznych;

— przekazywanie fałszywych meldunków o zniszczonych obiektach lotniczych;

— wytwarzanie chmur antyradarowych przez helikoptery i izolowanie tym samym OP Iraku.

Dziennikarz - lotnik, James P. Coyne[68], wypowiadając się na temat OP Iraku, stwierdza, iż rzeczą najważniejszą jest to, że system ten zbudowany był zgodnie z modelem rosyjskim, uzależnionym w 100% od kontroli scentralizowanej. Główne (centralne) stanowisko dowodzenia Saddama, infrastruktura dowodzenia i łączności zostały poważnie zdezorganizowane zaraz po rozpoczęciu nalotu powietrznego i nie były usprawnione do końca wojny. Baterie obrony przeciwlotniczej, po zerwaniu łączności z centrum dowodzenia,

---

[67]W. A. Burhans: *Iraqi Air Defenses - Initial Soviet Post – Mortem.* W: *„Journal of Electronic Defense"*, October 1991, s.17.

[68]J. P. Coyne:*(Of the 35 first-day targets in Baghdad, 29 were Command centers, headquarters complexes and telephone and electrical switching centers). Airpower in the Gulf.* W: *„Air Force Association"*, 1992, s.9.

nie były w stanie prowadzić żadnych skoordynowanych działań. Nie działał żaden system wczesnego wykrywania i ostrzegania o celach powietrznych. Obronę przeciwlotniczą stać było tylko na prowadzenie ognia zaporowego, który nie był zagrożeniem dla samolotów sił koalicyjnych.

Oficerowie sił zbrojnych Rosji, którzy uczestniczyli w naradzie okrągłego stołu, poświęconej wojnie w rejonie Zatoki Perskiej stwierdzili, że były dwa powody zniszczenia systemu powietrznego Iraku. Po pierwsze: całkowite, bez żadnego oporu bombardowanie irackich pozycji ze średnich wysokości (systemy obrony nie miały możliwości wykrywania i zwalczania celów powietrznych na tych wysokościach). Po drugie: stosowanie przez Irak technologii lat 1950/1970, które Amerykanie poznali dokładnie w ciągu wojen arabskich i znaleźli antidotum na nie. Ponadto sam czas trwania tak intensywnej operacji jest sam w sobie ewidentnym niszczycielskim czynnikiem, który mógłby być pokonany przez zastosowanie walki elektronicznej[69].

A. Campen zadaje kilka pytań: Co należy robić z rolą informacji, jaką odegrała w Pustynnej Burzy? Czy będzie to zwiastun jednego z rzadkich w historii wojen momentu, który kształtuje strukturę i doktrynę sił zbrojnych? Dalej konkluduje, że odpowiedź w dużej mierze zależy od tego, na ile ludzie, którzy określają struktury sił zbrojnych, będą mogli zrozumieć i zastosować istotę walki informacyjnej: tzn. systemy, stan osobowy, procedury i kierowanie tymi strukturami, które doprowadzi ich do perfekcyjnego działania i bez którego strategia wiedzy, prowadząca do zwycięstwa, nie mogłaby być zastosowana w ogóle.

Przez odpowiednie wykorzystanie danych Amerykanie i ich sojusznicy pokonali potężną machinę wojenną Iraku, zadziwiając świat oraz najbardziej zaciekłych krytyków departamentu obrony. Ponadto dostrzeżono znaczenie mediów na współczesnym polu walki; stały się one nowym, ważnym narzędziem w walce informacyjnej.

Historia walki informacyjnej jest tak samo długa, jak długa jest historia wojen. Prowadzona była od czasów najdawniejszych, od kiedy tylko pojawiły się konflikty.

W czasie wojny w rejonie Zatoki Perskiej Stany Zjednoczone ujawniły radykalnie nową kategorię walki, którą formalnie nazwano „walką informacyjną".

Przez stosowanie elementów walki informacyjnej uzyskano dużą elastyczność, synchronizację i szybkość prowadzonych działań, krótki czas reakcji ogniowej i wysoką precyzję rażenia w skali do tej pory niespotykanej w historii wojskowości. Może to

---

[69] O. Falicber: *Shilka`versus the B-52*. W: *„Krasnaja Zwiezda"* (Red Star), April 3, 1991.

spowodować całkowitą zmianę standardów użycia sił zbrojnych w konflikcie zbrojnym w przyszłości.

Dzięki stosowaniu technologii informacyjnych, znacznie mniej liczebne i słabiej wyposażone siły zbrojne mogą odnieść zwycięstwo nad liczebniejszym i lepiej wyposażonym przeciwnikiem.

Po wojnie w rejonie Zatoki Perskiej wiele krajów zaczęło przywiązywać dużą uwagę do obszaru walki informacyjnej. W problematyce tej przodują Stany Zjednoczone, które mają szeroko zakrojone plany zrewolucjonizowania obszaru działań zbrojnych za pomocą techniki informacyjnej, tak jak zrewolucjonizowały go czołgi podczas pierwszej i bomba atomowa podczas drugiej wojny światowej.

Nowe środki walki i przewidywania co do ich rozwoju powodują zmiany w poglądach i sposobach prowadzenia działań wojennych. Same prototypy, lub tylko naukowo-techniczne pomysły przyszłej broni, są zaczynem nowych koncepcji i założeń taktycznych i operacyjnych, a nawet strategicznych. Można powiedzieć, że wiedza wojskowa jest produktem myślenia prognostycznego, rezultatem refleksji o przyszłym polu walki.

1.7. Wnioski

„Informacja" to bodziec oddziałujący na układ recepcyjny człowieka, powodujący wytwarzanie w jego wyobraźni przedmiotu myślowego, odzwierciedlającego obraz rzeczy materialnej lub abstrakcyjnej (przedmiotu, procesu, zjawiska, pojęcia). Innymi słowy, informacja to tylko takie doznanie, które inspiruje umysł ludzki do pewnej wyobraźni.

„Dane" to informacje potencjalne, które dopiero po odpowiednim opracowaniu (przy wykorzystaniu odpowiedniego klucza) mogą stać się informacjami przydatnymi w działaniu celowym. Dlatego konieczne jest ich przekształcanie w odpowiednie sygnały informacyjne bądź sterujące.

„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.

„Komunikat" to pewna porcja informacji przekazana adresatowi (do układu odbierającego) w „czystej" formie, czyli w postaci komunikatywnej dla zmysłów człowieka.

„System informacyjno — sterujący" to zespół sił i środków powiązanych ze 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.

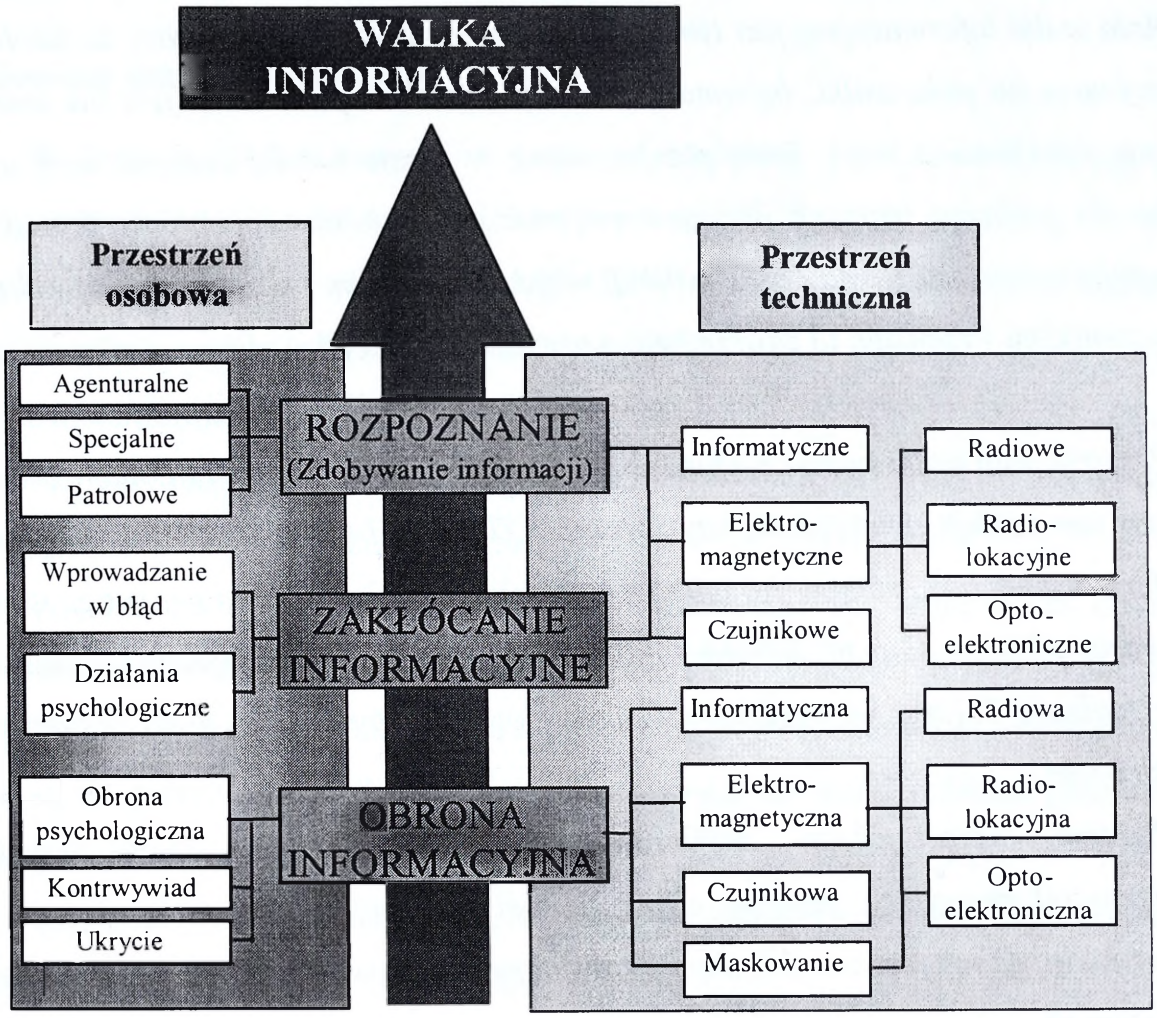
„Walka informacyjna" jest to kooperacja negatywna wzajemna realizowana w sferze rozpoznania (zdobywania informacji), zakłócania informacyjnego i obrony informacyjnej, gdzie każdemu działaniu jednego podukładu tej walki jest przyporządkowane działanie antagonistyczne dwóch pozostałych podukładów strony przeciwnej.

Istota walki informacyjnej sprowadza się do stwarzania sytuacji utrudniających przeciwnikowi podejmowanie trafnych decyzji, wykonywanie sprawnych ruchów wojskami i precyzyjnych uderzeń ogniowych, przy jednoczesnej obronie przed tym samym wojsk własnych. Innymi słowy, ukierunkowana jest na dezorientowanie przeciwnika co do sytuacji na polu walki, komplikowanie jego warunków działania i w efekcie zmuszanie go do podejmowania błędnych decyzji.

„Przedmiotem walki informacyjnej" są systemy informacyjno — sterujące i ich otoczenie.

Celem walki informacyjnej jest dążenie do stworzenia przeciwnikowi fałszywego obrazu rzeczywistości i przez to ukierunkowanie jego wysiłków na planowanie i prowadzenie działań w stosunku do nieistniejących lub nieistotnych odniesień. Do realizacji tego celu każda ze stron tworzy system rozpoznania, zakłócania i obrony informacyjnej. W skład tych systemów wchodzą zespoły ludzkie i wszelkiego rodzaju urządzenia techniczne (dostosowane do spełniania swej roli w środowisku elektromagnetycznym, akustycznym, elektrycznym, magnetycznym i chemicznym), które można nazwać narzędziami walki informacyjnej. Urządzenia te wspomagają możliwości recepcyjne i analityczne człowieka w przestrzeni bezpośrednio dla niego niepoznawalnej, wykraczającej poza jego zmysły. Np. w zakresie rozpoznania do urządzeń tego typu można zaliczyć między innymi: odbiorniki, namierniki radiowe, stacje radiolokacyjne, bezzałogowe aparaty latające, czujniki, rejestratory, analizatory, fotopowielacze, scyntylatory itp. W walce informacyjnej każda ze stron będzie dążyć do wypracowania takiej decyzji o użyciu narzędzi walki, które będą sprzyjać najlepszemu ich wykorzystaniu i tym samym osiągnięciu zwycięstwa nad przeciwnikiem.

„Przestrzeń walki informacyjnej" 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 (rys.1.7.1).



Rys. 1.7.1. Podział przestrzeni walki informacyjnej

Na podstawie analizy literatury przedmiotu badań należy stwierdzić, że w historii miało miejsce wiele wojen i bitew, w których stosowane były elementy walki informacyjnej. W niniejszej pracy przedstawiono najbardziej charakterystyczne przykłady jej prowadzenia. Odzwierciedlają one jej rangę i znaczenie w skali światowej oraz pozwalają na dokonanie syntezy w tym obszarze wiedzy.

Historia walki informacyjnej jest tak samo długa, jak długa jest historia wojen. Walka informacyjna prowadzona już była od czasów najdawniejszych, jednak tylko w przestrzeni osobowej. Odkrycia naukowe w połowie XIX w. spowodowały, że zaczęła ona być realizowana również w przestrzeni technicznej. Formalnie zaczęto ją nazywać walką informacyjną po wojnie w rejonie Zatoki Perskiej.

„Informacja" zawsze była czynnikiem, który warunkował osiągnięcie powodzenia w prowadzonych działaniach zbrojnych. Zazwyczaj nie zdarzało się, aby sukces w walce zbrojnej uzyskała strona będąca przegraną w walce informacyjnej. Przez odpowiednie

stosowanie elementów walki informacyjnej, mniej liczebnie i słabiej wyposażone siły zbrojne odnosiły zwycięstwo nad liczebniejszym i lepiej wyposażonym przeciwnikiem.

Rola walki informacyjnej jest tym większa, im bardziej zaawansowane technologie są wykorzystywane na polu walki. Informacja na współczesnym polu walki jest tak ważna jak precyzyjnie wycelowana broń. Dane przekazywane w czasie niemal rzeczywistym stały się niezbędne do podjęcia trafnych decyzji i prowadzenia działań wojennych. Innymi słowy aktualna informacja umożliwia ocenę sytuacji wojskom własnym i pozwala uzyskać przewagę nad przeciwnikiem Przewaga ta zawsze była ważna, często decydowała o zwycięstwie na polu walki.

Przyszłe pole walki będzie cechować się dużą skutecznością rażenia, manewrowością, krótkim czasem reakcji. Dlatego też siły zbrojne XXI wieku będą mniej liczebne, a elementy walki informacyjnej będą stanowić o ich sile. Zastosowane w walce zbrojnej, mogą w znaczny sposób wprowadzić w błąd przeciwnika co do posiadanych sił i prowadzonych działań, co zwiększy zdolność bojową własnych wojsk i częściowo zrekompensuje braki w posiadanych systemach broni.

Pomimo wzrastającego zainteresowania prowadzeniem działań wojennych w przestrzeni informacyjnej, pomimo coraz liczniejszych publikacji nawiązujących do tej problematyki, wciąż nie jest ona dostatecznie dostrzegana, naświetlana i rozwijana w naszych siłach zbrojnych.

2. WALKA INFORMACYJNA WEDŁUG POGLĄDÓW AMERYKAŃSKICH

2.1. Geneza walki informacyjnej

W Stanach Zjednoczonych, w teorii współczesnej wojskowości, funkcjonują trzy terminy dotyczące walki informacyjnej, a mianowicie:

— walka z systemami dowodzenia i kontroli (C2W — Command and Control Warfare);

— walka informacyjna (Information Warfare — IW);

— działania informacyjne (Information Operations).

Pierwszy termin był używany już w latach 80 — tych, zaś drugi i trzeci — dopiero od 1991 r., po wojnie w rejonie Zatoki Perskiej.

W 1993 roku Winn Schwartau wydał opracowanie dotyczące walki informacyjnej („Information Warfare-Cyberterrorism: Protecting Your Personal Security in the Electronic Age"). Zgodnie z zasadami taksonomii wyróżnia on trzy rodzaje walki informacyjnej, które oparte są na poważnych studiach koncepcji prowadzenia walki informacyjnej-szczególnie w połączeniu z infrastrukturą ekonomiczną.

Klasa 1 — indywidualna walka informacyjna. Zawiera badania dotyczące wszystkich źródeł informacji o każdym z nas jako indywiduum.

Klasa 2 — zespołowa walka informacyjna. Zawiera studia o informacji jako przedmiocie dotyczącym towarzystw, spółek, korporacji w sferze interesów, handlu lub ekonomii.

Klasa 3 — globalna walka informacyjna, wszystkie aspekty dotyczące interesów narodowych.

Duży wpływ na teorię współczesnej wojskowości wywarła praca Heidi i Alvina Tofflerów: „War and Anti-War: Survival at the Dawn of the Twenty First Century", w której przedstawili, pochodzącą od ich nazwiska teorię fali. Obecnie są doradcami przewodniczącego Izby Reprezentantów Newta Gingricha. Na ich opinie powołuje się wielu wojskowych. Ich poglądy znalazły odzwierciedlenie, między innymi, w książce generała Gordona Sullivana (byłego szefa Sztabu Wojsk Lądowych) zatytułowanej „Przyszłość walki zbrojnej" (Envisioning Future Warfare).

Istota tofflerowskiej teorii fali polega na tym, że jej twórcy podzielili rozwój społeczeństwa i sposoby prowadzenia wojen na trzy „fale":

— „Falą pierwszą" określili okres funkcjonowania: w stosunku do społeczeństwa — gospodarki rolnej, natomiast w stosunku do wojen — uzbrojenia prymitywnego (muszkietów i pik).

— „Falą drugą" — erę przemysłową, kiedy to w wojnach stosowano czołgi i bombowce.

— „Falą trzecią" — współczesne społeczeństwo, tak zwanych wojowników wiedzy — intelektualistów w mundurach.

Minione wojny sięgają poprzez czas, wpływając na dzisiejsze życie. Podczas gdy wojny aktualne czy potencjalne, a także namiastki wojen, kształtują istnienie ludzi, pojawia się całkowicie zapomniana odwrotność tej sytuacji, bo przecież życie każdego człowieka kształtują również te wojny, których nie prowadzono, którym udało się zapobiec, ponieważ zwycięstwo odniosły antywojny. Jednakże wojna i antywojna nie są przeciwstawieniem typu „albo — albo". Antywojen nie prowadzi się za pomocą przemówień, modłów, demonstracji, marszów i pikiet nawołujących do pokoju. Antywojny obejmują przede wszystkim działania podejmowane przez polityków, a nawet przez żołnierzy, mające na celu stworzenie warunków, które odstraszałyby od wojny albo ograniczały jej zasięg. Zdarza się bowiem w tym skomplikowanym świecie, że wojna staje się niezbędnym narzędziem zapobiegającym większej, straszliwszej wojnie. Wojna bywa więc antywojną. W ostateczności antywojny wiążą się ze strategicznym wykorzystaniem siły militarnej i ekonomicznej, jak również potencjału informacyjnego, dla ograniczenia przemocy, tak często towarzyszącej zmianom na scenie świata. Gdy forma wojny właściwa trzeciej fali nabiera wyraźniejszych kształtów, zaczyna się wyłaniać nowy gatunek wojowników — „wojownicy wiedzy". Są nimi intelektualiści, zarówno umundurowani, jak i bez mundurów, głęboko przekonani o tym, że dzięki wiedzy wygrywa się wojny albo też wojnom się zapobiega. Jeśli przyjrzeć się temu, co czynią niektórzy, można dostrzec, jak krok po kroku zmierzają od początkowo wąskich, technicznych zainteresowań ku uogólniającej koncepcji, która pewnego dnia zyska sobie nazwę „strategii opartej na wiedzy". W miarę jak rośnie zrozumienie tych faktów, we wszystkich częściach świata rodzi się przekonanie, że porządek gospodarczy oparty na pracy umysłu, taki, jaki istnieje w Stanach Zjednoczonych, w Japonii i w Europie, pociągnie za sobą porządek militarny oparty na pracy umysłu. Może nadejść taki dzień, że więcej żołnierzy będzie posługiwało się komputerem niż karabinem. Ujmując rzecz pokrótce, wiedza jest teraz głównym środkiem niszczenia, tak samo jak głównym środkiem tworzenia[70].

---

[70] Alvin i Heidi Toffler: *„Wojna i antywojna"* (War and Antiwar), 1993, s.207.

Zdobywanie danych jest jednym z najważniejszych elementów walki informacyjnej. Dane można zdobywać za sprawą rozpoznania osobowego (wywiadu) i technicznego, badań i ich rozwoju, mediów, a także innych źródeł. Należy określić, które z nich są najważniejsze, aby można było je doskonalić już w czasie pokoju.

W 1993 roku Kolegium Połączonych Szefów Sztabów wydało „Memorandum of Policy" (MOP) No 30 (Command and Control Warfare). Określono w nim:

— sposób prowadzenia walki (atak na obiekty dowodzenia i kontroli — C2 oraz ochronę tych samych obiektów);

— wprowadzanie wroga w błąd, działania psychologiczne, walkę elektroniczną, niszczenie fizyczne.

Powyższe przedsięwzięcia są wspierane przez wywiad, po to aby nie dopuścić do przepływu informacji, uzyskać wpływ na C2 przeciwnika, osłabić je, zniszczyć, ochraniając przy tym C2 własnych wojsk. Właściwe działanie takiego systemu daje dowódcy możliwość zadania „nokautującego ciosu" jeszcze przed wybuchem tradycyjnej wojny.

Departament Obrony USA (Department of Defense — DOD) wydał ściśle tajną dyrektywę 3600.1, dotyczącą walki informacyjnej.

W listopadzie 1993 r. Komendant Uniwersytetu Obrony Narodowej (National Defense University) wysłał pismo do Szefa Kolegium Połączonych Sztabów w sprawie powołania Szkoły Strategii i Walki Informacyjnej (School of Information Warfare and Strategy), w której cykl szkolenia trwałby 44 tygodnie. W listopadzie 1994 roku szkoła przyjęła pierwszych 16 oficerów.

W sierpniu 1996 r. Dowództwo Szkolenia i Doktryn (TRADOC — Trainining and Doctrine Command) opublikowało „Regulamin walki SL USA" (FM—100—6) zawierający doktrynę[71] (koncepcję) działań informacyjnych.

2.2. Definicja walki informacyjnej

Według Amerykanów jest niemożliwe prowadzenie dyskusji nt. walki informacyjnej bez ścisłego zdefiniowania znaczenia samej „informacji". Ma ona związek ze zjawiskami,

[71] Doktryna - podstawowe zasady, którymi kierują się SZ lub ich elementy w trakcie działalności zmierzającej do osiągnięcia celów państwowych. W literaturze zachodniej termin doktryna używany jest najczęściej w odniesieniu do zasad działania wyspecjalizowanych struktur wojskowych (doktryna SL, SP, wojsk specjalnego przeznaczenia, itd.), które są zbiorami ustaleń normatywnych zawierającymi szczegółowe instrukcje określające sposób prowadzenia działań bojowych. Doktrynę można porównać do koncepcji działań. Wojska prowadzą działania w sposób określony przez doktrynę, opracowane z uwzględnieniem ustaleń obowiązującej koncepcji strategicznej oraz możliwości bojowej wojsk.

zdarzeniami lub faktami, które istnieją wszędzie w otoczeniu człowieka. Zjawiska muszą być zauważone i wyjaśnione aby stały się „informacją", która jest rezultatem dwóch rzeczy:
- spostrzeżonych zjawisk (dane, komunikaty, wiadomości);
- instrukcji wymaganych do zinterpretowania tych danych aby wyjaśnić ich znaczenie.

Na przykład jeżeli drzewo zostaje złamane przez wiatr, ale nie ma osoby, która mogłaby to spostrzec lub usłyszeć, wtedy nie można mówić o zjawisku informacji. Upadające drzewo powoduje powstawanie fal w atmosferze, czyli pewne zjawisko fizyczne. „Informacja" oznaczająca upadające drzewo ma miejsce, jeżeli człowiek usłyszy hałas, a mózg człowieka po dokonaniu analizy, rozpozna ten odgłos jako upadające drzewo. W związku z tym kontekstem, nie ma żadnego upadającego drzewa jeśli człowiek tego nie usłyszy (lub zauważy). Zjawisko (zdarzenie) może stać się „informacją" dopiero po przeprowadzonej obserwacji i analizie. Dlatego też, „informacja" jest zjawiskiem abstrakcyjnym. „Informacja" jest rezultatem percepcyjnych i indywidualnych możliwości człowieka, które mogą być zwielokrotnione przez technologię. Technologia w sposób decydujący zwiększa nasze możliwości obserwacyjne człowieka, poszerza możliwości zbierania i gromadzenia, kodowania i rozkodowania danych.

Pojęcie „walki informacyjnej" jest różnie interpretowane nawet w samych środowiskach wojskowych USA.

Były płk sił powietrznych USA Alan D. Campen podaje, że walka informacyjna to akcje manipulacyjne lub destrukcyjne, prowadzone z ukrycia lub jawnie, w czasie pokoju, kryzysu lub wojny i skierowane na przemysłowe lub militarne elektroniczne systemy informacyjne w aspekcie społecznym, politycznym, ekonomicznym itp.

Według zastępcy sekretarza obrony ds. działań C2W, walka informacyjna to akcje prowadzone w celu ochrony integralności własnych systemów informacyjnych przed eksploatacją, uszkodzeniem lub destrukcją (zniszczeniem) i jednocześnie w celu eksploatacji, uszkodzenia lub destrukcji (zniszczenia) systemów informacyjnych przeciwnika.

Siły Powietrzne USA definiują walkę informacyjną jako jakiekolwiek działania mające na celu: zdobycie i wykorzystanie informacji; pozbawienie tych możliwości przeciwnika lub zniszczenie jego informacji; ochronę własnych sił przed działaniem przeciwnika.

Departament Obrony Stanów Zjednoczonych określił walkę informacyjną jako akcje podjęte w celu uzyskania przewagi informacyjnej przez wpływanie na informacje, procesy informacyjne, systemy informacyjne i sieci komputerowe przeciwnika, przy jednoczesnej ochronie własnej informacji, procesów informacyjnych, systemów informacyjnych i komputerowych.

Powyższe definicje nie wyjaśniają w sposób jednoznaczny i wyraźny pojęcia „walka informacyjna". Powołując się na opinię ekspertów A. i H. Tofflerów, należy stwierdzić, że takie terminy jak: infodoktryna, cyberwojna, system C2 oraz tym podobne, odzwierciedlają wciąż jeszcze wstępne stadium dyskusji w obszarze walki informacyjnej.

Zdaniem Amerykanów, walka informacyjna będzie prowadzona w globalnym środowisku informacyjnym, ponieważ obecne technologie elektroniczne pozwolą ujawnić wszelkie operacje wojskowe na całym świecie.

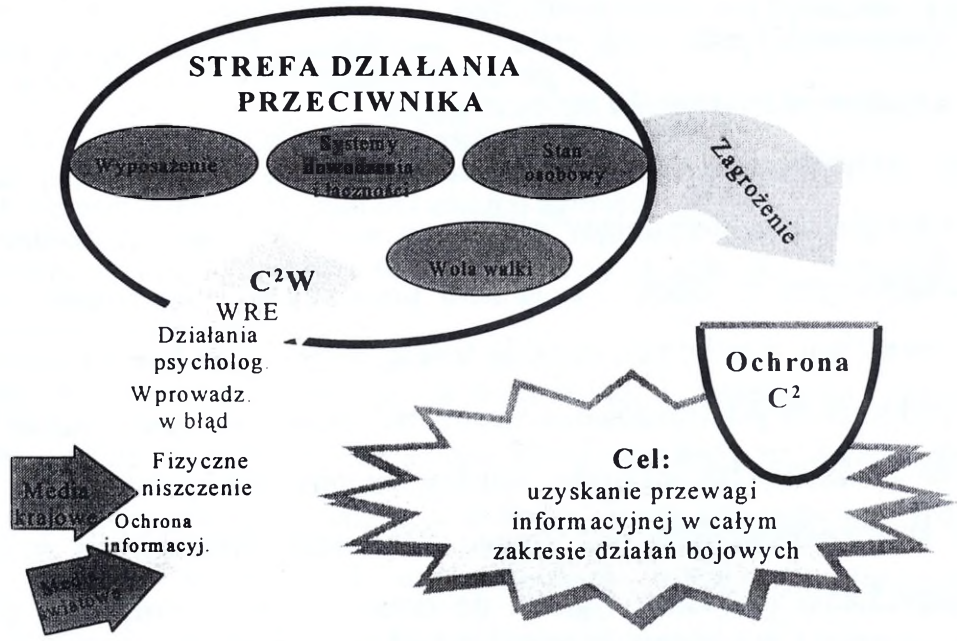
2.3. Zakres walki informacyjnej

Walka informacyjna obejmuje trzy fundamentalne komponenty:

— zdobywanie informacji z rozpoznania i wywiadu;

— wykorzystanie systemów informacyjnych;

— kombinację działań: C2W (Command and Control Warfare), CA (civil affairs) i PA (public affairs) w celu uzyskania przewagi informacyjnej (rys. 2.1).



Rys. 2.1.Elementy walki informacyjnej[72]

Zdobywanie informacji z rozpoznania i wywiadu. (RII). Chodzi tu o zdobycie jak największej liczby wiadomości o:

— własnych siłach zbrojnych (ich dyslokacji, skuteczności prowadzenia walki oraz aktualnej działalności);

— siłach zbrojnych przeciwnika (ich dyslokacji, możliwościach bojowych, skuteczności walki, zamiarach), które mogłyby być przydatne dla odniesienia sukcesu w walce.

---

[72] Opracowano na podstawie *„Military Review"* 2/1997.

„Informacja" jest niezbędna dla dowództwa w celu podjęcia decyzji (bez niej nie może nastąpić planowanie działań).

„Informacja" ma bezpośredni związek z wojskowym środowiskiem informacyjnym ze względu na dwa ważne aspekty:

— zdobywanie, analizowanie, wykorzystanie i przekazywanie danych jest realizowane przez dowództwa, jednostki wojskowe, organizacje lub systemy wchodzące w skład wojskowego środowiska informacyjnego (MIE);
— jest ona wykorzystywana przez tych samych zawodowców (dowództwa), którzy planują działania informacyjne.

Zdobywanie, analizowanie, wykorzystanie i przekazywanie danych jest podstawą uzyskania oceny sytuacji przez siły zbrojne, które mogą dzięki temu zjednoczyć wszystkie wysiłki w celu wykonania zadania bojowego. Działalność informacyjna realizowana w ramach wojskowego środowiska informacyjnego musi być dostosowana do globalnego środowiska informacyjnego. Dowódcy wykorzystują informacje z rozpoznania i wywiadu (RII) oraz przesyłane przez media. Kluczem do osiągnięcia sukcesu jest informacyjne przygotowanie (preparacja) pola walki (IPB — Intelligence Preparation of the Battlefield), realizowana w wojskowym środowisku informacyjnym.

Zdolność pozyskiwania danych o przeciwniku, ich analizowanie, przekazywanie i wykorzystanie będzie mieć decydujący wpływ na wynik przyszłych działań. Jak wynika z danych przedstawionych w tabeli 2.1, sposób prowadzenia rozpoznania uległ zmianie, począwszy od obserwacji wzrokowej, poprzez lunetę, telegraf, do bardzo skomplikowanych urządzeń mikroelektronicznych (urządzenia satelitarne, samoloty rozpoznawcze, bezzałogowe statki powietrzne ze skanerami, czujniki, między innymi: optoelektroniczne, wykrywania zapachów itp.) wykorzystywanych pod koniec XX wieku. Szczególnie zmienił się czas prowadzenia rozpoznania (od kilku tygodni do czasu realnego) oraz czas podejmowania decyzji (od kilku miesięcy do godziny). Czas uzyskania informacji w przyszłej wojnie będzie decydował o przebiegu działań wojennych. Informatyka umożliwi wojskom walczącym zobrazowanie sytuacji z pola walki w czasie niemal rzeczywistym i pozwoli na szybkie podjęcie trafnych decyzji. W ciągu kilku lat możliwe będzie zbudowanie małego satelitarnego systemu rozpoznawczego o wykrywalności obiektów ruchomych wielkości 2,5 metra. Jeśli zostanie on połączony z czujnikiem na podczerwień, będzie mógł wykryć nawet obiekty zamaskowane i przekazać informację w czasie rzeczywistym[73].

[73]Magazyn *„Signal"*, 4/1992.

Tabela 2.1.

Prowadzenie rozpoznania a podejmowanie decyzji[74]

Rodzaj wojny ---------- **Wyszczególnienie**	**Wojna o niepodległość /1776-1783/**	**Wojna secesyjna /1861-1865/**	**II wojna światowa**	**Wojna w Zatoce Perskiej**
Środek prowadz. rozpoznania	Luneta /teleskop/	Telegraf	Odbiornik radiowy	Urządzenia mikroelektron.
Czas prowadzenia rozpoznania	Kilka tygodni	Kilka dni	Kilka /kilkanaście g./	Czas realny /kilka minut/
Czas podejmow. decyzji	Kilka miesięcy	Kilka tygodni	Kilka dni	Godzina /do kilku godz./

Wykorzystanie systemów informacyjnych (IS — Information Systems) daje dowódcom i sztabom możliwość kontrolowania aktualnej sytuacji na polu walki, synchronizacji działań oraz integracji z systemami walki (BOSs — Battlefield Operation Systems). Zapewniają one:

— koordynację działań z SP 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 informacje dla sił prowadzących obecne i przyszłe działania. Pomimo dużych możliwości w zakresie automatyzacji transmisji danych, ludzie w dalszym ciągu stanowią najbardziej efektywny element przy ocenie ważnych i wartościowych informacji. Integracja systemów informacyjnych odbywa się na płaszczyźnie zarówno pionowej, jak i poziomej.

W architekturze pola walki zarówno systemy wojskowe, jak i cywilne odgrywają ważną rolę.

Działania C2W obejmują:

— wprowadzanie w błąd przeciwnika (Deception);

— walkę elektroniczną (Electronic Warfare);

— działania psychologiczne (PSYOP);

---

[74] Opracowano na podstawie *„Military Review"* 4/1994.

— fizyczne niszczenie systemów informacyjnych przeciwnika (Physical Destruction);

— ochronę własnych systemów i działań (Operations Security);

Wprowadzanie w błąd — stanowi element sprytu wojennego, który stwarza u przeciwnika fałszywe wrażenie co do rzeczywistego położenia sił i ich stanu, zamiaru działania, kierunkach i charakterze przyszłej operacji oraz „kieruje" przeciwnikiem w stronę nieprzewidzianych i niewygodnych dla niego sposobów walki.

Zapewnienie bezpieczeństwa własnym systemom i operacjom — polega na zmniejszeniu efektywności działań strony przeciwnej. Do różnorodnych sposobów ochrony własnych systemów informacyjnych dołączone zostają przedsięwzięcia przeciwdziałania środkami rozpoznania, maskowania, zapewniające skrytość zamiaru działań, obezwładnienia radioelektronicznego, ogniowego oddziaływania i in.

Działania (operacje) psychologiczne w walce informacyjnej polegają na:

— dyskredytowaniu kierownictwa państwowego w oczach społeczeństwa i wśród wojsk;

— demonstracji siły;

— namawianiu do nieposłuszeństwa i oddania się w niewolę.

Walka elektroniczna (electronic warfare) obejmuje:

— rozpoznanie elektroniczne (ES — Electronic Support);

— przeciwdziałanie (CM — Countermeasures);

— kontrprzeciwdziałanie (CCM — Counter-Countermeasures).

Ponadto w trakcie prowadzenia walki informacyjnej może być stosowany atak elektroniczny (EA — Electronic Attack) i obrona elektroniczna (EP — Electronic Protection).

Media rządowe (CA — Civil Affairs) spełniają integralną rolę w działaniach 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 o zasięgu światowym (PA — Public Affairs) odgrywają dużą rolę w kształtowaniu opinii publicznej. Krytykują one cele operacji militarnych, 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 widzów.

Działalność mediów Amerykanie zaczęli doceniać dopiero od wojny w rejonie Zatoki Perskiej. Nowoczesna technologia przekazu informacji spowodowała, że media odegrały

jedną z ważniejszych ról. Spełniły one rolę wsparcia moralnego dla celowości prowadzonych działań.

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 walce informacyjnej. 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.

2.4. Wnioski

Uwieńczeniem koncepcji działań informacyjnych, wg poglądów amerykańskich, będzie stworzenie globalnego informacyjnego systemu sił zbrojnych USA, mogącego ciągle kontrolować stan i działania sił zbrojnych innych państw oraz zapewniającego bezsprzeczną przewagę nad rozczłonkowanymi regionalnymi systemami dowodzenia i łączności prawdopodobnych przeciwników. Zwiększenie możliwości tego systemu będzie realizowane dzięki stworzeniu nowego rodzaju broni elektronicznych (zaliczanych do tzw. nieśmiercionośnego uzbrojenia), mogącego zarówno odstraszać przeciwnika, jak i zapewnić realizację ataku elektronicznego.

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.

Technologia informacyjna oferuje „śmierć chirurgiczną" niedostępną w przeszłości. O roli, jaką może odegrać walka informacyjna, niech świadczą następujące przykłady: w 1881 r. Brytyjczycy ostrzelali Egipskie forty w pobliżu Aleksandrii używając 3000 pocisków, z których tylko 10 trafiło do celu; w czasie wojny w rejonie Zatoki Perskiej samolot F—117 SP USA spowodował takie szkody jak samoloty bombowe USA w ciągu II wojny światowej wykonujące 4500 lotów i zrzucające 9000 bomb.

Po wojnie w rejonie Zatoki Perskiej wiele krajów zaczęło przywiązywać dużą uwagę do obszaru walki informacyjnej. W problematyce tej przodują Stany Zjednoczone, które mają

szeroko zakrojone plany zrewolucjonizowania obszaru działań zbrojnych za pomocą techniki informacyjnej, tak jak zrewolucjonizowały go czołgi podczas pierwszej i bomba atomowa podczas drugiej wojny światowej.

Nowe środki walki i przewidywania co do ich rozwoju powodują zmiany w poglądach i sposobach prowadzenia działań wojennych. Same prototypy, lub tylko naukowo-techniczne pomysły przyszłej broni, są zaczynem nowych koncepcji i założeń taktycznych i operacyjnych, a nawet strategicznych. Można powiedzieć, że wiedza wojskowa jest produktem myślenia prognostycznego, rezultatem refleksji o przyszłym polu walki.

3. NIEMIECKIE POGLĄDY NA PROWADZENIE WALKI INFORMACYJNEJ

„Informacja stała się czynnikiem kluczowym w prowadzeniu współczesnych działań wojennych"[75].

Zdolność zdobywania, przetwarzania i wykorzystania danych o przeciwniku we własnych siłach zbrojnych oraz przeszkadzanie przeciwnikowi w tym samym zakresie będzie miało decydujący wpływ na wynik przyszłych działań wojennych.

Według niemieckich teoretyków, jak i praktyków „informacja"jest dzisiaj i będzie w przyszłości tym, czym był karabin maszynowy w pierwszej i czołg w drugiej wojnie światowej. Tym novum jest technologia informatyczna. Nowy wymiar także uzyskują relacje między nakładem sił a osiągniętymi efektami.

Na dzisiejsze systemy uzbrojenia przeciwnika można oddziaływać w stopniu ograniczonym, natomiast „wirus komputerowy" może sparaliżować sieć informacyjną o zasięgu światowym. Niezbędne oprogramowanie w tym zakresie osiągalne jest na wolnym rynku, co oznacza, że środki te dostępne są nie tylko wyłącznym użytkownikom lecz także potencjalnemu przeciwnikowi, terrorystom i kryminalistom.

3.1. Definicja walki informacyjnej

W dużej ilości istniejących określeń dotyczących tego terminu znajdują się również takie, które raczej przyczyniają się do większego zamieszania niż do jasności. Według poglądów niemieckich „walka informacyjna" („Information Warfare"[76]) rozumiana jest jako wszystkie przedsięwzięcia, które służą zapewnieniu przewagi własnym siłom zbrojnym w zakresie danych dotyczących potencjalnego przeciwnika. Innymi słowy jest to zespół przedsięwzięć związanych z pozyskaniem, obróbką i rozpowszechnianiem danych służących do wsparcia własnych operacji wojskowych.

3.2. Geneza walki informacyjnej

Prowadzenie walki informacyjnej (szczególnie manipulowanie wiadomościami) miało duże znaczenie w czasie „zimnej wojny". W wielu konfliktach o małej intensywności

---

[75] *Peterson K., Pracht U.:Information warfare w: „Soldat und Technik", 12/95.*

[76] Niemieckie poglądy na walkę informacyjną opierają się głównie na doświadczeniach amerykańskich, dlatego też nie używają swojego nazewnictwa, tylko przyjmują amerykańskie terminy w języku angielskim, takie jak: „Information Warfare", "C2W" itp.

(najczęściej były to „zastępcze" wojny między supermocarstwami) wysiłki ówczesnej strony radzieckiej były nakierowane na osiągnięcie następujących trzech celów:

— inwigilacja zachodnich grup religijnych i ruchów pokojowych;

— inwigilacja zachodnich rządów, systemów społecznych i mediów;

— inwigilacja prądów neutralnych i, jeśli to możliwe, tworzenie powiązań z własnymi organizacjami.

Jednocześnie w myśl własnych interesów w każdym podbitym kraju oddziaływano na opinię publiczną, rząd i ludność poprzez:

— rozpowszechnianie fałszywych, zniekształconych lub niepełnych danych (tzw. propaganda);

— organizowanie sterowanych, masowych manifestacji i przekazywanie wiadomości, które w sposób zamierzony wprowadzały w błąd i przedstawiały rzeczywistość w krzywym zwierciadle.

Na Zachodzie również szybko zauważono jak ważne było sterowanie i manipulowanie wiadomościami. Osiągano to stosując ofensywne i defensywne środki. W wypadku stosowania tych pierwszych polegało to na:

— utrzymaniu przychylnego nastawienia opinii publicznej;

— uściśleniu własnych interesów i wymogów co do realizacji celu;

— nagłośnieniu niepublikowanych powszechnie lub istniejących w ukryciu poglądów;

— dokonywaniu szczegółowych sprawozdań z każdego konfliktu.

Przy wykorzystaniu drugiej grupy środków polegało to na:

— prowadzeniu działań przeciwdezinformacyjnych;

— zmienianiu lub neutralizacji poglądów wroga.

Obok powyższych przedsięwzięć, nowego znaczenia nabiera rozpowszechnianie nieprawdziwych danych i skracanie lub przekształcanie już istniejących komunikatów. Zastosowanie nowoczesnych sieci komputerowych stwarza tutaj optymalne przesłanki przy minimalnych nakładach finansowych i osobowych. Otwierające się przy tym możliwości wychodzą daleko poza dotychczas znane spektrum walki elektronicznej. Niezauważalne przez przeciwnika zmiany w treściach danych mogą wyrządzić dużo więcej szkód niż jeden fizycznie zniszczony węzeł łączności. Dane operacyjne (pisemne operacyjne rozkazy, położenie wojsk) będą jak zwykle wysyłane i odbierane, jednak podczas transmisji mogą być one przez przeciwnika zniekształcane.

Elementy walki informacyjnej mają zastosowanie we wszystkich możliwych scenariuszach wojennych w zakresie dowodzenia, wsparcia i planowania walki. Poznanie zamiarów i możliwości przeciwnika, dokładnej dyslokacji jego sił oraz przypuszczalnych obiektów ataku, a także dyslokacji własnych sił jest nieodzowne do skutecznego prowadzenia walki. Najistotniejsze więc w tym zakresie staje się:

— pozyskiwanie danych o przeciwniku;

— analiza danych;

— niezwłoczne ich przekazanie do zainteresowanych odbiorców;

— niezawodność (prawdziwość) danych.

Do pozyskiwania i przekazywania danych w siłach zbrojnych są wykorzystywane różne systemy, takie jak:

— radiolokacyjny, zintegrowany system rozpoznawczo – uderzeniowy – JSTARS[77];

— zintegrowany system kierowania lotnictwem taktycznym – JTAGS[78];

— powietrzny system wczesnego wykrywania i ostrzegania – AWACS[79];

— rozpoznawczy, elektroniczny system meldunkowy – Fm Elo Aufkl Systeme[80];

— zintegrowany system dystrybucji danych - JTIDS[81].

Duży problem stanowi analiza i opracowywanie zebranych danych. Muszą one być zebrane i posegregowane na ważne i potrzebne oraz na nieważne. W idealnym przypadku należałoby do zainteresowanych odbiorców przekazywać tylko te dane, które oni w konkretnym czasie i miejscu potrzebują. Dlatego tak ważne w tym zakresie staje się stworzenie systemu informacyjnego, który umożliwiłby optymalną współpracę pomiędzy różnymi rodzajami sił zbrojnych lub strukturami wielonarodowymi.

Reasumując, zarówno podczas przygotowania, jak i prowadzenia operacji wyniki zdobytych danych przyczyniają się do optymalizacji użycia sił oraz do wzrostu efektywności zastosowanych systemów broni.

W przyszłości technika komputerowa będzie odgrywać jeszcze większą rolę w projektowanych systemach uzbrojenia i broni. Już dzisiaj koszt urządzeń elektronicznych wynosi 50% łącznych kosztów uzbrojenia. Wymagania dotyczące samych mechanizmów broni będą bardziej odchodziły na plan dalszy. Główny nacisk będzie położony na rozwój

---

[77] JSTARS - Joint Surveillance and Target Acquisition Radar System.
[78] JTAGS - Joint Tactical Air to Ground System.
[79] AWACS - Airborne Warning and Control System.
[80] Fm Elo Aufkl Systeme - Fernmelde Electronische Aufklärung Systeme.
[81] JTIDS - Joint Tactical Information Distribution System.

technologii informacyjnych i oprzyrządowania, na polepszenie sprawności dowodzenia, kontroli, wprowadzanie systemów komputerowych oraz zwiększenie precyzji rażenia broni.

W dalszym ciągu pracuje się nad systemem, który zastąpi istniejący obecnie, bazujący na przestarzałej technologii system powietrzno - kosmicznej koordynacji. Celem tych zabiegów jest dostarczanie we właściwym czasie niezbędnych danych, w całej złożoności ich dynamiki do systemów uzbrojenia.

Prowadzone są również prace nad udoskonaleniem procesów decyzyjnych podczas prowadzenia operacji powietrzno - lądowych - przez integrację sygnałów o zagrożeniach, sygnałów z czujników o położeniu samolotu w przestrzeni, systemów przechwytywania celów, systemów broni i kierowania ogniem, jak również systemów nawigacji i łączności. Straty powinny zmniejszyć się o 30 - 60%, prawdopodobieństwo zniszczenia celu powinno się znacznie poprawić, a skrócenie planowania misji powinno wynosić od 20 do 30%.

Żołnierz XXI wieku dzięki osiągnięciom mikroelektroniki będzie dysponował kompletnymi danymi o swoim położeniu na polu walki, które będą wyświetlane za pomocą wizjera zamontowanego na hełmie (rys. 3.2.1).

Rys. 3.2.1. Uzbrojenie żołnierza XXI wieku[82]

Legenda do rysunku:

1) zintegrowane urządzenie elektroniczne w hełmie, zbierające i uaktualniające dane.

[82] Opracowano na podstawie poglądów amerykańskich i niemieckich.

2) osłona ciała, mieszcząca w swej dolnej części komputer, chroniąca żołnierza przed napromieniowaniem i środkami chemicznymi.
3) komputer sterujący wyposażeniem technicznym żołnierza, umożliwiający identyfikację „swój – obcy", wykrywający miny, chemikalia i podający aktualną pozycję.
4) lekki hełm skuteczniej chroniący przed pociskami i odłamkami. Zamontowany na nim ekranik zawiera czujniki do widzenia w nocy, miniaturową tabliczkę do sterowania obrazem wideo i głosowym sterowaniem komputerem.
5) celownik na podczerwień (umieszczony na broni) przesyłający obraz z pola walki do dowództwa, umożliwiający ocenę zniszczeń.
6) bezprzewodowe połączenie łączące broń z monitorem na hełmie, pozwalające żołnierzowi celować bez wystawiania swego ciała na ostrzał przeciwnika.

Coraz większe nasycenie własnych systemów uzbrojenia tą techniką sprawia, że one bardziej podatne na ataki przeciwnika. Należy więc wziąć pod uwagę to, że wszelkie planowane działania, które oparte są na elektronicznie przekazywanych danych, mogą mieć miejsce tylko wtedy, kiedy będzie zagwarantowany będzie wysoki stopień ich zabezpieczenia przed możliwością manipulacji.

3.3. Systemy informacyjne przeciwnika

Zależność wysoko uprzemysłowionych społeczeństw od sieci komputerowych wykorzystywanych praktycznie we wszystkich płaszczyznach życia publicznego, w energetyce, w transporcie, na polu gospodarki i finansów, jak również w komunikacji daje potencjalnym przeciwnikom, ale także terrorystom i kryminalistom liczne możliwości ingerencji.

Na pewno w przyszłych konfliktach należy liczyć się z tym, że strona rozpoczynająca je będzie paraliżować siły i środki strony przeciwnej. Oznacza to, po pierwsze - konieczność ochrony własnych systemów przed tego rodzaju ingerencją, a po drugie - możliwość zastosowania podobnych środków, aby chronić życie ludności i oszczędzić wartościowe zasoby i środki własne.

Sieci zaopatrywania w energię są w nowoczesnych społeczeństwach głównym czynnikiem umożliwiającym wszelkiego rodzaju działalność produkcyjną, usługową i inną. Stanowiły one już wcześniej cele ataków w wojnach konwencjonalnych. Osiągnięcia techniczne ostatnich lat dają całkiem nowe możliwości ingerencji w tym zakresie bez

powodowania ogromnych zniszczeń. Na przykład siły powietrzne USA (USAF)[83] w czasie wojny w rejonie Zatoki Perskiej sparaliżowały na krótki czas sieci zasilania w energię elektryczną poprzez zrzucanie pasków folii włókna węglowego na stacje transformatorowe.

Ponieważ w systemach zasilania w energię wykorzystywane są urządzenia sterowania i regulacji (oparte na komputerach), mogą być tutaj dokonywane manipulacje, np. przez wprowadzenie wirusów komputerowych lub zmian w programie, co dawałoby gwarancję swobodnego działania siłom własnym i potem ponowne osiągnięcie istniejących wcześniej możliwości bez wymaganego dużego nakładu sił i środków na ich odbudowę.

W nowoczesnych społeczeństwach podział pracy i zdecentralizowana produkcja zależą od dobrze funkcjonującego, kompleksowego systemu transportu kołowego, kolejowego, wodnego i powietrznego. Jego bezkolizyjne funkcjonowanie może zapewnić wykorzystanie techniki informatycznej. Obok przypadkowych błędów technicznych należy liczyć się również z ograniczeniami spowodowanymi sabotażami. Może dojść do unieruchomienia transportu lub celowo wywołanych ogromnych kolizji, na przykład w sieciach kolejowych czy lotniczych.

Zamieszanie i panikę może wywołać także paraliż ważnych obszarów gospodarki lub finansów, np. przez zmianę lub fałszowanie danych w systemach bankowych.

Sieci telekomunikacyjne są istotnym czynnikiem szybkiego przekazywania ważnych danych. Wysokim wymaganiom szybkiej transmisji licznych danych mogą sprostać tylko środki o najnowocześniejszej technologii. W komunikacji o zasięgu światowym są głównie wykorzystane łącza satelitarne. Systemy te są również narażone na ingerencję sił wroga wskutek możliwości wprowadzania wirusów komputerowych czy najprzeróżniejszych zmian lub zniekształceń sygnałów radiowych. Mogłoby to spowodować izolację sił kierowania państwem, przerwanie połączeń zagranicznych lub celowe wyłączenie poszczególnych regionów w ramach państwa.

3.4. Cele militarne

Ponieważ skuteczne dowodzenie wojskami możliwe jest tylko wtedy, gdy do zainteresowanych odbiorców dotrą we właściwym czasie aktualne i wyczerpujące dane z rozpoznania dotyczące przeciwnika, to kluczem do osiągnięcia tego celu w dzisiejszych i przyszłych konfliktach JEST system C4I2[84]. Toteż jednym z najważniejszych celów operacji

[83] USAF – United States Air Force
[84] C4I2 - Command, Control, Communication, Computers, Intelligence and Information System.

militarnych było od dawna obezwładnianie wszystkich urządzeń elektronicznych służących do pozyskiwania i transmisji danych.

Rodzaje celów zmieniły się tylko na tyle, że obecnie należy uwzględnić w tej walce instalacje w kosmosie. Nowe są jednakże możliwości techniczne, po które można sięgnąć. Możliwa jest dzisiaj taka manipulacja danymi (podczas ich odbioru lub przekazywania), w wyniku której przeciwnik otrzymuje niepełny lub fałszywy obraz sytuacji. Zostaną mu przekazane nieużyteczne dane, które będą go wprowadzać w błąd lub osłaniać własne operacje. W ten sposób „głuchy" i „ślepy" przeciwnik będzie szybko zmuszony do zaniechania swoich zamiarów.

W coraz większym stopniu nowoczesne technologie wykorzystuje się podczas przekazywania danych w systemach dowodzenia wojskami. Są one zdolne do pracy na dużych odległościach, ze względu na stosowanie łączy satelitarnych. Przy zwalczaniu i niszczeniu nowoczesnych, na wysokim poziomie technologicznym, systemów uzbrojenia przeciwnika, będzie się w przyszłości zwracać mniejszą uwagę na ich konwencjonalne, fizyczne niszczenie, natomiast większą - na obezwładnienie systemów oprogramowania i układów silnie zminiaturyzowanych. Konstruktorzy uzbrojenia proponują, aby podczas produkcji systemów broni instalować odpowiednie układy, które w określonych sytuacjach, np. przy eksporcie do innych krajów, zmniejszałyby ich skuteczność, np. udaremniały start rakiety, zmieniały jej kurs podczas lotu lub blokowały detonator głowicy bojowej po jej starcie. W ten sposób pociski rakietowe nigdy nie trafiłyby do celu, ponieważ urządzenia nawigacyjne, komputery pokładowe (wypracowujące tor lotu), czujniki wszelkiego typu byłyby niezdolne do właściwego funkcjonowania.

3.5. Symulacja, gry wojenne

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, przy użyciu sztucznej inteligencji i systemów eksperckich, sprawdzenia czy w konkretnym starciu zbrojnym można osiągnąć powodzenie. Z ostatnich obliczeń prowadzonych przez Amerykanów, na podstawie pewnej „symulowanej" wojny na lądzie wynika, że jedna dywizja

w sile 20 000 ludzi, wyposażona w nowoczesne środki techniki informacyjnej, różnego rodzaju czujniki i tzw. inteligentną broń, pokonać może bez trudu trzykrotnie silniejszego przeciwnika, który nie dysponuje takimi środkami.

Naukowcy z Uniwersytetu John Hopkins 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 dopasowania we właściwym czasie swojego taktyczno - operacyjnego planowania do aktualnego położenia. Firmy amerykańskie są obecnie na etapie tworzenia specjalnego wyposażenia piechoty, które będzie (poprzez zamontowany na hełmie układ) przekazywać żołnierzowi w sposób nieprzerwany obraz sytuacji pola walki, niezależnie od warunków atmosferycznych i widoczności,. Tak więc zastosowanie kompletnego trenażera, za pomocą którego żołnierz w zabezpieczonym bunkrze będzie mógł walczyć z „wirtualnym" przeciwnikiem, wydaje się już bardzo bliskie. Jak niedawno opisali pracownicy grupy „RAND"[85], istnieje wiele międzynarodowych sieci telekomunikacyjnych, które w istotny sposób przyczyniają się do ogromnych ułatwień w dziedzinie wymiany danych i doświadczeń, szczególnie w obszarze badań naukowych. Jedną z najbardziej znanych sieci jest Internet, który wywodzi się z lat sześćdziesiątych - z Pentagonu. Został on później przekazany do użytku cywilnego. Przeciętny obywatel o średnim poziomie wykształcenia może wykorzystać taką sieć w dowolny sposób do najprzeróżniejszych własnych interesów.

Jak szybka w działaniu może być sieć komputerowa, udowodnił test pewnego Amerykanina, który w połowie lat sześćdziesiątych wprowadził do Internetu „wirus" w postaci słynnej „choinki", który w ciągu 6 godzin rozprzestrzenił się na tysiące węzłów tej sieci w całym świecie i wrócił później ponownie do nadawcy. Dzięki wykorzystaniu sieci telekomunikacyjnych możliwe jest „przekraczanie" granic państw oraz dezorganizowanie struktur społecznych. Komputery umożliwiają tworzenie się grup interesów niezależnie od położenia geograficznego, przynależności narodowej i dają potencjalnemu przestępcy do ręki broń o nieograniczonym zasięgu.

Społeczeństwo, które nie ma świadomości tego zagrożenia i nie czyni przygotowań do obrony przed nim, może zostać całkowicie zdezorganizowane za pomocą technologii informacyjnych, podobnie, jak na początku XX. wieku przez wojnę błyskawiczną (Blitzkrieg).

---

[85] RAND Group – grupa zajmująca się badaniem problematyki walki informacyjnej. Nazwa RAND została przyjęta od grup rozpoznawczych Mongołów z czasów Czyngis – chana.

Tabela 3.5.1

Formy walki informacyjnej i obiekty ataku[86]

FORMY	OBIEKTY ATAKU
Impuls elektromagnetyczny (EMP – Electromagnetic Pulse). Przenośne urządzenie wytwarzające impuls elektromagnetyczny rozmieszcza się w pobliżu urządzeń elektronicznych.	Systemy kierowania bronią, dowodzenia, sieci łączności, centra administracyjne i rządowe.
"Wirusy" komputerowe wprowadzane przez przeciwnika do sieci komputerowych.	Sieci komputerowe, telefoniczne i dalekopisowe, systemy transportu.
Dezinformujące wiadomości wysyłane z satelitów lub samolotów.	Wojskowe systemy dowodzenia, rozgłośnie radiowe i telewizyjne.
„Śpiące oprogramowanie" wywołujące w pewnym czasie lub określonych warunkach środowiskowych niewłaściwe funkcjonowanie komputerów.	Systemy uzbrojenia, sieci komputerowe i telekomunikacyjne rządowe, administracji, banków, zaopatrzenia.

3.6. Wnioski

Zastosowanie elementów walki informacyjnej 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 uwzględniać nowe zagrożenia. Siły zbrojne będą mogły użyć najnowocześniejszych technologii informacyjnych tylko przeciwko tym siłom, które oparte są na tych technologiach, ale również i one będą narażone na oddziaływanie strony przeciwnej. Także 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 na zakup systemów uzbrojenia i broni, które zresztą objęte są zakazem eksportu do tych regionów. Rozwój nowych technologii w tych regionach będzie z pewnością długotrwały, dlatego już teraz muszą być poczynione wysiłki, które uodpornią własne systemy na oddziaływanie środków walki informacyjnej przeciwnika.

[86] Opracowano na podstawie artykułu Information warfare w: „Soldat und Technik", 12/95.

4. WALKA INFORMACYJNA WEDŁUG POGLĄDÓW ROSYJSKICH

4.1. Geneza walki informacyjnej

Podczas „Zimnej Wojny" niezwykle trudno było uzyskać dane na temat radzieckich działań psychologicznych. Przez lata Rosjanie utrzymywali swoje archiwa, struktury sił zbrojnych i procedury operacyjne w ścisłej tajemnicy.

Od 1992 roku Rosjanie przestali uważać za tajne dane dotyczące istnienia i szkolenia swoich jednostek działań psychologicznych. Jednak pozyskiwanie wiadomości o tych jednostkach i ich działaniu nadal pozostaje trudne. Pewne źródła są przekonane, że główny zarząd wywiadu wojskowego kontroluje te jednostki.

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.

W przeszłości oficerowie polityczni byli zobligowani do utrzymywania ideologicznej, moralnej i psychologicznej stabilności żołnierza. Jednakże rosyjskie społeczeństwo jest w okresie przemian, a rosyjscy socjologowie uważają, że ludność oraz siły zbrojne są psychologicznie niestabilne i szczególnie podatne na obce operacje informacyjne. Zatem szczególnie ważne okazuje się wymaganie zdolności do przeciwdziałania informacyjno-psychologicznemu potencjałowi przeciwnika. Przeciwdziałanie ekspansjonizmowi informacyjnemu i ochrona narodowych interesów Rosji są w pewnym stopniu tożsame. Prawdopodobna jest obecnie sytuacja, w której może nastąpić cicha agresja (atak informacyjny), poprzedzająca na kilka tygodni czy miesięcy rozpoczęcie operacji wojskowych na pełną skalę. Niektórzy teoretycy rosyjscy uważają, że choć w rzeczywistości nie ma wojny lub konfliktu zbrojnego, to faktyczna agresja już się rozpoczęła. Tak więc, jeśli środki przeciwdziałania agresji informacyjno-psychologicznej nie zostaną we właściwy sposób rozwinięte i udoskonalone, konsekwencje dla kraju w przyszłości mogą okazać się niezwykle poważne.

W „Military Review" nr 7/94, w artykule zatytułowanym: „Poglądy rosyjskich specjalistów na przyszłą wojnę" stwierdzono, że *„przyszły teatr wojny charakteryzować będzie duża dynamika i intensywność powietrzno-lądowych operacji prowadzonych na dużych przestrzeniach. Działania taktyczne będą znacznie skuteczniejsze i będą prowadzone*

w sposób nielinearny, a linia teatru zniknie. Łączność będzie sporadyczna, a dowodzenie trudne. Walka informacyjna będzie najważniejszym elementem". Walka informacyjna może być prowadzona samodzielnie, bez stosowania tradycyjnych środków i sposobów działań bojowych (zbrojnych) oraz w połączeniu z nimi.

Rezultatem walki informacyjnej jest dezorganizacja funkcjonowania elementów infrastruktury przeciwnika (stanowisk dowodzenia, stanowisk ogniowych i startowych artylerii oraz pocisków rakietowych, lotnisk, baz morskich, wojskowych i cywilnych systemów łączności, składów amunicji, itp.) Jej celem są systemy informacyjne, a w szczególności materialne nośniki danych. W takim przypadku zabezpieczenie tych systemów i obiektów będzie urzeczywistniać się w ochronie ich materialnych nośników.

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

Współczesny konflikt można rozpatrywać jako połączenie dwu komponentów: „ognia elektronicznego" i „informacji". Ogień elektroniczny - to zniszczenia dokonane przez środki ogniowe oraz potencjał walki radioelektronicznej mające bezpośrednie oddziaływanie na sprzęt i żołnierzy przeciwnika. Komponent informacyjny jest określany możliwościami środków zdobywania informacji i wykorzystania ich w celu zwiększenia potencjału bojowego. Do zadań środków aktywnych w tym zakresie będzie należało:

- wprowadzanie „wirusów" do programów przeciwnika lub uszkodzenie ich w inny sposób;
- wykonywanie uderzeń za pomocą broni wykorzystującej wiązkę super wysokiej częstotliwości lub „impuls elektromagnetyczny".

Do zadań środków pasywnych będzie należało:

- wykorzystanie nowoczesnych rakiet przeciwradiolokacyjnych i środków bezpilotowych;
- spowodowanie zakłóceń w pracy systemów przeciwnika;
- użycie broni jądrowej i nowoczesnej amunicji konwencjonalnej;
- wykorzystanie wirusa komputerowego.

Współczesny konflikt zbrojny powinien być rozpatrywany w świetle synergii dwóch elementów składowych:

- sprzężenia ognia i elektroniki;
- systemów informacyjnych.

Rosjanie, podobnie jak Amerykanie za główne formy walki informacyjnej uważają:

— podstęp;

— operacje psychologiczne;
— niszczenie fizyczne;
— ochrona tajemnicy wojskowej;
— walka elektroniczna

4.2. Definicje ogólne

Rosyjscy teoretycy wojskowi utożsamiają „walkę informacyjną" z „wojną informacyjną", stosując te pojęcia zamiennie. Ich zdaniem „walkę informacyjną" można umieścić między „zimną" wojną obejmującą wojnę ekonomiczną, a wojną „gorącą" z użyciem broni konwencjonalnej lub jądrowej[87]. W porównaniu z ekonomiczną, rezultatem wojny informacyjnej jest dezorganizacja funkcjonowania elementów infrastruktury przeciwnika (stanowisk dowodzenia, stanowisk ogniowych i startowych artylerii oraz pocisków rakietowych, lotnisk, baz morskich, wojskowych i cywilnych systemów łączności, składów amunicji, itp.) W porównaniu z wojną otwartą (w której masowo stosuje się środki rażenia), celem wojny informacyjnej nie są materialne obiekty, tylko systemy informacyjne lub ich materialne nośniki. W takim przypadku zabezpieczenie tych systemów i obiektów będzie urzeczywistniać się w ochronie ich materialnych nośników.

Wojna informacyjna może być prowadzona samodzielnie, bez stosowania tradycyjnych środków i sposobów działań bojowych (zbrojnych) oraz w połączeniu z nimi.

Sposoby. – w czasie pokoju- elektroniczne zastraszanie;
— w czasie narastania kryzysu – selektywne (pod względem celów) i zmasowane (pod względem intensywności) użycie środków elektronicznych przeciwko wojskowym i cywilnym strukturom dowódczym i informacyjnym przeciwnika;
— w czasie trwania konfliktu zbrojnego – zmasowane użycie zarówno środków radioelektronicznych jak i ogniowych przeciwko wojskowym i cywilnym strukturom dowódczym i informacyjnym przeciwnika.

W 1996 roku została opracowana Doktryna Operacji Informacyjno – Psychologicznych. W siłach zbrojnych nie używa się terminu operacje psychologiczne. W czasach radzieckich (byłego ZSRR) operacje takie były określane mianem "specjalnej propagandy". Aktualnie rosyjscy autorzy wojskowi używają terminu "działania informacyjno-psychologiczne", określając to, co na Zachodzie określa się mianem operacji psychologicznych. Tak więc termin działania informacyjno-psychologiczne i bardziej znany

[87] Пожидаев Д.: *Информационная Война В Планах Пентагона. W: "Зарубежное Военное Обозрение".* 2/1996.

amerykański "Operacje Psychologiczne" używane są zamiennie.

Jest to kompleks przedsięwzięć, obejmujących: wsparcie, przeciwdziałanie i obronę informacyjną, prowadzonych według jednolitej koncepcji i planu, w celu wywalczenia i utrzymania panowania nad przeciwnikiem w dziedzinie informacyjnej podczas przygotowania operacji wojskowych oraz prowadzenia działań bojowych.

W Związku Radzieckim partia komunistyczna używała propagandy jako środka kontroli społeczeństwa i sił zbrojnych. Przejście od komunizmu do demokracji pozostawiło pustkę ideologiczną, lecz stworzyło nową koncepcję: ochronę informacyjną społeczeństwa. Aby dostosować się do tej nowej koncepcji Rosjanie wprowadzili kilka zmian.

Po pierwsze: walka informacyjno-psychologiczna zastąpiła walkę propagandowo-agitacyjną marksizmu-leninizmu.

Po drugie, niektórzy teoretycy uważają operacje psychologiczne za niezależną formę działań militarnych, która wymaga wyspecjalizowanego personelu i ćwiczeń.

Po trzecie, jako konsekwencja powyższego, rosyjskie siły zbrojne będą rozwijały dodatkową specjalność militarną skierowaną na konfrontację psychologiczną.

Po czwarte, rosyjska kadra oficerska uświadamia sobie, że informacyjno psychologiczne potyczki są integralną częścią działań informacyjnych.

4.3. Doktryna operacji informacyjno – psychologicznych

W rosyjskiej Doktrynie Operacji Informacyjno - Psychologicznych stwierdza się, że działania te będą obejmować zwykle transmisje RTV, akcje ulotkowe oraz elektroakustyczne. W przeszłości Rosjanie stosowali transmisje RTV w celu zakłócenia audycji nadawanych przez przeciwnika. Oficjalne komunikaty rządu rosyjskiego są wykorzystywane do wprowadzenia sił przeciwnika w błąd.

Według teoretyków jak i praktyków rosyjskich, niektóre nietradycyjne działania informacyjno-psychologiczne również się sprawdzają. Na przykład: wstrząs i terror psychologiczny wywołany atakami artylerii i lotnictwa od dawna uważane są przez niektóre dowództwa za działanie psychologiczne. Gdy rosyjskie czołgi zaatakowały budynek parlamentu rosyjskiego w październiku 1993, głównym celem ataku było wywołanie wstrząsu lub wpływu psychologicznego na osoby okupujące budynek. Kiedy w styczniu 1996 w mieście Pierwomajskaja Rosjanie zaatakowali czeczeńskich rebeliantów ciężkim ostrzałem artylerii i rakiet, dowódca rosyjski opisał te działania jako formę operacji psychologicznych.

Innym nietradycyjnym działaniem informacyjno-psychologicznym jest rosyjska koncepcja „oddziaływania zwrotnego", dział teorii kontroli odnoszący się do wpływania na

decyzje innych. W kontekście wojskowym może być określony jako sposób zapewnienia dowódcy wojskowemu możliwości bezpośredniego utrzymywania kontroli nad procesem podejmowania decyzji przez dowódców przeciwnika. Oddziaływanie zwrotne jest procesem manipulowania danymi tak, aby wróg zmuszony był do podjęcia działań korzystnych dla drugiej strony.

Rosjanie uważają, że oddziaływanie to można prowadzić zarówno na poziomie strategicznym, operacyjnym, jak też taktycznym. Niektórzy postrzegają Inicjatywę Obrony Strategicznej (SDI), jako manewr polityczny przeznaczony do zmuszenia ZSRR do podjęcia działań korzystnych dla USA. W wysiłkach dotrzymania kroku osiągnięciom amerykańskim w obszarze SDI były ZSRR wyczerpał się gospodarczo. Obecnie niektórzy Rosjanie pytają, czy koncepcja wojny informacyjnej jest po prostu kolejną próbą oddziaływania na nich i nakłonienia ich do zainwestowania ogromnych sum pieniędzy w technologie, które są prawdopodobnie poza rosyjskim zasięgiem w bliskiej przyszłości.

Rosyjskie Siły Zbrojne na poziomach taktycznym i operacyjnym długo badały wartość oddziaływania zwrotnego zarówno w kontrolowaniu procesów decyzyjnych wroga, jak i rozwijaniu technik "maskirowki" (mylenie, dezinformacja). Na początku 20. wieku istniała wojskowa szkoła „maskirowki", która stała się podstawą rozwoju tej koncepcji dla przyszłych pokoleń. Szkoła została rozwiązana w 1929.

Ostatnio obfitość artykułów na temat oddziaływania zwrotnego pojawiających się w rosyjskich pismach wojskowych wskazuje, że teoria „maskirowki" żyje i przechodzi odnowę w celu dostosowania do bieżących warunków wliczając w to zawiłości wieku komputerowego. Generał Major M. Jonow (w stanie spoczynku) napisał artykuł nt. oddziaływania zwrotnego, który ukazał się w "Morskoj Sbornik" w 1995 roku. Przedstawił kilka zasad kontroli przeciwnika. Po pierwsze inicjator musi przewidzieć odpowiedź przeciwnika na warunki, które planuje wprowadzić. Po drugie inicjator powinien przewidzieć, że przeciwnik może odkryć to działanie i wprowadzić swoje własne środki przeciw kontroli. Po trzecie inicjator powinien być świadomy technicznego poziomu środków walki przeciwnika, szczególnie rozpoznania (im wyższy poziom technologiczny tym bardziej prawdopodobne jest prowadzenie działań dezinformujących). Po czwarte inicjator powinien rozważyć efekt użycia ostrych form nacisku na przeciwnika, biorąc pod uwagę elementy społeczne oraz czynniki intelektualne, psychologiczne, etyczne i ideologiczne.

Wielu rosyjskich socjologów rozumie, że rosyjskie siły zbrojne (po części z powodu braku treningu moralno-psychologicznego) są aktualnie bardzo podatne na informacyjno-psychologiczny atak. W przeszłości system szkolenia organów propagandy wypełniał rolę

treningu moralno-psychologicznego. Jednakże wobec braku politycznych organów partii komunistycznej, ideologia już nie ma roli dominującej w psychologii, socjologii, psychiatrii i innych działach nauki.

Moralno-psychologiczne wsparcie może być zdefiniowane jako celowy wpływ na umysły i psychikę rosyjskiego personelu wojskowego. Dowódcy, sztaby i jednostki indoktrynujące są odpowiedzialne za umacnianie psychologicznej odporności wśród personelu i formowanie ich moralnej gotowości do działania w dowolnych warunkach. Dowódcy polowi powinni podejmować szczególne wysiłki na utrzymanie korelacji moralno-psychologicznej podległych sił w równowadze.

Według rosyjskich analityków, wydarzenia lat 90-tych spowodowały zasadniczą zmianę militarno - politycznej sytuacji w świecie, a także socjalno-ekonomicznych i moralno-psychologicznych stosunków wewnątrz krajów. Współczesne tendencje w rozwoju sił zbrojnych, środków i zdolności walki zmieniły się w związku z ich funkcjami, podobnie jak znaczenie zasad sztuki wojennej oraz ich zależności od stosunku sił moralno-psychologicznych przeciwnych stron. Istnieje zatem rzeczywista potrzeba tworzenia struktur moralno-psychologicznego wsparcia w siłach zbrojnych.

Informacyjno-psychologiczne bezpieczeństwo polega na zagwarantowaniu stabilności psychiki i świadomości osób w czasie pokoju i wojny. Obejmuje środki do zwalczania wrogich akcji, które mogłyby mieć negatywny wpływ na kondycję moralno-psychologiczną sił oraz środki do osłabiania lub zniwelowania informacyjno-psychologicznego oddziaływania na grupy populacji lub całe rosyjskie społeczeństwo. Informacyjno-psychologiczne bezpieczeństwo winno przeciwdziałać negatywnym skutkom operacji informacyjnych na moralno-psychologiczne przygotowanie żołnierza.

System informacyjno-psychologicznego bezpieczeństwa jest obecnie szczególnie ważny, ponieważ w ciągu ostatniego półwiecza dramatycznie wzrosła zdolność kształtowania świadomości, psychiki oraz morale społeczeństwa i sił zbrojnych. Jedną z głównych przyczyn są znaczące dokonania wielu krajów na drodze systematycznych badań w dziedzinach psychologii, psychotroniki, parapsychologii[88], innych nowych psychofizycznych zjawisk.

---

[88] Parapsychologia jako odrębna dyscyplina naukowa powstała w Europie Zachodniej w drugiej połowie XIX wieku. Następnie zaczęto stosować pojęcie psychotronika. Obydwa te terminy w literaturze są zastępowane skrótem *psi,* obejmującym cały szereg zjawisk, których poznanie dokonuje się poprzez nieznane bliżej kanały poznawcze, z wyłączeniem zmysłów człowieka. Innymi słowy jest to poznanie ponadzmysłowe. Zjawiska te świadczą, że istnieje jakaś rzeczywistość niewykrywalna i nieuchwytna poprzez zmysły człowieka oraz, że człowiek ma bliżej nieokreśloną możliwość, za pomocą której tę rzeczywistość okrywa. Jednak tylko około 20% ludzi posiada taką możliwość.

Podstawowe założenia rosyjskich działań informacyjno-psychologicznych obejmują:

- ✓ Analizowanie stanu moralno-psychologicznego środowiska w Rosji, w obszarach strategicznych oraz operacyjnych.
- ✓ Poszukiwanie, zbieranie, analizowanie i uogólnianie danych o możliwościach potencjalnych uczestników konfliktu.
- ✓ Przewidywanie prawdopodobnej natury i możliwego wpływu operacji psychologicznych przeciwnika na rosyjskie siły zbrojne i ludność.
- ✓ Blokowanie (lub łagodzenie efektów) tych operacji na poziomie strategicznym, przy użyciu wszelkich dostępnych rodzajów działań.
- ✓ Dostarczenie środków do przeciwdziałania stałemu i wielkoskalowemu ideologicznemu i informacyjno-psychologicznemu wpływaniu na rosyjskie siły zbrojne i ludność.
- ✓ Neutralizowanie negatywnych konsekwencji oddziaływania na świadomość, morale i stan ducha.
- ✓ Ciągłą ochronę wojsk i ludności przed informacyjno-psychologicznym oddziaływaniem.
- ✓ Przygotowanie sił i środków do prowadzenia walki informacyjno-psychologicznej.
- ✓ Prowadzenie informacyjno-psychologicznych i specjalnych operacji obniżających morale i stan psychologiczny wojsk przeciwnika i jego ludności oraz demoralizowanie i dezinformowanie ich.
- ✓ Wywieranie stałego wpływu informacyjno-psychologicznego na siły i ludność przeciwnika.
- ✓ Prowadzenie działań psychologicznych i innych typów niekonwencjonalnych sposobów wpływu na świadomość i stan psychiczny przeciwnika.
- ✓ Rozwijanie metodologii i teorii informacyjno-psychologicznej walki oraz rozwój zaleceń oraz propozycji dla agencji rządowych i dowództwa wojskowego.

4.4. Atak psychologiczny

Niektórzy rosyjscy teoretycy wojskowi wierzą, że współczesny rozwój technik walki informacyjnej powoduje, że informacyjno-psychologiczna konfrontacja staje się nieodłącznym typem działań militarnych, podobnie jak obrona i atak. Ich zdaniem, w dowolnym konflikcie zbrojnym, działania militarne będą poprzedzone przez środki projektowane do oddziaływania na świadomość, morale i psychikę ludności.

Istnieje ścisły związek pomiędzy walką informacyjną, a konfrontacją informacyjno-psychologiczną. Głównym celem walki informacyjnej będzie kształtowanie świadomości ludności Federacji Rosyjskiej w celu osłabienia moralno-psychologicznego potencjału sił

zbrojnych, to jest umożliwienia politycznej, ekonomicznej i psychologicznej penetracji. Przy takim założeniu zarówno informacyjne, jak i psychologiczne akcje są nieustannie prowadzone i to zarówno przez potencjalnych przeciwników Rosji.

W krytycznej sytuacji operacje informacyjno - psychologiczne mogą spowodować większe szkody moralne, niż jakakolwiek poprzednia wojna. W rezultacie siły zbrojne muszą podjąć to informacyjno-psychologiczne wyzwanie poprzez tworzenie systemu zdolnego do kontrakcji.

Rosjanie uważają, że jednostki wojskowe prowadzące informacyjno-psychologiczne operacje winny być traktowane jako odrębny rodzaj sił zbrojnych. Niezdolność do kontrakcji lub odpowiedzi na te operacje, które nazywane są "propagandą", będą skutkowały porażką, jak to było w przypadku armii irackiej w czasie wojny w rejonie Zatoki Perskiej. Rosjanie analizując amerykańską koncepcję operacji informacyjnych z 1996 roku, oświadczyli że

- zasadne jest zapewnienie zrozumiałego, teoretycznego opracowania problemu propagandy i wsparcia psychologicznego w czasie pokoju, w czasach wzrostu napięć wojskowo-politycznych i w czasie wojny.
- istotne jest połączenie struktur zaangażowanych w prowadzenie propagandy i psychologicznego wsparcia dla sił zbrojnych Rosji z ogólnymi zadaniami i konkretnymi strukturami kontrolno-decyzyjnymi.
- dowódcy wszystkich szczebli powinni wykorzystywać organy psychologicznego wsparcia, a ćwiczenia z ich udziałem należy włączyć do zadań organizacyjnych wojska.

4.5. Nowa specjalność wojskowa

Jedną z ciekawszych propozycji jest sformowanie osobnej specjalności w ramach rosyjskich sił zbrojnych, rekrutujących specjalistów w sztuce zbierania i oddziaływania informacyjnego. Wymagane będą specjalne fundusze ze względu na unikalny charakter treningu tych jednostek. Ta sugestia jeszcze raz potwierdza rosyjski zamiar uruchomienia w czasie pokoju specjalności, która zdolna będzie wykryć operacje informacyjne skierowane przeciw ludności bądź armii, oraz zainicjować własną ofensywną operację informacyjną. Takie operacje mogłyby rozciągać się od subtelnych, prowokacyjnych operacji syntezy głosu - projektowanych do "hipnotyzowania" ofiar, po „wirusowy" atak komputerowy.

Jak uważają specjaliści, dużo gorzej jest pozostać w tyle w dziedzinie konfrontacji informacyjno-psychologicznej, niż w dziedzinie cybernetyki. Nie rozwiązanie problemu informacyjno-psychologicznej konfrontacji czyni niemożliwym konsolidację społeczeństwa i stabilizację sytuacji w państwie, choć są one fundamentalne dla odbudowy Rosji.

4.6. Wnioski.

Rosja jest szczególnie zainteresowana w rozwoju i wdrażaniu technik operacji informacyjno-psychologicznych przez światowe potęgi. Operacje informacyjne mają poważne implikacje dla Rosji zarówno w technicznym, jak i moralno-psychologicznym aspekcie. Z powodu aktualnej psychologicznej niestabilności, która dotyka Rosję, Rosjanie odnoszą się do operacji informacyjnych z zaniepokojeniem, podejrzeniami i brakiem zaufania. Wskazują, że informacyjne bezpieczeństwo jednostki i całego społeczeństwa jest jednym z priorytetów interesu narodowego.

Armia rosyjska jest szczególnie zainteresowana wpływem operacji informacyjno-psychologicznych na swoich żołnierzy - co wynika z doktryny wojennej. Należy oczekiwać, że rosyjska armia będzie gotowa do prób wykorzystania narzędzi operacji informacyjnych przeciw innym krajom.

Wzmaga się dyskusja na temat koncepcji operacji informacyjno-psychologicznych i związanych z nimi zagadnień. W marcu 1994 roku w rosyjskiej telewizji stwierdzono, że jakkolwiek każda armia ma psychologów, to problem utworzenia służb psychologicznych nie jest rozwiązany. 29 marca 1996 doniesiono, że o podjęciu decyzji w sprawie odtworzenia zunifikowanego systemu służby prasowej w armii.

W artykule z 23.05.1996 roku Moskiewskiego Komsomolca, rozważa się powrót do struktur militarnych jednostek "propagandy", jako środka kontroli informacyjnej. Doniesiono, że do wszystkich okręgów wojskowych przesłano szyfrowane depesze, w których prosi się dowódców o wyrażenie opinii na temat podporządkowania się okręgowych centrów prasowych głównemu zarządowi Pracy Wychowawczej. Artykuł sugeruje, że takie podporządkowanie będzie prowadziło do przejęcia przez Zarząd Wychowawczy kontroli nad okręgowymi centrami prasowymi, prasą wojskową i jednostkami propagandowymi. Innymi słowy, począwszy od 1991 roku, wszystkie te służby, łącznie z agendami politycznymi utworzyły, na wzór radziecki, Główny Zarząd Polityczny Wojska i Marynarki Wojennej.

Operacje informacyjno – psychologiczne w niedalekiej przyszłości staną się niezbędnymi, ze względu na możliwość wpływania zarówno na decydentów, jak i na żołnierzy. Jednolite zespoły działań informacyjno - psychologicznych mogą stać się niezależnym rodzajem sił zbrojnych, wartym bliższych studiów i bardziej nowatorskiego wykorzystania.

Strona dysponująca przewagą w dziedzinie rozpoznania, dowodzenia i walki radioelektronicznej, będzie zawsze miała większe możliwości bojowe nawet w sytuacji, kiedy

przeciwnik ma wyraźną przewagę w dziedzinie broni jądrowej, a tym bardziej jeśli ta przewaga ogranicza się do broni konwencjonalnej.

Z punktu widzenia efektywnego wykorzystania środków finansowych wzrost liczbowy sprzętu jest obecnie ślepym zaułkiem zwiększania potencjału bojowego wojsk. Wyposażenie w nowe urządzenia radioelektroniczne i komputerowe środków ogniowych, walki radioelektronicznej, systemów rozpoznania i dowodzenia jest obecnie najszybszą metodą zwiększania efektywności bojowej sił zbrojnych. Możliwości bojowe systemów rozpoznania, dowodzenia i walki radioelektronicznej muszą być uwzględniane przy wszelkich analizach i ocenach siły ugrupowania bojowego zarówno przeciwnika jak i własnego.

Wyścig zbrojeń wkracza w dziedzinę oprogramowania; im bogatszy wachlarz przydatnych programów w funkcjonowaniu autonomicznych środków walki i systemach podejmowania decyzji, tym większa możliwość skutecznego ich użycia w warunkach bojowych.

5. WŁOSKIE POGLĄDY NA PROWADZENIE WALKI INFORMACYJNEJ

5.1. Pojęcie walki informacyjnej

Włoscy eksperci wojskowi uważają, że rozwój elektroniki i systemów informacyjnych spowodował powstanie nowych form walki określanych mianem walki informacyjnej. Ponadto stwierdzają, że stosowany w niektórych państwach termin "wojna informacyjna" budzi wiele kontrowersji, dlatego też został on zastąpiony określeniem „operacje informacyjne". W działaniach tego typu ważne jest prawidłowe rozumienie sposobów funkcjonowania systemów przekazywania danych, wykorzystania sieci łączności i baz danych, a przede wszystkim rozpoznanie całej "architektury" systemów informacyjnych przeciwnika. Problematyka walki informacyjnej nabrała dużego znaczenia w wielu krajach i stała się aktualnym przedmiotem badań.

5.2. Zakres walki informacyjnej

Według poglądów włoskich walka informacyjna obejmuje siedem różnych wzajemnie uzupełniających się elementów:

- zakłócanie systemów dowodzenia i kontroli przeciwnika (C2);
- operacje rozpoznawcze;
- operacje psychologiczne;
- walkę elektroniczną;
- walkę ekonomiczną;
- piractwo komputerowe;
- walkę cybernetyczną.

Zakłócanie systemów dowodzenia i kontroli przeciwnika ma na celu ograniczenie wykorzystania systemów C2, tak aby nie mógł on przekazywać danych, dowodzić i kierować swoimi wojskami. Innymi słowy będą to działania polegające na "atakowaniu" systemów dowodzenia i kontroli przeciwnika.

Operacje rozpoznawcze prowadzone są w celu ustalenia podstawowych danych o przeciwniku (dyslokacji elementów ugrupowania bojowego, zamiaru działania oraz możliwości manewru). Inaczej działania te będą polegać na rozpoznaniu systemu, który będzie "atakowany".

Operacje psychologiczne (PSYOPS) są skierowane na świadomość dowódców i żołnierzy. Mają na celu wywołanie u nich dużego dyskomfortu psychicznego, irytacji lub

zdenerwowania. Są to przedsięwzięcia bardzo złożone i trudne, ponieważ dotyczą nie tylko sfery umysłowej, ale także emocjonalnej osób poddawanych presji psychicznej. Mogą być wystarczające do zmiany stylu ich działania i mieć znaczny wpływ na podejmowane decyzje.

Walka elektroniczna to przedsięwzięcia związane z zapewnieniem dostępu do spektrum elektromagnetycznego dla wojsk własnych i pozbawieniem takich możliwości strony przeciwnej. Innymi słowy polegać ona będzie na wykrywaniu i zakłócaniu systemów elektronicznych przeciwnika i zapewnieniu niezakłóconego wykorzystywania własnych systemów.

Walka ekonomiczna obejmuje przedsięwzięcia związane ze zdobywaniem informacji gospodarczych i oddziaływaniem na gospodarkę przeciwnika.

Piractwo komputerowe polega na dokonywaniu włamań do komputerów. „Hackerom" udaje się ten proceder, ponieważ potrafią ominąć specjalne zabezpieczenia. Najczęściej monitorują wybraną sieć, a następnie podszywają się pod jakiś zaufany komputer w tej sieci i przechwytują dane, na podstawie których otwierają sobie drzwi do systemu informacyjnego. Włamywacze nie muszą korzystać wyłącznie z luk w systemach bezpieczeństwa. Mają możliwość „podglądania" interesującej ich sieci dzięki urządzeniom wbudowanym w sprzęt komputerowy. Mogą także analizować emisję pola elektromagnetycznego generowanego przez monitor (np. głównego komputera w sieci) i na tej podstawie odtwarzać dane wyświetlane na ekranie komputera.

Walka cybernetyczna polega na uszkadzaniu i niszczeniu systemów informatycznych przeciwnika. Walka ta jest wiele groźniejsza od piractwa komputerowego. Są to przede wszystkim działania zorganizowane, prowadzone w określonym celu, nie tylko przeciwko pojedynczym osobom, ale także przeciwko organizacjom czy konkretnym państwo. Obszary zastosowania walki cybernetycznej są wszędzie tam, gdzie pozwala na to dostęp do systemów informacyjnych.

5.3. Wnioski

Obiektami walki informacyjnej mogą być zarówno wojskowe, jak i cywilne systemy informacyjne, które nasycone są techniką komputerową.

Specjaliści włoscy uważają, że użycie środków walki informacyjnej jest z kilku powodów skuteczniejsze niż oddziaływanie broni.

Po pierwsze, może ono nastąpić w sposób zorganizowany, przy znikomych stratach wojsk własnych.

Po drugie, wykrycie tych środków walki może nastąpić zbyt późno, co praktycznie uniemożliwi podjęcie przeciwdziałania.

Po trzecie, skuteczność nie zależy od liczebności armii czy ilości uzbrojenia, lecz od „inteligencji" użytych środków i ich skutecznego działania.

Wprowadzenie narzędzi walki informacyjnej spowoduje, że stanie się ona kluczem do sukcesu w operacjach militarnych. Umożliwi wygranie konfliktu, czy wojny przy wykorzystaniu mniejszej ilości sił i środków oraz minimalnych stratach własnych.

Rosnące znaczenie tej walki wymusza konieczność zmian w teorii sztuki wojennej oraz przygotowywaniu i prowadzeniu operacji militarnych i innych.

ZAKOŃCZENIE

Zastosowanie narzędzi walki informacyjnej może spowodować, nie tylko jak dotychczas straty powstałe w wyniku walk, lecz w krótkim czasie doprowadzić do totalnego zniszczenia nowocześnie zorganizowanego systemu całego państwa. Właśnie dlatego wysoko uprzemysłowione społeczeństwa są zmuszone do zastanawiania się nad środkami ochrony własnych systemów telekomunikacyjnych i informatycznych nie tylko w aspekcie militarnym. Polityka bezpieczeństwa i obrony zyskuje więc pewien zupełnie nowy wymiar. Formy organizacji i strategii muszą być dopasowane do nowych zagrożeń. W sytuacji gdy wyposażone w najnowszą technikę do prowadzenia „walki informacyjnej" siły zbrojne mogą ją zastosować tylko przeciwko tym siłom, które oparte są na tej technice, mogą one być też same narażone na straty spowodowane przez siły zbrojne strony przeciwnej, która ma do dyspozycji znacznie mniej środków w tej dziedzinie. Także siły polityczno-militarne z punktu widzenia bezpieczeństwa politycznego 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 na zakup systemów uzbrojenia, które zresztą objęte są zakazem eksportu do tych regionów. Rozwój technologiczny 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 przeciwnika środkami „walki informacyjnej".

Dlatego tez racjonalne modelowanie sił zbrojnych podporządkowywane jest kryterium minimalizacji kosztów i maksymalizacji siły bojowej wojsk. Osiągnięcie tego staje się możliwe przy umiejętnym adaptowaniu postępu naukowo-technicznego do uzbrojenia i wyposażenia wojsk. W efekcie tego mniej doskonała i bardziej kosztowna ilość jest zastępowana doskonalszą i mniej kosztowną jakością.

Redukcja wydatków jest możliwa poprzez wdrażanie do wojsk postępu naukowo-technicznego. Umożliwia to opracowywanie i produkowanie coraz lepszego i tańszego sprzętu. W następstwie tego, przy zachowywaniu tej samej a nawet zwiększonej siły bojowej wojsk, istnieje możliwość redukowania stanów osobowych i tym samym zmniejszania kosztów utrzymywania armii.

Potencjalny przeciwnik może zadać poważne straty bez użycia tradycyjnych sposobów walki oraz narażania własnych sił i środków. Oddziałując tylko na systemy

informacyjno — sterujące, przeciwnik może obezwładnić czy wręcz zniszczyć istotne elementy infrastruktury cywilnej i wojskowej. Ponadto atakujący może ukryć swoją tożsamość, a zaatakowane państwo nie będzie w stanie jednoznacznie wskazać agresora. Wynika z tego, że walka o informację staje się realnym 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 przestrzeń bezpieczeństwa państwa w sferze ekonomicznej, politycznej i militarnej. Są to argumenty przemawiające za potrzebą ciągłego doskonalenia i rozwijania narzędzi zdobywania, zakłócania i obrony informacyjnej.

Problematyka ta jest *sensu proprio* 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 „Regulamin walki" (FM—100—6) zawierający doktrynę operacji informacyjnych.

Ponadto we wszystkich rodzajach sił zbrojnych USA organizuje się formacje do prowadzenia walki informacyjnej. Środki i technologie informacyjne stosowane w walce informacyjnej, 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.

LITERATURA:

1. Burhans W. A.: *Iraqi Air Defenses — Initial Soviet Post — Mortem.* W: *„Journal of Electronic Defense"*, October 1991.
2. Campen A. D: *„The first Information War"*. Virginia 1992.
3. Ciborowski L.: *„Przestrzenie walki informacyjnej"*. AON, Warszawa 1997.
4. Ciborowski L.: *"Walka informacyjna"*. Wyd. A. Marszałek. Toruń 1999.
5. Falicber O.*: Shilka `versus the B-52* . W: *„Krasnaja Zwiezda"* (Red Star), 4/1991.
6. Fitzgerald M. C.: *Russian views on information warfare.* W: *„Army"*, 5/1994.
7. FM - 100 - 6 (Information Operations), Waszyngton, sierpień 1996.
8. Giboney T. B.: *Chaos informacyjny.* W: *„Military Review"*, 11/91.
9. Grabau. R.: *Sechs Dimensionen des Kriegers.* W: *„Soldat und Technik"*, nr 6/1986.
10. Grange D. L., Kelly J.A.: *Information Operations for the Ground Commander.* W: *"Military Review"*. March - April 1997.
11. Grier P.: *Information Warfare.* W: *„Air Force"*, 4/1994.
12. Joint Doctrine for Command and Control Warfare (C2W), luty 1996.
13. Koncepcja Operacji Informacyjnych NATO (Information Operations Concept), kwiecień 1998.
14. Nowacki G.: *Niemieckie poglądy na walkę informacyjną, „Zeszyty Naukowe"* AON 3/2000.
15. Nowacki G.: *Pojęcie walki informacyjnej, „ZN"* AON 3/97.
16. Nowacki G.: *"Walka informacyjna - próba kategoryzacji"*. Rozprawa doktorska pod kier. naukowym L. Ciborowskiego. AON, Warszawa 1999.
17. Nowacki G.: *Walka informacyjna według poglądów amerykańskich, „PWL"* 5/1998.
18. Nowacki G.: *Wpływ walki informacyjnej na walkę zbrojną, „ZN"* AON 4/97.
19. Nowacki G.: *Współczesne formy walki informacyjnej, „ZN"* AON 2/2000.
20. Peterson K., Pracht U.: *Walka informacyjna.* W: *„Soldat und Technik"*, 12/95.
21. Пожидаев Д.: Информационная Война В Планах Пентагона. W: "Зарубежное Военное Обозрение". 2/1996.
22. Riccardelli R. F.: The Information and Intelligence. W: „Military Review", 5/95.
23. Ross J. D.: *Wojna o informację.* W: *„Army"*, 2/1994.
24. Schwartau Winn.: „Information Warfare — Cyberterrorism: Protecting Your Personal Security in the Electronic Age". 1993.

25. Starry M. D., Arneson C. W.: Działania informacyjne. W: „Military Review", 6/96.
26. Sullivan G. R., Dubik J. M.: War in the Information Age. W: „Military Review", 4/1994.
27. Toffler Alvin i Heidi: „Wojna i antywojna" (War and Antiwar). 1993.

SPIS TREŚCI