AKADEMIA
OBRONY NARODOWEJ

Mjr mgr inż. Gabriel NOWACKI

WALKA INFORMACYJNA – PRÓBA KATEGORYZACJI

Rozprawa doktorska

WARSZAWA 1999

AKADEMIA
OBRONY NARODOWEJ

Mjr mgr inż. Gabriel NOWACKI

WALKA INFORMACYJNA – PRÓBA KATEGORYZACJI

Rozprawa doktorska

WARSZAWA 1999

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH

KATEDRA ROZPOZNANIA WOJSKOWEGO I ARMII OBCYCH

mjr mgr inż. Gabriel Nowacki

WALKA INFORMACYJNA — PRÓBA KATEGORYZACJI

Rozprawa doktorska

Promotor:

płk dr hab. Leopold CIBOROWSKI
profesor nadzwyczajny AON

WARSZAWA 1999

SPIS TREŚCI

WPROWADZENIE

Do skutecznego prowadzenia walki zbrojnej konieczny jest szybki i niezawodny obieg informacji na wszystkich szczeblach dowodzenia. W ostatnim czterdziestoleciu nastąpił gwałtowny rozwój elektroniki i nowoczesnych technologii przekazywania danych. Sytuacja ta znalazła swoje odzwierciedlenie również w architekturze pola walki. Do procesów rozpoznania, systemów uzbrojenia oraz do procedur planowania, organizowania i nadzorowania walki zbrojnej wprowadzono elektronikę. Wyposażenie wojsk wzbogacono w nowe rodzaje amunicji o cechach „inteligentnych". Udoskonalono środki przenoszenia broni oraz *de facto* zwiększono ich zasięg i skuteczność działania. Skrócono w sposób zasadniczy czas reakcji ogniowej i zwielokrotniono stopień manewrowości wojsk. Dlatego też wielu teoretyków uważa, że współczesna walka zbrojna cechować się będzie dużą ruchliwością, precyzją rażenia i intensywnością obiegu informacji. Jeżeli wszystkie strony konfliktu będą dysponowały środkami rażenia o zbliżonej skuteczności i porównywalnej manewrowości, to informacja, lub jej brak, będzie *conditio sine qua non* przesądzającym o sukcesie lub porażce. Nowoczesne, precyzyjne środki rażenia — zarówno ogniowego, jak i elektronicznego — będą więc wymagały posiadania ciągle aktualnych informacji o położeniu przeciwnika, rozmieszczeniu elementów jego ugrupowania, możliwościach bojowych oraz położeniu wojsk własnych. Wynika z tego, że racjonalne modelowanie walki zbrojnej powinno prowadzić do optymalnego wykorzystywania siły rażenia wojsk przez stwarzanie warunków do osiągania jak największej precyzji ognia i jednocześnie warunków do maksymalnego skracania czasu reakcji — niezależnie od tego, czy ogień ten zostanie ostatecznie wykonany, czy też nie. Są to dwa podstawowe kryteria, których nieprzestrzeganie będzie zawsze prowadzić do wzrostu kosztów działań i zwiększania prawdopodobieństwa porażki. Niedoskonałości jakościowe w tym zakresie muszą być zrekompensowane ilością ognia oraz zwiększeniem liczby posiadanych sił i środków walki, jak również wydłużeniem czasu przebywania w strefie rażenia przeciwnika[1]. Wokół tego zlokalizowana jest istota walki informacyjnej. Informacje z rozpoznania wpływają na

[1]W dobrze funkcjonujących armiach świata, głównie w armii Stanów Zjednoczonych, doktryny wojenne zdeterminowane są dwoma lapidarnymi hasłami: „odpal i zapomnij" oraz „zwyciężaj wcześniej". Oznacza to, że wszelkie zmiany dokonywane w siłach zbrojnych uzyskują akceptację tylko wtedy, kiedy ich wdrożenie gwarantuje większą niż dotychczas precyzję rażenia i krótszy czas reakcji ogniowej. Dotyczy to zarówno struktur organizacyjnych wojsk, jak i zasad ich wykorzystywania, wdrażania nowej techniki i akceptowania programów naukowo-badawczych wojska.

precyzję rażenia, a zakłócanie i obrona informacyjna — na wyprzedzenie przeciwnika w użyciu celnego ognia. Środki i technologie informacyjne, stosowane w walce zbrojnej, mogą w znaczny sposób wprowadzić w błąd przeciwnika co do posiadanych sił i prowadzonych działań, zwiększając tym samym zdolność bojową wojsk własnych. Dowódcy zatem powinni mieć stworzone warunki do szybkiego podejmowania decyzji oraz sprawnego i skrytego wdrażania ich do realizacji.

Problematyka ta jest *sensu proprio* dostrzegana w wielu państwach NATO. Najwyższą jednak rangę nadano jej w SZ USA. W 1993 roku w waszyngtońskim Uniwersytecie Obrony Narodowej (National Defense University) została otwarta Szkoła Strategii i Walki Informacyjnej (School of Information Warfare and Strategy). Potencjał do organizowania i prowadzenia walki informacyjnej lokowany jest w sztabach i wojskach.

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 dalszym ciągu jest to *terra incognita*). Innymi słowy: brak jest na ten temat wyczerpujących publikacji naukowych w skali światowej, szczególnie zaś — w naszych siłach zbrojnych. W prezentowanych poglądach daje się zauważać *coincidentia oppositorum* oraz *contradictio in terminis*. Jedni utożsamiają walkę informacyjną z walką radioelektroniczną, drudzy — z działaniami psychologicznymi, a jeszcze inni włączają w to elementy materialne infrastruktury informacyjnej oraz procedury dowodzenia. Niekiedy walka informacyjna utożsamiana jest z pojęciem „wojna informacyjna", cyberwojna lub walka z systemami dowodzenia i łączności (C2W)[2]. Alvin i Heidi Tofflerowie[3] oceniają to jako „terminologiczny bełkot", który odzwierciedla wciąż jeszcze początkowe stadium dyskusji. Dalej konkludują, że nikt jeszcze nie podjął się tego, co stanowi tu ostatni krok, a więc opracowania systematycznej teorii walki informacyjnej i wieńczącej dzieło wojskowej „strategii opartej na wiedzy (informacji)". Jedno jest pewne, że aby zacząć konstruować ogólną strukturę tej „strategii" należy przeanalizować samą informację oraz możliwości w zakresie jej zdobywania, przetwarzania, rozdziału i ochrony. Po dokonaniu tego będzie możliwe opracowanie ogólnych zasad opartych na wiedzy, co stanie się kluczem do wielu, jeśli nie do wszystkich, militarnych zwycięstw *pro futuro*.

---

[2]C2W - walka z systemami dowodzenia i kontroli (Command and Control Warfare).

[3]A. i H. Tofflerowie: *„War and Anti-War: Survival at the Dawn of the Twenty First Century"* (twórcy pochodzącej od ich nazwiska teorii fali) są obecnie doradcami przewodniczącego Izby Reprezentantów Newta Gingricha. Ponadto na ich opinie powołuje się również wielu wojskowych.

Uwzględniając *ex professo* wyżej wymienione powody oraz wzrost zainteresowania tym tematem, można stwierdzić, że jest to problem:

— 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.

Wynika więc z tego, że temat rozprawy jest z punktu naukowego jak najbardziej aktualny. Przy pomyślnym sfinalizowaniu go można by dokonać wielu rozstrzygnięć, które dziś są tematem licznych dyskusji i sporów.

Prowadzone 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 przedmiotu badań (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. Wymaga to jednak naukowego potwierdzenia drogą rozwiązania szeregu problemów, z których część podjęto w ramach rozprawy. Należy mieć świadomość, że obszar prowadzonych badań naukowych jest ogromny i przekracza możliwości realizacyjne jednego wykonawcy, a rozprawa jest jedynie „uruchomieniem" procedury poznawczej w tej problematyce.

Rozprawa zawiera wyniki badań, ujęte w formie teorii, oraz propozycje przyszłościowych rozwiązań dotyczących walki informacyjnej. Praca składa się z wprowadzenia, trzech rozdziałów i zakończenia.

Wprowadzenie obejmuje założenia merytoryczno — metodologiczne, niezbędne do przeprowadzenia badań. Ujęto w nim cel badań i problemy badawcze. Ponadto przedstawiono przyjęte hipotezy robocze oraz metody badawcze, których realizacja pozwoliła zweryfikować hipotezy robocze i osiągnąć cel badań.

Zasadniczą treścią rozdziału pierwszego jest uporządkowana teoria walki informacyjnej. Zawiera on rozważania i ustalenia dotyczące interpretacji terminów:

„informacja", dane, sygnał informacyjny i sterujący, komunikat, system informacyjno — sterujący oraz „walka informacyjna". Scharakteryzowano w nim przestrzeń oraz istotę walki informacyjnej.

W rozdziale drugim przedstawiono genezę formalną oraz nieformalną walki informacyjnej. Ustosunkowano się również do amerykańskich poglądów w tym zakresie.

Rozdział trzeci obejmuje związki pomiędzy walką informacyjną a walką zbrojną. Scharakteryzowano w nim wpływ informacji na walkę zbrojną (w tym korzyści wynikające z uzyskania przewagi informacyjnej) oraz znaczenie walki informacyjnej na współczesnym polu walki.

W zakończeniu rozprawy podkreślono trafność wyboru i sformułowania celu badań, problemów badawczych, przyjętych założeń oraz hipotez roboczych. Przedstawiono ocenę stopnia realizacji zadań badawczych, propozycje dotyczące zastosowania wyników badań oraz kierunki dalszego pogłębiania i rozszerzania badań.

Założenia merytoryczno — metodologiczne

W badaniach *sine ira et studio* przyjęto, że czynnością decydującą o ich powodzeniu było uświadomienie sytuacji problemowej, sformułowanie celów badań naukowych oraz wysunięcie i sprecyzowanie problemów naukowych[4].

Sformułowane problemy naukowe oparte zostały na przyjętych założeniach[5]. Założenia sformułowano przede wszystkim w oparciu o dotychczas nagromadzoną wiedzę o walce informacyjnej. Zasadnicze twierdzenia, ważne dla właściwego rozumienia i ujęcia problemu naukowego zostały przyjęte jako założenia podstawowe, pierwotne. Podczas definiowania walki informacyjnej szczególną uwagę zwrócono na ujęcie czynnościowe i systemowe. Przy dokonywaniu podziału przestrzeni walki informacyjnej na podprzestrzenie uwzględniono kryteria rozstrzygalności (zgodnie z zasadami teorii mnogości i logiki), skupiając się głównie na zasadniczym, jednorodnym podziale.

Nie mniej ważnym elementem było wysunięcie hipotez roboczych. O ile sprecyzowanie problemów naukowych miało na celu określenie obszaru niewiedzy o walce informacyjnej, o tyle hipotezy robocze były drogą, sposobem pomyślnego rozwiązania problemów badawczych.

---

[4]Przyjęto następującą interpretację terminu „problem naukowy": subiektywne odzwierciedlenie obiektywnych niedostatków w nauce; fragment uświadomionej w obszarze nauki obiektywnej niewiedzy; swoiste pytanie, określające jakość i rozmiary niewiedzy.

[5]Założenie to teza stanowiąca podstawę i punkt wyjścia do dalszych wywodów; główna myśl, zasada czegoś. *Słownik języka polskiego*, t 3, PWN, Warszawa 1981, s.924.

Do przeprowadzenia badań niezbędny był również wybór i zastosowanie odpowiednich metod, technik i narzędzi badawczych.

Cele badań

Treść poznawcza rozprawy została podporządkowana osiągnięciu *głównego celu:*

1. ***Wyodrębnić, zdefiniować i uporządkować podstawowe pojęcia i desygnaty walki informacyjnej, odzwierciedlające najistotniejsze związki w jej przedmiocie, narzędziach i przestrzeni.***

Ponadto:

2. *Dowieść, że walka informacyjna zawsze towarzyszyła walce zbrojnej i wywierała istotny wpływ na jej przebieg i wynik, niezależnie od tego, czy formalnie była tak nazywana, czy też nie.*
3. *Określić związki funkcjonalne występujące pomiędzy walką informacyjną i walką zbrojną.*

Problemy badawcze

Osiągnięcie głównego celu badań nastąpiło na drodze rozwiązania *głównego problemu badawczego*:

Czym jest walka informacyjna i jak ją można kategoryzować?

Z głównego problemu badawczego wyniknęły następujące *problemy szczegółowe*:

1. *Jakie są podstawowe pojęcia i desygnaty walki informacyjnej, odzwierciedlające najistotniejsze związki w jej przedmiocie, narzędziach i przestrzeni?*
2. *Jaka jest geneza walki informacyjnej w aspekcie wcześniej zdefiniowanego desygnatu tego pojęcia?*
3. *W jaki sposób za pomocą walki informacyjnej można wpływać na działania zbrojne przeciwnika i wojsk własnych?*

Hipotezy robocze

Rozwiązywanie głównego problemu naukowego realizowano drogą weryfikacji głównej hipotezy roboczej:

Właściwie przygotowana, zorganizowana i prowadzona walka informacyjna umożliwia racjonalne wykorzystanie sił zbrojnych oraz systemów uzbrojenia, co stanowi podstawę osiągania sukcesu w walce zbrojnej.

W odniesieniu do przedstawionych problemów szczegółowych przyjęto następujące szczegółowe hipotezy robocze:

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

   „Przedmiotem walki informacyjnej" są systemy informacyjno — sterujące i ich otoczenie. Każda ze stron dąży do tego, aby jej system funkcjonował lepiej i zdobył jak najwięcej danych o przeciwniku, pozwalających identyfikować jego stan aktualny i zamiary działania.

   „Narzędzia walki informacyjnej" tworzą zespoły ludzkie i wszelkiego rodzaju urządzenia techniczne, które są dostosowane do spełniania swej roli w środowisku elektromagnetycznym, akustycznym, elektrycznym, magnetycznym i chemicznym. Urządzenia te wspomagają możliwości recepcyjne, percepcyjne i analityczne człowieka w przestrzeni bezpośrednio dla niego niepoznawalnej, wykraczającej poza jego zmysły.

   „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;

   — obrony informacyjnej.

2. *Prawa walki zbrojnej mają charakter obiektywny i są trwałe. Są też niezależne od woli i świadomości ludzkiej. Dowodzą, że sukces w tej walce może osiągnąć tylko silniejszy. Na tle tego formułowane są zasady*[6] *sztuki wojennej, które już w konkretnych uwarunkowaniach określają zasadnicze sposoby dochodzenia do sukcesu bojowego. Procedury przygotowania i rozgrywania walki zbrojnej, rzutujące na efekt końcowy, determinowane są natomiast względami subiektywnymi. Z tej przyczyny odnotowywane są w historii fakty materialnie nieuzasadnionych klęsk i materialnie nieuzasadnionych wygranych. Analizując fakty gruntowniej, można dostrzec, że konkretne efekty były następstwem sukcesu bądź klęski w prowadzonej wcześniej walce, którą dziś można nazwać „walką informacyjną". Walka informacyjna zawsze towarzyszyła walce*

[6]Zasada to teza, w której treści zawarte jest prawo rządzące jakimiś procesami; podstawa, na której coś się opiera, reguła. *Słownik języka polskiego*, t 3, op. cit., s. 955.

zbrojnej i wywierała istotny wpływ na jej przebieg i wynik, niezależnie od tego, czy formalnie była tak nazywana czy też nie.

3. *Podstawą sukcesu w walce zbrojnej jest zawsze precyzja rażenia i czas reakcji ogniowej. Warunki ku temu stwarza właściwie i pomyślnie przeprowadzona walka informacyjna. Rozpoznanie, zdobywając dane o przeciwniku, wpływa na precyzję rażenia, a zakłócanie informacyjne i obrona informacyjna — na osiąganie wyprzedzenia w użyciu celnego ognia. Wiarygodna i aktualna informacja stanowi podstawę do podjęcia trafnej decyzji oraz osiągnięcia optymalnej mocy bojowej. Moc bojowa danego zgrupowania (jednostki wojskowej) jest wprost proporcjonalna do wielkości potencjału rażenia, możliwości manewrowych wojsk oraz sprawności systemu informacyjno —sterującego. Każdą walkę zbrojną powinna poprzedzać walka informacyjna, bo niemożliwe jest odniesienie zwycięstwa zbrojnego bez wcześniejszego pokonania systemów informacyjno—sterujących przeciwnika.*

Metody i narzędzia badawcze

Krótki czas oraz duże przestrzenie, w których zachodzą procesy walki informacyjnej, wymuszają stosowanie metod i technik zapewniających *sine ira et studio* ich ocenę. Musi też być spełniony warunek umożliwiający selektywny wybór, obserwację i rejestrację poszczególnych elementów obiektu badań.

Szeroki obszar problemowy rozprawy oraz potrzeba przeprowadzenia badań wymagała przyjęcia określonej procedury badawczej, w której budowie kierowano się głównie podejściem systemowym, w którym badany obiekt traktuje się jako system.

System jest pojęciem desygnującym pewną całość tworzoną przez określony zbiór obiektów (elementów) i powiązań (relacji) między nimi, rozpatrywaną z określonego punktu widzenia (aspektu badań)[7]. Innymi słowy, jest to wszelki skoordynowany wewnętrznie i wykazujący określoną strukturę układ elementów; rozpatrywany od zewnątrz jest całością, rozpatrywany od wewnątrz — zbiorem, do którego przynależność warunkuje związki między wszystkimi jego elementami; ogół elementów systemu w tym rozumieniu nazywa się składem, ogół zaś związków (relacji) pomiędzy elementami, które są uwarunkowane przez ich przynależność do systemu, nazywa się strukturą. Przeważnie do tej definicji przyjmuje się dodatkowo dwa aksjomaty:

1) istnieje wzajemne oddziaływanie systemu i środowiska; oznacza to, że system ma

[7]P. Sienkiewicz: *„Podstawy teorii systemów"*, AON, Warszawa 1993, s.16.

wejście i wyjście;

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

Analiza systemowa, rozumiana jako metoda rozwiązywania złożonych problemów naukowych i praktycznych, przewija się w samym formułowaniu zadań, ich rozwiązywaniu, jak również w organizacji procesu badawczego. W metodzie tej w pierwszej kolejności definiuje się badany obiekt, a następnie, uwzględniając relacje systemowe, dokonuje się rozłożenia systemu na podsystemy i podejmuje ich badania.

Za wyborem analizy systemowej przemawiał fakt, że informacja jest nierozerwalnie związana z systemem, praktycznie zaś trzeba uwzględnić co najmniej trzy systemy:

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

— system, w którym informacja obiega, jest gromadzona, przechowywana, przetwarzana;

— system językowy, w którym informacja jest wyrażona (język opisu).

Z powyższego wynika, że badanie informacji „jako takiej", bez wymienionych systemów, byłoby błędem metodologicznym. Przykładowo, żądanie informacji o jakimś obiekcie jest bezsensowne. Rozpoznanie potrzeb informacyjnych użytkownika sprowadza się do zdefiniowania systemu, którego ten użytkownik jest częścią, w jakim funkcjonuje. Pytanie więc użytkownika o to, jakich informacji potrzebuje, nie musi być ani konieczne, ani wystarczające. Ponadto jednym z ważniejszych aspektów jest to, że liczba wiadomości[8] w danym systemie o jakimś innym systemie w skończonym przedziale czasu jest skończona oraz że każda wiadomość zawiera informację tylko w ramach tego systemu. Wiadomość zawierająca bogatą treść w jednym systemie może więc nie zawierać żadnej informacji, gdy znajdzie się w innym systemie.

W wypadku badania procesów informacyjnych zarówno w układzie nerwowym, jak i w sieci telekomunikacyjnej daje się zauważyć daleko idące analogie strukturalne tych zjawisk. To podobieństwo umożliwia zastosowanie do ich badania takiego samego aparatu pojęciowego, języka i sposobu rozumowania. Te elementy stawia do dyspozycji badacza cybernetyka. Świadczy ona usługi w badaniu czynności ludzkiego intelektu, leżących u podstaw procesów heurystycznych wykonywanych przez człowieka podczas rozwiązywania różnego rodzaju zadań. Każdy obiekt (w tym również urządzenie mechaniczne) może być traktowany jako funkcjonujący system sprzężonych i wzajemnie

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

działających elementów, w którym zachodzą różne procesy. Daje to możliwość metodycznego i zorganizowanego badania tych procesów i wnioskowania o stanie systemu. Cybernetyka zajmuje się badaniem zagadnień *sensu latiori* rozumianej komunikacji. Stwarza to możliwości zastosowania jej do badania i opisu procesów informacyjnych. Procesy cybernetyczne niewątpliwie mają jako swą wewnętrzną podstawę procesy termodynamiczne (podlegające drugiej zasadzie termodynamiki), w ramach których istnieje możliwość zmniejszenia entropii, podobnie jak w ramach zjawisk chemicznych istnieje możliwość powstania życia. Proces cybernetyczny realizuje rozpatrzoną wyżej możliwość., a więc jest procesem antyentropijnym, co nie oznacza, że każdy proces antyentropijny jest procesem cybernetycznym. Układ cybernetyczny i przebiegający w nim proces odznacza się specyficznymi osobliwościami makroskopowymi, pozwalającymi wyodrębnić go spośród różnorodności prawidłowych procesów antyentropijnych. Rezultat prawidłowego procesu — gdy jest on już znany — obserwator zewnętrzny zawsze może zinterpretować *post factum* jako cel. W cybernetycznym układzie celowość istnieje jednak niezależnie od interpretacji obserwatora. Można zgodzić się z N. Bernsztejnem, że w charakterystyce procesu biologicznego obok podawania odpowiedzi na pytania: jak? dlaczego? — pojawia się potrzeba podawania odpowiedzi na pytanie: po co? „Po co?" z kolei jest uwarunkowane przyczynowo, tj. nie wyklucza pytania: „dlaczego?". „Po co?" ma wewnętrzne mechanizmy funkcjonowania, tj. nie wyklucza pytania „jak?". Celowość nie wyklucza determinizmu, jest ona jedną z form jego przejawiania się. Pytanie „po co?" jest charakterystyczne nie tylko dla biologicznego, ale i dla dowolnego procesu cybernetycznego. Cybernetykę można rozpatrywać jako racjonalną „teleologię", tj. naukę o celu, zaś ruch cybernetyczny — jako ruch celowy.

Cybernetyka wykazała, że zapewnienie celowego zachowania układów jest możliwe tylko za pośrednictwem procesu operowania informacją. Proces ten obejmuje szereg komponentów elementarnych, zorganizowanych w określonym porządku: a więc proces cybernetyczny odznacza się pewną minimalna strukturą, bez której jest niemożliwy. Układ cybernetyczny zawsze obejmuje dwa podukłady: część sterującą S_1 i część sterowaną S_2. Sterowanie zakłada:

a) obecność w S_1 celu, zakodowanego w taki czy inny sposób. Cel, który kontroluje przebieg procesu, może być immanentny względem układu cybernetycznego, tj. wytworzyć się w procesie samorozwoju danego układu (jak to ma miejsce w układach

biologicznych) bądź też może znajdować się na zewnątrz (jak to ma miejsce w układach technicznych);

b) zdolność S_2 do zmieniania ściśle lub w sposób przybliżony „odległości" S_2 od celu;

c) wypracowanie takich oddziaływań na S_2, które zmniejszają tę „odległość".

W bardziej rozwiniętej formie sterowanie jakimś obiektem obejmuje następujące funkcje, których realizacja przeplatać się będzie w czasie:

a) wstępne uzyskanie i nagromadzenie informacji o sterowanym układzie, a także o jego funkcjonowaniu w obecności lub braku oddziaływań zewnętrznych;

b) opracowanie na podstawie przetworzenia tej informacji strategii osiągania celu, tj. ukazanie możliwych linii zachowania oraz porównanie i wybór wariantów;

c) realizowanie wybranej strategii, tj. nieprzerwane zbieranie informacji o sterowanym obiekcie, jej konfrontacja z dotychczasową rolą zmiennych, wypracowanie i przekazanie danemu obiektowi oddziaływań sterujących.

Cybernetyka zajmuje się ilościową stroną informacji, co pozwala sprecyzować w ogólnym znaczeniu samo pojęcie informacji oraz logikę przetwarzania informacji. Cybernetyczne podejście do logiki wymaga koniecznie włączenia do niej nie tylko algorytmów świadomego przetwarzania informacji przez myślenie, ale także algorytmów i heurystycznego przetwarzania informacji na poziomie poznania zmysłowego, w toku przechodzenia od obrazów zmysłowych do abstrakcyjnych przedstawień, podczas intuicyjnego poszukiwania rozwiązania problemów itd.

Sub specie cybernetyki, proces informacyjny nie jest możliwy poza układami materialnymi i bez określonych przemian energetycznych. Informacja wymaga obecności nośnika materialnego i materialnego charakteru przekazu. Informacja zawsze wymaga obecności różniących się od siebie wzajemnie obiektów fizycznych, czy będą to lampy elektronowe, przekaźniki elektromechaniczne, czy też rozmaite litery alfabetu. Proces cybernetyczny jest związany z określonym rodzajem materii, z określoną klasą tworów materialnych.

Cybernetyka formułuje swoje prawa przeważnie w formie matematycznej. Wykrywa ona ilościowe związki i podaje ścisły opis struktur realizujących określone funkcje. Są to struktury, o których mówią: teoria informacji, teoria automatów, gier, oraz struktur algorytmicznych i in. Wiele z owych struktur w formie aparatu matematycznego stosuje się i poza analizą procesów sterowania. Zastosowanie matematyki łączy się ściśle z ogólną naturą poznania teoretycznego oraz procesem wzrostu znaczenia metod teoretycznych w nauce. Stosowanie koncepcji i metod matematycznych do badania

rozmaitych procesów nie oznacza przy tym po prostu stosowania nowych, bardziej „dokładnych" metod badawczych, jest ono narzędziem pomagającym odkrywać ukryte cechy i całościową strukturę badanych obiektów. Dostarcza w ten sposób podstawy dla szerokiej syntezy różnych dziedzin wiedzy niewiele dotychczas mających ze sobą wspólnego.

Wykorzystanie matematyki do badania określonej dziedziny zjawisk oznacza przede wszystkim opracowanie odpowiedniej teorii naukowej będącej podstawową formą, w której zostaje wyrażona nasza wiedza o przedmiocie badań.

Problemy badawcze rozprawy dotyczyły różnych kwestii merytorycznych oraz metodologicznych. Stąd wynikała potrzeba zastosowania różnych metod badawczych odpowiadających charakterowi rozwiązywanych problemów.

Podczas weryfikacji poszczególnych hipotez zastosowano następujące metody i narzędzia badawcze:

Hipotezę roboczą nr 1 zweryfikowano za pomocą: definiowania, indukcji, dedukcji, analogii, analizy (matematycznej, przyczynowej, strukturalnej i systemowej), porównania i uogólnienia. Pozwoliło to na dokonanie teoretycznej konfrontacji dotychczasowych określeń „walki informacyjnej", „informacji" oraz pojęć pochodnych, wyjaśnienie występujących kontrowersji, a następnie sprecyzowanie definicji walki informacyjnej i jej desygnatów w celu określenia jednoznaczności i ścisłości języka problemu. Ponadto umożliwiło dokonanie teoretycznego podziału przestrzeni walki informacyjnej na podprzestrzeń: zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej. Wykorzystano przy tym następujące materiały: rozprawy naukowe i opracowania studyjne, publikacje specjalistyczne, opracowania zagraniczne, obliczenia probabilistyczne i wyniki analizy matematycznej oraz macierze przedstawiające działania informacyjne strony A i B.

Hipotezę roboczą nr 2 zweryfikowano na podstawie analizy historycznej i uogólnienia. Po dokonaniu analizy faktów historycznych (bitew i wojen), począwszy od starożytności, wyszczególniono przedsięwzięcia, które przyczyniały się do odniesienia zwycięstw lub poniesienia porażki w prowadzonych działaniach wojennych. Na zasadzie powtarzalności (prawidłowości) tych zjawisk sprecyzowano, jaki miały one wpływ na rezultat prowadzonej walki, co w efekcie umożliwiło sformułowanie ogólnych reguł prowadzenia walki informacyjnej.

Hipotezę roboczą nr 3 zweryfikowano na zasadzie analizy przyczynowej, logicznej i matematycznej. Celem walki zbrojnej jest pokonanie przeciwnika. Na osiągnięcie tego celu główny wpływ wywierają trzy czynniki: ruch, rażenie i informacja. Po dokonaniu analizy powyższych czynników udało się określić zależności występujące między nimi oraz który z nich wywiera najistotniejszy wpływ. Przydatne w tym zakresie były obliczenia matematyczne.

Ponadto w całym procesie badawczym wykorzystano wyniki obserwacji naukowej (bezpośredniej), prowadzonej w czasie ćwiczeń dowódczo — sztabowych i z wojskami w Pomorskim Okręgu Wojskowym oraz w siłach pokojowych ONZ.

W dysertacji przyjęto trzyetapową procedurę badań (tabela 1).

Tabela 1

Realizacja przedsięwzięć badawczych i uzyskane rezultaty badań[9]

PRZEDSIĘWZIĘCIA BADAWCZE		REZULTAT BADAŃ
ETAP WSTĘPNY BADAŃ	1. Uświadomienie sytuacji problemowej 2. Analiza literatury przedmiotu badań 3. Ocena stanu teorii walki informacyjnej 4. Organizacja badań	1. Cel badań 2. Problemy badawcze 3. Hipotezy robocze 4. Metody badawcze
ETAP BADAŃ WŁAŚCIWYCH	1. Definiowanie pojęcia walki informacyjnej i pojęć pochodnych 2. Analiza informacji w aspekcie walki informacyjnej 3. Analiza elementów struktury walki informacyjnej 4. Analiza historyczna doświadczeń wojennych z zakresu walki informacyjnej 5. Analiza wpływu walki informacyjnej na skuteczność prowadzenia walki zbrojnej	1. Zdefiniowanie pojęcia walki informacyjnej i pojęć pochodnych 2. Ustalenie cech informacji 3. Określenie przedmiotu, narzędzi i przestrzeni walki informacyjnej 4. Określenie genezy walki informacyjnej 5. Ustalenie wpływu walki informacyjnej na walkę zbrojną
ETAP KOŃCOWY BADAŃ	1. Weryfikacja wyników badań przez: — konsultacje naukowe; — seminaria, konferencje naukowe. 2. Zastosowanie wyników badań	1. Zestawienie wyników badań 2. Publikacje: — artykuły; — wydawnictwa dydaktyczne. 3. **Rozprawa doktorska**

[9] Opracowanie własne. Pozostałe rysunki i tabele bez indeksów należy traktować jako autorskie.

„Informacja stanie się czynnikiem kluczowym na przyszłym polu walki. Informacja jest już dziś oraz będzie w przyszłości tym, czym był karabin maszynowy w pierwszej i czołg w drugiej wojnie światowej[10].

1. POJĘCIA, PRZEDMIOT, NARZĘDZIA I PRZESTRZENIE WALKI INFORMACYJNEJ

Możliwość istnienia walki informacyjnej jest kwestionowana przez wielu teoretyków tego problemu. Najwięcej kontrowersji wzbudzają jej dwa aspekty:

— po pierwsze — jeżeli nie można zdefiniować pojęcia walki informacyjnej, to nie może ona istnieć.

— po drugie — jeżeli walka informacyjna jest wszystkim, wtedy jest niczym[11].

Druga wątpliwość może być odrzucona *in promptu* na zasadzie analogii: np. jeżeli życie jest wszystkim wtedy jest niczym, z czym w żadnym wypadku nie można się zgodzić. Należy przyjąć, że jest ono wszechstronne i rozległe w swoich wymiarach, aby je zrozumieć, powinno się uwzględnić jego zbiory, podzbiory i mikrozbiory. Zastosowanie zasad kategoryzacji[12] jest tu niezbędne. Życie dzieli się na świat roślinny i zwierzęcy. Każdy z tych światów dzieli się na typy, gromady, rzędy, rodziny, rodzaje i gatunki. Gatunki reprezentowane przez populacje osobników są podstawowymi jednostkami systematycznymi, rzeczywiście istniejącymi w przyrodzie. Wszystkie pozostałe jednostki systematyczne, od rodzaju do królestwa, są jednostkami sztucznymi, które wymyślone zostały przez człowieka, aby ułatwić mu orientację. Do pełnego zrozumienia czym jest życie, nie wystarczy poznanie samych właściwości osobniczych danego gatunku. Konieczne jest poznanie wyższych poziomów organizacji życia — zależności, związków i zachowań — między osobnikami żyjącymi w zgrupowaniach tego samego gatunku, między populacjami różnych gatunków, jak również między populacjami a ich środowiskiem. Niezbędne jest także poznanie praw rządzących przebiegiem trwającej nadal ewolucji.

---

[10] Tezę tę postawił adm. Wiliam Owens – zastępca przewodniczącego Kolegium Połączonych Szefów Sztabów SZ USA.

[11] Winn Schwartau: *„Information Warfare-Cyberterrorism: Protecting Your Personal Security in the Electronic Age"*, 1993, s.9.

[12] Kategoria – to rodzaj lub klasa wyróżnione w jakiejś klasyfikacji, typ, rodzaj, grupa;
- w znaczeniu tradycyjnym (wg Arystotelesa) – najogólniejsze pojęcia, klasy, działy orzeczeń, najważniejsze rodzaje (np. substancje, wielkości, jakości, relacje, miejsca, czasy, stany rzeczy);
- wg J. Kanta – „czyste" pojęcia zespalające w przedmioty poszczególne wyobrażenia (przestrzeń, czas).

T. Kotarbiński: *„Elementy teorii poznania, logiki formalnej i metodologii nauk"*. Wrocław – Warszawa – Kraków 1991, s. 67 – 77. *Encyklopedia powszechna PWN*, t 2, Warszawa 1987, s.443.

In puncto pierwszej wątpliwości, zarówno pojęcie życia jak i walki informacyjnej można zdefiniować. Definicję życia w aspekcie metabolicznym podaje fizyk Schroedinger. Według niego życie jest przeciwstawieniem się przyrody drugiemu prawu termodynamiki, tj. dążności materii do bezwładnego ruchu cząsteczek, czyli entropii. Podobnie procesy cybernetyczne opierające się na informacji, mają jako swą wewnętrzną podstawę drugą zasadę termodynamiki, zgodnie z którą entropia skończonego izolowanego układu dąży do maksimum. Jak wykazał L. Boltzman, entropia układu pozostającego w pewnym stanie jest proporcjonalna do logarytmu z prawdopodobieństwa zaistnienia tego stanu. Takie podejście pozwoliło następnie teorii informacji i tworzącej się teorii układów uogólnić pojęcie entropii. Entropię traktuje się jako miarę przybliżenia układu do najbardziej prawdopodobnego, chaotycznego stanu; odpowiednio negentropię traktuje się jako miarę odchylenia od stanu chaotycznego, jako miarę zorganizowania układu. Procesy cybernetyczne to przede wszystkim procesy sterowania. Sterowanie jest przeciwstawne wobec dezorganizacji i na pierwszy rzut oka wydaje się, że samo istnienie procesu cybernetycznego sprzeciwia się prawom termodynamiki, że cybernetyczne i termodynamiczne procesy absolutnie wykluczają się nawzajem. W rzeczywistości tak nie jest. Boltzman nadał drugiej zasadzie termodynamiki interpretację statystyczną: zmniejszenie entropii w takim czy innym układzie nie jest niemożliwe, jest ono tylko mało prawdopodobne. Bez względu na to, jak małe byłoby to prawdopodobieństwo, jest ono skończone, a więc obniżenie entropii jest możliwe. Termodynamika wcale nie neguje w sposób kategoryczny zmniejszenia entropii. W ramach procesu termodynamicznego istnieje możliwość zmniejszenia entropii, podobnie jak w ramach zjawisk chemicznych istnieje możliwość powstania życia. Proces cybernetyczny realizuje rozpatrzoną wyżej możliwość.

Z powyższych konkluzji wynika, że walkę informacyjną da się porównać do życia — podobnie jak ono może być również definiowana. Dalsze dywagacje wymagają jednak wyjaśniania pojęcia „walka informacyjna", które coraz częściej używane, nie zostało dotychczas zdefiniowane w klasyfikacji naukowej.

1.1. Desygnat pojęcia „walka informacyjna" i zasady w tworzeniu pojęć pochodnych

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 tego złożonego pojęcia 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"[13].

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. Przy kooperacji negatywnej wzajemnej nie tylko „B" przeszkadza „A", lecz i odwrotnie".[14] 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:

---

[13]T. Kotarbiński: *Traktat o dobrej robocie,* Wrocław 1982, s.221.
[14]*Mały słownik cybernetyczny,* op. cit., s.195.

— 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.

Wniosek z podrozdziału 1.1.

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[15]. 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 z przenoszeniem i przetwarzaniem informacji w procesach fizycznych. Jest to obiekt abstrakcyjny, 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);

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

— przetwarzany i użyty do sterowania (np. komputerem steruje program będący zakodowaną informacją).[16]

Stanisław Koziej określa informację jako niematerialny czynnik zespalający pozostałe elementarne czynniki walki zbrojnej (ruch, rażenie) w zharmonizowaną całość starcia zbrojnego.[17]

Informacjami mogą być: obrazy optyczne, dźwięki, słowa, liczby, wskazania przyrządu pomiarowego itp. Źródłem informacji jest podający je obiekt: mówiący człowiek, przyrząd pomiarowy itp. W tym aspekcie wyróżniane są źródła:

— binarne, podające jeden z dwóch możliwych stanów, np. element logiczny o 2 wyróżnionych stanach: „tak" i „nie";

— ziarniste (dyskretne), podające jedną spośród skończonej liczby wiadomości, np. źródło podające litery;

— ciągłe, podające wiadomości różniące się między sobą dowolnie mało, np. termometr rtęciowy, obiektyw optyczny.

W cybernetyce informacja stanowi jedno z podstawowych pojęć, którego desygnat jest nie w pełni definiowalny z uwagi na jego pierwotny i elementarny charakter[18]. 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".

---

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

- ✓ 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".

> *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[19] stanów wyróżnionych układu będącego nadawcą[20] 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.

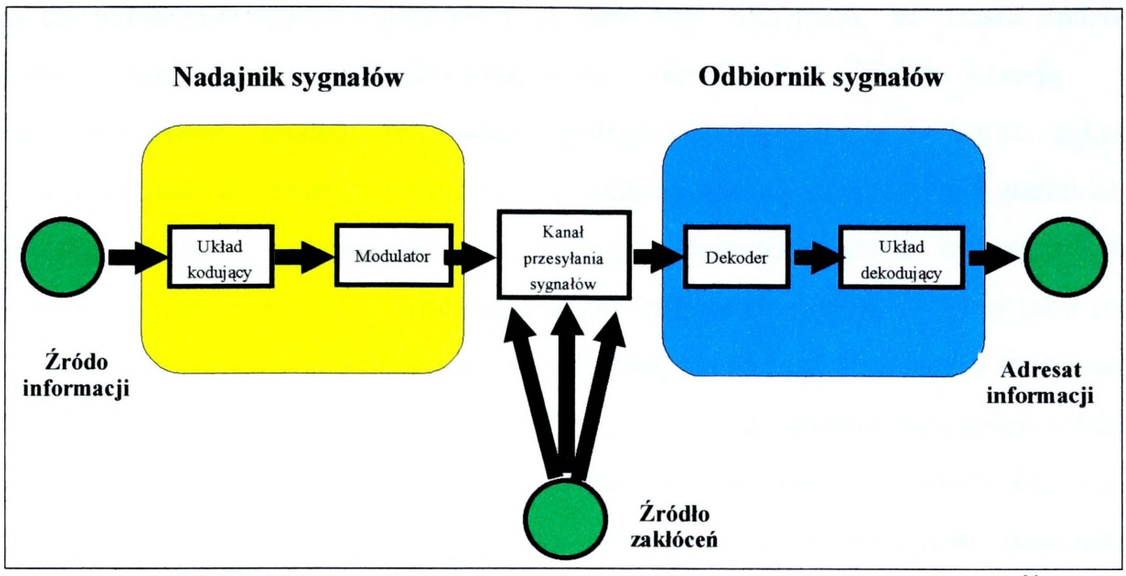
Podsumowując należy stwierdzić, że w cybernetyce pojęcie informacji nie zostało określone w sposób zadowalający. Wprawdzie N. Wiener wyraźnie wskazał, że nie należy utożsamiać informacji ani z masą, ani z energią, nie określił jednak dokładnie, czym jest informacja.

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:

---

[19]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.

[20]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.



Rys. 1.2.1. Model przesyłania wiadomości analizowany przez C.E. Shannona[21]

— źródła informacji;

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

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

— 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 ilość informacji, 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

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

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 prowadzącej do znalezienia pożądanej odpowiedzi na postawione pytanie metodą przyjmowania stanów systemu o największym prawdopodobieństwie. Informację można przechowywać i przekazywać. Ilość otrzymanej informacji można określić jako różnicę między ilością informacji posiadanej przez odbiorcę przed i po otrzymaniu komunikatu[22]. Szybkość, z jaką informacja jest przekazywana, zależy od kanałów łączności, a także od tak zwanych szumów, powstających w trakcie przekazywania wiadomości. Shannon uwzględnił również związki między sygnałami[23], tzn. właściwości zbioru komunikatów. Jeżeli wszystkie sygnały są pod względem statystycznym podobne, to obserwacje poczynione na przykładzie jednego z nich można ekstrapolować na cały zbiór sygnałów.

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 informacji 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 ilości informacji nie ujmuje ani sensu, ani wartości wiadomości, ani wariancji zdarzeń. Informację rozpatruje się tylko w aspekcie syntaktycznym[24], nie można na podstawie ilości informacji orzec, czy jest to informacja prawdziwa, czy wprowadzająca w błąd. Dlatego też należałoby łączyć teorię ilościową (aspekt syntaktyczny) z teorią wartościową (aspekt semantyczny)[25]. Pozwoliłoby to wyeliminować informację nieprawdziwą. 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

---

[22]Komunikat" to pewna porcja informacji przekazana adresatowi (do układu odbierającego) w „czystej" formie. „Dane" – informacje potencjalne, które dopiero po odpowiednim opracowaniu (przy wykorzystaniu odpowiedniego klucza) mogą stać się informacjami przydatnymi w działaniu celowym. *Mały słownik cybernetyczny*, op. cit., s. 74.

[23]„Sygnał" – stan lub proces fizyczny będący nośnikiem informacji.

[24]Przez aspekt syntaktyczny informacji należy rozumieć relacje pomiędzy sygnałami niosącymi wiadomość, w której zawarta jest informacja, oraz pomiędzy sygnałami a kanałem komunikacyjnym.

[25]Aspekt semantyczny obejmuje relacje pomiędzy sygnałem a niesioną przez niego wiadomością.

propozycji Shannona.

W dyskusjach nad sposobem rozumienia „informacji" celowe jest rozróżnienie pomiędzy aspektem syntaktycznym, semantycznym i pragmatycznym[26].

Próbę rozwinięcia aspektu semantycznego informacji podjął M. Mazur[27], 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. M. Mazur wyróżnia trzy rodzaje dotychczasowego traktowania terminu informacji w publikacjach:

— publikacje, których autorzy stosują termin informacja jako określenie całkowicie potoczne bez prób jego wyjaśnienia;
— publikacje, których autorzy rozumieją przez ten termin ilość informacji;
— publikacje, których autorzy starają się wyjaśnić pojęcie informacji przez inne równie nieokreślone terminy takie, jak treść, wiadomość itp.

M. Mazur sugeruje więc, że brak jest wciąż czwartego rodzaju publikacji, który by dostatecznie obiektywnie wyjaśniał to zjawisko. W publikacjach *in status quo* przede wszystkim i prawie wyłącznie rozpatrywano informację w aspekcie jej przekazywania w łączności, systemie komunikacji. Stąd zwracano uwagę na zagadnienia relacji między źródłem — nadajnikiem i odbiornikiem informacji oraz na zagadnienia kwantyfikowanego ujęcia: ilość informacji, określoność, złożoność prawdopodobieństwo.

Wychodząc z analizy systemów łączności, próbowano wyjaśnić pojęcie informacji, wyróżniając trzy stopnie: sygnał, wiadomość oraz informację. 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 informacji, analizując elementy układu sterowania. Wszystko co bywa nazywane informacją zawsze powstaje w sytuacjach, w których dąży się do jakiegoś celu, a więc w sytuacjach

[26]Aspekt pragmatyczny informacji dotyczy z kolei relacji pomiędzy niesioną przez sygnał wiadomością a jej nadawcą lub odbiorcą.
[27]M. Mazur M: *„Jakościowa teoria informacji"*, Warszawa 1970, s. 47.

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*[28]*. 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 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.

Niezmiernie trudno jest podać adekwatne określenie informacji. Niezależnie jednak 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 w związku z sytuacją

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

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 informacji pragmatycznej przedstawił K. Szaniawski, definiując wartość informacji ze względu na problem decyzji. Autor ten rozumie wykorzystywanie informacji 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[29]. Z uwagi na swój ogólny charakter propozycja K. Szaniawskiego może stanowić model dla interpretacji pragmatycznej wartości informacji w każdej sytuacji decyzyjnej.

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.

Jeżeli pomiędzy zbiorem sygnałów emitowanych ze źródła $X = \{x_1, \ldots, x_m\}$ a zbiorem możliwych stanów źródła $H = \{h_1, \ldots, h_n\}$ zachodzi relacja wzajemnie jednoznaczna, to każdemu sygnałowi przyporządkowany jest wówczas dokładnie jeden stan źródła i odwrotnie. Zależność tę można więc określić jako prawo deterministyczne.

---

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

Przy takiej zależności prawdopodobieństwo warunkowe emisji określonego sygnału przy danym stanie źródła równe jest jedności bądź zeru:

1) $p(x_i/h_j) = 1$;

2) $p(x_i/h_j) = 0$.

W pierwszym wypadku sygnał x_i będzie emitowany zawsze i tylko wtedy, gdy źródło przyjmie stan h_j. Gdy przyjmie się $z(h_j)$ jako funkcję zdania stwierdzającego, iż zachodzi stan h_j, oraz $z(h_i)$ jako funkcję zdania orzekającego emisji sygnału x_i, schematy funkcjonowania systemu kodującego mają postać reguł wnioskowania:

1. $z(h_j) \Leftrightarrow z(x_i)$

2. $z(h_j)$

więc: $z(x_i)$

Ponieważ reguły te są schematami wnioskowania niezawodnego, dlatego też informację o stanie źródła uzyskaną na drodze transformacji sygnałów w systemie dekodującym należy określić jako niezawodną.

Jeżeli prawdopodobieństwo warunkowe emisji sygnałów przy danym stanie źródła spełnia nierówność: $0 < p(x_i/h_j) < 1$, to pomiędzy stanem źródła a emisją sygnału jest jedynie związek probablistyczny. Dla danego zbioru sygnałów $X = \{x_1, ..., x_m\}$ oraz stanów źródła $H = \{h_1, ..., h_n\}$ rozkład prawdopodobieństw warunkowych emitowanych sygnałów przy określonych stanach źródła przedstawia macierz rozkładu (mac. 1.2.1), w której suma

X \ H	h_1	h_2	...	h_n
x_1	$p(x_1/h_1)$	$P(x_1/h_2)$	...	$p(x_1/h_n)$
x_2	$p(x_2/h_1)$	$p(x_2/h_2)$	...	$p(x_2/h_n)$
. . .	. . .	. . .	. ... .	. . .
x_m	$p(x_m/h_1)$	$p(x_m/h_2)$	...	$p(x_m/h_n)$

Mac. 1.2.1. Rozkład prawdopodobieństw warunkowych emitowanych sygnałów przy określonych stanach źródła[30]

[30] Opracowano na podstawie książki A. Bieli: *„Informacja a decyzja"*, PWN, Warszawa 1976.

prawdopodobieństw w każdej kolumnie równa jest jedności. Po uzyskaniu sygnału x_i decydent nie może z całkowitą pewnością określić, jaki jest aktualny stan rzeczy. Przetwarzanie sygnału x_i na informację o zbiorze H może być oparte jedynie na regułach wnioskowania probablistycznego. Powszechnie znanym schematem tego wnioskowania jest reguła Bayesa, pozwalająca na ustalenie rozkładu *a posteriori* prawdopodobieństw na zbiorze H po uzyskanym sygnale x_i. Ponieważ model Bayesa stanowi podstawę wnioskowania probablistycznego, decydent może na jego podstawie przetwarzać sygnały jedynie na informację zawodną.

> *Na tle przedstawionych poglądów można przyjąć wniosek, że zjawisko informacji należy rozpatrywać w sposób możliwie syntetyczny uwzględniając jego różne aspekty. Należy uwzględnić zarówno ujęcie materialistycznej teorii odzwierciedlenia, jak i uogólnienie cybernetyki z ilościowym ujęciem oraz powiązania go z ujęciem semiotycznym i pragmatycznym (które rozpatrują znaczenie i cenność informacji).*

Wnioski z podrozdziału 1.2.

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 charakter informacji — 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.*

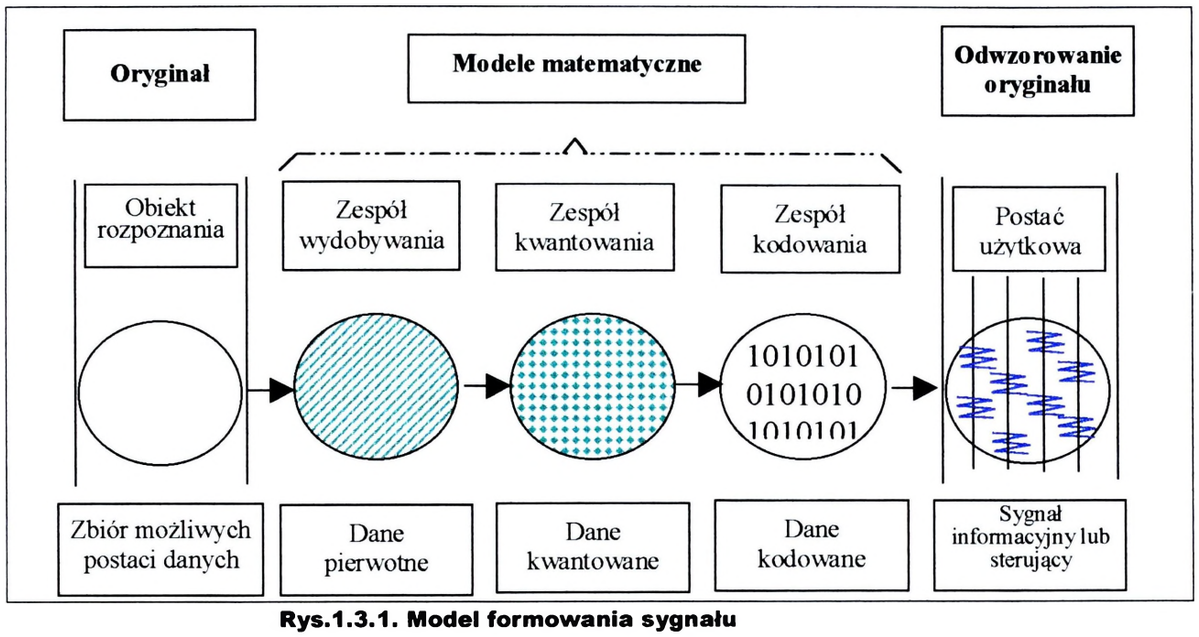
Na przykład w telekomunikacji zarejestrowanie parametrów modulacji sygnału nośnego nie spowoduje, że jego odbiorca będzie wiedział, jakie treści logiczne niesie ta informacja. Dowie się o tym dopiero wówczas kiedy zarejestrowane parametry modulacji zostaną skonfrontowane z regułą modulacji w układzie przetwarzającym, to znaczy z uzależnieniem stanów sygnału nośnego od sygnału modulującego, który niesie w sobie informację logiczną dla odbiorcy. Takie informacje są 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. Spotkać się też można z podziałem na informację w ogóle i informację, którą człowiek, organizm żywy lub automat stara się dostarczyć, w sposób świadomy lub zaprogramowany, innemu człowiekowi, organizmowi żywemu czy też automatowi. O takiej informacji mówi się, 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 informacji i zależą od innych czynników. Tylko w skrajnych wypadkach, gdy sygnał w całej rozciągłości zależy od informacji, można utożsamiać go z informacją. 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[31]. 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)

[31]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.

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

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.

Na przykład:

Jeśli dyskretna zmienna losowa X_d charakteryzować się będzie ciągiem rozkładów:

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

dla:

$$i = 1; 2; 3; 4$$

gdzie:

$$p_1(x_1) = 0{,}25; \quad p_2(x_2) = 0{,}5; \quad p_3(x_3) = 0{,}125; \quad p_4(x_4) = 0{,}125.$$

Wówczas średnia ilość informacji przypadająca na każdy komunikat niosący wiadomość o dowolnym zdarzeniu należącym do zbioru dyskretnej zmiennej losowej X_d wynosić będzie:

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

$$= -(0{,}25\log_2 0{,}25 + 0{,}5\log_2 0{,}5 + 0{,}125\log_2 0{,}125 + 0{,}125\log_2 0{,}125) = 1{,}75 bita$$

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:

$$k_r = \frac{I_r}{I}$$

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:

$$k_k = \frac{I_r}{I_0},$$

przy czym $I_0 \geq I_r$.

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:

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

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:

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

Za informację niewiarygodną uznajemy zatem taką, dla której:

$$\delta > \delta_0 \quad \text{lub} \quad k_w < 0.$$

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

$$\mathbf{V} = [k_a, k_r, k_k, k_p, k_w]$$

*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**.*

Wnioski z podrozdziału 1.3.

W procesie walki informacyjnej należy uwzględniać, iż:

- *Użytkowymi postaciami informacji są różnego rodzaju sygnały informacyjne i sygnały sterujące.*
- *Sygnały informacyjne i sterujące są 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 informacji odbywa się w systemie informacyjno-sterującym, którego strukturę tworzą:*

— *źródła informacji;*
— *przetworniki informacji;*
— *układy odbierające;*
— *nośniki informacji;*
— *relacje systemowe.*

- *Informacja jest niezniszczalna i zawsze prawdziwa (brak jakiejkolwiek informacji jest również informacją). Nie oznacza to jednak, 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

Struktura to rozmieszczenie elementów składowych i zespół relacji między tymi elementami, charakterystyczny dla danego układu[32]. Zdaniem Umberto Eco, struktura to model zbudowany za pomocą określonych działań upraszczających, które pozwalają utożsamiać różne zjawiska ze wspólnego punktu widzenia[33]. Innymi słowy, struktura to całość, części tej całości oraz stosunki pomiędzy tymi częściami. Struktura jest modelem jako system zróżnicowań. Cechą charakterystyczną tego modelu jest możliwość przenoszenia go z fenomenu na fenomen oraz z zespołu fenomenów na inny zespół fenomenów. Metodologia strukturalna ma sens tylko przy spełnieniu powyższych

[32]Leksykon techniczny, Wydawnictwa Naukowo - Techniczne, Warszawa 1983, s. 528.
[33]Umberto E.: *„Nieobecna struktura"*, Milano 1991, s. 259.

postulatów.

Ojcem refleksji strukturalnej był już Arystoteles[34], który opisując strukturę zastosował trzy terminy: *morfe*, *eidos* i *ousia*.

Zdaniem jego *morfe* to fizyczna forma zewnętrzna przedmiotu. *Eidos* składa się wraz z materią na substancję, ale nie znajduje się na zewnątrz *ousia*, jest jej aktem. Jest do tego stopnia związany z przedmiotem, któremu daje życie, że nie staje się, nie rodzi się. Jest tylko z i w substancji. *Eidos* współuczestniczy w powołaniu do życia *ousia*. Jeśli eidos to racjonalna i podlegająca racjonalizacji struktura szczegółowej substancji, to rzecz powinna opierać się nie na niej samej, lecz na systemie relacji. Ale u Arystotelesa trudno jest zdefiniować *eidos* z pominięciem materii, której jest aktem, a więc z pominięciem *ousia*, w której się ucieleśnia.

> *Z powyższego można wnioskować, że u Arystotelesa występuje wyraźne wahanie pomiędzy modelem strukturalnym a ustrukturowanym przedmiotem, jego rozwiązanie odgrywa determinującą rolę przy poprawnym zdefiniowaniu metodologii strukturalistycznej. Mają tu miejsce dwie oscylacje:*
> — *jedna pomiędzy aspektem ontologicznym i epistemologicznym eidos (czy eidos jest czymś „danym", czy „ustanowionym", czy można go odnaleźć w rzeczy, zastosować do rzeczy, by uczynić ją poznawalną?);*
> — *druga pomiędzy aspektem konkretnym a aspektem abstrakcyjnym, pomiędzy przedmiotem a modelem przedmiotu, pomiędzy indywidualnym i uniwersalnym.*

Niektórzy autorzy, jak np. P. Bridgman, określają strukturę (zgodnie z zasadami lingwistyki) jako „procedurę operacyjną" — sposób na sprowadzenie do jednorodnego dyskursu żywego doświadczenia różnokształtnych przedmiotów, a więc coś w rodzaju prawdy logicznej, rozumowej, a nie faktycznej. W tym wypadku należy rozpatrywać pojęcie struktury w klimacie metodologii operacjonistycznej; nie implikuje ono żadnego twierdzenia ontologicznego. Druga oscylacja, zauważona w arystotelesowskiej dyskusji o ustrukturowanej substancji pomiędzy biegunem ontologicznym a epistemologicznym, wygasa na korzyść drugiego z nich.

> *Badacz korzystający w swej pracy z modeli powinien więc uważać podobnie jak Bridgman, że model jest pożytecznym i niezastąpionym narzędziem umysłu — pozwala myśleć o rzeczach niezwykłych w kategoriach odnoszących się do rzeczy zwykłych.*

Tego typu badania oparte są na hipotezie, przedmiot opisu jest pojmowany jako struktura (a więc analizowany według metody strukturalnej, pozwalającej na rozpoznanie stosunków między konstytuującymi go częściami) lub część struktury (a więc syntetyzowany

[34]Por. Arystoteles: *„Fizyka i Metafizyka"*, Torino 1956.

z innymi przedmiotami, z którymi wchodzi w relacje, które umożliwiają rozpoznanie i określenie rozleglejszego przedmiotu, którego te przedmioty są częściami).

> *Wynika z tego, że przyjęcie metody strukturalnej nie jest narzucone przez przedmiot dociekań, lecz wynika z arbitralnego wyboru badacza.*

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:

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

gdzie:

$\Re$ — relacja

I — informacja;

Z_i — źródło informacji;

N_i — nośnik informacji;

U_o — układ odbierający.

Z powyższego wynika, że na informacje 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:

	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

Mac. 1.4.1. Funkcjonalne powiązania walki informacyjnej

— 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";

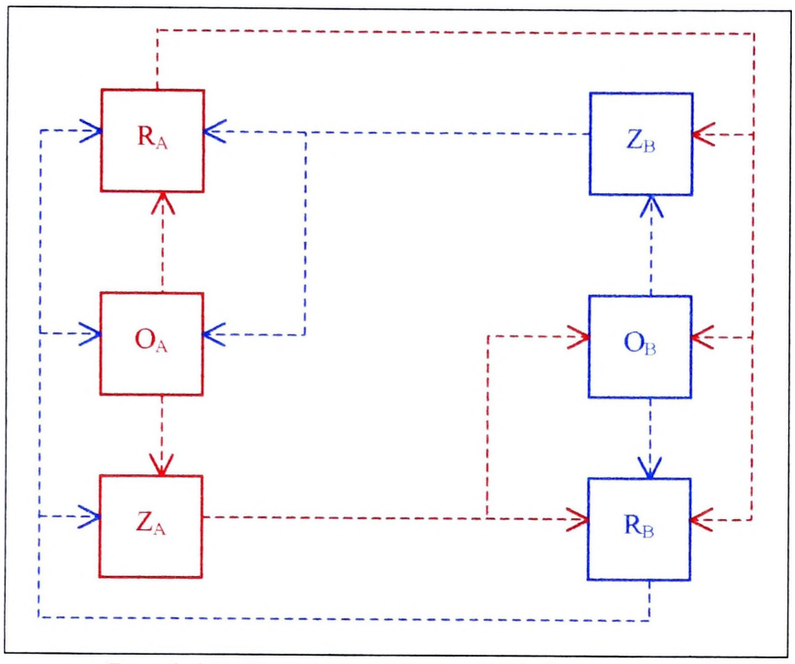
— O_A — podukład obrony informacyjnej strony „A";

— 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

Wnioski z podrozdziału 1.4.

- *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

Zgodnie z *communis opinio* pojęcie „przestrzeń" używane jest najczęściej w rozumieniu trójwymiarowej rozciągłości, nieokreślonej i nieograniczonej, w której zachodzą wszelkie zjawiska fizyczne. Używane jest również jako interpretacja rozciągłości objętej jakimiś granicami, a także w rozumieniu pewnego obszaru, powierzchni i odległości. Nieograniczony stopień ogólności i fundamentalność faktu trójwymiarowości przestrzeni zawsze zwracały uwagę filozofów, dla których możliwość lokalizacji przedmiotów w przestrzeni trójwymiarowej stanowiła jakże często kryterium ich materialności[35], podczas gdy sama trójwymiarowość była w istocie rzeczy nie wyjaśniona. Trójwymiarowość przestrzeni przyjmowano jako oczywisty aksjomat podczas tworzenia licznych teorii fizycznych, sam jednak aksjomat wymykał się wszelkim próbom uzasadnienia. *Sine ira et studio* tego typu ujęcie problemu nie może być uznane za poprawne.

Według I. Kanta, przestrzeń i czas są formami istnienia materii w zastosowaniu do danego przypadku, co oznacza, że trójwymiarowość przestrzeni fizycznej powinna być wyjaśniona poprzez zjawiska materialne i ich wzajemne oddziaływanie. Doniosłość takiego ujęcia przestrzeni polegała nie tylko na zawartej w nim hipotezie o pochodzeniu trójwymiarowości przestrzeni (ze współczesnego punktu widzenia niedostatecznie przekonująca), ale również na ogólnofizycznym ujęciu zagadnienia wtórności takiej fundamentalnej własności przestrzeni, jak jej wymiar w stosunku do podstawowych sił przyrody.

Ad vocem przestrzeni należałoby się zastanowić nad jej wymiarem, co będzie wymagało ścisłego, matematycznego wyjaśnienia. Pojęcie wymiaru przestrzeni ulegało ciągłej ewolucji, co doprowadziło wreszcie do współczesnego, topologicznego pojęcia wymiaru. Jest on jedną z takich właściwości, które są zachowane dla dowolnych

[35]R. Descartes: *„Zasady filozofii"*, Warszawa 1960, s.57

wzajemnie jednoznacznych i ciągłych homemograficznych przekształceń lub, inaczej, dla takich przekształceń, dla których każdemu punktowi jednego obiektu odpowiada tylko jeden punkt drugiego obiektu, a nieskończenie bliskim punktom jednego obiektu odpowiadają nieskończenie bliskie punkty drugiego. Współczesna definicja wymiaru, która jest rozwinięciem definicji Poincar`ego, została podana przez Ursynowa i Mengera, którzy twierdzą, że:

— zbiór pusty posiada wymiar —1;

— wymiar przestrzeni X jest najmniejszą całkowitą liczbą n taką, że każdy punkt $p \in X$ posiada dowolnie małe otoczenie, którego ograniczenie ma wymiar mniejszy niż n.

W topologii dowodzi się twierdzenia, że n — wymiarowa w sensie intuicyjnym przestrzeń euklidesowa posiada rzeczywiście wymiar n. Wynika z tego, że linia ma wymiar 1, powierzchnia euklidesowa — 2, a przestrzeń — 3. A więc trójwymiarowość przestrzeni jest niewątpliwie faktem fizycznym. Jako jego doświadczalne potwierdzenie przytacza się fakt posiadania objętości przez ciała przyrody, możliwość przeprowadzenia w każdym punkcie przestrzeni nie więcej niż trzech wzajemnie prostopadłych prostych, możliwość opisania dowolnego punktu przestrzeni przez trzy niezależne parametry; wreszcie możliwość osiągnięcia dowolnego punktu przestrzenie poprzez trzy prostopadłe przesunięcia. Ponadto w przestrzeni naszej można zbudować modele materialne jedynie takich obiektów geometrycznych, które należą do trójwymiarowej przestrzeni matematycznej.

> *Jeśli porównamy przestrzeń matematyczną (topologiczną) z rzeczywistą przestrzenią fizyczną, to można dojść do wniosku, że albo nie znajdzie się ani jednej przestrzeni, która pozwoliłaby na opisanie bez naruszenia zwykłych właściwości — wzajemnej łączności przyczynowej, albo przestrzenie takie istnieją, a wówczas opierając się na teorii Brouwera można pokazać, że będą to jedynie przestrzenie trójwymiarowe.*

Poincar`e i jego następcy twierdzili, że jeśli zmieniłoby się radykalnie prawa fizyki, np. dopuściłoby się przyczynowe anomalie, to formalnie można by przyjąć model przestrzenny o wymiarowości różnej od 3. Jednak prawidłowości fizyczne, podstawowe fizyczne pojęcia przyczynowości nie zmieniają się w sposób dowolny, powstają one w procesie uogólnienia danych doświadczalnych i stają się ograniczonym elementem rozwijających się teorii fizycznych.

Teoria względności pokazała, że nawet metryczne właściwości przestrzeni i czasu nie mogą być rozpatrywane jako całkowicie konwencjonalne, tym bardziej odnosi się to do ich topologicznych właściwości. Można wykazać, że konwencjonalne podejście do

problemu trójwymiarowości przestrzeni wynika z traktowania przestrzeni i czasu jako form postrzegania zmysłowego (jako tworów naszego umysłu) pozbawionego kantowskiego aprioryzmu: jeżeli „niedorzecznością" jest mówić o rzeczywistej przestrzeni istniejącej niezależnie od postrzegającego podmiotu, to wybór modeli przestrzenno-czasowych przez badacza podyktowany jest jedynie przez kryterium dogodności, prostoty, celowości, ekonomiki myślenia itd.

> *W ostatecznym wyniku u podstaw takiego podejścia leży nieuzasadnione sprowadzanie rzeczywistej przestrzeni, w której są zlokalizowane rzeczywiste obiekty, do przestrzeni percepcyjnej (przestrzeni postrzegania), w której są zlokalizowane nasze wrażenia.*

Z przeprowadzonych analiz oraz twierdzeń materializmu dialektycznego (przestrzeń i czas są obiektywnymi formami istnienia materii; ruch jest istotą przestrzeni i czasu) wynikają następujące wnioski:

— po pierwsze, że istnieją jakościowo różne formy przestrzeni i czasu, należące do różnych postaci materii;

— po drugie zaś, że należy liczyć się z ilościową i jakościową zmiennością oraz rozwojem przestrzeni i czasu, ponieważ z przechodzeniem materii (wskutek ruchu) z jednej postaci do drugiej powinny zmieniać się jej własności.

Z cybernetycznego[36] punktu widzenia desygnat przestrzeni interpretowany jest jako „zbiór dowolnych przedmiotów (liczb, stanów układu, wektorów itp.), między którymi zostały ustalone pewne relacje natury geometrycznej bądź abstrakcyjnej".

> *Konfrontując to z regułami stosowanymi w teorii mnogości relacje te należy rozumieć jako cechy wyróżnialności (kryteria rozstrzygalności), które pozwalają określać czy dany element zbioru, ze względu na zachowanie warunku jednorodności, należy do tego zbioru czy też nie. Dlatego też liczba przestrzeni jest nieskończona, tak jak nieskończone są możliwości wyznaczenia relacji pomiędzy nieskończoną liczbą elementów materialnych i niematerialnych.*

Co się zaś tyczy „przestrzeni walki informacyjnej", to przede wszystkim trzeba uwzględniać złożoność pojęcia. W jego strukturze wyrazem podstawowym jest „przestrzeń", a wyrazami dopełniającymi, konkretyzującymi desygnat całości, są pojęcia: „walka" i rodzaj tej walki zwany „informacyjną". Dlatego też desygnat tego trójczłonowego pojęcia powinien zawierać w swoim zbiorze przedmiotowym wszystkie te elementy, które są właściwe pojęciom: „przestrzeń"; „walka" oraz „walka informacyjna", co można oznaczyć następująco:

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

---

[36] *Mały słownik cybernetyczny*, op. cit., s.251.

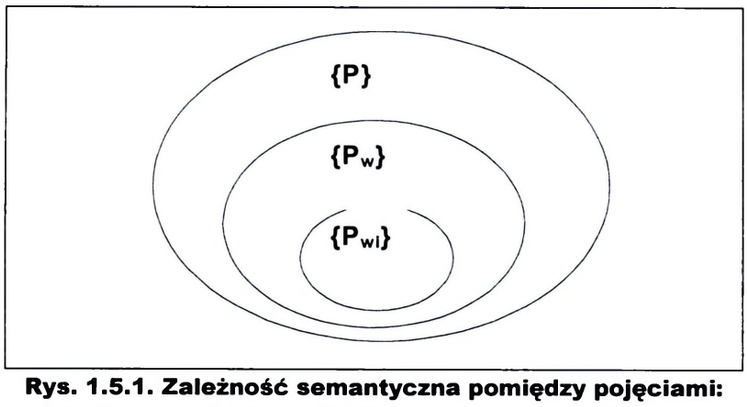
— $\{P_w\}$ — zbiór elementów składających się na desygnat „przestrzeń walki";

— $\{P_{wi}\}$ — 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).



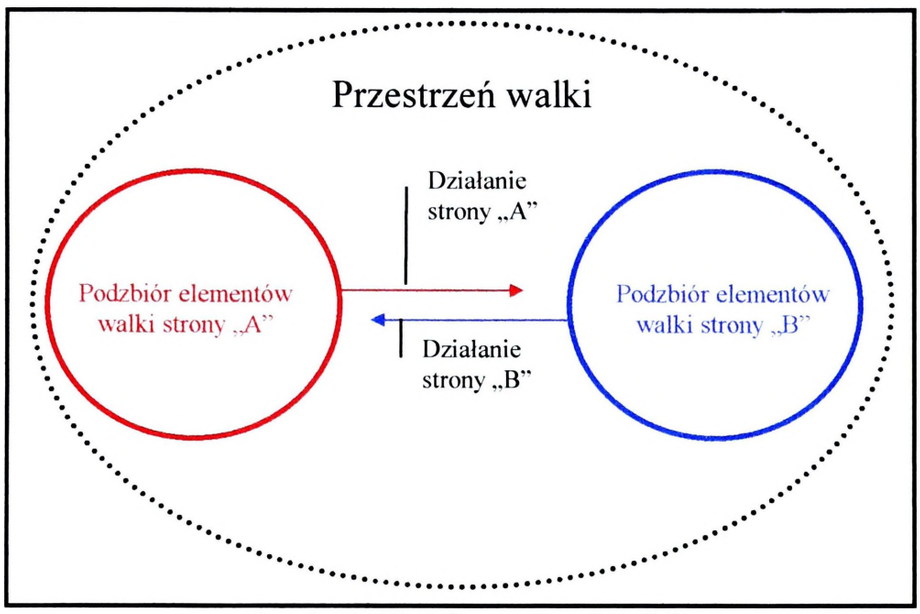
Rys. 1.5.1. Zależność semantyczna pomiędzy pojęciami: „przestrzeń", „przestrzeń walki" i „przestrzeń walki informacyjnej"

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.*

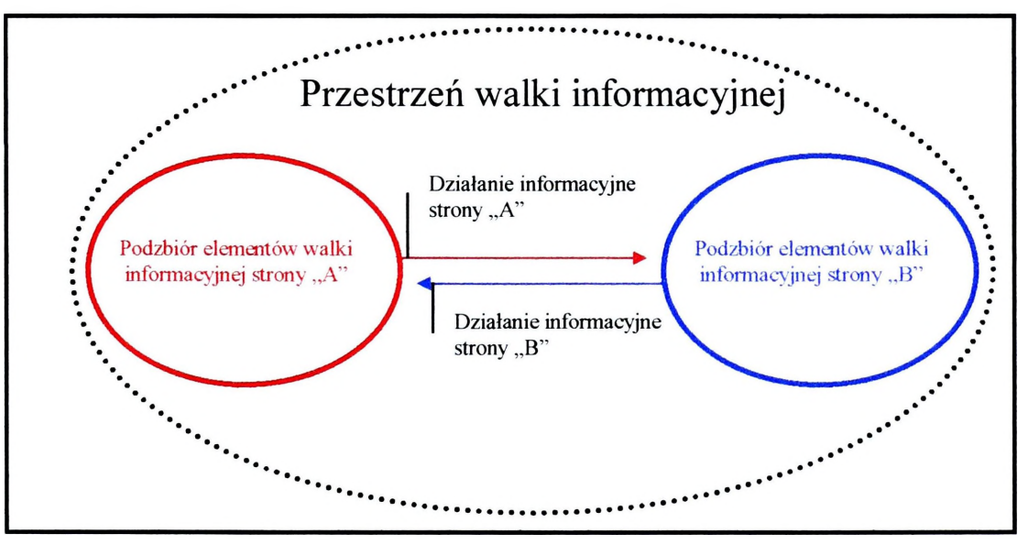
Podstawą przedmiotu myślowego „przestrzeń walki" jest to, że w strukturze tej przestrzeni (w strukturze tego zbioru) muszą istnieć przynajmniej dwa podzbiory elementów, pomiędzy którymi, ze względu na funkcję celu, zachodzi kooperacja negatywna wzajemna. Oznacza to, że „przestrzenią walki" można nazywać 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).

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



Rys. 1.5.2. Model przestrzeni walki

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).

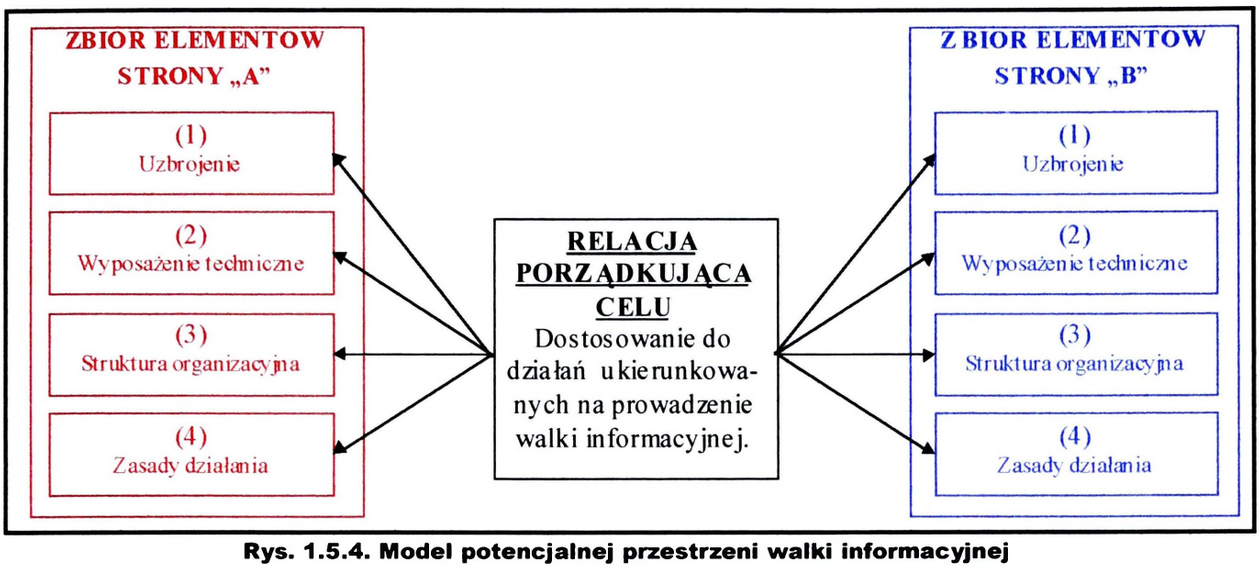


Rys. 1.5.3. Model przestrzeni walki informacyjnej

> *Z powyższego wynika, że podstawową strukturę[37] 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 techniczne, system organizacyjny i system szkolenia wojsk oraz sposoby wykorzystywania tego w działaniach.*

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

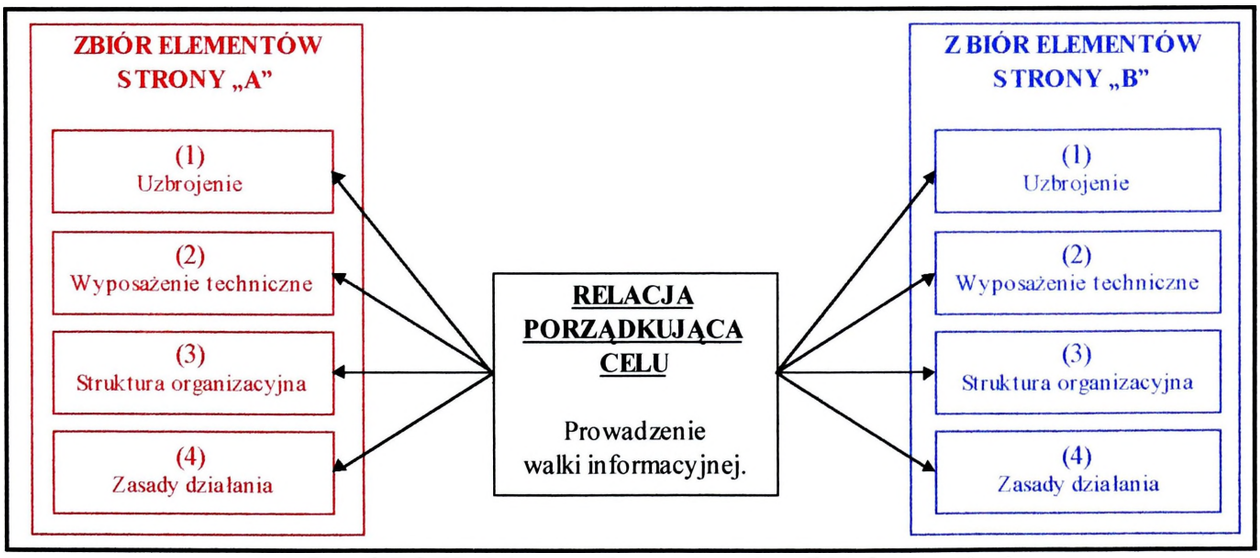
[37]Struktura to układ i wzajemne relacje elementów stanowiących całość. *Słownik języka polskiego*, t 3, PWN, Warszawa 1981r., s. 352.



Rys. 1.5.4. Model potencjalnej przestrzeni walki informacyjnej

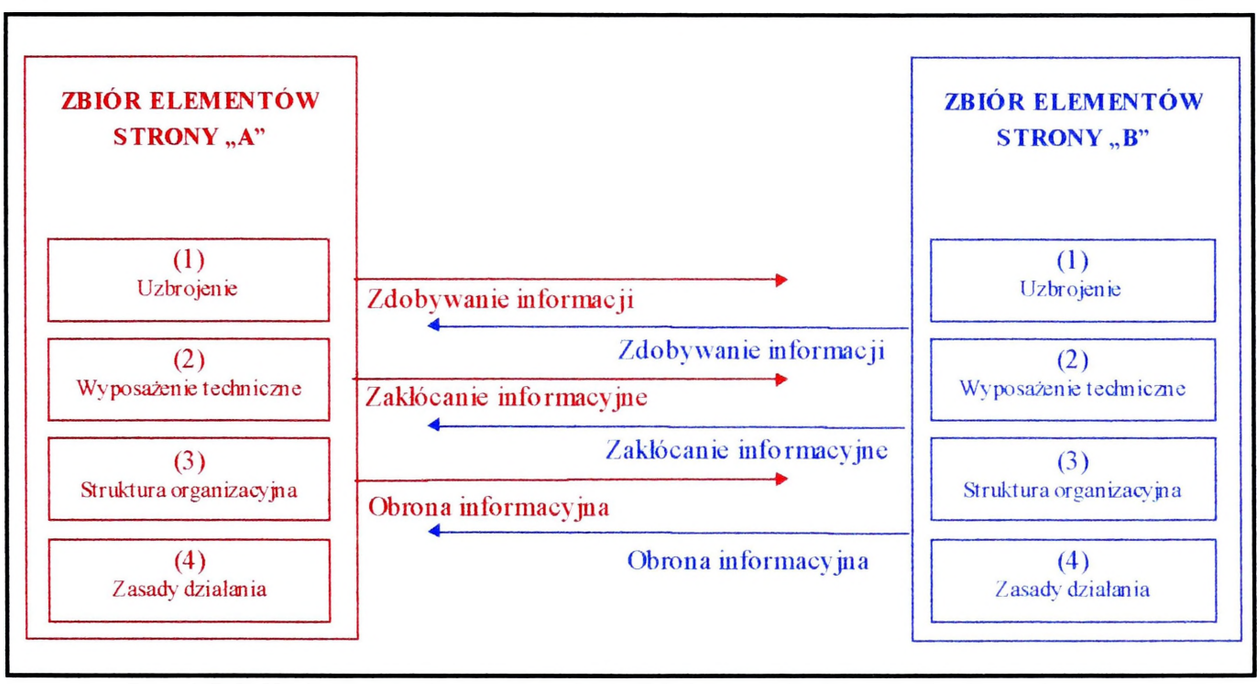
Wynika z tego, że wyróżnione elementy zespolone są tylko relacją porządkującą, której celem jest dostosowanie elementów do prowadzenia walki informacyjnej. Nie oznacza to jednak, że walka taka będzie kiedykolwiek prowadzona — może być prowadzona ale nie musi. Innymi słowy, w przestrzeni tej zawarty jest 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.



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

> *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.*

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[38]. 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[39], 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;
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.

---

[38] 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.

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

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:

$$A_1 \cup A_2 \cup \ldots \cup A_n = 1^*$$

— 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 $\Re$ do y oraz element y w relacji $\Re$ do z, to x pozostaje w relacji $\Re$ do z:

$$\wedge_x \wedge_y \wedge_z [(x\Re y) \wedge (y\Re z)] \rightarrow (x\Re z)$$

— relacja spójności — jeśli $x = y$, to albo x pozostaje w relacji $\Re$ do y, albo y w relacji $\Re$ do x:

$$\wedge_x \wedge_y [(x = y) \vee (x\Re y) \vee (y\Re x)]$$

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:

$$\wedge_i \wedge_j (A_i \cap A_j) \neq 0 *$$

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:

$$A_1 \cup A_2 \cup ... \cup A_n = 1 *$$

$$\wedge_i \wedge_j (A_i \cap A_j) = 0 *$$

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*[40]*. 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;

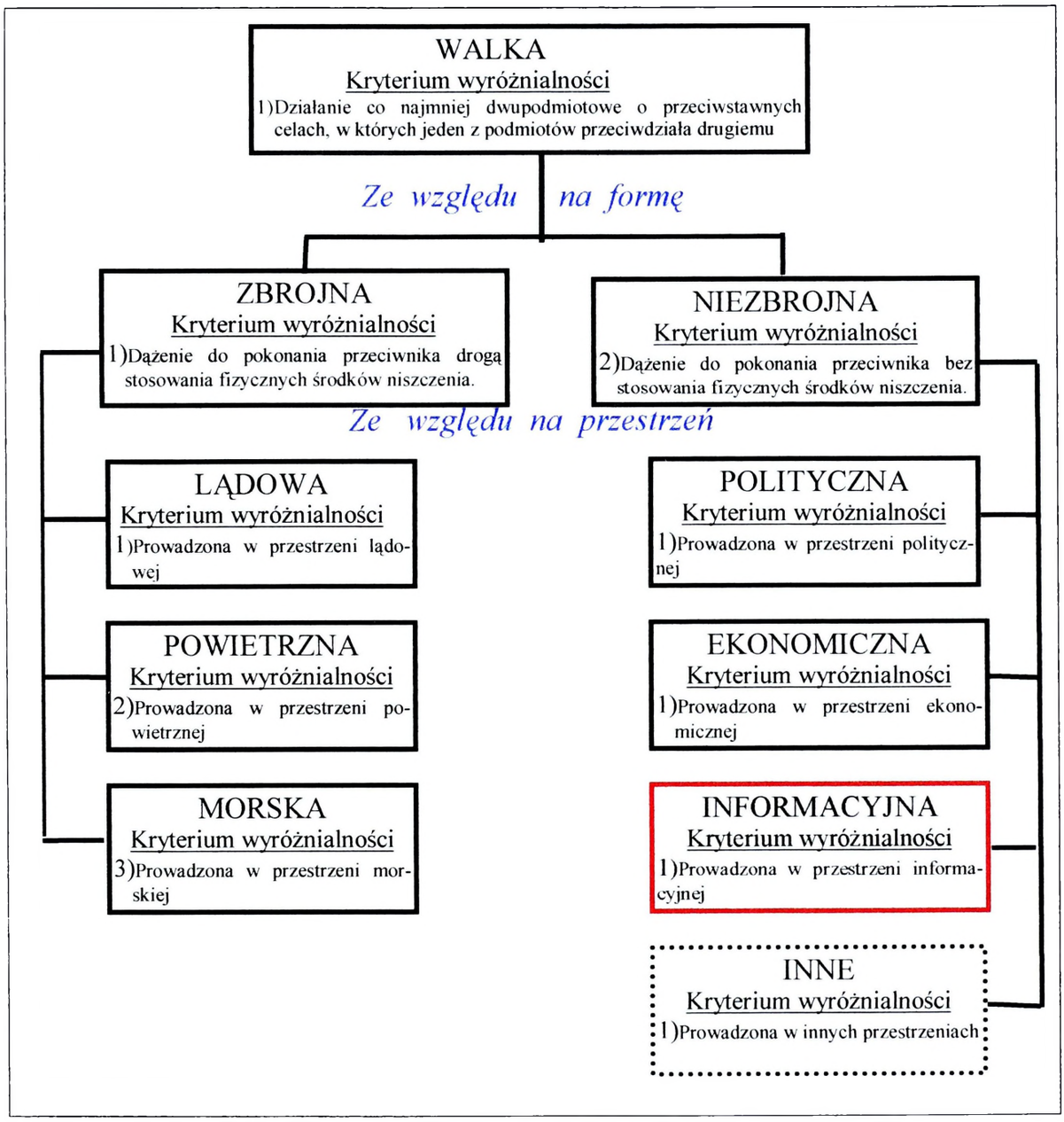
---

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

— 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).



Rys. 1.5.7. Miejsce walki informacyjnej w ogólnej przestrzeni walki

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[41], tzn. o raz na zawsze ustalonej mocy[42]— o raz na zawsze ustalonej liczbie jego elementów materialnych i niematerialnych oraz procesów i rozwiązań funkcjonalnych. Interpretacja taka ograniczałaby podział tylko do znanych dziś elementów zbioru. Nie mogłaby być uwzględniana w nim (w tym podziale) sytuacja rozwojowa wojsk, a więc nie byłoby miejsc wolnych (miejsc zarezerwowanych) dla tych wszystkich elementów, które mogą się pojawić w przyszłości w składzie walki informacyjnej, a które są dziś trudne, a nawet niemożliwe do dokładniejszego ustalenia. Dlatego też przestrzeń tę należy traktować jako zbiór skończony, ale tylko w aspekcie teraźniejszości. Co do przyszłości należy ją widzieć jako zbiór nieskończony[43], rozwijający się w rytm postępu naukowego i technologicznego.

> *Niezależnie jednak od liczby i rodzajów pojawiania się nowych elementów zbioru[44], 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)*

[41]Zbiór skończony – zbiór o skończonej liczbie elementów.
[42]Moc zbioru – liczba elementów zbioru skończonego lub jego liczba kardynalna dla zbiorów skończonych i nieskończonych.
[43]Zbiór nieskończony – zbiór o nieskończonej liczbie elementów.
[44]Element zbioru – dowolnie wyróżniony obiekt rzeczywisty czy też myślowy.

techniki (uzbrojenia i wyposażenia) i stanów osobowych, które na kolejnych poziomach podziału prowadziłoby do coraz to większego ujednorodnienia zasad działania tych grup na polu walki i procesu ich szkolenia w okresie pokoju. Spełnienie tego warunku sprzyjać może właściwemu profilowaniu:

— *wewnętrznych struktur organizacyjnych wojsk;*
— *wymagań profesjonalnych;*
— *kryteriów naboru stanu osobowego;*
— *procesu przygotowywania kadr i szkolenia wojsk.*

Jak już stwierdzono 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).

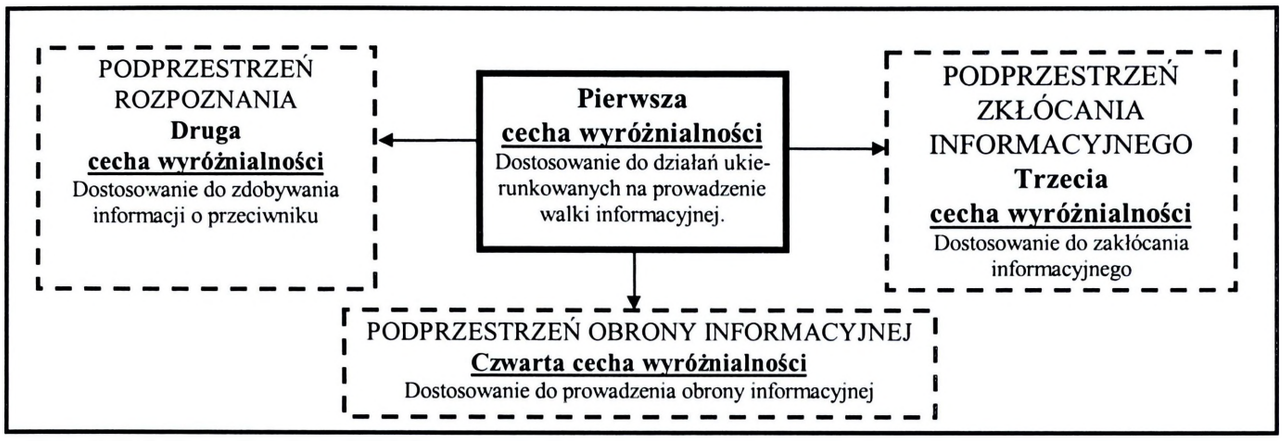
Podział ten spełnia wszystkie warunki dobrego porządkowania zbioru. Jest poprawny merytorycznie, ponieważ:

— 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)

Znaczenie informacji wzrosło tak drastycznie w ciągu ostatnich kilkunastu lat, dlatego, że człowiek nauczył się ją przetwarzać w sposób przemysłowy. Znakiem czasu stał się bit — podstawowa jednostka informacji w systemach informatycznych. Gdy zaczęto zmieniać dowolny komunikat — tekst, dźwięk oraz obraz na bity pojawiło się stwierdzenie, że ma miejsce rewolucja informacyjna. Wielu naukowców twierdzi, że jej znaczenie będzie takie jak rewolucji przemysłowej sprzed blisko dwustu lat. W XXI wieku podstawowym surowcem strategicznym nie będzie węgiel, miedź czy żelazo ale informacja. Dlatego też o ekonomicznej potędze nie będzie decydował tonaż wyprodukowanej stali i liczba samochodów, lecz odsetek obywateli z wyższym wykształceniem oraz ilość pieniędzy przeznaczonych na badania naukowe.

Potrzeby informacyjne na przyszłym polu walki, ograniczony czas podejmowania decyzji oraz konieczność szybkiego przetwarzania dużych ilości informacji stwarzają potrzebę wykorzystania komputerów (maszyn cyfrowych) na wszystkich szczeblach dowodzenia. Dlatego też należy poświęcić większą uwagę zagadnieniom i możliwościom współdziałania człowieka z elektroniczną maszyną cyfrową. Dzisiaj istnieją dwa wiążące się ze sobą poglądy dotyczące ludzi i maszyn[45]. Zgodnie z pierwszym można budować maszyny zdolne do wykonywania tych samych czynności, które wykonują ludzie. Według drugiego poglądu — ludzie są nie tylko podobni do maszyn, lecz wręcz są skomplikowanymi maszynami. Mózg człowieka i maszyna cyfrowa wzajemnie się uzupełniają w swych funkcjach. Mózg do pewnego stopnia wybiera, jaką informację chce uzyskać, decydując, z jaką częścią swego otoczenia chce wejść w kontakt, formułując pytania itd., podczas gdy maszyna cyfrowa automatycznie przyjmuje każdą informację,

[45]Apter M. J.: *„Komputery a psychika. Symulacja zachowania"*, PWN, Warszawa 1973, s.11.

jaką się jej poda. Mózg filtruje również informacje, które w danym czasie otrzymuje, tak że w rzeczywistości przyjmuje tylko małą część napływającej informacji. Podstawowa różnica polega na tym, że mózg na wielu swych obszarach wykazuje zdolność kompensacyjną[46], której nie ma komputer. Jeżeli pewne partie żywego mózgu usuniemy, pozostałe automatycznie przejmują funkcje partii usuniętych. Wydaje się również, że wyuczone nawyki nie są „zmagazynowane" na określonej małej przestrzeni, lecz są rozsiane w pewien sposób na większym obszarze, wskutek czego wycięcie ograniczonej części mózgu niekoniecznie oznacza utratę nawyku. Jeżeli natomiast jakaś część maszyny cyfrowej zostanie zepsuta, spowoduje to co najmniej utratę informacji zawartej w tej części (programu lub w innych danych), a niekiedy nawet awarię całego układu. Jest zrozumiałe, że w komputerze nie występuje tak duża redundacja, czyli „nadmierność", jak w mózgu ludzkim, dlatego komputer nie posiada rezerw informacji, którymi mógłby zastąpić informacje utracone i pozostać niezawodnym. Mózg jest jeszcze niezawodny pod innym względem: funkcjonuje on w kategoriach struktur i jeżeli zabraknie jakichś elementów struktury, to mózg je rekonstruuje.

Z punktu widzenia optymalizacji systemu informacyjnego komputer powinien pracować z należytą szybkością i dokładnie przetwarzać wprowadzone dane, stosownie do potrzeb wynikających z warunków konkretnej sytuacji.

Ze strony człowieka oczekuje się zazwyczaj określenia form i zakresu informacji o warunkach otoczenia, i to takiej, która może być interesująca w konkretnej sytuacji. Poza tym żąda się od niego ustalenia kryteriów przydatności informacji i wyselekcjonowania wyników przetwarzania danych oraz wszelkich czynności mających na celu zmianę warunków otoczenia i przystosowania ich do potrzeb człowieka z punktu widzenia jego zadań. Człowiek i maszyna cyfrowa wzajemnie uzupełniają się w swej roli i funkcjach.

Organizm ludzki jest złożoną całością przetwarzającą informacje w takich kategoriach, jak: percepcyjna, lingwistyczna, symboliczna, wartościująca (systemy postaw i wartości), a wszystkie te schematy współdziałają ze sobą i oddziałują wzajemnie na siebie. Dlatego też człowiek w dalszym ciągu zostanie niezastąpionym ogniwem w procesie decyzyjnym.

Systemy informacyjne przeniknęły już do życia wojskowego i cywilnego, została przekroczona nowa granica wieku informacji, którą będzie XXI wiek. Walka informacyjna staje się kluczowym sposobem prowadzenia konfliktów zbrojnych i będzie najważniejsza

[46]Kompensacja – wszelkie działanie mające na celu równoważenie niepożądanych wpływów lub zastępowanie innego działania.

w operacjach w XXI wieku. To oznacza, że już dzisiaj należy inwestować w ludzi, sprzęt i badania, wykorzystywać każdą nadarzającą się okazję, aby zaspokoić ambicje i przybliżyć się do następnego stulecia.

Rozwój technologii informacyjnych może spowodować drastyczne zmiany w prowadzeniu konfliktów zbrojnych w przyszłości. Technologia pozwoli na zobrazowanie sytuacji z pola walki nawet na najniższych szczeblach dowodzenia. Dlatego każdy dowódca będzie musiał zrozumieć rolę zdobywania informacji w swoim rodzaju sił zbrojnych (służb). Zarówno żołnierz sił lądowych, jak i marynarz czy lotnik będą musieli wiedzieć i rozumieć, że prowadzenie rozpoznania walnie przyczyni się do odniesienia sukcesu w walce zbrojnej.

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 informacji o miejscu pobytu przeciwnika, jego ugrupowaniu i zamiarach było bardzo ważnym elementem, niezbędnym do podejmowania decyzji, zwłaszcza dla tych dowódców, którzy wiedzieli jak je wykorzystać. 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.*

Jednak nawet najlepsza informacja o przeciwniku staje się bezwartościowa, jeśli dotrze zbyt późno do adresata. Również jej treść i wiarygodność jest znacznie ważniejsza od ilości. Po przestudiowaniu literatury przedmiotu można stwierdzić, że:

> *Współczesna walka zbrojna dostarcza ogromnych ilości informacji 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. W takim ujęciu „informacjami" o przeciwniku są wszystkie te dane , które dotyczą m.in.:*
> — *sytuacji politycznej, gospodarczej i geostrategicznej, a także ich wzajemnych związków i zależności;*

— *możliwości operacyjno-technicznych sił i środków własnych i przeciwnika;*
— *cech charakterystycznych oraz sytuacji geograficznej, meteorologicznej, geologicznej, biologicznej, ekologicznej, chemicznej, medycznej oraz sposobów wykorzystania spektrum elektromagnetycznego;*
— *treści przekazów mówionych, obrazowych lub pisanych, tj. rozkazów, meldunków, wiadomości, informacji rozpowszechnianych przez środki masowego przekazu oraz sieci informatyczne o zasięgu globalnym (np. Internet), krajowym, lokalnym lub resortowym;*
— *sposobów postępowania, z uwzględnieniem m.in. zasad dowodzenia i działania, regulaminów a także innych przepisów;*
— *stanu i rozwoju cech intelektualnych, psychicznych i moralnych sił przeciwnika oraz ludności cywilnej;*
— *cybernetycznych współzależności pomiędzy informacjami pojedynczymi a dużą ilością danych.*

Na podstawie przeprowadzonej analizy (ze względu na treść) można wyróżnić informacje (dane):

— o przeciwniku;

— i wojskach własnych.

Elementami decydującymi o wartości danych (o przeciwniku) w kontekście treści w nich zawartych są:

— wiarygodność,

— i aktualność.

Obok danych wiarygodnych o przeciwniku występuje także duża ilość danych dezinformujących, które mogą oddziaływać na procesy decyzyjne w postaci czynników zakłócających. Można zatem wnioskować, że:

Problem nie tkwi w braku czy niedostatku danych, lecz w tym, że:
— *nie zawsze istnieje możliwość dysponowania informacjami we właściwym czasie;*
— *brak jest informacji na pewnych szczeblach dowodzenia, tam gdzie są najbardziej potrzebne w danym momencie;*
— *informacje nie zawsze są pełne i często sprzeczne;*
— *występuje nadmiar danych utrudniający wyselekcjonowanie we właściwym czasie tych naprawdę ważnych.*

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 informacji.
- 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.

Istotną rolę w przygotowaniu baz danych o przeciwniku ma przyjęcie odpowiednich kryteriów podziału informacji o jego siłach i środkach, tj. określenie odpowiednich struktur tej informacji.

Złożoność procesów współczesnego pola walki powoduje, że decydenci żądają coraz większej ilości informacji, o coraz szerszym zasięgu tematycznym. Wszystkie informacje dotyczące potencjalnego przeciwnika, jego sił zbrojnych, polityki, ekonomiki, infrastruktury, demografii, nastrojów oraz terenu, warunków hydrologicznych i meteorologicznych, wykorzystywane przez rozpoznanie, noszą nazwę *informacji rozpoznawczych.* Ważną rolę w procesie ich gromadzenia oraz przetwarzania stanowią *bazy danych* o siłach i środkach przeciwnika.

Informacje wprowadzane do baz danych o siłach i środkach przeciwnika powinny być usystematyzowane oraz zgromadzone w niezależnych zbiorach.

Z uwagi na *sytuację polityczno-militarną RP* można wyróżnić trzy wzajemnie uzupełniające się zbiory danych o siłach i środkach przeciwnika:

- Zbiór okresu pokoju.
- Zbiór okresu zagrożenia wojennego.
- Zbiór okresu wojny (początkowego okresu wojny).

W okresie pokoju powinna być najbardziej rozbudowana baza danych o siłach i środkach potencjalnego przeciwnika. Szczególną uwagę należy zwrócić na te państwa, z którymi kraj nasz nie zawarł sojuszy obronnych. Informacje powinny być gromadzone i weryfikowane na bieżąco. Baza danych o siłach i środkach potencjalnego przeciwnika *(okresu pokojowego)* powinna obejmować zbiory treści dotyczące:

— struktur organizacyjnych sił zbrojnych państw obcych, składu bojowego, organizacji, wyposażenia dowództw i jednostek poszczególnych rodzajów sił zbrojnych;

— poziomu rozwoju technicznego sił zbrojnych, modernizacji poszczególnych rodzajów broni, wzrostu ich możliwości ogniowych i gotowości bojowej. Szczególną uwagę należy zwrócić także na rozwój systemów rozpoznania i walki radioelektronicznej, dowodzenia, łączności i informatyki, obrony powietrznej oraz zabezpieczenia logistycznego;

— kierunków rozwoju strategii, sztuki operacyjnej i taktyki w poszczególnych państwach;
— systemów mobilizacyjnych oraz operacyjnego rozwijania sił zbrojnych (rodzajów wojsk, związków taktycznych i oddziałów), możliwych kierunków ich użycia oraz prawdopodobnych zadań;
— przebiegu manewrów i ćwiczeń, procesów dydaktyczno-wychowawczych oraz zmian w koncepcjach ich prowadzenia oraz sposobach zabezpieczenia;
— przebiegu lokalnych konfliktów zbrojnych oraz taktyki użycia wydzielonych sił i środków państw obcych w misjach pokojowych;
— sylwetek ważniejszych dowódców, ich przebiegu służby wojskowej oraz stosowanych stylów i sposobów dowodzenia.;

Struktura bazy danych *okresu zagrożenia wojennego* powinna stanowić uzupełnienie (a niekiedy jedynie uaktualnienie) bazy okresu pokojowego i obejmować dane dotyczące:
— sygnałów alarmowych, zarządzeń dotyczących wprowadzania wyższych stanów gotowości bojowej sił zbrojnych potencjalnego przeciwnika;
— zakresu uruchomienia jego systemu mobilizacyjnego;
— zmian dyslokacji (bazowania), przegrupowania wojsk potencjalnego przeciwnika oraz operacyjnego rozwijania jego sił zbrojnych;
— stanu gotowości stacjonarnych oraz rozwijanych polowych systemów dowodzenia i łączności;
— rejonów rozmieszczenia obiektów kluczowych przeciwnika;
— stanu ilościowego i ugrupowania wojsk przeciwnika w strefach przygranicznych oraz obszarach operacyjnego rozwinięcia jego sił zbrojnych a także możliwości narastania sił w wyniku mobilizacji lub przerzutów z innych kierunków operacyjnych;
— zmian operacyjnego przygotowania terenu w rejonach przygranicznych i na kierunkach potencjalnych działań;
— zakresu, kierunków i metod działalności psychologiczno — dywersyjnej przeciwnika.

Struktura bazy danych *okresu wojny* (*początkowego okresu wojny)* powinna stanowić uzupełnienie (uaktualnienie) dwóch poprzednich baz oraz obejmować dane dotyczące:
— głównych zgrupowań uderzeniowych pierwszego rzutu operacyjnego przeciwnika, ich stanów ilościowo-jakościowych, kierunków działania oraz prawdopodobnych zadań;

— składu i rejonów rozmieszczenia drugich rzutów oraz odwodów wojsk operacyjnych, ich przegrupowań do obszaru działań wojennych, możliwych kierunków, rubieży oraz terminów ich wprowadzenia;
— przebiegu formowania i możliwości nowych związków, stopnia osiągania przez nie gotowości bojowej oraz prawdopodobnego czasu zdolności do działań;
— stanu i dyslokacji sił powietrznych, zmian bazowania lotnictwa oraz sposobów jego wykorzystania w ramach wsparcia i zabezpieczenia działań wojsk;
— zmian w rozmieszczeniu i działaniu sił morskich, sposobów ich użycia, wykorzystania baz morskich i portów do przerzutów wojsk i zaopatrzenia;
— stopnia przygotowania, czasu, kierunków i rejonów oraz celu użycia wojsk powietrzno — desantowych;
— zmian w strukturach organizacyjnych wojsk oraz w taktyce i sztuce operacyjnej;
— zmian w uzbrojeniu oraz w specjalistycznych środkach technicznych wprowadzanych do wyposażenia wojsk;
— skuteczności systemów bojowego oraz logistycznego zabezpieczenia działań zbrojnych;
— składu narodowościowego i społecznego wojsk przeciwnika, zdyscyplinowania, stanu moralnego i psychicznego żołnierzy oraz ich doświadczenia bojowego;
— zmian kadrowych, sylwetek nowych dowódców, przebiegu ich służby wojskowej oraz stosowanych stylów i technik dowodzenia.

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.

W zależności od stopnia wykorzystania dane można podzielić na: bojowe i studyjne.

Dane bojowe — to takie, które ze względu na stopień szczegółowości i wiarygodności mogą być bezpośrednio wykorzystywane do rażenia przeciwnika lub wykonania określonego manewru bez potrzeby ich opracowywania i uzupełniania. *Umieszczone w bazach danych powinny być dostępne dla odbiorców bez ograniczeń.*

Dane studyjne — to takie, które z różnych względów nie mogą być bezpośrednio wykorzystane i wymagają dodatkowych analiz i opracowania przez sztabowe organa rozpoznawcze. Są one z reguły wykorzystywane w ogólnej ocenie sytuacji. *Umieszczenie ich w bazach danych powinno być związane z określeniem stopni ich dostępności dla różnych kategorii odbiorców.* Jednak w zależności od rozwoju sytuacji ich charakter może ulec zmianie.

W procesie pozyskiwania, opracowywania i wykorzystywania danych istnieje prawidłowość, iż ta sama postać dla jednego odbiorcy jest daną bojową, a dla drugiego — studyjną. Jednocześnie, po wykorzystaniu, dane bojowe stają się danymi studyjnymi, a dane studyjne, po odpowiednim opracowaniu, mogą się stać bojowymi.

Należy mieć na uwadze, że potrzeby informacyjne na poszczególnych szczeblach dowodzenia, różnią się stopniem szczegółowości. Typowe zapotrzebowanie informacyjne *związku operacyjnego lub taktycznego* ma zazwyczaj charakter ogólny.

Dowódcy tych szczebli potrzebują danych studyjnych niezbędnych do podjęcia decyzji — poszukują zatem odpowiedzi na pytania: co? gdzie? kiedy? w jaki sposób? Dlatego też działania rozpoznawcze na tych szczeblach dowodzenia powinny być ukierunkowane przede wszystkim na pozyskiwanie danych niezbędnych do podjęcia decyzji, a szczególnie do wypracowania wniosków, jak ugrupować swoje siły i gdzie skupić główny wysiłek walki.

> *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. Jednostki niższego szczebla potrzebują mniej danych studyjnych dotyczących oceny sytuacji a więcej danych bojowych wykorzystywanych do prowadzenia ognia i manewru wojskami, stosownie do szybko zmieniającej się sytuacji na polu walki. Dlatego też w ich działalności bojowej jest więcej meldowania, a mniej analizy. Natomiast związki wyższego szczebla opierają się głównie na analizach i ocenach. Zazwyczaj brygady, bataliony i kompanie przekazują dane bojowe w górę, a otrzymują stamtąd ich opracowane postacie w formie komunikatów o przeciwniku i sytuacji na polu walki.*

Konieczność orientacji we współczesnym świecie stwarza potrzeby poznawcze (intelektualne), a ich zaspokojenie warunkuje posiadanie odpowiedniej wiedzy. Człowiek odbiera za pośrednictwem układu nerwowego sygnały wysyłane przez środowisko i na ich podstawie reaguje na różne czynniki i zjawiska. Bodźce fizyczne (np. światło, dźwięk) po skomplikowanych procesach w narządach odbiorczych (np. w oku, uchu) i w układzie nerwowym (obwodowym i ośrodkowym) stają się sygnałami niosącymi określone

informacje. Mózg dokonuje syntezy danych dostarczanych mu z różnych narządów odbiorczych.

Poprzez zwiększenie rodzaju i zakresu uzyskiwanych danych człowiek wychodzi poza ograniczenia, jakie narzucają mu możliwości percepcyjne narządów zmysłowych, pokonuje barierę czasu i przestrzeni, uzyskuje możliwość wyboru optymalnych rozwiązań w różnych sytuacjach, uniezależnia się od zmian w środowisku. Liczne fakty z codziennego życia wskazują, że człowiek coraz bardziej wychodzi poza granice możliwości receptorów — oka, ucha itp. Pozytywna rola informacyjna polega na tym, że umożliwia mu przystosowanie się do otoczenia, jego przekształcenie, przewidywanie zdarzeń i zmniejszenie ryzyka podejmowania decyzji. Badania w zakresie psychologii i cybernetyki pozwoliły na ścisłą analizę procesów – składowych aktywności człowieka, do których można zaliczyć:

— odbiór danych (przyjęcie i odczytanie sygnałów, spostrzeganie, zapamiętywanie);

— przetwarzanie danych (analiza, wnioskowanie);

— wykorzystanie informacji (podejmowanie decyzji).

Psychologia stosuje tradycyjnie podział funkcji poznawczych na wrażenia, spostrzeżenia, wyobrażenia, pamięć i myślenie — które w ujęciu cybernetycznym zostały sprowadzone do trzech podstawowych procesów (odbiór, przetwarzanie i wykorzystanie informacji). 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[47] i wielospektralnego[48] postrzegania zjawisk w materialnej przestrzeni przeciwnika, co umożliwiają urządzenia elektroniczne.

---

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

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

Biorąc pod uwagę pierwszą cechę wyróżnialności, czyli formę, rozpoznanie będzie odzwierciedlać zespół skoordynowanych elementów, który dostosowany jest do zdobywania danych o przeciwniku. Elementami tymi są:

— *źródła informacji;*
— *nośniki informacji;*
— *układy odbierające.*

Podstawowymi elementami w strukturze przestrzeni zdobywania informacji są źródła informacji, które wybierają ze zbioru możliwych postaci danych o przeciwniku tylko te, które są im fizycznie dostępne.

Ze względu na formę dostępu informacyjnego, można wyróżnić:

— *rozpoznanie osobowe (wg terminologii NATO HUMINT — Human Intelligence);*
— *rozpoznanie nieosobowe (można je nazywać technicznym ze względu na to, że jest realizowane głównie przy wykorzystaniu techniki).*

Przestrzeń rozpoznania osobowego tworzy człowiek i wszelkie narzędzia przystosowane do zdobywania danych w postaciach bezpośrednio odbieranych przez układ recepcyjny człowieka. Bezpośrednie ludzkie doznania zmysłowe stanowią podstawowe sygnały informacyjne w identyfikowaniu stanu otoczenia. Pomiędzy zbiorem możliwych postaci danych o otoczeniu i ludzkimi zmysłami nie mogą występować żadne przetworniki zmieniające ich postać. Oznacza to, że jest dopuszczalne stosowanie urządzeń wspomagających zasięg i czułość doznań zmysłowych, ponieważ te nie zmieniają postaci danych, a czynią je tylko bardziej wyrazistymi. Innymi słowy, określony sygnał informacyjny o przeciwniku dociera do człowieka (zwiadowcy) prowadzącego rozpoznanie w formie bezpośrednio dla niego zrozumiałej. Mogą to być dane zawarte w paśmie promieniowania widzialnego, drgań akustycznych, jak również informacje odbierane dotykowo, smakowo i przez powonienie. Należy w tym wypadku wykluczyć transformowanie na ludzkie doznania danych z obszarów pozazmysłowego poznania i tych, które po detekcji przetwarzane są na sygnały spoza tego poznania. Dlatego też człowiek nie może być pewien, czy poza zasięgiem jego doznań nie dokonano jakiejś deformacji postaci danej, stanowiącej sygnał informacyjny.

Rozpoznanie osobowe jest jednym z najstarszych rodzajów rozpoznania. Do jego prowadzenia można wykorzystywać przedstawicielstwa dyplomatyczne oraz pododdziały wojskowe. Praktycznie przedstawicielstwa dyplomatyczne mogą prowadzić je na szczeblu strategicznym, natomiast pozostałe organa tylko na szczeblu taktycznym. Rozpoznanie osobowe prowadzi zatem człowiek. Jego bezpośredni kontakt ze zbiorami różnych postaci danych o przeciwniku może być zapewniony przez:

— ściśle zakonspirowane działania wywiadowcze;

— fizyczne penetrowanie obszaru drogą patrolowania;

— fizyczne penetrowanie obszaru drogą specjalnie przygotowanych działań.

A zatem przestrzeń rozpoznania osobowego 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 nieosobowego tworzy zespół skoordynowanych źródeł rozpoznania, dostosowany do zdobywania danych w postaciach bezpośrednio nieodbieranych przez układ recepcyjny człowieka. W przestrzeni tej występują przetworniki informacji przekształcające jej pierwotnie przechwyconą postać w postać odbieraną przez układ recepcyjny człowieka. Urządzenia te są zawsze dostosowywane konstrukcyjnie do rejestrowania określonych efektów, charakterystycznych dla danego środowiska (np. elektromagnetycznego, chemicznego). Przez pryzmat rejestrowanych stanów jest identyfikowana sytuacja panująca w ich otoczeniu. Identyfikacji tej dokonuje ostatecznie człowiek, jako najważniejszy element układu decyzyjnego. Rejestrowane przez

przetworniki wartości pomiarowe nie stanowią jednak dla człowieka form bezpośrednio komunikatywnych. Znajdują się poza jego możliwościami postrzegania zmysłowego. Dlatego też muszą być przetwarzane, według odpowiednich algorytmów, do postaci zrozumiałych dla człowieka. Klasycznym tego przykładem może być telewizja, gdzie odbierany na wejściu sygnał elektromagnetyczny — nieodbierany bezpośrednio przez człowieka — przetwarzany jest w torze wizyjnym na konkretny obraz, a w torze fonicznym — na konkretny głos, które człowiek jest już w stanie odbierać. Innymi słowy, rozpoznanie nieosobowe ma na celu zdobywanie i przetwarzanie tych postaci danych o przeciwniku, których nośnikami są fale elektromagnetyczne oraz inne efekty uboczne towarzyszące działaniom bojowym. Postęp naukowo-techniczny pozwolił już na konstruowanie wielu takich urządzeń. Między innymi opracowano całą rodzinę urządzeń dostosowanych do rejestrowania określonych efektów, charakterystycznych dla danego środowiska — elektromagnetycznego, akustycznego, magnetycznego, elektrycznego, chemicznego (tab. 1.5.1.1).

> *Biorąc pod uwagę powyższe kryterium (środowisko nośników danych) i treści zawarte w tab. 1.5.1.1. przestrzeń rozpoznania nieosobowego można podzielić na:*
> *— podprzestrzeń rozpoznania elektromagnetycznego (wg NATO SIGINT — Signal Intelligence, zdobywanie danych na podstawie emisji elektromagnetycznej obcych systemów elektronicznych);*
> *Biorąc pod uwagę powyższe kryterium (środowisko nośników danych) i treści zawarte w tab. 1.5.1.1. przestrzeń rozpoznania nieosobowego 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).*

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 (patrz tab. 1.5.1.1). 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[49], ultradźwięki[50]) oraz wszelkiego rodzaju uboczne efekty towarzyszące działaniom bojowym, na przykład: akustyczne, sejsmiczne, magnetyczne, chemiczne, zapachowe itp.
- Rozpoznanie informatyczne[51] powinno być natomiast prowadzone z uwagi na masowy rozwój sieci informatycznych, które są bogatymi źródłami danych o siłach i środkach przeciwnika.

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

W widmie elektromagnetycznym wykorzystywane są głównie fale radiowe, mikrofale i promieniowanie widzialne. Biorąc to pod uwagę, należy jeszcze w przestrzeni rozpoznania elektromagnetycznego wyróżnić podprzestrzenie:

— rozpoznania radiowego;

— rozpoznania radiolokacyjnego;

— rozpoznania optoelektronicznego.

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

[49]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.

[50]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.

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

Rozpoznanie radiolokacyjne[52] 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[53]. Do pracy w tym paśmie skonstruowano całą rodzinę urządzeń optoelektronicznych[54], pozwalających na prowadzenie rozpoznania w ultrafiolecie, w zakresie promieniowania widzialnego oraz w zakresie bliskiej, średniej, dalekiej i skrajnej podczerwieni. Wykorzystywane są tutaj wszelkiego rodzaju urządzenia:

---

[52]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.

[53]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).

[54]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.

telewizyjne[55], termowizyjne[56], noktowizyjne[57] oraz laserowe[58]. 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;

---

[55]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.

[56]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).

[57]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.

[58]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).

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

— wskazywania celów.

Rozpoznanie to jest perspektywiczne, szczególnie na szczeblach taktycznych. Umożliwia bowiem pozyskiwanie danych z najbardziej niedostępnych stref [59] 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.

Wnioski z podrozdziału 1.5.1.

- *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.*

[59] 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);*

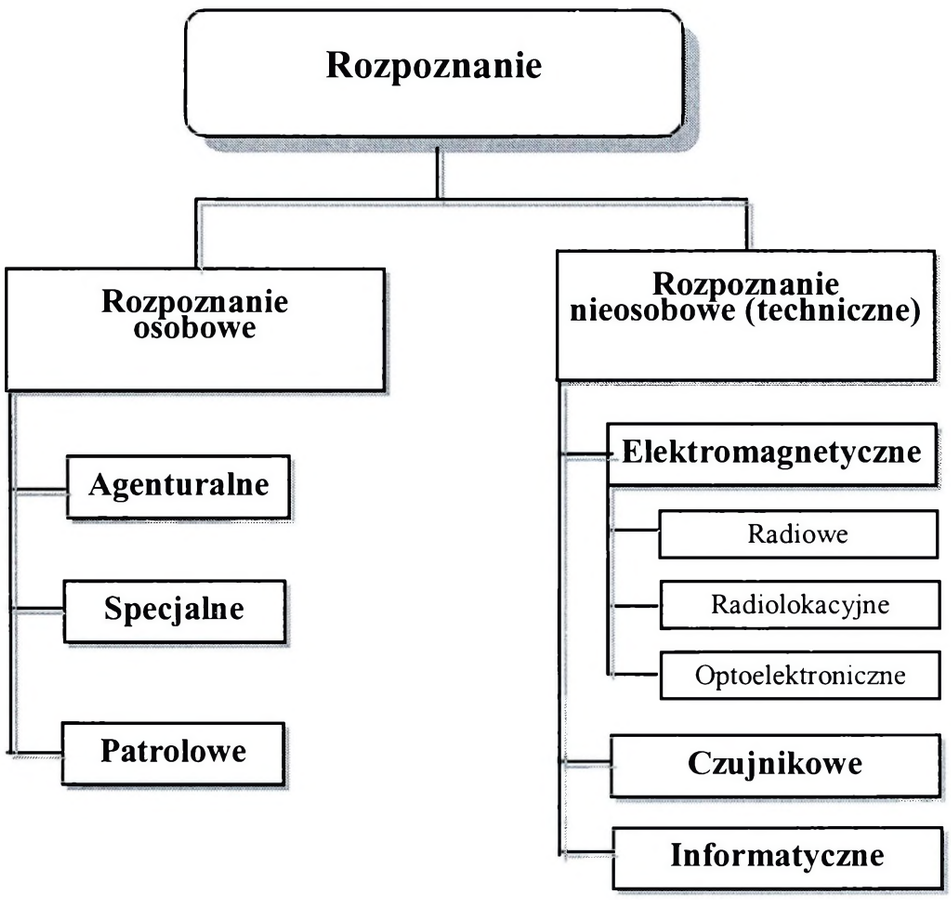
— *graficzne obrazowanie sytuacji;*

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

• *Przestrzeń zdobywania informacji (przestrzeń rozpoznania) tworzą zbiory następujących elementów:*

— *rozpoznania osobowego;*

— *rozpoznania nieosobowego (technicznego).*
• *Podprzestrzeń rozpoznania osobowego tworzą:*
— *rozpoznanie agenturalne;*
— *rozpoznanie specjalne;*
— *i rozpoznanie patrolowe.*
• *Podprzestrzeń rozpoznania nieosobowego (technicznego) tworzą:*
— *rozpoznanie elektromagnetyczne, a w tym:*
✓ *rozpoznanie radiowe;*
✓ *rozpoznanie radiolokacyjne;*
✓ *rozpoznanie optoelektroniczne;*
— *rozpoznanie czujnikowe;*
— *rozpoznanie informatyczne.*



Podział przestrzeni (zbioru) zdobywania informacji

1.5.2. Przestrzeń zakłócania informacyjnego

Każda instytucja, organizacja, a także osoba fizyczna dysponuje różnymi informacjami, które są niezbędne do jej normalnego funkcjonowania. Należy zgodzić się z tezą, że informacja w każdym organizmie społecznym lub gospodarczym odgrywa taką samą rolę, jak krew w organizmie żywym[60], a obieg informacji można porównać do

[60]A. Z. Idźkiewicz: *„Ochrona informacji w procesie przetwarzania"*, Państwowe Wydawnictwo Ekonomiczne, Warszawa 1979, s.7.

krwiobiegu. Rozszerzając to porównanie można stwierdzić, że podobnie jak organizm żywy umiera na skutek wykrwawienia lub zatrucia krwi, organizm gospodarczy lub społeczny może niedomagać lub zginąć, jeśli umożliwiająca mu funkcjonowanie informacja ulegnie zniszczeniu, przekłamaniu lub zostanie wykradziona, albo jeśli obieg tej informacji ulegnie zakłóceniu[61].

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 informacji pożądanej, jej deformacji lub wytwarzania informacji nieprawdziwych 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

---

[61] Zakłócenie to naruszenie ustalonego porządku, biegu spraw, dezorganizacja; niepożądany sygnał występujący jednocześnie z sygnałem użytecznym i pochodzący z innego źródła niż źródło sygnału użytecznego. *Leksykon techniczny*, op. cit., s. 624.

napływu informacji 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 (wojska). Próbowali wprowadzić w błąd przeciwnika aby podjął niekorzystną decyzję w stosunku do realnej sytuacji na polu walki. Ponieważ działalność ta była głównie skierowana na percepcję decydentów, strategię tą nazywano *zakłócaniem percepcyjnym (osobowym)*.

Obecnie systemy informacyjno — sterujące posiadające takie cechy, jak: centralna baza danych, duża szybkość przekazu oraz duży zasięg transmisji. Umożliwiają bezpośrednie przesyłanie danych ze źródła do miejsca przeznaczenia, automatyczne przekazywanie ich oraz automatyczne sterowanie nimi.

Wiek informacji nie zabezpiecza jednak nowych środków technicznych i procesu zdobywania, przetwarzania oraz wykorzystania danych przed niszczeniem na tyle, aby ten atak stał się nierealny. Dlatego też jest to inny rodzaj prowadzenia walki informacyjnej, który można nazwać *zakłócaniem nieosobowym (technicznym)*.

Na podstawie powyższej analizy ze względu na kryterium dostępu, przestrzeń zakłócania informacyjnego można podzielić na:
— *osobową;*
— *nieosobową (techniczną).*

— *Osobowe zakłócanie informacyjne* to zespół przedsięwzięć polegających na zdobywaniu wiadomości o przeciwniku i rozpowszechnianiu odpowiednich informacji w jego wojskach w celu oddziaływania na jego morale (postawy, zachowania) i intencje, aby podjął niekorzystną dla siebie decyzję. Według poglądów amerykańskich do tego rodzaju przedsięwzięć zalicza się:

— wprowadzanie w błąd (Deception);

— działania psychologiczne (PSYOP — Psyhological Operation).

Zdaniem profesora K. Nożki wprowadzanie w błąd, dezinformacja oraz takie przedsięwzięcia jak pozorowanie, mylenie, ukrywanie są formami maskowania operacyjnego[62]. Natomiast A. Szydłowski[63], traktując maskowanie jako działalność perseweracyjną, ze względu na cel maskowania wyróżnia:

— wprowadzanie w błąd (dezinformowanie, pozorowanie);

— ukrycie (kamuflaż, zakrycie).

---

[62]K. Nożko: *„Walka o przewagę"*. Wydawnictwo MON, Warszawa 1985, s.157.
[63]A. Szydłowski: *Prakseologiczne aspekty maskowania*. W: *„Myśl wojskowa"*, 6/96, s. 53.

Powyższy podział jest częściowo zgodny z poglądami amerykańskimi, jeśli chodzi o wprowadzanie w błąd i ukrycie. Nie uwzględnia on jednak działań psychologicznych. Z powyższej analizy wynika, że najbardziej wskazany byłby podział osobowego zakłócania informacyjnego na:

— *wprowadzanie w błąd (dezinformacja, pozoracja);*
— *działania psychologiczne(mylenie).*

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:

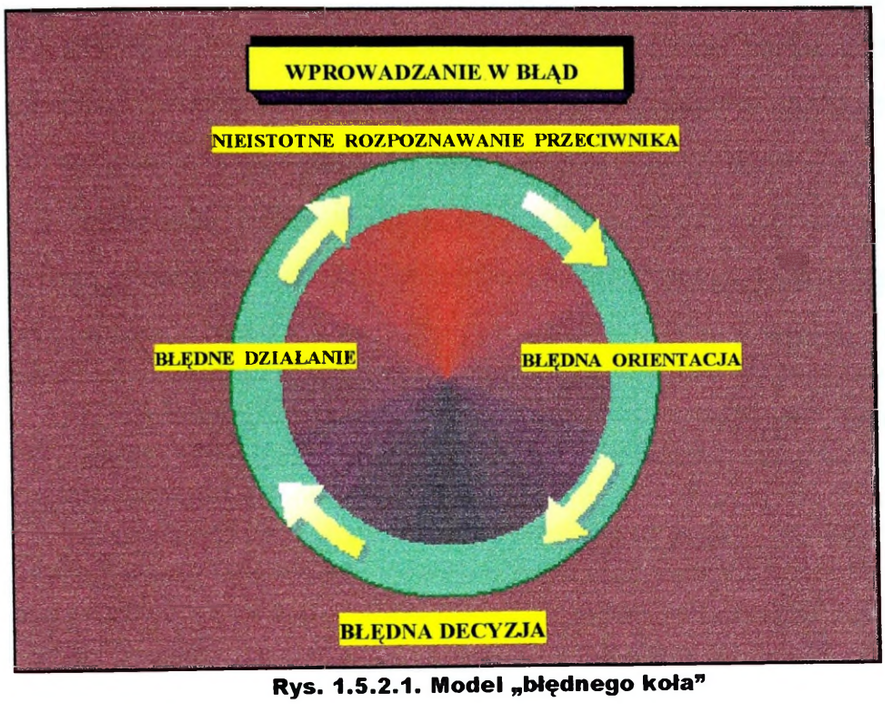
— nie zauważył przedsięwzięć wprowadzających go w błąd (mylących);
— oceni działania mylące — po analizie — jako prawdziwe;
— podejmie działania przeciwko pozorowanym celom i sytuacjom.

Efekty tego rodzaju zakłócania można zobrazować w postaci błędnego koła, w którym (rys. 1.5.2.1):

— 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.

W terminologii natowskiej wprowadzanie w błąd utożsamiane jest z prowadzeniem

— dezinformacji (disinformation);
— pozorowania (simulation).



Rys. 1.5.2.1. Model „błędnego koła"

Dezinformacja to wprowadzanie w błąd przez podanie nieprawdziwych (mylących) informacji[64]. W ujęciu wojskowym, to rozpowszechnianie nieprawdziwych wiadomości i dokumentów dla wprowadzenia w błąd przeciwnika co do zamiaru, organizacji i prowadzenia operacji lub walki, a także charakteru ich działania. Dezinformacja uprawiana przez podmiot działań może potencjalnie stanowić *in praxi* jeden z głównych elementów wprowadzania w błąd żołnierzy i ludności cywilnej kraju przeciwnika oraz jego mniejszości narodowej. Dezinformacją będzie takie oddziaływanie podmiotu działań na wojska i ludność przeciwnika, które oparte na przekazie danych nieprawdziwych doprowadzi do wyciągnięcia takich wniosków i przekonań, jakie będą zgodne z celem prowadzonych działań. Dezinformacja *ex professo* stawia sobie za cel realizację konsekwentnego programu działania zmierzającego do zastąpienia w świadomości, w przekonaniach poglądów uznanych za niekorzystne dla podmiotu oddziaływań na takie, które są korzystne dla sił prowadzących działania bojowe. Dezinformując, podmiot działań może się posłużyć dwoma modelami przekazu danych.

— Pierwszym jest model odbijający — deflekcyjny, w którym podmiot działań *ex professo* posługuje się nieprawdziwym źródłem przekazu informacyjnego, co powoduje, że jest on całkowicie nieznany przedmiotowi oddziaływań.

— Drugi z modeli — legitymizacyjny opiera się na zasadzie przekazywania odpowiedzialności za przekazywaną informację. Sprowadza się on do tego, że podmiot

[64] *Słownik języka polskiego*, t II, op. cit., s.390.

działań chcąc ukryć swoje autorstwo danego komunikatu *K1*, przekazuje go najpierw do tzw. podmiotu — nadawcy zastępczego, następnie pobiera od niego „swój" komunikat *K2* i wysyła do przedmiotu oddziaływań jako pochodzący „nie od siebie" lecz od uprzednio wybranego nieprawdziwego źródła informacji. Tym sposobem można przekazywać informacje, które w danej chwili nie są lub nie mogą być wiarygodne, ponieważ pochodzą ze źródła o niewiadomym pochodzeniu.

> *Na podstawie analizy literatury przedmiotu, możliwe wydaje się wyodrębnienie takich oto dwóch generalnych ograniczeń w aspekcie stosowania dezinformacji:*
> - *Dezinformacja może być stosowana tylko wtedy, gdy istnieje pewna grupa — „masa krytyczna żołnierzy" lub ludności cywilnej przeciwnika już zdezorientowana lub podatna na wpływ.*
> - *Dezinformacji nie wolno stosować „pod prąd", to znaczy niecelowe jest przekazywanie informacji, które nie tylko, nie wywołają dezorientacji, ale nawet mogą wzbudzić sprzeciw. Dezinformacja może potencjalnie pobudzać aberacyjne trendy w celu zaognienia sytuacji w szeregach wojsk przeciwnika i jego społeczeństwie, de facto jednak skuteczna potencjalnie będzie wtedy, gdy wykorzysta już istniejące ogniska zapalne.*

Powyższe ograniczenia wypływają bezpośrednio ze specyfiki oddziaływań dezinformacyjnych, które to w swej istocie polegają nie na tym, by przedmiot uwierzył w coś, co podsuwa podmiot, lecz na zmodyfikowaniu jego postaw i zachowań.

Działania dezinformacyjne powinny być: kompleksowe, wiarygodne, nieszablonowe, skryte, terminowe, zwielokrotnione i elastyczne.

Kompleksowość przedsięwzięć dezinformacyjnych odnosi się do stosowania jak najszerszego spektrum środków przekazu danych z uwzględnieniem wszystkich rodzajów sił zbrojnych i instytucji cywilnych oraz paramilitarnych sił prowadzących działania obronne.

Spójność oddziaływań dezinformacyjnych opiera się na przestrzeganiu zasady logicznego ciągu w prowadzonych przedsięwzięciach systemowych. Innymi słowy, dezinformacja winna mieć cel tożsamy z celem prowadzonych działań bojowych, zarówno przy użyciu środków orężnych, jak i nie orężnych.

Wiarygodność in praxi potencjalnie wyrażać się będzie w tym, by podmiot oddziaływań i przekazywane za jego pośrednictwem dane, stanowiły dla przedmiotu działań, na tle sytuacji polityczno - militarnej informacje prawdopodobne lub prawdziwe.

Nieszablonowość dezinformacji wydaje się konieczna i celowa. Polegać ona może na niepowtarzaniu już raz zastosowanych „chwytów" dezinformacyjnych. Innymi słowy, podmiot działań winien dążyć do sytuacji, gdzie kolejne podejmowane działania nie zawierają już wcześniej stosowanych sposobów, a kolejne oddziaływania mają charakter

nowatorskich rozwiązań podporządkowanych jednakże dążeniu do efektu synergicznego w realizowanym całokształcie działań bojowych.

Znajomość planów przeciwnika stanowi inheretny element procesu przygotowania oddziaływań dezinformacyjnych. Podmiot działań, wykorzystując wszelkie elementy rozpoznawcze zintegrowanego systemu rozpoznania sił zbrojnych (a także elementy rozpoznania agenturalnego), zdobywając niezbędne i w pełni wiarygodne informacje dotyczące planowanych działań zbrojnych i niezbrojnych przeciwnika oraz realizowanych przez jego struktury rozpoznawcze przedsięwzięć, może dostarczyć przeciwnikowi tak spreparowanych informacji, które będą dla niego stanowić przyczynek podjęcia takich, a nie innych działań.

Skrytość w oddziaływaniu dezinformacyjnym to warunek niezbędny dla prowadzenia jakichkolwiek działań opartych na technice „czarnej propagandy". Wydaje się celowe, by przedsięwzięcia działań dezinformacyjnych były planowane, organizowane i realizowane przez wyznaczone siły w ścisłej tajemnicy zarówno przed przeciwnikiem, jaki i przed wojskami własnymi, z wyjątkiem osób z kręgu planującego całokształt działań bojowych.

Terminowość niesie za sobą wymóg dostarczenia przeciwnikowi spreparowanych informacji w takim czasie, by mógł on zareagować właściwie i w odpowiednim czasie, z punktu widzenia na cel prowadzonych działań. Podjęcie działań dezinformacyjnych i wsparcie przekazanych nieprawdziwych danych rzeczywistymi działaniami innych sił i środków, *ex ante* doprowadzi do podjęcia przez siły przeciwnika pożądanych postaw i zachowań.

Zwielokrotnianie przedsięwzięć dezinformacyjnych stanowi element niezbędnego uwiarygodnienia przekazywanych preparowanych danych. Podmiot oddziałując na przedmiot może stosować wielość kanałów przekazywania informacji, hołdując zasadzie: „im więcej informacji wiarygodnych, z większej ilości wiarygodnych źródeł, tym potencjalnie większe prawdopodobieństwo przyjęcia pożądanych postaw i zachowań".

Elastyczność w działaniach dezinformacyjnych opiera się na zasadzie stosowania takich sposobów oddziaływania, które są w danej chwili, ze względu na zaistniałą sytuację militarną i polityczną, potencjalnie skuteczne. W tym celu konieczne wydaje się permanentne analizowanie, przez wydzielone siły, skuteczności prowadzonych oddziaływań skierowanych na wojska przeciwnika i jego ludność.

Pozorowanie polega na sztucznym tworzeniu „obrazu" (obiektu, czynności itp.) zbliżonego do rzeczywistego. Osiąga się je poprzez:

— tworzenie obiektów pozornych;
— pozorowanie innych form działań bojowych niż faktycznie prowadzone;
— stosowanie manewru pozornego oraz pozornych przedsięwzięć organizacyjnych;
— deformowanie obiektów rzeczywistych;
— tworzenie dowództw pozorujących istnienie nie istniejących oddziałów i związków taktycznych.

Zagadnienia działań pozornych zostały przedstawione w regulaminie SL USA FM-100-5, w którym pisze się o planie działań pozornych jako nieodłącznej części planu działań bojowych. Celem działań pozornych jest okłamanie przeciwnika, wprowadzenie go w błąd i osiągnięcie zaskoczenia.

Działania pozorne należy zdefiniować jako kompleks organizacyjnych, materiałowych i praktycznych zadań, zgodnych z celem i zadaniami operacji, miejscem, czasem oraz sposobem działania wojsk, przedsięwzięć, mających na celu zmylenie przeciwnika co do przyjętego rzeczywistego zamiaru walczących sił, ich składu, stanów, prawdziwych zadań i przewidywanych przedsięwzięć w toku przygotowywania i prowadzenia operacji. Działania pozorne należą do tych czynności, które w sposób pośredni wywierają wpływ na przeciwnika. Oddziałują bowiem na wyniki jego rozpoznania jako główne źródło danych. Jeżeli zostaną uznane za działania prawdziwe, sprawią, że decyzje będą błędne, a wykorzystanie systemów uzbrojenia — niecelowe. Chęć okłamania przeciwnika była, jest i pozostanie ważnym elementem przygotowania oraz prowadzenia walki i operacji. Będzie dowodem mistrzostwa dowódcy i jego zdolności narzucenia przeciwnikowi swej woli, przejęcia inicjatywy, zaskoczenia go, stworzenia jak najlepszych warunków własnym wojskom do osiągnięcia celu operacji. Dzięki prowadzeniu działań pozornych można osiągać wielkie sukcesy przy małych stratach ludzi, niskim zużyciu materiałów i czasu. W tym sensie działania pozorne pozostaną ściśle związane z zasadami sztuki operacyjnej, głównie zaskoczeniem.

Wyposażenie wojsk w coraz doskonalsze systemy rozpoznania ma zasadniczy wpływ na rozwój środków pozoracji uzbrojenia na polu walki. Umiejętne wykorzystanie urządzeń i obiektów pozornych pozwala znacznie zmniejszyć straty własne. Wymóg jaki powinien spełniać sprzęt pozorujący pole walki, to maksymalne utrudnienie przeciwnikowi możliwości rozpoznania elementów ugrupowania bojowego, systemów dowodzenia i ważnych obiektów infrastruktury obronnej oraz skierowanie jego wysiłku rozpoznawczego i uderzeniowego na rejony pozorne. Budowa wiarygodnych rejonów

i obiektów pozornych pozwala wprowadzić w błąd przeciwnika co do rzeczywistego stanu rozbudowy inżynieryjnej rejonu obrony, dyslokacji elementów ugrupowania bojowego i ważnych obiektów infrastruktury terenowej. Działania te zmuszają przeciwnika do rozproszenia wysiłku uderzeniowego, co z kolei zmniejsza prawdopodobieństwo zniszczenia elementów obrony. Sprzęt do pozoracji pola walki spełni swoje zadanie, jeśli jego najważniejsze parametry będą w maksymalnym stopniu zbliżone do rzeczywistych. Powinny to być środki umożliwiające budowę obiektów pozornych o bardzo zbliżonym do rzeczywistych charakterystykach wizualnych, termalnych i elektromagnetycznych. Takie możliwości posiada system DECEPTION — szwedzkiej firmy Barracuda. W większości są to obiekty wykonane w skali 1:1, pozorujące sprzęt bojowy, systemy rakietowe, mosty, bazy lotnicze itp. Obiekty te są szczególnie efektywne przy ataku z powietrza, ponieważ pilot ma zaledwie kilka sekund na identyfikację obiektu i podjęcie decyzji. Prawdopodobieństwo przeprowadzenia ataku na cel pozorny przy zastosowaniu właściwej techniki pozoracji jest bardzo wysokie. Rozproszenie wysiłku rozpoznawczego przeciwnika zwiększa szansę na przetrwanie elementów rzeczywistych obrony. Środki te będą ulegały ciągłemu rozwojowi, ponieważ pozwalają przy niskich nakładach finansowych znacząco zmniejszyć straty własne. Są to środki, których koszt stanowi około 0,25% ceny pozorowanego obiektu.

Działania psychologiczne na polu walki nazywane są często działaniami propagandowo — psychologicznymi ze względu na środki realizacji (słowo, dźwięk, obraz, gest, ruch czy światło) i stanowią nieodłączny element konfliktów zbrojnych.

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.

Jedną z form prowadzenia działań psychologicznych jest *manipulacja*. Termin ten nie jest jednoznaczny i trudny do zdefiniowania. Próby podejmowane na gruncie psychologii społecznej, socjologii i socjotechniki, nie dają jednoznacznych rezultatów[65]. Mówiąc o manipulacji, często *de facto* każdy człowiek otwiera usta po to tylko, by kimś manipulować. To właśnie instrumentalne podejście wydaje się być właściwe dla tego typu działań, ze względu na zadania, jakie realizuje podmiot tych oddziaływań i relacje, jakie zachodzą między podmiotem i przedmiotem tych działań. By zrozumieć istotę manipulacji, jej gnoseologiczne podstawy, celowe wydaje się rozpatrzenie tegoż pojęcia w kontekście wpływu społecznego i perswazyjnego oddziaływania na postawę i zachowanie człowieka. Każdy żołnierz, członek społeczności bezpośrednio lub pośrednio zaangażowanej w walkę zbrojną, podlega pewnemu wpływowi społecznemu.

> *Na podstawie analizy literatury przedmiotu można wnioskować o różnego rodzaju percypowaniu wpływu manipulacji, a mianowicie:*
> - *Po pierwsze — w zachowaniu osoby (lub grupy) zawarte są wyraźne wskazówki świadczące o tym, że osoba ta wywiera wpływ na inną osobę lub grupę w celu zmiany, modyfikacji postawy i zachowania.*
> - *Po drugie — wskazówki świadczące o wywieranym wpływie są ukryte, lecz dostępne poznaniu osoby (grupy) będącej przedmiotem wpływu po dokonaniu przez nią odpowiedniej analizy zachowania lub intencji osoby wywierającej wpływ.*
> - *Po trzecie, osoba (grupa) będąca przedmiotem wpływu, ani jej świadomość, nie zdaje sobie sprawy z wywieranego wpływu.*
> - *Po czwarte — percepcja danych, jawnych bądź ukrytych, świadczy o tym, czy mamy do czynienia z całkowicie lub częściowo jawnymi metodami wpływu społecznego (wpływaniem na konformizm perswazją), czy też manipulacją.*
> - *Po piąte — manipulacja odnosi się do trzeciego rodzaju percypowania wpływu — może być wykorzystywana jako technika wpływania na behawioralny komponent postawy*[66].
> - *Po szóste — epistemologiczną istotą oddziaływania manipulacyjnego jest proces sterowania, który prowadzi do realizacji celów podmiotu działań — sprzecznych ex professo z celami i obiektywnym interesem własnych sił prowadzących działania bojowe. Innymi słowy manipulację można znaleźć tam, gdzie odpowiedni przekaz informacyjny (sterowanie) będzie modyfikował postawy i zachowania żołnierzy oraz ludności przeciwnika, tak że sterowana grupa społeczna (pododdział), nie urzeczywistni (poniecha lub zaniedba) jakichkolwiek*

---

[65]Maliszewski W.: *„Oddziaływanie psychologiczne w operacji obronnej"*. Rozprawa doktorska, AON, Warszawa 1998. Ponadto: M. Montana Czarnawska: *„Jak się bronić przed indoktrynacją"*, Warszawa 1997; K. Czuba: *„Media i władza"*, Warszawa 1995; G.H. Green, C.Cotter: *„Nie pozwól sobą manipulować"*, Warszawa 1997; P. Honey: *„Jak radzić sobie lepiej z ludźmi"*, Warszawa 1997; J. Kirschner: *„Manipulować – ale jak?"*, Warszawa 1994; R. Nawrat: *Manipulacja społeczna - przegląd technik i wybranych wyników badań*. W: *„Przegląd Psychologiczny"* 1/1989, s. 125 - 154; J.Reykowski: *„Osobowość a społeczne zachowanie się ludzi"*, Warszawa 1976.

[66]Por. R. Nawrat, op. cit., s.125 - 127.

starań ważnych dla własnej pomyślności, własnych interesów bądź celów tego, kto formalnie nią kieruje i dowodzi[67]*. Manipulacją będą wiec takie działania, które zmuszają przedmiot do przyjmowania takich postaw i generowania zachowań, czynienia czegoś, czego przedmiot nie chce albo sobie nie życzy. Jest to wyrafinowane sterowanie świadomością przedmiotu działań przy wywoływaniu u nich wrażenia jakoby to, co czynią, wynikało z ich własnych planów i własnych wypracowanych decyzji.*

Manipulacja operuje uczuciami i wywołuje emocje. Wyznaczone siły, przekazując spreparowane dane, biorąc pod uwagę to, iż działania te prowadzone są w gęstym otoczeniu społecznym, a przedmiot cierpi na tzw. głód informacyjny, są w stanie wywołać u przedmiotu szereg emocji i uczuć w celu sprowokowania określonych zachowań czynnościowych i werbalnych. Podmiot będzie w tym wypadku permanentnie dążył do uaktywnienia mechanizmu w celu ograniczenia bądź całkowitego zablokowania mechanizmów kontrolnych świadomości przedmiotu, który umożliwi narzucenie wzorców postaw i zachowań pochodzących od podmiotu.

Konkludując, pojmując emocje i ich efekt w postaci określonych postaw oraz zachowań, jako pewien proces kompensacji deficytu informacyjnego, można pokusić się o przedstawienie ich jako iloczynu motywu podjęcia określonego zachowania i różnicy danych niezbędnych do normalnego procesu decyzyjnego oraz danych posiadanych.

Najczęściej spotykanymi sposobami manipulowania procesem informacyjnym w celu kształtowania postaw i zachowań człowieka, są:
— *przekazywanie danych nieprawdziwych;*
— *preparowanie i przesyłanie do przedmiotu danych nieważnych lub mało ważnych z pominięciem najważniejszych;*
— *przekazywanie danych o dużym znaczeniu jako marginalnych;*
— *udostępnianie danych preparowanych w celu wywołania określonych interwencji;*
— *przesyłanie danych wieloznacznych, utrudniających zrozumienie;*
— *generowanie nadmiaru danych , by spowodować tzw. „chaos informacyjny".*

Pierwszy sposób polega, *exempli causa,* na podaniu przedmiotowi oddziaływań danych z gruntu nieprawdziwych, jednak takich, które w podświadomości tkwią jako możliwe do wystąpienia.

Drugi sposób odnosi się do przekazania danych skierowanych do żołnierzy wojsk przeciwnika i jego ludności na zasadzie przedstawienia rzeczywistego obrazu w krzywym zwierciadle.

[67]Por. P. Kołtunowski, op. cit., s. 180 -181.

Kolejna technika opiera się na założeniu, że każda postać danej, nawet sensacyjna, przekazana w dalszej kolejności całokształtu komunikatu informacyjnego staje się mniej ważną, nieznaczącą wiadomością, na którą przedmiot nie zwróci uwagi.

Czwarta technika *in praxi* może być sprowadzona do poruszania, wywoływania tzw. tematów dyżurnych. Permanentne przekazywanie danych (np. o rzezi ludności cywilnej) w tym wypadku może stanowić swoisty impuls do podjęcia działań interwencyjnych, to znaczy dociekania prawdy, ucieczki z pola walki i innych tego typu zachowań.

Przekazywanie danych wieloznacznych, stereotypowych może doprowadzić u ich odbiorcy (przedmiotu oddziaływań) do wytworzenia przekonania o tym, co ważne z punktu widzenia celu prowadzonych działań. Np. informacja o „pełnej izolacji strony przeciwnika w trakcie rozmów na forum ONZ" niesie za sobą treść z pewnością trafiającą do świadomości przedmiotu, że jego rząd, kraj i naród jest izolowany. Dane o tym, że rozmowy na forum ONZ toczą się nadal, jest „rozmydlona" i *ex ante* nie dostrzegana przez przedmiot oddziaływań.

Ostatni sposób to przekazywanie danych w nadmiarze, prowadzące do „chaosu informacyjnego". Podmiot może zasypać przedmiot działań tak dużą ilością danych o faktach i zjawiskach pola walki, że spowoduje u niego brak wrażliwości na istotne i ważne wiadomości.

> *Jak wykazują doświadczenia z minionych konfliktów zbrojnych, szczególnie wojny w Zatoce Perskiej, dezinformacja i manipulacja 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.

Techniczne zakłócanie informacyjnego 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)[68]. 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.

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

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

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.

Zakłócanie informatyczne będzie jednym z najważniejszych sposobów walki informacyjnej w XXI wieku. Przekonały się o tym Stany Zjednoczone, których komputery, zarówno w sferze cywilnej jak i wojskowej są wrażliwe na atak informatyczny. Systemy komputerowe Departamentu Obrony 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. Włamywacze dostają się do komputerów, ponieważ potrafią ominąć specjalne zabezpieczenia. Najczęściej monitorują wybraną sieć, a następnie podszywają się pod jakiś zaufany komputer w tej sieci i przechwytują informacje, 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 informacje wyświetlane na ekranie komputera.

Jim Settle, konsultant ds. bezpieczeństwa FBI, jest przekonany, że przyszła wojna będzie polegać na blokowaniu dostępu do informacji i wprowadzaniu w błąd strony przeciwnej. W odróżnieniu od zasobów nuklearnych, środki walki informacyjnej (zakłócania informatycznego) są osiągalne prawie dla każdego. Celem tej walki będzie zarażenie wirusem programów komputerowych przeciwnika, tak aby był niezdolny do podejmowania jakichkolwiek działań. Skoro systemy obrony większości krajów oparte są na systemach komputerowych, wystarczy zakłócić pracę tego systemu, aby przeprowadzić skuteczny atak. Wpadli na to Amerykanie podczas wojny z Irakiem. Pół roku wcześniej sprzedali do Iraku drukarki komputerowe, których odbiorcą było wojsko. Wewnątrz drukarek były zainstalowane specjalne mikronadajniki, które codziennie podawały swoją pozycję do satelity. W ten sposób można było zlokalizować cele wojskowe w Iraku. Lotnictwo amerykańskie bombardowało te pozycje, na których znajdowały się drukarki.

Wnioski z podrozdziału 1.5.2.

- *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:*

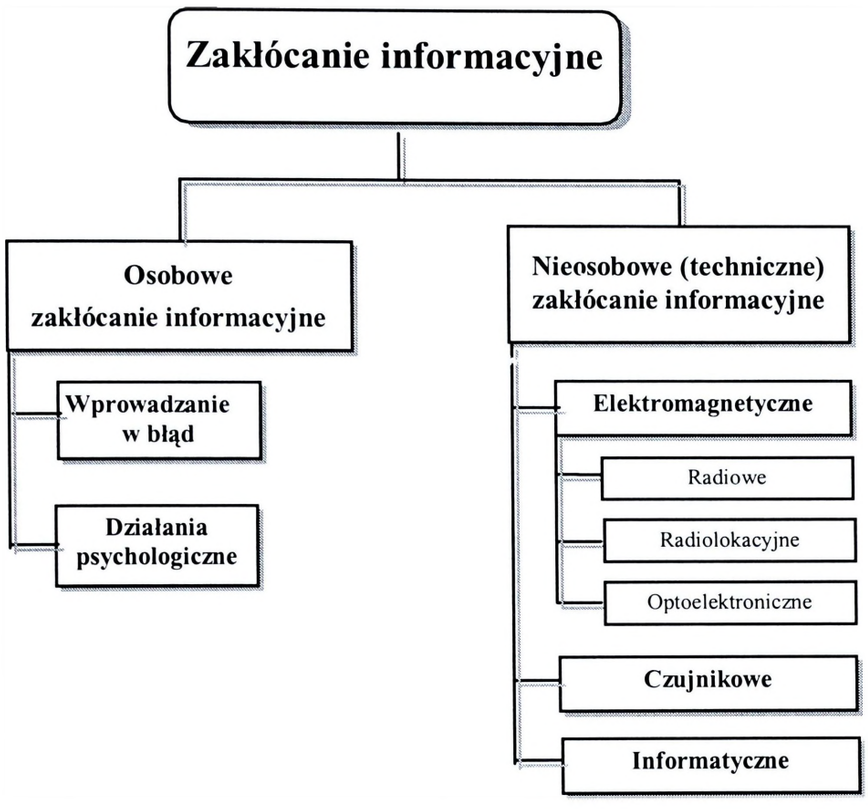
— *Posiadanie wiedzy o stanie i funkcjonowaniu procesów informacyjnych u przeciwnika, o wykorzystywanej przez niego technice, metodach zdobywania i gromadzenia informacji, o dowodzeniu itp. Wiedza ta jest niezbędna głównie po to, aby móc przygotować od strony technicznej, metodologicznej i organizacyjnej 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.*
- *Przestrzeń zakłócania informacyjnego tworzą zbiory następujących elementów —patrz rysunek niżej.*



Podział przestrzeni zakłócania informacyjnego

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[69]. Nie ma istotnych powodów, aby

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

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 wymaga 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. We wrześniu 1994 r. Sejm 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.

W tradycyjnych systemach dane gromadzone były w sposób zdecentralizowany. Wynikało to z tego, że żadne stanowisko pracy, żadna osoba nie posiadała pełnej informacji na temat określonego zagadnienia, co zmniejszało np. zagrożenie pełnego ujawnienia danych. Przechowywanie danych było tylko w niewielkim stopniu sformalizowane. W związku z tym jedynie niewielka liczba osób związanych bezpośrednio z określoną działalnością umiała te dane wykorzystać. Dla innych były one nieczytelne. Jeśli chodzi o zabezpieczenie danych, systemy te stwarzały niewątpliwie wiele okazji do wystąpienia błędów. Ponieważ jednak istniała świadomość tego, wprowadzono liczne stanowiska kontroli poprawności danych, zmniejszając w ten sposób prawdopodobieństwo, że błąd przemknie się niezauważenie i spowoduje w dalszym biegu przetwarzania narastające zniekształcenie informacji.

Wprowadzenie automatycznego przetwarzania danych (APD) spowodowało niespotykaną dotychczas centralizację. Pociąga to za sobą w konsekwencji uzależnienie całej działalności od ośrodka APD. W ośrodku tym rejestrowane są wszystkie treści niezbędne do funkcjonowania określonej organizacji oraz koncentruje się w nim cały system kontroli i sterowania.

Dodatkowo wzrasta wrażliwość APD na wszelkiego rodzaju zagrożenia na skutek coraz szerszego wprowadzania systemów przetwarzania z końcówkami zdalnego dostępu (terminalami). Dane mogą być zdalnie pobierane lub modyfikowane, praktycznie bez możności zidentyfikowania, kto rzeczywiście dokonuje tych czynności. Z uwagi na to, że ani zarejestrowane zapisy, ani manipulowanie nimi nie może być bezpośrednio kontrolowane, za ścisłość i prawdziwość tych zapisów odpowiadają w równej mierze ośrodek APD oraz korzystający z usług tego ośrodka użytkownicy.

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 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:*
  — *osobową obronę informacyjną;*
  — *nieosobową (techniczną) obronę informacyjną.*

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;*
— *maskowanie.*

Obrona psychologiczna polega na utrzymywaniu wysokiego morale i dobrego stanu psychicznego człowieka. 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*[70] *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"*[71].

Maskowanie to utrudnianie przeciwnikowi dostrzeżenia pozycji obronnych przez wizualne dostosowanie ich do otoczenia[72]. Można przyjąć, że maskowanie jest reakcją na

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

rozpoznanie. Podstawą takiego twierdzenia jest powszechnie znane prawo *akcji* i *reakcji*. Z jego sensu wynika jednoczesność występowania akcji — tu rozpoznania i reakcji — maskowania. Tymczasem oprócz reakcji związanych z określoną akcją istnieją też działania opóźnione, wyprzedzające i profilaktyczne. Działania profilaktyczne trudno nazwać reakcją, albowiem jeszcze żadna akcja nie występuje. Co jest więc przyczyną działań profilaktycznych? Tą przyczyną jest domniemanie o możliwości wystąpienia akcji. Czyli inaczej — zagrożenia wystąpieniem określonej akcji.

Analogicznie ująć można maskowanie. Prowadzone jest ono przede wszystkim wyprzedzająco, ale i po zakończeniu rozpoznania. Wobec tego również o maskowaniu można mówić, że jest ono reakcją na prowadzone przez przeciwnika rozpoznanie i na zagrożenie nim. Dlatego za przyczynę maskowania uznać można proces rozpoznania oraz przekonanie o zagrożeniu nim. W stwierdzeniu tym znajduje się uzasadnienie zasady ciągłości maskowania. nakazuje ona prowadzenie działań maskujących we wszystkich etapach walki.

- *Maskowanie ma na celu:*
— *ukrycie sił i środków przed rozpoznaniem przeciwnika;*
— *oszukanie przeciwnika co do położenia wojsk i prowadzonych przez nie działań wojennych;*
— *utrudnienie przeciwnikowi skutecznego oddziaływania elektromagnetycznego i ogniowego oraz podejmowania prawidłowych decyzji.*
- Za domenę maskowania uważa się przede wszystkim ukrywanie.

Ukrywanie ma na celu uczynienie maskowanego 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. Sąd ten znajdzie odzwierciedlenie w meldunku rozpoznawczym i będzie dalej skażał przedstawienia kolejnych podmiotów rozpoznania. A o to przecież chodzi prowadzącemu rozpoznanie.

Druga forma ukrywania – *kamuflaż* polega na obniżeniu kontrastu maskowanego przedmiotu poniżej wartości progowej. Powoduje to, najogólniej rzecz biorąc, zlanie się kształtów, barw i wypromieniowanej energii (np. cieplnej) maskowanego 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 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.[73] Swoja 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 w maskowaniu rolę szczególną z uwagi na fakt, że dotyczy ono bezpośrednio rzeczywistego przedmiotu rozpoznania. Tym też można tłumaczyć priorytet ukrywania w maskowaniu bezpośrednim.

W wyposażeniu współczesnych armii znajduje się wiele środków przeznaczonych do maskowania 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.

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;*

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

— *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 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 trojański, 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[74].

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. Do najczęściej stosowanych środków maskowniczych należy zaliczyć:

— siatki (pokrycia) maskujące (zespołowe środki maskowania), które wykonywane są z tworzyw sztucznych i tkanin bawełnianych;

— farby do malowania deformującego (farby na dyspersji alkidowej, poliuretanowej, farby rozpuszczalne w wodzie);

---

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

— zestawy do maskowania sprzętu bojowego (zestawy Barracuda, składające się z kilku dużych parasoli ustawionych bezpośrednio na sprzęcie lub obok niego oraz tzw. maski deformujące);

— środki maskowania przeciwradiolokacyjnego (pokrycia przeciwradiolokacyjne w postaci siatek oraz różnego rodzaju materiały radioabsorpcyjne, paski folii metalowej);

— środki do maskowania przed rozpoznaniem termalnym (osłony termiczne, maty tekturowe, ekrany termoizolacyjne);

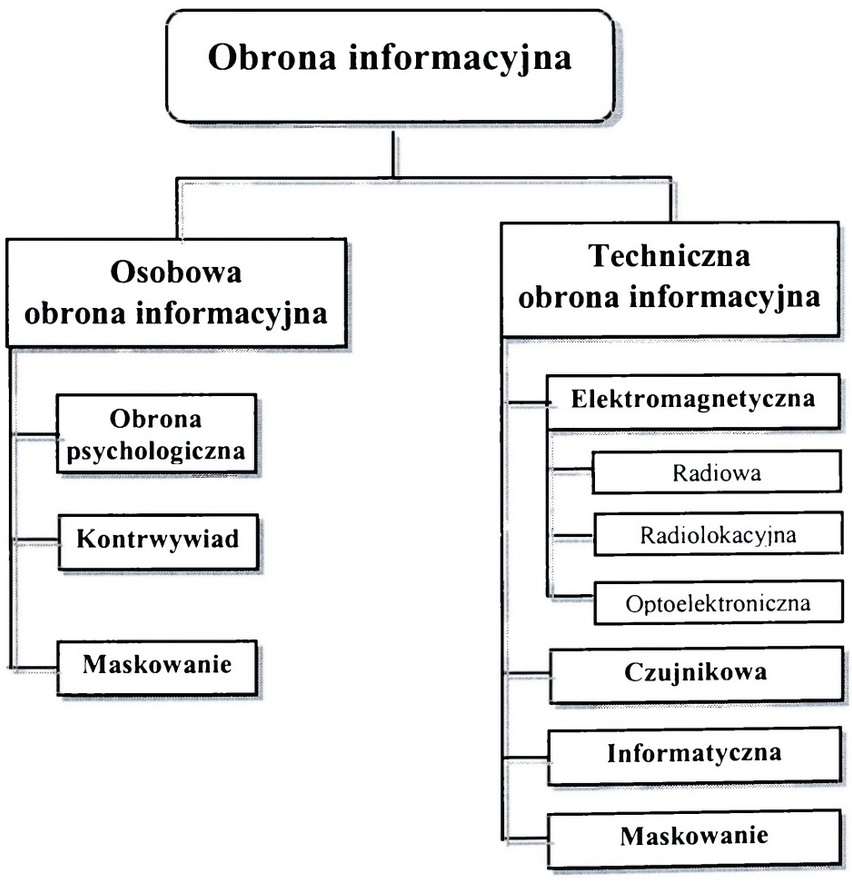
— piany maskujące (o charakterze krótkotrwałym, trwałym, emisyjne);

— środki systemu maskowania aktywnego (urządzenia ostrzegające o opromieniowaniu obiektu wiązką laserową lub radiolokacyjną, wyrzutnie środków dymnych, wyrzutnie substancji i ładunków emitujących energię cieplną, cele radiolokacyjne).

Dobrym sposobem jest kombinowane jednoczesne odpalanie zasobników z paskami folii i flarami.

Wnioski z podrozdziału 1.5.3.

Przestrzeń obrony informacyjnej tworzą zbiory następujących elementów— patrz rysunek niżej.



Podział przestrzeni obrony informacyjnej

1.6. Kluczowe efekty poznania

1. *Na podstawie analizy literatury przedmiotu badań należy stwierdzić, że wyjaśnienie pojęć dotyczących walki informacyjnej i informacji staje się obecnie niezbędne ze względu na dużą różnorodność podejść (różne ich ujmowanie i znaczne różnice w rozumieniu potocznym i specjalistycznym). Dotychczasowe próby zdefiniowania walki informacyjnej są niezadowalające ze względu na to, że obejmują one głównie jej aspekt wojskowy i nie traktują problemu jednoznacznie. Dużo więcej kontrowersji budzi interpretacja pojęcia informacja, które jest używane w wielu różnych i odmiennych znaczeniach, od najbardziej ogólnego, filozoficznego: „informacja jest odbiciem realnego świata", do najbardziej wąskiego, praktycznego: „informacja to wszelka wiadomość". Powodem takiego stanu rzeczy jest fakt, że teoria informacji stanowi dziedzinę niezbadaną jeszcze dostatecznie dogłębnie, kryjącą w sobie wiele nieoczekiwanych właściwości. Podstawy teoretyczne w tym zakresie dotyczą najbardziej ogólnych zagadnień związanych z techniką informacyjną. Wieloznaczność terminu informacja prowadzi do powstania dodatkowych, nieścisłych pojęć oraz powoduje niejednoznaczność w komunikowaniu się. Dlatego też w celu określenia jednoznaczności i ścisłości języka problemu należało zdefiniować takie pojęcia, jak: informacja, dane, sygnał informacyjny, sygnał sterujący, komunikat, system informacyjno — sterujący, walka informacyjna.*

   „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". W każdym rodzaju walki (dotyczy to także walki informacyjnej) organizowane są wojskowe i cywilne systemy informacyjno — sterujące. Każda z zaangażowanych stron A i B dąży do tego, aby jej system funkcjonował lepiej. Wykorzystując tylko te systemy, jedna ze stron może obezwładnić, czy nawet zniszczyć, istotne elementy infrastruktury cywilnej i wojskowej drugiej strony. Co więcej może ukryć swoją tożsamość, a państwo zaatakowane nie będzie w stanie jednoznacznie wskazać agresora. Potencjalny przeciwnik jest w stanie zadać poważne straty bez użycia tradycyjnych środków walki oraz narażania własnych sił. Wynika więc z tego, że systemy informacyjno-sterujące tworzone są przez człowieka w aspekcie spełniania konkretnych potrzeb wynikających z realizacji jakiegoś działania celowego. Oznacza to, że są one nierozerwalnie związane z każdym działaniem celowym, realizowanym w warunkach kooperacji negatywnej wzajemnej. Ich niezakłócone funkcjonowanie względnie zniszczenie lub zdezorganizowanie przyczyniać się będzie, w sposób pośredni ale bardzo istotny, do osiągnięcia celów głównych w konkretnych działaniach. Dlatego taką kooperację negatywną wzajemną, w której cel destrukcyjnego oddziaływania skoncentrowany jest na systemach informacyjno — sterujących przeciwnych sobie stron można nazwać walką informacyjną.

2. *„Przedmiot walki informacyjnej". Na polu walki każda ze stron dąży do uzyskania przewagi czasowej i jak najlepszej precyzji działania. Dlatego też stara się, aby jej system informacyjno — sterujący funkcjonował sprawnie, skutecznie i skrycie. Innymi słowy, obydwie strony zmierzają do tego, aby jej źródła rozpoznania zdobyły ze zbiorów danych o przeciwniku jak najwięcej tych postaci, których posiadanie pozwala identyfikować jego stan aktualny i zamiary działania. Jest to jednak trudne do realizacji dlatego, że systemy te funkcjonują w otoczeniu zakłóceń. Są narażone na*

zakłócenia zarówno losowe, jak również celowe. System informacyjno — sterujący funkcjonuje w otoczeniu, które do spełnianych przez niego funkcji wnosi ciągle pewną entropię informacyjną oraz destrukcję fizyczną do nośników danych (do sygnałów informacyjnych lub sterujących), jak również do źródeł danych, przetworników i układów odbierających, a w tym i do zmysłów człowieka. Wynika z tego, że walka informacyjna ulokowana jest częściowo wewnątrz systemu informacyjno — sterującego, a częściowo — w jego otoczeniu. Uogólniając można stwierdzić, że przedmiotem walki informacyjnej są systemy informacyjno — sterujące i ich otoczenie.

3. *„Narzędzia walki informacyjnej". 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.*
4. *„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;*

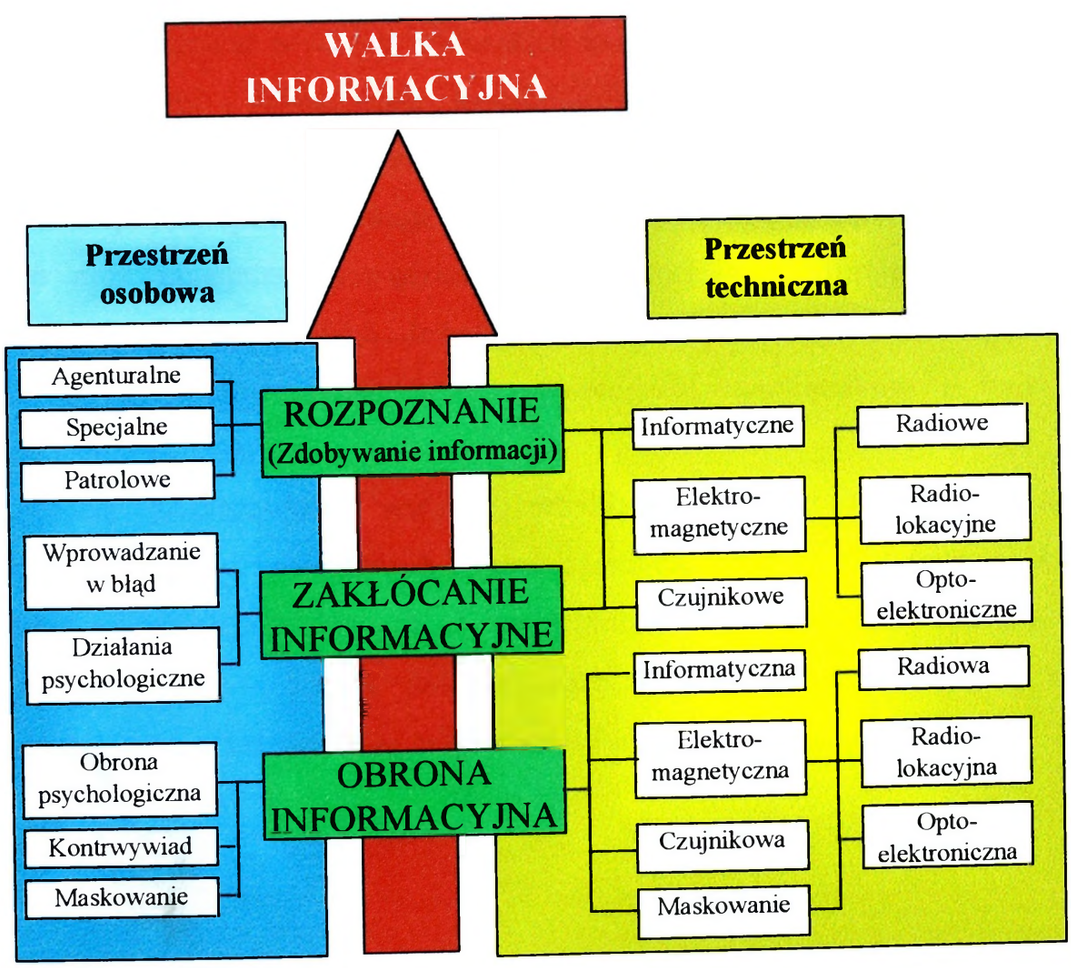
   „Podprzestrzeń zdobywania informacji" (rozpoznania) to układ skoordynowanych elementów dostosowanych do spełniania swej roli w środowisku elektromagnetycznym, akustycznym, magnetycznym i chemicznym, przez których pryzmat możliwe jest identyfikowanie aktualnego stanu pola walki.

„Podprzestrzeń zakłócania informacyjnego" to układ skoordynowanych elementów dostosowanych do wnoszenia entropii informacyjnej do komunikatów i powodowania destrukcji fizycznej nośników tych komunikatów i nośników danych.

„Podprzestrzeń obrony informacyjnej" to układ skoordynowanych elementów, których celem jest uniemożliwienie i utrudnienie zdobywania danych o fizycznej naturze aktualnego i planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania oraz uniemożliwienie i utrudnienie wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do ich nośników.

„Przestrzeń osobowej walki informacyjnej" tworzą narzędzia i procesy dostosowane do oddziaływania w sferze środowiska informacyjnego, które jest bezpośrednio postrzegalne zmysłami ludzkimi.

„Przestrzeń technicznej walki informacyjnej" tworzą wszelkie narzędzia i procesy dostosowane do oddziaływania w sferze środowiska informacyjnego, które jest bezpośrednio niepostrzegalne zmysłami ludzkimi.



Podział przestrzeni walki informacyjnej

„Wojna przyszłości już się zaczęła,
kto dziś jej nie dostrzeże — ten jutro
będzie manipulowany"[75].

2. GENEZA WALKI INFORMACYJNEJ.

Nauka wojenna zawsze zajmowała się bardzo rozległym wachlarzem problemów mniej lub bardziej dostosowanym do złożoności zjawiska, jakim jest wojna oraz do wymagań, jakie stawiała w tym zakresie szeroko rozumiana praktyka i teoria. Myśliciele i filozofowie dążyli do wyjaśnienia istoty wojny, jej sensu lub bezsensu, jej podstawowych prawidłowości rozwojowych, związków i zależności zewnętrznych i wewnętrznych, oraz do stworzenia najogólniejszej systematyki wojen. Historycy natomiast próbowali dokonać możliwie pełnej i pouczającej oceny tych wydarzeń, wyciągnąć z nich ważne wnioski dla współczesnych i potomnych.

Przekazywanie doświadczeń wojennych ma ważne znaczenie naukowo badawcze, szkoleniowe i dydaktyczno-wychowawcze[76]. Studia z doświadczeń wojennych pozwalają młodej kadrze zdobywać wiedzę o wielorakich formach prowadzenia działań wojennych, o ich specyficzności i konieczności kształtowania określonych umiejętności, a także o sposobach przygotowania podwładnych do działania w ekstremalnych sytuacjach na polu walki. Edukacja historyczna pomaga więc w rozwiązywaniu bieżących zadań szkolenia bojowego oraz zagadnień prowadzenia współczesnej walki zbrojnej. Dla tego też konieczne jest opisywanie tych doświadczeń oraz badanie nowych, dotychczas nie ujawnionych materiałów archiwalnych, autobiografii, pamiętników i innych prac poświęconych walce zbrojnej.

Poniżej przedstawiono wybrane przykłady bitew z okresu starożytności, średniowiecza, czasów nowożytnych i współczesnych. Ukazują one rangę i znaczenie, jakie nadawano walce informacyjnej na całym świecie. Nie oznacza to jednak, że były to bitwy najważniejsze — jest to zresztą trudne do obiektywnego ustalenia. Ponadto uwypuklono bitwy, w których dużą rolę odegrali Polacy.

---

[75] K. Peterson, U. Pracht: *Information warfare*. W: *„Soldat und Technik"*, 12/95.
[76] J. Kunikowski: „Człowiek a technika wojenna", AON, 1995, s. 22.

2.1. Analiza doświadczeń wojennych z przygotowywania i prowadzenia 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[77], 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, 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 gruntowniej, 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,

[77]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.

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".[78]

> *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;*
> *— 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[79].

> *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;*

---

[78]Sun Tzu: *Sztuka wojny*. Wydawnictwo Przedświt, Warszawa 1994, s.116.
[79]D. Strasburger: *„Zasady sztuki wojennej"*. Wydawnictwo Bellona, Warszawa 1996, s.17.

— 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.

Niestosowanie elementów walki informacyjnej było z kolei przyczyną klęski Rzymian w roku 9 n.e. w bitwie z Germanami, w Lesie Teutoburskim. Dowódcą trzech legionów rzymskich (około 18 tys. żołnierzy) był Publis Quintilius Warus, pełniący wcześniej obowiązki gubernatora Syrii. Jego zadaniem było stłumienie buntów na ziemiach germańskich. Posiadając dużą przewagę liczebną i wyszkolonych żołnierzy, był tak pewny siebie, że w ogóle nie prowadził żadnego rozpoznania ani też maskowania swoich wojsk. Uważał, że rozruchy mają charakter lokalny, dlatego też nie zarządził stanu pogotowia dla wojsk oraz pozwolił żołnierzom zabierać ze sobą rodziny.

Cheruskowie pod wodzą Arminiusa wiedzieli, że łatwo wpada w zasadzkę ten dowódca, który czuje się całkiem bezpiecznie. Dlatego też przeprowadzili rozpoznanie przeciwnika i terenu oraz wybrali jak najdogodniejsze miejsce do prowadzenia bitwy. Ponadto Arminius wywołał niewielkie powstanie (element zakłócania informacyjnego), licząc na to, że Warus zechce osobiście zbadać sytuację na miejscu, a wtedy zaatakuje go w Lesie Teutoburskim. Wuj Arminiusa, który nie darzył bratanka sympatią, ostrzegł Warusa o zamiarach swego krewnego, ale ten zlekceważył wiadomość, ponieważ uznał, że jest ona nieprawdziwa.

Rzymianie zostali zaatakowani przez Cherusków nocą, w terenie otoczonym zewsząd bagnami. Ponadto zerwała się gwałtowna ulewa, połączona z huraganem, łamiąc drzewa i zamieniając leśne ścieżki w błoto. Spowodowało to przerażenie wśród legionistów, a ponadto nie mieli oni możliwości rozwinięcia szyku. Warus i jego wyżsi oficerowie popełnili samobójstwo, aby nie dać się wziąć żywcem. Kilku oddziałom jazdy udało się przebić i uciec, ale cała reszta — żołnierze, kobiety i dzieci — została zabita w lesie.

Biorąc pod uwagę same fakty, wydawać by się mogło, że zasadzka zorganizowana przez Cherusków była przyczyną klęski Rzymian. Analizując fakty gruntowniej należy stwierdzić, że to właśnie elementy walki informacyjnej (dokładne rozpoznanie, wprowadzenie przeciwnika w błąd oraz ukrywanie wojsk własnych), zastosowane przez plemiona germańskie przyczyniły się do uzyskania zaskoczenia nad legionami. Rzymianie natomiast zlekceważyli prowadzenie rozpoznania i obrony informacyjnej, w wyniku czego znaleźli się w sytuacji bez wyjścia. Pomimo przewagi liczebnej, lepszego uzbrojenia i wyszkolenia ponieśli całkowitą klęskę.

Znaczenie informacji z pełną ostrością dostrzegał też chan Bułgarii Krum. Potwierdzeniem tego może być bitwa pod Pliską, która rozegrała się w 811r. Cesarz Bizancjum, Nikefor I sformował armię w sile 70 000 żołnierzy, do której dołączył się jego syn Staurakios oraz jednostki z Azji Mniejszej i Tracji. Bizantyńczycy opanowali miasto Pliskę i zamordowali ponad 12000 mieszkańców, nie rozbili jednak armii bułgarskiej. Krum wiedział, że nie wygra z Bizancjum w otwartym polu. Uznał zatem, że wykorzystując doskonałą znajomość terenu (przewaga w rozpoznaniu) oraz stosując maskowanie (obrona informacyjna) i pozorowanie (zakłócanie informacyjne), zwabi armię cesarską w zasadzkę. Nikefor natomiast upojony sukcesem zapomniał o tym. Przestał stosować jakiekolwiek środki ostrożności, a przede wszystkim nie prowadził rozpoznania terenu i przeciwnika. Innymi słowy, zlekceważył znaczenie zdobywania informacji o przeciwniku, jego obrony informacyjnej i zakłócania informacyjnego. W następstwie tego jego wojska dostały się w zasadzkę, którą stanowiła głęboka dolina górska znajdująca się na północ od Pliski. Bułgarzy zablokowali wcześniej wyjście, a następnie wejście palisadą. Skaliste i wysokie góry po obu stronach doliny uniemożliwiały jakąkolwiek ucieczkę żołnierzy armii cesarskiej. Jedynym rozwiązaniem dla nich stało się przebicie przez jedną z palisad. Armia Bizancjum, chociaż liczebnie wielokrotnie przewyższająca Bułgarów, nie podjęła próby przebicia się przez palisady. Widząc to, Bułgarzy zaatakowali niczego nie spodziewających się Bizantyńczyków. Wojska Nikefora zostały w mgnieniu oka rozbite. W walce zginął również sam cesarz.

> *Konstatując można stwierdzić, że klęska Bizancjum była efektem stosowania przez Bułgarów elementów walki informacyjnej. Chan Krum, zdając sobie sprawę z tego, że nie pokona liczniejszego przeciwnika w walnej bitwie, dokładnie rozpoznał teren i wybrał najkorzystniejsze dla siebie miejsce do prowadzenia bitwy. Ukrył swoje wojska, co można utożsamiać z obroną informacyjną. W wyniku prowadzenia działań pozornych (zakłócanie informacyjne) wprowadził w błąd przeciwnika, który źle ocenił sytuację i znalazł się w bardzo niekorzystnej sytuacji. W efekcie tego Bizantyńczycy ponieśli całkowitą klęskę, mimo przewagi liczebnej.*

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[80]. 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

[80]S. Kałużyński: *„Imperium mongolskie"*, Warszawa 1970, s.76 - 82.

liczyły w przybliżeniu 150 do 200 tysięcy żołnierzy. Hordy Mongołów znane jako „RAND"[81], 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.*

Kolejnym przykładem może być bitwa pod Bannockburn z 1314 roku. Edward II, król Anglii, wyruszył do Szkocji na odsiecz Anglikom oblężonym w zamku Stirling. Dysponował siłą 17 tysięcy rycerzy oraz dużą loczbą łuczników. Szkoci mogli przeciwstawić mu tylko 6 tysięcy piechurów i 500 jeźdźców. Jak wiadomo, druzgocącą klęskę ponieśli Anglicy, a sam król ledwie zdołał ujść z pola bitwy tylko z 500 rycerzami. W historii fakt ten tłumaczy się tym, iż Anglicy dali się wciągnąć w bitwę na terenie pełnym grzęzawisk i stawów, położonym tuż przy ujściu rzeki, której poziom zmieniał się podczas przypływów morza. Pokonując grząski teren nigdzie nie mogli znaleźć twardego gruntu — a kiedy udało im się przejść na drugą stronę rzeki kilkoma brodami — znaleźli

[81]P. Grier: *Information Warfare w:* „Air Force", 4/1994, s.34 - 37. Aktualnie nazwę „Rand Corps" przyjęła grupa fachowców zajmująca się walką informacyjną.

się na bardzo wąskim odcinku, gdzie zostali zaatakowani przez Szkotów. Nie mogli zatem wykorzystać w walce ciężkiej jazdy, co uczyniło ich całkowicie bezbronnymi.

> *Analizując powyższe fakty pod kątem walki informacyjnej, należy stwierdzić, że zarówno sukces Szkotów, jak i klęska Anglików nie były przypadkowe. Zaskoczenie, które uzyskali Szkoci, zostało osiągnięte przez doskonałe maskowanie (obronę informacyjną) i pozorowanie działań (zakłócanie informacyjne). Klęska Anglików była natomiast konsekwencją niedoceniania problemu zdobywania informacji o przeciwniku, terenie i warunkach atmosferycznych.*

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.[82] 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.[83] 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.[84]

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,

---

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

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 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).[85] 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

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

rosyjsko – austriacka liczyła 95 000 żołnierzy, a francuska 75 000[86]. 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 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.*

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

Niestosowanie elementów walki informacyjnej przyczyniło się do klęski wojsk francuskich pod Waterloo w 1815 roku. Napoleon wyruszył na front północno — wschodni 12 czerwca 1815 r. Jego armia składała się z pięciu korpusów i liczyła około 127 000 żołnierzy. Natomiast siły sprzymierzonych liczyły: armia angielska dowodzona przez gen. A. Wellingtona — 67 000, a armia pruska generała G. L. Bluchera — 84 000 żołnierzy. 16 czerwca cesarz zaatakował Prusaków pod Ligny. Gdy zaczęli ustępować, cesarz skierował do walki przeciwko nim 33 — tysięczny korpus Grouchy`ego, a sam ruszył pod Waterloo. Posłał po korpus rezerwowy Neya, by uderzył na skrzydło Prusaków. D`Erlon, dowodzący korpusem rezerwowym, pomaszerował ku Ligny. Ney, gdy się o tym dowiedział, w dzikim wybuchu pasji zmienił rozkaz cesarza. D`Erlon, słuchając swojego bezpośredniego zwierzchnika wrócił z powrotem do Quarte — Bras. W rezultacie korpus ten liczący 20 000 żołnierzy nie wziął udziału w bitwie i nie oddał ani jednego strzału. Gdyby D`Erlon przybył tego dnia do Ligny i zaatakował prawe skrzydło z trudem utrzymujących się na pozycjach Prusaków, armia Bluchera zostałaby całkowicie pokonana. Wtedy 33 000 żołnierzy Grouch`ego byłoby do dyspozycji Napoleona i Wellington nie mógłby się utrzymać pod Waterloo. Zmiana rozkazu cesarza przez Neya zniweczyła wszystko. 18 czerwca doszło do decydującej bitwy. Napoleon, pod Waterloo, po wydaniu ogólnych dyspozycji Neyowi, całą taktykę pozostawił marszałkom. Nie było tu już wielkiej improwizacji (wprowadzania przeciwnika w błąd), jaką stosował cesarz. Tu o wszystkim decydował Ney, który zlekceważył prowadzenie rozpoznania i całkowicie stracił zmysł orientacji. Nie wiedział, gdzie znajduje się przeciwnik oraz wojska własne. Ponadto, zamiast dowodzić i obserwować przebieg bitwy, wpadł w atak złości i szablą uderzał w jedną z armat. Ney, widząc ustępującą brygadę francuską, przedarł się ku niej i nakazał zawrócić, ale nie dotrzymała ona kroku przeciwnikowi. W pobliżu La Bella Alliance natrafił na trzy czworoboki żołnierzy starej gwardii i walczył na ich czele, dopóki nie wyginęli. Wellington odpierał wszystkie ataki Francuzów, gdy tymczasem na plac boju zaczęły nadchodzić kolejno trzy korpusy Bluchera, który zmylił Grouchy`ego. Związał go walką jednym korpusem, a z resztą pospieszył na pomoc Wellingtonowi. Gdy sprzymierzeni przeszli do kontrataku — Francuzi załamali się i rozpoczęli odwrót, który przekształcił się w ucieczkę. Straty wojsk francuskich wyniosły 25 000, wojsk sprzymierzonych 22 000. Klęska Napoleona spowodowała jego ponowną abdykację.

Z powyższej analizy wynika, że zlekceważenie elementów walki informacyjnej przez marszałków Napoleona przyczyniło się w głównej mierze do klęski wojsk francuskich. Nie prowadzili oni rozpoznania przeciwnika i terenu, jak też

wymiany danych o sytuacji na polu walki. Nie wiedzieli dokładnie gdzie znajduje się przeciwnik i jaką siłą dysponuje. W efekcie tego źle ocenili sytuację. Dlatego też korpusy Grouchy`ego i D`Erlona zostały wprowadzone w błąd, co w głównej mierze przyczyniło się do klęski Napoleona.

Uogólniając treści zawarte we wcześniejszych wnioskach należy stwierdzić, że:

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[87].

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 ja,k i technicznej była bitwa pod Tangą, we wschodniej Afryce w 1914 roku, pomiędzy wojskami brytyjskimi i niemieckimi.[88] Na dowódcę brytyjskich sił ekspedycyjnych, liczących 8000 żołnierzy, został wyznaczony generał Aitken. W skład sił wchodzili

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

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. 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*

Podobnym przykładem jest wielka klęska Anglików w bitwie pod Sommą 1 lipca 1916 roku.[89] Atak żołnierzy brytyjskich został poprzedzony ostrzałem artyleryjskim, który miał zniszczyć zasieki z drutu kolczastego i pozycje niemieckich karabinów

[89]G. Regan, op. cit., s.114-115.

maszynowych. Pomimo ostrzału druty kolczaste i pozycje karabinów maszynowych zostały nietknięte. Nie prowadząc żadnego rozpoznania pola walki, żołnierzy brytyjskich uprzedzono, że całe przedpole zostało oczyszczone i nie spotkają oni ani jednego Niemca. Ponadto ostrzał artyleryjski został zakończony 10 minut przed wyjściem z okopów, co spowodowało, że Niemcy zostali w ten sposób uprzedzeni o mającym nastąpić natarciu i mieli dość czasu, aby przygotować się do odparcia ataku. Pod koniec dnia Brytyjczycy stracili 57 470 żołnierzy, spośród 120 000, którzy ruszyli rano do ataku. Był to jeden z najczarniejszych dni w historii wojsk brytyjskich.

> *Z analizy powyższych faktów wynika, że Brytyjczycy zlekceważyli prowadzenie rozpoznania przeciwnika i terenu. Nie śledzili efektów własnej działalności, co spowodowało, że ostrzał artyleryjski nie przyniósł pożądanych rezultatów, a żołnierze idący do ataku nie wiedzieli nic o czekającym ich niebezpieczeństwie. Ponadto nie prowadzili maskowania swoich wojsk (element obrony informacyjnej). Zbyt długi czas pomiędzy ostrzałem a atakiem umożliwił Niemcom przygotowanie się do obrony. Niestosowanie elementów walki informacyjnej przez Brytyjczyków spowodowało ich klęskę i utratę 50% stanu osobowego.*

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.[90]

Dowódca Frontu Płn — Zach., M. Tuchaczewski rozpoczął 4 lipca 1920 roku ofensywę w kierunku Warszawy, mając 105 000 żołnierzy i 595 dział.[91] 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);

---

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

— 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 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.*

Na szerszą skalę elementy walki informacyjnej stosowano podczas bitwy pod El Alamein. 17 stycznia 1942 r. siły niemiecko — włoskie, pod dowództwem feldmarszałka

Rommla, rozpoczęły ofensywę w Afryce Północnej przeciwko wojskom brytyjskim, które zostały odrzucone o czterysta pięćdziesiąt kilometrów na wschód. Włoski wywiad wojskowy wszedł w posiadanie amerykańskiego tajnego szyfru (tzw. czarnego kodu). Wszystkie meldunki wysyłane przez amerykańskiego pułkownika Franka Fellersa z Kairu do Waszyngtonu były przechwytywane przez niemiecką stację nasłuchową w Lauf. Dlatego też Rommel znał dokładnie poczynania przeciwnika. Np. 23 stycznia Rommel dowiedział się o odesłaniu z Afryki Północnej na Daleki Wschód dwustu siedemdziesięciu samolotów brytyjskich. 29 stycznia otrzymał dokładny spis jednostek pancernych przeciwnika (liczbę czołgów, ich miejsca postoju, ocenę wartości bojowej). 1 lutego Fellers przesłał ocenę wartości bojowej różnych jednostek brytyjskich wraz z informacją, że amerykańskie czołgi M—3 nie będą użyte wcześniej niż w połowie lutego. Były to dane bezcenne dla feldmarszałka. Ostrzegały go o zamiarach Brytyjczyków, ujawniały miejsca najsilniejsze i najsłabsze. Informowały o skutkach działania wojsk niemiecko — włoskich, o stanie wiedzy dowódców brytyjskich i ich planach.

W maju Rommel podjął kolejną ofensywę. Jego siły miały dotrzeć do Egiptu, zdobyć Palestynę i połączyć się w Iraku z wojskami niemieckimi, przegrupowującymi się przez były Związek Radziecki. Depesze Fellersa informowały, że Brytyjczycy mają zamiar stworzyć główną linię obrony w rejonie miasta Marsa Matruh, a następnie powiadomiły, że dowództwo brytyjskie zrezygnowało z tego planu. Wojska niemiecko — włoskie posuwały się bardzo szybko do przodu. Brytyjczycy zaczęli odczuwać coraz większy respekt przed feldmarszałkiem i jego pancernymi dywizjami. Brytyjski generał Auchinleck, aby podnieść morale swoich wojsk, skierował do podległych dowódców rozkaz: *„pojawia się autentyczne niebezpieczeństwo, że nasz przyjaciel Rommel staje się rodzajem magika lub straszydła dla naszych żołnierzy, którzy mówią o nim stanowczo za dużo... Oczekuję od was, abyście rozpraszali z pomocą wszelkich dostępnych środków wiarę, że Rommel jest kimś więcej niż zwykłym niemieckim generałem... Musimy używać określeń „Niemcy", „wojska osi", a nie „Rommel". Proszę zapewnić natychmiastowe wykonanie tego rozkazu i uzmysłowić dowódcom, że z psychologicznego punktu widzenia jest to sprawa najwyższej wagi*[92]. Głównodowodzący wyczuwał doskonale nastroje wśród żołnierzy. W brytyjskich szeregach rosła legenda Rommla — „lisa pustyni" — którego czołgi pojawiały się nagle, precyzyjnie realizowały plan, a gdy wycofywały się, po bokach ich drogi stały działa kalibru 88 mm. Niskie, świetnie zamaskowane za piaszczystymi pagórkami lub w kępach

[92]B. Wołoszański: *„Sensacje XX wieku. II wojna światowa"*. Warszawa 1998, s.119.

suchych krzaków, były niezwykle trudne do zniszczenia. Ponadto ich pociski, wystrzeliwane z odległości 2 km., przebijały pancerze brytyjskich i amerykańskich czołgów. Nagły odwrót niemieckich czołgów rodził u przeciwnika obawę, że jest to zasadzka, świadomy manewr, który ma wciągnąć brytyjskie czołgi w pułapkę. Rommel wygrywał, chociaż jego siły były słabsze. Stałym problemem Rommla był brak paliwa, części zamiennych, amunicji. Hitler, zajęty wojną ze Związkiem Radzieckim, nie dbał o należyte wyposażenie wojsk w Afryce Północnej. W końcu maja 1942 r. doszło do kolejnych starć pomiędzy Brytyjczykami a siłami „osi". Rommel wiedział, że jego wojska są mniej liczebne od alianckich. Ponadto miał o połowę mniej czołgów. Początkowo walka toczyła się ze zmiennym szczęściem. Na prawym skrzydle Afrika Korps rozbił hinduską 3 brygadę zmotoryzowaną, ale w starciu z 7 dywizją pancerną stracił wiele czołgów. Na lewym skrzydle sytuacja Rommla była znacznie gorsza: alianci zatrzymali włoski XX korpus, a dywizje „Trieste" i „Ariete" poniosły poważne straty. Rommel postanowił zastosować elementy walki informacyjnej. Wycofał swoje wojska i przegrupował. Pod Sollum przygotował 13 armat kalibru 88 mm, które były dobrze ukryte. Niespodziewający się takiego obrotu sprawy Brytyjczycy dali się wciągnąć w zasadzkę, w efekcie czego stracili sto dwadzieścia trzy z dwustu trzydziestu ośmiu czołgów.

12 czerwca niemiecka stacja nasłuchowa zarejestrowała depeszę następującej treści: *„W nocy z 12 na 13 czerwca brytyjskie jednostki sabotażowe równocześnie zaatakują samoloty na dziewięciu lotniskach „osi". Planuje się użycie oddziałów spadochronowych i zmotoryzowanych patroli dalekiego zasięgu. Ta metoda daje możliwość dokonania sporych zniszczeń przy niewielkim ryzyku w zestawieniu z ewentualnymi korzyściami. RAF jest przygotowany do wsparcia akcji jednostek lądowych. Dzisiaj Brytyjczycy przerzucają dużą liczbę żołnierzy z Syrii do Libii"*[93]. Rommel, znając treść depeszy, miał dużo czasu na ostrzeżenie zagrożonych lotnisk. Gdy brytyjscy spadochroniarze wylądowali w nocy, na pasach startowych lotnisk zostali ostrzelani, nie udało im się zbliżyć do samolotów.

W Bletchley Park w Anglii zespół kryptologów odczytywał już większość depesz Rommla nadawanych do Rzymu i Berlina za pomocą Enigmy. Dzięki temu większość danych zaczęła być przekazywana do kwatery generała Auchinlecka w Kairze. W połowie czerwca gdy generał dowiedział się o planowanej przez Rommla zasadzce w pobliżu lotniska El Adem, wysłał natychmiast szefa wywiadu, pułkownika de Guinganda

[93]B. Wołoszański, op. cit., s.120.

z ostrzeżeniem dla generała Ritchiego. Dowódca VIII armii nie mógł dopuścić myśli, że w Kairze wiedzą więcej o planach przeciwnika niż on na polu bitwy. Ocenił, że dane przywiezione przez szefa wywiadu pochodzą z jego własnych źródeł wywiadowczych lub z zeznań jeńców wojennych. Dlatego też nie uwierzył w ostrzeżenie i w połowie czerwca trzysta czołgów ruszyło w stronę El Adem. Z pełną szybkością wjeżdżały w świetnie zamaskowane „wilcze doły" i pola minowe. Te, którym udało się tego uniknąć, stawały się celem niemieckich dział kal. 88 mm. W ciągu kilku godzin Brytyjczycy stracili 230 czołgów. Dzięki temu siły „osi" przełamały kolejny pas brytyjskich umocnień. Brytyjska VIII armia, straciwszy 10 000 żołnierzy, wycofała się do Egiptu, pozostawiając załogę w Tobruku. 20 czerwca załoga skapitulowała, a Rommel wziął do niewoli 33 000 jeńców. Brytyjczycy cofnęli się do El Alamein i zajęli pozycję obronną od morza do depresji Qattara.

Pod koniec czerwca Brytyjczycy złamali amerykański „czarny kod". Nie podobały im się szczegółowe raporty Fellersa, w których niepochlebnie wyrażał się o umiejętnościach dowódców brytyjskich. W końcu czerwca zawiadomili Waszyngton, że Niemcy uzyskują cenne informacje z biura Fellersa. Dokładne śledztwo nie wykazało żadnych uchybień, ale na wszelki wypadek pułkownika odwołano do Stanów Zjednoczonych. „Czarny kod" pozostał dalej w użyciu, a nowy attache`, do przekazywania najważniejszych wiadomości stosował szyfr M — 138.

W sierpniu premier Winston Churchil, niezadowolony z porażek wojsk brytyjskich, uznał, że przyczyna klęsk tkwi w nieudolnym dowodzeniu. Dlatego też dowodzenie w wojnie na pustyni powierzył generałowi H. Alexandrowi. Na dowódcę VIII armii został wyznaczony generał B. Montgomery. Alianci wzmacniali swoje siły i rozbudowywali pozycje obronne w rejonie El Alamein. Rommel, wiedząc o tym, dążył do tego, aby jak najszybciej uderzyć na nieprzygotowanego przeciwnika. Rozpoznanie i wywiad poinformowały, że pozycje brytyjskie są najsłabsze na południe od El Alamein. Dlatego też postanowił tam uderzyć i ruszyć w stronę Alaksandrii, aby opanować główną bazę zaopatrzeniową przeciwnika. Powodzenie planu zależało od zaskoczenia przeciwnika, które można było osiągnąć przez ukrywanie wszelkich ruchów wojsk. Rommel przerzucał swoje oddziały w nocy, pozostawiając na miejscach, z których wyruszyły, makiety czołgów i dział, namioty, stosy beczek i kilkudziesięciu żołnierzy, którzy udawali, że jest kilkanaście tysięcy. Cała akcja przebiegała bardzo sprawnie. Brytyjskie samoloty rozpoznawcze nie mogły śledzić sytuacji w nocy, natomiast w dzień fotografowały „niemieckie wojska", ciągle tkwiące na północy.

Brytyjczycy, mający dużą przewagę liczebną, ale ciągle ponoszący porażki, zdali sobie sprawę, że jedynym sposobem pokonania przeciwnika będzie wprowadzenie go w błąd. Dlatego też zaczęli przekazywać nieprawdziwe dane, które Niemcy przechwytywali za pomocą stacji w Lauf. 26 sierpnia Rommel otrzymał wiadomość następującej treści: *„Potwierdzam wiadomość opartą na najbardziej wiarygodnych źródłach, że VIII armia przygotowuje się do ostatecznej obrony w rejonie Alam Halfa. Oczekuje na posiłki, ale obecnie nie jest zdolna do stawienia poważniejszego oporu"*[94]. Rommel nie potwierdzał danych, przyjął je jako prawdziwe. 31 sierpnia siły niemiecko — włoskie ruszyły w kierunku pozycji brytyjskich. Jednak okazało się, że sytuacja nie rozwija się zgodnie z planem, na kierunku gdzie miała walczyć jedna dywizja brytyjska — walczyły trzy. W południe 2 wrześnie zaczęło brakować paliwa. Następnego dnia feldmarszałek podjął decyzję odwrotu. Pod Al. Halfa siły „osi" straciły 1100 żołnierzy i 49 czołgów. Straty Brytyjczyków wynosiły 1750 żołnierzy i 67 czołgów.

W październiku 1942 r. Rommel posiadał łącznie 80 000 żołnierzy, 540 czołgów, 350 samolotów. Siły aliantów wynosiły: 230 000 żołnierzy, 1440 czołgów, 1500 samolotów. Rommel przeprowadził szereg przeciwnatarć. 2 listopada brytyjski XXX korpus przedarł się z ciężkimi stratami przez niemiecko — włoskie pola minowe. Po południu 4 listopada VIII armia przerwała front w rejonie Tell el Aqqaqir. W bitwie pod El Alamein wojska „osi" straciły 25 000, a alianci 13 560 żołnierzy. Rommel, wiedząc, że dane przekazywane do Berlina są rozszyfrowane przez Brytyjczyków, przestał informować przełożonych o swoich planach. To zmyliło przeciwnika, który uwierzył że feldmarszałek nie planuje żadnego działania i jest bezradny. 3 listopada Rommel rozpoczął odwrót, który przeprowadził po mistrzowsku, bez strat.

> *W Afryce Północnej na pustyni miała miejsce „wielka walka" szpiegów, szyfrów, depesz oraz nie istniejących w rzeczywistości oddziałów. Rommmel, prowadząc rozpoznanie przeciwnika i terenu oraz posiadając dane z wywiadu, miał przewagę nad przeciwnikiem. Często wprowadzał go w błąd. Nawet zarządzając odwrót, był przygotowany do stoczenia walki z przeciwnikiem. Doskonale maskował swoje wojska, a wszelkie przegrupowania wykonywał pod osłoną nocy. Zastosowane elementy walki informacyjnej pozwalały mu na właściwą ocenę sytuacji na polu walki i swobodę działania, co w efekcie przyczyniało się do osiągania sukcesów. Brytyjczycy doskonale zapamiętali, jak wielką rolę w działaniach bojowych dywizji pancernych odegrał podstęp. Wszystkie doświadczenia wykorzystali do organizacji największej operacji desantowej w historii świata: inwazji na Normandię.*

[94]B. Wołoszański, op. cit., s.138.

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[95]. 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 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.

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

Aby upewnić się, że Niemcy odbierają fałszywe komunikaty, sprzymierzeni rozkodowywali przechwycone szyfrowane komunikaty „Ultra”[96]. 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[97], 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.

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

---

[96]„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.

[97]F. W. Winterbotham: *„The Ultra Secret”*, Londyn 1974.

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.

Zlekceważenie danych z rozpoznania było natomiast przyczyną klęski Brytyjczyków w operacji powietrznodesantowej pod kryptonimem „Market Garden" w 1944 r. Planując operację, wykonano olbrzymią liczbę zdjęć lotniczych dla zorientowania się, czy wojska po wylądowaniu napotkają opór ze strony przeciwnika.. Marszałek polny Montgomery był pewny, że opór przeciwnika będzie słaby. Raporty wywiadu holenderskiego ostrzegały jednak, że niedaleko Arnhem rozlokowały się 9 i 10 niemiecka dywizja pancerna. Poza tym ze zdjęć lotniczych wynikało wyraźnie, że w rejonie tym znajdują się czołgi. Dowódca Brytyjskiego I Korpusu Powietrznodesantowego, gen. Browning, postanowił jednak zignorować to, co było widać na fotografiach i przystąpił do realizacji desantu na Arnhem. Przy najważniejszym moście pod Arnhem zrzucono na wschodnim brzegu rzeki 1 DPDes. Gen. R. Urquharta i pierwszy rzut szybowcowy z polskiej I Samodzielnej Brygady Spadochronowej. W rejonie zrzutu znajdował się korpus pancerny SS gen W. Bittricha (9 i 10 DPanc.) Niemcy podjęli natychmiast kontratak. Było to możliwe, gdyż posiadali komplet planów operacyjnych, który znaleźli przy jednym z zabitych oficerów brytyjskich. Do mostu dotarł tylko 2 batalion spadochroniarzy, który stoczył bohaterską, ale beznadziejną walkę z przeważającymi siłami przeciwnika. Ponadto jednostki dywizji brytyjskiej nie mogły między sobą nawiązać łączności ze względu na wadliwe działanie radiostacji. Montgomery kazał w końcu ewakuować żołnierzy angielskich i polskich. Operacja zakończyła się całkowitą porażką. Z 10 000 spadochroniarzy zrzuconych wokół Arnhem udało się uratować tylko 2163.

Przyczyną klęski wojsk alianckich było zlekceważenie elementów walki informacyjnej przez brytyjskich dowódców. Nie zwrócono zwłaszcza uwagi na otrzymane dane z wywiadu i rozpoznania lotniczego. Ponadto nie utrzymano w tajemnicy terminu ani miejsca realizacji operacji „Market Garden". W efekcie tego wojska powietrznodesantowe, które zostały zrzucone pod Arnhem, znalazły się w bardzo trudnej sytuacji, z której praktycznie nie było wyjścia. Dlatego też tak wielu żołnierzy poległo, a operacja zakończyła się całkowitym fiaskiem.

Reasumując poprzednie wnioski można stwierdzić, że:

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.

Kolejnym przykładem prowadzenia osobowej i technicznej walki informacyjnej jest agresja Izraela na państwa arabskie (Egipt, Jordanię i Syrię) w 1967 roku[98]. Plan agresji zakładał wykonanie zmasowanego, zaskakującego uderzenia lotnictwa, uzyskanie panowania w powietrzu, a następnie prowadzenie manewrowych działań siłami lądowymi wspieranymi z powietrza. Za jeden z najważniejszych elementów uznano określenie terminu wykonania uderzenia lotnictwa. Rozpoznanie izraelskie na początku czerwca 1967 roku stwierdziło, że egipski personel lotniczy jest już znużony utrzymywaniem od trzech tygodni wysokiej gotowości bojowej. Codziennie bowiem, od świtu, na każdym lotnisku gotowych było do startu po kilka samolotów, z których część wykonywała loty patrolowe. Ustalono, że około godziny 8.30 sprawność tych dyżurów słabnie, podobnie jak praca stacji radiolokacyjnych. Wzięto również pod uwagę, że około godziny 7.30 w rejonie delty Nilu ustępuje mgła i powstają dobre warunki do prowadzenia obserwacji. Ponadto uwzględniono, że w Egipcie pracę w biurach rozpoczyna się o godzinie 9.00, uznano więc, że najlepiej zaatakować w tym właśnie czasie. Pierwsze uderzenie lotnicze planowano wykonać podczas uzupełniania paliwa przez ostatnie grupy samolotów egipskich, po ich powrocie na lotniska z porannych lotów patrolowych. Za optymalny czas wykonania uderzenia uznano godziny 8.00 — 9.00. Powyższe przedsięwzięcia równoznaczne są ze zdobywaniem informacji o przeciwniku.

---

[98]Z. Gołąb: *„Wojna a system obronny państwa"*. Wydawnictwo MON, Warszawa 1984, s. 259 - 261.

Na kilka dni przed planowanym uderzeniem od strony Morza Śródziemnego lotnictwo izraelskie wykonało demonstracyjne loty rozpoznawcze nad południowym obszarem Egiptu, aby „zasugerować" możliwość uderzenia na tym właśnie kierunku. Podstęp się udał — Egipcjanie faktycznie przegrupowali z rejonu głównego określoną liczbę samolotów, które potem, skierowane na północ kraju, miały trudności z wylądowaniem, ponieważ wskutek nalotów lotnictwa izraelskiego zostały zniszczone pasy startowe. Ponadto Izrael dokonywał grupowych lotów codziennych nad półwyspem Synaj, w kierunku granicy z Egiptem. Wykonywano je o świcie, na tydzień przed planowaną agresją. „Sugerowano" więc uderzenie i na tym kierunku. Po zakończeniu lotów stwierdzono zmniejszenie czujności systemu obrony przeciwlotniczej Egiptu. Również w dniu agresji, 5 czerwca o świcie, część lotnictwa izraelskiego wykonała tego typu loty w kierunku półwyspu Synaj i powróciła na macierzyste lotniska, aby o godzinie 8.30 wystartować już całością sił do ataku na Egipt z kierunku Morza Śródziemnego. Powyższe przedsięwzięcia są tożsame z zakłócaniem informacyjnym.

> *Z powyższych faktów wynika, że prowadzenie rozpoznania przeciwnika i terenu pozwoliło wojskom izraelskim ustalić bardzo precyzyjnie najkorzystniejszy termin ataku. Realizacja działań pozornych lotnictwa (zakłócanie informacyjne) pozwoliła wprowadzić wroga w błąd, w wyniku czego Egipcjanie źle ocenili sytuację rzeczywistą i przebazowali samoloty do rejonów nieistotnych. Stosowane elementy walki informacyjnej przez wojska izraelskie doprowadziły do uzyskania zaskoczenia i przyniosły wymierne efekty w trakcie prowadzenia działań wojennych. W ciągu trzech godzin zniszczono 2/3 stanu lotnictwa egipskiego, w tym 90% na lotniskach.*

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:[99]

— 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 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

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

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"[100]. 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 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

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

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[101], 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[102], 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, 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

---

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

[102]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.

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[103].

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.*

Wnioski z podrozdziału 2.1.

- *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 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.*

2.2. Walka informacyjna według poglądów amerykańskich

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);

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

— walka informacyjna (Information Warfare — IW);

— działania informacyjne (Information Operations).

Pierwszy termin był używany już w latach 70 — 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[104].

> *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

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

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[105] (koncepcję) działań informacyjnych.

Działania informacyjne (IO — Information Operations) są definiowane jako ciągłe działania sił zbrojnych w ramach wojskowego środowiska informacyjnego (MIE), które przyczyniają się do wzmocnienia i obrony możliwości sił własnych w zakresie zdobywania, przetwarzania i przekazywania informacji w celu uzyskania przewagi w całym spektrum walki zbrojnej prowadzonej wewnątrz globalnego środowiska informacyjnego[106] (GIE), przy jednoczesnym pozbawieniu takich możliwości strony przeciwnej.

---

[105] 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.

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

Pomimo opracowania koncepcji działań informacyjnych, 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.*

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. 2.2.1).

Rys. 2.2.1.Elementy walki informacyjnej[107]

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.

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 informacji 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 informacji 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*

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

(preparacja) pola walki (IPB — Intelligence Preparation of the Battlefield), realizowana w wojskowym środowisku informacyjnym..

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);

— 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.

> *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.*

Zdolność pozyskiwania informacji o przeciwniku, ich analizowanie, przekazywanie i wykorzystanie będzie mieć decydujący wpływ na wynik przyszłych działań. Jak wynika z danych przedstawionych w tabeli 2.2.1, sposób prowadzenia rozpoznania uległ zmianie,

Tabela 2.2.1.

Prowadzenie rozpoznania a podejmowanie decyzji[108]

Rodzaj wojny ---------- Wyszczególnienie	**Rewolucja /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./

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

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

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 wielkości 2,5 metra. Jeśli zostanie on połączony z czujnikiem na podczerwień, będzie mógł wykryć nawet obiekty zamaskowane i przekazać informację w czasie rzeczywistym[109].

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.

Wnioski z podrozdziału 2.2.

- ✓ *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.*
- ✓ *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.*

2.3. Kluczowe efekty poznania

1. *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*

[109]Magazyn *„Signal"*, 4/1992.

przykłady jej prowadzenia. Odzwierciedlają one jej rangę i znaczenie w skali światowej oraz pozwalają na dokonanie syntezy w tym obszarze wiedzy.

2. *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.*
3. *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.*
4. *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.*
5. *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.*

„Optymalizacja zdolności bojowej sił lądowych w przyszłości będzie mogła być osiągnięta przez efektywne wykorzystanie informacji, czasu, energii i środków. Precyzyjna informacja na przyszłym polu walki będzie tak ważna jak precyzyjnie wycelowana broń"[110].

3. WPŁYW WALKI INFORMACYJNEJ NA WALKĘ ZBROJNĄ

Walka zbrojna to całokształt przedsięwzięć realizowanych w czasie działań wojennych przez siły zbrojne przy użyciu broni[111]. Jej celem jest zawsze rażenie przeciwnika, lub doprowadzanie do tak oczywistych i przekonujących sytuacji, w których przeciwnik, w obawie przed konsekwencjami zagrażającego mu niebezpieczeństwa — myśląc o uniknięciu lub pomniejszeniu strat — podporządkuje się woli sprawcy tego zagrożenia, rezygnując ze stawiania oporu czy też prowadzenia agresji. Zatem w całym potencjale militarnym zasadniczą rolę odgrywają środki rażenia. Wszystko pozostałe, czyli reszta uzbrojenia, wraz z obsługami i szeroko rozumianymi przedsięwzięciami organizacyjno — zabezpieczającymi, spełniają tylko funkcje usługowe w stosunku do rażenia. Służą do tego, aby środki rażenia w stosownym czasie przemieszczać w takie rejony i miejsca — na takie pozycje bojowe — z których możliwe będzie najskuteczniejsze rażenie przeciwnika. Dotyczy to zarówno broni strzeleckiej, broni pokładowej, artylerii, środków rakietowych, jak i wszystkich innych, które w danym czasie znajdować się będą w wojskach. Służy temu całe planowanie walki zbrojnej, cały ruch wojsk i wszystkie inne przedsięwzięcia, które bardziej lub mniej bezpośrednio, ale zawsze do tego nawiązują. A zatem podstawą sukcesu w walce zbrojnej jest zawsze precyzja rażenia i czas reakcji ogniowej, o których skuteczności w głównej mierze decyduje informacja. Zdobycie aktualnych danych o przeciwniku umożliwia dowódcom kontrolę sytuacji w konflikcie lub działaniach wojennych. Innymi słowy, dowódca powinien mieć przewagę w wiedzy nad przeciwnikiem. Dziś dowódcy mogą uzyskiwać taką przewagę dzięki zastosowaniu nowych technologii i technik, które pozwalają podnieść moc bojową wojsk, przejąć inicjatywę, zwiększyć skuteczność prowadzonej walki oraz uodpornić własne systemy informacyjno — sterujące na oddziaływanie przeciwnika. Aby to osiągnąć, należy:

— zdobyć kluczowe dane o przeciwniku z odpowiednim wyprzedzeniem czasowym;

---

[110] „Information and Combat Power". Military Review, 6/1995, s.56.
[111] *Leksykon wiedzy wojskowej*, Warszawa 1979, s.474.

— sensownie zarządzać danymi (przekazywać dane we właściwe miejsca i w odpowiednim czasie), aby osiągnąć pożądane rezultaty.

Informacja wpływa w znacznym stopniu na trafność decyzji, która zawsze warunkuje osiągnięcie celu. Decyzja w procesie przygotowywania walki jest elementem bardzo ważnym. Podjęcie decyzji jest zawsze związane z pewnym ryzykiem. Wszelkie oceny dokonywane przez jedną ze stron są tylko sformułowaniami prawdopodobnymi, opartymi na zdobytych danych. Dlatego też wiarygodna i aktualna informacja stanowi podstawę do podjęcia trafnej decyzji.

3.1. Informacja a decyzja

Jak już stwierdzono wcześniej, pozytywna rola informacji polega na tym, że umożliwia ona człowiekowi przewidywanie zdarzeń, a tym samym zmniejszenie ryzyka decyzyjnego.

Termin „decyzja" pochodzi od łacińskiego słowa *decisio*, co oznacza: postanowienie, rozstrzygnięcie, uchwała. Decyzja jest aktem będącym wolnym wyborem jednego z możliwych przyszłych zachowań[112]. Jest to zatem wybór jednego z rozwiązań jakiegoś problemu[113].

Pojęcie decyzji ma różne interpretacje w różnych warunkach. W cybernetyce decyzja jest zdarzeniem, które wchodzi do treści tworzącej układ i daje się opisać za pomocą informacji zawartej w układzie i strukturze połączeń[114].

J. Kurnal pisze, że podejmowanie decyzji polega na akcie świadomego wyboru jednego z rozpoznanych i dostępnych wariantów działania[115].

Prakseologia rozpatruje decyzję z punktu widzenia sprawności, wprowadza zasady działań racjonalnych. Na tle tych działań rozpatruje znaczenie i związki zachodzące między takimi pojęciami, jak: cel, dzieło, działanie, sprawca, oszczędność, marnotrawstwo, skutek itp.

Matematyczne podejście polega na poszukiwaniu „optymalnej decyzji", a więc odpowiadającej rzeczywistym warunkom[116]. Za pomocą teorii matematycznej badane są związki zachodzące między konkretnymi prawdopodobieństwami zdarzeń, prób losowych

---

[112] T. Rudniański: *„Przed decyzją"*. Warszawa 1965, s. 88.
[113] *Encyklopedia organizacji i zarządzania.* PWE, Warszawa, 1985, s. 53.
[114] S. Beer: *„Cybernetyka a zarządzanie"*. Warszawa 1986, s. 16.
[115] J. Kurnal: *„Zarys teorii organizacji i zarządzania"*. Warszawa 1970.
[116] A. Czerminski, M. Czapiewski: *„Organizacja procesów decyzyjnych"*. Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 1995, s. 13.

oraz zbiorów zdarzeń. Decydent stara się wybrać taką decyzję (optymalną), która prowadzi do możliwie małych strat.

Z punktu widzenia psychologii właściwa decyzja zależy od człowieka, który w sposób bezpośredni lub pośredni będzie ją podejmował. Nader ważną cechą są predyspozycje decydenta, umiejętność rozróżnienia złożoności i nowości problemu decyzyjnego[117]. Na zachowanie decydenta mają wpływ takie cechy, jak: wykształcenie, kwalifikacje, percepcja, pamięć, intuicja, temperament, emocjonalność, aspiracje, poziom lęku. Te wszystkie cechy powinny być determinantą decydenta.

Ponadto decyzję można rozpatrywać w zależności wynikowej i czynnościowej.

W sensie wynikowym decyzja rozumiana jest jako akt wyboru celu lub sposobu działania, pożądanego z punktu widzenia systemu, w ramach którego wybór ten jest dokonywany, przy czym aktowi wyboru są stawiane określone wymagania. W tym wypadku istotą decyzji jest skupienie uwagi na rezultacie określonego ciągu zdarzeń lub czynności, doprowadzających do aktu wyboru przyszłego działania.

W sensie czynnościowym decyzja rozumiana jest jako szczególna aktywność ludzi, wyrażająca się w poszukiwaniu takich rozwiązań pojawiających się problemów, które mogą zapewnić realizację zamierzonych celów systemu. Istotą takiego wyjaśnienia pojęcia decyzji jest koncentracja na czynnościach, które składają się na tę szczególną aktywność ludzi, a których efektem ma być rozwiązanie pojawiających się na tle realizacji zadań systemu — problemów decyzyjnych.

Aspekt informacyjny decyzji, na którym skoncentrowano się w dysertacji, jest podnoszony przez W. Flakiewicza[118]. Traktuje on decyzję jako proces transformacji przekształcającej sytuację decyzyjną w zbiór wariantów, z których wybrany jest traktowany, jako decyzja ostateczna.

Z powyższego wynika, że decyzja jest wolnym, nielosowym i świadomym wyborem jednego z wariantów — z możliwych wariantów w danym momencie. Innymi słowy, jest to wybór alternatywy lub podzbioru alternatyw ze zbioru możliwych alternatyw.

Proces informacyjno — decyzyjny można przedstawić w postaci relacji:

$$W = T_1 \{B\}$$

$$D = T_2 \{W\}$$

---

[117] J. Kozielecki: „Psychologiczna teoria decyzji". Warszawa 1977, s. 19.
[118] W. Flakiewicz: „Podejmowanie decyzji kierowniczych". Warszawa1983, s. 23.

gdzie:

B — zbiór informacji bazowych;

W — zbiór wariantów dopuszczalnych decyzji;

D — decyzja ostateczna (stanowiąca podstawę działań wykonawczych);

T_1, T_2 — transformacja.

Stąd wynika:

$$D = T_2 [T_1 \{B\}]$$

Zgodnie z powyższym można stwierdzić, że:

— w procesie decyzyjnym występują dwie różne transformacje;

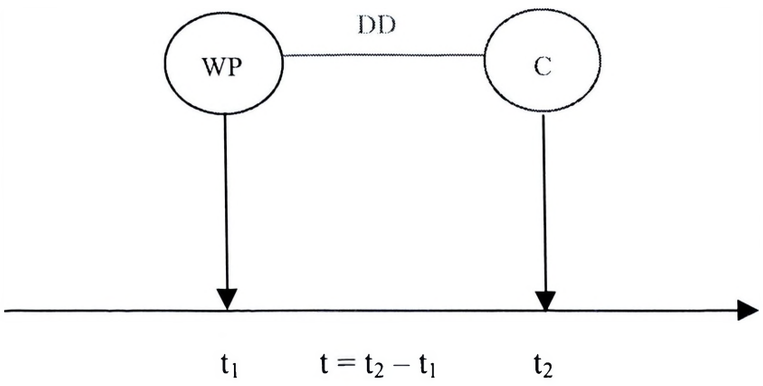
— w wyniku działania transformacji T_1, traktowanej jako operator na informacjach bazowych, otrzymuje się tzw. dopuszczalne warianty decyzji ostatecznej;

— w wyniku działania transformacji T_2 jest dokonywany wybór jednego z wariantów. Wyboru tego dokonuje podmiot decyzyjny, uznając dany wariant za decyzję ostateczną.

Ciąg czynności wykonywanych przez ludzi, najczęściej pozostających w otoczeniu podmiotu decydującego, związany z przygotowaniem wariantów decyzji dopuszczalnych, też wymaga podejmowania decyzji, z tym że są one podrzędne w stosunku do decyzji ostatecznej, związanej z pełnym rozstrzygnięciem określonego problemu. Stąd też ustalenia zbioru W dokonuje się na podstawie tego drugiego typu decyzji, zwanej dalej „wewnętrzną". Można stwierdzić, że system informacyjno — decyzyjny ma budowę hierarchiczną, wielostopniową. Na szczycie tej hierarchii znajduje się decyzja ostateczna, która rozkłada się na decyzje wewnętrzne, również wielostopniowe. Np. jeśli na szczeblu G podejmuje się decyzję ostateczną, to na szczeblu G_1 ustala się, które z wariantów uznaje się za dopuszczalne, a na szczeblu G_2 ustala się warianty decyzji dopuszczalnych w danych warunkach itd. Dokonując dalej tej dekompozycji, dochodzi się do momentu, w którym pracownik, przygotowując pewne materiały cząstkowe, sam dokonuje wyboru zarówno „wewnętrznego", jak i „ostatecznego" w postaci gotowego materiału, który np. przekazuje swemu zwierzchnikowi.

> *Z powyższej analizy wynika, że podstawową właściwością każdej decyzji jest wybór (alternatywa). Bez możliwości alternatywy nie można mówić o decyzjach. Drugą cechą każdej decyzji jest uznanie jej za informację sprawczą, tj. taką, która nakazuje człowiekowi lub ludziom przystąpić do określonego działania. Nakaz ten może mieć różny stopień obligatoryjności, od zlecenia, jako formy najsłabszej, do rozkazu, czyli najsilniejszej formy decyzji.*

W każdym świadomym działaniu człowieka (rys. 3.1.1), niezależnie od tego, czego



Rys. 3.1.1. Warunki działania człowieka

konkretnie dotyczy, muszą być uwzględnione cztery główne składniki:

1) określenie warunków początkowych *(WP)* działania, tzn. warunków, w jakich przystępuje się do działania. Wymaga to odpowiednich danych, tzw. danych początkowych;
2) ustalenie celu działania *(C)*. Wymaga to już znacznie głębszego i bardziej wszechstronnego przetworzenia posiadanych danych, które mogą się okazać niedostateczne i wymagające uzupełnienia;
3) wybór dojścia do celu *(DD)*. Składnik ten odgrywa podwójną rolę:
   — weryfikatora możliwości realizacji celu;
   — precyzującego sposób jego osiągnięcia;
4) określenie ΔT, czyli czasu potrzebnego do realizacji celu. Należy podkreślić, że ΔT, zwane „horyzontem czasowym" decyzji, może w pewnych warunkach przekreślić działanie. Może to nastąpić wtedy, gdy cel będzie nie do zrealizowania w czasie ΔT, mimo że dysponuje się środkami lub gdy cel jest realny, ale w ΔT nie można zdobyć takich środków, które będą mogły wyznaczyć pożądaną *DD*.

> *Z powyższych rozważań wynika, że decyzja to wygenerowanie (utworzenie) pewnej informacji o charakterze sprawczym, w wyniku wyboru alternatyw dopuszczalnych, związanych z oceną WP, C, DD oraz ΔT, opracowanych na podstawie posiadanych danych bazowych.*

Realizacja aktu decyzyjnego wymaga spełnienia pewnych warunków. Np. jeśli dany zbiór możliwych alternatyw decyzyjnych X zawiera co najmniej dwie alternatywy x_1 i x_2, gdzie:

$$x_1 \cup x_2 = 1^* = X$$

$$x_1 \cap x_2 = 0^*$$

to akt decyzyjny będzie polegał na wyborze ze zbioru X jednego elementu tego zbioru. Zatem można rozpatrywać sytuacje, w których określony człowiek lub grupa ludzi, mając

wyróżniony zbiór wariantów działania, dokona przyporządkowania temu zbiorowi jednego z działań. W tym wypadku będzie to prosta sytuacja decyzyjna. W sytuacji bardziej złożonej decydent może sformułować zasadę (procedurę) dokonywania przyporządkowywania. Ogólnie rzecz ujmując, decydenta cechuje prawo do kreowania zasady, czy wręcz przepisu, dokonywania aktu decyzyjnego. W sytuacjach, gdy przepis ten można ująć w formę precyzyjnego, sformalizowanego wyrażenia, określa on po prostu funkcję, zgodnie z którą zbiorowi X zostaje przyporządkowany jego element. Funkcję tę nazywa się funkcją decyzyjną, a wskazany przez nią element — decyzją. W tym wypadku powinny być spełnione następujące postulaty:

1) Każdy element zbioru X powinien być opisany przez wszystkie mogące interesować decydenta właściwości.
2) Każde dwa elementy zbioru X powinny być różne.
3) Zbiór X powinien obejmować wszystkie elementy, mogące interesować decydenta.
4) Ani zbiór X, ani jego elementy nie powinny zmieniać swych właściwości.

Funkcja decyzyjna powinna być tak skonstruowana, aby istniała możliwość porównywania dowolnych elementów, przy czym porównywalność musi być zupełna i przechodnia[119]. Celem powyższego jest uzyskanie maksimum informacji o zbiorze możliwych wariantów działania. Gdy zbiór wariantów działania X jest określony precyzyjnie, punkt ciężkości problemu decyzyjnego przenosi się na zasady kreowania funkcji decyzyjnych. Zgodnie z przyjętą interpretacją, funkcję decyzyjną tworzy decydent.

Jest oczywiste, że żaden decydent nie działa w izolacji i dlatego akt tworzenia pewnej funkcji decyzyjnej podlega pewnym ogólnym prawidłowościom.

Jeżeli w problemie decyzyjnym znane są wszystkie niezbędne informacje o zbiorze wariantów działania X oraz istnieje funkcja decyzyjna, pozwalająca porównać każde dwa elementy tego zbioru i wskazać jednoznacznie element, który jest decyzją, to mówi się, że podjecie decyzji nastąpiło w warunkach pewności lub, inaczej, w warunkach pełnej informacji. Natomiast jeśli nie posiada się pełnej informacji o problemie decyzyjnym, wtedy można stwierdzić, że podjęcie decyzji nastąpiło w warunkach ryzyka. Dlatego też w celu sprawnego i trafnego podejmowania decyzji należy utworzyć odpowiednie zbiory

[119] Zupełność i przechodniość – warunki podziału zbiorów, zostały omówione podczas dokonywania klasyfikacji przestrzeni walki informacyjnej. Rozdział drugi, s. 51 - 52.

informacji, które muszą być uporządkowane, przygotowane i aktualizowane. Wymaga to budowy systemu informacyjno — sterującego. Należy w tym wypadku określić:

— sposób zdobywania informacji — co?, kiedy?, jak?

— sposób ich aktualizowania — co?, kiedy?, jak?

— sposób utrzymywania informacji — na jakich nośnikach?, w jakiej ich organizacji?

— sposób przetwarzania informacji — na podstawie jakich procedur i algorytmów?, przy wykorzystaniu jakich technik i technologii?

— sposób przekazywania informacji — jakie?, komu?, kiedy? , w jaki sposób?

Wnioski z podrozdziału 3.1.

- ✓ *Zdobycie aktualnych, dokładnych i wyprzedzających danych jest najważniejszym czynnikiem na polu walki. Każdy dowódca usiłuje odpowiedzieć na pytania: Co się dzieje? Co to oznacza? Co należy zrobić? Jednocześnie stara się uniemożliwić przeciwnikowi zdobycie podobnych danych.*
- ✓ *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).*
- ✓ *Dzisiejsza technologia informacyjna umożliwia zobrazowanie sytuacji z pola walki w czasie niemal rzeczywistym. Świadomość sytuacyjna dowódców w połączeniu z najnowocześniejszymi urządzeniami technicznymi, stosowanymi w systemach informacyjno — sterujących, pozwala podjąć trafną decyzję, przejąć inicjatywę na polu walki i osiągnąć przewagę nad przeciwnikiem.*

3.2. Informacja a moc bojowa

Za najbardziej elementarne czynniki walki zbrojnej należy uznać rażenie, ruch i informację, natomiast pozostałe, takie jak manewr, ogień, uderzenie, opór, oddziaływanie psychologiczne oraz obezwładnianie elektromagnetyczne, itp. — należy traktować bądź to jako czynniki syntetyczne, będące syntezą tych pierwszych, bądź też jako szczególny przypadek (rodzaj, konkretną formę przejawiania się) czynników elementarnych[120].

Rażenie to bezpośrednie fizyczne lub psychiczne oddziaływanie destrukcyjne na siły i środki przeciwnika. Podstawową formą rażenia jest ogień, który umożliwia realizację zadań bojowych przez niszczenie i obezwładnienie przeciwnika oraz osłonę własnych wojsk przed uderzeniami.

Ruch to wszelkie przesunięcia, zmiany rozmieszczenia sił i środków. Najważniejszymi jego wskaźnikami są odległość i czas przesunięcia oraz ich iloraz, czyli

[120]Koziej S.: „Podstawy i zasady sztuki wojennej", AON, Warszawa 1993, s.100.

prędkość lub tempo działania. Podstawową formą ruchu na polu walki jest manewr, będący zaplanowanym przemieszczeniem wojsk bezpośrednio przed lub po starciu (pod oddziaływaniem przeciwnika, ale bez prowadzenia z nim bezpośredniej walki) w celu zajęcia dogodnego położenia i uzyskania oraz wykorzystania przewagi sytuacyjnej.

Informacja zespala pozostałe czynniki walki zbrojnej w zharmonizowaną całość starcia zbrojnego.

Przedstawiona powyżej interpretacja czynników walki zbrojnej, stanowi pewną analogię do spotykanej w literaturze, np. u F. Focha, S. Roli-Arciszewskiego, R. Simpkina i R. Leonharda[121]. Wielkościami opisującymi wymienione uprzednio elementarne czynniki walki zbrojnej w tym wypadku są: masa, prędkość i przyspieszenie.

Masa odpowiada czynnikowi rażenia, odzwierciedla potencjał niszczycielski wojsk. Prędkość jako stosunek przestrzeni do czasu nie wymaga szerszej interpretacji. Przyspieszenie jest definiowane jako tempo zmiany prędkości.

Iloczyn masy i prędkości to w fizyce kategoria pędu, która w mechanice walki zbrojnej odpowiada kategorii uderzenia, będącej syntezą rażenia i ruchu.

Jak twierdzi gen. prof. dr hab. Stanisław Koziej do charakterystyki efektywności działania danego zgrupowania bojowego dobrze nadaje się kategoria energii, jako zdolności do wykonania odpowiedniej pracy, mierzonej iloczynem masy i kwadratu prędkości[122]. Zdolność bojową[123] jednostek wojskowych — zwłaszcza do wykonania zadań na manewrowym polu walki — można zwiększać przez zwiększenie albo masy (zdolności rażenia), albo potencjalnej prędkości (ruchliwości).

Przyspieszenie na polu walki będzie odzwierciedlać sprawność, w tym szybkość reagowania na zmieniającą się sytuację. Wynika z tego, iż kluczową rolę w przyspieszeniu odgrywa sprawność całego systemu informacyjno — sterującego (zdobywanie danych o przeciwniku, podejmowanie decyzji i przekazywanie jej do realizacji). Iloczyn masy

---

[121]Simpkin R.: Race to the Swift. Oxford and London 1985. Leonhard R.: The art of Maneuver. Novato 1991.
[122]Koziej S., op. cit., s.103-106.
[123]Według gen. prof. dr. hab. Stanisława Kozieja, zdolność bojowa wojsk jest kategorią zsyntetyzowaną, odzwierciedlającą potencjał rażenia (ognia), ruchu, systemu informacyjnego, stopnia zorganizowania, morale, dyscypliny itp. Rozróżnia się pełną zdolność bojową, wyrażającą się w możliwościach natychmiastowego podjęcia walki oraz niepełną - charakteryzującą się ograniczonymi możliwościami wykonania zadań bojowych. Główne czynniki decydujące o zdolności bojowej to: poziom wyszkolenia bojowego wojsk oraz ich odporność; ilość środków walki i sprzętu bojowego, ich stan techniczny i gotowość do użycia w walce; stopień przygotowania pododdziałów i oddziałów do walki; możliwość rozpoznawania wojsk i środków walki przeciwnika; stan oraz sprawność środków i systemów elektronicznych do wykorzystania dla celów dowodzenia i kierowania środkami walki; stan i możliwości materiałowego oraz technicznego zaopatrywania wojsk; sprawność wsparcia logistycznego. O zdolności bojowej wojsk w walce decydują ponadto: umiejętność uchylania się przed uderzeniami oraz sprawne i zorganizowane odtwarzanie potencjału bojowego wojsk, a także sprawności bojowej środków walki i dowodzenia po uderzeniach.

i przyspieszenia wyraża w fizyce siłę. W walce zbrojnej jest on odpowiednikiem siły niszczącej wojsk. O wartości przyspieszenia w głównej mierze decyduje informacja.

Najbardziej kompleksowym wskaźnikiem charakteryzującym wartość bojową wojsk jest oczywiście iloczyn wartości wszystkich trzech elementarnych czynników walki zbrojnej — rażenia, ruchu i informacji. Moc bojowa danego zgrupowania (jednostki wojskowej) jest wprost proporcjonalna do wielkości potencjału rażenia, możliwości manewrowych (ruchliwości) wojsk oraz sprawności systemu informacyjno — sterującego.

Z powyższej analizy wynika, że czynnik informacji odzwierciedla całą niematerialną sferę walki, w tym moralną. Każde oddziaływanie na przeciwnika jest jednocześnie działaniem materialnym i niematerialnym. O skuteczności rażenia i manewrowości w głównej mierze decyduje informacja.

> *Skuteczność i precyzja na polu walki dzięki informacji i cyfrowemu zobrazowaniu sytuacji, stwarzają możliwość uzyskania potężnej mocy bojowej jakiej do tej pory nie znano. Większej mocy bojowej nie będzie można jednak tworzyć przez gromadzenie większej ilości informacji. Natomiast będzie można zwiększyć moc bojową przez wykorzystanie własnych aktywów, ale tylko w pewnym miejscu i czasie, kiedy one będą niezbędne do osiągnięcia celów militarnych. Dlatego też zwiększenie „świadomości sytuacyjnej" może nastąpić na skutek zdobycia istotnych (kluczowych) informacji, co doprowadzi do wyeliminowania niepewności i podjęcia niezbędnych środków bezpieczeństwa.*

Aby przegrupować wojska z jednego punktu do drugiego, niezbędna jest pewna ilość czasu (*T*). Celem działań zbrojnych będzie zredukowanie do minimum wielkości czasu oraz ilości sił i środków bojowych, które to wartości są potrzebne do wykonania zadań pośrednich (związanych z zajęciem terenu, orientowaniem), jak i zadań bezpośrednich, mających na celu uderzenie na przeciwnika i osiągnięcie zwycięstwa. Aby wykonać zadanie, dowódcy potrzebują odpowiedniej informacji (*I*), która daje im dostateczną ilość czasu na przeprowadzenie manewru swoich oddziałów i pododdziałów, tak że wojska te zostają przegrupowane na wyznaczone pozycje z odpowiednim wyprzedzeniem czasowym, aby wykonać specjalne zadania. Informacja posiada czynnik czasu (*TI*), który określa, ile czasu można wykorzystać na prowadzenie działań. Podczas rozważania możliwości manewru dowódcy powinni znać ilość czasu (*T*), który potrzebują na przegrupowanie swoich wojsk na pozycje bojowe z odpowiednim wyprzedzeniem czasowym.

Powyższe zależności można zapisać równaniem:

$$\Delta TI = TI - T$$

gdzie:

ΔTI — rezerwa informacyjna;

TI — terminowość informacyjna;

T — czas krytyczny.

Jeśli różnica TI - T daje pozytywny wynik, inaczej mówiąc, jeśli $\Delta TI > 0$, wtedy dowódca ma możliwość przeprowadzenia manewru swoich wojsk z odpowiednim wyprzedzeniem czasowym, aby dominować fizycznie nad przeciwnikiem na polu walki.

Jeśli $\Delta TI < 0$, wtedy na podstawie dostępnych informacji dowódca nie będzie mógł przeprowadzić manewru swoich sił w terminie. Dlatego też będzie musiał rozmieścić swoje wojska tak, aby były bliżej punktów newralgicznych (krytycznych) lub w taki sposób, aby jego strefa działań zazębiała się z zadaniami innych jednostek, które będą zdolne podjąć walkę.

Aby stworzyć sprzyjające okoliczności i przejąć inicjatywę na polu walki, należy zwiększyć rezerwę informacyjną. Można to zrobić dwoma metodami.

Pierwsza metoda polega na wzroście efektywności informacji bojowej o położeniu wojsk. Im większa jest wiedza nt. walki, tym większy zakres sposobów jej prowadzenia. Aby zwiększyć efektywność informacji, dowódca może wykorzystać do tego celu wszystkie systemy rozpoznawcze, organiczne i przydzielone.

Druga metoda wzrostu efektywności czasu polega na zmniejszeniu czasu manewru przez wykorzystanie jednostek o dużej manewrowości i przegrupowanie ich na pozycje położone w pobliżu rejonów, gdzie będą wykonywać zadanie.

Najlepszym rezultatem zwiększenia efektywności czasu (rezerwy informacyjnej ΔTI) jest stosowanie obydwu metod jednocześnie i manipulowanie terminowością informacji (TI) i wartością czasu (T) równocześnie.

Obecnie niektóre kraje, w tym głównie USA, mają dostęp do znacznie lepszego, zarówno powietrznego, jak i kosmicznego rozpoznania, ale jeszcze mała szybkość przekazywania dowódcom na polu walki danych z tych systemów rozpoznawczych ogranicza ich wykorzystanie. Teraz tylko systemy cyfrowe umożliwiają przekazanie na czas danych z rozpoznania strategicznego czy operacyjnego dowódcom szczebla taktycznego. Taka sytuacja oznacza, że dowódcy będą śledzić sytuację na polu walki, czyli $\Delta TI > 0$, zgodnie z ustaloną metodą postępowania.

> *Rezerwa informacyjna większa od zera ($\Delta TI > 0$) — to jest właśnie logiczna zasada, która oferuje optymalne warunki dla uzyskania maksymalnej mocy bojowej i zrewolucjonizowania cyfrowego zobrazowania sytuacji z pola walki. Umożliwia śledzenie zmian zachodzących w największym obszarze (przestrzeni)*

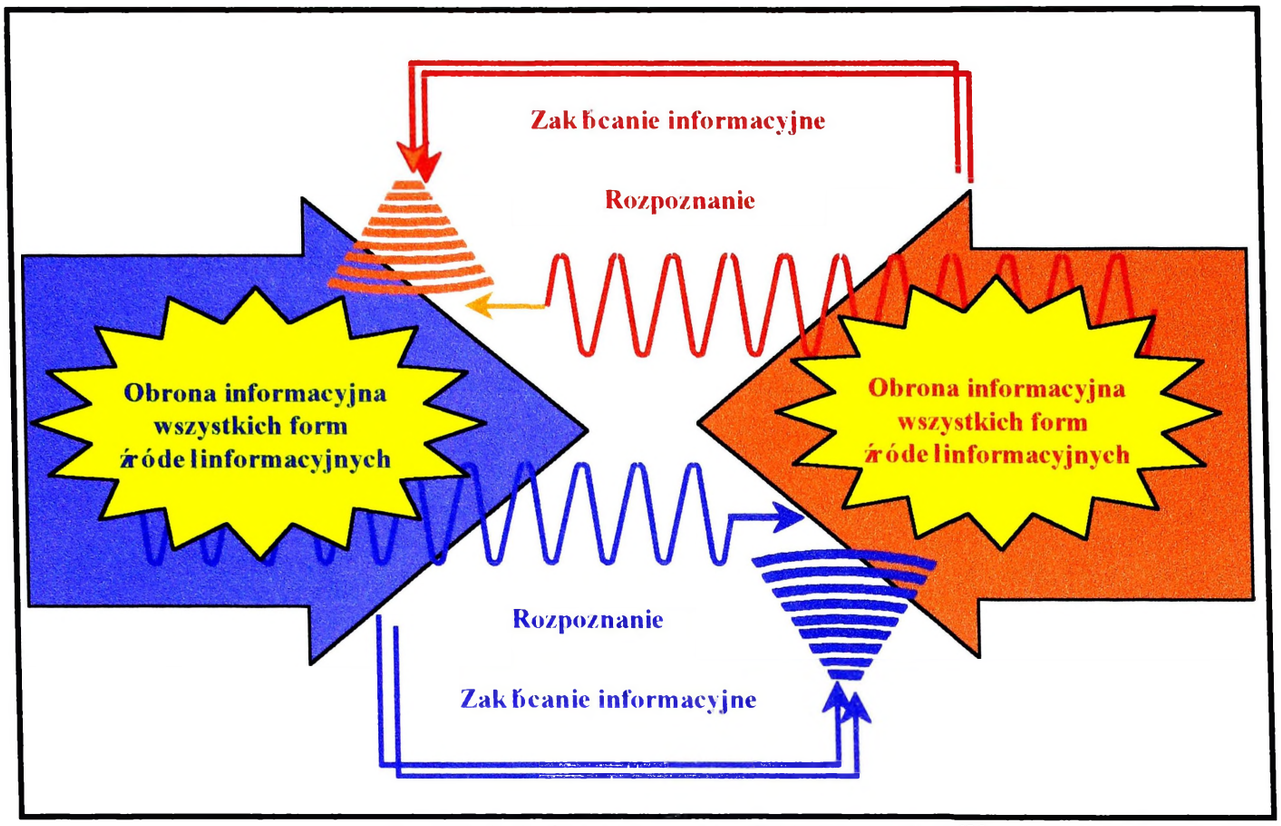
lub strukturze pola walki. Może oznaczać, że linia styczności wojsk FLOT (forward line of troops) zniknie z pola walki i działania będą miały charakter nielinearny. Nowym sposobem prowadzenia działań bojowych w przyszłości będzie optymalne wykorzystanie wszystkich wymiarów pola walki. Przez wykonanie szybkiego manewru lub dużą skuteczność rażenia dowódcy będą mogli podwyższyć efektywność wojsk, a tym samym zwiększyć ich moc bojową. Gwarantem realizacji tego jest wiarygodna i aktualna informacja.

Wnioski z podrozdziału 3.2.

- ✓ *Konstatując można stwierdzić, że siły zbrojne na polu walki mają tylko ograniczoną ilość czasu i dostępnej energii. Jednostki zużywają czas i energię, kiedy prowadzą działania bojowe, zabezpieczające i logistyczne. Działania logistyczne, takie jak: tankowanie, uzupełnianie rezerw, obsługiwanie, planowanie, naliczanie kosztów i odpoczynek są prowadzone bardziej skutecznie i efektywnie, kiedy ciężar działań bojowych jest zredukowany.*
- ✓ *Projekt struktury sił zbrojnych XXI wieku musi uwzględniać znacznie mniejszą armię, składającą się z oddziałów (formacji) o większej manewrowości i większej skuteczności rażenia niż siły zbrojne posiadały w przeszłości. Siły lądowe będą posiadać większą moc bojową z powodu technologii informacyjnych, podnoszących walory stosowanej broni i taktyki.*
- ✓ *Moc bojowa danego zgrupowania (jednostki wojskowej) jest wprost proporcjonalna do wielkości potencjału rażenia, możliwości manewrowych (ruchliwości) wojsk oraz sprawności systemu informacyjno — sterującego. W sumie moc bojowa w walce zbrojnej odzwierciedla jedność czynnika materialnego i niematerialnego.*
- ✓ *Optymalizacja mocy bojowej w operacjach sił lądowych w przyszłości będzie mogła być osiągnięta przez efektywne wykorzystanie informacji, czasu, energii i środków. Precyzyjna informacja na przyszłym polu walki będzie tak ważna jak precyzyjnie wycelowana broń.*

3.3. Znaczenie walki informacyjnej na współczesnym polu walki

Jak już stwierdzono wcześniej, podstawą sukcesu w walce zbrojnej jest zawsze precyzja rażenia i czas reakcji ogniowej. Przy porównywalnych ilościowo i jakościowo stanach uzbrojenia zwycięstwo będzie po tej stronie, która szybciej i precyzyjniej razi przeciwnika. Wynika z tego, że racjonalne modelowanie walki zbrojnej powinno prowadzić do optymalnego wykorzystywania siły rażenia wojsk poprzez stwarzanie warunków do osiągania jak największej precyzji ognia i jednocześnie warunków do maksymalnego skracania czasu reakcji w tym zakresie. Są to dwa podstawowe kryteria, których nieprzestrzeganie prowadzić będzie zawsze do wzrostu kosztów działań i zwiększania stopnia zagrożenia porażką. Niedoskonałości jakościowe muszą być rekompensowane masą ognia oraz zwiększonym posiadaniem sił i środków walki, jak również wydłużonym czasem przebywania w strefie możliwości rażenia przeciwnika. Wokół tego właśnie zlokalizowana jest istota walki informacyjnej (rys.3.3.1).



Rys. 3.3.1. Ogólny schemat walki informacyjnej[124]

> *Rozpoznanie, zdobywając dane o przeciwniku, wpływa na precyzję rażenia, a zakłócanie informacyjne i obrona informacyjna — na osiąganie wyprzedzenia w użyciu celnego ognia. Korzyści materialne tego można postrzegać chociażby przez pryzmat zużycia amunicji wynikający z dokładności wskazywania celów do porażenia ogniowego*[125].

Wielu teoretyków wojskowych uważa, że perspektywiczna walka zbrojna cechować się będzie dużą manewrowością, ukierunkowaną na ciągłe zajmowanie dogodniejszego położenia w stosunku do przeciwnika. Do osiągnięcia tego niezbędna będzie znajomość sytuacji po stronie przeciwnika, tak w przedniej strefie, jak i w głębi ugrupowania. Wykonujący manewr muszą zatem dysponować stosownymi środkami wykrywania, lokalizacji i zwalczania elementów ugrupowania przeciwnika, a dowódcy muszą mieć stworzone warunki do szybkiego podejmowania trafnych decyzji oraz sprawnego i skrytego wdrażania ich do realizacji. Warunki ku temu stwarza właściwie i pomyślnie przeprowadzona walka informacyjna. Dlatego też wymogi przyszłego pola walki nadają walce informacyjnej nową jakość.

---

[124] L. Ciborowski: *„Przestrzenie walki informacyjnej"*. AON, Warszawa 1997.

[125] $Z = x^2 + 2x + 1$, co oznacza, że jednokrotny wzrost błędu normatywnego przy wskazywaniu celu powoduje czterokrotnie większe zużycie amunicji, dwukrotny powoduje dziewięciokrotne jej zużycie itd. L. Ciborowski: *Wpływ informacji na walkę zbrojną*. W: *„Systemy rozpoznania i walki radioelektronicznej"*. I KNTWRE, Wyd. WAT, Zegiestów 1995.

Każdą walkę zbrojną powinna poprzedzać walka informacyjna, bo niemożliwe jest odniesienie zwycięstwa zbrojnego bez wcześniejszego pokonania systemów informacyjno — sterujących przeciwnika. Wszelkie działania związane z walką informacyjną sprowadzają się w swej istocie do stwarzania sytuacji utrudniających przeciwnikowi: podejmowanie trafnych decyzji, wykonywanie sprawnych ruchów wojskami i precyzyjnych uderzeń ogniowych. Innymi słowy, działania te ukierunkowane są na ciągłe dezorientowanie przeciwnika co do sytuacji pola walki, komplikowanie jego warunków działania i w efekcie — zmuszanie go do podejmowania błędnych decyzji. Niekoniecznie musi się to od razu wiązać ze stosowaniem nowoczesnych technik informacyjnych. Nowoczesna technika - najnowsze systemy elektroniczne — nie stworzyły nowego wymiaru walki. Nadały mu jedynie dostrzegalną w ostrzejszych zarysach nową jakość.

Już w przeszłości dowódcy poszukiwali odpowiedniej okazji (sposobności), aby dobrze poznać przeciwnika, teren i warunki atmosferyczne. Armie, które będą dążyć do odniesienia zwycięstwa przez prowadzenie walki informacyjnej, mogą bardzo szybko stracić moc bojową i być stroną przegraną jeśli napływ danych z pola walki zostanie zakłócony. Np. nowoczesne bronie inteligentne będą bezużyteczne, jeśli nie zostaną przekazane aktualne dane o przeciwniku za pomocą systemów informacyjno — sterujących.

Wnioski z podrozdziału 3.3.

- ✓ *Walka informacyjna ma zastosowanie we wszystkich scenariuszach walki zbrojnej. Właściwie przygotowana, zorganizowana i prowadzona umożliwia racjonalne wykorzystanie sił zbrojnych oraz systemów uzbrojenia, co stanowi zasadniczą podstawę osiągania sukcesu bojowego.*
- ✓ *Doświadczenia ostatnich konfliktów zbrojnych, a przede wszystkim rozwój techniki komputerowej, skłaniają do traktowania sił i środków przeznaczonych do prowadzenia walki informacyjnej jako specjalistycznej służby, funkcjonującej pod jednolitym dowództwem. Stwarzają potrzebę przygotowania dla nich wyspecjalizowa*nych ośrodków szkoleniowych.

3.4. Kluczowe efekty poznania

1. *Podstawą sukcesu w walce zbrojnej jest zawsze precyzja rażenia i czas reakcji ogniowej. Są to dwa podstawowe kryteria, których nieprzestrzeganie prowadzić będzie zawsze do wzrostu kosztów działań i zwiększania stopnia zagrożenia porażką. Warunki ku temu stwarza właściwie i pomyślnie przeprowadzona walka informacyjna. Dlatego też wymogi przyszłego pola walki nadają walce informacyjnej nową jakość. Rozpoznanie, zdobywając dane o przeciwniku, wpływa na precyzję rażenia,*

a zakłócanie informacyjne i obrona informacyjna — na osiąganie wyprzedzenia w użyciu celnego ognia.

2. *Każdy konflikt zbrojny poprzedza walka informacyjna i nie jest możliwe odniesienie zwycięstwa zbrojnego bez wcześniejszego pokonania systemów informacyjno — sterujących przeciwnika.*
3. *Walka zbrojna w XXI wieku będzie w głównej mierze oparta na informacji przekazywanej w czasie rzeczywistym, co wpłynie także na zmianę działań bojowych prowadzonych przez siły lądowe, które będą prowadzić operacje zarówno w czasie pokoju, jak i konfliktu. Walka informacyjna będzie podstawowym sposobem wykonania szerokozakresowych misji sił lądowych, włącznie z zabezpieczeniem państwa, przestrzeganiem umów pokojowych, zapobieganiem konfliktom i pokonaniem przeciwnika w walce.*
4. *Walka informacyjna koncentruje się na wykorzystaniu „świadomości sytuacyjnej", czyli uzyskaniu przewagi w wiedzy nad przeciwnikiem. Pozwala ona zastosować systemy informacyjno — sterujące i ich możliwości, uzyskać zaskoczenie, kontrolować sytuację w konflikcie lub krótkich działaniach wojennych, przy jednoczesnym pozbawieniu strony przeciwnej takich możliwości.*
5. *Siły zbrojne winny ciągle dysponować czynnym, dobrze zorganizowanym i w pełni zintegrowanym systemem walki informacyjnej, umożliwiającym śledzenie bieżącej sytuacji w otaczającej przestrzeni, a w sytuacjach kryzysowych i wojny — umożliwiającym rozwiązywanie problemów na wszystkich szczeblach dowodzenia.*

ZAKOŃCZENIE

Problemy badawcze rozwiązywane w rozprawie i uzyskane wyniki badań doprowadziły do osiągnięcia celu głównego, to jest wyodrębnienia, zdefiniowania i uporządkowania podstawowych pojęć i desygnatów walki informacyjnej, które odzwierciedlają najistotniejsze związki w jej przedmiocie, narzędziach i przestrzeni.

W procedurze poznawczej wykorzystywane były metody badań dostosowane do poznawania zjawisk złożonych. Podejście systemowe pozwoliło uzyskanie nowych efektów poznawczych, do których można zaliczyć:

1. Zdefiniowanie pojęć z zakresu walki informacyjnej, określenie jej przedmiotu i narzędzi oraz dokonanie podziału na podprzestrzenie, w jakich jest prowadzona.
2. Przedstawienie genezy walki informacyjnej i znaczenia, jakie odgrywała w przeszłości.
3. Określenie wpływu walki informacyjnej na współczesne i przyszłe działania zbrojne przeciwnika i wojsk własnych.

Przeprowadzone, w ramach rozprawy badania, potwierdzają ważność i aktualność walki informacyjnej na współczesnym polu walki, jak również w sferze cywilnej. Prowadzona była od czasów najdawniejszych, od kiedy tylko pojawiły się konflikty. Chociaż wcześniej nie była tak nazywana, to jednak w istocie rzeczy przez cały czas spełniała te same funkcje, sprowadzające się do uzyskiwania przewagi informacyjnej nad kooperantem negatywnym wzajemnym. Dziś, kiedy zarówno w życiu cywilnym, jak i wojskowym na szeroką skalę wykorzystywane są systemy informacyjno — sterujące, problematyka ta nabrała szczególnego znaczenia i wyrazistości. Dane o osobach, zdarzeniach, zjawiskach i procesach — w otoczeniu ciągle trwającej konkurencji — nabrały konkretnych wartości materialnych. Uzyskiwana w tym zakresie przewaga stała się nie tylko gwarantem, ale wręcz warunkiem bezpiecznej egzystencji i to nie tylko w skali pojedynczego człowieka czy instytucji, ale nawet w odniesieniu do państwa czy koalicji.

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 informacyjna 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 walki informacyjnej.

Zakres badań i zastosowane metody badawcze pozwoliły na osiągnięcie założonego celu badań, realizację zadań badawczych o charakterze poznawczym i końcową weryfikację hipotez roboczych.

Wnioski zawarte w poszczególnych rozdziałach są odpowiedzią na postawione problemy badawcze, a rozdział pierwszy, w którym dokonano definiowania pojęć i kategoryzacji walki informacyjnej, jest priorytetowy.

W zakresie porządkowania teorii walki informacyjnej dalszymi badaniami należałoby objąć problem planowania i organizowania walki informacyjnej na szczeblu operacyjnym i taktycznym.

*

* *

Autor wyraża serdeczne podziękowania Kierownikowi Naukowemu niniejszej rozprawy — Panu Pułkownikowi Doktorowi Habilitowanemu Leopoldowi Ciborowskiemu za pomoc merytoryczną i metodologiczną oraz wyrozumiałość i życzliwość w toku badań i podczas opracowywania rozprawy.

BIBLIOGRAFIA

1. Arystoteles: *„Fizyka i Metafizyka"*. Torino 1956.
2. Beer S.: *„Cybernetyka a zarządzanie"*. Warszawa 1986.
3. Bendkowski J.: *„Informacja ekonomiczna w przedsiębiorstwie"*. Politechnika Śląska, Gliwice 1993.
4. Berg A. I.: *„Informacja i cybernetyka"*. Wydawnictwa Naukowo — Techniczne, Warszawa 1970.
5. Biela A.: *„Informacja a decyzja"*. PWN, Warszawa 1976.
6. Brillouin. L.: *„Nauka a teoria informacji"*. PWN, Warszawa 1969.
7. Burhans W. A.: *Iraqi Air Defenses — Initial Soviet Post — Mortem*. W: *„Journal of Electronic Defense"*, October 1991.
8. Campen A. D: *„The first Information War"*. Virginia 1992.
9. Ciborowski L.: *Informacyjna preparacja pola walki*. Referat w materiałach III KNTWRE. Wyd. WAT, Zegiestów 1997.
10. Ciborowski L.: *„Organizacja rozpoznania w sztabach*. AON 1991.
11. Ciborowski L.: *„Planowanie i organizowanie walki zbrojnej wg poglądów NATO, cz.I, Procedura pracy dowódczo-sztabowej i jej techniczne wspomaganie"*. AON 1996.
12. Ciborowski L, Polko M.: *„Planowanie i organizowanie walki zbrojnej wg poglądów NATO, cz.II, Informacyjna preparacja pola walki"*. AON, Warszawa 1996.
13. Ciborowski L.: *„Przestrzenie walki informacyjnej"*. AON, Warszawa 1997.
14. Ciborowski L.: *„Rola i miejsce rozpoznania w systemie obronnym RP"*. AON, Warszawa 1993.
15. Ciborowski L., Nowacki G.: *Walka informacyjna*. Referat w materiałach III KNTWRE. Wyd. WAT, Zegiestów 1997.
16. Ciborowski L.: *„Wnioski z ćwiczeń prowadzonych przez wojska Sojuszu Atlantyckiego"*. AON, Warszawa 1993.
17. Ciborowski L.: *Wpływ informacji na walkę zbrojną*. W: *„Systemy rozpoznania i walki radioelektronicznej"*. I KNTWRE, Wyd. WAT, Zegiestów 1995.
18. Ciganik M.: *„Systemy informacyjne w nauce, technice i ekonomice"*. PWE, Warszawa 1984.

19. Czermiński A., Czapiewski M.: *„Organizacja procesów decyzyjnych"*. Uniwersytet Gdański, Gdańsk 1995.
20. Czarnawska M.: *„Jak się bronić przed indoktrynacją"*. Warszawa 1997.
21. Descartes R.: *„Zasady filozofii"*. Warszawa 1960.
22. Donald R., White J.: *„A Handbook Series on Elektromagnetic Interference and Copmpatibility"*. Wyd. Germantown, Maryland 1973.
23. Dudek Z.T., Sosnowski J.: *„Organizacja przesyłania informacji w systemach cyfrowych"*. PWN, Warszawa 1981.
24. Falicber O.: *Shilka`versus the B-52* . W: *„Krasnaja Zwiezda"* (Red Star), 4/1991.
25. Fitzgerald M. C.: *Russian views on information warfare*. W: *„Army"*, 5/1994.
26. Flakiewicz W.: *„Podejmowanie decyzji kierowniczych"*. Warszawa1983.
27. Gaładyk J.: *Rozpoznanie jako czynnik sztuki wojennej*. W: *„Przegląd Piechoty"* 1939.
28. Giboney T. B.: *Chaos informacyjny*. W: *„Military Review"*, 11/91.
29. Gołąb Z.: *„Wojna a system obronny państwa"*. Wydawnictwo MON, Warszawa 1984.
30. Grabau. R.: *Sechs Dimensionen des Kriegers*. W: *„Soldat und Technik"*, nr 6/1986.
31. Green G. H., Cotter C.: *„Nie pozwól sobą manipulować"*. Warszawa 1997.
32. Grier P.: *Information Warfare*. W: *„Air Force"*, 4/1994.
33. Hercman K.: *„Teoria informacji na użytek szkoły"*. Wydawnictwa Szkolne i Pedagogiczne, Olsztyn 1977.
34. Janczak J.: *„Obrona radioelektroniczna mobilnych systemów łączności"*. Wyd. AON, Warszawa 1998.
35. Janczak J.: *„Wybrane problemy walki radioelektronicznej"*. Wyd. WSOWŁ, Zegrze 1996.
36. Kaczmarek J.: *„Nauki wojskowe? (problem dyskusyjny)"*. „ZN" 1/92. AON, Warszawa.
37. Kaczmarek W.: *„Natarcie związku taktycznego"*. AON, Warszawa 1997.
38. Kaczmarek W., Ścibiorek Z.: *„Przyszła wojna —jaka?"*. ISBN. Warszawa 1995.
39. Kałużyński. S.: *„Imperium mongolskie"*. Warszawa 1970.
40. Kamiński S.: *„Nauka i metoda. Pojęcie nauki i klasyfikacja nauk"*. TN KUL, Lublin 1992.

41. Kamiński A.: *Metoda, technika, procedura badawcza w pedagogice empirycznej. Metodologia środowiskowych badań pedagogicznych.* W: *„Studia Pedagogiczne"*, Tom XIX, Wrocław 1970.
42. Keramas J. G.: *„Workforce Training for Global Copmpetitivenes"*. AFCEA — Stockholm Symposium and Exposition, 1995.
43. Keuren E. V., Knighten J.: *„Implications of the High — Power Microwave Weapon Threat in Electronic System Design"*. IEEE Intern. Symp. on EMC, 1991 Cherry Hill.
44. Killen H.B.: *„Transmisja cyfrowa w systemach światłowodowych i satelitarnych"*. Wyd. KiŁ, Warszawa 1992.
45. Kirschner J.: *„Manipulować — ale jak?"*. Warszawa 1994.
46. Kolman R.: *„Poradnik dla doktorantów i habilitantów"*. ISBN, Bydgoszcz 1994.
47. Kopaliński. W.: *Słownik wyrazów obcych i zwrotów obcojęzycznych.* Wiedza Powszechna, Warszawa 1980.
48. Kotarbiński T.: *„Elementy teorii poznania, logiki formalnej i metodologii nauk"*. Ossolineum. Wrocław — Warszawa — Kraków 1961.
49. Kotarbiński. T.: *„Traktat o dobrej robocie"*., Wrocław 1982.
50. Kotarbiński T.: *„Wykłady z dziejów logiki"*. Zakład Naukowy im. Ossolińskich,
51. Kozaczuk W.:"*„Wojna w eterze"*. Warszawa 1977.
52. Kozaczuk W.: *„W kręgu Enigmy"*. Wydawnictwo „Książka i Wiedza". Warszawa 1986.
53. Koziej St.: *Czynniki walki zbrojnej.* W: *„ZN"*, 4/93.
54. Koziej St.: *Czynniki walki zbrojnej.* W: „ZN", 4/93.
55. Koziej S.: *„Podstawy i zasady sztuki wojennej"*. AON, Warszawa 1993.
56. Koziej S.: *„Teoria sztuki wojennej"*. AON, Warszawa 1993.
57. Kozielecki J.: „Psychologiczna teoria decyzji". Warszawa 1977.
58. Kulikowski J. L.: *„Komputery w badaniach doświadczalnych"*. PWN, Warszawa 1993.
59. Kunikowski J.: *„Człowiek a technika wojenna"*. AON, 1995.
60. Kuratowski K., Mostowski A.: *„Teoria mnogości"*. PWN, Warszawa 1978.
61. Kurnal J.: *„Zarys teorii organizacji i zarządzania"*. Warszawa 1970.

62. Kwećka R., Nowak A.: *„Budowa modelu systemu rozpoznania wojskowego w aspekcie organizacyjnym i informacyjnym"*. Rozprawa doktorska, Wyd. AON, Warszawa 1994.
63. Leonhard R.: *„The art of Maneuver"*. Novato 1991.
64. Łobocki M.: *„Metody badań pedagogicznych"*. PWN, Warszawa 1978.
65. Łokociejewski M.: *Ogólne założenia rozpoznania wojskowego*. W: *"Zeszyty Naukowe"*, nr 4, AON , Warszawa 1996.
66. Maliszewski W.: *„Oddziaływanie psychologiczne w operacji obronnej"*. Rozprawa doktorska, AON, Warszawa 1998.
67. Markiewicz L.: *„Ultradźwięki i infradźwięki"*. PWN, Warszawa 1979.
68. Mazur M.: *„Jakościowa teoria informacji"*, Warszawa 1970.
69. Mendel T.: *„Metodyka pisania prac doktorskich"*. ISBN, Poznań 1995.
70. Mitiugow W.: *„Fizyczne podstawy teorii informacji"*. PWN, Warszawa 1980.
71. Mróz W.: *Usprawnienie funkcjonowania wojskowych organów kierowania*. W: *„Zeszyty Naukowe"*, AON, 2/1994.
72. Nadolski A.: *„Grunwald 1410"*. Wydawnictwo Bellona, Warszawa 1993.
73. Nawrat.: *Manipulacja społeczna — przegląd technik i wybranych wyników badań*. W: *„Przegląd Psychologiczny"*, 1/1989.
74. Neri F.: *„Introduction to Electronic Defense Systems"*. Artech House, Inc., 1991.
75. Nożko K.: *„Walka o przewagę"*. MON, Warszawa 1985.
76. Ochman J.: *„Integracja w systemach informatycznych zarządzania"*. Państwowe Wydawnictwo Ekonomiczne, Warszawa 1992.
77. Okoń W.: *„Elementy dydaktyki szkoły wyższej"*. PWN, Warszawa 1971.
78. Okoń W.: *„Słownik pedagogiczny"*. PWN, Warszawa 1992.
79. Peterson K., Pracht U.: *Walka informacyjna*. W: *„Soldat und Technik"*, 12/95.
80. Piekarski H.: *„Istota i charakter walki radioelektronicznej w SZ RP"*. AON, Warszawa 1993.
81. Piekarski H.: *„Osłona radioelektroniczna systemu obronnego RP"*. AON, Warszawa 1992.
82. Piekarski H.: *„Podstawowe kategorie sztuki wojennej"*. AON, Warszawa 1996.
83. Piekarski H.: *„Walka radioelektroniczna"*. MON, Warszawa 1980.
84. Piekarski H.: *„Właściwości działań bojowych sił i środków walki radioelektronicznej w obezwładnieniu systemów broni precyzyjnej"*. ASG, Warszawa 1987.

85. Pierce J. R.: *„Symbole, sygnały i szumy"*. PWN, Warszawa 1967.
86. Pieter J.: *„Ogólna metodologia pracy naukowej"*. Warszawa 1967.
101. Pilch T.: *„Zasady badań pedagogicznych"*. Wydawnictwo „Żak", Warszawa 1995.
102. Pindlowa W.: *„Infometria w nauce o informacji"*. Universitas, Kraków 1994.
103. Picq A.: *„Studium o walce"*. Warszawa 1927.
104. Popper K. R.: *„Logika odkrycia naukowego"*. PWN, Warszawa 1977.
105. Pytkowski W.: *„Organizacja badań i ocena prac naukowych"*. PWN, Warszawa 1985.
106. Reykowski J.: *„Osobowość a społeczne zachowanie się ludzi"*. Warszawa 1976.
107. Riccardelli R. F.: *The Information and Intelligence*. W: *„Military Review", 5/95.*
108. Rogucki A.: *„Analiza systemów w planowaniu obrony"*. Wydawnictwo MON, Warszawa 1975.
109. Ross J. D.: *Wojna o informację*. W: *„Army"*, 2/1994.
110. Rotkiewicz W.: *„Kompatybilność elektromagnetyczna w radiotechnice"*. Wyd. KiŁ, Warszawa 1978.
111. Rudniański T.: *„Przed decyzją"*. Warszawa 1965.
112. Rutkowski C.: *Podstawowe pojęcia z dziedziny bezpieczeństwa i obronności państwa*. W: *„Myśl Wojskowa"* nr 2, 1996.
113. Ryniewicz Z.: *„Bitwy świata"*. Leksykon, Wiedza Powszechna, Warszawa 1995.
114. Schwartau Winn.: *„Information Warfare — Cyberterrorism: Protecting Your Personal Security in the Electronic Age"*. 1993.
115. Seidler J.:*„Podstawy, modele źródeł i wstępne przetwarzanie informacji"*. Wydawnictwo Naukowo — Techniczne. Warszawa 1983r.
116. Seidlar. J.: *„Nauka o informacji"*. T I, II. WNT, Warszawa 1983.
117. Shannon. C. E, Warren. W.: *„The Mathematical Theory of Communication"*. The University of Illinois Press, Urbana 1949.
118. Sienkiewicz P.: *Analiza systemowa: geneza, rozwój, zastosowanie problemu naukowego p.k. „Doskonalenie"*. AON, Warszawa 1992.
119. Sienkiewicz P.: *„Analiza systemowa: metodologia modelowania systemowego; przykłady modeli systemowych; podstawy metodologiczne teorii, analizy i inżynierii systemów"*. AON, Warszawa 1994.
120. Sienkiewicz P.:*„Badania systemowe w wojsku: studium metodologiczne"*. ASG, Warszawa 1980.
121. Sienkiewicz P.: *„Inżynieria systemów"*. MON, Warszawa 1983.

122. Sienkiewicz P.: *Metodologiczne podstawy oceny potencjałów i efektywności bojowej systemów wojskowych: sprawozdanie z II etapu realizacji problemu naukowego p.k. „Doskonalenie"*. AON, Warszawa 1992.
123. Sienkiewicz P.: *„Podstawy teorii systemów"*. AON, Warszawa 1993.
124. Sienkiewicz P.: *„Systemy kierowania"*. Wiedza Powszechna, Warszawa 1989.
125. Sienkiewicz P.: *„Zastosowanie techniki komputerowej w dowodzeniu wojskami: opracowanie modeli matematycznych; nowe tendencje w modelowaniu walki"*. AON, Warszawa 1994.
126. Sienkiewicz P.: *Wartości, oceny i efektywność systemów*. W: *„Zeszyty Naukowe"*, AON, 4 /1994.
127. Sikorski K.: *„Doskonalenie obrony radioelektronicznej DZ w początkowym okresie wojny"*. Rozprawa doktorska. Wyd. ASG, Warszawa 1989.
128. Simpkin R.: *„Race to the Swift"*. Oxford and London 1985.
129. Słupecki J., Hałkowska K., Piróg — Rzepecka K.: *„Logika i teoria mnogości"*. PWN, Warszawa 1994, s.204.
130. Sochal Cz., Wierciński L.: *„Rozpoznanie wojskowe"*. MON, Warszawa 1975.
131. Sokołowski A.: *„Ochrona informacji komputerowych". Wydawnictwo MON, Warszawa 1987.*
132. Stankiewicz W.: *„Ekonomika wojenna"*. Wydawnictwo MON. Warszawa 1981.
133. Starry M. D., Arneson C. W.: *Działania informacyjne*. W: *„Military Review"*, 6/96.
134. Strasburger D.: *„Zasady sztuki wojennej (od XI wieku do 1871 roku)"*. Skrypt AON.
135. Sullivan G. R., Dubik J. M.: *War in the Information Age*. W: *„Military Review"*, 4/1994.
136. Sun Tzu: *„Sztuka wojny"*. Wydawnictwo Przedświt, Warszawa 1994.
137. Szaniawski K.: *Pragmatyczna wartość informacji*. W: *„Problemy psychologii matematycznej"*, pod red. J. Kozieleckiego. Warszawa 1971, PWN.
138. Sztumski J.: *„Wstęp do metod i technik badań społecznych"*, Katowice 1976.
139. Szulc B., Zieliński J., Sadowski S.: *Prawa i reguły walki zbrojnej pk. „Walka zbrojna — 2"*. AON, Warszawa 1997.
140. Szulc B.: *Przywództwo w dowodzeniu wojskami pk. „Oficer"*. AON, Warszawa 1995.
141. Szulc B.: *Przywództwo w dowodzeniu wojskami: (cechy i procedury przywództwa — wyniki do badań sondażowych) pk. „Oficer — 2"*. AON, Warszawa 1997.

142. Szulc B.: *Przywództwo w dowodzeniu wojskami: kształtowanie cech przywódczych pk. „Oficer — 3"*. AON, Warszawa 1998.
143. Szulc B.: *„Walka zbrojna w kontekście ogólnej teorii walki i teorii konfliktów"*. AON, Warszawa 1996.
144. Szulc B., Sikorski B.: *Zakres i treść rozwiązywania problemów przez oficerów funkcyjnych w operacji obronnej pk. „Proces — 2"*. AON, Warszawa 1996.
145. Szydłowski A.: *O psychologicznym podłożu maskowania*. W: *„Myśl wojskowa"* 4/96.
146. Ścibiorek Z.: *„Obrona związku taktycznego (oddziału)"*. AON, Warszawa 1993.
147. Ścibiorek Z., Kaczmarek W.: *„Przyszłe pole walki"*. AON, Warszawa 1995.
148. Ścibiorek Z: *„Wpływ nowych środków walki na działania bojowe wojsk lądowych"*. AON, Warszawa 1993.
149. Świątnicki W. Z.: *„Bronie inteligentne"*. ISBN, Warszawa 1992.
150. Tiemnikow F. E., Afonin W. A., Dmitrijew W. I.: *„Podstawy techniki informacyjnej"*. Wydawnictwo Naukowo — Techniczne, Warszawa 1974.
151. Toffler Alvin i Heidi: *„Wojna i antywojna" (War and Antiwar)*. 1993.
152. Twardowski K.: *„Wybór pism psychologicznych i pedagogicznych"*. Warszawa 1992.
153. Umberto E.: *„Nieobecna struktura"*. Milano 1991.
154. Wiatr M., R. Kwećka.: *„Sztuka wojenna lat dziewięćdziesiątych"*. AON, Warszawa 1997.
155. Winterbotham F. W.: *„The Ultra Secret"*. Londyn 1974.
156. Wojnar A.: *„Systemy RRL"*. Wyd. KiŁ Warszawa 1989.
157. Woźnicki J.: *„Techniki informacyjne — integracja wiedzy"*. Krajowe Sympozjum Telekomunikacji, 1995.
158. Wróblewski Z.: *„Działalność informacyjna wydziału rozpoznawczego sztabu związku taktycznego w obronie"*. Rozprawa doktorska, AON 1993.
159. Zaczyński W.: *„Praca badawcza nauczyciela"*. Warszawa 1968.
160. Zieliński J.: *„Teoria rozpoznania wojskowego"*. Rozprawa doktorska, ASG, Warszawa 1986.
161. Zieliński J.: *„Rozpoznanie i ocena nieprzyjaciela w działaniach bojowych"*. Rozprawa habilitacyjna, AON 1993.
162. Ziembiński Z.: *„Logika praktyczna"*. PWN, Warszaw 1994.