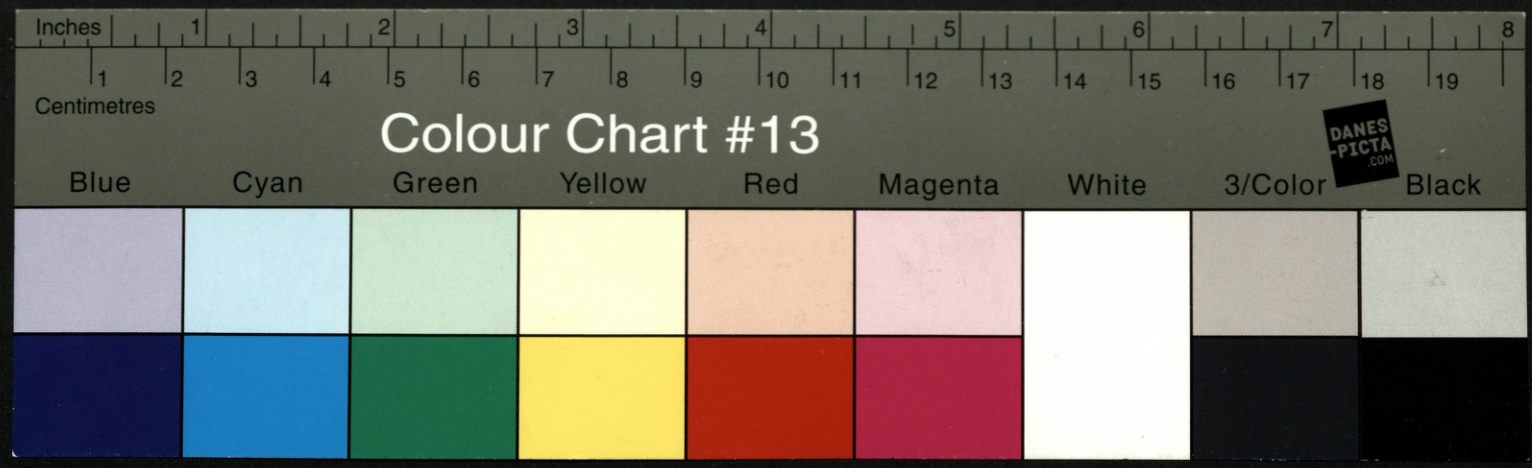
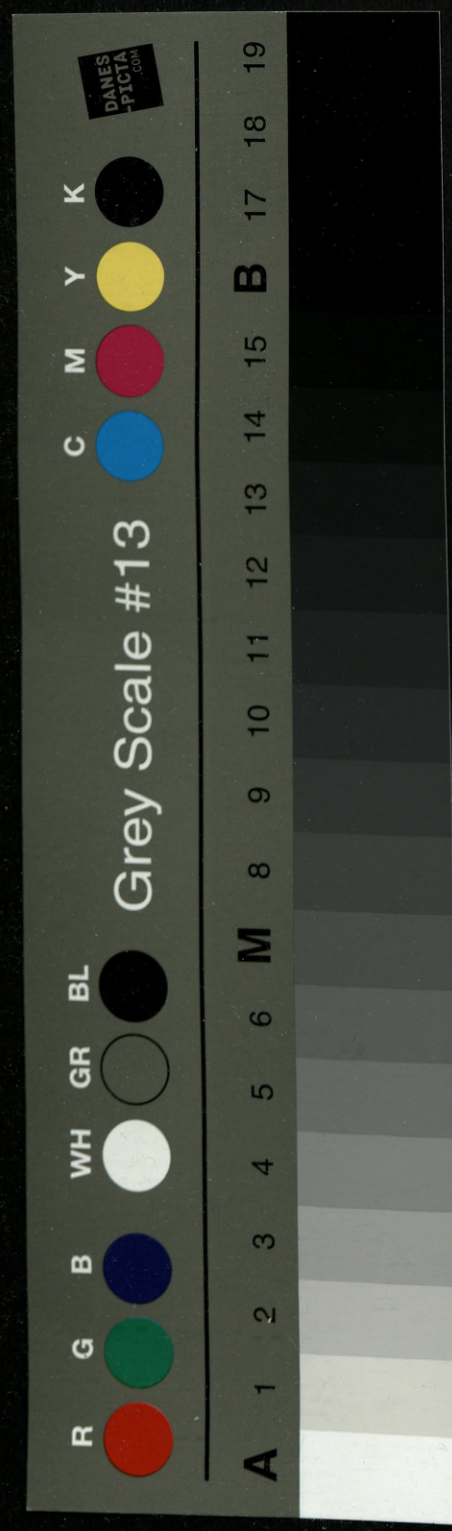




RYSZARD SZPYRA



MILITARNE OPERACJE INFORMACYJNE

AKADEMIA OBRONY NARODOWEJ

AKADEMIA OBRONY NARODOWEJ

Ryszard Szpyra

MILITARNE OPERACJE INFORMACYJNE

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid.
Akademii Obrony Narodowej
56910

Warszawa 2003

Projekt okładki: **Ewa Wiśniewska**

Redaktor: **Jerzy Wajs**

Redaktor techniczny: **Beata Klarowska**

Korekta: **Małgorzata Sęktas**

ISBN 83-89423-40-5

Sygn. AON 5568/03

Skład, druk i oprawa: Akademia Obrony Narodowej – Wydział Wydawniczy
00-910 Warszawa, al. gen. A. Chruściela 103, tel. 681-40-55, tel./faks 681-37-52
Zam. nr 989/2003

SPIS TREŚCI

WSTĘP 5

1. IDENTYFIKACJA UWARUNKOWAŃ ISTOTY MILITARNYCH OPERACJI INFORMACYJNYCH 8
1.1. Uwarunkowania cywilizacyjne operacji informacyjnych 8
1.2. Ocena piśmiennictwa 12
1.3. Analiza terminologiczna 25
1.3.1. Terminologia ogólna 25
1.3.2. Pojęcia „sztuka wojskowa" i „sztuka wojenna" 28
1.4. Działania międzynarodowe państwa 44
1.5. Operacje militarne państwa 53
1.6. Militarna walka o interesy 60

2. TEORIA INFORMACJI A OPERACJE INFORMACYJNE 66
2.1. Przegląd teorii informacji 66
2.2. Podejście społeczne teorii informacji 74

3. GENEZA, ISTOTA I ROZWÓJ OPERACJI INFORMACYJNYCH 81

4. ELEMENTY MILITARNEJ WALKI INFORMACYJNEJ 106
4.1. Walka elektroniczna 106
4.2. Formy ataku informacyjnego 109
4.2.1. Atak informatyczny (w sferze przetwarzania danych cyfrowych) 109
4.2.2. Atak elektroniczny 118
4.2.3. Atak ogniowy 129
4.2.4. Działania psychologiczne (atak psychologiczny) 130
4.2.5. Dezinformacja wojskowa (mylenie) 135
4.3. Formy obrony informacyjnej 140
4.3.1. Obezwładnianie i odstraszanie rozpoznania informacyjnych ataków 143
4.3.2. Ochrona własnej informacji i systemów informacyjnego komunikowania 143

5. INFORMACYJNE ZABEZPIECZENIE 149
5.1. Ustalenia terminologiczne 149
5.2. Rozpoznanie osobowe 156
5.3. Rozpoznanie techniczne 157
5.4. Rozpoznanie informatyczne 159
5.5. Rozpoznanie powietrzne 160

6. PRZYSZŁA MILITARNA WALKA INFORMACYJNA 165
6.1. Wnioski dotyczące identyfikacji trendów i konstrukcji koncepcji militarnej walki informacyjnej przyszłości 165
6.2. Walka o przewagę informacyjną 166
6.2.1. Dominacja powietrzna 167
6.2.2. Dominacja informacyjna 170
6.3. Informacyjny atak strategiczny 176
6.3.1. Powietrzny atak strategiczny 176
6.3.2. Informacyjny atak strategiczny 184
6.4. Informacyjne działania wspierające 193
6.4.1. Izolacja 193
6.4.2. Bezpośrednie wspieranie informacyjne 196

ZAKOŃCZENIE 199

BIBLIOGRAFIA 202

SPIS RYSUNKÓW 208

SPIS TABEL 210

WSTĘP

Przełom XX i XXI w. jest spektakularny przede wszystkim ze względu na zaistniałe zadziwiające i dramatyczne zjawiska. Ich przykładem może być ekspansja Internetu oraz eskalacja terroryzmu z dramatycznym, niekonwencjonalnym atakiem lotniczym na wieże World Trade Center w Nowym Jorku i Pentagon w Waszyngtonie 11 września 2001 r.

Implikacje zmian wynikających z tworzenia się nowej cywilizacji – społeczeństwa informacyjnego – są jeszcze słabo uzmysłowione nie tylko w zbiorowej świadomości, lecz także w sferze różnych obszarów aktywności naukowej. Wiele zagadnień związanych z rozwojem cywilizacyjnym, ciągle jeszcze traktuje się bardziej jako ciekawostka, aniżeli realne zjawisko. Przykładem takiego podejścia jest ów tragiczny atak lotniczy. Sygnalizowane wcześniej przez niektórych badaczy zagrożenia terroryzmem były przyjmowane do wiadomości, lecz uzyskały małe poparcie w praktyce. Dopiero dramatyczna weryfikacja uwiarygodniła oceny i prognozy.

Rozwój cywilizacyjny w sferze informacyjnej również niesie ze sobą dramatyczne zmiany w możliwościach prowadzenia walki zarówno w sferze stosunków międzypaństwowych, międzyorganizacyjnych, jak i międzyludzkich. Stwarza też nowe jakości w kreowaniu współpracy we wszystkich tych sferach. Wielu badaczy na arenie międzynarodowej już podejmuje te sprawy w swojej działalności naukowej. Pojawiły się także pierwsze próby refleksji naukowej w tym obszarze i w Polsce. Ciągle jednak nie znajdują one wystarczającego zainteresowania praktyki, ale także nauki. Wiadomo już przecież, że w wyniku ataków informacyjnych można sparaliżować wysoko rozwinięty kraj. Można nawet zmieniać świadomość całych społeczeństw. Możliwości informacyjnego atakowania dotyczą wszystkich sfer aktywności społecznej i państwowej. Stanowi to z jednej strony poważne zagrożenie, z drugiej zaś stwarza nowe możliwości ataku.

Wstępne analizy piśmiennictwa dotyczącego działań w sferze informacyjnej ujawniły koncentrowanie się badaczy na wnętrzu badanych zjawisk lub na próbach wpasowania nowych zjawisk w starą rzeczywistość. Przykładem takiego podejścia jest stanowisko Leopolda Ciborowskiego, który uważa np., że walka informacyjna jest służebna wobec innej zasadniczej walki wspieranej. Nigdy zaś nie może występować w oderwaniu, bo nigdy też sama dla siebie nie może stanowić celu. Jej

cel wynika zawsze z charakteru i celu walki wspieranej[1]. Stanowisko takie zabarwione jest obawą przed naruszaniem status quo, w którym istnieją klasyczne walki, a nowe zjawiska są usługowe w stosunku do nich. Tymczasem zarówno walka lądowa, jak i walka w powietrzu, a także walka informacyjna nie tyle zmierzają do osiągnięcia swoich celów, co do osiągnięcia nadrzędnego celu politycznego, dla którego są prowadzone. Należałoby więc uznać, że wszystkie walki są walkami wspierającymi wysiłek związany z osiągnięciem celu politycznego.

Powszechnie znane są też sytuacje, w których tylko walka informacyjna doprowadziła do osiągnięcia celu politycznego. Warto tu przypomnieć amerykańską operację pomocy humanitarnej w Somalii. Amerykanie próbowali ukrócić negatywną działalność grupy kierowanej przez lokalnego przywódcę, zaangażowali się więc w działania zbrojne przeciwko tej grupie. Atakowany przywódca postanowił pozbyć się Amerykanów. Mógł próbować pokonać ich na lądzie. Wymagało to jednak czasu i znacznych kosztów. Sięgnął więc do arsenału nowych form walki – walki informacyjnej. Uprowadzono i zabito kilku amerykańskich żołnierzy, co nie było trudne, gdyż żołnierze ci w większości brali udział w dystrybucji żywności, a nie w walce. Równolegle sprowadzono ekipy telewizyjne i na oczach całego świata bezczeszczono zwłoki zabitych. Docierająca do Stanów Zjednoczonych informacja wywołała szok w amerykańskim społeczeństwie i jego presję na rząd. Ten atak informacyjny spowodował raptowne wycofanie się Stanów Zjednoczonych z prowadzonej operacji. Doprowadził więc do osiągnięcia pożądanego celu politycznego tańszym kosztem i w krótszym czasie, niżby to miało miejsce przy zastosowaniu klasycznej walki zbrojnej. Walka informacyjna wystąpiła więc nie w roli walki wspierającej, lecz głównej.

Takie przykłady można mnożyć. W rezultacie utrwala się nie tylko przekonanie o tym, że walka informacyjna może być samodzielna, lecz także o tym, że coraz częściej może ona być główną formą walki.

Rezultaty przeglądu piśmiennictwa uzmysłowiły konieczność unikania fałszywych odniesień. Stało się oczywiste, że nie sposób badać działania komponentu militarnego w sferze informacyjnej, nie poznając istoty działań całego mechanizmu, w którym ulokowany jest ten komponent. Takim mechanizmem – w odniesieniu do komponentu państwa, jakim są siły zbrojne – jest niewątpliwie państwo i jego działania. To przeświadczenie stało się inspiracją do konstrukcji procesu badawczego.

Wyniki badań przedstawiono w postaci opracowania składającego się ze wstępu, sześciu rozdziałów, zakończenia i bibliografii.

Rozdział pierwszy poświęcono identyfikacji uwarunkowań istoty militarnych operacji informacyjnych.

Rozdział drugi koncentruje się na prezentacji najbardziej przydatnej, z punktu widzenia niniejszej publikacji, koncepcji teorii informacji.

---

[1] Zob. L. Ciborowski, *Walka informacyjna*, Toruń 1999, s. 69.

Rozdział trzeci omawia treści zmierzające do zidentyfikowania istoty operacji informacyjnych oraz militarnych operacji informacyjnych.

Rozdział czwarty prezentuje elementy militarnej walki informacyjnej. Treść rozdziału rozpoczyna dekompozycja militarnej walki informacyjnej oraz prezentacja przyjętego rozumienia komponentów tej walki i towarzyszących jej kategorii. W dalszej części znajduje się charakterystyka komponentów militarnej walki informacyjnej prowadzona z uwzględnieniem ich podziału według kryterium rodzaju działań.

Rozdział piąty poświęcono informacyjnemu zabezpieczeniu. Początkowe treści tego rozdziału są poświęcone analizie znaczeniowej różnych kategorii funkcjonujących w tym obszarze w piśmiennictwie i praktyce Zachodu i Polski oraz zalet i wad istniejących układów kategorii. Następnie omówiono poszukiwania adekwatnego do potrzeb koncepcji badań sposobu dekompozycji rozpoznania oraz przedstawiono przyjęty wielokryterialny podział pragmatyczny. Rozdział zamyka prezentacja syntetycznej charakterystyki elementów przeprowadzonej dekompozycji.

Rozdział szósty prezentuje prawdopodobne kierunki rozwoju militarnych operacji informacyjnych, określone w wyniku zastosowania analogii rozwoju – bardzo zbliżonej właściwościami – teorii walki sił powietrznych.

1. IDENTYFIKACJA UWARUNKOWAŃ ISTOTY MILITARNYCH OPERACJI INFORMACYJNYCH

1.1. Uwarunkowania cywilizacyjne operacji informacyjnych

Przełom wieków przyniósł wiele rewolucyjnych zmian oraz niebywały ferment intelektualny w wielu obszarach ludzkiego myślenia. Dotyczy to w pełni także sfery militarnej. Obecnie toczą się dyskusje, m.in. na temat istoty wojny, form operacji militarnych, militarnych operacji pozawojennych, niemilitarnych operacji wojennych. Refleksja teoretyczna jest często stymulowana wyprzedzającymi ją działaniami praktycznymi. Czasem można odnieść wrażenie, że nie nadąża za praktyką. Przyczyną tego jest powszechnie obserwowane przyspieszenie rozwoju cywilizacyjnego i pojawianie się w rezultacie tego coraz większej dynamiki zmian. Przeobrażenia, które w przeszłości trwały wieki lub dziesięciolecia, obecnie zachodzą w ciągu pojedynczych lat, a nawet szybciej. Gwałtowny rozwój sieci komputerowych i pojawiające się spontaniczne formy walki w tych sieciach to jeden ze spektakularnych przykładów. Wbrew pozorom efekty tej walki mogą być bardziej dotkliwe od użycia klasycznej broni. Walka tego typu dotyczyła najpierw poziomu mikro, co w sferze militarnej oznacza niski szczebel taktyczny, wkrótce jednak objęła swoim zasięgiem również najwyższe poziomy makro, docierając do szczebla strategicznego. W reakcji na obserwowane zjawisko wiele środowisk i wielu myślicieli podjęło wysiłek intelektualny nad badaniem tej sfery walki.

To nie jedyny przykład dotyczący nowych zjawisk. Głębokim i dynamicznym zmianom cywilizacyjnym towarzyszy też poszukiwanie nowych idei. Nie jest ono obce i środowisku wojskowemu. W militarnych kręgach intelektualnych Zachodu popularny jest postulat *outside box thinking*, co w wolnym przekładzie oznacza zachętę do przekraczania własnych barier myślenia i pokonywania istniejących, szeroko rozumianych dogmatów.

Ten ferment intelektualny trwa nie tylko w krajach Zachodu. Wiele nowych idei i pomysłów wykluwa się także w innych cywilizacjach. Niektóre z nich są niezwykle interesujące i twórcze. Przykładem mogą tu być propozycje intelektualne wyłożone przez dwóch chińskich oficerów w niedawno wydanej przez nich książce

zatytułowanej *Nieograniczona walka*[2]. Prezentują w niej wiele interesujących tez. Do najbardziej radykalnych należy przekonanie, iż **„[...] granice między żołnierzami i nie żołnierzami zostały obecnie zatarte, a przepaść między walką i nie walką niemalże zanikła, także globalizacja uczyniła wszystkie problemy współzależnymi i wzajemnie powiązanymi, dlatego też należy znaleźć klucz do stawienia czoła tym zjawiskom. Klucz, który powinien otworzyć wszystkie zamki zamykające drzwi do wojny. Ponadto klucz ten powinien pasować do wszystkich poziomów i wymiarów wojny od polityki, przez strategię, operacyjne techniki, po taktykę. Powinien on także być użyteczny zarówno dla polityków i generałów, jak i zwykłych żołnierzy. Trudno sobie wyobrazić bardziej odpowiedni klucz niż nieograniczona walka"**[3].

Wobec takiego stanowiska pojawia się szereg wątpliwości, wynikających m.in. z ustaleń sztuki wojennej. Wątpliwości te autorzy starają się rozwiać szeroką argumentacją. Pytają oni m.in. – Dlaczego ludzie, mając niemalże nieograniczone możliwości wyboru dogodnej formy prowadzenia walki, mieliby się ograniczać do wyboru form, które sprowadzają się do sfery sił zbrojnych i potęgi militarnej. – i zarazem odpowiadają: Przecież formy, które nie charakteryzują się użyciem sił zbrojnych i potęgi militarnej, a nawet nie są związane z występowaniem przelewu krwi i ofiar, tak samo gwarantują pomyślne osiąganie celów wojny, a nawet osiąganie większych korzyści, niż gdy używa się potęgi militarnej"[4].

Dostrzegają oni także granice tradycyjnych możliwości sfery militarnej.

„Przez długi okres przed wynalezieniem broni palnej, pola walki były małe i zwarte. Gwałtowny rozwój technologii militarnych spowodował systematyczne rozszerzanie przestrzeni walki. Przechodzenie od punktowego do liniowego, a następnie od dwuwymiarowego do trójwymiarowego pola walki, zajęło stosunkowo mało czasu w procesie historycznego rozwoju ludzkości. Obecnie z punktu widzenia rozwoju technologii przestrzeń walki osiągnęła swoje limity. Prawdziwie rewolucyjną zmianą jest przeniesienie pola walki do nienaturalnych przestrzeni. [...] Jeśli ograniczymy się jedynie do walki rozumianej w wąskim, militarnym sensie, prowadzonej na tradycyjnym polu walki zbrojnej, odzyskanie punktu zaczepienia w przyszłości będzie nader trudne. Jakakolwiek wojna, która wybuchnie w przyszłości, charakteryzować się będzie walką postrzeganą w szerokim sensie. Będzie ona koktajlem – mieszaniną różnych form walki, zarówno tych prowadzonych przez siły zbrojne, jak i tych stosowanych przez pozamilitarne organizacje"[5].

Autorzy ci wskazują także na praktykę, twierdząc, że: „Obecnie ludzkość dysponuje bogatą gamą technologii, które mogą wywoływać strach. Wymaga to jedynie nieco wyobraźni w modyfikacji i zastosowaniu znanych już technologii. Tego

---

[2] Q. Liang, W. Xiangsu, *Unrestricted Warfare: Assumptions on War and Tactics in the Age of Globalization*, Beijing 1999, tłumaczenie na język angielski: US CIA's Foreign Broadcast Information Service, udostępnione w 2000 r. pod adresami:
http://www. terrorism.com/documents/unrestricted.pdf – lub – http://cryptome.org/cuw.zip.

[3] Tamże.

[4] Tamże.

[5] Tamże.

typu bronie są intensywnie rozwijane. Czyni się to jednak najczęściej skrycie. Jest wystarczająco dużo sygnałów potwierdzających to zjawisko"[6].

Mimo kontrowersyjności postulatu nieograniczonej walki, diagnoza obecnej sytuacji jest niezwykle trafna, sama zaś sytuacja zachęca do podejmowania poszukiwań badawczych w wyłaniających się obszarach aktywności militarnej. Należy się zgodzić z wieloma tezami autorów, które są rezultatem ich głębokich przemyśleń i szerokiej argumentacji. Niewątpliwie następuje intensywny rozwój nowych rodzajów broni oraz poszukiwanie i wdrażanie nowych form prowadzenia walki i wojny. Jednak sam rozwój technologiczny, nawet na najwyższym poziomie, nie jest gwarancją bezpieczeństwa i sukcesów w rozstrzyganiu przyszłych konfliktów, a rozwinięte technologie nie mogą stać się synonimem przyszłej broni i walki. Nowe koncepcje broni nie opierają się na osiągnięciach nowych technologii, lecz na twórczym myśleniu. Dla dostrzeżenia i uznania takich koncepcji, niezbędne jest porzucenie przywiązania do tradycyjnego myślenia i zaakceptowanie nowego paradygmatu. Paradygmat ten można opisać szeregiem tez, takich jak: *Jako broń należy traktować wszystko, co wykracza poza sferę militarną, jednakże – co może być użyte w operacjach militarnych. Wszystko, co może przynosić korzyść człowiekowi może mu także szkodzić, będąc w rezultacie bronią.*

Mogą złagodzić formy prowadzenia wojny, ale nie zmieni się jej istota, którą jest przemoc i dlatego też nie zmieni to okrutności rezultatów wojny. Perspektywą przyszłych zmian nie jest mechaniczne rozszerzanie istniejących przestrzeni walki, jest nią natomiast przeniesienie pola walki do nienaturalnych przestrzeni. Przykładem może być przestrzeń elektromagnetyczna, cybernetyczna, finansowa.

Czas fundamentalnych zmian przestrzeni walki nie jest odległy. W przeszłości walka w cyberprzestrzeni czy walka w przestrzeni *nano*[7] była trudna do wyobrażenia, a tymczasem na naszych oczach staje się rzeczywistością. Coraz częściej nowe formy walki prowadzone będą równolegle z tradycyjnymi sposobami. Te różne przestrzenie walki będą się nakładać na siebie i wzajemnie uzupełniać. Dlatego też walka toczyć się będzie zarówno w sferze makroskopowej, jak i mikroskopowej, a także w wielu innych sferach definiowanych przez wykorzystywane w nich zjawiska. Tworzyć to będzie niezwykle bogate, nieznane w historii ludzkości pole walki.

Wraz z postępującym zacieraniem się różnic pomiędzy technologią wojskową i cywilną oraz między profesjonalnym żołnierzem i nieprofesjonalnym wojownikiem przestrzeń walki będzie się coraz bardziej mieszać z innymi przestrzeniami, w których nie toczy się walka. Granice ograniczające przestrzenie walki będą zanikać. Walka będzie obejmować przestrzenie cywilnej sfery działalności, stając się wszechobecną. Do prowadzenia ataku w określonej sferze potrzebne będzie jedy-

---

[6] Tamże.

[7] Jest to przestrzeń skali mikro. Podejmuje się działania mające na celu budowanie urządzeń, składających się z komponentów zawierających jedynie niewielkie ilości pojedynczych molekuł. Urządzenia takie mogłyby np. wnikać do wnętrza organizmów żywych lub struktur materii nieożywionej i modyfikować je odpowiednio do potrzeb.

nie posiadanie określonych zdolności i woli osiągnięcia pożądanego celu. Wyraźnie dostrzegalna jest tendencja ucywilniania walki. Zanikają także tradycyjne podziały ról w społeczeństwie. Walka przestaje być domeną jedynie żołnierzy. Technologiczne elity społeczeństwa przełamały bariery i wdarły się w obszar zastrzeżony do tej pory dla żołnierzy, stawiając wojsko w kłopotliwej sytuacji. Współczesna technologia zmienia bronie i pole walki oraz zamazuje obraz tego, kto prowadzi i bierze udział w walce, a kto nie.

W koncepcjach militarnych pojawiła się już kategoria **militarnych operacji pozawojennych**, wskazująca drogę postępowania siłom zbrojnym we wszelkich sytuacjach niezwiązanych z polem walki. Pojawia się też nowa kategoria **pozamilitarnych operacji wojennych**, która poszerza rozumienie i zmienia istniejącą percepcję walki i wojny. Koncepcja ta wkracza niemalże w każdą sferę ludzkiej aktywności i obejmuje obszary położone daleko poza zakresem klasycznych operacji militarnych. Rozszerzenie tego typu jest rezultatem ludzkiej determinacji w użyciu wszelkich możliwych środków dla osiągnięcia swoich celów. Formy, które nie charakteryzują się użyciem sił zbrojnych, a nawet nie są związane z przelewem krwi i ofiarami, tak samo gwarantują pomyślne osiąganie celów konfliktu i wojny, a nawet osiąganie większych korzyści, niż używając przemoc militarną.

W rezultacie pojawiają się rozmaite rodzaje walki: handlowa, finansowa, terrorystyczna, psychologiczna, przemytnicza (prowadząca do zachwiania rynku i ekonomicznego porządku), medialna (manipulowanie tym, co ludzie widzą i słyszą, dla kierowania nimi), narkotykowa (uzyskiwanie szybkich i znacznych nielegalnych profitów z rozprzestrzeniania katastrofy w innych krajach), informacyjna (w sieciach informacyjnych), technologiczna (tworzenie monopolu przez niezależne ustanawianie standardów), surowcowa (grabież zasobów i dóbr innych), fałszywa pomoc ekonomiczna (jawne obdarowywanie kogoś, przy skrytym zdobywaniu nad nim kontroli), kulturowa (kreowanie i narzucanie trendów kulturowych w celu asymilowania tych, którzy reprezentują inny punkt widzenia), poprzez prawo międzynarodowe i inne, temu podobne. Różnorodność form niemilitarnej wojny jest tak duża, że trudna do pełnego zidentyfikowania. Jest to szczególnie aktualne w odniesieniu do współczesności, gdzie lawinowo pojawiające się nowe technologie, tworzą coraz rozleglejsze możliwości prowadzenia walki. Możliwe jest także twórcze stosowanie różnych, mieszanych form walki, co jeszcze bardziej wzbogaca jej arsenał.

Współczesna i przyszła wojna będzie się charakteryzowała szerokim postrzeganiem walki, która będzie mieszaniną różnych jej form, zarówno tych prowadzonych przez siły zbrojne, jak i tych stosowanych przez pozamilitarne organizacje. Wojny nowego typu toczyć się będą permanentnie z użyciem wszelkich dostępnych środków militarnych i niemilitarnych, krwawych i bezkrwawych celem zmuszenia przeciwnika, by długotrwale służył interesom prowadzącego wojnę. Istnienie tych wojen będzie często ukrywane i kwestionowane przez prowadzących je.

Pierwszym nowym obszarem intensywnie wyłaniającym się jest sfera informacyjna. We współczesnych warunkach rozwoju, wykorzystujący tę sferę podmiot

bez żadnego przeszkolenia wojskowego i powiązań ze sferą militarną może zagrozić bezpieczeństwu państwa. Sfera informacyjna jest płaszczyzną dostępną zarówno dla świata pozamilitarnego, jak i militarnego. Obecnie jednym z nietradycyjnych obszarów walki jest nowa jakość wykorzystania sfery informacyjnej. Nowość ta polega głównie na tym, że informacja w przeszłości wykorzystywana głównie do zasilania procesów decyzyjnych, teraz staje się dodatkowo środkiem walki, czyli bronią. W wyniku gwałtownego rozwoju technologicznego, szczególnie w obszarze elektroniki, pojawiło się głębokie uzależnienie od informacji, a w węższym znaczeniu – także od sieci komputerowych. W rezultacie zarówno w sferze praktyki, jak i w teorii pojawiła się walka informacyjna[8].

Koncepcja ta od początku koncentrowała się na atakowaniu informacji i systemów informacyjnych przeciwnika oraz obronie własnej sfery informacyjnej. Obecnie wielu badaczy jest zgodnych co do tego, że zarówno pomiotem, jak i przedmiotem tej walki może być tak sfera militarna, jak i cywilna.

1.2. Ocena piśmiennictwa

W stosunkowo niedługim czasie[9] pojawiło się wiele materiałów naukowych dotyczących wykorzystania sfery informacyjnej w działaniach różnych podmiotów. W celu zarysowania sytuacji, warto syntetycznie omówić najważniejsze obszary i pozycje określonego piśmiennictwa.

Tuż po wojnie w Zatoce Perskiej w 1992 r. Alan Campen zebrał zestaw referatów wielu autorów, dodał kilka swoich i opublikował książkę[10]. Książka ta odnosiła się do niedawno zakończonej kampanii przeciwko Irakowi, jednakże jej uwaga koncentrowała się na informacyjnej stronie tej kampanii. Analizując zakończoną kampanię Campen uznał, iż była ona „pierwszą informacyjną wojną" i tak też zatytułował całość opracowania. Opracowanie to stanowi cenny materiał z zakresu analizy informacyjnego aspektu konfliktu z Irakiem. Pojawia się tu wiele uogólnień i prawidłowości dotyczących wpływu informacji i informacyjnych systemów na przebieg współczesnej walki zbrojnej i wojny.

Opracowanie to nie zakończyło działalności badawczej Campena. Po wcześniejszym przygotowaniu pojedynczych artykułów, w 1996 r. wspólnie z dwoma innymi głównymi autorami, wydaje książkę[11] dotyczącą problematyki cyberwojny. Książka ta zawiera wiele stanowisk wobec omawianej problematyki, gdyż zamieszcza również referaty kilkunastu specjalistów w tym zakresie. Mimo popularnonaukowego charakteru całości, wiele fragmentów stanowi dobrze udokumento-

[8] Szerszy opis genezy walki informacyjnej zawarto w rozdziale 3.

[9] Liczący się dorobek naukowy w tym obszarze miał miejsce w ostatnim dziesięcioleciu.

[10] A. Campen, *The First Information War. The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War*, Fairfax 1992.

[11] A. Campen, D.H. Dearth, R.T. Goodden, *Cyberwar: Security, Strategy, and Conflict in the Information Age*, Fairfax 1996.

wane i uargumentowane rozważania naukowe. Do wartościowych dokonań autorów należy zaliczyć autorskie propozycje definicji i charakterystyki walki informacyjnej w sferze cywilnej i militarnej oraz rozważania z zakresu moralnej, prawnej i organizacyjnej strony tej walki. Autorzy określają znaczenie rewolucji w sferze militarnej i rolę potencjału walki informacyjnej dla bezpieczeństwa narodowego. Uzasadniają konieczność posiadania narodowej strategii informacyjnej dla przetrwania w XXI w. Proponowane szerokie rozumienie walki informacyjnej, uwzględnia oddziaływanie mediów jako komponentu tej walki. W treści zawarto także charakterystykę form oddziaływań medialnych i możliwości wpływania na świadomość odbiorców. Szczególnie interesująca jest propozycja wykorzystania telewizji do kształtowania woli innego narodu przez zmianę jego postrzegania rzeczywistości. Opracowanie zawiera także treści prognostyczne co do kształtu walki informacyjnej pod koniec bieżącego ćwierćwiecza.

Również stosunkowo wcześnie problematykę walki informacyjnej w obszernym studium zaprezentował Winn Schwartau[12]. Zamieścił w nim, oprócz własnych poglądów, wypowiedzi 37 innych specjalistów z tej dziedziny. W rezultacie praca ta, a szczególnie jej drugie wydanie, odnosi się do wielu aspektów wyłaniającej się nowej sfery walki. Sam Schwartau definiuje i charakteryzuje walkę informacyjną oraz dokonuje jej podstawowej dekompozycji[13]. Jego zasługą jest zwrócenie uwagi na szeroki kontekst nowego zjawiska i skalę zagrożenia zarówno dla bezpieczeństwa personalnego, jak też organizacji i państw. Ponadto obszernie charakteryzuje wiele rodzajów zagrożeń sfery informacyjnej oraz możliwych sposobów prowadzenia informacyjnych ataków oraz informacyjnej obrony. Część materiałów zawartych w opracowaniu ma charakter naukowy, jednak większość z nich można zaliczyć do popularnonaukowych.

Autorem, który należał do grupy kształtującej pierwsze koncepcje walki w sferze informacyjnej, jest także Martin Libicki. Napisał on wiele książek, referatów, artykułów i wystąpień na ten temat. Do szczególnie interesujących zaliczyć należy opracowania[14]: *Czym jest walka informacyjna* i *Obrona cyberprzestrzeni*. Obie pozycje zostały wydane przez Uniwersytet Obrony Narodowej USA. Pierwsza zawiera odmienne od często spotykanego rozumienie walki informacyjnej. Autor twierdzi w niej, że nie istnieje jakiś odrębny sposób prowadzenia wojny, którym byłaby walka informacyjna. Tę zaś rozumie jako mozaikę różnych form walki w sferze informacyjnej. Zalicza do nich: walkę o przewagę w dowodzeniu, walkę w sferze rozpoznania, walkę elektroniczną, walkę psychologiczną, walkę hakerską, walkę ekonomiczną, walkę informacyjną i cyberwalkę (mającą się pojawić w przyszłości). Charakteryzuje także te formy oraz analizuje poszczególne sposoby i techniki tego obszaru, identyfikując istniejące od dawna i nowe. Ponadto, w przeciwień-

---

[12] *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, New York 1994. Drugie, znacznie rozszerzone wydanie, ukazało się w 1996 r.

[13] Propozycje tego autora omówiono w rozdziale 3.

[14] M.C. Libicki, *What Is Information Warfare?* Washington 1995; oraz tenże, *Defending Cyberspace and Other Metaphors*, Washington 1997.

stwie do wielu specjalistów, nie zgadza się z tezą o wielkim zagrożeniu systemów informacyjnych działaniami walki informacyjnej. Czyni tak będąc przekonany, iż systemy te są coraz bardziej rozproszone i łatwo mogą być redundantne, co uodparnia je na zagrożenia.

Druga publikacja, *Obrona cyberprzestrzeni*, poświęcona jest wspomnianej wcześniej cyberwalce. Całe opracowanie koncentruje się na koncepcji obrony w sferze cyberwalki. Zauważa przy tym, że celem ataku może być raczej cywilna infrastruktura informacyjna niż siły zbrojne. Dostrzega także zagrożenie możliwością manipulowania społeczeństwem za pomocą technik medialnych, Internetu, multimediów. Zagrożenie to zawiera się w możliwości stosowania mieszanych technik tradycyjnej propagandy, manipulowania prawdą i nowych technik manipulacyjnych. W pracy znajdują się także ciekawe propozycje dotyczące odstraszania informacyjnych ataków. Interesująca jest też koncepcja organizacji obrony immunologicznej systemu informacyjnego, opracowana na podstawie analizy systemu immunologicznego żywego organizmu.

Walka w sferze informacyjnej pozostawała od początków tworzenia się tej koncepcji w sferze zainteresowania amerykańskiego instytutu badań naukowych *RAND*. Rezultatem badań tego obszaru było opublikowanie kilku opracowań. Jednym z tych, które bezpośrednio odnoszą się do problematyki walki informacyjnej jest publikacja[15] poświęcona przygotowaniu do konfliktu w informacyjnym wieku. Jest to zbiór dziewiętnastu referatów będących wynikiem badań zamówionych przez Biuro Sekretarza Obrony USA oraz prowadzonych według własnych planów instytutu. W toku badań stwierdzono, że rewolucja informacyjna transformuje naturę konfliktu w obszar rozległego spektrum rozciągającego się od otwartej walki, przez terroryzm, przestępczość, po radykalną aktywność socjalną. W konflikcie socjalnym Internet i inne media znacznie wzmacniają możliwości jednostek i małych grup w zakresie ich wpływania na działania państw. Przygotowania do konfliktu w takich warunkach wymagać będą zmiany form organizacji. Zmiana ta będzie jednakże trudna dla państw i tradycyjnych sił zbrojnych, które pozostają bastionem struktur hierarchicznych i będą się opierać radykalnym zmianom. Symbol tego świata, Mars, musi ustąpić Atenie, patronce informacyjnego wieku. Jest to warunkiem nie tylko przygotowania się do przyszłych konfliktów, lecz także skutecznego zapobiegania im. Według takiego głównego motywu określono charakterystykę nowych warunków, w jakich pojawią się konflikty, zidentyfikowano istotę urzeczywistniającej się rewolucji w sferze militarnej, dokonano identyfikacji cech walki toczącej się w informacyjnej cywilizacji oraz zaproponowano kilka podejść badawczych do walki informacyjnej. Jest wśród nich m.in. szeroka perspektywa (proponowana przez Martina Libickiego w omawianej wcześniej jego pracy) oraz podejście społeczne.

---

[15] J. Arguilla, D. Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica 1997.

RAND prowadził także badania w omawianym obszarze na zlecenie sił powietrznych USA. Efektem tych badań jest publikacja[16] zatytułowana *Strategiczna ocena. Zmiana roli informacji w walce*. Jest to praca zbiorowa dwudziestu znanych badaczy. Niektórzy z nich byli współautorami wcześniej wymienianych publikacji. Prezentowana praca jest obszerną analizą nowej roli informacji w walce. Wiele miejsca poświęcono w niej badaniu wpływu informacyjnych technologii na społeczeństwa, gdyż wpływ ten wywoła największe implikacje dla narodowego bezpieczeństwa. Niektórzy współautorzy[17] uważają, że zmiany te zmniejszą znaczenie państwa, zwiększając jednocześnie potencjał i znaczenie organizacji niepaństwowych. Zgodnie z zamówieniem badania koncentrują się na sytuacji Stanów Zjednoczonych, jednakże podłożem ich są zjawiska i ich prawidłowości. Jednym z takich zjawisk jest zależność państwa od informacyjnej infrastruktury oraz wynikająca z tego wrażliwość. O ile wszyscy badacze akceptują istnienie takiej wrażliwości, to panuje odmienność poglądów na skalę tej zależności. Uzasadnione wydaje się przekonanie Davida Ochmanka, że dominacja informacyjna zapewni utrzymanie przewagi w sferze militarnej. Praca zawiera także interesujące propozycje utrzymywania zdolności projekcji siły i obezwładnienia broni masowego rażenia przeciwnika oraz osiągnięcia nowej jakości działań psychologicznych. Autorzy analizują techniki i taktyki, które mogą być zastosowane w ramach ataku na narodowe zasoby strategiczne, takie jak system finansowy, sieć telekomunikacyjna czy system transportu. Analizują także zależność działań sił powietrznych od informacji i systemów informacyjnych, wskazując na istniejące prawidłowości. Autorzy konstatują, że podobnie jak nie sposób całkowicie wyeliminować wrażliwość na atak jądrowy, tak i niemożliwe jest całkowite uodpornienie się na ataki informacyjne. Dlatego też najbardziej obiecująca jest strategia odstraszania tych ataków i zapobiegania uzyskiwaniu zdolności do ich prowadzenia przez przeciwników. Praca definiuje także walkę informacyjną oraz prezentuje jej części składowe z charakterystyką elementów. Badania te koncentrują się na strategicznym poziomie zastosowania. Zleceniodawcom, czyli siłom powietrznym, autorzy uświadamiają istnienie problemu decyzyjnego związanego z wybraniem obszaru swoich kompetencji w przyszłości. Siły powietrzne zawsze argumentowały konieczność istnienia samodzielnej organizacji specjalizującej się w eksploatacji jakiejś przestrzeni. Gdyby to było prawdziwe, oznaczać by mogło konieczność wyłonienia organizacji odpowiedzialnej za walkę w sferze informacyjnej. Możliwe jest jednak przenoszenie akcentu z operacji powietrznych na informacyjne, z rozwijaniem zdolności do działań zarówno w sferze powietrznej, jak i informacyjnej. Wymaga to jednak przynajmniej częściowego odchodzenia od kultury opartej na lataniu.

Kolejne badania, zlecone RAND przez Biuro Sekretarza Obrony USA, również dotyczyły problematyki walki informacyjnej, lecz na poziomie strategicznym.

---

[16] Z.M. Khalilzad, J.P. White, *Strategic Appraisal. The Changing Role of Information in Warfare*, Santa Monica 1999.

[17] Należą do nich: J. Arquilla, D. Ronfeldt i M. Zanini.

W rezultacie, w odstępie dwuletnim ukazały się dwa opracowania[18], w których zawarto wyniki badań. W pierwszym, zatytułowanym *Strategiczna walka informacyjna: nowe oblicze wojny*, badacze uznali obecną w wielu wypowiedziach tezę o zwiększającej się roli informacyjnej rewolucji dla narodowego bezpieczeństwa. Zjawisko to wynika z rosnącego uzależnienia cywilnej i militarnej aktywności od komputerów i informacyjnej komunikacji. Autorzy przyznają, że wraz z wieloma korzyściami płynącymi z komputeryzacji i rozwoju telekomunikacji pojawiły się poważne zagrożenia. Strategicznie ważne elementy państwa znalazły się w zasięgu łatwego do przeprowadzenia informacyjnego ataku przez jakiegokolwiek przeciwnika. Pojawiła się więc możliwość prowadzenia strategicznej walki informacyjnej. To z kolei stawia wyzwanie tradycyjnemu podejściu do obrony i obronności kraju. Bronią w tej nowej sytuacji może być program komputerowy, a nosicielem tej broni dowolny komputer, telefon komórkowy i Internet. Nowe wrażliwości i zagrożenia są ciągle słabo rozumiane i mało dostrzegane. Dla tego typu zagrożeń i napastników nie istnieją granice i rubieże obrony. W tej sytuacji militarna obrona może być całkowicie nieskuteczna. Obrona ta musi być masowa, organizowana przez każdy komponent państwa, a nawet przez każdego obywatela. W sferze konstrukcji aparatu pojęciowego autorzy uznali, że jest jeszcze za wcześnie na precyzyjne definiowanie walki informacyjnej. Określili więc przybliżony zakres dwóch zjawisk – walki informacyjnej i walki strategicznej – a następnie obszar swojego zainteresowania, jakim jest strategiczna walka informacyjna. Niezwykle ciekawy jest opis narzędzia badawczego, jakim jest specjalnie skonstruowane przez RAND ćwiczenie badawcze, które prowadzi się z udziałem personelu odpowiedzialnego za kierowanie sprawami bezpieczeństwa narodowego oraz gospodarki, a także przedstawicieli biznesu. Autorzy prezentują także przebieg takiego ćwiczenia.

W drugim opracowaniu – *Wyłanianie się strategicznej walki informacyjnej* – autorzy prezentują wyniki kontynuacji badań problematyki strategicznej walki informacyjnej. W rezultacie ustalają dwie kategorie zagrożeń dla bezpieczeństwa narodowego – zagrożenia dla narodowego bezpieczeństwa ekonomicznego oraz dla narodowej strategii militarnej. Identyfikują także dwie generacje koncepcji strategicznej walki informacyjnej: jedną składającą się z kompozycji różnych instrumentów walki strategicznej oraz drugą – samodzielną formę informacyjną składającą się z różnych właściwych jej komponentów. Praca zawiera także wiele sugestii dla praktyki o charakterze wdrożeniowym. Cenną wartością obu prac są zidentyfikowane prawidłowości dotyczące strategicznego poziomu walki informacyjnej.

Inną pracą z zakresu walki informacyjnej jest monografia Edwarda Waltza[19], pt. *Walka informacyjna – zasady i działania*. Zawiera ona autorską koncepcję oraz charakterystykę walki informacyjnej. Jest rezultatem m.in. kilku seminariów prowadzonych w Stanach Zjednoczonych i Europie na ten temat. Waltz identyfikuje

---

[18] R.C. Molander, A.S. Riddile, P.A. Wilson, *Strategic Information Warfare. A New Face of War*, Santa Monica 1996 oraz R.C. Molander, P.A. Wilson, D.A. Mussington, R. F. Mesic, *Strategic Information Warfare Rising*, Santa Monica 1998.

[19] E. Waltz, *Information Warfare Principles and Operations*, Boston 1998.

sferę walki informacyjnej, w której informacja jest zarówno obiektem ataku, jak i bronią oraz zagrożeniem dla cywilnych i militarnych systemów informacyjnych. Określa także rolę technologii w walce bazującej na informacji, koncepcję przewagi informacyjnej, środki rażenia, komponenty i zasady prowadzenia walki informacyjnej. Jego teoria jest syntezą koncepcji informacyjnej dominacji, informacyjnej obrony i informacyjnego ataku.

Także w 1998 r. została wydana obszerna monografia Dorothy Denning, zatytułowana[20] *Walka informacyjna i bezpieczeństwo*. Autorka, profesor informatyki Uniwersytetu Georgetown, zawarła w swojej publikacji zarówno treści naukowe, jak i popularnonaukowe. Do treści naukowych zaliczyć należy koncepcję i zasady walki informacyjnej. Proponowany przez nią model walki informacyjnej składa się z czterech komponentów: informacyjnych zasobów, uczestników walki, działań ofensywnych oraz działań defensywnych. Walka informacyjna wiązana jest tu z czterema aspektami ludzkiej aktywności: zabawą, przestępczością, indywidualnymi wolnościami i prawami oraz bezpieczeństwem narodowym. Autorka obszernie charakteryzuje komponenty walki informacyjnej, ilustrując ją wieloma przykładami, zahaczając o poziom beletrystyki. Bada jednak walkę informacyjną zarówno w skali mikro, jak i makro. Dużo miejsca poświęca problematyce obrony narodowej oraz możliwości manipulowania społeczeństwami. Do niedostatków zaliczyć należy powierzchowne traktowanie niektórych zagadnień, co może wynikać z rozległości podjętej problematyki. Spowodowało to także zauważalną niespójność treści. Ponadto podejście autorki nie jest wolne od stronniczości w ocenach zachowań podmiotów areny międzynarodowej.

Kolejna podobna publikacja, dotycząca problematyki walki informacyjnej, ukazała się w 1999 r. Jest to[21] *Sztuka walki informacyjnej: spojrzenie w głąb filozofii wojownika wiedzy* napisana przez dwóch autorów: Richarda Forno i Ronalda Baklarza. Publikacja ta ma charakter popularnonaukowy. Jednakże znajdują się w niej oryginalne propozycje wywiedzione z analizy klasycznej chińskiej filozofii walki. Autorzy uznali, że jak Szekspir jest przykładem dla dramatopisarzy, tak Sun Tzu dla twórców teorii militarnych. Dlatego też dużo uwagi poświęcili analizie poglądów tego klasyka. Z analizy tej wywiedli szereg wniosków dla poprawy bezpieczeństwa narodowego. Autorzy ci zwrócili również uwagę na zagrożenie możliwością stosunkowo łatwego manipulowania świadomością społeczeństw. Proponowane treści zabarwione są raczej społecznym niż technokratycznym podejściem do walki informacyjnej.

Polskie środowisko naukowe również wykazywało sporo zainteresowania najpierw problematyką znaczenia informacji w walce, a następnie walką informacyjną. Przykładem mogą tu być m.in. prace Piotra Sienkiewicza. W jednej z nich: *Inżynieria systemów*[22], cały rozdział poświęcił informacji i informowaniu, doko-

---

[20] D.E. Denning, *Information Warfare and Security*, 1998.

[21] R. Forno, R. Baklarz, *The Art Of Information Warfare: Insight into the Knowledge Warrior Philosophy*, 1999.

[22] P. Sienkiewicz, *Inżynieria systemów*, Warszawa 1983.

nując nie tylko przeglądu definicji informacji, lecz także określenia podstawowych zjawisk zachodzących w sferze informacyjnej, przede wszystkim zaś informowania, czyli procesu informacyjnego[23]. Analizuje także rozwój systemów informacyjnych, szczególnie w sferze społecznych procesów informacyjnych, oraz przeprowadza systemową analizę tych procesów. Już wtedy wspomina o walce informacyjnej[24], mając jednak na myśli raczej nasilającą się wówczas walkę propagandową między przeciwstawnymi systemami ideologicznymi. Ponadto duża część aktywności badawczej i publicystycznej tego autora jest poświęcona aspektom wykorzystania informacji w procesach zarówno współpracy, jak i walki[25].

Polski wkład w rozwój studiów nad rolą działań informacyjnych, w tym nad rolą czynnika informacji w zmaganiach zbrojnych, wyraża się także w pracach Stanisława Kozieja. Już w 1978 r. zwracał on uwagę na rolę informacji jako jednego z podstawowych czynników walki zbrojnej obok rażenia (ognia), ruchu (manewru) oraz uderzenia[26]. Następnie myśl tę rozwinął w kolejnych swoich publikacjach[27]. Koncepcje te znalazły zastosowanie nie tylko w myśli naukowej, ale i w praktyce szkoleniowej wojsk oraz w dydaktyce na początku lat dziewięćdziesiątych[28]. Zostały także wprowadzone do wydawanych wówczas regulaminów walki. W rezultacie zaczęto np. wyróżniać w systemach obrony i natarcia podsystem informacyjny (oprócz tradycyjnych składników, jakimi były: ugrupowanie wojsk, infrastruktura pasa (rejony) działań, system ognia).

Prace te akcentowały rolę informacji w walce bądź jako ważnego elementu zabezpieczenia procesów walki, bądź też jako elementu systemu walki w postaci jego podsystemu. W wyniku nowych przemyśleń i oddziaływania docierających rezultatów badań prowadzonych na Zachodzie, pojawiły się pierwsze polskie koncepcje wykorzystania informacji jako narzędzia walki.

W 1999 r. ukazała się publikacja na temat walki informacyjnej, opracowana przez L. Ciborowskiego[29]. Jest to cenny wkład polskiego środowiska naukowego do badań nad zjawiskiem walki informacyjnej. Autor w publikacji tej dokonał syntetycznego przeglądu problematyki w aspekcie historycznym oraz zaproponował swoją koncepcję walki informacyjnej. Koncepcja ta jest osadzona w matematyczno-cybernetyczno-prakseologicznym podejściu. Szczególnie cenne jest naukowe uzasadnienie wartości informacji w sferze militarnej. Autor dostrzega sze-

---

[23] Tamże, s. 73–74.

[24] Tamże, s. 111.

[25] Są to m.in.: P. Sienkiewicz, *Wojna informatyczna*, „ComputerWorld" 1997, nr 31; T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne – szanse, zagrożenia, wyzwania*, Kraków 1999, P. Sienkiewicz, *Współczesne koncepcje walki informacyjnej*, [w:] *Informacyjny wymiar współczesnych działań powietrznych*, Materiały sympozjum naukowego, red. R. Szpyra, Warszawa 2002.

[26] Zob. S. Koziej, *Ciągłość oddziaływania na przeciwnika podczas natarcia*, „Myśl Wojskowa" 1978, nr 5.

[27] Por.: S. Koziej, *Współczesna myśl taktyczna*, „Myśl Wojskowa" 1987, nr 10; tenże, *Teoria sztuki wojennej*, Warszawa 1993.

[28] Por. podręczniki akademickie AON: *Działania taktyczne wojsk lądowych*, red. S. Koziej, Warszawa 1992 oraz *Działania operacyjne wojsk lądowych*, Warszawa 1992.

[29] L. Ciborowski, *Walka informacyjna*, Toruń 1999.

roki kontekst walki informacyjnej, m.in. obszernie cytując Sun Tzu; jednakże nie nawiązuje do ustaleń badaczy Zachodu. Koncepcja walki informacyjnej autora jest wywiedziona z niemalże dosłownego rozumienia konstatacji, że „informacją jest wszystko to, co nie jest ani energią, ani masą, czyli nie jest zasilaniem"[30] oraz że „[...] informacja nie może istnieć bez umysłu ludzkiego"[31]. Autor wyprowadza stąd m.in. wniosek, że „informacji nie można też bezpośrednio zakłócać"[32]. Tu rodzi się wątpliwość: jak należy rozumieć kategorię „umysł ludzki"? Jeżeli szeroko, jako rezultat procesu myślenia, to informacja może istnieć poza mózgiem – żywym organem. Wyobrażenia człowieka oraz jego wyobraźnia są przecież rejestrowalne na zewnątrz organizmu, w przeciwnym razie nie byłoby całego dorobku intelektualnego ludzkości. Wyobrażenia i wyobraźnia, o których pisze autor, to przecież sfera symboli, które mogą być przekazywane między ludźmi. Przez celową preparację tych symboli można wywołać pożądane wrażenia. Powinna więc istnieć informacja poza umysłem, w przeciwnym wypadku nie można by mówić nawet o zakłócaniu informacji poza umysłem ludzkim, co jednak jest proponowane przez autora. Jeżeli kategorię *umysł* traktować wąsko, jako organ biologiczny, to znaczyłoby, że informacja istnieje tyko w obecności człowieka, co przeczyłoby możliwości prowadzenia walki informacyjnej przy nieobecności człowieka w czasie atakowania informacji. Ponadto, zdaniem autora, walka informacyjna „nigdy nie może występować w oderwaniu"[33], gdyż zawsze towarzyszy jakiejś walce, którą wspiera. Jednocześnie przytacza słuszne tezy Sun Tzu, takie jak: „[...] największym osiągnięciem jest pokonanie wroga bez walki", czy „[...] najwyższą sztuką jest zwyciężyć wroga bez wydania bitwy. Zająć miasto wroga bez oblegania i zająć tereny jego państwa bez inwazji"[34]. Przecież zwycięstwo bez wydania bitwy, czy bez inwazji, oznacza zwycięstwo przy umiejętnym wykorzystaniu informacji jako broni. Zwycięstwo więc, może być osiągnięte w wyniku wygrania walki informacyjnej. Stąd kontrowersyjność tezy autora. Jest ona słuszna w wielu wypadkach, lecz nie we wszystkich. W warunkach rodzącej się cywilizacji informacyjnej przypadki samodzielnego występowania walki informacyjnej (a nie tylko towarzyszenia innym walkom) będą coraz powszechniejsze, a informacja stawać się będzie bronią podstawową. Przekonanie o tym wśród badaczy na całym świecie jest niemal powszechne.

Również w 1999 r. Gabriel Nowacki obronił pracę doktorską na temat *Walka informacyjna – próba kategoryzacji*[35], a w 2001 r. wydał studium teoretyczne – *Współczesne poglądy na prowadzenie walki informacyjnej*[36]. W obu opracowaniach prezentuje zasadniczo tę samą, co L. Ciborowski, koncepcję walki informacyjnej.

---

[30] Tamże, s. 51.

[31] Tamże, s. 59.

[32] Tamże, s. 68.

[33] Tamże, s. 69.

[34] Tamże, s. 13.

[35] G. Nowacki, *Walka informacyjna – próba kategoryzacji*, rozprawa doktorska, Warszawa 1999.

[36] Tenże, *Współczesne poglądy na prowadzenie walki informacyjnej. Studium teoretyczne,* Warszawa 2001.

Różnice dotyczą jedynie obszarów towarzyszących, takich jak poglądy innych państw na walkę informacyjną. Ponadto drugie opracowanie ma charakter syntezy w stosunku do pierwszego. Wartościowym dorobkiem autora jest tu przegląd poglądów na temat istoty informacji, aczkolwiek niektóre wnioski wydają się kontrowersyjne, jak chociażby ten, że „informacja jest niezniszczalna i zawsze prawdziwa"[37]. Podobnie jak poprzedni autor również twierdzi, że „[...] informacja nie może istnieć bez umysłu ludzkiego"[38]. Ponieważ ludzi można zniszczyć (teoretycznie istnieje możliwość zniszczenia całej ludzkości), to i informację można zniszczyć. Można też inaczej niszczyć informację, jednak ten argument przeczy prawdziwości prezentowanej tezy. Ocena tego czy informacja jest zawsze prawdziwa jest również względna, zależy bowiem od pojmowania prawdy, a także od przyjętych założeń. Wydaje się słuszna teza autora o istnieniu trzech komponentów walki informacyjnej. Można mieć wątpliwości co do nazewnictwa tych komponentów – polemika w tym zakresie jest prowadzona w dalszych rozważaniach[39]. Niezrozumiałe są wynikające z konstrukcji modelu struktury walki informacyjnej[40] relacje, a dokładniej brak tych relacji między elementami zakłócania walczących stron. Znaczyłoby to, że komponent zakłócający jednej strony, może jedynie oddziaływać na komponenty rozpoznania i obrony przeciwnika bez możliwości tego oddziaływania na jego komponent zakłócający. Nie wydaje się to słuszne również z powodów teoretycznych, gdyż w walce występuje wzajemne zakłócanie, nic więc nie stoi na przeszkodzie, by komponenty zakłócające zakłócały się wzajemnie. Także praktyka wskazuje na istnienie takich przedsięwzięć, jak kontrprzeciwdziałanie, kontrdezinformacja. Niezwykle wartościowe są badania nad definiowaniem przestrzeni walki informacyjnej. Wyniki tych badań mogą być przydatne również do innych potrzeb. Autor, dokonując dekompozycji walki informacyjnej, stosując jednolite kryteria, wyodrębnił podziały, które częściowo należy zaakceptować, po części zaś zakwestionować. Słuszne wydaje się umieszczenie, w przeciwieństwie do stanowiska L. Ciborowskiego, walki informacyjnej w równoważnej pozycji w stosunku do innych walk, a nie jako walki wspierającej inne walki. Wątpliwości zaś budzi zakwalifikowanie walki informacyjnej do walki niezbrojnej, w sytuacji gdy proponowane dalej sposoby i metody tej walki mieszczą się w arsenale walki zbrojnej. Przy okazji warto zaznaczyć, iż obecnie istnieją trudności ze znalezieniem precyzyjnego kryterium uznania jakiejś walki za zbrojną lub niezbrojną. Autor podjął też znaczny wysiłek w porządkowaniu sposobów prowadzenia walki informacyjnej. Zaproponowana metoda wydaje się racjonalna, w rezultacie czego został zarysowany interesujący obraz proponowanego przez autora modelu walki informacyjnej. Inne, bardziej szczegółowe polemiki z poglądami autora są treścią dalszych rozważań niniejszej pracy.

---

[37] Tenże, *Walka informacyjna...* s. 36.
[38] Tamże, s. 27.
[39] Zob. rozdział 3.
[40] G. Nowacki, *Walka informacyjna...* s. 42.

Powstanie omawianych dzieł w środowisku polskich naukowców wojskowych jest niezwykle cenne, gdyż wprowadza dostrzeganą powszechnie problematykę do sfery zainteresowań polskiego środowiska nauk wojskowych oraz inspiruje do dalszego, twórczego rozwijania i pogłębiania badań walki w sferze informacyjnej.

Oprócz omówionych opracowań książkowych, ukazało się także wiele innych publikacji. W rezultacie poszukiwań internetowych, używając hasła *information warfare* w specjalistycznej witrynie internetowej *Barnes&Noble*[41], znaleziono około 70 publikacji książkowych. Podobne poszukiwania w witrynie *Amazon*[42] wyłoniły ponad 50 publikacji. Były wśród nich zarówno pozycje omówione, jak i takie, które dopiero się ukażą. Ponadto analiza informacji o nich sugeruje, że większość z nich ma charakter popularnonaukowy lub beletrystyczny. Wiele z nich odnosi się do wybranych aspektów walki informacyjnej. Niektóre mają w rzeczywistości niewielki związek z walką informacyjną[43].

Bogactwo publikacji książkowych, mimo swej rozległości, jest skromne, w porównaniu z ilością artykułów dotyczących omawianej problematyki, zamieszczonych w periodykach i Internecie. Rozmaite próby poszukiwań doprowadziły do ustalenia, że na pewno dostępnych jest ich ponad tysiąc. Artykuły te można podzielić na trzy grupy: prezentujące naukowo uzasadnione koncepcje, opisy faktograficzne i diagnozy oraz informacje o wydarzeniach bieżących. Niektóre z tych artykułów publikowane są w grupowych zestawieniach, jako materiały przeprowadzonych konferencji. Zestawienia takie publikowane są także jako materiały zwarte w formie książkowej i jednocześnie w Internecie. Jednym z takich opracowań, godnych omówienia, są materiały sympozjum[44] na temat działań informacyjnych, przeprowadzonego w 1999 r. w holenderskiej akademii wojskowej. Opublikowane tuż po sympozjum opracowanie[45] zawiera wprowadzenia i osiemnaście referatów, w większości autorów, którzy brali aktywny udział[46] w sympozjum. Referaty dotyczyły poszczególnych sfer problematyki operacji informacyjnych i walki informacyjnej. Czterech autorów rozważało problematykę podstaw teoretycznych w poszukiwaniu koncepcji operacji informacyjnych i walki informacyjnej. Wśród tych autorów warto wymienić Geoge'a Steina, który także w innych swoich wypowiedziach[47] prezentuje wiele argumentów dla poparcia tezy o tym, że współcześnie

---

[41] Zob. www.barnsandnoble.com.

[42] Zob. www.amazon.com.

[43] Przykładem może być *Biological Warfare and Chemical Gases.*

[44] Było to międzynarodowe sympozjum nt. *„Informacja jako środek, obiekt ataku i broń. Operacje informacyjne, co to oznacza?"*– zorganizowane przez holenderską Królewską Akademię Wojskową w grudniu 1999 r.

[45] *Information Operations*, red. J.M.J. Bosh, H.A.M. Luiijf, A.R. Mollema, NL ARMS. Netherlands Annual Review of Military Studies 1999, Breda 1999.

[46] Wiedza ta wynika z bezpośredniego uczestnictwa w sympozjum autora niniejszej publikacji.

[47] Zob. G. Stein, *Information War – Cyberwar – Netwar,* [w:] *Battlefield of the Future. 21st Century Warfare Issues.* Air University Maxwel AFB 1995; tenże, *Information Warfare*, [w:] A.D. Campen, D.H. Dearth, R.T. Goodden, *Cyberwar: Security, Strategy, and Conflct in the Information Age*, Fairfax 1996; tenże, *Information Warfare. Learning with Sun Tzu*, [w:] *Information Operations...* wyd. cyt.

informacja jest bronią i to niezwykle groźną. Jest on jednym z tych badaczy, którzy sięgają do chińskiego dorobku naukowego i intelektualnego. Kolejni czterej autorzy omawianego wydawnictwa koncentrują się na koncepcjach operacji informacyjnych prezentowanych z różnych perspektyw, teoretycznej i praktycznej. Pozostali przedstawiają albo poszczególne aspekty, albo istniejące poglądy na omawianą problematykę w różnych regionach świata.

Wśród artykułów szczególnie dużo jest takich, które prezentują opisy faktograficzne obserwowanych zdarzeń[48] oraz stanu współczesnej sytuacji[49]. Różnorodność zawartych w nich podejść, szczegółowość analiz oraz tematyki, umożliwiają uzyskiwanie wysokiej jakości diagnoz i są przesłanką do wykrywania istniejących prawidłowości. Treści artykułów naukowych, najogólniej ujmując, mieszczą się w granicach koncepcji prezentowanych przez badaczy w formie książkowej. Często są one elementami procesu badawczego, w wyniku którego powstają dzieła zwarte. Artykuły są oczywiście publikowane nie tylko w Internecie, ale też w różnych periodykach w formie pisemnej. Jednak obecnie jest niemalże powszechne jednoczesne publikowanie na papierze i w formie elektronicznej. Coraz częściej forma elektroniczna jest jedyną, dlatego wiele uwagi poświęcono Internetowi. Cenną wartością Internetu, wiązaną z niniejszymi badaniami, jest także posiadanie niezwykle bogatych zestawień źródeł w postaci specjalistycznych witryn. Niektóre z nich zawierają setki adresów źródeł informacji dotyczących operacji informacyjnych i walki informacyjnej. Adresy najciekawszych są zestawione na oddzielnej stronie po bibliografii. Treści zawarte w poszczególnych witrynach i pod kolejnymi adresami mają znacznie zróżnicowaną wartość. Spora część jest niemalże bezwartościowa. Jednak znajdują się tam także wartościowe opracowania, m.in. te, które zostały omówione. Jedną z istotnych wartości źródeł internetowych jest zaprezentowana w nich wiedza na temat kierunków podejmowanych badań i ich rezultatów. Wskazuje ona dobrze zbadane obszary oraz obszary naukowo słabo spenetrowane.

Odrębną grupę literatury stanowią dokumenty doktryn. Nie mają one co prawda charakteru naukowego, jednakże prezentują stan istniejący w sferze praktyki. Z dokumentów tych wynika m.in. stan wdrażania koncepcji teoretycznych do praktyki. W tej grupie szczególnie cenne okazały się amerykańskie połączone doktryny operacji informacyjnych i walki informacyjnej[50] oraz odpowiadające im

---

[48] *UK: Cyber-attacks*, www.infowar.com/mil_c4i/00/mil_c4i_120100a_j.shtml; *Taiwan to Launch „Cyber Warfare" Unit*, www. infowar.com/mil_c4i/00/mil_c4i_112400a_j.shtml; *DOD Closes off GPS Segment*, www.infowar.com/mil_c4i/00/mil_c4i_ 033199a_j. shtml; *Yugoslavia: Air War Leads Us Astray*, www.infowar.com/mil_c4i_041099b_j.shtml.

[49] B. Frezza, *The Militarization of Cyberspacel*, http://techweb.cmp.com/nc/frezza/frezza.html; Joint Economic Committee Hearing, Radio Frequency Weapons and Proliferation: Potential Impact on the Economy. Wednesday, February 25, 1998. http://www. house.gov/jec/hearings/02-25-8h.htm; *The Global Course of the Information Revolution: Technological Trends*; Proceedings of an International Conference, http://www.rand.org/publications/CF/CF157/.

[50] Pub 3-13: *Joint Doctrine for Information Operations*, Washington 1998.

dokumenty rodzajów sił zbrojnych[51]. Również w dokumentach doktryny działań połączonych NATO pojawiła się już problematyka operacji informacyjnych i walki informacyjnej. Oczywiście, wartościowym materiałem okazały się także dokumenty wspomnianych doktryn dotyczące obszarów pokrewnych lub bardziej szczegółowych[52].

W zakresie teorii informacji, z punktu widzenia potrzeb prezentowanych badań, za najcenniejsze uznano prace: Mariana Mazura *Jakościowa teoria informacji*[53], zbiorowa *The Value and Impact of Information*[54], Leona Brillouina *Nauka a teoria informacji*[55]. Szczególnie wartościową publikacją, z powodu społecznego podejścia do informacji, okazała się praca Briana i Aliny Vickery'ch *Information Science in Theory and Practice*[56]. Istnieje oczywiście obszerniejsze piśmiennictwo z tego zakresu, jednakże dużo materiałów poświęconych jest matematyczno-fizycznej koncepcji informacji, która mimo swojej wartości, okazała się mniej przydatna w tych badaniach.

Kojarzący się z informacją jest także współczesny trend rozwoju cywilizacji, nazwanej nawet „społeczeństwem informacyjnym". Charakterystykę i analizę tego zjawiska najpełniej odzwierciedlały przede wszystkim wspólna praca Tomasza Gobana-Klasa i Piotra Sienkiewicza[57], oraz praca zbiorowa[58] czternastu badaczy różnych aspektów społeczeństwa informacyjnego, pod redakcją naukową Lecha Zachera. Korzystano także z wielu publikacji dotyczących trendów rozwojowych współczesnej cywilizacji i ich charakterystyki.

Problematyka bezpieczeństwa i stosunków międzynarodowych jest obecna w rozległej grupie publikacji. Po wstępnym oglądzie najcenniejsze okazały się prace Raymonda Arona[59], Janusza Świniarskiego[60], Bolesława Balcerowicza[61], Edwarda Haliżaka[62], Ryszarda Zięby[63], Konstantego Wojtaszczyka[64]. Prace te stały się źró-

---

[51] Zob.: FM 100-6: *Information Operations*, Washington 1996; AFDD 2-5: *Information Operations*, Maxwell AFB 1998.

[52] Amerykańskie doktryny są dostępne m.in. pod internetowym adresem: http://www.dtic.mil/doctrine/.

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

[54] M. Feeney, M. Grieves, *The Value and Impact of Information*, London 1994.

[55] L. Brillouin, *Science and Information Theory*. Wyd. pol. *Nauka a teoria informacji*, Warszawa 1969.

[56] B. Vickery, A. Vickery, *Information Science in Theory and Practice*, London, 1987.

[57] T. Goban-Klas, P. Sienkiewicz, wyd. cyt.

[58] *Społeczeństwo informacyjne. W perspektywie człowieka, techniki, gospodarki*, red. nauk. L.W. Zacher, Warszawa 1999.

[59] R. Aron, *Pokój i wojna między narodami*, Warszawa 1995.

[60] J. Świniarski, *O naturze bezpieczeństwa. Prolegomena do zagadnień ogólnych*, Warszawa–Pruszków 1997.

[61] B. Balcerowicz, *Sojusz a obrona narodowa*, Warszawa 1999.

[62] *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, red. D.B. Bobrow, E. Haliżak, R. Zięba, Warszawa 1997.

[63] R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje – struktury – funkcjonowanie*, Warszawa 1999.

[64] K.A. Wojtaszczyk, *Kompendium wiedzy o państwie współczesnym*, Warszawa 1998.

dłem inspiracji w zakresie roli państwa w stosunkach z innymi podmiotami sceny międzynarodowej. Ponadto ugruntowały przekonanie autora o roli komponentu militarnego państwa we wspominanych stosunkach.

Kolejną grupę literatury stanowiły opracowania z zakresu nauk wojskowych, a szczególnie sztuki wojennej. Znajdowały się tu zarówno koncepcje klasyków[65], jak też prace badaczy współczesnych. Prace klasyków koncentrują się na ogólnych prawach wojny. We współczesnym piśmiennictwie dotyczącym sztuki wojennej ukształtował się pewien kanon i zgodność co do zasadniczych ustaleń. Jednakże praktyka i warunki, jakie się tworzą w związku z rozwojem cywilizacyjnym, kreują poważne wyzwania wielu ustaleniom sztuki wojennej. Do wyzwań tych zaliczyć: należy pojawianie się nowych rodzajów broni, w tym broni niezabójczej; coraz szersze stosowanie działań militarnych mających charakter pozawojenny; wzrost znaczenia pozamilitarnych form walki; poszerzanie się obszarów działań mających charakter cywilno-militarny. Dostrzega to coraz wyraźniej wielu badaczy. Należą do nich m.in. B. Balcerowicz[66], S. Koziej[67], J. Świniarski[68]. Przemyślenia tych i innych badaczy, uświadomiły konieczność zbadania niektórych założeń sztuki wojennej i poszukiwania koncepcji lepiej przystających do nowej rzeczywistości.

Jest także rozległe piśmiennictwo, które stanowiło pomoc w ustalaniu szczegółowych aspektów poszczególnych elementów tworzących się w wyniku badań koncepcji. Materiały te zostały wymienione w bibliografii i w przypisach.

Z powyższych rozważań wynika, że:

- **Istnieje powszechna zgodność wśród badaczy, iż rola sfery informacyjnej w jakichkolwiek działaniach w warunkach wyłaniającej się cywilizacji informacyjnej staje się pierwszoplanowa.**
- **Rola ta dla komponentu militarnego państwa jest o ile nie większa, to przynajmniej taka sama jak dla komponentów niemilitarnych.**
- **Zarówno refleksja teoretyczna, jak i praktyka dostrzegają dwa obszary zastosowania informacji w walce: tradycyjny jako zasilanie informacyjne i nowy jako wyłaniający się rodzaj broni.**
- **Problematyka walki oraz innych działań w sferze informacyjnej staje się przedmiotem powszechnego zainteresowania badaczy.**
- **Mimo wielości prób definiowania nie ustalił się powszechnie akceptowany aparat pojęciowy. Poszczególne koncepcje są adekwatne do określonych szkół myślenia.**

Nietrudno także zauważyć, że mimo bogactwa poglądów brak jest spójnej koncepcji operacji informacyjnych, którą można by zaakceptować dla potrzeb niniejszych badań. Wobec tego uznano postulat badania istoty i charakteru całości

---

[65] Szczególnie przydatne były: Sun Tzu, *Sztuka wojny*, Warszawa 1994; C. Clausewitz, *O wojnie*, Warszawa 1958.

[66] B. Balcerowicz, *Sojusz a obrona...* wyd. cyt.

[67] S. Koziej, *Przełom w sztuce wojennej*, [w:] *Sztuka wojenna. Konteksty teoretyczne i praktyczne*, red. M. Krauze, B.M. Szulc, Toruń 2000.

[68] J. Świniarski, *O zasadach, regułach i dyrektywach sztuki wojennej. Próba spojrzenia filozoficznego*, [w:] tamże.

zjawiska, jakim są operacje informacyjne, za uzasadniony. Wykonanie tego zadania warunkowane było poznaniem teorii odnoszących się do głównej kategorii operacji informacyjnych, jaką jest informacja. Nie wszystkie ujęcia teorii informacji mogą być przydatne w naszych rozważaniach, dlatego też uznano, że definiowanie operacji informacyjnych musi być poprzedzone zidentyfikowaniem zgodnego z potrzebami ujęcia teorii informacji.

Definiowanie operacji informacyjnych powinno być prowadzone ze świadomością potrzeby jednoczesnego identyfikowania tej części tych operacji, która mogłaby być stosowana przez siły zbrojne. Było oczywiste, że siły zbrojne są komponentem struktury państwa, nie podlegają więc jakiemukolwiek innemu ośrodkowi decyzyjnemu, niż władze państwa. Siły zbrojne są instrumentem polityki państwa. Ponieważ celem państwa jest ochrona i obrona grupy społecznej, którą obejmuje[69] i tylko państwo dysponuje pełnią władzy, to tylko ono może realizować wszystkie funkcje w tym zakresie. Mając świadomość ujawnionej już rozległości operacji informacyjnych, oczywiste stało się, że jedynie państwo może być podmiotem prowadzącym pełnię tych działań. **Operacje informacyjne sił zbrojnych, są więc jedynie częścią operacji informacyjnych państwa. Nie sposób** więc **badać operacje informacyjne sił zbrojnych, nie znając charakteru operacji informacyjnych państwa**. W rezultacie zaistniała konieczność **zidentyfikowania istoty operacji informacyjnych państwa.** Istota ta będzie fundamentem do definiowania militarnych operacji informacyjnych.

1.3. Analiza terminologiczna

1.3.1. Terminologia ogólna

Siły zbrojne są elementem państwa przeznaczonym do stosowania przemocy zbrojnej. Analizując najczęściej spotykane kategorie, oznaczające komponent związany ze stosowaniem przemocy zbrojnej, dostrzec można, iż wśród polskich badaczy funkcjonują nazwy: „siła zbrojna", „siły zbrojne", „siła militarna", „środki wojskowe", „środki militarne", „sfera wojskowości", „przemoc zbrojna"[70], „armia", „wojsko". Czasami nawet ten sam autor stosuje jednocześnie różne nazwy, traktując je jako synonimy.

Poszczególne nazwy są obarczone pewnymi słabościami. Zacznijmy od nazwy „siła zbrojna". Według *Słownika języka polskiego* „siła" to „energia fizyczna lub duchowa, zdolność do wysiłku, do działania, możność podołania czemuś; zaś „moc" w znaczeniu wojskowym: wojsko, armia, oddziały wojska" oraz „ zdolność bojowa wojska oceniana liczbą żołnierzy i uzbrojeniem"[71]. Słowo „zbrojny" znaczy zaś tyle, co: „zaopatrzony w broń, w sprzęt wojskowy; uzbrojony" oraz „zwią-

[69] K.A. Wojtaszczyk, wyd. cyt., s. 22.
[70] B. Balcerowicz, *Sojusz a obrona...* wyd. cyt.
[71] *Słownik języka polskiego*, red. nauk. M. Szymczak, t. 3, PWN, Warszawa 1981, s. 217–218.

zany z użyciem broni, z walką, z wojną, dokonany za pomocą broni"[72]. W sumie znaczenie tej nazwy może się zawierać pomiędzy sformułowaniem „energia (fizyczna lub duchowa) związana z użyciem broni" a „wojsko zaopatrzone w broń". „Siły zbrojne" zaś to: „organizacja militarna oparta na powszechnym obowiązku służby wojskowej lub zaciągu ochotniczym [...] armia, wojsko"[73].

Tymczasem słowo „wojsko" oznacza „siły zbrojne państwa, armia"[74], a „wojskowy" to „związany z wojskiem, ze służbą w wojsku; przeznaczony dla wojska, należący do wojska"[75]. Kolejne słowo – „militarny" to tyle co, „dotyczący wojska, wojskowości; wojskowy", a przytaczane formy użycia to „Siła militarna. Przygotowania militarne. Państwo militarne"[76]. Również w języku angielskim słowo „military" może mieć znaczenie przymiotnikowe i rzeczownikowe. Jako przymiotnik oznacza coś, co ma związek z żołnierzami, armiami lub wojną; jako rzeczownik znaczy „żołnierzy, armię". Z analizy tej wynika, że słowo „zbrojny" ma podobne znaczenie jak „militarny", jednakże akcentuje kontekst „bycia uzbrojonym", podczas gdy to drugie uwypukla związek z wojskiem, które jest w istocie organizacją społeczną, nazywaną również siłami zbrojnymi.

Również słowo „militarny" ma podobne znaczenie jak „wojskowy", jednak w *Słowniku języka polskiego*, w objaśnieniu znaczenia „wojskowy" nie pojawia się słowo „militarny". Można z tego wnioskować, że słowa te, aczkolwiek mają zbliżone znaczenia, to nie są tożsame. Słowo „wojskowy", zawiera się bowiem w znaczeniu słowa „militarny", a nie odwrotnie. Słowo „militarny" ma nieco szerszy zakres znaczeniowy. **Można uznać, że słowo „wojskowy" lepiej pasuje do opisywania struktury zbrojnej i aspektów jej funkcjonowania, innymi słowy, lepiej służy praktyce, zaś słowo „militarny" oznacza całą sferę organizowanej przez państwo przemocy zbrojnej przeciwko aktorom sceny międzynarodowej.** Obejmować więc może zarówno wojsko (siły zbrojne), jak i wspierającą go infrastrukturę cywilną. Jednym z przykładów jest chociażby Ministerstwo Obrony Narodowej. Jego cywilne departamenty trudno zaliczyć do sił zbrojnych. Również cywilne instytuty naukowe prowadzące badania w sferze militarnej, przemysł zbrojeniowy, a nawet firmy cywilne świadczące całą gamę usług także na polu walki – to tylko przykłady desygnatów, które określać można przymiotnikiem „militarny", a nie „wojskowy".

Powszechnie się spotyka, również w literaturze, słowo „obronność". *Słownik języka polskiego* traktuje je jako „rzeczownik od *obronny* podnosić obronność kraju; obronność pozycji, postawy." „Obronny" natomiast to tyle, co „stanowiący obronę przed atakiem, napaścią, broniący, przystosowany, służący do obrony, mogący stanowić obronę"[77]. Autorzy *Słownika terminów z zakresu bezpieczeństwa*

[72] Tamże, s. 987.
[73] Tamże.
[74] Tamże, s. 745.
[75] Tamże, s. 746.
[76] *Słownik języka polskiego*, t. 2, PWN, Warszawa 1981, s. 176.
[77] Tamże, s. 424.

narodowego „obronność" uznają za „jedną z podstawowych dziedzin działalności państwa, mającą na celu przeciwdziałanie wszelkiego rodzaju zagrożeniom"[78].

Można więc przyjąć, że obronność oznacza przede wszystkim zdolność obronną państwa. Obronność odnosi się nie tylko do zagrożeń militarnych. Odpowiednio więc do rodzaju zagrożeń, można wyróżnić obronność militarną, obronność ekonomiczną i inne. Zdolność ta dotyczy obrony przed zagrożeniami oraz obrony własnych interesów narodowych. Do najważniejszych z nich należy zapewnienie bezpieczeństwa istnienia i rozwoju danego państwa i tworzącego go narodu. Interesy te mogą być sprzeczne z interesami innych państw i narodów. Każdy z tych podmiotów jest obrońcą swoich interesów i w ramach tej obrony może stosować także instrument militarny. Może się tak zdarzyć, że to, co dla jednego podmiotu jest „obronnością", dla innego jest „agresywnością". Nazwa „obronność" jest więc rodzajem szyldu noszącego w sobie cechy poprawności politycznej. Słowo „militarny" jest przymiotnikiem oznaczającym, że coś jest jakieś. Co więc dla tego słowa jest wyróżnikiem, kryterium oznaczającym, że owo „coś" jest militarne? Najlepiej byłoby znaleźć takie kryterium, za pomocą którego można byłoby dokonać podziału dychotomicznego na militarny i niemilitarny. Za kryterium takie należy uznać zdolność do stosowania przemocy zbrojnej w stosunkach międzynarodowych, gdyż sfera militarna ma na nią monopol. Jest to więc cecha właściwa jedynie tej sferze.

Zapytać więc należy, jaką przemocą jest przemoc „zbrojna"? Semantycznie jest nią przemoc wynikająca z zastosowania uzbrojenia, bo „zbrojny" to „zaopatrzony w broń, [...] związany z użyciem broni"[79]. Sytuacja była klarowna, gdy na arenie międzynarodowej istniała „klasyczna" broń wojskowa. Obecnie jednak pojawiają się nowe, coraz bardziej „cywilne" rodzaje broni. Są to chociażby: broń biologiczna, informacyjna, psychotroniczna, klimatyczna, ale również broń ekonomiczna, kulturowa. Historia wskazuje, że wraz z rozwojem cywilizacyjnym pojawiają się nowe rodzaje uzbrojenia, a proces ten trwa nieustannie. Gdyby tak nie było, to np. samolot nie mógłby być zaliczany do broni. Należy więc uznać, że równolegle z poszerzaniem się zbioru broni, poszerza się zakres przemocy zbrojnej. Zakres ten jest otwarty, a w związku z obserwowaną obecnie akceleracją rozwoju cywilizacyjnego, także poszerzanie zakresu przemocy zbrojnej będzie coraz szybsze. W najszerszym kontekście również instrumenty ekonomiczne traktowane są jako broń ekonomiczna. Wobec tego uznać należy, iż **znaczenie ma tu nie tyle charakter broni, lecz wywoływany przez nią skutek. Podstawową cechą broni jest jej zdolność do dezintegracji lub paraliżu.**

Od zarania dziejów skrajną formą przemocy była walka zbrojna, a jej istotą jest destrukcja, w której wyniku następuje dezintegracja bądź paraliż. Również obecnie należy uznać, iż niezależnie od rodzaju broni **zdolność do destrukcji jest głównym atrybutem sfery militarnej**, której główną częścią są siły zbrojne, a de-

---

[78] *Słownik terminów z zakresu bezpieczeństwa narodowego*, pod kier. J. Pawłowskiego, AON, Warszawa 2002, s. 83.

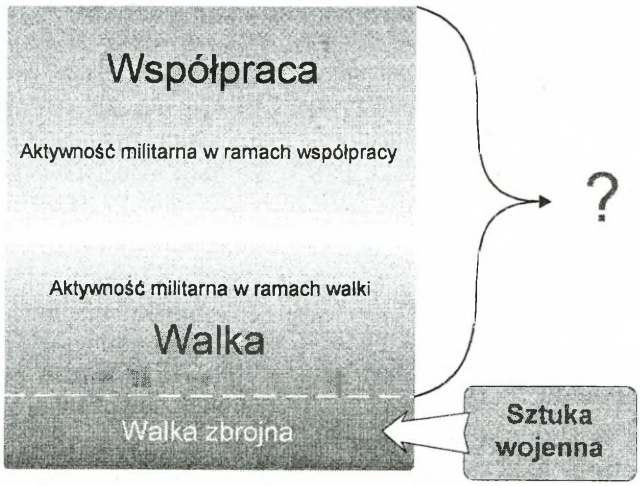
[79] *Słownik języka polskiego*, t. 3, wyd. cyt., s. 987.

strukcja jest istotą przemocy zbrojnej. Wobec tego **„militarny" to zdolny do stosowania przemocy zbrojnej, której istotą jest destrukcja. Siły powietrzne są więc jednym z militarnych komponentów państwa, zdolnym do stosowania przemocy zbrojnej.**

1.3.2. Pojęcia „sztuka wojskowa" i „sztuka wojenna"

Badanie zjawisk sfery militarnej, w której ulokowana jest działalność sił powietrznych, a szczególnie tych związanych ze stosowaniem przemocy zbrojnej, jest najczęściej utożsamiane z uprawianiem sztuki wojennej. Sztuka ta będąca częścią nauk wojskowych jest ściśle wiązana ze zjawiskiem wojny.

Wojna jest przedmiotem badań sztuki wojennej, która zajmuje się teorią i praktyką przygotowania i prowadzenia wojny. Jednakże sfera militarna państwa, poza okresami wojny angażowana jest nie tylko do przygotowywania się do kolejnej wojny. Uczestniczy w wielu formach aktywności międzynarodowej oraz narodowej, czasami równie ważnej jak wojna, bo prowadzącej do osiągania ważnych celów politycznych narodu. Czy wobec tego można założyć, iż sztuka wojenna obejmuje swoim zainteresowaniem całą sferę aktywności militarnej? Ponadto – czy należałoby się zajmować tymi obszarami działalności militarnej, które nie dotyczą wojny oraz jaka dyscyplina nauki powinna się nimi zajmować? Wobec tak postawionego pytania można założyć hipotezę, że **tradycyjnie rozumiana sztuka wojenna nie obejmuje wszystkich obszarów aktywności militarnej** (rys. 1).



Opracowanie własne.

Rys. 1. Obszary aktywności militarnej oraz ich relacje ze sztuką wojenną

Poszukując odpowiedzi na te pytania warto zbadać najistotniejsze poglądy na sztukę wojenną. Według *Małej encyklopedii wojskowej* sztuka wojenna to dziedzina wiedzy i umiejętności dotycząca przygotowania i prowadzenia walki zbrojnej[80].

Według *Leksykonu wiedzy wojskowej* sztuka wojenna to teoria i praktyka przygotowania państwa (koalicji) i sił zbrojnych do wojny oraz wykorzystania w czasie działań wojennych materialnych, moralnych i militarnych możliwości do realizacji celów i zadań (strategicznych, operacyjnych, taktycznych), nakreślonych przez politykę państwa, oraz kierowanie prowadzonymi działaniami[81]. W *Słowniku terminów z zakresu bezpieczeństwa narodowego*, sztukę wojenną definiuje się jako dziedzinę wiedzy i umiejętności dotyczącą form i sposobów przygotowania oraz prowadzenia działań wojennych w skali strategicznej, operacyjnej i taktycznej[82].

Uogólniając te poglądy, można by uznać, iż działalność militarna związana z wojną, a będąca przedmiotem zainteresowania sztuki wojennej, sprowadza się do prowadzenia wojny bądź przygotowywania się do niej. Tymczasem wielu myślicieli dostrzega obszary aktywności militarnej, które nie są ani prowadzeniem wojny, ani przygotowywaniem się do niej.

Praktyka również dostarcza nam takich przykładów. Przykładem szczególnie wyraźnym jest tu grupa obecnie prowadzonych na szeroką skalę działań pozawojennych (*military operations other than war – MOOTW*). Działania te stały się przedmiotem zainteresowania wielu teoretyków, zarówno wojskowych, jak i cywilnych. Opracowane zostały także odnoszące się do nich doktryny. Kłopoty z wyraźnym określeniem zakresu sztuki wojennej wynikają głównie z trudności definiowania wojny, która mimo powszechności występowania w dziejach ludzkości nie jest zjawiskiem wyraźnie określonym.

Carl von Clausewitz traktuje wojnę jako czyn nie tylko polityczny, lecz prawdziwe narzędzie polityki, dalszy ciąg stosunków politycznych prowadzonych innymi środkami[83]. Również Franciszek Skibiński uznaje, iż wojna to „kontynuacja polityki prowadzona środkami przemocy w celu zmuszenia przeciwnika do spełnienia naszej woli". Dodaje jednak, iż „nosi charakter krwawej walki zbrojnej, staczanej przez zorganizowane siły zbrojne"[84]. *Encyklopedia powszechna PWN* wojną nazywa „zjawisko społeczne, historyczne i klasowe, polegające na regulowaniu sporów lub realizowaniu celów politycznych, przez zastosowanie przemocy w postaci sił zbrojnych"[85]. Także *Mała encyklopedia wojskowa* definiuje wojnę jako „konflikt zbrojny między państwami, blokami państw, narodami lub klasami społecznymi, kontynuacja polityki środkami przemocy w celu osiągnięcia określonych interesów politycznych, ekonomicznych lub ideologicznych"[86]. *Słownik terminów z zakresu bezpieczeństwa narodowego* podaje syntetyczną wersję definicji wojny,

---

[80] *Mała encyklopedia wojskowa*, t. 3, Warszawa 1971, s. 268.
[81] *Leksykon wiedzy wojskowej*, Warszawa 1979, s. 43.
[82] *Słownik terminów...* s. 144.
[83] Zob. C. Clausewitz, *O wojnie*, Warszawa 1958, s. 15.
[84] F. Skibiński, *Rozważania o sztuce wojennej*, Warszawa 1978, s. 29.
[85] *Encyklopedia powszechna PWN*, Warszawa 1976, s. 697.
[86] *Mała encyklopedia wojskowa*, Warszawa 1971, t. 3, s. 494.

uznając ją za „kontynuację polityki środkami przemocy, której głównym przejawem jest walka zbrojna"[87]. *Nowa encyklopedia powszechna PWN* wojną nazywa „zjawisko społeczno-polityczne stanowiące integralną część dziejów ludzkości od początków organizacji społecznej, o zasięgu rosnącym wraz z rozwojem technologii; [...] zorganizowaną walkę zbrojną między państwami, narodami lub grupami społecznymi"[88]. *Encyklopedia prawa* uznaje, że „wojna była ściśle związana z rozwojem państw i historią świata. Pomimo tego nie znalazła ona zdefiniowania w nauce prawa międzynarodowego. Można ogólnie jedynie stwierdzić, że jest to przeciwstawienie stanu pokoju polegające na stanie walki zbrojnej pomiędzy państwami, bez względu na przyczynę wywołującą ten stan. Szerszymi od wojny pojęciami są konflikt zbrojny oraz użycie siły"[89].

Analizując różne definicje wojny, dostrzec można, iż dosyć powszechnie za główny desygnat wojny uznaje się walkę zbrojną prowadzoną przez państwa lub narody. Postrzeganie wojny przez pryzmat walki zbrojnej ma jednak swoje słabości, gdyż nie każdy przypadek walki zbrojnej możemy uznać za wojnę. Rodzi to problem, który mobilizuje do jego rozwiązania. Według jednej grupy badaczy zjawiska wojny, należy zachować dotychczasowy stan, dokonując jedynie niewielkich korekt. Ilustracją tego typu stanowiska są poglądy S. Kozieja oraz Bogdana Szulca. Uznając, iż istotą wojny jest walka zbrojna, stajemy przed problemem, czy każda walka zbrojna oznacza wojnę. Rodzi się także pytanie, czy wojna to tylko walka zbrojna.

Przed takim dylematem staje w swoich rozważaniach S. Koziej, który dostrzega, że „działania wojenne to nie tylko działania sił zbrojnych, lecz wszelkie działania, jakie podejmowane są w toku wojny, by osiągnąć jej cele"[90]. Jednocześnie dostrzega występujący w stosunkach międzynarodowych stan pośredni, nazywany przez różnych autorów zimną wojną, wojną pośrednią, wojną nieorężną czy też wojną niekonwencjonalną, a także wojną ideologiczną, wojną psychologiczną, wojną gospodarczą. „Stan ten charakteryzuje się brakiem walki zbrojnej. Stwarza to konieczność poszerzenia definicji wojny tak, aby objąć nim także stosowanie samych pozazbrojnych form przemocy politycznej albo zachowania jej dotychczasowego pojmowania, a stosowanie wyłącznie niezbrojnej przemocy do narzucania swej woli stronie przeciwnej uważać za jakościowo inne zjawisko i nazwać inaczej"[91]. Wobec tego dylematu, posługując się głównie argumentem niebezpieczeństwa rewolucji terminologiczno-pojęciowej w całym systemie nauk wojennych, proponuje „wojną nazywać tylko to, co dotychczas tak się nazywało. Natomiast działań politycznygh o celach konfrontacyjnych (polityczną kooperację negatywną) – osiąganych bez zniszczenia przeciwnika za pomocą siły zbrojnej – nie uwa-

[87] *Słownik terminów...* s. 156.
[88] *Nowa encyklopedia powszechna PWN*, Warszawa 1996, t. 6, s. 848.
[89] *Encyklopedia prawa*, Warszawa 1999, s. 856.
[90] S. Koziej, *Teoria sztuki wojennej*, Warszawa 1993, s. 14.
[91] Tamże, s. 10.

żać za wojnę"[92]. Według takiego założenia wojna jest zjawiskiem, którego nieodłączną cechą jest walka zbrojna. Bez tego nie ma pojęcia wojny i nie istnieje samo pojęcie „wojna".

Stanowisko takie rodzi pewną sprzeczność, z inną proponowaną przez niego definicją wojny, która uznaje, iż „wojna da się opisać jako taki stan stosunków politycznych (działanie polityczne), w którym cele stron mają charakter konfrontacyjny i dąży się do ich osiągnięcia środkami zbrojnymi (wspieranymi przez środki niezbrojne)"[93]. Sprzeczność ta wynika z faktu, że „dążenie do osiągnięcia celów środkami zbrojnymi" nie musi oznaczać walki zbrojnej definiowanej jako „bezpośrednie starcie zgrupowań wojsk, wzajemne destrukcyjne oddziaływanie za pomocą posiadanych środków rażenia, to przede wszystkim fizyczne niszczenie i psychologiczne obezwładnianie przeciwnika, jako przeszkody na drodze do celu"[94]. Jest wiele przykładów na osiągnięcie celów środkami zbrojnymi bez walki zbrojnej. Jednym z nich jest ultimatum Hitlera i groźba użycia siły militarnej w wypadku jego odrzucenia. W wyniku tego bez walki zbrojnej zajęta została Czechosłowacja. Przywoływany już jeden ze starożytnych klasyków sztuki wojennej Sun Tzu, twierdzi wręcz, że „najwyższym osiągnięciem jest pokonać wroga bez walki"[95].

Jednocześnie zdając sobie zapewne sprawę z istnienia dużej ilości konfliktów lokalnych, w których występuje walka zbrojna i powszechnej niechęci do traktowania ich jako wojen, S. Koziej proponuje nazwanie wszystkich konfliktów, w których stosowana jest walka zbrojna, „konfliktami zbrojnymi". Klasyczne wojny są zaś „konfliktami wojennymi". Proponuje też kolejną kategorię, która jest trzecim, pośrednim między wojną a pokojem stanem stosunków międzynarodowych. Kategoria ta to „konflikt niezbrojny". Nazwa ta obejmuje konflikt między dwiema i więcej stronami, rozgrywany bez użycia sił zbrojnych[96]. Powstaje pytanie o granice „konfliktu niezbrojnego" i „konfliktu zbrojnego". Skoro konflikt niezbrojny nie obejmuje użycia sił zbrojnych to znaczy, że siły te nie są w nim w jakimkolwiek stopniu zaangażowane, bowiem nie tylko nie toczy się walka zbrojna, lecz również siły zbrojne pozostają neutralne i nie podejmują działań związanych z konfliktem. Inaczej byłyby one w jakimś stopniu używane. Wynika z tego, że przyjmując za kryterium użycie sił zbrojnych, wyróżnić można jedynie dwa stany – z użyciem sił zbrojnych i bez ich użycia. Ten pierwszy równa się co najmniej konfliktowi zbrojnemu, ten drugi zaś obejmuje pokój i konflikt niezbrojny.

Nieco odmiennego zdania jest B. Szulc, który analizując poglądy S. Kozieja, uznał, że:

„W najogólniejszym ujęciu można by przyjąć rozwiązanie tegoż autora. Dopatrujemy się tu jednak pewnych nieścisłości. Otóż, jeżeli byśmy przyjęli te kategorie w oderwaniu od ogólnej teorii czynu skutecznego, wówczas mają one układ

[92] Tamże.
[93] Tamże, s. 9.
[94] Tamże, s. 16.
[95] Sun Tzu, s. 35.
[96] S. Koziej, *Teoria sztuki...* s. 11.

racjonalny. Ponieważ jednak wywodzimy je z tej teorii, to musimy dokonać pewnych korekt. Walka, jak już wskazywaliśmy, jest czynem jako takim, a zatem prowadzenie jej to nic innego, jak działanie. Działania w walce mogą mieć charakter niezbrojny lub zbrojny. S. Koziej mówi tu o wojnie. Jeżeli utożsamiać będziemy wojnę z walką (w ujęciu Tadeusza Kotarbińskiego), wówczas podział ten (do tego etapu) jest przekonujący. Problem zaczyna się przy podziale zbrojnych działań wojennych, w których wyodrębnia walkę (starcie) zbrojną, przemieszczanie wojsk i pogotowie zbrojne. Nasze wątpliwości przejawiają się w tym, że atrybutami walki są: przestrzeń, czas i rażenie. Zważmy, że walka taka toczy się w określonym obszarze, w którym obok starć mas, uderzeń (ogniowych i innych) wojska są (powinny być) w ciągłym ruchu. Uwzględniają to i wskazywane przez nas twierdzenia, i powszechnie przyjmowane zasady walki (Kozieja – MANEWR). Tak więc w obszarze tym (obszar walki) wojska będą (w zależności od sytuacji) maszerować i przegrupowywać się po to, aby przyjąć odpowiednią pozycję, ugrupowanie. W czasie tych ruchów przeciwnik może na nie oddziaływać orężnie i one mogą oddziaływać orężnie. W takim kontekście, działanie takie – w myśl przyjętej definicji – jest walką zbrojną. Nie może być zatem wyodrębnione jako inna klasa zjawisk, poza walką zbrojną.

Być może przyczyną tej klasyfikacji jest rozumienie bezpośredniego starcia (strefa bezpośredniego starcia z przeciwnikiem). Otóż kategoria ta w wojnach przeszłych miała swoje uzasadnienie. Musimy jednak dostrzegać, iż obecnie – ze względu na wzrost możliwości bezpośredniego oddziaływania – zatraciła ona rację bytu. Tak samo jak rację bytu zatraciło pojęcie wojny klasycznej, której nie możemy zdefiniować, choćby ze względu na fakt, iż każda wojna była inna. Kwestie powyższe dotyczą również pogotowia zbrojnego. Gdybyśmy dziś chcieli określić stany wojsk w walce zbrojnej, to możemy je ująć w trzech sferach. W walce zbrojnej (wojnie) wojska są w stanie starcia (walki bezpośredniej), przemieszczania (przegrupowania) lub przygotowania (odpoczynek, uzupełnianie, szkolenie). Innych stanów – jak się wydaje – nie jesteśmy w stanie wyodrębnić.

Tu wypada podnieść jeszcze jedną kwestię. W ostatnich latach często wyodrębnia się jako zjawiska poza wojną (rozumianą jako walka zbrojna) różnego rodzaju konflikty zbrojne (np. konflikt przygraniczny, ograniczony konflikt zbrojny). Otóż stoimy na stanowisku, iż każde starcie dwóch podmiotów z użyciem oręża jest walką zbrojną (wojną). Wprowadzanie nowych nazw dla tej samej klasy zjawisk jest, w naszym przekonaniu, jedynie wprowadzaniem nowych rytów językowych dla tych samych zjawisk, modą na nowe, które nowym nie jest"[97].

Tymczasem na ścisłe związki cywilnej i militarnej aktywności zarówno w czasie pokoju, jak i wojny zwraca uwagę Raymond Aron. Uważa on, iż „każde państwo pozostaje w jakichś stosunkach z innymi; tak długo, jak państwa pozostają w stosunkach pokojowych, muszą, chcąc nie chcąc, dawać sobie radę i w jakiś sposób ze sobą współżyć. Jeśli nie chcą sięgać po przemoc, próbują się wzajem prze-

[97] M. Szulc, *Dylematy epistemologiczne i metodologiczne teorii sztuki wojennej*, [w:] *Sztuka wojenna*... s. 49–50.

konywać. W chwili gdy zaczynają ze sobą walczyć, próbują się wzajem do czegoś zmusić. W tym znaczeniu dyplomację można nazwać sztuką przekonywania bez użycia siły, strategię zaś sztuką zwyciężania najmniejszym kosztem. Lecz przymus jest również sposobem przekonywania. Także demonstracja siły może spowodować, że przeciwnik ustąpi – choć jest ona raczej symbolem przymusu, niż realnym jego zastosowaniem. Kto więc posiada przewagę w siłach zbrojnych w czasach pokoju, ten może przekonać sojuszników, rywali czy przeciwników, nie uciekając się do użycia siły. Ale z drugiej strony państwo, które zdobyło sobie opinię sprawiedliwego i umiarkowanego, ma większe szanse na to, by osiągnąć swoje cele bez odnoszenia ostatecznego zwycięstwa wojskowego. Nawet w czasie wojny więcej osiągnie perswazją niż przymusem.

Rozróżnienie między dyplomacją i strategią jest bardzo względne. Oba te terminy odpowiadają uzupełniającym się aspektom tej samej sztuki politycznej – sztuki kształtowania stosunków z innymi państwami w sposób najkorzystniejszy dla interesu narodowego. Chociaż, z samej definicji nie można mówić o strategii, czyli o sposobie prowadzenia operacji wojskowych, w chwili gdy takie operacje nie mają miejsca, to jednak środki wojskowe stanowią także integralną część narzędzi, którymi posługują się dyplomaci. I odwrotnie, do arsenału środków, jakimi dysponuje przywódca wojującego państwa w stosunku do sojuszników, państw neutralnych i dzisiejszych nieprzyjaciół, czyli wczorajszych lub jutrzejszych sojuszników, należą również słowa, noty, obietnice, gwarancje i groźby"[98].

Dlatego też inna grupa badaczy postuluje szersze podejście. Jeden z nich, J. Świniarski, w swoich rozważaniach filozoficznych o naturze bezpieczeństwa zauważa, iż „ich [sił zbrojnych – R.S.] zadaniem pierwszym i oczywistym jest bezpieczeństwo militarne. A to bezpieczeństwo, wiązane z bezpośrednimi i pośrednimi działaniami wojska, realizowane jest tak w walce zbrojnej, jak i poza tą walką, i to nie tylko przez prowadzenie regularnych operacji zaczepnych, ale również przez obecność militarną. Właśnie udział sił zbrojnych w misjach i operacjach międzynarodowych zmienia oblicze armii, uwypukla pomijaną kiedyś jej rolę i funkcję, jaką jest utrzymywanie i przywracanie bezpieczeństwa, także przez pośrednie działania zbrojne, środki pokojowe i metody konstrukcyjno-profilaktyczne. Ale udział ten nie pomniejsza wcale ich tradycyjnej roli i funkcji, jaką były i są starcia orężne, bezpośrednie działania zbrojne i metody dekonstrukcyjno-konserwacyjne. Te ostatnie również służą bezpieczeństwu. Intencje i praktyka wykorzystywania sił zbrojnych w misjach i operacjach pokojowych dobrze argumentują za propagowanym przez filozofię bezpieczeństwa spojrzeniem na wojnę i pokój. Rzecz w tym, że bezpieczeństwa w długim czasie nie daje się osiągać bez środków wojennych i pokojowych. Najlepiej zaś osiągać bezpieczeństwo umiarkowaniem w wykorzystywaniu tak środków i metod wojennych, jak i środków, i metod pokojowych, starć orężnych (aby osiągnąć przewagę) i zagrożeń"[99].

---

[98] R. Aron, *Pokój i wojna...* s. 41–42.
[99] J. Świniarski, *O naturze...* s. 234.

W innej swojej wypowiedzi proponuje szerokie, holistyczne rozumienie zarówno wojny, jak i sztuki wojennej, twierdząc, iż:

„W przywołanym spojrzeniu starożytnym i współczesnym sztuka wojenna dotyczy raczej szeroko pojmowanej wojny, jako pierwszej ludzkiej pracy i starania o trwanie, przetrwanie i doskonalenie życia. Od tego uniwersalnego spojrzenia starano się odchodzić w ramach nowożytnego paradygmatu nauki. W jego ramach wojnę starano się często identyfikować tylko z walką zbrojną. Celowali i celują w tym przede wszystkim ci teoretycy wojskowi, którzy tylko z faktów, opisów walk i zmagań orężnych – doświadczenia – starają się wyprowadzać teorię sztuki wojennej jako teorię, w rzeczy samej, zmagań orężnych. Ale dziś – u schyłku paradygmatu scientystyczno-pozytywistycznego nauki i nawet, jak przekonują niektórzy, kryzysu ery nauki – powraca się do szerokiego i uniwersalnego pojmowania wojny i sztuki wojennej. Coraz bardziej przekonujące są argumenty za tym, że sztuka wojenna to nie tylko sztuka zmagań zbrojnych, lecz każdego zmagania o ściśle określonych skutkach. Jednocześnie sztuka ta odróżniana jest od sztuki sprawiania pokoju, której skutki są inne, aczkolwiek też ściśle określone"[100].

Również Marian Laszczyk oraz Włodzimierz Miszalski uważają, iż zmieniające się obecnie warunki polityczno-militarne zmuszają do przewartościowania ustaleń nauk wojskowych. Napływające z Zachodu nowe poglądy, wzbudzały pewien opór. Jednakże po głębszej refleksji okazało się, że:

„Sztuka wojenna nie została bowiem w żaden sposób podważona. Wręcz przeciwnie, została ona rozwinięta, zmodyfikowana, a jej zakres i znaczenie uległy znacznemu rozszerzeniu. Najbardziej widocznym przeobrażeniom należało poddać przede wszystkim strategię, będącą najwyższym poziomem sztuki wojennej. To, co dzisiaj mieści się w pojęciu „strategia", nie odpowiada już z pewnością swemu greckiemu pierwotnemu znaczeniu, czyli sztuce użycia wojsk przez wodza w celu pobicia wroga. Obecnie przyjmuje się, że strategia to przygotowanie państwa do wojny lub zapobieganie jej. Nie jest to więc już jedynie prowadzenie wielkich operacji, jak to przyjmowano w okresie istnienia Układu Warszawskiego.

Strategia postrzegana jest jako metoda przekształcania możliwości państwa w konkretne działania polityczno-militarne. Jest to więc w pewnym sensie metoda transformacji siły w politykę"[101].

Najszerzej problematykę tę podjął B. Balcerowicz, uznając, iż kluczem do zrozumienia roli sił zbrojnych w państwie, jak też w stosunkach międzynarodowych jest właściwe rozpoznanie relacji zachodzących między polityką a narzędziami (środkami) polityki[102]. Analizując te relacje, słusznie zauważył, że: „Siła – siła militarna – jest oczywiście do dziś narzędziem polityki, ale – jak wyraźnie można zaobserwować – **narzędziem jednym z wielu**, a ponadto narzędzie owo może być wykorzystane na różne sposoby (pośrednio lub bezpośrednio), w stanie:

---

[100] J. Świniarski, *O zasadach...* s. 70.

[101] M. Laszczyk, W. Miszalski, *Niektóre dylematy współczesnej sztuki wojennej*, [w:] *Sztuka wojenna. Konteksty teoretyczne i praktyczne*, red. M. Krauze, B. Szulc, Toruń 2000, s. 203.

[102] Zob. B. Balcerowicz, *Sojusz a obrona...* s. 20.

pokoju, kryzysu, wojny. Zakłada się, że polityka dla osiągnięcia swoich celów dysponuje szerokim instrumentarium, posługuje się wieloma narzędziami.

Zarówno zakresy znaczeniowe pojęcia siły militarnej jako „środka przemocy", jak też „narzędzia polityki" uległy znacznym przewartościowaniom"[103].

Rozwijając tę myśl, stwierdza m.in.:

„Od zarania dziejów, odkąd istnieją zorganizowane społeczności, a szczególnie odkąd zorganizowane są one w formie państw, wśród narzędzi polityki zawsze trzy odgrywały rolę najważniejszą:

- **dyplomacja;**
- **ekonomika (gospodarka);**
- **siły zbrojne.**

Znaczenie i skuteczność tych narzędzi oraz preferencje w ich stosowaniu są i były zależne od wielu czynników. Nie są one jednakowe w polityce poszczególnych państw, a w zależności od okresu historycznego różna jest ich ‚moc'. O skuteczności w osiąganiu celów polityki przesądzało zawsze jednak odpowiednio ‚zestrojone' zastosowanie kilku instrumentów, w tym oczywiście wymienionych powyżej. [...] Żadna więc polityka ani dyplomacja nie może być skuteczna w przypadku bezsilności militarnej. To truizm, ale truizm, którego nie da się zignorować. Polityczna funkcja siły militarnej zależna jest oczywiście od jej wielkości. Tak samo rzecz się ma z potęgą gospodarczą. Za pomocą złota (pieniądza) można zdziałać wiele, ale – jak uczy historia – bogactwo niebronione ktoś zawsze bezkarnie zawłaszczał. Środki gospodarcze mogą być stosowane na różne sposoby. Państwo bądź koalicja państw, by zmusić lub ‚przekonać' inne państwo do ustępstw, może zastosować nacisk gospodarczy. Nacisk gospodarczy (sankcje) bywa nawet ostatnio legitymizowany decyzjami Narodów Zjednoczonych. [...] Rola sił zbrojnych, ich znaczenie w polityce zagranicznej są wyraźnie różne w różnych stanach państwa (pokoju – kryzysu – wojny). Powszechnie oczywista, nie wymagająca wyjaśnienia, jest rola sił zbrojnych w stanie wojny – wynik starć zbrojnych ma bowiem znaczenie przesądzające dla osiągnięcia generalnych celów wojny. W czasie kryzysu natomiast – choć stosuje się spektakularne zazwyczaj, ale jedynie pośrednie formy wykorzystania sił zbrojnych – ich rola jest niewątpliwie znaczna, niekiedy pierwszoplanowa, ale nie rozstrzygająca. Rola sił zbrojnych w stanie wojen i kryzysów jest na tyle oczywista, że częstokroć spotykamy się z opiniami skrajnymi, rolę tę absolutyzującymi. By z kolei uświadomić sobie, na czym polega rola sił zbrojnych w stanie pokoju, trzeba pamiętać, że wciąż jeszcze istnieją dwa odrębne podejścia do traktowania relacji: okres pokoju – okres wojny.

Pierwsze – to podejście sięgające rodowodem czasów rewolucji październikowej, podczas której (i przez jeszcze dalsze pół wieku) stan pokoju traktowany był jako swoisty ‚antrakt' między wojnami. Należało zatem ten czas spożytkować na rzecz przygotowań do wojny. Naturalną konsekwencją takiego podejścia była rola wyznaczona siłom zbrojnym, która w oficjalnej wersji doktryny miała spro-

[103] Tamże, s. 21.

wadzać się li tylko do przygotowań ‚na wypadek wojny', ‚zainicjowanej przez przeciwnika'.

Zarówno radzieckie, jak i ‚satelickie' siły zbrojne, oprócz przygotowywania się do wojny, spełniały też inne funkcje, jednak to filozofia swoistego oczekiwania na wojnę przesądzała o ich liczebności, kształcie, wyposażeniu, szkoleniu. Takie jednostronne traktowanie roli i funkcji siły militarnej w państwie w czasie pokoju wiedzie w okolice absurdu. W miarę przedłużania się bowiem owego antraktu, czyli normalnego dla większości społeczeństw okresu pokoju, nadmiernie rozbudowane siły zbrojne (szykowane jedynie do wojny) stają się mało użytecznym balastem.

Tymczasem, rzecz ma się przecież zupełnie inaczej – to stan wojny jest tym, który wypełnia lukę między okresami (stanami) pokoju. Celem wojny jest właśnie zawarcie pokoju, ale pokoju na nowych warunkach. To czas wojny ma zatem niejako ‚pracować' na czas pokoju, a nie odwrotnie. Przy powyższym, w pełni naturalnym założeniu, zmienia się punkt widzenia na rolę, znaczenie i funkcje sił zbrojnych; spektrum ich funkcji i zadań musi się rozszerzyć.

Tak to już jest, że w czasie pokoju państwa poza środkami dyplomatycznymi, gospodarczymi i innymi, np. psychologiczno-politycznymi – posługują się także przemocą. [...] R. Aron rozważając kwestie przemocy rozróżnia ‚przemoc symboliczną' i ‚przemoc niejawną', czyli ‚rozproszoną'. [...]

Jednak podstawowym środkiem przemocy są siły zbrojne i to one mogą być używane (wykorzystywane) w sposób bezpośredni lub pośredni.

Granica między bezpośrednim a pośrednim użyciem sił zbrojnych nie jest zbyt wyraźna i trudno ją (szczególnie obecnie) wyznaczyć.

Tradycyjne bezpośrednie użycie sił zbrojnych polegało na zaangażowaniu się w konflikt zbrojny. Najczęściej oznaczało to konieczność lub wysokie prawdopodobieństwo podjęcia walki zbrojnej. Dziś coraz częściej bezpośrednie użycie sił zbrojnych to podejmowanie misji, niekoniecznie wojennych.

Możliwości bezpośredniego użycia sił zbrojnych nie wyczerpuje dziś ani obrona militarna, ani agresja zdefiniowana w rezolucji Zgromadzenia Ogólnego ONZ (XII 1974), w której wymienia się takie formy, jak: inwazja, atak zbrojny, okupacja, bombardowanie terytorium innego państwa lub użycie przeciwko niemu jakiejkolwiek broni, użycie sił zbrojnych znajdujących się na terytorium drugiego państwa w sposób sprzeczny z wzajemnym porozumieniem, wysyłanie przez państwo lub w jego imieniu zbrojnych grup dokonujących poważnych aktów zbrojnych przeciw innemu państwu. Listę tę należy współcześnie na pewno uzupełnić, rozszerzyć.

Form pośrednich użycia sił zbrojnych wymienia się w literaturze przedmiotu wiele: od obecności militarnej – po demonstracje zbrojne"[104].

Ponadto B. Balcerowicz dostrzega jeszcze inne zjawisko, które ogranicza skalę stosowania walki zbrojnej i prowadzenia wojny w stosunkach międzynaro-

[104] Tamże, s. 21–25.

dowych. Według niego „Bezpośrednie użycie siły zbrojnej (jako instrumentu polityki) jest dziś w praktyce politycznej państw zjawiskiem nieczęstym. Używa się jej aktywnie (a przynajmniej powinno używać się) jedynie wtedy, gdy wymaga tego w sposób oczywisty interes narodowy lub inaczej: gdy wymaga tego zagrożenie żywotnych interesów narodowych. Potrzebne przy tym jest swoiste moralne alibi, udzielone przez opinię międzynarodową, dostatecznie uzasadniające interwencję, a są nim racje prawne i moralne. W realiach ostatnich dziesięcioleci rolę arbitra udzielającego mandatu na określone działania najlepiej spełniały organizacje międzynarodowe o uznanym autorytecie, np. Organizacja Narodów Zjednoczonych.

Aktualnie klimat moralny w środowisku międzynarodowym wymaga, aby każda interwencja militarna wynikała z czegoś więcej niż tylko z interesu narodowego"[105].

Warto zauważyć, że ze względu na globalizację stosunków międzynarodowych wojna jest coraz trudniej akceptowana w krajach słabo rozwiniętych, a w krajach wysoko rozwiniętych nieakceptowana. Z punktu widzenia prawa międzynarodowego „w epoce współczesnej wojna przestała być także legalnym instrumentem realizowania celów polityki zagranicznej państw. W rezultacie, zapoczątkowanego jeszcze przed pierwszą wojną światową, rozwoju prawa przeciwwojennego, wojna agresywna (napastnicza) została całkowicie zdelegalizowana. Złożyły się na to przede wszystkim postanowienia Paktu Brianda-Kelloga z 1 sierpnia 1928 r. oraz Karty Narodów Zjednoczonych i Deklaracji zasad prawa międzynarodowego, uchwalonej przez Zgromadzenie Ogólne ONZ 24 października 1970 r. Zakaz stosowania siły lub groźby jej użycia został podniesiony do rangi jednej z podstawowych zasad stosunków między państwami uczestniczącymi w procesie KBWE, a następnie w Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE)"[106].

Również z punktu widzenia moralnego oraz racjonalnego wojna nie znajduje uzasadnienia, co dobitnie wyraził Umberto Eco. Argumentuje on, iż:

„Świat widzi obecnie wojnę oczyma innymi niż te, którymi dysponował na początku stulecia, i gdyby dziś ktoś wysławiał piękno wojny jako jednej higieny dla świata, trafiłby na karty nie historii literatury, lecz psychiatrii. [...]

Zastanawiając się nad warunkami, w jakich staje się ona możliwa, i dochodząc do wniosku, że nie sposób już prowadzić wojny, gdyż skutkiem istnienia społeczeństwa momentalnej informacji, szybkiej komunikacji i ciągłych migracji międzykontynentalnych (do czego dołącza się sama istota nowej techniki wojennej) wojna stała się niemożliwa i nieracjonalna. Wojna pozostaje w sprzeczności z racjami, w imię których się toczy.

Jaki w ubiegłych stuleciach bywał cel wojny? Prowadzono ją dla pokonania przeciwnika, w taki sposób, by wyciągnąć korzyści z jego przegranej oraz by nasze zamysły (określone działania zmierzające do określonego rezultatu) taktycznie bądź strategicznie zrealizować tak, żeby przeciwnik nie mógł urzeczywistnić swoich. Żeby to osiągnąć, należało rzucić do walki wszelkie możliwe siły, jakie mogli-

[105] Tamże, s. 26.

[106] *Bezpieczeństwo narodowe i międzynarodowe...* wyd. cyt., s. 13.

śmy mieć do dyspozycji. Ostatecznie gra toczyła się między nami a przeciwnikiem.[...]

Dopiero w naszym stuleciu zrodziło się pojęcie ‚wojny światowej', mogącej wciągnąć nawet społeczności tej historii, jak i ludy polinezyjskie. Wraz z odkryciem energii atomowej, wraz z telewizją, transportem powietrznym i powstaniem rozlicznych form wielonarodowego kapitalizmu ujawniły się warunki niemożliwości wojny. [...] Z tych wszystkich i innych powodów wojna obecna, w odróżnieniu od dawnych, nie jest już podobna do inteligentnego systemu ‚szeregowego' lecz do takiegoż systemu ‚równoległego'. Inteligentny system szeregowy, stosowany np. do budowania maszyn tłumaczących bądź wyciągających wnioski z określonych danych informacyjnych, zostaje tak zaprogramowany, żeby mógł – opierając się na skończonej liczbie reguł – podejmować kolejne decyzje, z których każda zależy od decyzji poprzedniej. Działa on według schematu drzewa, drogą następujących po sobie rozwiązań binarnych. Dawna strategia wojenna kierowała się taką właśnie metodą: jeśli wróg przesunął swe oddziały na wschód, muszę przewidzieć, że następnie skieruje, postępując wedle tej samej logiki, ja rzucę moje wojska w kierunku północno-wschodnim, żeby niespodziewanie odciąć mu drogę. Reguły wroga były również naszymi regułami i każdy mógł podejmować decyzję kolejno, jak w partii szachów.

Natomiast w systemie równoległym każda komórka sieci wyposażona jest w zdolność decydowania, jaką zajmuje pozycję w końcowej konfiguracji stosowane do rozkładu obciążeń, których operator nie jest w stanie określić ani przewidzieć z góry, sieć bowiem wynajduje reguły, jakich wcześniej nie otrzymała, automodyfikuje się w celu znalezienia rozwiązania i nie zna rozróżnienia między regułami a danymi [...].

Współczesna wojna niweczy wszelką ludzką inicjatywę, ba, że nawet jej pozorny cel (i pozorne zwycięstwo którejś ze stron) nie jest w stanie powstrzymać samoistnej już gry ważkich mas uwikłanych we własną sieć"[107].

Argumenty powyższe wzmacniają znaczenie działań militarnych innych niż walka zbrojna. Istnieje więc wyraźnie artykułowana przez środowisko naukowe potrzeba rozpatrzenia na nowo treści sztuki wojennej, nauk wojskowych oraz roli i znaczenia wojny i walki zbrojnej.

Ciekawą propozycję zgłosił Wojciech Łepkowski, twierdząc: „Cały czas dyskutujemy o sztuce wojennej. Nie negując istnienia takiej sztuki, pragnę jednak zwrócić uwagę, że jest to sztuka prowadzenia wojny, wojny będącej kontynuacją polityki, która jest domeną polityków i uprawianą przez polityków. Natomiast wojskowi uprawiają sztukę prowadzenia walki zbrojnej, będącej elementem wojny. Najważniejszym, ale elementem, którego nie można utożsamiać z wojną. A zatem wojskowi uprawiają **sztukę walki zbrojnej** albo **sztukę wojskową**, której nie można utożsamiać ze sztuką wojenną – prowadzenia wojny"[108].

---

[107] U. Eco, *Pięć pism moralnych*, tłum. I. Kania, Kraków 1999, s. 13–22.

[108] W. Łepkowski, *Nauka i sztuka wojenna*, [w:] *Sztuka wojenna*... wyd. cyt., s. 89.

Jest jednak grupa badaczy, którzy widzą potrzebę innego podejścia. Jeden z nich, B. Balcerowicz, prezentując wizję przyszłej sylwetki osobowej oficera, uznał, że „żołnierz w przyszłości ma myśleć i zachowywać się nie tylko według czysto militarnych praw i norm. Oficer ma być zdolny do myślenia w kategoriach politycznych i dyplomatycznych, co powinno być przedmiotem kształcenia i szkolenia"[109]. Skoro więc każdy oficer ma się tym zajmować, to tym bardziej nauki wojskowe.

Również M. Laszczyk oraz W. Miszalski w dyskusji nad dylematami współczesnej sztuki wojennej, uznali, iż:

„Coraz szerszy staje się też związek nauki wojennej z innymi dziedzinami nauki.

Izolacja naukowa obecnie nie jest do zaakceptowania. Rozczłonkowanie nauki wynikało nie tylko z uznania jej wieloaspektowości (co podkreśla jej podział na dziedziny, kierunki, dyscypliny), lecz było także wynikiem pewnego separatyzmu poznawczego, któremu nie mogła dość długo zapobiec właściwie nadal nieugruntowana inwencja badań interdyscyplinarnych.

Instytucjonalizacja form współpracy przedstawicieli poszczególnych dyscyplin jest nadal zjawiskiem rzadkim, podczas gdy separowanie – zjawiskiem powszechnym. Nie wiadomo, w imię jakiej sprawy próbuje się izolować również nauki wojskowe.

Współczesność wymaga, a ściślej wymusza, prowadzenie interdyscyplinarnych badań nad istotą konfliktów zbrojnych i sposobami ich rozwiązywania za pomocą wszystkich dostępnych środków, w tym militarnych. Siła (tu: siła militarna) jest po prostu narzędziem polityki, które może być wykorzystywane na różne sposoby (pośrednio lub bezpośrednio) i w każdym stanie (pokoju, kryzysu, wojny)"[110].

Również P. Sienkiewicz uznaje, iż „[...] naukom wojskowym daleko do stanu wyłączności w badaniach nad konfliktami i walką. Zbyt wiele w nich bowiem »sztuki wojennej« i pragmatyzmu wymuszanego przez praktykę i potrzeby typu szkoleniowego (training) niż edukacyjnego (education). Być może na tym polega ich swoistość, z czym trudno się pogodzić. Ale być może czas na podjęcie dyskusji nad ich tożsamością, swoistością relacji, w jakich niewątpliwie pozostają z innymi, »cywilnymi«, naukami (dyscyplinami). Im wcześniej zostanie taka dyskusja podjęta, tym lepiej, bowiem z konfrontacją mamy już do czynienia"[111].

Nauki wojskowe powinny przestać się koncentrować jedynie na inżynierii prowadzenia wojny czy nawet walki zbrojnej. Wojna i walka zbrojna, mimo swej obecności w historii, występują jednak sporadycznie; **natomiast siła militarna jest trwałym zjawiskiem stale obecnym w polityce i stosunkach międzynarodowych zarówno w czasie konfliktów, jak i pokoju**. Rozumienie roli siły militarnej w polityce i stosunkach międzynarodowych oraz zachodzących między ty-

[109] B. Balcerowicz, *Sojusz a obrona*... s. 38.

[110] M. Laszczyk, W. Miszalski, s. 200.

[111] P. Sienkiewicz, *Wojna i walka zbrojna a współczesne teorie konfliktów*, [w:] *Sztuka wojenna*... s. 117.

mi elementami relacji jest niezwykle ważne na Zachodzie. Nasze nauki wojskowe, a szczególnie sztuka wojenna, koncentrują się jedynie na inżynierii przygotowania i prowadzenia walki zbrojnej, abstrahując od wspomnianych relacji. Ponadto, zakładając pewne uproszczenie, można uznać, iż sztuka wojenna w naszej rzeczywistości zajmuje się inżynierią walki zbrojnej w warunkach poligonowych. Tymczasem walka zbrojna zawsze toczy się w określonej rzeczywistości politycznej i warunkach międzynarodowych. Rzeczywistość ta jest ciągle obecna i stanowi jeden z najważniejszych czynników wpływających na decyzje dowódców nie tylko na poziomach strategicznych i operacyjnych, lecz także taktycznym. Działanie nawet drużyny piechoty może mieć konsekwencje strategiczno-polityczne i odwrotnie – polityczne uwarunkowania wpływają na działania najmniejszych elementów siły militarnej. Nawet zachowanie pojedynczego żołnierza może wywoływać efekty polityczne. Prawdziwe jest to zwłaszcza w epoce przezroczystości wynikającej z powszechnej obecności mediów i trudności z ukryciem informacji. Żołnierz jest nie tylko wojownikiem, lecz także uczestnikiem procesu politycznego. Działa on w imieniu swojego narodu i dlatego powinien rozumieć procesy, w których uczestniczy, znać reguły toczącej się gry oraz swoje rzemiosło.

W przeszłości, w poprzednim systemie, wojsko było „oddanym niewolnikiem", który miał ślepo wykonywać otrzymywane instrukcje. W procesy decyzyjne angażowani byli jedynie nieliczni zaufani i wtajemniczeni. Tego typu organizacja mogła funkcjonować w warunkach systemu totalitarnego oraz w okresie wojen masowych epoki industrialnej. Nawet wówczas jednak inaczej funkcjonowali przedstawiciele dyplomacji, wywiadu, a nawet sił specjalnych. Musieli oni działać bardziej autonomicznie i samodzielnie, dlatego też troszczono się przede wszystkim o ich motywacje i włączano do kręgu elity. Tymczasem w warunkach demokracji i powszechnego dostępu do informacji oraz w środowisku wymuszającym szybkie działania manewrowe w rozproszeniu, znajomość reguł gry i rozumienie zachodzących procesów mają niezwykle ważne znaczenie.

Współczesny żołnierz nie tylko prowadzi walkę zbrojną, lecz również uczestniczy w procesie kształtowania opinii publicznej. Ustanawianie rzeczników prasowych jest rozwiązaniem doraźnym i przejściowym. Rzecznicy mogą w przyszłości istnieć jako instytucjonalny kanał informowania, lecz tak jak odmowa udzielenia pomocy, tak odmowa udzielenia wywiadu będzie naganna. Nie musi to oznaczać anarchii – pod warunkiem uzyskania wysokiej świadomości uczestników zachodzącego procesu. Tak jak rzecznicy panują nad swoimi wypowiedziami, tak każdy żołnierz w przyszłości musi posiąść tę zdolność.

Kolejną sprawą jest reglamentacja przemocy. Tworzy to bardzo często konfliktowe, w stosunku do zasad sztuki wojennej, warunki. Zjawisko to było bardzo wyraźnie widoczne w czasie operacji „Sojusznicza Siła" skierowanej przeciw Serbii. Ograniczenia nakładane przez polityków radykalnie zmniejszały efektywność działań militarnych, wydłużały czas ich trwania, a nawet zakłócały wykonywanie poszczególnych zadań bojowych.

„[...] W początkowym okresie kampanii warunki pogodowe, ograniczona ilość sprzętu wydzielonego do działań i polityczne ograniczenia w zakresie wyboru obiektów uderzeń miały większy wpływ na kształt faz kampanii niż jakikolwiek plan strategiczny. [...]

Działania powietrzne prowadzone były w warunkach znacznych ograniczeń politycznych i ciągłej interwencji polityków w realizowane zadania. Odnosiło się to zarówno do wyznaczania obiektów uderzeń, jak i do działania. Niektóre kraje europejskie ciągle wetowały próby poszerzania listy obiektów ataku, a nawet ingerowały w wykonywanie pojedynczych zadań. [...]

W czasie działań kampanii Sojusznicza Siła dowódcy wojskowi mieli bardzo trudne warunki, borykając się ciągle z politycznymi aspektami tej kampanii. Każdy z dziewiętnastu członków Sojuszu chciał coś znaczyć i mieć coś do powiedzenia. Było to wielkim wyzwaniem dla dowódców. Należy jednak pamiętać, że z natury demokracji wynika konieczność politycznego i cywilnego nadzoru działań militarnych.

Zarówno w sferze politycznej, jak i militarnej NATO wyrażało brak woli i nie było przygotowane, aby od razu użyć takiego zgrupowania sił na początku działań, które spowodowałoby szybkie osiągnięcie zakładanych celów. Poprzez konieczność prowadzenia długich działań zwiększyła się liczba zabitych i wypędzonych w Kosowie. Występował brak zrozumienia asymetrycznej natury tej wojny. Nie próbowano w zdecydowany sposób użyć potęgi powietrznej tak, by wstrzymać czystki etniczne. Pozostawiono Serbom sanktuaria – miejsca bezpieczne oraz dosyć wolno zwiększano skalę zaangażowanych sił i działań. Umożliwiało to łatwiejsze akceptowanie strat. Zmasowane użycie większych sił przyniosłoby Serbom szybsze i trudniejsze do zaakceptowania straty, a tym samym przyspieszyłoby osiągnięcie celu"[112].

Reglamentowanie takie jest nie tylko domeną współczesnych konfliktów zbrojnych. Miało również miejsce w nieco mniejszym stopniu także w czasie drugiej wojny światowej. Jest ważny powód ku temu, że tak jest. Pisze o tym m.in. R. Aron:

„Zawarte w sformułowaniu Clausewitza podporządkowanie wojny polityce, jako środka służącego do osiągnięcia celu, tworzy podstawy i uzasadnia rozróżnienie pomiędzy wojną absolutną i wojnami rzeczywistymi. Tym bardziej należy obawiać się osiągnięcia przez wojnę skrajności i tym łatwiej prawdziwa wojna przybliża się ku wojnie absolutnej, im bardziej przemoc wymyka się spod kontroli przywódcy państwa. [...]

Jako teoretyk racjonalnego działania [Clausewitz – R.S.] przypomina tylko przywódcom czasu wojny i pokoju o zasadzie, którą i jedni, i drudzy powinni respektować: o prymacie polityki, o tym, że wojna jest tylko narzędziem na usługach celów wyznaczonych przez politykę, że jest ona tylko pewnym, chwilowym stanem, jakimś aspektem stosunków pomiędzy państwami, w ramach których każde

[112] R. Szpyra, *Polityczno-militarne i operacyjne aspekty kampanii „Sojusznicza Siła"*, [w:] *Allied Force – współczesny model kampanii powietrznej*, Warszawa 2001.

państwo musi być posłuszne zasadom polityki, a więc logice trwałych interesów danej zbiorowości"[113].

Reglamentowanie przemocy militarnej wynika także z podpisanych traktatów międzynarodowych oraz innych form porozumień, które tworzą prawo wojenne. To, że potęga militarna jest zawsze psem na smyczy, a często nawet i w kagańcu, znajduje swój wyraz m.in. w stałej obecności na Zachodzie tzw. *rules of engagement*, czyli reguł stosowania przemocy zarówno w procesie planowania, jak i w każdym planie działań militarnych wszystkich poziomów. Reguły te są dopasowywane do sytuacji i potrzeb, i doprowadzane do pojedynczego żołnierza, a ich przekroczenie grozi odpowiedzialnością karną. Stykali się z nimi w przeszłości po raz pierwszy polscy żołnierze wyjeżdżający na misje pokojowe ONZ. Są one jednak stałym atrybutem nie tylko operacji pokojowych, lecz i wszystkich innych prowadzonych przez państwa Zachodu.

Reglamentowanie to wynika także z doraźnych potrzeb politycznych, stopnia poparcia społecznego własnych działań, warunków sojuszu czy koalicji i wielu innych trudnych do zidentyfikowania powodów.

Kolejnym czynnikiem są warunki cywilizacyjne. Jak trafnie zauważył Alvin Toffler, „jak cywilizacja tworzy dobra, tak również prowadzi wojny"[114]: innymi słowy, jak organizuje produkcję dóbr i usługi, tak też i walkę zbrojną. Jedną z zasadniczych zmian oprócz technologicznych, są te, które zaszły we współczesnym przemyśle i usługach, i odnoszą się do sfery organizacyjnej. Po zmianach ustrojowych w Polsce największym problemem była nie tyle nowa technologia, ile nowy sposób zarządzania. Znamy przykłady, gdzie wprowadzenie nowego sposobu zarządzania postawiło zakłady na nogi. Wśród wielu aspektów nowej jakości zarządzania dostrzec można m.in. TQM (total quality management), którego istotą jest zarządzanie jakością, a także zarządzanie zasobami ludzkimi (HR) czy zarządzanie informacją. W ramach zarządzania jakością opracowano m.in. standardy jakości ISO, które można stosować w każdej organizacji, również w sferze militarnej. Podobnie jest z zarządzaniem zasobami ludzkimi i informacją.

Są to tylko przykłady ilustrujące rozległe i dynamiczne zmiany zachodzące w teorii organizacji i zarządzania. Militarna sfera cywilizacji, chcąc dopasowywać się do jej charakteru, musi podążać za jej zmianami, by nie znaleźć się na jej peryferiach. Jest to bardzo dobrze rozumiane na Zachodzie, gdzie w organizacjach wojskowych dużą wagę przywiązuje się do rozumienia istoty swojej organizacji, jej misji, procesów, w których uczestniczy. Przejawia się to m.in. w tym, że w procesie edukacji militarnej zakres przekazywanej wiedzy zdecydowanie się różni od naszych rozwiązań. Edukacja militarna zarówno na niższych poziomach (licencjackim), jak i na poziomie średnim (magisterskim) dotyczy przede wszystkim problematyki bezpieczeństwa narodowego, międzynarodowego oraz militarnego. Obejmuje także problematykę stosunków międzynarodowych oraz roli i miejsca

[113] R. Aron, *Pokój i wojna*... s. 40, 41.

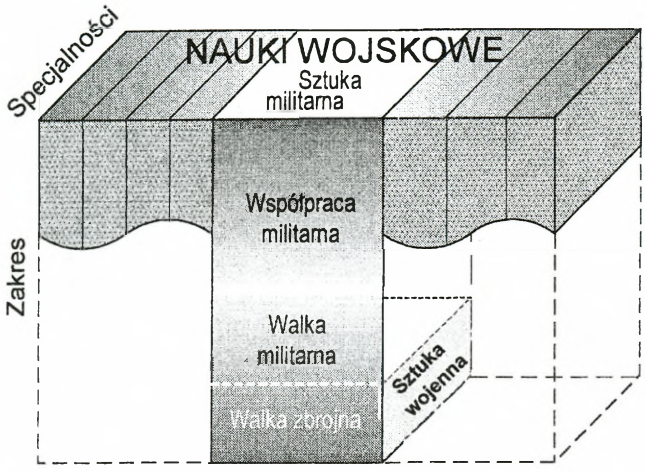
[114] A. Toffler, H. Toffler, *Wojna i antywojna. Jak przetrwać na progu XXI wieku*, Warszawa 1997, s. 82.

siły militarnej w kreowaniu tych stosunków oraz bezpieczeństwa. Organizowane są kursy dla młodej kadry oficerskiej o problematyce porównywalnej z kursami dla najwyższych dowódców. Kursy te w skondensowany sposób zapoznają wszystkich uczestników z procesami, w których ci w różnych miejscach będą uczestniczyć. Uczestnicy ci poznają procesy podejmowania decyzji i planowania od najwyższego poziomu strategicznego (polityczno-militarne, narodowe procesy decyzyjne), poprzez operacyjny (planowanie kampanii militarnych teatru działań wojennych), po taktyczny. Inżynierii wojowania, czyli swojego rzemiosła, uczą się głównie w procesie szkolenia. Podobnie jak w środowisku cywilnym według wymogów ISO, wymaga się, aby nawet najniżsi rangą pracownicy znali cel i misję swojej firmy, byli świadomi całości sytuacji, w jakiej ona działa i rozumiejąc ją, wykazywali maksimum swojej inicjatywy i innowacyjności dla wspierania jej wysiłków, tak i w środowisku militarnym niezbędne jest podobne podejście. Znajduje to wyraz we wspomnianym podejściu edukacyjnym.

Ponadto, mimo że decyzje o zastosowaniu przemocy militarnej podejmują politycy, to warianty decyzji, kryteria oceny oraz analiza skutków są przygotowywane przez środowisko militarne. Również z tego powodu środowisko to powinno mieć wiedzę nie tylko z obszaru rzemiosła.

W rezultacie spośród różnych nazw w odniesieniu do problematyki obejmującej stosowanie przemocy zbrojnej przez państwo najlepszą jest kategoria „militarny" i dlatego też taką przyjęto. Podstawowymi atrybutami kategorii „militarny" jest zdolność do stosowania przemocy zbrojnej, której istotą jest destrukcja.

Należy uznać, iż **cała sfera zastosowania potencjału militarnego w uprawianiu polityki międzynarodowej powinna być przedmiotem badań dyscypliny nauki zajmującej się tą sferą**. Granice między dyscyplinami naukowymi nie są ostre. Również i w tym wypadku istnieją obszary związane ze stosowaniem siły militarnej, którymi zajmują się inne dyscypliny naukowe, jednakże nauki wojskowe powinny wyróżniać się swoistym podejściem do badań. Taką dyscypliną powinny być nauki militarne (*military science*). Uwzględniając jednak trudności z wprowadzeniem zmiany nazwy dyscypliny nauki, można pozostawić dotychczasową – „nauki wojskowe". **Nauki wojskowe powinny jednakże poszerzyć zakres swoich zainteresowań o obszary walki militarnej nie będące wojną i tradycyjnie rozumianą walką zbrojną, a także o obszar współpracy militarnej państw.** Wobec oporu środowiska na znaczne rozszerzanie zakresu sztuki wojennej, a także wyraźnego związku nazwy „wojenna" z wojną, **celowe byłoby utworzenie na gruncie nauk wojskowych dziedziny wiedzy i umiejętności dotyczących form i sposobów stosowania potencjału militarnego w kooperacji pozytywnej i negatywnej państw. Mogłaby to być np. *sztuka militarna*. Częścią *sztuki militarnej* powinna być tradycyjnie pojmowana *sztuka wojenna*** (rys. 2).



Opracowanie własne.

Rys. 2. Relacje między naukami wojskowymi, sztuką wojskową i sztuką wojenną

Szeroko rozumiana aktywność militarna, obejmująca zarówno współpracę, jak i walkę, to *operacje militarne*. Operacje te dekomponują się na militarną współpracę i walkę. Aktywność militarna może przybierać formy współpracy i walki.

1.4. Działania międzynarodowe państwa

Jedną z podstawowych funkcji państwa jako formy organizacji grupy społecznej jest zabezpieczenie interesów tej grupy. Interes to „pożytek, korzyść, zysk; rzecz opłacalna"[115] (rys. 3). Jednocześnie próbuje się szukać innych, równoległych do interesów lub uzupełniających kategorii. Warto przytoczyć tu chociażby stanowisko Cezarego Rutkowskiego, który dostrzega znaczenie kategorii „interesy"[116], jednakże prezentuje ją jako jedną z trzech uzupełniających się.

[115] *Słownik języka polskiego*, t. 1, PWN, Warszawa 1981, s. 799.

[116] Twierdzi nawet, że „Jakiekolwiek byłyby cele ostateczne, interes jest zawsze celem bezpośrednim", C. Rutkowski, *Prakseologiczne aspekty strategii wojskowej*, rozprawa habilitacyjna, Warszawa 1998, s. 66.



Źródło: C. Rutkowski, *Prakseologiczne aspekty strategii wojskowej*. Rozprawa habilitacyjna, Warszawa 1998, s. 66.

Rys. 3. Byt, jakość bytu i interes – pierwotne motywy działania

Tymczasem wszystkie kategorie typu „byt, jakość bytu", a także „bezpieczeństwo", „rozwój" stanowią pożytek, korzyść dla danej grupy społecznej. Oznacza to, że zawierają się w kategorii „interesy", co obrazuje rys. 4.



Opracowanie własne.

Rys. 4. Interesy, pierwotne motywy działania i ich wzajemne relacje

Stosunki międzynarodowe zajmujące się relacjami między państwami, zrodziły różne szkoły myślenia o nich. Jednak w dalszym ciągu największy wpływ zarówno na refleksję teoretyczną, jak i na praktykę wywiera realistyczna szkoła myślenia, szczególnie klarownie wyłożona przez Hansa Morgenthaua w dziele *Politics Among Nations* opublikowanym w 1948 r. Sercem realistycznej teorii stosunków międzynarodowych jest **koncepcja interesów**. Polityka definiowana jest tu jako zmaganie się (walka) o potęgę i władzę. **Działanie to jest częścią ludzkiej natury i w społeczeństwie przybiera formy zależne od rywalizacji lub zależności interesów. Współpraca występuje, gdy pojawia się zbieżność interesów. Rywalizacja, współzawodnictwo oraz konflikt wynikają ze sprzeczności interesów**[117].

[117] *Encyclopaedia Britannica*, http://www.britannica.com/bcom/eb/article/2/0,5716,117542+2+109549,00.html.

Grupą społeczną tworzącą państwo jest naród[118], wobec czego istnieje interes narodowy. Kategorię tę, cytując inne źródła, definiuje *Słownik terminów z zakresu bezpieczeństwa narodowego* jako „zespół ogólnych i stałych celów, na rzecz których działa naród" oraz „ogólne, długookresowe i kontynuowane cele funkcjonalne w stosunku do celu ostatecznego, któremu służy państwo, naród i władza". Autorzy tego słownika podają także własną definicję interesu narodowego, traktując go jako „zespół wartości, na rzecz których działa dany naród"[119]. W odniesieniu do działania interesy stanowią więc cele tego działania.

Jedną z podstawowych kategorii nauk politycznych jest „polityka", którą definiuje się jako „działalność władzy państwowej, rządu w dziedzinach społecznej, gospodarczej, kulturalnej, wojskowej i innych, dotyczącą spraw wewnętrznych państwa lub stosunków z innymi krajami [...]"[120]; w innym zaś ujęciu jako: „sferę wzajemnych stosunków i oddziaływań pozytywnych, negatywnych i kompromisowych pomiędzy państwem a innymi organizacjami (włączając w to państwa w przypadku polityki międzynarodowej), dotyczących celów środków działalności państwa, a także charakteru władzy państwowej"[121].

Z punktu widzenia prakseologicznego oraz w ujęciu czynnościowym, wymiarem polityki są **działania państwa** rozumiane jako zorganizowana aktywność prowadząca do osiągnięcia określonych celów politycznych. Działania państwa zmierzające do osiągnięcia celów politycznych prowadzą do zaspokojenia interesów zorganizowanej w państwo ludności. Działania te dotyczą wszelkich obszarów i form aktywności państwa.

Niewątpliwie chodzi tu o celowe działanie zorganizowane, warto więc sięgnąć do dorobku prakseologii, która działania tego typu dzieli na kooperację pozytywną (współpracę) i kooperację negatywną (walkę). Rys. 5.

Według teorii czynu skutecznego działanie zorganizowane może przybierać formę kooperacji pozytywnej, czyli współpracy lub kooperacji negatywnej, czyli walki. Jest to zbieżne z poglądami realistów w stosunkach międzynarodowych, jednakże ci nie kładą akcentu na binarność, to jest wyróżnianie albo stanu współdziałania, albo walki, lecz dostrzegają spektrum działań rozkładających się od współpracy, poprzez rywalizację i współzawodnictwo, do konfliktu. Jednocześnie biorąc pod uwagę mnogość interesów, jakie występują w odniesieniu do każdego państwa, nieczęstym zjawiskiem jest występowanie albo wyłącznie zbieżności, albo tylko sprzeczności. Dlatego też najczęściej jednocześnie występują zarówno zbieżności, jak i sprzeczności interesów, a działania państw w relacjach z innymi państwami zawierają zarówno elementy współdziałania, jak i walki (rys. 6).

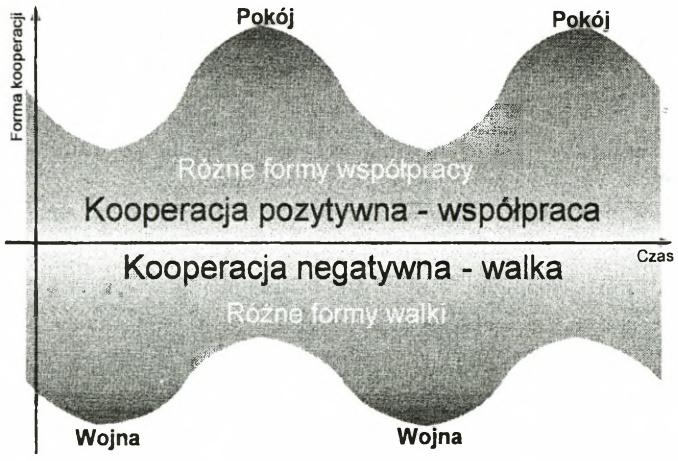
---

[118] Węższe rozumienie narodu jako grupy społecznej tworzącej państwo.
[119] *Słownik terminów...* s. 49.
[120] *Słownik języka polskiego*, t. 2, PWN, Warszawa 1979, s. 785.
[121] *Słownik terminów...* s. 97–98.



Źródło: B.M. Szulc, *Dylematy epistemologiczne i metodologiczne teorii sztuki wojennej*, [w:] *Sztuka wojenna. Konteksty teoretyczne i praktyczne*, red. M. Krauze, B.M. Szulc, Toruń 2000, s. 46.

Rys. 5. Formy kooperacji



Opracowanie własne.

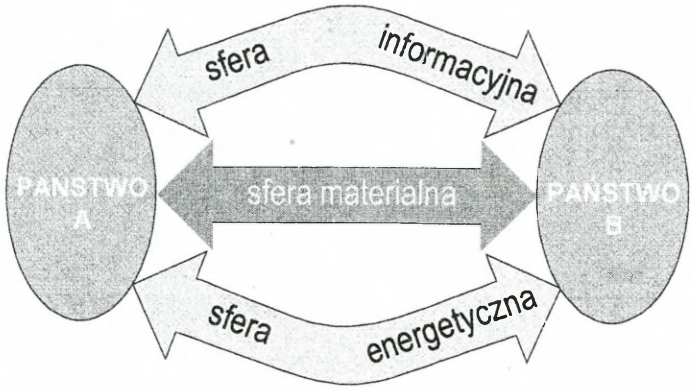
Rys. 6. Spektrum aktywności państwa na arenie międzynarodowej

Istotą aktywności państwa na arenie międzynarodowej jest jednoczesne prowadzenie różnorodnych działań, obejmujących zarówno formy kooperacji pozytywnej, jak i negatywnej. W zależności od aktualnego stanu relacji zachodzących między interesami państw, w aktywności tej dominować mogą bądź formy

kooperacji pozytywnej, bądź negatywnej. Jak uważa R. Aron, „stosunki pomiędzy państwami są czymś stałym, dyplomacja zaś i wojna to tylko dwie, wzajem się uzupełniające ich odmiany – z których raz jedna, raz druga przeważa, lecz nigdy żadna z nich nie ustępuje całkowicie na korzyść drugiej, poza skrajnymi przypadkami absolutnej wrogości, całkowitej przyjaźni lub zawiązania federacji"[122].

Ponadto argumentuje, iż „w czasach pokoju polityka posługuje się środkami dyplomatycznymi, nie wykluczając możliwości odwołania się do sił zbrojnych, a przynajmniej zagrożenia ich użyciem. W czasach wojny polityka nie rezygnuje z działalności dyplomatycznej, gdyż dyplomacja nadal utrzymuje stosunki z sojusznikami i państwami neutralnymi, a także – w sposób ukryty – podejmuje działania w stosunku do nieprzyjaciela, raz grożąc mu całkowitym zniszczeniem, raz otwierając przed nim perspektywę zawarcia pokoju"[123].

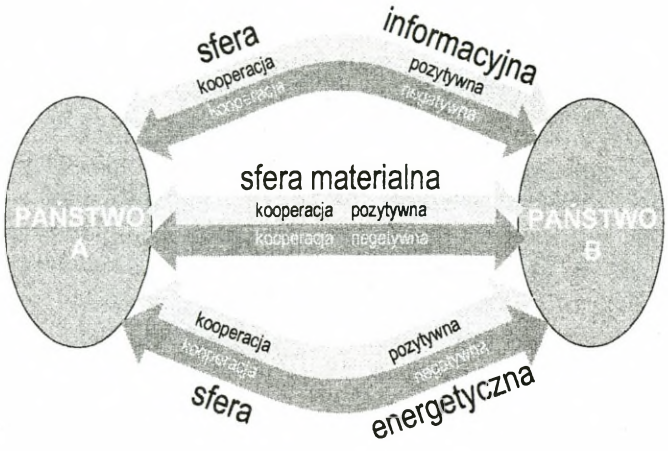
Relacje między państwami ulokowane są w jakichś sferach. W zależności od przyjętych kryteriów, można identyfikować różne sfery. Identyfikując najbardziej ogólne, warto zastanowić się nad składnikami bytu. Przy okazji rozważań nad istotą informacji, Norbert Wiener słusznie zauważył, że **„podstawowymi kategoriami bytu są materia, energia i informacja"**[124]. **Kategoriom tym odpowiadają więc właściwe im sfery oddziaływań materialnych, energetycznych i informacyjnych** (rys. 7). Z punktu widzenia społecznego, gdy oddziaływania zawarte w tych sferach są rezultatem celowej ludzkiej aktywności – a takie są przedmiotem naszych rozważań – **mogą, zgodnie z prakseologią, przybierać formy kooperacji pozytywnej (współpracy) i negatywnej (walki)** (rys. 8).



Opracowanie własne.

Rys. 7. Sfery oddziaływań państwa w relacjach z innymi podmiotami

[122] R. Aron, *Pokój i wojna*... s. 61.
[123] Tamże, s. 41.
[124] Cyt. za: M. Mazur, *Jakościowa teoria*... s. 19.



Opracowanie własne.

Rys. 8. Pozytywne i negatywne formy sfer oddziaływań

Państwo, jako organizacja społeczna, charakteryzuje się aktywnością wewnętrzną i zewnętrzną, gdyż „każde państwo realizuje funkcję zewnętrzną i wewnętrzną" i „koncentruje swoją aktywność wokół zarządzania"[125]. **Zachodzące w państwie i jego poszczególnych komponentach procesy, wymagają zasilania materialnego, energetycznego oraz informacyjnego** (rys. 9). W związku z zachodzącymi rewolucyjnymi zmianami cywilizacyjnymi następuje „zmiana ZNACZENIA informacji"[126]. Zmiana ta ma charakter silnego wzrostu tego znaczenia. Sfera materialna i sfera energetyczna oddziaływań zewnętrznych nie budzą wątpliwości. Rodzić się może pytanie o to, jaki charakter może mieć informacyjna sfera oddziaływań państwa, jeżeli może ona mieć formę kooperacji pozytywnej lub negatywnej?

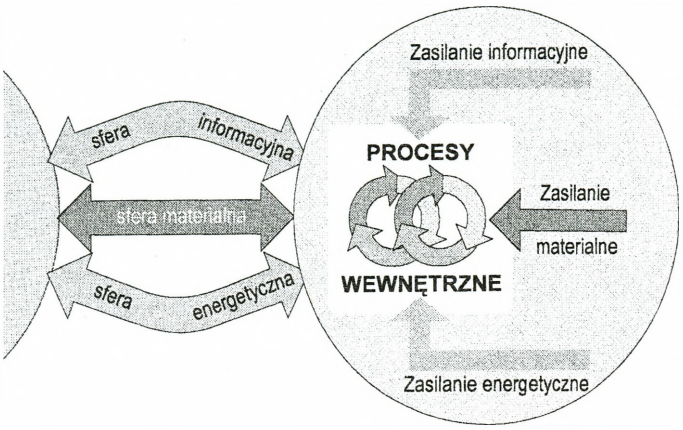
Państwo, działając w otoczeniu zewnętrznym, stanowiącym warunki zewnętrzne jego działania oraz, w określonych uwarunkowaniach wewnętrznych, dąży do osiągania celów grupy społecznej tworzącej to państwo. Generowanie celów i woli ich osiągania oraz skali akceptowalnych kosztów, jakie należy ponieść dla osiągania tych celów w systemach demokratycznych, należy do narodu[127]. W systemach totalitarnych bywają one określane przez sprawujące władzę reżimy. Zarówno w systemach totalitarnych, jak i demokratycznych bieżące i bezpośrednie określanie tych treści spoczywa na władzy danego kraju. To władze kraju określają cele działań państwa na forum zewnętrznym i wewnętrznym. Władze te wyrażają także wolę i maksymalne koszty osiągania określonych celów.

---

[125] K.A. Wojtaszczyk, s. 12, 22.

[126] P.F. Drucker, *Zarządzanie w XXI wieku*, Warszawa 2000, s. 99.

[127] Przyjmując, że „[...] za naród uważa się dowolną, terytorialnie zorganizowaną, zbiorowość polityczną", R. Aron, *Pokój i wojna*... s. 16.



Opracowanie własne.

Rys. 9. Zewnętrzne sfery oddziaływań oraz sfery zasilania procesów wewnętrznych

Ze względu na charakter ustroju politycznego państwa, stanowisko jego władz może być tożsame ze stanowiskiem narodu lub też rozbieżne. Jednak nawet, gdy ta rozbieżność jest znaczna, to ze względu na przyjęty sposób organizacji społeczeństw, władza danego państwa posiada bezpośrednie uprawnienia w tym zakresie.

Szczególnie interesujące jest funkcjonowanie państw w środowisku zewnętrznym, jako że w istocie na arenie międzynarodowej panuje anarchia. Pomimo pewnych namiastek nie istnieją władze świata. Nie ma parlamentu światowego stanowiącego prawo, nie istnieje rząd światowy z aparatem egzekucji prawa, nie istnieje też światowa władza sądownicza. Nawet jeżeli uznamy, że jest to uproszczenie, to i tak nie zmienia to faktu, iż o interesy poszczególnych państw muszą się troszczyć przede wszystkim one same.

Państwa mogą więc znaleźć się w sytuacji, gdy formułowane przez nie cele są całkowicie lub częściowo zbieżne z celami innych państw lub też całkowicie bądź częściowo sprzeczne. W sytuacji zgodności następuje kooperacja pozytywna, w sytuacji zaś sprzeczności – negatywna. Występować może zarówno współdziałanie, jak i walka. W sytuacji gdy podmiotem formułującym cele działania, wolę oraz dopuszczalne koszty ich osiągania są władze kraju, również przedmiotem zarówno współdziałania, jak i walki powinny być przede wszystkim te władze.

Przed epoką państw narodowych zarówno współdziałanie, jak i walka mogły mieć charakter tak bezpośredni, jak i pośredni. Ówcześni władcy spotykali się i uzgadniali swoje cele i działania, i bezpośrednio uczestniczyli w walkach zbrojnych. Praktykowano również ich pośrednie uczestnictwo, przez kierowanie swoimi wojskami. W tym okresie możliwe więc było zarówno bezpośrednie, fizyczne, jak i pośrednie oddziaływanie na władzę.

Jednakże w praktyce z chwilą uformowania się państw narodowych w XIX w., jako główną formę wpływania na władze innego państwa przyjęto oddziaływanie pośrednie. Uznano, iż wszelkie formy przemocy są dopuszczalne, włącznie z walką zbrojną. Władze państw w dalszym ciągu mogą prowadzić zarówno współdziałanie, jak i walkę. Zrezygnowano jednak z bezpośredniego uczestnictwa władz w walce zbrojnej. Nie jest też akceptowane na forum międzynarodowym zabijanie przywódców państw i rządów. Sytuacja ta bardzo upodobniła się do gry w szachy, gdzie na przeciwnika oddziałuje się za pośrednictwem jego pionków. Nawet wielkie wojny toczą się o to, by pożądany przez władze jednego państwa stan rzeczy zaakceptowały władze państwa przeciwnika. Najczęściej oznacza to, że decyzje władz akceptuje naród. Zdarzają się jednak sytuacje, gdy istnieją odmienne stanowiska władz i narodu. Z tego wynika, że głównym przedmiotem jakiejkolwiek akcji pozytywnej lub negatywnej w stosunkach międzynarodowych jest w istocie władza, a pośrednio rządzony przez nią naród. Zdarza się też sytuacja, gdy naród jest negatywnie nastawiony do swojej władzy i może wspierać działanie aktora zewnętrznego. Trudniejszą sytuacją jest ta, w której władza jest uległa w stosunku do zewnętrznych żądań, a naród tego nie akceptuje. Wówczas należy prowadzić walkę z narodem. Zawsze jednak znajduje się jakiś nowy przywódca akceptowany przez naród i sytuacja staje się typowa. Jej istotą jest to, że **bezpośrednim przedmiotem oddziaływania na arenie międzynarodowej są władze innych państw, a podstawową formą tego oddziaływania jest pośrednie stymulowanie pożądanych działań. Władze nie doświadczają więc fizycznego oddziaływania na siebie, a główna forma tego oddziaływania ma charakter informacyjny**.

Można się tu posłużyć skrajnymi przykładami, w których tyran, skupiający całość władzy, taki jak Hitler, Stalin czy współcześnie Saddam Hussein, pozostaje w ukryciu, mając kontakt ze światem zewnętrznym jedynie za pomocą informacji. Również przedstawiciele demokratycznej władzy współczesnego państwa nawet w czasie pokoju pozostają w pewnym stopniu izolacji, związanej z ochroną przed terroryzmem oraz natarczywością społeczeństwa. Można spotkać opinie o wyalienowaniu władzy od społeczeństwa. Władza kontaktuje się ze światem zewnętrznym głównie za pomocą informacji, dostarczanych jej przez system zasilania władzy w informację.

Jeśli władze jakiegoś państwa stwierdzają, że władze innego państwa mają sprzeczne cele działania, to mogą podejmować różne formy aktywności, w których efekcie generowana będzie informacja o korzyściach, kosztach lub ubezwłasnowolnieniu (paraliżu). O ile informacje o korzyściach i kosztach stymulują określone działania, o tyle informacja o paraliżu oznacza brak możliwości działania niezbędnego dla osiągnięcia pożądanego celu.

Informacje te mogą wywodzić się z różnych obszarów aktywności państwa, ale mogą też dotyczyć spraw osobistych rządzących. Jednym z obszarów kreowania zarówno korzyści, jak i kosztów jest obszar ekonomiczny. Na tym polu można kreować oprócz korzyści również grupę kosztów. Mogą one być bardzo dotkliwe dla państwa. Jednakże obszar najbardziej dotkliwych kosztów w ich spektrum

przynależy sferze militarnej. Destrukcja ekonomiczna nie bywa tak dotkliwa, jak destrukcja fizyczna infrastruktury państwa, wraz z zabijaniem jego przedstawicieli. Koszty te są więc bardzo wysokie. Informacje o kosztach, jakie przynosiły kolejne dni operacji „Sojusznicza Siła", były dla Miloszevicia bardziej negatywne, aniżeli wcześniejsze informacje o kosztach kolejnych dni sankcji ekonomicznych. Ze względu na złożony charakter systemu przetwarzania informacji można nie tylko stymulować umysły przedstawicieli władzy prawdziwymi informacjami, lecz także fałszywymi, maskując ich fałszywość. Jest to szczególnie istotne w dobie współczesnych osiągnięć w zakresie zarówno przetwarzania informacji, jak i kreowania rzeczywistości wirtualnej.

Nie mniej ważną sprawą od informacyjnego oddziaływania na umysły członków władzy państwa przeciwnika oraz narodu tego państwa jest zapewnienie sobie poparcia dla planowanych działań ze strony własnego narodu. Ma to szczególne znaczenie w warunkach umiejętnie prowadzonego ataku informacyjnego na społeczeństwo przez przeciwnika. Skutkiem takiego ataku może być niepowodzenie kampanii militarnej lub nawet wycofanie poparcia narodu na jej prowadzenie. W systemach demokratycznych może to skutkować polityczną rezygnacją z prowadzonych działań, jak stało się w przypadku amerykańskiej operacji pokojowej w Somalii. Stymulowanie informacyjne może mieć także charakter sterowania emocjami, zmniejszającego racjonalność podejmowanych decyzji.

Jak z tego wynika, **w warunkach współczesnego świata ostateczną formą każdej akcji w stosunku do innego państwa jest informacja docierająca do świadomości sprawujących władzę**. Wobec praktycznej rezygnacji cywilizowanego świata z fizycznego oddziaływania na sprawujących władzę, jedyną dostępną formą bezpośredniego ataku na nią jest informacja. O ile w przeszłości celem wygenerowania określonych porcji informacji docierających do umysłów rządzących niezbędne było przeprowadzenie określonych działań fizycznych, o tyle obecnie staje się coraz bardziej możliwe generowanie podobnych informacji bez podejmowania owych działań fizycznych. Przez to **informacja stawać się będzie w przyszłości głównym narzędziem stymulacji, a jednocześnie podstawową bronią przyszłej walki między państwami. Jednocześnie informacja w dalszym ciągu spełniać będzie swoje dotychczasowe funkcje zabezpieczania każdej formy działalności ludzkiej**.

W konkluzji należy uznać, że:

- **Państwo prowadzi działania, których celem jest zabezpieczenie interesów jego obywateli.**
- **Działania państwa w stosunku do podmiotów sceny międzynarodowej mogą przybierać formę współpracy i walki. Najczęściej obie formy tych działań występują jednocześnie.**
- **Relacje między państwami, identyfikowane według składników bytu, zachodzą w trzech sferach: materialnej, energetycznej i informacyjnej. Relacje te mogą przybierać formy współpracy i walki** (zob. rys. 8).

- **Oprócz oddziaływań zewnętrznych, niezbędne jest zabezpieczenie zasilania procesów wewnętrznych. Zasilanie to realizowane jest również w sferach: materialnej, energetycznej i informacyjnej** (zob. rys. 9).
- **W relacjach z innymi państwami bezpośrednim przedmiotem oddziaływania są władze innych państw, a podstawową formą tego oddziaływania jest pośrednie, informacyjne stymulowanie pożądanych działań i postaw.**
- **Efektem pośredniego oddziaływania na władze przeciwnika jest informacja o korzyściach, kosztach lub paraliżu.**
- **Informacja staje się głównym narzędziem stymulacji oraz podstawową bronią w walce między państwami. Informacja w dalszym ciągu pozostanie też jedną z najważniejszych form zasilania aktywności wewnętrznej państwa.**

1.5. Operacje militarne państwa

Mimo różnic w poglądach poszczególnych badaczy **istnieje powszechna akceptacja tezy o tym, że militarny komponent organizacji państwa jest jednym z głównych instrumentów jego polityki**. Warto więc poznać istotę tego instrumentu i jego rolę w aktywności państwa.

Narzędziem polityki w stosunkach międzynarodowych jest możliwy do wykorzystania szeroko rozumiany potencjał państwa. Cytowany już R. Aron potencjał ten nazywa potęgą, przy czym nie jest on autorem tego pojęcia, lecz zapożycza je od realistów, dla których stopień zabezpieczenia interesów jest funkcją wielkości potęgi państwa, stąd dążenie do zwiększania potęgi państwa jest przedmiotem stałych zabiegów państw. Polityka tego typu jest nazywana w języku angielskim *power politics*, w niemieckim *Macht Politik*, we francuskim *politique de puissance*.

W najogólniejszym rozumieniu Arona, „potęga jest zdolnością czynienia, tworzenia lub niszczenia. Potęga środka wybuchowego jest wymierna, podobnie jak moc wiatru, przypływu morskiego i trzęsienia ziemi. Potęga jakiejś osoby lub jakiejś zbiorowości nie może zostać dokładnie zmierzona, już choćby ze względu na mnogość celów, jakie może sobie ona wyznaczać i środków, jakimi się posługuje. To, że ludzie używają swojej potęgi przede wszystkim w stosunku do swoich bliźnich, powoduje, że właśnie w polityce pojęcie to odnajduje swoje autentyczne znaczenie. Potęga jakiejś osoby jest zdolnością czynienia, lecz przede wszystkim wywierania wpływu na postępowanie lub uczucia innych osób. Potęgą na scenie międzynarodowej nazywam zdolność jakiejś jednostki politycznej do narzucenia swej woli innym jednostkom politycznym”[128]. Również B. Balcerowicz, przyjmując podejście „realistyczne” i „neorealistyczne”, uznaje, iż głównym motywem sprawczym działania państw na arenie międzynarodowej jest potęga[129].

[128] R. Aron, *Pokój i wojna...* s. 69.
[129] Zob. B. Balcerowicz, *Sojusz a obrona...* s. 17.

Potencjał państwa, nadający mu zdolność do osiągania pożądanych rezultatów, składa się z komponentów odzwierciedlających sfery aktywności państwa, identyfikowane według rodzaju tych komponentów. Najważniejsze sfery to: dyplomatyczna, militarna i ekonomiczna; ostatnio znaczenia nabiera także kulturowa. Komponent militarny, będący przedmiotem zainteresowania naszych rozważań, jest więc militarną częścią potęgi państwa i stanowi potęgę militarną. Ponieważ, jak już ustalono, głównym atrybutem militarności jest zdolność do destrukcji, za **potęgę militarną uznać należy potencjał destrukcyjny państwa zdolny do trwałego lub okresowego niszczenia elementów organizacji innego państwa**.

Potęga militarna jest stałym składnikiem potęgi państwa i już sama jej obecność stanowi instrument polityki. Poszczególnym składnikom potęgi państwa odpowiadają charakterystyczne dla nich formy stosowania. Istnieją więc militarne i niemilitarne formy stosowania potęgi państwa na arenie międzynarodowej. Nazywane są one także instrumentami potęgi państwa[130]. Ponadto, oprócz form czysto militarnych oraz czysto niemilitarnych, właściwych cywilnym komponentom potęgi państwa, rozróżnia się również mieszane formy stosowania potęgi militarnej. Autorzy *Strategic Assessment 1996. Instrument of U.S. Power* wyróżniają trzy grupy instrumentów[131] stanowiących formy stosowania wszystkich komponentów potęgi państwa. Są to niemilitarne, polityczno-militarne i militarne instrumenty prowadzenia polityki (tabele 1–3).

Z analizy tych tabel wynika, że trudno wyznaczyć precyzyjną granicę między cywilnymi i militarnymi formami stosowania potęgi państwa; podobnie trudno wyznaczyć taką granicę między komponentami potęgi państwa. Istnieje obszar przejściowy, który jest konglomeratem form militarnych i cywilnych. Wiele form cywilnych potęgi państwa wymaga współistnienia form militarnych. Na przykład: ambasady wymagają ochrony, handel zagraniczny potrzebuje swobody żeglugi, którą zapewnia komponent militarny, pomoc humanitarna w rejonach zagrożonych potrzebuje wsparcia komponentu militarnego, sankcje ekonomiczne również wymagają militarnego wsparcia aparatu ich egzekwowania. Także B. Balcerowicz jest przekonany, że „[...] siła militarna jest oczywiście do dziś narzędziem polityki, ale – jak wyraźnie można zaobserwować – **narzędziem jednym z wielu**, a ponadto narzędzie owo może być wykorzystywane na różne sposoby (pośrednio lub bezpośrednio), w stanie pokoju, kryzysu, wojny"[132].

---

[130] *Strategic Assessment 1996. Instrument of U.S. Power*, Washington D.C. 1996, s. ix.
[131] Tamże.
[132] B. Balcerowicz, *Sojusz a obrona...* s. 20.

Tabela 1. Instrumenty niemilitarne potęgi państwa

Grupa	Nazwa komponentu	Formy użycia
Instrumenty niemilitarne	Dyplomacja	Działalność Rady Bezpieczeństwa Narodowego
		Działalność Departamentu Stanu
		Działalność Departamentu Obrony
		Działalność specjalistycznych agencji spraw zagranicznych
		Działalność innych departamentów rządu
		Działalność ambasad
		Działalność aktorów nieoficjalnych (dyplomacja nieoficjalna)
	Publiczna dyplomacja	Oświadczenia publiczne
		Działalność ambasad oraz personelu przebywającego za granicą
		Emitowanie audycji oraz wykorzystanie mediów elektronicznych
		Wizyty oraz imprezy kulturalne i edukacyjne
		Wizyty na wysokim szczeblu
		Promowanie demokracji
		Wojenne wykorzystanie środków przekazu (mediów)
	Organizacje międzynarodowe	Działania w ramach ONZ
		Działania w ramach specjalizowanych agencji ONZ
		Działania w ramach organizacji regionalnych
		Działania w prywatnych organizacjach pozarządowych
	Ekonomia	Polityka handlowa
		Polityka finansowa oraz makroekonomiczna
		Pomoc zagraniczna
		Sankcje ekonomiczne
	Wywiad	Gromadzenie informacji
		Analiza i meldowanie
		Kontrwywiad
		Działania skryte

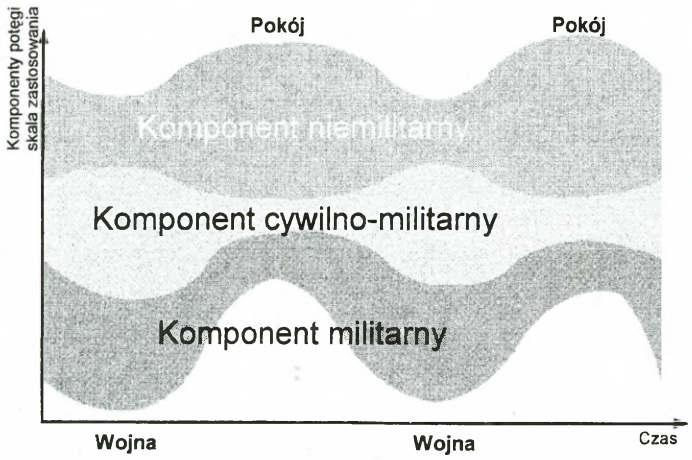
Tabela 2. Instrumenty polityczno-militarne potęgi państwa

Instrumenty polityczno-militarne	Baza produkcyjna i technologiczna	Produkowanie i usługi
		Wykorzystanie globalizacji do wywierania wpływów
		Wykorzystanie technologii informacyjnych jako strategicznego przemysłu
		Wykorzystanie przemysłu obronnego
	Kontrola zbrojeń	Kontrola rozprzestrzeniania broni jądrowej
		Wzajemna redukcja zagrożenia
		Kontrola zbrojeń konwencjonalnych
		Przedsięwzięcia budowy zaufania i bezpieczeństwa
		Nierozprzestrzenianie
		Kontrola eksportu
	Pokojowa działalność obronna	Pomoc militarna – *finansowanie i transfer broni*
		Edukacja militarna – *finansowanie, kształcenie*
		Wspólne planowanie, ćwiczenia i działania – *finansowanie, przygotowywanie, prowadzenie*
		Dyplomacja obronna – *kontakty dowódców wysokiego szczebla, rozmowy sztabowe, wymiana doświadczeń, kształtowanie świadomości obronnej cywilnego establishmentu, badania naukowe i wspieranie polityki*
	Układy (stosunki) bezpieczeństwa i zamorska obecność	Działalność w NATO
		Działalność w innych formalnych sojuszach
		Działalność w sojuszach nieformalnych
		Działalność w koalicjach
		Wysunięte rozmieszczenie sił
		Ćwiczenia militarne
		Wysunięte składowanie sprzętu i zaopatrzenia
	Operacje pokojowe i pomoc humanitarna	Zapobieganie konfliktom i tworzenie pokoju
		Utrzymywanie pokoju
		Poszerzone utrzymywanie i wymuszanie pokoju
		Operacje pomocy humanitarnej

Tabela 3. Militarne instrumenty prowadzenia wojny

Militarne instrumenty prowadzenia wojny	Niekonwencjonalne instrumenty militarne	Zwalczanie terroryzmu – *zachęcanie do współpracy międzynarodowej, nieuleganie żądaniom terrorystów, przechwytywanie terrorystów i przekazywanie ich sądowi, nakładanie sankcji na kraje sponsorujące terroryzm, działania odwetowe wobec krajów wspierających terroryzm, zapobieganie, uprzedzanie i dezorganizowanie działalności terrorystycznej*
		Działania przeciwnarkotykowe
		Kontrolowanie imigrantów i uchodźców
		Działania specjalne – skryte uderzenia lub zdobywanie informacji, działania humanitarno-pokojowe
		Walka niekonwencjonalna
		Stosowanie broni niezabójczej
		Działania psychologiczne
		Szkolenie zagraniczne sił egzekwowania prawa
	Ograniczona interwencja militarna	Rozmieszczenie sił dla wsparcia dyplomacji
		Misje ratunkowe i ewakuacyjne
		Wymuszanie sankcji
		Ograniczone uderzenia powietrzne
		Wsparcie sojuszników w konfliktach i powstaniach
		Prowadzenie małych wojen przez siły zbrojne
	Klasyczne instrumenty militarne	Użycie sił lądowych – *odstraszanie lub zatrzymanie agresji, tworzenie zgrupowania, kontrofensywa, zabezpieczenie stabilizacji postkryzysowej*
		Użycie sił powietrzno-kosmicznych – *wywalczenie przewagi w powietrzu, obezwładnienie OP przeciwnika, atakowanie obiektów strategicznych, wspieranie innych rodzajów sił zbrojnych*
		Użycie sił morskich
	Wyłaniające się instrumenty militarne	Eksploatacja zdolności „systemu systemów"
		Eksploatacja rozległej dominacji informacyjnej – *walka informacyjna*
		Eksploatacja walki hakerskiej
	Przeciwdziałanie broni masowego rażenia	Zapobieganie rozprzestrzenianiu broni ABC
		Odstraszanie jądrowe
		Zdolności przeciwuderzeniowe
		Obrona aktywna
		Obrona pasywna

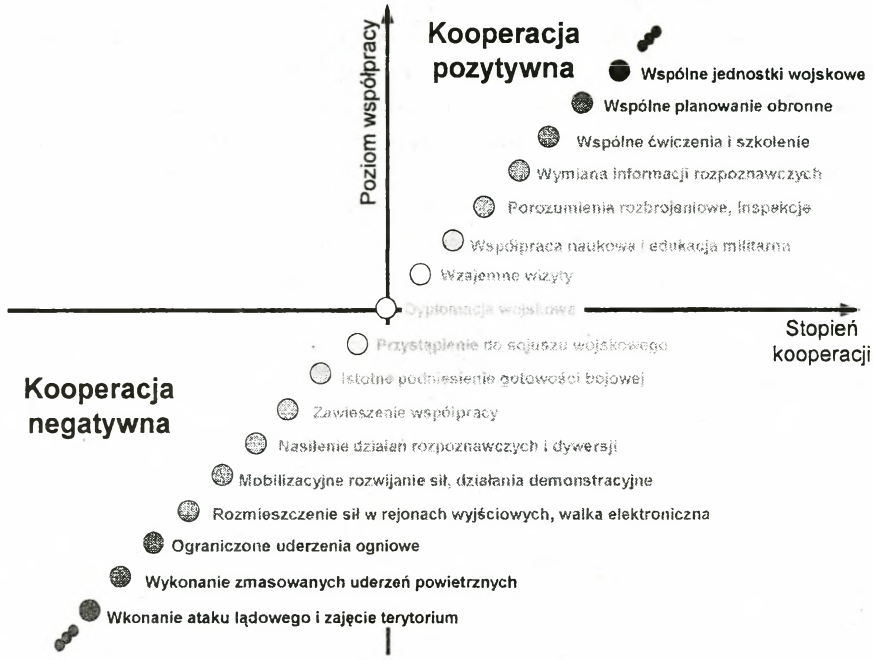
W tej sytuacji należy uznać, iż **potęga militarna jest stałym uczestnikiem polityki międzynarodowej, obecnym zarówno w czasie pokoju, kryzysu, jak i wojny.** W zależności od stanu stosunków międzynarodowych proporcje udziału poszczególnych komponentów potęgi państwa w jego działaniach ulegają zmianie. W czasie pokoju największa część tego udziału przypada komponentom cywilnym. Jednakże nawet w czasie pokoju występują różne sprzeczności interesów w pozastrategicznych obszarach. Ponadto także ze względu na odstraszanie zarówno komponent cywilno-militarny, jak i militarny jest stale obecny w działaniach państwa. Również w odwrotnej sytuacji, to jest w stanie wojny oraz w stanach pośrednich, nie zanika aktywność komponentu cywilnego i cywilno-militarnego. Zmieniają się tylko ich proporcje (rys. 10).



Opracowanie własne.

Rys. 10. Skala zastosowania komponentów potęgi państwa (przykład)

Istotną sprawą jest ponadto forma użycia poszczególnych komponentów potęgi państwa, w tym także i potęgi militarnej. Z teorii czynu skutecznego wynika, że użycie komponentów potęgi państwa może mieć formę współpracy (kooperacji pozytywnej) lub walki (kooperacji negatywnej). Poszczególne komponenty potęgi państwa, w tym także potęga militarna, ze względu na swoje właściwości, mają swoje preferencje użycia, niezależnie jednak od tego **każda z nich może być stosowana zarówno w ramach współpracy, jak i walki. Potęga militarna może być stosowana w całym spektrum działań, rozciągających się od skrajnych form walki po głęboką współpracę** (rys. 11).



Opracowanie własne.

Rys. 11. Spektrum działań militarnych

Stosowanie to zachodzi w sferze materialnej, energetycznej i informacyjnej. Jest to w pełni aktualne w odniesieniu do modelu państwa dysponującego całym zakresem współcześnie znanych komponentów potęgi oraz mającego interesy ponadlokalne. Wówczas należy uznać, iż **potęga militarna w stosunkach międzynarodowych jest stałym uczestnikiem zarówno współpracy, jak i walki**. W sytuacji mniejszych państw obecność ta w niektórych okresach może mieć mniejszy wymiar, jednakże istnieje.

Jest zrozumiałe, że nauki wojskowe koncentrują się na problemach walki, mimo tego problematyka współpracy jest również ważna, gdyż służy zapobieganiu kryzysom i wojnom, a to należy do najważniejszych interesów państwa. Interesy te, są bowiem celem wszelkich działań podejmowanych przez państwo.

Rekapitulując, można przyjąć, że:

- **Głównym motywem sprawczym zabezpieczania interesów państw na arenie międzynarodowej jest potęga państwa. Komponent militarny państwa jest częścią jego potęgi i stanowi potęgę militarną.**
- **Potęgą militarną jest potencjał destrukcyjny państwa, zdolny do trwałego lub okresowego niszczenia elementów organizacji innego państwa.**

- **Obszary zakresowe poszczególnych komponentów państwa częściowo nakładają się na siebie. Również formy stosowania potęgi państwa mają wspólny obszar. Oprócz militarnych i niemilitarnych form stosowania potęgi państwa, istnieje mieszana polityczno-militarna odmiana tych form.**
- **Potęga militarna jest stałym uczestnikiem polityki międzynarodowej, obecnym w czasie pokoju, kryzysu i wojny.**
- **Potęga militarna jest stosowana w całym spektrum działań, rozciągających się od skrajnych form walki po głęboką współpracę. Stosowanie to zachodzi w sferze materialnej, energetycznej i informacyjnej**.

1.6. Militarna walka o interesy

Pamiętając o znaczeniu współpracy, przenieśmy jednak uwagę na walkę, bo ta stanowi jedną z podstawowych kategorii nauk wojskowych, a szczególnie ***sztuki wojennej***. Walka występuje w przyrodzie poza społeczeństwem ludzkim, a człowiekowi towarzyszy od zarania jego dziejów. Odpowiednio zorganizowana walka może przybrać formę wojny. Czymże więc jest walka? Walka ma szeroki zakres znaczeniowy – jest pojęciem wieloznacznym. Do najistotniejszych znaczeń należą: ścieranie się sprzecznych interesów, współzawodnictwo, rywalizacja, jak i działanie mające na celu usunięcie, zmuszenie, pozbycie się, przezwyciężenie czegoś, także zmaganie się [...] a i zorganizowane działanie sił zbrojnych stron przeciwnych[133]. Podstawowym atrybutem walki jest przemoc, to jest działanie wbrew czyjejś woli, użycie siły fizycznej, narzucanie komuś swojej woli, zmuszanie kogoś do przyjęcia narzucanej mu woli.

Można przyjąć[134], że istotą walki jest zmuszanie kogoś do przyjęcia narzucanej mu woli, a więc przemoc. Jakie jest odniesienie walki do areny międzynarodowej? Arena międzynarodowa jest miejscem nieustannych działań zmierzających do zabezpieczenia interesów działających na niej państw. Działania te przybierają formy zarówno współpracy, jak i walki. Na arenie międzynarodowej walka jest jedną z form działań państw, podejmowanych dla osiągania celów politycznych wynikających z interesów tych państw. **Na arenie międzynarodowej oprócz współpracy toczy się walka o interesy państw. Jest ona konglomeratem wszelkich możliwych do stosowania przez państwa form walki**.

Ponieważ istotą walki jest przemoc, można uznać, iż **walka o interesy to osiąganie celów politycznych poprzez użycie przemocy**. Walka o interesy jest podzbiorem większego zbioru obejmującego wszelkie możliwe formy walki w ogóle. Jedną z form walki o interesy jest militarna walka o interesy, obejmująca część obszaru zakresowego walki o interesy.

---

[133] *Słownik języka polskiego*, t. 3, PWN, Warszawa 1979, s. 653.

[134] R. Szpyra, *Nauki militarne, ich przedmiot poznania i dekompozycja*, [w:] *Sztuka wojenna*... wyd. cyt.

Militarna walka o interesy to osiąganie celów politycznych przez użycie przemocy militarnej, czyli stosowanie wobec przeciwnika szeroko rozumianego potencjału destrukcyjnego państwa, wbrew woli tego przeciwnika, dla osiągania własnych celów politycznych.

Warto zwrócić uwagę na to, iż w tym ujęciu walką militarną jest stosowanie potencjału destrukcyjnego państwa. Stosowanie to może mieć charakter czynienia fizycznej destrukcji, jak też być niedestrukcyjne fizycznie. Przykładem niedestrukcyjnych fizycznie form walki, mogą być odstraszanie i działania pośrednie. Dużo uwagi poświęca im, m.in. B. Balcerowicz. Poszukując istoty odstraszania i autorów tej koncepcji, pisze m.in.: „Beaufre w definicji „odstraszania" przyjmuje, że ma ono na celu powstrzymanie wrogiego mocarstwa od powzięcia decyzji o użyciu swej broni lub, mówiąc bardziej ogólnie, od działania czy też określonego reagowania na działanie w danej sytuacji. Odstraszanie osiąga się dzięki posiadaniu środków, które stanowią wystarczającą groźbę i zapewniają uzyskanie pożądanego efektu psychologicznego.

Psychologiczny skutek, według Beaufre'a, uzyskuje się przez wywołanie u przeciwnika kombinacji wyrachowania (przy którym porównuje się ryzyko ze stawką) i obawy (wywołanej przez groźbę niebezpieczeństwa oraz niewiadomy efekt konfliktu)"[135].

Według *Słownika terminów z zakresu bezpieczeństwa narodowego* „odstraszanie to niekonfrontacyjne przedsięwzięcie polegające na zniechęcaniu strony przeciwnej do działań agresywnych", lecz także „jedna z funkcji systemu obronnego państwa, której istota polega na zniechęceniu strony przeciwnej do działań agresywnych". „Odstraszanie militarne to jedna z funkcji sił zbrojnych, której istotą jest przekonanie strony przeciwnej o nieopłacalności podjęcia działań zbrojnych"[136].

B. Balcerowicz uznaje też ważność działań pośrednich, przyznając iż „[...] do strategii działań pośrednich uciekali się świadomie lub mniej świadomie wielcy wodzowie minionych wieków. Ojcem nowoczesnej, pełnej teorii działań pośrednich jest bezsprzecznie właśnie B. Liddell Hart.

Istota strategii działań pośrednich tkwi w przeświadczeniu, że obok walki, obok bezpośrednich starć zbrojnych, strony walczące rozporządzają całą gamą innych środków, a zwycięstwo osiąga się prędzej w wyniku osłabienia ducha i zdemoralizowania dowództwa przeciwnika niż wskutek fizycznego zniszczenia jego sił.

W myśl idei strategii działań pośrednich sztuka zwyciężania polega nie tyle na dążeniu do nawiązania bitwy z nieprzyjacielem, co na stworzeniu takiej sytuacji strategicznej, która, jeśli sama przez się nie da rozstrzygnięcia, to zapewni, że przyniesie je stoczona w jej warunkach bitwa. [...]

Strategię działań pośrednich stosuje się oczywiście nie tylko w stanie wojny i odnosi się ona nie tylko do działań wojennych. **Celem działań pośrednich jest przecież stworzenie sytuacji, w której przeciwnik odstąpi od zamiaru agresji**

---

[135] Cyt. za: B. Balcerowicz, *Obronność państwa średniego*, Warszawa 1997, s. 149–150.
[136] *Słownik terminów...* s. 86 i 87.

(ataku) bądź zaniecha oporu w wyniku zastosowania środków innych niż walka. Jest to zatem strategia czasu pokoju, kryzysu i wojny"[137].

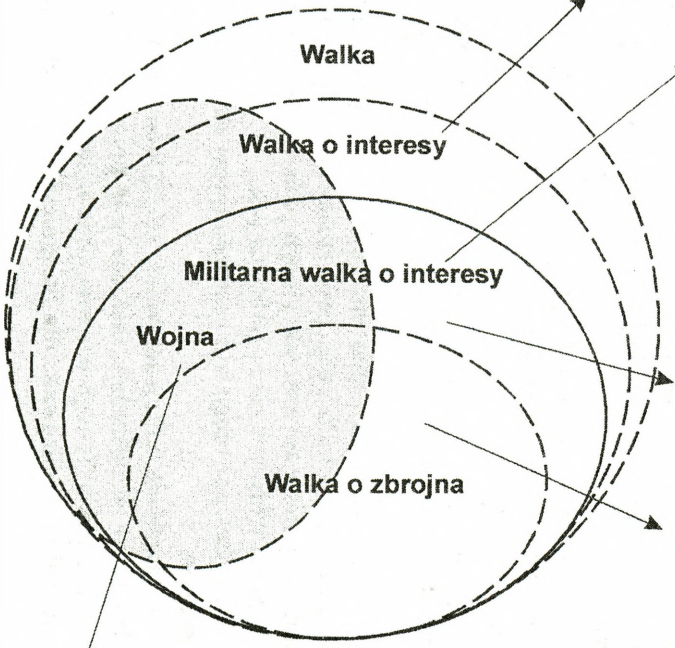
Wątpliwości budzi tu stwierdzenie „w wyniku zastosowania środków innych niż walka". Należy sądzić, iż chodzi tu o wąskie rozumienie słowa *walka* – jako walki zbrojnej. Tymczasem przedsięwzięcia podejmowane przeciwko komuś wbrew jego woli, nie stanowią współpracy, lecz walkę. Działania pośrednie, są więc formą walki zmierzającej do narzucenia przeciwnikowi swojej woli.

Częścią militarnej walki o interesy jest walka zbrojna. Jaka jest więc różnica między tymi formami? By znaleźć odpowiedź warto przypomnieć, iż *zbrojny* to związany z użyciem broni, zdolny do destrukcji, podstawową zaś cechą broni jest zdolność osiągania dezintegracji lub paraliżu. **Od zarania dziejów destrukcja przedmiotów materialnych i ludzi stanowiła istotę walki zbrojnej**. O ile więc, **w militarnej walce mogą być stosowane zarówno formy destrukcyjne, jak i niedestrukcyjne fizycznie**, to **walka zbrojna jest tą częścią militarnej walki, której właściwa jest fizyczna destrukcja**. G. Nowacki w swoich badaniach, proponując układ dekompozycji walki, również uznał, iż kryterium wyróżnialności walki zbrojnej jest dążenie do pokonania przeciwnika drogą stosowania fizycznych środków niszczenia[138]. Destrukcja fizyczna może być dokonywana za pomocą różnych form energii, ma charakter rażenia i jest możliwa do zidentyfikowania i pomiaru. Walka zbrojna nie składa się jednak tylko z rażenia. W jej skład wchodzą również przedsięwzięcia umożliwiające rażenie. Jednakże przedsięwzięcia te bez rażenia nie mogą stanowić walki zbrojnej. Mieszczą się natomiast w zakresie walki militarnej (rys. 12).

Można więc uznać, iż walka zbrojna to bezpośrednie zastosowanie potęgi militarnej do niszczenia elementów organizacji innego państwa oraz ochrony przed podobnym działaniem przeciwnika dla osiągnięcia własnych celów politycznych.

Czy jednak zastosowanie walki zbrojnej jest równoważne wojnie? W praktyce nawet w sytuacji wystąpienia walk zbrojnych o ograniczonej skali, nie zawsze traktuje się je jako wojnę. Kryterium tego czy dana przemoc staje się wojną, czy nie, jest skutek tej przemocy. Jeżeli w wyniku zastosowania przemocy zagrożone lub naruszone zostają najistotniejsze (tzw. żywotne) interesy danego państwa lub narodu[139], taka przemoc staje się wojną. Oczywiście **trudno mówić o bezwzględnych miarach i granicach wojny, bo mają one subiektywny charakter**. To, co jedni postrzegają jako nieważne, dla innych może być sprawą o żywotnym znaczeniu. Są jednak pewne wspólne wartości, takie jak niepodległość, suwerenność, integralność terytorialna, jednak jest ich niewiele. Ustalenie tego, co jest dla danego narodu żywotnie ważne, zależy tylko od tego narodu, dlatego też dany naród musi ocenić czy stosowana przemoc zagraża jego żywotnym interesom, i czy oznacza to dla niego wojnę. W istocie wojna zawsze była środkiem oddziaływania na świa-

[137] B. Balcerowicz, *Obronność państwa...* s. 158–159.
[138] Zob. G. Nowacki, *Współczesne poglądy...* s. 38.
[139] Rozumianego tutaj jako zbiór obywateli państwa.



Walka o interesy to osiąganie celów politycznych przez użycie przemocy.

Militarna walka o interesy to osiąganie celów politycznych przez użycie przemocy militarnej. Bezpośrednie cele działań militarnych to **cele militarne.**
Przemoc militarna to zastosowanie potęgi militarnej wbrew woli przeciwnika do osiągania własnych celów politycznych.
Potęga militarna to potencjał destrukcyjny państwa zdolny do trwałego lub okresowego niszczenia bądź modyfikowania elementów organizacji innego państwa, a także do ochrony przed podobnym działaniem przeciwnika.

Militarna walka o interesy jest więc stosowaniem wobec przeciwnika szeroko rozumianego potencjału destrukcyjnego państwa, wbrew woli tego przeciwnika, dla osiągania własnych celów politycznych.

Walka zbrojna to bezpośrednie zastosowanie potęgi militarnej do niszczenia elementów organizacji innego państwa oraz ochrony przed podobnym działaniem przeciwnika, realizowane dla osiągnięcia własnych celów militarnych.

Wojna jest kategorią obejmującą wszystkie formy walki, jednakże jej istnienie zależy od uznania, w przeciwieństwie do walki istniejącej obiektywnie. Wojna jest takim poziomem walki, a szczególnie walki o interesy, który w ocenie zaangażowania państwa zagraża głównym celom istnienia tego państwa.

Źródło: R. Szpyra, *Nauki militarne, ich przedmiot poznania i dekompozycja*, [w:] *Sztuka wojenna. Konteksty teoretyczne i praktyczne*, red. M. Krauze, B.M. Szulc, Toruń 2000, s. 102.

Rys. 12. Wybrane kategorie militarnego aspektu walki

domość narodów i ich decydentów. Działania wojenne miały wywierać wrażenie na atakowanym społeczeństwie i powodować zmianę jego świadomości. Obecnie pojawia się coraz więcej możliwości oddziaływania na świadomość narodów. W wojnach prowadzonych przez najwyżej rozwinięte, społeczeństwa stopniowo zmniejsza się skala zabijania. Nie zmniejsza się jednak skala przemocy, przyjmuje ona jednak inne formy.

Taki stan prowadzi do stopniowego kwestionowania podstawowego przekonania, jakie było dotychczas przyjmowane, że istotą wojny jest walka zbrojna, której główną formą jest fizyczna destrukcja. Może się okazać, że podobnie jak newtonowska mechanika jest prawdziwa tylko w określonych warunkach, tak i klasyczne rozumienie wojny jest prawdziwe w odniesieniu do określonych poziomów rozwoju cywilizacji ludzkiej. Przekroczenie pewnej granicy rozwoju tej cywilizacji i wejście w wyższe jego stadia, może wymagać zmodyfikowania rozumienia zjawiska wojny. Jest wiele przesłanek świadczących o tym, że taki stan już nastąpił i należy to uwzględniać w koncepcjach opracowywanych na gruncie nauk wojskowych.

Podział ten, jak każdy inny, jest dokonywany w określonym celu. Zaproponowana forma tego podziału ma na celu uporządkowanie obserwowanych w praktyce zjawisk oraz stworzenie bardziej uniwersalnego od funkcjonujących modelu, który lepiej oddawałby związki sfery militarnej z polityką międzynarodową, a także obejmowałby pojawiające się coraz liczniej nowe środki i formy walki.

Wobec przytoczonej argumentacji, do dalszych rozważań przyjęto, że:

- **Walka jest historycznym zjawiskiem obecnym nie tylko w społeczeństwie ludzkim, lecz i w przyrodzie. Istotą walki jest przemoc, czyli zmuszanie kogoś do przyjęcia narzucanej mu woli.**
- **Na arenie międzynarodowej oprócz współpracy toczy się walka o interesy państw. Jest ona konglomeratem wszelkich możliwych do stosowania przez państwa form walki.**
- **Walka o interesy to osiąganie celów politycznych przez użycie przemocy. W zakresie znaczeniowym walki o interesy mieści się militarna walka o interesy.**
- **Militarna walka o interesy, czyli walka militarna, to osiąganie celów politycznych przez użycie przemocy militarnej, czyli stosowanie wobec przeciwnika szeroko rozumianego potencjału destrukcyjnego państwa, wbrew woli tego przeciwnika, dla osiągania własnych celów politycznych.**
- **W militarnej walce stosowane mogą być zarówno formy destrukcyjne, jak i niedestrukcyjne fizycznie.**
- **Walka zbrojna jest tą częścią militarnej walki, której właściwa jest fizyczna destrukcja. Walka ta to bezpośrednie zastosowanie potęgi militarnej do niszczenia elementów organizacji innego państwa oraz ochrony przed podobnym działaniem przeciwnika, realizowane dla osiągnięcia własnych celów militarnych.**

- **Wojna jest kategorią obejmującą wszystkie formy walki, jednakże jej istnienie zależy od uznania – w przeciwieństwie do walki istniejącej obiektywnie. Wojna jest takim poziomem walki, a szczególnie walki o interesy, który w ocenie zaangażowanego państwa zagraża głównym celom istnienia tego państwa.**

2. TEORIA INFORMACJI A OPERACJE INFORMACYJNE

2.1. Przegląd teorii informacji

Cały świat ożywiony wykorzystuje informację, dlatego od zarania dziejów była ona jednym z podstawowych komponentów cywilizacji ludzkiej. Zachodzące w drugiej połowie XX w. rewolucyjne zmiany technologiczne gwałtownie zwiększyły znaczenie informacji, czyniąc ją podstawowym dobrem oraz główną cechą charakterystyczną nowej formacji cywilizacyjnej.

Mimo swego znaczenia, informacja oraz pokrewne jej kategorie w dalszym ciągu nie są zadowalająco zdefiniowane. Nie jest to zadanie proste[140], z powodu istnienia dużej różnorodności poglądów. Warto przy okazji zauważyć, iż poglądy te zmieniały się wraz z upływem czasu i prawdopodobnie będzie się tak dziać nadal. Przedstawiciele różnych poglądów prezentowali odmienne definicje informacji i związanych z nią pojęć.

Warta odnotowania jest praktyczna nieobecność definicji informacji w literaturze. Co prawda, często cytowane jest w literaturze stwierdzenie, że informacja jest tym, co redukuje niepewność, jednakże nie jest to zadowalający identyfikator informacji. Można bowiem zidentyfikować również inne czynniki redukujące niepewność, jak chociażby emocjonalne wsparcie. W pewnym uproszczeniu, prezentowane przez różnych autorów poglądy przedstawiono w tabeli 4.

Prezentowane w tabeli definicje pogrupowane są w trzy sekcje. W pierwszej od góry informacja jest postrzegana jako coś, co tworzy wiedzę. Sekcja dolna wywodzi informację z wiedzy, uznając, iż ta tworzy informację. Sekcja środkowa traktuje informację jako funkcję prawdopodobieństwa. Wśród przedstawicieli tego podejścia wyróżnić można dwa kierunki: jeden koncentrujący się na entropii i sugerujący rolę informacji jako konkretnego zjawiska bytu oraz drugi, akcentujący prawdopodobieństwo i finansowy wymiar możliwych skutków.

Również G. Nowacki, badając definicje informacji, zauważył, iż „niezmiernie trudno jest podać adekwatne określenie informacji"[141].

---

[140] Zob. M. Feeney, M. Grieves, *The Value and Impact of Information*, London 1994, s. 10–11.

[141] G. Nowacki, *Walka informacyjna – próba kategoryzacji*, Rozprawa doktorska, Warszawa 1999, s. 24.

Tabela 4. Definicje informacji

Źródło	Definicja informacji	Informacja a wiedza
Blumenthal 1969	Zapisane, sklasyfikowane i zorganizowane dane odnoszące się do lub interpretujące przekazywane znaczenie.	Informacja jest ogniwem pomiędzy wiedzą a obserwowanymi zjawiskami.
Bell 1979	Wzór lub projekt przeorganizowania danych dla instrumentalnych potrzeb.	Informacja jest ogniwem pomiędzy wiedzą a obserwowanymi zjawiskami, akcentującym interpretację zjawiska (danych).
Burch 1974	Rezultat modelowania, formatowania, organizowania lub przekształcania danych dokonywanych w taki sposób, który zwiększa poziom wiedzy ich odbiorcy.	Informacja zasila i wspiera wiedzę.
Deeson 1991	To, co zwiększa ludzką wiedzę.	Informacja zasila wiedzę.
Arrow 1984	Redukcja niepewności.	Wiedza jest odzwierciedleniem niepewności zdarzeń realnego świata; informacja jest zmianą prawdopodobieństwa tego stanu; wynika z tego, że informacja jest „użyteczną wiedzą".
Stonier 1990	Informacja jest funkcją złożoności.	Wiedza jest zorganizowaną w głowach ludzi informacją.
OED	Przekazywana wiedza dotycząca konkretnego faktu, przedmiotu lub zdarzenia.	Informacja jest ekspresją wiedzy.
Farradane 1976	Reprezentacja wiedzy lub myśli.	Informacja jest ekspresją wiedzy.

Źródło: M. Feeney, M. Grieves, *The Value and Impact of Information*, London 1994, s. 11.

Autorzy *Information Science in Theory and Practice*[142] przytaczają opracowaną przez Belver Griffith interesującą mapę poszczególnych kierunków nauki o informacji i ich przedstawicieli. Mapa ta powstała w wyniku zastosowania kilku specjalnych metod analizy poglądów poszczególnych autorów i stanowi ciekawą syntezę tej analizy (rys. 13).

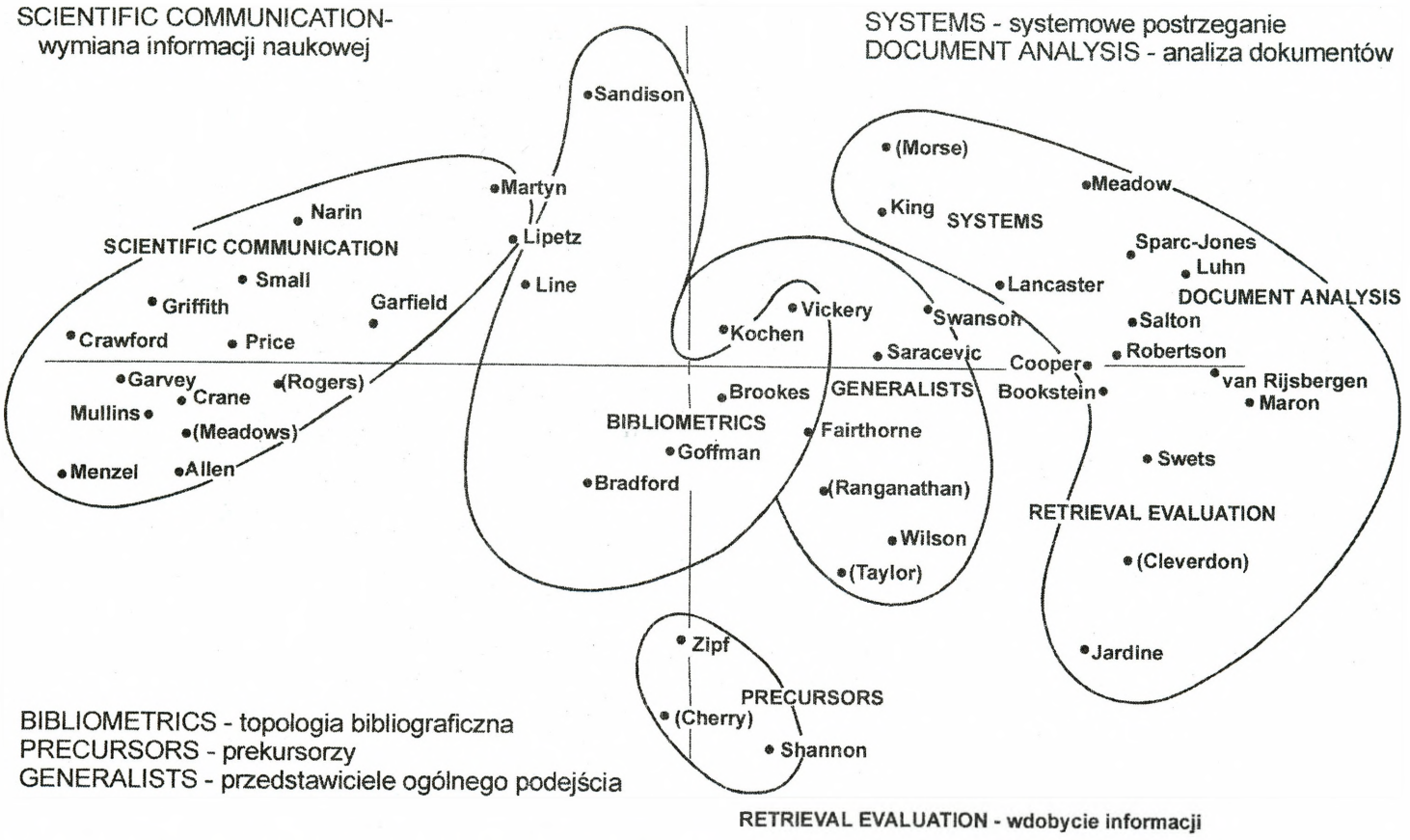
W badaniu informacji stosowane są różne podejścia. W polskim środowisku nauk wojskowych, a także wielu nauk cywilnych, dosyć popularne jest podejście, które ogólnie można nazwać fizyczno-cybernetycznym. Naukowcy hołdujący takiemu podejściu, opierają swoje rozważania zwykle na teorii informacji Shannona[143].

[142] B. Vickery, A. Vickery, *Information...* s. XIII.

[143] Teoria ta bazuje na pojęciu *entropii informacyjnej*. Entropia ta wyrażona jest równaniem:

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

gdzie: X_d – dyskretna zmienna losowa; p_i – prawdopodobieństwo i-tej realizacji dyskretnej zmiennej losowej X_d; a – jednostkowa miara ilości informacji.



Źródło: B. i A. Vickery, *Information Science in Theory and Practice*, London, 1987, s. XIV.

Rys. 13. Mapa teoretyków, ich poglądów oraz zachodzących między nimi relacji

Teoria ta zrodziła się na gruncie telekomunikacji i w tej dziedzinie ma najwięcej zastosowań. Według niej natura informacji i entropii fizycznej jest taka sama. Entropia jest miarą braku szczegółowej informacji o układzie fizycznym. Im większa będzie informacja, tym mniejsza będzie entropia. Teorii informacji nie można rozwijać jako oddzielnej całości. Powiązanie z termodynamiką jest tak ścisłe, że w konsekwencji wymagana jest fizyczna teoria informacji[144].

Tak rozumiana teoria informacji ma pewne zalety i wady. Do zalet należy głównie to, iż „może być z powodzeniem stosowana przy rozwiązywaniu wszystkich zagadnień technicznych, w których informacja odgrywa rolę, w szczególności zagadnień dotyczących: kodowania, telekomunikacji, maszyn matematycznych. W tych wszystkich przypadkach mamy do czynienia z przetwarzaniem informacji lub przekazywaniem jej z jednego miejsca na drugie. Teoria informacji jest bardzo użyteczna przy ustalaniu praw dotyczących przekazywania i przetwarzania informacji oraz przy określaniu dokładnych granic tego, co można robić, a czego nie"[145].

Podstawowa niedoskonałość polega na tym, że w ramach tej teorii „nie jesteśmy na razie w stanie analizować procesów myślenia i nie możemy w tej chwili wprowadzić do naszej teorii żadnego elementu zawierającego pojęcie wartości informacji w sensie potocznym. Wyeliminowanie pojęcia wartości informacji jest bardzo poważnym ograniczeniem, lecz jest to cena, jaką musieliśmy zapłacić za możliwość stworzenia tej gałęzi wiedzy"[146].

„Dlaczego więc, mimo tej istotnej wady, teoria ta stała się popularna? Powodem tego było zapotrzebowanie ze strony rozwijającej się telekomunikacji. Ograniczenie, o którym mowa, pozwala na podanie definicji ilości informacji; dzięki niej możemy traktować informację jako wielkość fizycznie mierzalną. Definicja ta nie rozróżnia jednak informacji o wielkim znaczeniu od niezbyt ważnej dla odbiorcy. Na pierwszy rzut oka definicja ta może się wydać sztuczna, lecz w rzeczywistości definicja obiektywnej ilości informacji ma duże znaczenie praktyczne. Eliminacja czynnika wartości daje możliwość rozwiązania szeregu zagadnień. Inżyniera projektującego system telefoniczny nie obchodzi czy linią będą przesyłane wiadomości dyplomatyczne, kursy akcji na giełdzie, czy nic nie znaczące rozmowy. Problem techniczny pozostanie zawsze taki sam: przekazać informację bezbłędnie i dokładnie bez względu na to, jaką może ona mieć dla kogoś wartość. Projektant maszyny matematycznej nie wie czy będzie ona używana do obliczania tablic astronomicznych, czy też kont czekowych. Odrzucenie pojęcia wartości informacji stwarza możliwość naukowej analizy informacji bez uprzedzeń i wpływu czynników emocjonalnych[147].

---

[144] Zob. L. Brillouin, *Science...* s. 373.
[145] Tamże, s. 19.
[146] Tamże.
[147] Tamże, s. 20.

Mimo tych korzyści, niedoskonałości fizyczno-cybernetycznej teorii informacji stanowiły mocny bodziec do poszukiwania innych modeli teorii informacji. Zauważył to już w latach sześćdziesiątych dwudziestego wieku Marian Mazur, pisząc m.in.:

„[...] Znaczenie koncepcji, które stały się podstawą powstania i ogromnego rozwoju działu cybernetyki, zwanego powszechnie *teorią informacji*, polegało na wskazaniu możliwości ilościowego ujmowania informacji, co wyraziło się we wprowadzeniu pojęcia *ilość informacji*. Takie ujęcie informacji stało się przydatne do wszelkich procesów informacyjnych, bez względu na dziedzinę, oraz niezwykle owocne, czego dowodem jest mnogość publikacji z zakresu tej problematyki.

Nadało to jednak teorii informacji daleko idącą jednostronność, czyniąc z niej w rzeczywistości raczej *ilościową teorię informacji*.

W ostatnich latach zaczęły się pojawiać publikacje, zresztą bardzo jeszcze nieliczne, z zakresu, który można by nazwać *wartościową teorią informacji*, dotyczące zagadnień oceny przydatności informacji do rozwiązywania zagadnień decyzyjnych"[148].

Mazur zauważa także, iż:

„[...] Sam jednak termin *ilość informacji* stał się przyczyną zamieszania, sugeruje bowiem, że jeżeli wiadomo, co to jest ilość informacji, to również wiadomo, co to jest informacja.

Przypuszczenie to było szczególnie atrakcyjne dla humanistów, którym zaświtała nadzieja, że na tej podstawie będą mogli rozwiązywać swoje problemy metodami podobnymi do stosowanych w naukach ścisłych. Utwierdzała ich w tym okoliczność, że dla teorii opartej na przytoczonych powyżej wzorach utarła się nazwa *teoria informacji* sugerująca, że przedmiotem tej teorii jest informacja, a nie tylko ilość informacji – tym bardziej że *teorią informacji* zaczęto z czasem nazywać całą dziedzinę nauki zajmującą się teoretyczną stroną procesów informacyjnych. [...]

Tymczasem w odniesieniu do dotychczasowego stanu jest to nazwa na wyrost, na razie bowiem teoria informacji ma niekompletne podstawy i to, co najmniej pod dwoma względami.

Po pierwsze wymaga ona teoretycznego ujęcia samego pojęcia informacji.

Po drugie nawet pojęcie ilości informacji nie obejmuje wszystkich przypadków, w których zachodzi potrzeba ilościowego ujmowania informacji. Rzecz w tym, że posługiwanie się tym pojęciem wymaga określenia o jaki zbiór zdarzeń chodzi i jakie jest prawdopodobieństwo każdego z nich. Tymczasem często zachodzi potrzeba ilościowego określenia informacji, mimo że zbiór możliwości jest nieokreślony, a ich prawdopodobieństwo w ogóle nie wchodzi w grę. Na przykład, programy nauczania historii w szkole obejmują większą lub mniejszą liczbę faktów historycznych, przy czym dla nauczyciela jest oczywiste, że przy obszerniejszym programie uczeń otrzymuje więcej informacji niż przy mniej obszernym. Jednak do ilościowego określenia tej różnicy nauczyciel nie będzie mógł posłużyć się *ilością*

[148] M. Mazur, *Jakościowa teoria...* s. 11.

informacji w sposób przyjęty w teorii informacji, gdyż nikt nie potrafi określić liczby wszystkich faktów historycznych ani też nie miałoby sensu operowanie prawdopodobieństwem poszczególnych faktów, skoro każdy z nich już się przecież odbył. Z podobnych przyczyn niepodobna określić *ilość informacji* zawartą np. w stwierdzeniu, że teraz jest 1970 r. Do zbioru ilu lat należy bowiem wymieniony rok? Jak można mówić o prawdopodobieństwie występowania poszczególnych lat, zwłaszcza lat minionych, a więc nie mogących się już zdarzać z żadnym prawdopodobieństwem? A w jaki sposób zastosować pojęcie ilości informacji np. do mapy? Mapa zawiera przecież wiele informacji, np. można się z niej dowiedzieć, że Sztokholm leży na północ od Budapesztu, że odległość z Madrytu do Belgradu wynosi 2000 km lub że z Londynu jest dwa razy dalej do Rzymu niż do Genewy. Ile bitów zawiera każda z tych informacji? O jakie tu może chodzić prawdopodobieństwo? Przecież wszystkie elementy mapy i terenu istnieją, a nie zdarzają się z jakimś prawdopodobieństwem. A jak określać ilość informacji w geometrii, np. w stwierdzeniu, że pewien kąt stanowi połowę innego kąta, skoro elementy geometryczne w ogóle się nie zdarzają, są bowiem pojęciami fikcyjnymi?

Tego rodzaju niejasności wywołują zdziwienie, że chociaż istnieje już teoria informacji, nie można się z niej dowiedzieć ani co to jest informacja, ani nawet jaka jest ilość informacji (co przecież jest głównym pojęciem w tej teorii) w zwykłych, najczęściej w praktyce spotykanych zdaniach.

Można na to odpowiedzieć, że teoria informacji nie do takich potrzeb została stworzona, jednak argument ten jest przyznaniem, że teoria ta, jak dotychczas, mniej daje, niż jej nazwa obiecuje"[149].

Mazur przytacza też ciekawą opinię Abramsona – autora pracy *Teoria informacji i kodowania*, który zauważył, iż „praca Shannona dotyczy raczej przekazywania przenoszących informację sygnałów, nie zaś informacji jako takiej. Praca ta dotyczy raczej telekomunikacji niż trudno uchwytnego rezultatu końcowego telekomunikacji, jakim jest informacja"[150]. Zarówno Shannon, jak i inni przedstawiciele teorii informacji odcinali się od takich spraw, jak treść, sens, rozumienie. Oto deklaracja Shannona z cytowanego powyżej dzieła:

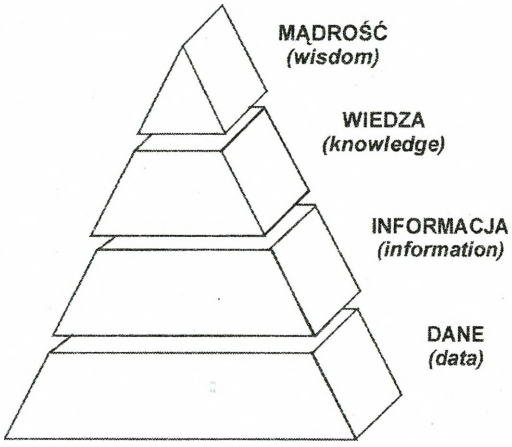
„[...] Podstawowe zadanie komunikacji polega na tym, żeby w sposób dokładny lub przybliżony odtworzyć w pewnym miejscu wiadomość, która w innym miejscu została wybrana do przekazania. Często wiadomości mają treść, to jest odnoszą się do pewnego systemu mającego fizyczny lub umysłowy sens bądź pozostają w odpowiedniości z pewnym systemem. Te semantyczne aspekty wiadomości nie dotyczą technicznej strony zagadnienia (*these semantic aspects of communication are irrelevant to the engineering problem*). Istotne jest tylko to, że przesyłana wiadomość jest wiadomością wybraną z pewnego zbioru możliwych wiadomości. System komunikacyjny powinien być tak zaprojektowany, żeby można go było wykorzystać do przekazania dowolnej możliwej wiadomości, a nie tylko tej, która

[149] Tamże, s. 16–17.
[150] Tamże, s. 18.

zostanie rzeczywiście wybrana, gdyż wynik takiego wyboru jeszcze nie jest znany w chwili projektowania"[151].

Wobec tego M. Mazur dochodzi do słusznej konstatacji, że „Głównym szkopułem w rozważaniach na temat pojęcia *informacja* ciągle jeszcze jest rola psychiki. Gdy się ją pomija, problem staje się fragmentaryczny. Gdy się ją uwzględnia, staje się niejasne, jak traktować procesy informacyjne w maszynach z punktu widzenia takich pojęć, jak *sens*, *treść*, *znaczenie*"[152].

Interesujące konstatacje przedstawił P. Sienkiewicz. Uznał on, że „obecnie do opisu *infosfery* (pojęcie wprowadzone przez J.L. Kulikowskiego w 1978 r.) posługujemy się następującymi pojęciami (rys. 14): dane (*data*), informacje (*information*), wiedza (*knowledge*), mądrość (*wisdom*).



Źródło: P. Sienkiewicz, *Wiek informacji. Wykład inauguracyjny Wyższej Szkoły Informatyki*, Warszawa 2000.

Rys. 14. Podstawowe kategorie opisu infosfery

Można je zdefiniować w sposób następujący:

- **(1) dane: uporządkowany zbiór nazw (N) i wartości liczbowych (V) opisujących określony obiekt (system, proces, zdarzenie), czyli:**

$$D \subset N \times V$$

- **(2) informacje: zbiór danych uporządkowanych zgodnie z potrzebami odbiorcy (użytkownika), wyrażającymi jego potencjalne (lub realne) działania, czyli:**

$$I_u = <D, R_u>, R_u \subset D \times D$$

[151] Tamże, s. 21.
[152] Tamże, s. 26.

- **(3) wiedza: zbiór informacji wykorzystywanych przez użytkownika zgodnie z wymaganiami (*C*), w podejmowanych działaniach (*A*), czyli:**

$$K_u = < I_u, C, A >, C: 2^{Iu} \longrightarrow A$$

- **(4) mądrość: wiedza, dzięki której podmiot (użytkownik) realizuje swoje cele (*G*) zgodnie z przyjętym systemem wartości (V_u), czyli:**

$$W_u = < K_u, G, V_u >$$

A zatem mądrość jest wiedzą podmiotu, którego czyny są skuteczne i służą osiąganiu celów *godziwych* (w ujęciu T. Kotarbińskiego).

Informację jako kategorię mierzalną charakteryzuje:

ilość wyrażoną jako różnicę między niepewnością (entropią) początkową, dotyczącą zjawiska *X*, a niepewnością (entropią) po otrzymaniu komunikatu *Y*:

$$I(X, Y) = H(X) - H(X/Y)$$

jakość wyrażoną jako stopień spełnienia wymagań użytkownika dotyczących: α – pełności (kompletności), β – aktualności (terminowości), γ – wiarygodności (niezawodności):

$$Q(I) = Q(\alpha, \beta, \gamma)$$

wartość wyrażoną jako wzrost użyteczności (wartości) określonego działania będącego rezultatem uzyskania informacji o pożądanej jakości (z uwzględnieniem kosztów jej uzyskania), np.:

$$V(I) = U(I, Q) - U_o - K$$

A zatem:

$$I \equiv < I(X, Y), Q(I), V(I) >$$

System informacyjny – taki system działania, którego zadaniem jest zbieranie (zdobywanie), przesyłanie, przetwarzanie, przechowywanie i udostępnianie informacji zgodnie z wymaganiami użytkownika w celu zaspokojenia jego potrzeb informacyjnych.

Można zatem przyjąć, że celem systemu informacyjnego *obsługującego* określony system użytkownika informacji jest stworzenie mu informacyjnych warunków efektywnego działania, czyli:

$$I \geq P_o, Q(I) \geq Q_o, V(I) \geq V_o$$

Gdzie: (I_o, Q_o, V_o) – potrzeby i wymagania informacyjne systemu użytkownika.

Zgodnie z propozycją M. Mazura procesy informowania obejmują następujące przypadki:

- **transinformowanie, czyli informowanie wierne,**
- **pseudoinformowanie, czyli informowanie pozorne (np. rozwlekłe, ogólnikowe, niejasne),**

- **dezinformowanie, czyli informowanie fałszywe,**
- **parainformowanie (np. wykorzystujące *domniemywania*, aluzje).**

System informacyjny zaspokajający potrzeby informacyjne systemu decyzyjnego jest w istocie *systemem transinformowania*. Systemy informacyjne, których cele są odmienne od sformułowanych wyżej, czyli służą zmniejszaniu ilości, jakości i wartości informacji, są w istocie systemami dezinformowania lub pseudoinformowania (parainformowania). Celem ich jest degradacja wartości zasobów informacyjnych określonych systemów działania (np. przeciwnika)"[153].

2.2. Podejście społeczne teorii informacji

Pojawiły się też inne kierunki poszukiwań. Jeden z nich naukę o informacji (*information science*) traktuje jako studiowanie przepływu informacji w społeczeństwie. Akcent jest więc tu położony na aspekt społeczny informacji. Kierunek ten jest klarownie wyłożony w pracy Briana i Aliny Vickery'ch zatytułowanej *Information Science in Theory and Practice*[154]. W pracy przyjęto najistotniejsze założenia tej koncepcji.

Jednostkowy akt transferu informacji może być przedstawiony jako układ: źródło – kanał – odbiorca. Kanał ma tu szerokie rozumienie od prostych fal głosowych przekazujących mowę po układy złożonych łańcuchów procesu transferu informacji. Transfer informacji zachodzi wtedy, gdy źródło ma informację i emituje ją, jeżeli odbiorca chce i akceptuje ją oraz gdy odpowiedni kanał jest dostępny dla źródła i dla odbiorcy.

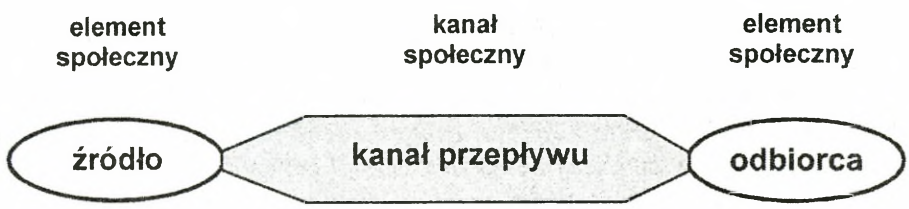
Warto zwrócić uwagę na fakt, że czynnik ludzki ma wielkie znaczenie zarówno w odniesieniu do źródła i odbiorcy informacji, jak też do kanału przepływu informacji. W odniesieniu do kanału ludzki udział może być bezpośredni – bo człowiek może również stanowić kanał przepływu informacji – lub pośredni, bo również charakterystyki kreowanych przez człowieka kanałów technicznych są kształtowane przez ludzi, którzy zarządzają, projektują i operują nimi. W ten sposób człowiek wpływa również na transmisję informacji przez kanał jej przepływu. W tej sytuacji istota jednostkowego aktu transferu informacji jest zespołem relacji pomiędzy ludźmi, którzy działają jako źródło lub są związani ze źródłem, odbiorcą lub kanałem przepływu informacji. Akty komunikacji mają więc społeczny charakter i w obrębie społeczeństwa dochodzi do transferów informacji. Ze społecznego punktu widzenia jednostkowy akt transferu informacji można zobrazować tak, jak na rys. 15.

Tak postrzeganymi, komunikującymi się społecznymi elementami mogą być pojedynczy ludzie, grupy ludzkie, organizacje lub jakiekolwiek inne formy społeczne. Studiowanie informacji w kontekście stosunków społecznych jest więc specyficznym podejściem badawczym nauki o informacji.

---

[153] P. Sienkiewicz, *Współczesne koncepcje walki informacyjnej*, [w:] *Informacyjny wymiar współczesnych działań powietrznych. Materiały z sympozjum naukowego*, red. R. Szpyra, Warszawa 2002.

[154] B. Vickery, A. Vickery, wyd. cyt.



Źródło: B. Vickery , A. Vickery, *Information Science in Theory and Practice*, London 1987, s. 13.

Rys. 15. Społeczne postrzeganie komunikacji informacji

Informacyjne systemy na dowolnym poziomie złożoności, ponad najprostszym, reprezentującym bezpośrednią rozmowę, wymagają pośrednictwa techniki. Aspekt techniczny jest istotny jedynie wtedy, gdy wpływa na relacje między informacją a stosunkami społecznymi.

Nieodłączną cechą każdej sytuacji społecznej jest proces komunikacji. W sytuacjach społecznych ludzie przekazują zamiary, instrukcje, porady, informacje, postawy, opinie, akceptację lub jej brak, odczucia, przekonania, nadzieje i obawy. Ludzie kontaktują się, aby dowodzić (komenderować), informować, instruować, perswadować, zadziwiać, zachęcać innych, zachęcać siebie, unikać myślenia, zrozumieć, o czym myślą inni, sprawdzić swoją wiedzę, wprowadzić siebie w odpowiedni nastrój.

Ogólnie głównymi funkcjami komunikowania się są: informowanie, instruowanie, dowodzenie (komenderowanie) oraz wywieranie wpływu. W praktyce, oprócz czystych przypadków występowania poszczególnych funkcji, najczęściej spotyka się komunikowanie realizujące kilka funkcji jednocześnie, mające więc charakter złożony.

Komunikowanie informacyjne zmienia stan wiedzy odbiorcy. Jest to z pewnością jednym z celów edukacji i instruowania. Akt informowania w większości jest inicjowany przez odbiorcę, który poszukuje informacji dla funkcjonowania lub uznaje taką potrzebę w momencie zetknięcia się z informacją. Instruowanie zaś, przekazuje informację zawczasu, z wyprzedzeniem. Tak przekazywana informacja jest więc wykorzystywana dopiero w przyszłości. Wybór między informowaniem a instruowaniem dokonywany jest przez nadawcę informacji. Z punktu widzenia nadawcy informacji może być ona kształtowana jako instruująca i jako taka może być odbierana przez odbiorcę, który występuje w roli ucznia czy trenowanego. Jednakże w ogólnym rozrachunku to odbiorca decyduje o tym, czy informacja ma dla niego jakieś znaczenie i czy jest akceptowalna. Odbiorca nie wymaga tego, by nadawca był świadomy potrzeb odbiorcy i jego zamiarów wobec otrzymanej informacji. Bezpośredni dostawca informacji może być nieświadomy przekazywanej informacji, występując jedynie jako pośrednie ogniwo.

W jakiejkolwiek sytuacji społecznej, to czy komunikowanie ma miejsce i czy następuje asymilowanie informacji, zależy od potrzeb odbiorcy, jego woli szukania

i akceptowania informacji, jego dostępu do kanału przesyłania informacji oraz jego zdolności do wyodrębnienia informacji z wiadomości.

Wyraźnie zarysowana potrzeba informacji powstaje wtedy, gdy przewiduje się jakieś jej użycie; przy czym użycie to interpretowane powinno być szeroko. Nie może być ono ograniczane jedynie do zasilania informacyjnego procesu decyzyjnego lub do zmniejszania niepewności przy rozwiązywaniu problemów. Są to oczywiście przypadki często występujące w praktyce, jednakże powody wykorzystywania informacji są tak różne, jak różne są ogólne motywy ludzkiego działania. Dana aktywność, której służy związany z nią akt informacyjnego komunikowania się, jest indywidualna i unikalna. Jednakże istnieje związek między ową aktywnością a zajmowaną przez podejmującego tę aktywność pozycją społeczną. Dlatego też istnieje sieć powiązań pomiędzy pozycją społeczną, aktywnością, używaniem informacji, potrzebami informacyjnymi oraz zachowaniem się w sferze informacyjnego komunikowania. Jeżeli nawet pojawia się uświadomiona potrzeba informacyjna, to może nie starczać woli do poszukiwania lub zaakceptowania informacji, co wynika z poziomu motywacji.

Innym powodem, dla którego zaistnieć może brak woli poszukiwania lub zaakceptowania informacji, może być nadmiar wiadomości. Reakcją na przeładowanie informacyjne może być przeoczenie. Przeładowanie wiadomościami może być też przyczyną błędów. Te spostrzeżenia prowadzą znowu do kolejnych właściwości komunikowania społecznego. Ludzie przywiązują rzeczywistą uwagę jedynie do tych wiadomości, które uznawane są przez nich za informatywne, tzn. za pełne, wiarygodne i odpowiednie do ich potrzeb oraz możliwe do wykorzystania. Jeżeli informacja jest trudna do zrozumienia lub nie jesteśmy w stanie zaakceptować jej zasadności bądź nie widzimy możliwości wykorzystania jej w konkretnej sytuacji, zwykle ją ignorujemy.

Taki stosunek ma odniesienie i do źródeł informacji. Również one podlegają osądowi pod kątem pewności, wiarygodności, adekwatności i autorytatywności. Ten zaś zależy od ogólnej orientacji i pozycji społecznej użytkownika. To zaś ilustruje kolejną sieć powiązań między pozycją społeczną użytkownika informacji, autorytetem źródła informacji, woli akceptacji informacji oraz zachowaniem się w procesie społecznego komunikowania.

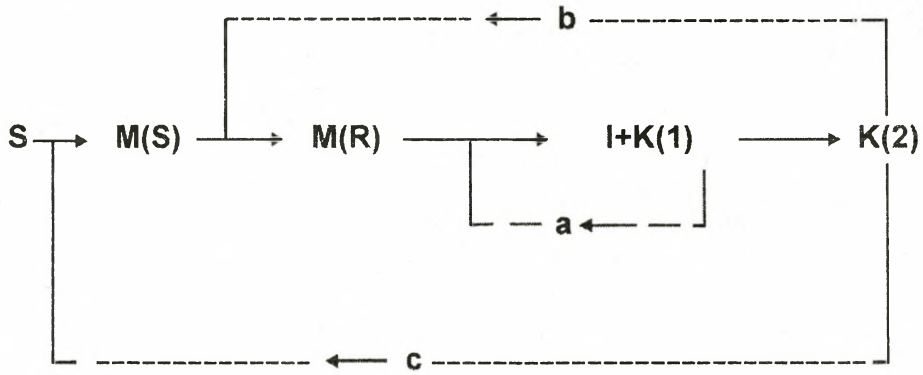
Reakcja odbiorcy informacji zależy od jego zdolności w zakresie wyodrębnienia informacji z wiadomości. Aby to się dokonało, nowa informacja musi być zasymilowana z istniejącą już u odbiorcy strukturą wiedzy. Struktura ta składa się z zestawu znanych i przyswojonych już koncepcji, kategorii i wartości. Struktura ta jest wykorzystywana w procesie odbioru nowej informacji. Zmienia się ona w zależności od zmian w pozycji społecznej, od stopnia edukacji i środowiska pracy. Często, to ograniczona wiedza jest przyczyną przeoczeń, niewłaściwych selekcji lub zniekształceń informacji. Indywidualna struktura wiedzy człowieka powstała z dwu rodzajów źródeł. Jednym jest asymilacja docierających od innych ludzi informacji w procesie komunikowania dokonującego się przez całe życie. Wiedza wywodzi się również przez przyswajanie informacji wyodrębnianej z wiadomości

płynących z niesterowanych interakcji ze środowiskiem naturalnym i indywidualnego kontaktu ze społeczeństwem.

Struktura wiedzy rozwija się więc dzięki ciągłemu przyswajaniu informacji, przez poddawanie się procesom edukacji i uczestnictwo w społecznym komunikowaniu. Tak więc kolejna sieć powiązań dotyczy pozycji społecznej, stopnia aktywności, generacji wiedzy i informacyjnego zasilania, struktury wiedzy, zdolności asymilacyjnych i zachowania się w sferze informacyjnego komunikowania.

Informacja może docierać do odbiorcy od informatora, którym może być osoba lub dokument. Osoba jako informator może być bezpośrednim źródłem informacji lub jedynie kanałem jej przekazu. Odbiorca może nie rozpoznawać właściwej roli. Obecnie coraz powszechniejsze staje się informowanie za pośrednictwem kanałów przekazu informacji. Wówczas źródło informacji może nawet nie wiedzieć, kto jest jej odbiorcą. Źródło informacji może więc wpływać na kanał jej przepływu. Ten zaś może wpływać na odbiorcę.

Już choćby z tego pobieżnego opisu wynika, że istnieje wiele współzależności między elementami społecznego procesu informacyjnego komunikowania się. Różne aspekty społecznego komunikowania się można przedstawić za pomocą modelu zobrazowanego na rys. 16.



Źródło: B. Vickery, A. Vickery, *Information Science in Theory and Practice*, London 1987, s. 42.

Rys. 16. Model informacyjnego transferu

Na modelu tym źródło S emituje wiadomość M(S). Jest ona transmitowana przez kanał, a w trakcie procesu tej transmisji może być modyfikowana do stanu M(R). Tego typu wiadomość dociera do odbiorcy i wyodrębniona z niej informacja I jest przez tego odbiorcę asymilowana. W konsekwencji stan odbiorcy zmienia się z K(1) na K(2).

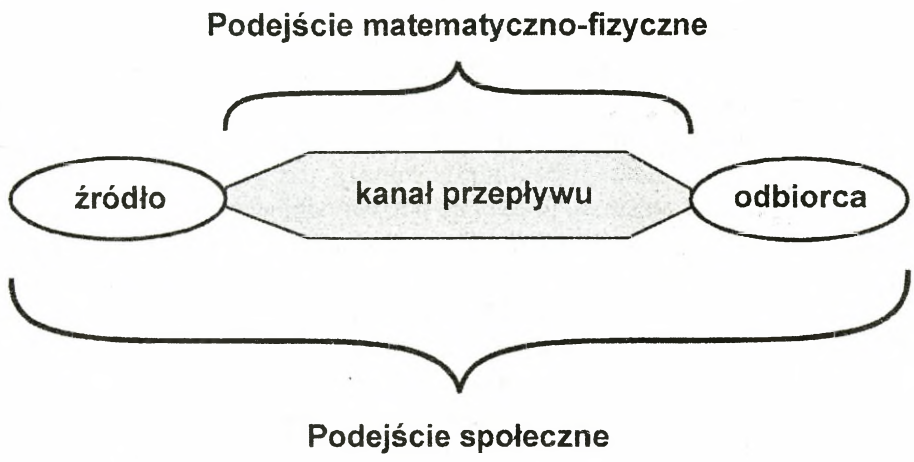
Model obrazuje ponadto trzy pętle sprzężenia zwrotnego. Krótsza z nich (a) z K(1) wskazuje, że informacja wyodrębniona z M(R) jest zależna od stanu K, przez co I nie jest prostą funkcją M(R). Górna pętla (b) od K(2) wskazuje, że w rezultacie otrzymania informacji jej odbiorca może próbować modyfikować re-

lacje pomiędzy M(S) a M(R), np. zwiększyć poziom głosu odbiornika radiowego, poprosić nadawcę o wyraźniejsze artykułowanie wiadomości, tak by zapewnić pomyślne przeprowadzenie transmisji. Najdłuższa pętla (c) z K(2) wskazuje, że odbiorca może próbować modyfikować emitowaną wiadomość: zmiana stanu zespołu automatycznej kontroli systemu ogrzewania przez człowieka jest tego przykładem, gdyż zamiarem tej interwencji jest inne sygnalizowanie stanu temperatury środowiska. Jakie więc implikacje dla początkowego modelu transferu informacji wynikają z tego rozszerzonego modelu? Model ten obrazuje sytuację, gdy człowiek, jako źródło informacji, celowo emituje wiadomości, które mają informować człowieka, odbiorcę aktywnie poszukującego wiadomości niosących pożądaną informację oraz kanał kontrolowany przez ludzi pragnących w jakiś sposób wpływać zarówno na źródło informacji, jak i jej odbiorcę. W rezultacie można uznać, że:

1. Informacja wydobyta z wiadomości przez konkretnego odbiorcę będzie w znacznym stopniu zależna od aktualnego stanu jego wiedzy oraz rodzaju zmiany jego stanu wiedzy wymaganej przez przyswojenie informacji. Od tego zależy, czy ta zmiana jest możliwa i pożądana dla odbiorcy.
2. Wydobyta z wiadomości informacja może jedynie w marginalnym stopniu odzwierciedlać to, co źródło informacji zamierza przekazać w wiadomości M(S) bądź to z powodu nieprecyzyjnego wyrażenia informacji w wiadomości, bądź też z powodu zniekształcenia jej przez kanał, przez co w zmodyfikowanej wersji M(R) stała się nie w pełni dostępna dla odbiorcy lub też z powodu niewłaściwego skoncentrowania się odbiorcy na odbiorze.
3. Relacja pomiędzy emitowaną a otrzymywaną informacją I będzie bliższa, gdy pętla sprzężenia zwrotnego (a) ma otwarty na wpływy charakter, a pętle (b) i (c) są aktywne. Tego typu sytuacja może najczęściej zaistnieć w nieformalnym, bezpośrednim komunikowaniu się ludzi twarzą w twarz; jest zaś mniej prawdopodobna w innych sytuacjach transferu informacji.
4. Wpływ kanału na przesyłane informacje jest ewidentny. Ludzie pełniący funkcje kanału lub kierujący działaniem kanału decydują o sposobie, czasie i wierności przesyłania informacji.

Informacyjna komunikacja jest wszechobecna w społecznych procesach. Rozpatrywana zaś w szerszym kontekście, komunikacja ta jest z natury powszechna. Materia, energia i informacja są trzema podstawowymi cechami tego świata.

Porównując podejścia matematyczno-fizyczne i społeczne teorii informacji warto zaznaczyć, iż **to drugie jest podejściem bardziej praktycznym. Obejmuje bowiem swoim zainteresowaniem zarówno kanał przepływu informacji, jak i jej źródło oraz odbiorcę** (rys. 17). **Z treści teorii informacji przyjmującej wzgląd społeczny wynika możliwość wpływania zarówno na informację przesyłaną kanałem przepływu, jak też na źródło generujące ją, a także na jej odbiorcę**. Modyfikując źródło, możemy kształtować wysyłane przez nie sygnały przeznaczone dla odbiorcy. Podobnie przekonując kogoś do złożenia pożądanego oświadczenia, rozmieszczając fałszywe obiekty czy zmniejszając powierzchnię odbicia samolotu wpływamy na generowane przez źródło sygnały przeznaczone dla odpowiedniego odbiorcy.



Opracowanie własne.

Rys. 17. Matematyczno-fizyczne i społeczne podejście teorii informacji

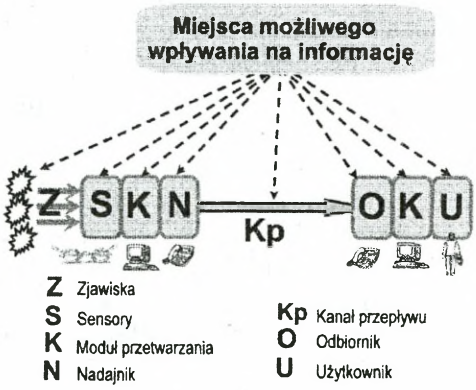
Klasycznym sposobem wpływania na kształt przeznaczonej dla odbiorcy informacji jest modyfikowanie jej w czasie transferu przez kanał przepływu. Istnieje wiele technik i sposobów, które zaliczane są do zakłócania kanałów przepływu. Może to być zapobieganie transferowi informacji, jej deformowanie, a nawet zamiana na fałszywą.

Również **ostatnie ogniwo przekazu, którym jest odbiorca, jest miejscem, w którym możliwe jest modyfikowanie płynącej do niego informacji**. Przykładowo, odbiorcę można oślepić i nie ujrzy napisanej informacji, można przytępić jego słuch, przez co nie usłyszy tego, co do niego płynie, można też zawczasu tak ukształtować jego stan psychiczny, że nie przyjmie do swojej świadomości płynącej do niego informacji. Jest to znane zjawisko działania propagandy, która tak kształtowała niektóre społeczeństwa, że uznawały za fałszywe płynące z zewnątrz prawdziwe informacje. W ten sposób, mimo że nie zniekształcono informacji przed dotarciem do odbiorcy, to efekt uzyskany przez oddziaływanie na niego był taki, jakby dostarczono mu inną informację. **W wyniku celowego działania można modyfikować zachowania odbiorcy, wpływając tym samym na ostateczną formę informacji docierającej do świadomości odbiorcy**.

Zmiany w społecznym komunikowaniu, jakie zaszły w drugiej połowie XX w., związane są z powszechnym zastosowaniem środków łączności i komputerów do tego procesu. W wyniku tego **rozbudowały się wszystkie komponenty procesu komunikowania społecznego.** Współczesne źródło informacji składa się najczęściej z jakiegoś sensora lub sensorów odbierających sygnały zewnętrzne. Sygnały te są zwykle w jakiś sposób modyfikowane i obrabiane. Bardzo często obróbka ta ma niezwykle skomplikowany charakter. Sygnały przetworzone na postać odpowiednią do charakteru nadajnika są w postaci danych przekazywane do niego. Ten

kieruje je do kanału przepływu. Kanał przepływu transferuje otrzymane dane do odbiornika odbiorcy. Odbiornik zaś przekazuje płynące dane do urządzenia przetwarzającego odbiorcy. Urządzenie to transformuje dane z postaci dogodnej do przesyłania na postać odpowiednią dla odbiorcy. Moduł ten zarówno przetwarza dane na formy odbieralne przez ludzkie zmysły, jak też dokonuje agregacji i przetwarzania, które dopasowuje dane do potrzeb odbiorcy. Operacje te w idealnej postaci zamieniają dane na informację, a więc selekcjonują dane zgodnie z potrzebami odbiorcy i transformują na postać najlepiej absorbowalną przez odbiorcę, zwiększając jego wiedzę w pożądanym obszarze. Jak słusznie zauważył Stanisław Lem, „[...] człowiek posiada *informacyjną przepustowość* obecnie taką samą, jak 100 000 lat temu", dlatego też obecnie „[...] potrzebne są nam nie sieci bezmyślne, nie utysiąckrotnione telefony, faksy, interakcyjne media, lecz ulokowane w sieci odpowiedniki wartościującej informację inteligencji, która wszystko, co jest informacyjnym śmieciem, pochłaniałyby i jako filtry zezwalały jedynie na przepływ wiadomości oraz wizualnych treści ani nie propagujących zła i głupoty, ani nie szkodzących wszystkiemu, co by mogło stać się dla człowieka pożyteczne"[155]. W szerszym kontekście nie tylko chodzi o selekcjonowanie „złych" i „głupich" informacji, lecz o dobór odpowiedni do potrzeb. Niewątpliwie głównym komponentem modułów przetwarzania są różnego rodzaju komputery.

Z powyższego wynika, że **ilość elementów procesu społecznej komunikacji jest w rzeczywistości większa niż w podstawowym modelu teoretycznym. Ponadto wszystkie są podatne na jakieś formy wpływania na transferowaną przez nie informację** (rys. 18).



Opracowanie własne.

Rys. 18. Miejsca możliwego modyfikowania treści informacji

[155] S. Lem, *Bomba megabitowa*, Kraków 1999, s. 12–13.

3. GENEZA, ISTOTA I ROZWÓJ OPERACJI INFORMACYJNYCH

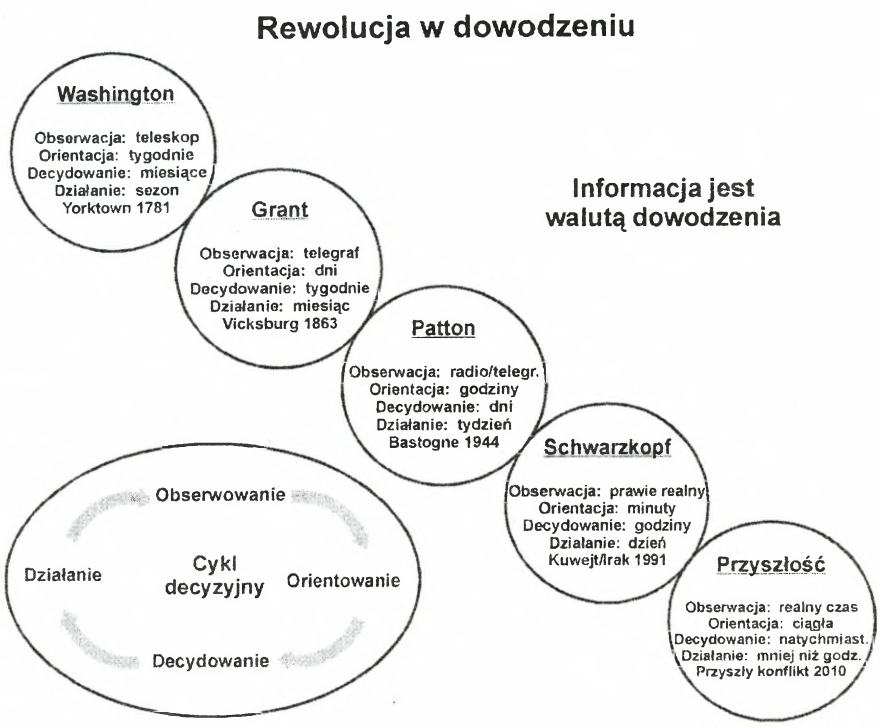
Główną wartością nowej cywilizacji XXI w. jest informacja i systemy jej zdobywania, przetwarzania i dystrybucji. Każda sfera funkcjonowania współczesnego społeczeństwa staje się coraz bardziej zależna od informacji. Ponadto dokonuje się masowy proces automatyzacji i robotyzacji, który jest możliwy dzięki komputeryzacji systemów kierowania. Wszystkie te zjawiska pogłębiają się dzięki możliwości szybkiego przesyłania informacji pomiędzy praktycznie nieograniczoną rzeszą użytkowników. Dla potrzeb zbliżonego do czasu realnego zasilania informacyjnego coraz większych rzesz użytkowników, ciągle się rozbudowuje sieci telekomunikacyjne i łączy je razem, co powoduje, że bardzo szybko rozrasta się globalna infrastruktura łączności. Infrastruktura ta staje się tak rozbudowana, że praktycznie niemożliwe jest wzbranianie dostępu do niej. To tworzy wrażliwość powstającej cywilizacji postindustrialnej. Jest ona niemalże całkowicie uzależniona od informacji i systemów informacyjnych. Jednocześnie łatwo z tej wrażliwości korzystać, poprzez powszechny dostęp do globalnej sieci informacyjnej.

Informacja do wygrywania wojny wykorzystywana była od dawna. Generał Lee w 1863 r. pokonał dwukrotnie silniejszego przeciwnika, mając przewagę informacyjną i odpowiednio ją wykorzystując do kierowania walką. Również w czasie drugiej wojny światowej alianci, wykorzystując rozszyfrowane przez siebie tajne informacje Niemców, mogli wielokrotnie paraliżować niemieckie inicjatywy, m.in. w Północnej Afryce, we Włoszech, w Normandii. Takich przykładów jest wiele. Informacja jest walutą dowodzenia.

Informacyjny wiek jest nową erą dla sił lądowych USA. W czasie wojny domowej kurier i telegraf były podstawowymi środkami łączności. To pozwalało dowódcy orientować się w sytuacji w czasie kilkunastu dni, podejmować decyzje w ciągu kilku tygodni i realizować je w ciągu miesiąca. W czasie drugiej wojny światowej podstawowym środkiem łączności było radio. Pozwalało na orientowanie się w sytuacji w ciągu godzin, decydowanie w ciągu dni i wykonywanie decyzji w ciągu tygodnia. Generał Schwarzkopf w czasie wojny z Irakiem obserwował sytuacje niemalże w czasie rzeczywistym, orientował się w czasie minut, decydował w czasie godzin i wcielał decyzje w czyn tego samego dnia[156] (rys. 19).

---

[156] R. Szpyra, *Walka informacyjna w przyszłych działaniach sił powietrznych*, Praca badawcza pod krypt. *„CYBERAWIATOR"*, Warszawa 2000, s. 6, 49–50.



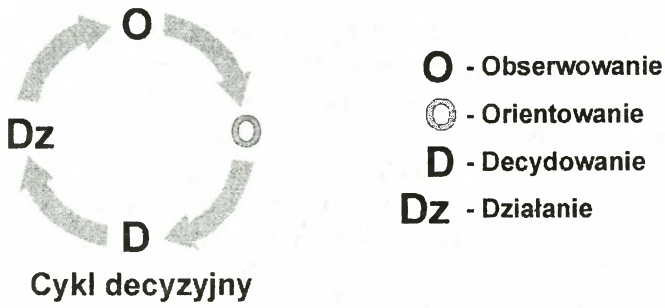
Źródło: *Army Focus 94. Force XXI. America's Army in the 21st Century*. Department of the Army, Washington D.C. 1994, s. 18.

Rys. 19. Rewolucyjne zmiany w dowodzeniu

W wyniku rozwoju elektroniki w toku automatyzacji procesów dowodzenia i kontroli uświadomiono sobie jeszcze bardziej konieczność dążenia do osiągania przewagi informacyjnej. Przewaga ta w połączeniu ze skracaniem cyklu decyzyjnego stała się podstawowym czynnikiem przewagi w dowodzeniu. W literaturze Zachodu często proces decyzyjny przedstawiany jest w postaci uproszczonego czterostopniowego modelu (rys. 20).

W modelu tym zamknięty powtarzający się cykl składa się z obserwowania (zbierania informacji), orientowania (poznania sytuacji), decydowania, działania i ponownego obserwowania rezultatów działania oraz sytuacji, orientowania się w nowej sytuacji podejmowania kolejnej decyzji, działania. Jest oczywiste, że jakość działania zależy od jakości informacji, gdyż ta bezpośrednio wpływa na decyzje.

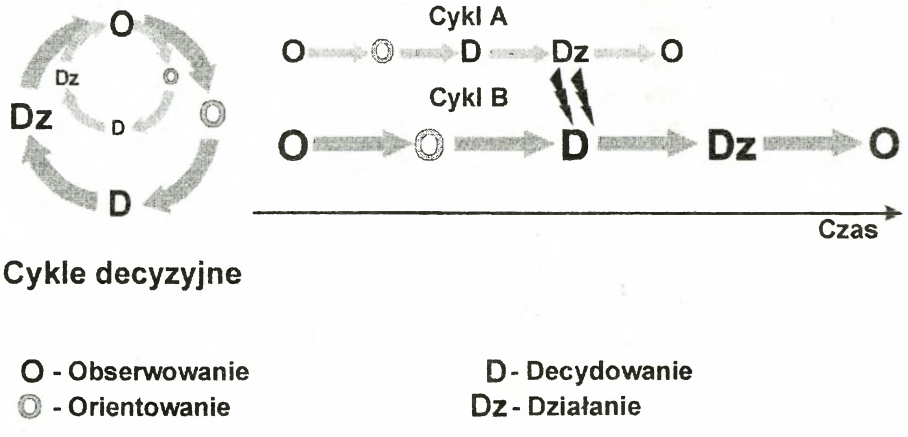
W procesach walki dąży się do zwiększania racjonalności własnego działania oraz pogarszania racjonalności w działaniach przeciwnika. Wobec znaczenia informacji zmierza się do zapewnienia sobie jak najlepszej informacji oraz uniemożliwienia lub ograniczenia przeciwnikowi dostępu do informacji.



Opracowanie własne.

Rys. 20. Model cyklu decyzyjnego

Kolejnym czynnikiem jest dynamika cyklu decyzyjnego wpływająca bezpośrednio na inicjatywę w działaniu. Gdy cykl decyzyjny jednej strony jest krótszy od cyklu drugiej, wówczas strona mająca krótszy cykl decyzyjny przejmuje inicjatywę w działaniu, a strona mająca ten cykl dłuższy musi dostosowywać swoje działanie do aktywności przeciwnika. Jeden z wariantów takiej sytuacji zobrazowano na rys. 21.



Opracowanie własne.

Rys. 21. Różne cykle decyzyjne

Widać na nim wyraźnie, że strona mająca krótszy cykl decyzyjny „A" już podejmuje działanie, podczas gdy strona „B" jest dopiero na etapie decydowania. W tej sytuacji będzie musiała reagować na działania przeciwnika. Wnika z tego, że oprócz walki o przewagę w jakości informacji, toczy się również walka o wyprze-

dzenie przeciwnika w cyklu decyzyjnym. Innymi słowy, ten, kto szybciej pozyska lepszą informację i szybciej zrealizuje swój cykl decyzyjny, uzyskuje co najmniej inicjatywę. Według teoretyków i praktyków Zachodu jest to istota przewagi w dowodzeniu i kontroli. Walka o uzyskanie takiej przewagi polega przede wszystkim na zapewnianiu sobie lepszej informacji i szybszych procesów decyzyjnych oraz na niedopuszczaniu do osiągnięcia tego samego przez przeciwnika. **Walka tego typu nazywana jest *Command and Control Warfare* (C2W), a jej istotą jest walka o przewagę w dowodzeniu**, a koncepcja tej walki była próbą integracji różnych działań w sferze informacyjnej w zorganizowaną całość. Walka ta przez niektóre źródła początkowo była utożsamiana z walką informacyjną. Obecnie w dalszym ciągu niektórzy traktują ją jako synonim walki informacyjnej.

Według treści amerykańskiej doktryny połączonej[157] walka o przewagę w dowodzeniu to: ***Zintegrowane wykorzystanie bezpieczeństwa działań (OPSEC), mylenia, działań psychologicznych (PSYOPS), walki elektronicznej (EW) i fizycznej destrukcji wspólnie wspieranych przez rozpoznanie w celu izolowania od informacji, wpływania, degradowania lub niszczenia systemów dowodzenia i kontroli, przy zabezpieczaniu własnych tego typu systemów przed podobnymi akcjami.***

W NATO walka o przewagę w dowodzeniu (*command and control warfare* – C2W) jest pierwotnie zdefiniowana w dokumencie MC-348, a następnie w innych dokumentach, jako[158]: ***zintegrowane użycie wszystkich możliwości wojskowych, włączając w to bezpieczeństwo działań (OPSEC), dezinformację, działania psychologiczne (PSYOPS), walkę elektroniczną (EW) i niszczenie fizyczne, wspierane przez wszystkie rodzaje rozpoznania oraz systemy łączności i informacyjne (CIS) w celu uniemożliwienia dostępu do informacji, jej modyfikowania oraz uszkadzania lub niszczenia potencjału dowodzenia i kontroli (C2) przeciwnika, przy jednoczesnej ochronie własnego potencjału przeciw podobnym jego akcjom.***

Podczas gdy walka o przewagę w dowodzeniu koncentruje się na dowodzeniu militarnym i kontroli w czasie użycia sił zbrojnych, to największe zainteresowanie wzbudziła ta część walki informacyjnej, która lokuje się poza obszarem tradycyjnego pola walki. Ten obszar zainteresowania jest uważany za najbardziej obiecujący. Rozwój technologiczny w elektronice, komunikacji, elektrooptyce i systemach komputerowych, w połączeniu ze znanymi formami działań, takimi jak działania psychologiczne i mylenie, oferują nowe formy osiągania celów narodowego bezpieczeństwa. Walka informacyjna może zniszczyć zdolność społeczeństwa do prowadzenia wojny bez wystrzelenia jednego pocisku poprzez destrukcję jego informacyjnej infrastruktury. W obszarze walki informacyjnej terytorium nie stanowi gwarancji jakiegokolwiek sanktuarium, granice są skrycie penetrowane w ciągu milisekund, a obiekty ataku są wszędzie. Przyszłe obiekty ataku należeć będą nie tylko do systemów militarnych, lecz także do infrastruktury cywilnej, takiej jak: sieci bankowe, telekomunikacyjne, energetyczne, transportowe czy rurociągowe.

---

[157] JP 3-13: *Joint Doctrine for Information Operations*, Washington 1998, s. GL 4.

[158] Między innymi w: AJP-01(B), *Glossary 3*, a także w AAP-6.

To cywilne zaangażowanie prowadzi do sedna obserwowanej ostatnio ewolucji walki informacyjnej. Wymyślona początkowo przez Departament Obrony USA koncepcja wewnętrznej odpowiedzi, wykorzystująca zarówno możliwości, jak i wrażliwości wynikające z informacyjnej eksplozji, okazała się rozleglejsza niż militarna sfera zainteresowania. Jeżeli realna użyteczność ofensywnej walki informacyjnej odnosi się również do pokoju, jak też do początkowych faz kryzysu, to dla uzyskania sukcesu niezbędne jest bezpośrednie zaangażowanie najwyższych władz państwowych oraz ścisła koordynacja i uczestnictwo wielu agend rządowych. Podobnie najbardziej zniechęcającym wyzwaniem jest nie tyle wpływ defensywnej walki informacyjnej na militarną efektywność, co raczej wrażliwość narodowej infrastruktury. Globalna eksplozja informacyjna jest bronią obosieczną. Równie łatwo jak my możemy zaatakować przeciwnika, on może zaatakować nas. Im bardziej stajemy się skomplikowani, tym większa staje się nasza wrażliwość. W 1994 r. Połączona Komisja Bezpieczeństwa USA oznajmiała w swoim raporcie: *jeżeli zamiast atakowania naszych systemów militarnych i baz danych nieprzyjaciel zaatakowałby nie zabezpieczoną cywilną infrastrukturę, ekonomiczne i inne skutki byłyby katastrofalne*[159].

Innym wymiarem walki informacyjnej jest wpływ mediów, takich jak CNN. Informacyjna rewolucja z bezpośrednimi transmisjami z pola walki spowodowała zmiany tej walki. Wizualne przedstawienie konfliktu w niemal realnym czasie zintensyfikowało niechęć do śmierci i wojennej destrukcji na całym świecie, co nieprzyjaciel może eksploatować. Amerykański rząd jest przekonany o konieczności pełnego zaangażowania w wojnę mediów przez transmitowanie swoich własnych wiadomości, szczególnie w początkowej fazie kryzysu. Jest to klucz do sukcesu informacyjnego odstraszania.

Potencjalne wrażliwości organizacji wykorzystujących sieci informatyczne związane z uzależnieniem od nich i małą troską o ich bezpieczeństwo, zostały bardzo szybko dostrzeżone i wykorzystane. Jest już wiele informacji na ten temat. Warto przytoczyć charakterystyczne przykłady.

„[...] W 1994 r. grupa rosyjskich hackerów ukradła kody i hasła klientów Citibanku, dzięki czemu zdołała przekazać dziesięć milionów dolarów na zamorskie konta. Sześciu Rosjan, jak podaje „NY Herald", zostało wszakże poddanych ekstradycji i przyznało się do przestępstwa. Według banku, udało się odzyskać pieniądze, z wyjątkiem 400 000 dolarów. [...]

Sumaryczne straty, jakie ponoszą amerykańskie korporacje rocznie, kiedy ów pojedynek, czy raczej ową milczącą, bo cichą elektroniczną wojnę przegrywają, oceniają eksperci na kwotę trzystu miliardów dolarów, czyli straty są mniej więcej porównywalne z ekonomicznymi stratami ponoszonymi w wojnie najzupełniej „normalnej". Głównymi bastionami jako celami ataków są chlubiące się światową supremacją przemysły, jak komputerowy, jak skoncentrowany na produkcji pro-

[159] B.E. Fredericks, *Information Warfare at the Crossroads*, „Joint Force Quarterly" 1997, Summer, s. 98–99.

gramów (*software*) i półprzewodników, jak molochy farmaceutyczne oraz wszystkie ośrodki, obsługujące zapotrzebowanie na broń"[160].

„[...] Zaczęło się wszystko od zbuntowanego dwudziestolatka ze skłonnościami do *science fiction,* komputerów i narkotyków, o pseudonimie Captain Hagbard. To on rozkręcił w 1985 r. hakerską akcję w Hanowerze, która dla niego samego zakończyła się samobójstwem, a dla kilku innych procesem sądowym.

»To niesamowite, że Hagbard potrafił włamać się do komputera w NORAD« – opowiadał później jeden z komputerowych maniaków z Hanoweru. Już w 1985 r. miał okazję oglądać niektóre z hakerskich sztuczek tego komputerowego pirata, który wyruszał w swoje wyprawy po informatyczne dane pod pseudonimem, zapożyczonym z powieści *science fiction.* Pod koniec 1985 r. Hagbard prezentował przy różnych okazjach sposób dotarcia do komputera amerykańskiego Dowództwa Obrony Powietrznej i Bombowców Strategicznych. Najczęściej droga prowadziła przez Fermi National Accelerator Laboratory (Fermilab), Laboratorium Badań Jądrowych w pobliżu Chicago, w którego sieci Hagbard czuł się jak w domu. Komputery serii VAX były jego komputerową ojczyzną. [...]

Dla Hagbarda dobrze się składało, że w Hanowerze znalazło się kilku hakerów, których zafascynowała możliwość włamania się do wojskowych komputerów połączonych siecią Milnet. Początkowo była to zabawa. Niewielka paczka hakerów z Hanoweru, do której należeli też profesjonalni programiści, interesowała się oprogramowaniem sieciowym i »inteligentnymi« programami. Bardzo chcieli podejrzeć, co robią inni, żeby wiedzieć więcej niż konkurencja. Tak właśnie ujął to jeden z hakerów o pseudonimie Brainware. [...]

Hakerzy niemal osiągnęli swój cel. Znaleźli drogę do bazy danych Pentagonu oraz centrów badań jądrowych Los Alamos i Lawrence Livermore. Jednak szczególnie fascynował ich SAC. „Przez około 5 godzin byliśmy w SAC, w taktycznej grupie symulacyjnej Dowództwa Lotnictwa Strategicznego" – opowiadał jeden z hakerów biorących udział we włamaniu do wojskowej bazy danych na Sesji Hakerów w 1986 r. – „Otworzyliśmy serwer". Z odrobiną szczęścia i sprytu udało się przeniknąć do maszyny. Niezwykle pomocny okazał się napisany przez nich program, znany później pod nazwą „kukułcze jajo".

„Kukułcze jajo" umieszczano w obcym komputerze, a następnie uruchamiano jako podrzędny program. Zapewniał on hakerom, jako superuserom, pełną kontrolę nad komputerem. [...]

Już we wrześniu 1986 r. Stoll odkrył wojskową „bazę wypadową" hakerów: Redstone Anny Depot w Anniston w stanie Alabama. To stąd przeprowadzano większość udanych skoków komputerowych, a włamano się nie tylko do Dowództwa Lotnictwa Strategicznego. Ta wojskowa baza należy do tego samego dowództwa co White Sands Missile Range w Nowym Meksyku, gdzie testuje się rakiety, które następnie przesyła się do Anniston. Na należących do niej komputerach opracowywano przede wszystkim zamówienia i problemy w zaopatrzeniu.

[160] Zob. S. Lem, *Bomba...* s. 171, 173.

Przez całe miesiące przesiadywali tu hakerzy z Hanoweru, przeszukali całą bazę danych, wykradli plik z hasłami dostępu i przez cztery miesiące wykonywali stąd dalsze komputerowe skoki. Przenosili się dalej, np. do centrów badań jądrowych Los Alamos i Lawrence Liyermore oraz do baz danych Pentagonu OPTIMIS i RECON. Ktoś, kto powinien o tym wiedzieć, stwierdził, że sporo stąd wyczytano. [...]

Na ich liście znajdowały się nie tylko komputery wojska, ale również firm zbrojeniowych specjalizujących się w elektronice. W grudniu 1986 r. jeden z hakerów podłączył się na wiele godzin do TRW w Redondo Beach w Kalifornii. TRW jest zakładem produkującym na potrzeby Air Force i NSA, dostarcza komputery i satelity szpiegowskie KH-11. KH oznacza tutaj key hole, czyli dziurkę od klucza. Haker poszukiwał danych o tym szpiegowskim satelicie, ale tego, co rzeczywiście mógł przeczytać, firma nie zdradziła"[161].

Opublikowana w 1992 r. przez Departament Obrony[162] Dyrektywa TS3600.1 zawierała zarys koncepcji walki informacyjnej. Była ona w istocie zbiorem wytycznych do dalszych badań i dyskusji. Jej szersze implikacje wyłoniły się z czasem w rezultacie studiów, gier wojennych i konferencji. Od początku szersze rozumienie walki informacyjnej ograniczane było przez sprawy bezpieczeństwa. Brak rozstrzygających detali definicji odnoszących się do sfery publicznej potęgowany był przez przedłużającą się nieobecność jawnej definicji walki informacyjnej.

W styczniu 1994 r. opublikowano pierwsze poważne rządowe wyjaśnienie sensu walki informacyjnej. Zawarte ono było w raporcie sekretarza obrony. Mimo iż raport ten nie zawierał definicji, to jednak stwierdzał, że ***walka informacyjna składa się z działań podejmowanych dla zachowania integralności własnych systemów informacyjnych i ich ochrony przed eksploatacją, degradacją lub destrukcją, przy jednoczesnym eksploatowaniu, degradowaniu lub destrukcji systemów informacyjnych przeciwnika oraz osiąganie przewagi informacyjnej w procesie użycia sił zbrojnych.***

Ten opis wyraźnie podkreśla ofensywne i defensywne aspekty walki informacyjnej. Co więcej, raport stwierdzał, że jest to zintegrowana strategia, która uaktywnia bardziej zdecydowane działania, zwiększając prawdopodobieństwo ich sukcesu i minimalizując straty.

Zdolność do izolowania przeciwnika od środków prowadzenia wojny przez zniszczenie jego systemów informacyjnych tworzy głęboki efekt odstraszający. Walka informacyjna ma potencjał wypełnienia luki między sankcjami a bojowym użyciem sił zbrojnych. Jej odstraszająca wartość zwiększa się wraz z tym, jak potencjalny nieprzyjaciel orientuje się w jej efektywności i naszej woli jej użycia.

Zainteresowanie defensywną walką informacyjną systematycznie rosło w ciągu ostatnich lat. Jak stwierdziła Agencja Obrony Systemów Informacyjnych USA, w 1996 r. ponad 95% globalnych potrzeb telekomunikacyjnych Departamentu Obrony było zaspokajanych przez cywilnych komercyjnych usługodawców tele-

[161] E.R. Koch, J. Sperber, *Infomafia, szpiegostwo komputerowe, handel informacją, tajne służby*, Gdynia 1999, s. 238–247.

[162] B.E. Fredericks, s. 97–98.

komunikacyjnych, a establishment obronny jest integralną częścią rosnącej globalnej infrastruktury informacyjnej, która wykracza poza przemysł, media i siły zbrojne. Defensywna walka informacyjna identyfikuje i zabezpiecza wrażliwe miejsca, które tworzą się w wyniku rosnącej zależności od światowej infrastruktury informacyjnej.

Utworzenie Prezydenckiej Komisji ds. Ochrony Krytycznej Infrastruktury w 1996 r. podkreśliło rosnącą świadomość potrzeby opracowania narodowej strategii ochrony funkcjonowania żywotnej dla kraju infrastruktury. Dotyczy to szczególnie systemów telekomunikacyjnych, finansowych, energetycznych, wodnych, rurociągowych i transportowych. Rosnąca zależność od wysoko rozwiniętych technologii jest nicią łączącą te systemy. Zagrożenie lokuje się w dwóch jego kategoriach: bardziej tradycyjne zagrożenia fizyczne i te powstające w wyniku zastosowania elektroniki, częstotliwości radiowych lub ataków typu komputerowego na informację, lub komunikacyjne komponenty, które kontrolują krytyczną infrastrukturę. Celem działań prezydenckiej komisji jest proponowanie rozwiązań, które dotrzymywałyby kroku wyłaniającym się zagrożeniom w szybko zmieniającym się środowisku technologicznym. Integralną częścią pracy komisji jest ustanowienie kompletnego programu obejmującego sektor prywatny.

W dyskusji nad zagadnieniami walki informacyjnej uczestniczyli nie tylko wojskowi, ale także szerokie kręgi specjalistów cywilnych. Jednym z pierwszych takich badaczy, którzy zajęli się tą problematyką, był Winn Schwartau. Już w 1993 r. wydał w formie książkowej obszerny zbiór materiałów dotyczących szeroko rozumianej problematyki walki informacyjnej. W 1996 r. pojawiło się kolejne, jeszcze obszerniejsze wydanie[163]. Oto kilka istotnych spostrzeżeń tego autora.

„[...] Fundamenty współczesnego społeczeństwa oparte są na dostępności do informacji, która zabezpiecza prosperującej ekonomii wzrost lub spycha słabą w uzależnienie od silniejszej. W dzisiejszym elektronicznie wzajemnie połączonym świecie, informacja przemieszcza się z prędkością światła, jest nieuchwytna i niezmiernie wartościowa. Dzisiejsza informacja jest ekwiwalentem wczorajszych fabryk, lecz jest dużo bardziej wrażliwa.

Obecnie Stany Zjednoczone przodują w świecie w zakresie rozbudowy globalnie spiętego sieciami informacyjnymi społeczeństwa. Społeczeństwo to wkracza w wiek informacji, gdzie informacyjne i ekonomiczne wartości stają się niemal synonimami. Ponad 125 milionów komputerów połączonych ze sobą przez kompleksowe lądowe i kosmiczne systemy łączności, stanowi podstawę ponad gigantycznej ekonomii, która zależna jest od ciągłych i pewnych operacji. Walka informacyjna jest elektronicznym konfliktem, w którym informacja jest strategicznym dobrem wartym podboju lub destrukcji. Komputery i inne komunikacyjne i informacyjne systemy stają się atrakcyjnymi obiektami pierwszego uderzenia.

---

[163] W. Schwartau, *Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, New York 1996.

Współczesny złodziej może ukraść więcej z komputerem niż z karabinem. Jutrzejszy terrorysta może być w stanie dokonać więcej zniszczeń za pomocą klawiatury niż za pomocą bomby. [...]

Walka informacyjna jest integralnym komponentem nowego ekonomicznego i politycznego porządku światowego. Ekonomiczne bitwy są toczone i będą toczone, wpływając na każdego amerykańskiego obywatela i każdą firmę, jak również na bezpieczeństwo narodowe Stanów Zjednoczonych. Współczesny terroryzm to nie tylko ataki na linie lotnicze i systemy zaopatrzenia w wodę, ale także na systemy zasilania pieniężnego, to formy terroru uderzającego w miliony ludzi za pomocą pojedynczego uderzenia klawisza. [...]

Cyberprzestrzeń jest całkowicie nowym światem, który tylko luminarze, tacy jak Marshall McLuhan i Arthur C. Clarke, ujrzeli w oczach swojej wyobraźni, lecz nawet oni nie byli w stanie przewidzieć niepewności, jaka zapanowała w ciągu ostatnich dwu dekad. Wyobraźmy sobie świat, gdzie informacja jest medium wymiany, a gotówka używana jest jedynie do zakupów podręcznych – świat, gdzie informacja, a nie język angielski, niemiecki, japoński czy rosyjski jest wspólnym językiem; świat, gdzie potęga wiedzy i informacji może uzurpować sobie siłę równą militarnej; świat całkowicie uzależniony od nowych narzędzi wysokiej techniki, która czyni informację dostępną permanentnie komukolwiek, gdziekolwiek, w każdym czasie; świat, gdzie ten, kto kontroluje informację, kontroluje ludzi; świat, gdzie elektroniczna prywatność już nie istnieje.

Teraz wyobraźmy sobie konflikt między przeciwnikami, w którym informacja jest wygraną, wojennym łupem – konflikt ze zwycięzcą i pokonanym; konflikt, który określa komputery i systemy komunikacyjne (łączności) jako podstawowe cele zmuszone do samoobrony przeciwko zabójczym, niewidzialnym kulom i bombom.

Wyobraźmy sobie rywalizujące ekonomie, które walczą o poszerzenie strefy globalnego wpływu na elektroniczne, finansowe infostrady, nie poświęcając żadnych wydatków dla zapewnienia zwycięstwa. Następnie wyobraźmy sobie świat złożony z firm, które rywalizują i rozwiązują spory za pomocą regularnych, wzajemnych najazdów – blitzkriegów na informacyjne infrastruktury; świat, gdzie elektroniczne i rywalizacyjne szpiegostwo jest oczekiwaną manierą prowadzenia biznesu.

Ponadto wyobraźmy sobie świat, w którym osobisty rewanż i odwet są w zasięgu uderzenia klawisza. Jakiego rodzaju jest to świat? To jest świat walki informacyjnej, a my jako jednostki i jako kraj nie jesteśmy przygotowani na przyszłość, którą sobie tworzymy. [...]

Walka informacyjna jako broń informacyjnego wieku zamieni bomby i naboje. Te bronie nie są już dłużej zastrzeżone dla rządu, CIA lub KGB. Komputerowe i informacyjne bronie są dostępne z katalogów i sklepów. Te arsenały mogą być budowane przez hobbystów w domu. Oczywiście, siły zbrojne rozwijają swoje arsenały broni, którymi prowadzi się walkę informacyjną.

Walka informacyjna dotyczy pieniędzy. Odnosi się do dystrybucji dóbr i polega na niedopuszczaniu ich do oponenta. Walka ta rodzi informacyjnych wojowników, którzy toczą walki na wskroś globalnej sieci w grze cyberryzyka.

Walka informacyjna dotyczy władzy. Ten, kto kontroluje informację, kontroluje pieniądze.

Walka informacyjna dotyczy także strachu. Ten, kto kontroluje informację, może zaszczepić strach tym, którzy chcą trzymać swoje sekrety w ukryciu. To jest strach, że np. bank Nowego Jorku upadnie, gdy tylko na jeden dzień powstanie w nim deficyt 23 miliardów dolarów i zostanie to ujawnione.

Walka informacyjna dotyczy także arogancji, arogancji płynącej z przekonania, że popełnia się przestępstwo doskonałe.

Walka informacyjna dotyczy też polityki. Gdy niemiecki rząd sponsoruje agencję wywiadowczą włamującą się do amerykańskich komputerów, koncepcja sojusznika powinna być zdefiniowana od nowa. Także gdy Iran bierze na cel amerykańską ekonomię przez sponsorowane przez rząd fałszerstwa, powinno to być dla nas sygnałem, że konflikt nie jest tym, czym był kiedyś.

Walka informacyjna dotyczy przeżycia. Francja i Izrael rozwinęły swoje ekonomie i oparły całe gałęzie przemysłu na kradzieży amerykańskich sekretów. Japonia i Korea przy pomocy swoich rządów kradną amerykańską technologię, gdy tylko schodzi ona z desek kreślarskich.

Walka informacyjna dotyczy wyzwań. Z zaniedbanych dzielnic cyberprzestrzeni zjawią się hakerzy marginesu społecznego nie mający nic do stracenia. Część z nich zorganizuje się w działające w cyberprzestrzeni gangi, zorganizowaną przestępczość cyberprzestrzeni. Uznają oni i docenią korzyści ekonomiczne płynące z prowadzenia walki informacyjnej.

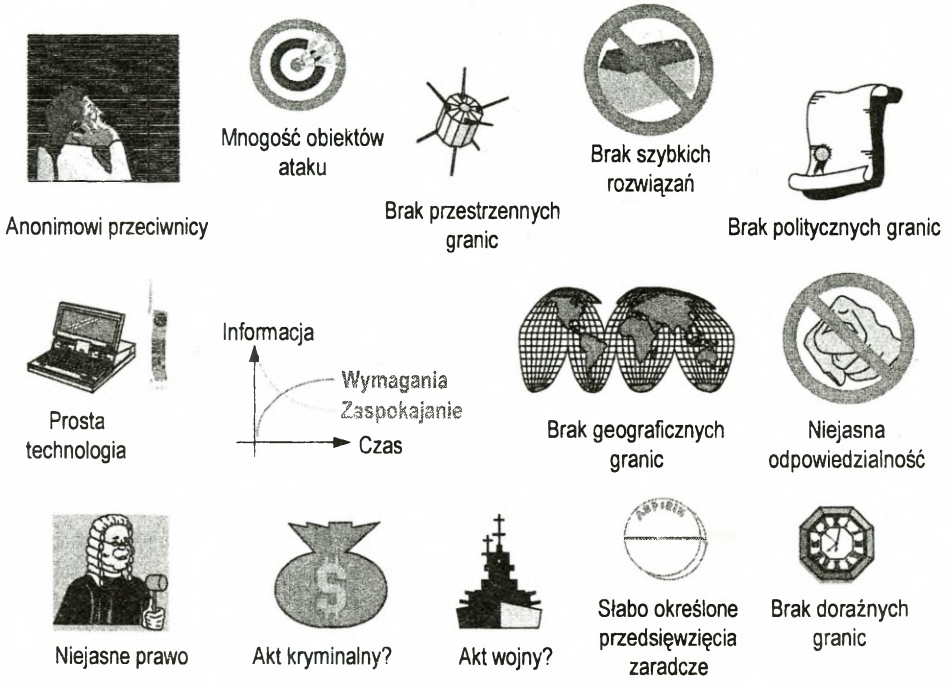
Walka informacyjna dotyczy także kontroli informacji. Jako społeczeństwo utrzymujemy coraz to mniej i mniej kontroli nad tym, jak cyberprzestrzeń się rozszerza i rozprzestrzenia się elektroniczna anarchia. Z uwagi na globalne warunki lat 80. i 90. walka informacyjna jest nieunikniona. Dzisiejsza planeta oferuje dojrzałe warunki do walki informacyjnej, warunki, które nie były przewidywane nawet kilka lat temu.

Walka informacyjna kosztuje Stany Zjednoczone około 100–300 miliardów dolarów rocznie i finansowy wpływ na ekonomię tego kraju zwiększa się z każdym rokiem. Prawie 5% produktu krajowego USA wyślizguje się przez globalną sieć spoza kontroli narodowej, osłabiając tym samym wysiłki czynione w kierunku ograniczania deficytu budżetowego, negatywnie wpływając na potencjał eksportowy i nierównowagę eksportową. [...]

Jednak roczne straty w wysokości ponad 200 miliardów dolarów dotyczą głównie ludzi – około ośmiu milionów ludzi mogłoby mieć pracę, gdyby nie efekty walki informacyjnej. Ludzie ci są również ofiarami walki informacyjnej. Walka informacyjna korzysta z uzależnienia od współczesnych automatycznych skomputeryzowanych drobiazgów.

Zagrożenie przyszłym komputerowym Czernobylem nie jest gołosłowne. Jest tylko kwestią: kto i kiedy. Walka informacyjna jest dostępna dla każdego, kto ma plan i odpowiedni stosunek do tego przedsięwzięcia. Walka ta może być prowadzona na trzech wyraźnych poziomach intensywności, każdy ze swoimi celami, metodami i obiektami"[164].

Naturę walki informacyjnej ilustruje rysunek 22.



Źródło: *Information Warfare. Legal, Regulatory, Policy and Organizational Considerations for Assurance*, 2nd edition, Washington 1996, s. 3.

Rys. 22. Natura walki informacyjnej

Mimo wyraźnego związku wyłaniającej się walki informacyjnej z postępem cywilizacyjnym końca XX w., L. Ciborowski jest słusznie przekonany, że:

„[...] Historia walki informacyjnej jest tak samo długa, jak historia ludzkich dziejów. Nikt jej jednak nie spisał. Co więcej – nigdy nawet nie używano takiego pojęcia. Nie oznacza to jednak, że kojarzone z nią dziś funkcje zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej zaistniały dopiero u schyłku XX w. Istniały zawsze. Teraz unaoczniają się tylko z niewspółmiernie większą wyrazistością. Postępująca politechnizacja życia i szybki rozwój szeroko rozumianej komunikacji spowodowały, że samo słowo *informacja* stało się dziś

[164] Tamże, s. 28–32.

pojęciem powszechnie używanym. Zawsze jednak walczące ze sobą strony rozpoznawały się wzajemnie. Zawsze starały się wzajemnie oszukiwać i wprowadzać w błąd. Zawsze też posiadały swoje sekrety, które z wielką skrupulatnością ukrywały przed wrogiem. Odnosząc to do współczesności, wszystkie te czynności mieszczą się w obszarach funkcjonalnych zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej, co w dwupodmiotowej kooperacji negatywnej wzajemnej tworzy przestrzeń walki informacyjnej [...]. Patrząc zatem na przeszłość pod takim kątem, widzimy, że historia walki informacyjnej zdaje się być tak samo długa, jak historia ludzkich dziejów. Najwięcej faktów na ten temat można znaleźć w historii wojen, bo i te w przeszłości stanowiły jedno z bardziej rozpowszechnionych zjawisk społecznych"[165].

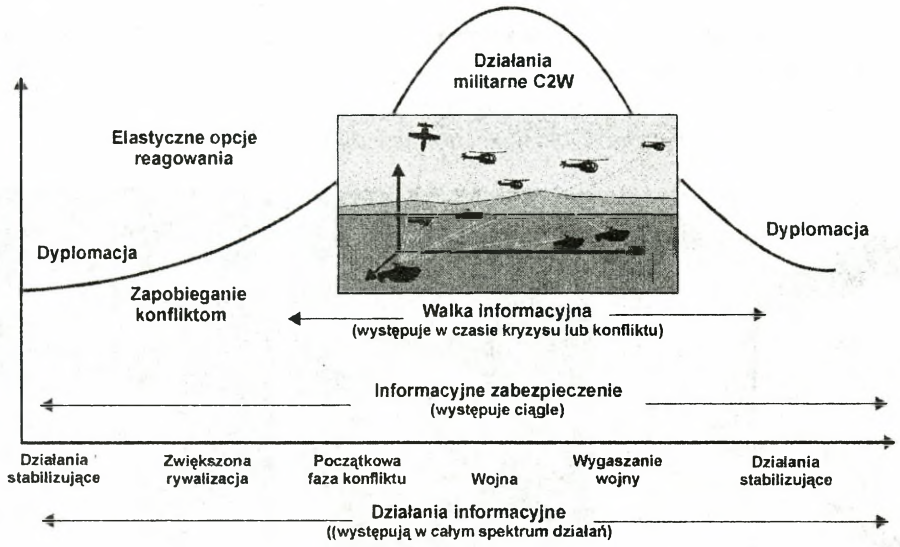
Prawdopodobnie najobszerniejsza dyskusja[166] w sprawie walki informacyjnej toczyła się w związku z opublikowaniem w 1996 r. przez Kolegium Szefów Sztabów wydawnictwa *Strategia dla pokoju: Decydujące ostrze wojny*. Stwierdzono tam, że walka informacyjna odnosi się do całego spektrum działań militarnych i do wszystkich poziomów walki. Walka informacyjna, mimo że nie jest jedynym instrumentem narodowej potęgi, to jednak przyczynia się do odstraszania przez rozładowywanie kryzysów i opóźnianie lub eliminowanie użycia sił. Defensywna walka informacyjna integruje i zabezpiecza informację i jej systemy przez oddziaływanie ofensywną walką informacyjną na informację przeciwnika i jego informacyjne systemy. W rezultacie rozległej dyskusji uświadomiono sobie nieadekwatność nazwy „walka informacyjna" do zakresu desygnatów przypisywanych temu pojęciu. Szeroka gama przedsięwzięć sfery informacyjnej jest prowadzona już w czasie pokoju i trudno je kwalifikować jako walkę.

Również ze względów propagandowych prezentowanie np. działań prewencyjnych i zabezpieczających jako „walki", może rodzić pejoratywne oceny i nastawienie. Wiele przedsięwzięć może być także stosowanych w działaniach niemilitarnych i pozawojennych.

Dlatego też postanowiono poszukać bardziej adekwatnej nazwy dla całego spektrum działań w sferze informacyjnej. Uznano, że najodpowiedniejszym będzie przyjęcie ogólnej nazwy „operacje informacyjne" (*information operations*). Nazwa ta nie budzi negatywnych skojarzeń. Może obejmować przedsięwzięcia zarówno militarne, jak i niemilitarne, a także równie dobrze zawierać formy walki, jak i współpracy. W takim ujęciu „walka informacyjna" dalej istnieje, jest ona jednakże komponentem operacji informacyjnych i obejmuje szerszy od nich zakres (rys. 23).

W 1996 r. Biuro Asystenta Sekretarza Obrony USA[167] do spraw C3I wydało wytyczne w zakresie opracowania nowej dyrektywy w tej sprawie, zastępującej tę z 1992 r. (TS3600.1). Wytyczne te służyć miały trzem celom: zapewnieniu, mimo niejawności części zagadnień, szerokiego dostępu do unormowań, odpowiadającego powszechnemu zainteresowaniu; zapewnieniu jednolitego rozumienia wewnątrz

[165] L. Ciborowski, s. 11. Znajduje się tam syntetyczna historia rozwoju walki informacyjnej.
[166] Zob. B.E. Fredericks, s. 98.
[167] Tamże, s. 97, 100.



Źródło: B.E. Fredericks, *Information Warfare at the Crossroads*, „Joint Force Quarterly" 1997, Summer, s. 99.

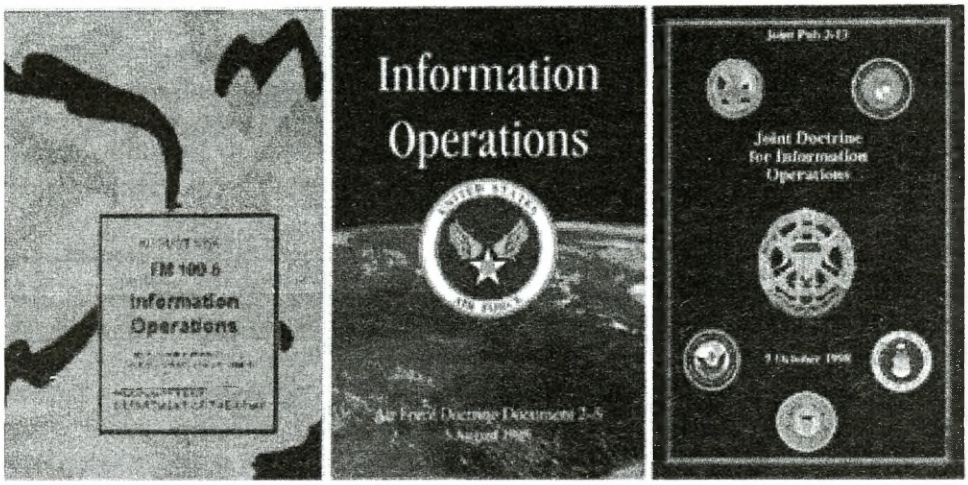
Rys. 23. Sfera operacji informacyjnych

Departamentu Obrony oraz koordynacji między różnymi agendami rządowymi oraz wskazaniu pełnego potencjału walki informacyjnej w całym spektrum działań militarnych, ze skupieniem głównej uwagi na zachowaniu pokoju i zapobieganiu eskalacji konfliktu. Z tymi wskazaniami została napisana też nowa dyrektywa Departamentu Obrony. Mimo iż w dalszym ciągu zawiera ona elementy niejawne, to zasadnicza część jest jawna. W jawnej części znajdują się wszystkie kluczowe definicje. Jest prawdopodobne, że wraz z dalszym dojrzewaniem koncepcji, kolejna jej wersja będzie całkowicie jawna.

W rezultacie już w grudniu 1996 r. opublikowano nową dyrektywę Departamentu Obrony S3600.1 „Information Operations", co otworzyło nową fazę w rozwoju walki informacyjnej. Mimo iż dyrektywa ta była niejawna i rozpowszechniana w wąskim kręgu odbiorców, to jednak spowodowała szybsze dojrzewanie koncepcji walki informacyjnej w środowisku establishmentu odpowiedzialnego za sprawy obronne. Dyrektywa ta uwzględniła wynikające z dojrzewania zmiany poglądów i wprowadziła USA w nowy wiek.

W związku z taką sytuacją w środowiskach wojskowych toczy się obecnie coraz szersza dyskusja nad problemami zagrożeń wynikających z działań w sferze informacyjnej. Wojskowi teoretycy i praktycy pracują nad kolejnymi wersjami koncepcji i doktryn działań w sferze informacyjnej. Aktywność ta toczy się zarówno w rodzajach sił zbrojnych, jak i w Kolegium Szefów Sztabów. W 1996 r. wydano doktrynę operacji informacyjnych amerykańskich sił lądowych w postaci FM 100–6.

Doktryna ta została już zmieniona i wydana pod kolejną postacią. Również amerykańskie siły powietrzne opublikowały w 1998 r. swoją doktrynę operacji informacyjnych. Także w 1998 r. została opublikowana przez amerykańskie Kolegium Szefów Sztabów *Połączona Doktryna Operacji Informacyjnych* (rys. 24).



Rys. 24. Doktryny operacji informacyjnych amerykańskich sił lądowych i powietrznych oraz doktryna połączona

Opublikowanie przez Stany Zjednoczone połączonej militarnej doktryny operacji informacyjnych, wielu ekspertów[168] uznało za ważny moment historyczny, oznaczający początek wyścigu zbrojeń w sferze działań informacyjnych. Zgodnie z nowym dokumentem (JP 3–13: *Joint Doctrine for Information Operations*) pierwszy raz oficjalnie uznano, iż ofensywne ataki na sieci komputerowe stają się nieodłączną częścią arsenału walki USA, a co jeszcze ciekawsze, arsenał ten może być używany także w czasie pokoju. W rezultacie każdy kraj musi się zatroszczyć o uzyskanie zdolności do prowadzenia ofensywnych i defensywnych operacji informacyjnych. Jeśli tego zaniecha, pozostanie bezbronny. Oficjalne wprowadzenie operacji informacyjnych do doktryny militarnej dokonało się m.in. wobec wyraźnych deklaracji wielu krajów, jak np. Chiny, gotowości wykorzystania tej sfery w walce. Jednocześnie wprowadzenie tej sfery do doktryny militarnej oznacza, że rozwinięte zostały możliwości gwarantujące pewność osiągania pożądanych efektów.

Stany Zjednoczone, jeszcze przed opublikowaniem doktryny operacji informacyjnych, prowadziły wiele badań i rozwijały swoje możliwości w zakresie operacji informacyjnych. Przykładowo, przygotowywano się do sparaliżowania systemu energetycznego przeciwnika lub jego węzłów telekomunikacyjnych przed wy-

[168] G.I. Seffers, *Joint Chiefs Inaugurate Information Combat Era*, „Defense News" 1998, November, s. 9–15.

konaniem ataku ogniowego lub brano pod uwagę informacyjne uderzenie jako alternatywa ataku ogniowego.

Po wielu rozważaniach uświadomiono sobie, że operacje informacyjne niosą korzyści niemożliwe do osiągnięcia przez użycie broni konwencjonalnej z arsenałów epoki pozimnowojennej.

Podstawową kwestią, godną szczególnej uwagi, jest to, że operacje informacyjne są bronią masowego rażenia. Właściwe zidentyfikowanie infrastruktury, połączone z wartościową informacją rozpoznawczą i wsparte dobrymi programami symulacyjnymi i wspomagającymi proces decyzyjny, może skutkować zniszczeniem narodu.

W formułowaniu doktryn przodują Amerykanie. Mimo koordynacji, dokumenty poszczególnych rodzajów sił zbrojnych i połączonych nie są jednakowe. Istnieją pewne różnice w podejściu i mimo opublikowania nieraz kolejnych już wersji doktryn operacji informacyjnych, dyskusja nabiera rozmachu.

W NATO również przyjęto dokumenty normatywne. Według dokumentu doktryny połączonej[169] AJP-01(B), wydanego w 2000 r., wyłaniająca się koncepcja operacji informacyjnych (INFO OPS) wiąże strategię militarną C2W z polityczną, dyplomatyczną i cywilno-militarną współpracą, publicznym informowaniem oraz innymi formami aktywności Sojuszu, które mogą wpływać na percepcję przeciwnika lub innych zaangażowanych stron. Operacje informacyjne są stosowane zarówno jako akcje defensywne, jak i ofensywne w szerokim spektrum poziomów od strategicznego, przez operacyjny, taktyczny, aż po pojedyncze systemy broni.

Operacje informacyjne w tej doktrynie definiowane są jako „działania podjęte dla wpływania na decydentów w ramach wspierania procesu osiągania celów politycznych i militarnych, mające charakter wpływania na informację, procesy informacyjne, systemy dowodzenia i kontroli oraz systemy komunikacyjno-informacyjne (CIS), przy eksploatowaniu i ochronie własnej informacji i systemów informacyjnych".

W prezentacji poglądów akcent położono na poglądy doktrynalne, bo są one wypadkową ogromnej ilości badań wielu zespołów ekspertów oraz pojedynczych badaczy. W wyniku tego odzwierciedlają zarówno szeroki horyzont potencjalnych możliwości, jak i realia rzeczywistości. Są w znacznym stopniu zweryfikowanymi w praktyce teoriami. W sferze teorii istnieje wielkie bogactwo poglądów na temat walki informacyjnej, ale też i coraz więcej w zakresie operacji informacyjnych. Niektóre zostały już zacytowane, warto przytoczyć jeszcze kilka z nich.

Według Roda Starka[170]

„[...] Nie istnieje powszechnie uzgodniona definicja walki informacyjnej. Jest jednak wspólna treść większości spotykanych definicji. Treść ta sprowadza się do tego, że walka informacyjna jest konfliktem, w którym informacja jest jednocześnie zasobem, obiektem ataku i bronią. Walka informacyjna obejmuje także fi-

[169] AJP-01: *Allied Joint Doctrine*, NATO, wyd. 1999 r., s. 14–1.

[170] R. Stark, *Future Warfare: Information Superiority through Info War*, http://www.smsu.edu.

zyczną destrukcję infrastruktury, która jest wykorzystywana przez przeciwnika do działań operacyjnych. [...]

Walka informacyjna jest ważnym elementem strategii Stanów Zjednoczonych, bo może działać jako mnożnik siły, umożliwiając planistom planującym walkę oraz decydentom politycznym podejmować racjonalne decyzje przed rozmieszczeniem wojsk. Umożliwia także zwiększenie narodowych zasobów.

Głównym aspektem walki informacyjnej jest wysiłek zmierzający do zdobycia i utrzymania kontroli środowiska informacyjnego, który prowadzi do dominacji informacyjnej.

Dla potrzeb działań militarnych XXI w. walka informacyjna obejmuje:

- **walkę o przewagę w dowodzeniu (*command and control warfare – C2W*);**
- **walkę bazującą na wiedzy rozpoznawczej *(intelligence-based warfare – IBW)*;**
- **walkę elektroniczną *(electronic warfare – EW)*: uniemożliwianie przeciwnikowi dostępu do dokładnej informacji;**
- **działania psychologiczne *(psychological operations – PSYOPS)*: używanie informacji do wpływu na jego rozumowanie;**
- **wojnę hakerską *(hackerwar)*: ataki softwareowe na systemy informacyjne;**
- **informacyjną walkę ekonomiczną *(information economic warfare – IEW)*: wojna za pomocą kontroli informacji handlowej;**
- **cyberwojnę *(cyberwar)*: walka w wirtualnej rzeczywistości;**
- **dezinformację militarną (*miliatry deception*): wprowadzanie w błąd co do możliwości i zamiarów;**
- **fizyczne niszczenie (*physical destruction*): użycie spektum broni od konwencjonalnej do impulsu elektromagnetycznego;**
- **przedsięwzięcia bezpieczeństwa (*security measures*)"**[171].

Według P. Sienkiewicza: „W ostatnich latach wyróżniono informacyjne operacje (działania) ofensywne i defensywne. Do operacji ofensywnych zalicza się takie działania, jak:

- **osłona operacji (*operations security*),**
- **operacje psychologiczne (*psychological operations*),**
- **pozoracja (military deception),**
- **destrukcja (physical attack),**
- **walka elektroniczna (*electronic warfare*),**
- **atak informatyczny (computer network attack),**
- **działania typu civil affairs i public affairs.**

Natomiast w ramach operacji defensywnych:

- **bezpieczeństwo informacyjne (*information assurance),**
- **osłona (operation security),**

[171] Tamże.

- **działania kontrpropagandowe (*counterpropaganda*),**
- **działania kontrwywiadowcze (*counterintelligence*),**
- **walka elektroniczna (*electronic warfare*),**
- **działania specjalne (special information operations)**"[172].

Zarówno więc praktyka, jak i badania teoretyczne wykazały, że każda sfera aktywności państwa, a nie tylko militarna, znajduje się w ogniu intensywnego oddziaływania informacyjnego mającego często charakter kooperacji negatywnej, czyli walki. Tak więc w atmosferze teoretycznych poszukiwań i wobec wysokiej dynamiki negatywnych zjawisk zachodzących w informacyjnej sferze praktyki, pojawiły się zarysy różnych koncepcji walki informacyjnej oraz operacji informacyjnych. Przegląd wybranych definicji walki informacyjnej i operacji informacyjnych zawierają tabele 5 i 6.

Tabela 5. Przegląd definicji walki informacyjnej

Walka informacyjna	
Joint Pub 3–13: *Joint Doctrine for Information Operations*, Joint Chiefs of Staff, Washington 1998.	Walka informacyjna to działania informacyjne prowadzone w czasie kryzysu lub konfliktu dla osiągnięcia pożądanych celów w relacjach z przeciwnikiem lub wsparcia działań prowadzących do tych celów.
AFDD 2–5: *Information Operations*. USAF, Maxwell AFB, 5 August 1998.	Walka informacyjna to działania informacyjne prowadzone dla obrony własnej informacji i systemów informacyjnych lub prowadzone dla atakowania i wywarcia wpływu na informację lub systemy informacyjne przeciwnika. Ta walka jest prowadzona głównie w czasie kryzysu lub konfliktu. Jednak defensywny komponent tej walki, podobnie jak obrona powietrzna, jest prowadzony w całym spektrum działań militarnych od pokoju do wojny.
DOD & Joint Staff – CJCSI 3210.01, [w:] FM 100–6: *Information Operations*, Headquarters, Department of the Army, 1996, s. 2–2.	Walka informacyjna to działania podejmowane dla osiągnięcia przewagi informacyjnej przez wpływanie na informację przeciwnika, jego zależne od informacji procesy, informacyjne systemy i sieci komputerowe, przy jednoczesnej obronie własnej informacji, zależnych od informacji procesów, informacyjnych systemów i sieci komputerowych.
S. Widnall, R. Fogleman, *Cornerstones of Information Warfare*, Headquarters, Department of the Air Force, Washington 1995.	Walka informacyjna to jakiekolwiek działania mające na celu wzbranianie przeciwnikowi dostępu do informacji i jej funkcji lub ich eksploatację, obniżanie jej wartości bądź niszczenie; ochrona siebie przeciwko takim działaniom oraz eksploatowanie własnych militarnych funkcji informacyjnych.
W. Schwartau, *Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, Thunder's Mouth Press 1996, s. 28–32.	Walka informacyjna jest elektronicznym konfliktem, w którym informacja jest strategicznym dobrem wartym podboju lub destrukcji.

[172] P. Sienkiewicz, *Współczesne koncepcje...* wyd. cyt.

E. Paige, [za:] G. Ivefors, *Information Warfare. Defeat the enemy before battle – a warfare revolution in the 21st century?* http://www.ida.liu.se/~guniv/Infowar/ 26.01.2001.	Walka informacyjna to działania podejmowane dla osiągnięcia przewagi informacyjnej, prowadzone w ramach wspierania narodowej strategii militarnej. Działania te mają na celu wpływanie na informację i systemy informacyjne przeciwnika, przy wpływaniu i obronie własnej informacji i jej systemów.
J. Arquilla, D. Ronfeldt, *Cyberwar is Coming*, [w:] *Comparative Strategy 12–1993*, s. 41–65 [za:] G. Stein, *Information Warfare*, [w:] A.D. Campen, D.H. Deart, R.T. Goodden, *Cyberwar: Security, Strategy, and Conflct in the Information Age*, AFCEA International Press, Fairfax 1996, s. 175.	Walka informacyjna w najogólniejszym sensie jest użyciem informacji dla osiągnięcia naszych narodowych celów. Podobnie jak dyplomacja, ekonomiczna rywalizacja czy użycie sił zbrojnych, informacja sama w sobie jest kluczowym czynnikiem narodowej potęgi. Ponadto, co jeszcze ważniejsze, informacja staje się głównym narodowym zasobem, który wspiera dyplomację, ekonomiczną rywalizację oraz przemoc militarną. Walka informacyjna w tym sensie może być postrzegana jako konflikt między państwami lub narodami, prowadzony częściowo przez globalnie połączoną infrastrukturę informacyjną i komunikacyjną.
R. Szafranski, *Cyberwar: A Theory of Information Warfare: Preparing For 2020*, [w:] A.D. Campen, D.H. Deart, R.T. Goodden, *Cyberwar: Security, Strategy, and Conflct in the Information Age*, AFCEA International Press, Fairfax 1996, s. 233.	Walka informacyjna jest formą konfliktu, w którym bezpośrednie atakowanie systemów informacyjnych jest środkiem atakowania wiedzy i przekonań przeciwnika. Walka informacyjna może być prowadzona jako komponent kompleksowej wrogiej działalności – w postaci wojny sieciowej (*netwar*) lub cyberwojny (*cyberwar*) – lub może przybierać formę walki samodzielnej.
R.J. Knecht, *Thoughts about Information Warfare*, tamże, s. 165.	Walka informacyjna jest przygotowaniem do użycia lub użyciem fizycznej bądź cyfrowej broni dla dezorganizacji lub niszczenia informacji bądź systemów informacyjnych w celu degradowania lub przerywania wykonywania funkcji, które zależą od informacji lub informacyjnych systemów.
R. Stark, *Future Warfare: Information Superiority through Info War*, Southwest Missouri State University, http://www.smsu.edu.	Walka informacyjna jest konfliktem, w którym informacja jest jednocześnie zasobem, obiektem ataku i bronią. Walka informacyjna obejmuje także fizyczną destrukcję infrastruktury, która wykorzystywana jest przez przeciwnika do działań operacyjnych.
L. Ciborowski, *Walka informacyjna*, Toruń 1999.	Walka informacyjna to działania kooperacji negatywnej wzajemnej, w których cel destrukcyjnego oddziaływania skoncentrowany jest na systemach informacyjno-sterujących przeciwnych sobie stron. Przedmiotem walki informacyjnej jest system informacyjno-sterujący.
G. Nowacki, *Walka informacyjna – próba kategoryzacji.* Rozprawa doktorska, AON, Warszawa 1999, s. 112–113.	Walka informacyjna – kooperacja negatywna wzajemna, w której cel destrukcyjnego oddziaływania skoncentrowany jest na systemach informacyjno-sterujących przeciwnych sobie stron. Przedmiotem walki informacyjnej są systemy informacyjno-sterujące i ich otoczenie.

M. Libicki, *What is Information Warfare?* NDU, Washington 1995, s. x.	Walka informacyjna jako samodzielna technika prowadzenia wojny nie istnieje. W zamian istnieje kilka oddzielnych form walki informacyjnej, z których każda pretenduje do bycia ogólniejszą koncepcją. Obecnie wyróżnić można siedem form walki informacyjnej – konfliktu, który zawiera ochronę, manipulację, degradację lub uniemożliwianie dostępu do informacji. Formami tymi są: walka o przewagę w dowodzeniu, walka bazująca na wiedzy, walka elektroniczna, walka psychologiczna, walka hackerska, ekonomiczna walka informacyjna i cyberwalka.
P. Sienkiewicz, *Współczesne koncepcje walki informacyjnej*, [w:] *Informacyjny wymiar współczesnych działań powietrznych*, materiały z sympozjum naukowego, red. R. Szpyra, Warszawa 2002.	Walką informacyjną (*information warfare, infowar*) nazywamy całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych). Istotą tak rozumianej walki informacyjnej jest: (1) zniszczenie (lub degradacja wartości) zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych; (2) zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych.

Tabela 6. Przegląd definicji operacji informacyjnych

Operacje informacyjne	
Joint Pub 3–13: Joint *Doctrine for Information Operations*, Joint Chiefs of Staff, Washington 1998.	Operacje informacyjne to akcje podjęte dla wpływania na informację i systemy informacyjne przeciwnika przy jednoczesnej ochronie własnej informacji i systemów informacyjnych.
FM 100–6: *Information Operations*, Headquarters, Department of the Army, 1996, s. 2–3.	Operacje informacyjne to ciągłe działania militarne w militarnym środowisku informacyjnym, które uaktywniają, wzmacniają i chronią zdolności własnych sił do gromadzenia, przetwarzania i działania na informacji dla osiągnięcia (korzyści) przewagi w pełnym spektrum działań militarnych. Operacje informacyjne zawierają interakcje z globalnym środowiskiem informacyjnym i eksploatację informacji przeciwnika lub uniemożliwianie mu dostępu do informacji i zdolności do podejmowania decyzji.
AFDD 2–5: *Information Operations*, USAF, Maxwell AFB, 5 August 1998.	Operacje informacyjne obejmują przedsięwzięcia podejmowane dla zdobycia, wykorzystania, obrony lub ataku na informację lub systemy informacyjne i łączą zarówno aspekt informacji w walce, jak i walkę informacyjną. Operacje te prowadzone są przez wszystkie fazy kampanii i w całym zakresie działań militarnych.
MC 422 – *NATO Information Operations Policy.*	Operacje informacyjne są zdefiniowane jako „przedsięwzięcia podjęte w celu wywarcia wpływu na decydentów w ramach wsparcia politycznych i militarnych celów poprzez oddziaływanie na informację innych, ich procesy informacyjne oraz systemy dowodzenia, kontroli, łączności i informacyjne, przy wykorzystaniu i ochronie własnej informacji i systemów informacyjnych".

AJP-01: *Allied Joint Doctrine*, NATO, Wyd. 1999.	Operacje informacyjne to działania podjęte dla wpływania na decydentów w ramach wspierania procesu osiągania celów politycznych i militarnych, mające charakter wpływania na informację, procesy informacyjne, systemy dowodzenia i kontroli oraz systemy komunikacyjno-informacyjne (CIS), przy eksploatowaniu i ochronie własnej informacji i systemów informacyjnych.

P. Sienkiewicz jest zaś przekonany, że

„Nowoczesne koncepcje walki zbrojnej bazują na tworzeniu wieloczynnikowej przewagi militarnej (*multifactor military superiority*) opartej na kontrolowanej, rozstrzygającej przewadze informacyjnej (*information superiority*) i technologicznej (*technological superiority*). Aczkolwiek potencjał informacyjny stanowił zawsze istotny czynnik potencjału bojowego, to w rozważaniach dotyczących sposobów tworzenia przewagi na polu walki był on raczej pomijany. W szczególności w matematycznych modelach walki (typu modele Lanchestera) uwaga koncentrowała się na *stosunku sił* uwzględniającym przede wszystkim *potencjały rażenia* stron walczących.

Potencjał informacyjny, jako czynnik potencjału militarnego, tworzą zasoby informacyjne systemu obronnego państwa oraz systemy informacyjne kształtujące infrastrukturę informacyjną państwa. Oznacza to, że potencjał informacyjny to wszelkie zasoby informacyjne (dane, informacje, wiedza), które tworzą infosferę określonego systemu działania (organizacji, instytucji). Ale także systemy informacyjne (informatyczne, telekomunikacyjne) niezbędne do efektywnego prowadzenia określonych, zamierzonych działań. [...]

Konsekwencją analizy systemowej procesów informacyjnych na współczesnym polu walki jest wprowadzenie stosunku wiedzy (*relative knowledge*) stron walczących, jako czynnika decydującego o rezultatach walki"[173].

W stosunkowo wczesnej fazie badań nad walką informacyjną uświadomiono sobie jej rozległy i wszechogarniający charakter. Dostrzeżono, iż dotyczy ona sfery pozamilitarnej w jeszcze szerszym zakresie niż militarnej. Również w układzie podmiotowym wyodrębnić można wiele obszarów. W. Schwartau[174] wyróżnił np. indywidualną, zespołową (korporacyjną) i globalną walkę informacyjną.

W tej sytuacji przyjęto, że:

- **Istnienie tak rozległych obszarów walki informacyjnej jest niewątpliwe, jednakże ze względu na ukierunkowanie niniejszych rozważań, przedmiotem zainteresowania jest walka informacyjna oraz operacje informacyjne państwa – bardziej ogólna kategoria zawierająca w sobie walkę informacyjną.**
- **Obszar ten jest badany w zakresie ustalenia ogólnych prawidłowości, które kształtują militarne operacje informacyjne.**

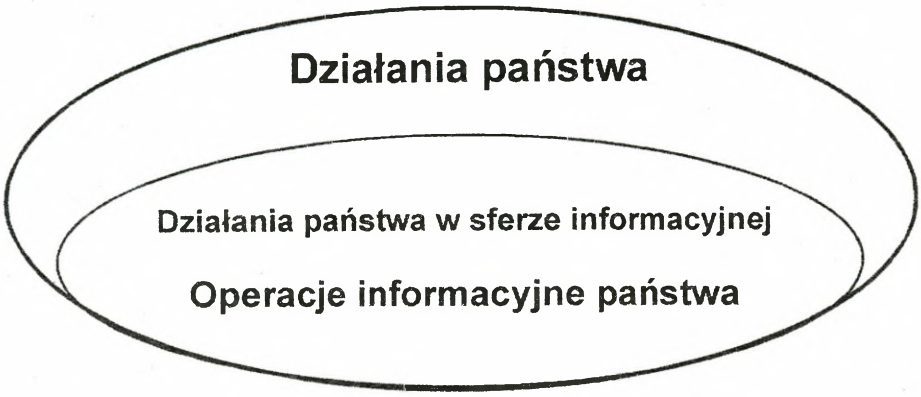
[173] Tamże.

[174] W. Schwartau, s. 33–35.

- **Siły zbrojne są elementem organizacji państwa. Ich podstawowe funkcje odnoszą się głównie do sfery zewnętrznej państwa. Siły zbrojne mają bowiem oddziaływać na elementy innego państwa. Jest to prawdziwe, nawet gdy oddziaływanie to zachodzi w obszarze własnego terytorium. Funkcje te wynikają z relacji zachodzących między państwami.**
- **Istotą aktywności państwa na arenie międzynarodowej jest jednoczesne prowadzenie działań w spektrum obejmującym zarówno formy kooperacji pozytywnej, jak i negatywnej;**
- **Jedną z podstawowych sfer oddziaływań państwa jest sfera informacyjna, a oddziaływania te są skierowane na informację i systemy informacyjne przeciwnika;**
- **Systemem informacyjnego komunikowania jest zbiór elementów procesu informacyjnego komunikowania oraz zachodzących między nimi relacji;**
- **System informacyjny to taki system działania, którego zadaniem jest zbieranie (zdobywanie), przesyłanie, przetwarzanie, przechowywanie i udostępnianie informacji, zgodnie z wymaganiami użytkownika w celu zaspokojenia jego potrzeb informacyjnych;**
- **Celem systemu informacyjnego *obsługującego* określony system użytkownika informacji jest stworzenie mu informacyjnych warunków efektywnego działania;**
- **Systemy informacyjne, które służą zmniejszaniu ilości, jakości i wartości informacji są w istocie systemami dezinformowania lub pseudoinformowania (parainformowania). Celem ich jest degradacja wartości zasobów informacyjnych systemów działania przeciwnika;**
- **Oddziaływania zawarte w sferze informacyjnej mogą, zgodnie z prakseologią, przybierać formy kooperacji pozytywnej (współpracy) i negatywnej (walki);**
- **Informacyjna sfera oddziaływań państwa obejmuje wszystkie obszary aktywności międzynarodowej państwa;**
- **Operacje informacyjne państwa są częścią ogółu jego działań.**

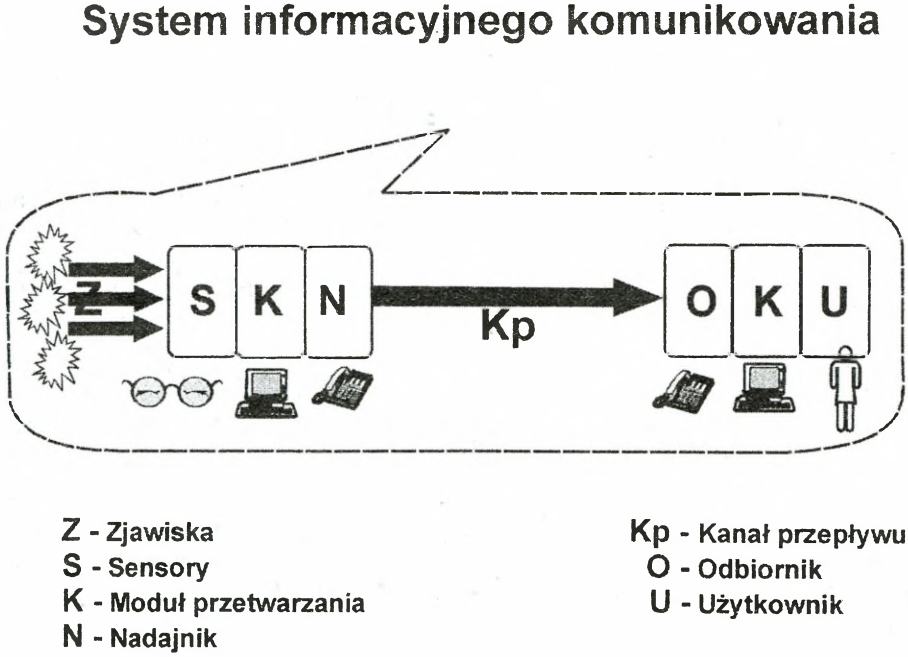
Działania państwa dotyczą wszystkich obszarów i form jego aktywności. Spośród tak wyodrębnionego zbioru, można wyróżnić podzbiór działań państwa obejmujący aktywność w sferze informacyjnej, mającą formę operacji informacyjnych (rys. 25). Elementy tego podzbioru muszą mieć wszystkie cechy wyróżnialności elementów zbioru „działania państwa" i przynajmniej jedną wspólną cechę wyróżnialności tych elementów spośród innych. Tą cechą wyróżnialności podzbioru „**operacje informacyjne państwa**" jest **przedmiot działań, jakim są zewnętrzne i własne systemy informacyjnego komunikowania lub przekazywana przez te systemy informacja** (rys. 26).

W rezultacie **operacje informacyjne państwa rozumiane będą jako zorganizowana aktywność państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na zewnętrzne i wewnętrzne systemy informacyjnego komunikowania lub przepływającą przez nie informację.**



Opracowanie własne.

Rys. 25. Działania państwa oraz operacje informacyjne państwa

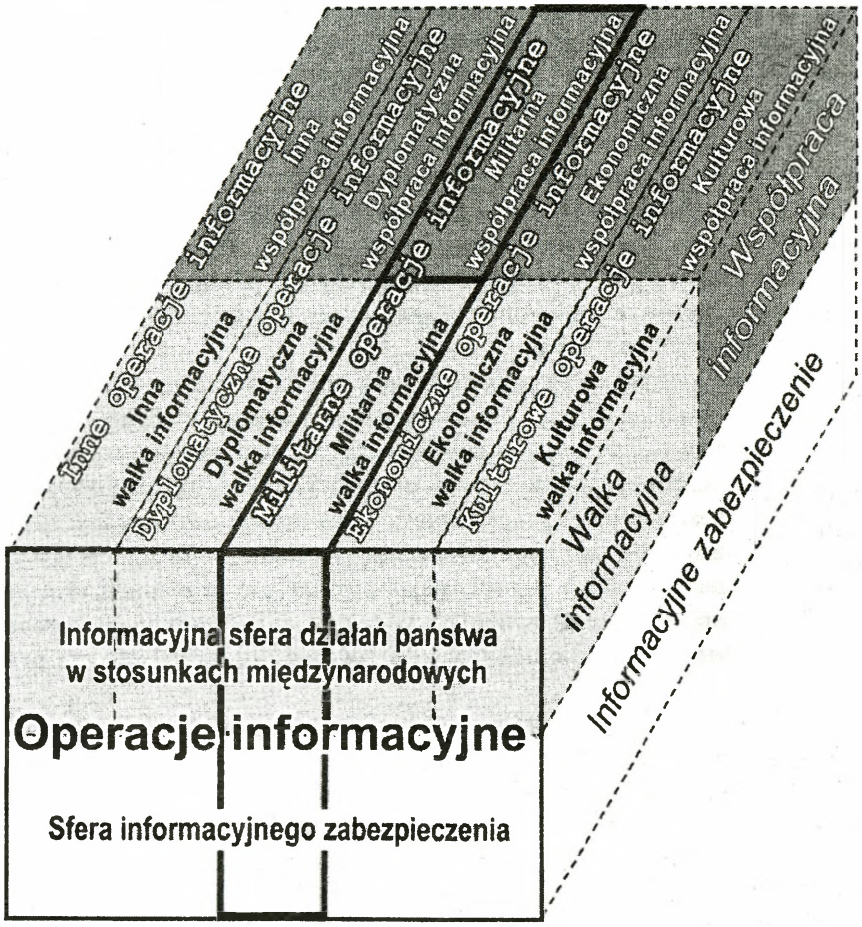


Opracowanie własne.

Rys. 26. Model systemu informacyjnego komunikowania

Odpowiednio do tego właściwe sferze militarnej państwa **militarne operacje informacyjne to zorganizowana aktywność militarna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na zewnętrzne i wewnętrzne systemy informacyjnego komunikowania lub przepływającą przez nie informację.**

Konstatacje te ilustruje rysunek 27.



Opracowanie własne.

Rys. 27. Operacje informacyjne państwa w relacjach międzynarodowych

Odpowiednio do potrzeb można definiować np.: ***operacje informacyjne sił powietrznych to zorganizowana aktywność militarna sił powietrznych prowadząca do osiągnięcia określonych celów politycznych, skierowana na zewnętrzne i wewnętrzne systemy informacyjnego komunikowania lub przepływającą przez nie informację.***

Operacje informacyjne składają się z trzech głównych komponentów, którymi są: informacyjna współpraca (kooperacja pozytywna); walka informacyjna (kooperacja negatywna) i informacyjne zabezpieczenie. Dwie pierwsze formy aktywności odnoszą się do stosunków między państwami, a więc do relacji zewnętrznych. Tymczasem istnieje jeszcze inny ważny obszar potrzeb[175]. Jest nim zasilanie informacyjne własnych procesów wewnętrznych. Zaspokajanie tych potrzeb jest domeną trzeciej formy: informacyjnego zabezpieczenia.

Walka informacyjna jest formą kooperacji negatywnej operacji informacyjnych. Ponieważ istotą walki jest przemoc[176], a przedmiotem tej walki są systemy informacyjnego komunikowania przeciwnika oraz przepływająca przez nie informacja, to można przyjąć, że **walka informacyjna to zorganizowana w formę przemocy aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłanej przez nie informacji przed podobnym działaniem przeciwnika.**

Częścią walki informacyjnej państwa jest militarna walka informacyjna. Główną cechą wyróżnialności tego podzbioru jest podmiot prowadzący działania, jakim jest komponent militarny państwa. W związku z tym **militarna walka informacyjna to zorganizowana w formę przemocy militarna aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłanej przez nie informacji przed podobnym działaniem przeciwnika.**

Podobnie jak w sytuacji definicji operacji informacyjnych również rozumienie walki informacyjnej można zawężać dla potrzeb poszczególnych rodzajów sił zbrojnych, np.: ***walka informacyjna sił powietrznych to zorganizowana w formę przemocy aktywność zewnętrzna sił powietrznych prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłanej przez nie informacji przed podobnym działaniem przeciwnika.***

Trzecim komponentem operacji informacyjnych jest **informacyjne zabezpieczenie.** Głównym jego celem jest zapewnienie właściwego zasilania informacyjnego własnych procesów wewnętrznych. Najważniejszymi z nich są procesy decyzyjne oraz procesy sterowania. Zabezpieczenie to obejmuje **zdobywanie informa-**

[175] Zob. podrozdział 1.2.
[176] Zob. podrozdział 1.3.

cji zachodzące w **procesach rozpoznania** oraz dostarczanie informacji **realizowane w procesach informacyjnej komunikacji**.

Operacje informacyjne mają charakter celowej zorganizowanej aktywności i podobnie jak każda taka aktywność dekomponują się na formy związane z współpracą i walką. **Operacje informacyjne mogą** więc **być prowadzone w formie informacyjnej współpracy i informacyjnej walki**.

Niniejsze rozważania koncentrują się na jednej z tych form, jaką jest walka, a identyfikacja form działań zostanie przeprowadzona przede wszystkim w odniesieniu do tej kategorii.

Poszukiwanie form działań walki informacyjnej warto zacząć od zidentyfikowania podstawowych kategorii jakiejkolwiek walki. Do kategorii tych należą „atak" i „obrona". Jeżeli niemalże powszechnie przyjmuje się istnienie **walki** informacyjnej, to konsekwencją tego powinno być uznanie istnienia „**informacyjnego ataku**" i „**informacyjnej obrony**". Tymczasem niektórzy badacze (np. L. Ciborowski, G. Nowacki) nie decydują się na ten krok, uznając istnienie *obrony informacyjnej* oraz *zakłócania informacyjnego* (zamiast ataku informacyjnego). Wydaje się to nieuzasadnione, gdyż jest to logiczna niekonsekwencja. Ponadto w praktyce stosuje się już pojęcia typu „atak na sieci komputerowe", „atak na sieci energetyczne", „atak na urządzenia nadawcze", „atak propagandowy". Niekiedy są wahania nad zakwalifikowaniem jakichś działań jako ataku, gdyż może on być skrywany, a prowadzący go może zaprzeczać jego istnieniu. Jednakże zarówno przy otwartym zastosowaniu, jak też w teoretycznych rozważaniach dla zachowania jednoznaczności i klarowności, należałoby uznać kategorię „**informacyjny atak**" za odpowiedniejszą niż *informacyjne zakłócanie*; tak też to zostało przyjęte.

4. ELEMENTY MILITARNEJ WALKI INFORMACYJNEJ

Zgodnie z wcześniejszymi ustaleniami militarna walka informacyjna to zorganizowana w formę przemocy militarna aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłanej przez nie informacji przed podobnym działaniem przeciwnika.

Militarna walka informacyjna dzieli się na **informacyjny atak** i **informacyjną obronę**.

Odpowiednio do przyjętego rozumienia walki informacyjnej, uznano, iż: ***informacyjny atak*** **to zorganizowana w formę przemocy militarna aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji**, zaś ***informacyjna obrona*** **to zorganizowana militarna aktywność państwa prowadząca do zapewnienia ochrony własnych systemów informacyjnego komunikowania i przesyłanej przez nie informacji przed rozpoznaniem i informacyjnym atakiem przeciwnika**.

Warto podkreślić, że obrona ta jest przeciwdziałaniem zarówno przedsięwzięciom rozpoznania, jak i informacyjnego ataku przeciwnika.

4.1. Walka elektroniczna

Przed charakterystyką poszczególnych form działań, należy zwrócić uwagę na istnienie w koncepcjach i doktrynach kategorii „walka elektroniczna", nazywanej w części polskiego piśmiennictwa „walką radioelektroniczną".

Zbigniew Dubrawski, w wyniku przeprowadzonych badań, uznał, iż: „[...] **walka elektroniczna to zespół przedsięwzięć i działań wyspecjalizowanych sił, sprzężonych ze sobą organizacyjnie i funkcjonalnie, których celem jest rozpoznanie i dezorganizacja systemów (środków) elektronicznych przeciwnika oraz zapewnienie warunków do stabilnej pracy analogicznym systemom (środkom) wojsk własnych**.

W sensie działania, dzieli się ona na określone składowe (części) i obejmuje:

a) **rozpoznanie radioelektroniczne**, którego zadaniem jest zdobywanie informacji o środkach radioelektronicznych przeciwnika, promieniujących energię EM. Dotyczą one parametrów technicznych emisji oraz działalności bojowej. Wykonuje się je przez poszukiwanie, śledzenie, przechwytywanie, namierzanie i analizę pracy nadajników energii elektromagnetycznej.

b) **obezwładnienie radioelektroniczne,** uniemożliwiające lub utrudniające przeciwnikowi efektywne wykorzystanie środków RE w wyniku zakłócania energią EM. Osiąga się je przez celowe aktywne i pasywne zakłócenia urządzeń odbiorczych oraz prowadzenie dywersji radiowej w kanałach łączności i transmisji danych, a także wywoływanie zmiany środowiska EM i wzbudzanie silnych impulsów elektromagnetycznych.

c) **obronę radioelektroniczną**, mającą na celu zapewnienie stabilnej i niezakłóconej pracy własnym systemom i środkom RE, podczas prowadzonej przez przeciwnika WRE, a także w warunkach wzajemnego oddziaływania środków RE wojsk własnych. Realizuje się ją, podejmując techniczne i organizacyjne przedsięwzięcia zabezpieczające obiekty RE przed rozpoznaniem RE, rażeniem środkami ogniowymi naprowadzającymi się (lub naprowadzanymi) na źródła energii EM, obezwładnieniem RE, a także uwzględniając przedsięwzięcia w zakresie kompatybilności EM i kontroli promieniowania EM"[177].

Według tego autora „**celem walki radioelektronicznej (elektronicznej) prowadzonej w siłach powietrznych** jest rozpoznanie pracujących systemów i środków radioelektronicznych (elektronicznych) lotnictwa uderzeniowego, obrony powietrznej i obrony przeciwlotniczej wojsk przeciwnika, ich obezwładnienie radioelektroniczne (elektroniczne), które powinno spowodować obniżenie jego sprawności działania, stwarzając tym samym dogodne warunki dla ognia i manewru własnego lotnictwa i środkom OP oraz zabezpieczenie stabilnej i niezakłóconej pracy własnym systemom i środkom radioelektronicznym (elektronicznym)"[178].

Podobna definicja[179] oraz identyczne komponenty składowe walki radioelektronicznej są także prezentowane w podręczniku „Walka radioelektroniczna w siłach zbrojnych RP" wydanym przez Wydział Wojsk Lądowych AON w 1994 r.

Według poglądów przyjętych w siłach powietrznych USA[180], walka elektroniczna jest związana z postępem technologicznym i rozwojem cywilizacyjnym. Nowoczesne uzbrojenie i systemy zabezpieczenia wykorzystują techniki radiowe, podczerwone, optyczne, ultrafioletowe, elektro-optyczne i laserowe. Dowódcy muszą przygotować swoje systemy uzbrojenia do działania w intensywnie wykorzy-

---

[177] Z. Dubrawski, *Walka radioelektroniczna prowadzona przez siły powietrzne. Studium operacyjne*, Warszawa 2000, s. 39, 56.

[178] Tamże, s. 45.

[179] Definicja ta brzmi: „Walka radioelektroniczna (Wre) to całokształt przedsięwzięć i działań wojsk, które wykorzystując energię elektromagnetyczną zmierzają do rozpoznania i zdezorganizowania systemów radioelektronicznych przeciwnika oraz zapewnienia warunków stabilnej pracy systemom własnych wojsk. *Walka radioelektroniczna w siłach zbrojnych RP*, Warszawa 1994, s. 11.

[180] Opracowano na podstawie: AFDD 2-5.1: *Electronic Warfare.*, Washington D.C. 1999.

stywanym i agresywnym środowisku elekromagnetycznym. Warunki te mogą być jeszcze bardziej pogorszone zarówno przez zamierzone, jak i przez niezamierzone emisje pochodzące od sojuszniczych, neutralnych i wrogich sił. Tymczasem do wykonania jakiejkolwiek misji niezbędna jest świadomość sytuacji, dynamiczne planowanie i elastyczność na wszystkich poziomach wojny. Nieskrępowany dostęp do wybranych zakresów spektrum elektromagnetycznego ma decydujące znaczenie dla efektywności systemów uzbrojenia.

Walką elektroniczną jest każde działanie militarne wiążące się z użyciem energii elektromagnetycznej lub wiązkowej, prowadzone dla kontroli spektrum elektromagnetycznego lub atakowania przeciwnika.

Działanie to nie jest ograniczone do użycia częstotliwości radiowych lub radiolokacyjnych, ale zawiera także wykorzystanie zakresów: podczerwonego, widzialnego, ultrafioletowego i innych. Walka elektroniczna wspiera wysiłki w uzyskaniu dostępu do przestrzeni walki i swobody działania wolnej od zagrożenia ze strony systemów przeciwnika.

Głównymi komponentami walki elektronicznej są: atak elektroniczny (EA), obrona elektroniczna (EP) i wsparcie elektroniczne (ES). Wszystkie te komponenty wspierają działania powietrzno-kosmiczne. Kontrola spektrum elektromagnetycznego jest uzyskiwana poprzez ochronę własnych systemów i przeciwdziałanie systemom przeciwnika. Atak elektroniczny ogranicza użycie spektrum elektromagnetycznego przez przeciwnika; obrona elektroniczna rozszerza użycie spektrum elektronicznego przez siły sojusznicze; wsparcie elektroniczne umożliwia dowódcy dokładną ocenę sytuacji w rejonie działania.

Stanowiska te są reprezentatywnym odzwierciedleniem panujących poglądów na walkę elektroniczną widzianą z powietrznej perspektywy. Perspektywa ta nie odbiega zbyt daleko od innych perspektyw. Kładzie jedynie większy akcent na pokonywanie obrony powietrznej. Porównanie obu koncepcji wskazuje, że wyróżnia się w istocie te same komponenty walki elektronicznej, jedynie nieco odmiennie je nazywając (tabela 7).

W środowisku polskim w dalszym ciągu obserwuje się wahania nad zmianą nazwy „radioelektroniczna" na „elektroniczna". Niektórzy, szczególnie z obszaru praktyki, uznają[181] bowiem, że gdy Polska nie dysponuje możliwościami prowadzenia walki w niektórych obszarach walki elektronicznej, to i nie może akceptować istnienia pojęć teoretycznych odnoszących się do takich obszarów. Przekonanie to wynika z mniemania, że zaakceptowanie pewnych definicji zobliguje do podejmowania działań w tym obszarze, co nie jest zgodne z prawdą, gdyż istnieje wiele akceptowanych teorii, które nie są realizowane w praktyce. Przykładem może być teoria wykorzystania samolotów bezzałogowych. Owo niezdecydowanie uwidacznia się również w cytowanej pracy Z. Dubrawskiego, który w definicji stosuje nazwę „elektroniczna", a w dalszej części pracy używa nazwy „radioelektroniczna", umieszczając czasami drugą nazwę, „elektroniczna" w nawiasach.

[181] Stanowisko takie uwidoczniło się w przeprowadzanych wywiadach w środowisku wojskowym zajmującym się tą problematyką.

Tabela 7. Porównanie głównych komponentów walki elektronicznej według poglądów USAF i polskich

Zbigniew Dubrawski oraz Wydział Wojsk Lądowych AON	Doktryna USAF
Rozpoznanie radioelektroniczne	Wsparcie elektroniczne
Obezwładnianie radioelektroniczne	Atak elektroniczny
Obrona radioelektroniczna	Obrona elektroniczna

W wielu ustaleniach doktrynalnych komponuje się zarówno operacje informacyjne, jak i walkę informacyjną z istniejących wcześniej elementów, takich jak walka elektroniczna. W odniesieniu do tych, które są jednorodnymi działaniami, jest to słuszne. Jednakże **walka elektroniczna jest złożoną koncepcją działań obejmującą przedsięwzięcia ofensywne, defensywne i zabezpieczające. Koncepcja walki elektronicznej może istnieć, gdy nie jest włączona w kompleks operacji informacyjnych i walki informacyjnej. Z punktu widzenia operacji informacyjnych wsparcie elektroniczne jest częścią informacyjnego wsparcia, elektroniczny atak i obrona są zaś elementami walki informacyjnej. Dlatego też zgodnie z podziałem dokonanym według kryterium rodzaju działań, wszystkie działania ofensywne, defensywne i zabezpieczające uporządkowano w jednorodne grupy, nie tworząc nakładających się na siebie podgrup.**

4.2. Formy ataku informacyjnego

Siły zbrojne, w ramach **informacyjnego ataku** mogą stosować następujące formy ataku:

- **atak informatyczny (w sferze przetwarzania danych cyfrowych);**
- **atak elektroniczny;**
- **atak ogniowy;**
- **działania psychologiczne;**
- **dezinformacja (mylenie).**

4.2.1. Atak informatyczny (w sferze przetwarzania danych cyfrowych)

Atak informatyczny[182] jest prowadzony w sferze przetwarzania danych cyfrowych (*digital data warfare*) i polega na skrytym wprowadzeniu przez atakującego złośliwego kodu komputerowego do określonego systemu komputerowego lub sieci komputerowej dla osiągnięcia pożądanych celów.

[182] Przyjęto za: L.G. Downs Jr., *Digital Data Warfare: Using Malicious Computer Code as a Weapon. A Research Report Submitted to the Faculty in Fulfillment of the Curriculum Requirement*, Maxwell AFB 1995.

W przeciwieństwie do innych złośliwych kodów, kod walki w sferze przetwarzania danych cyfrowych jest narzędziem – środkiem prowadzącym do osiągnięcia celu, a nie celem samym w sobie. Jest jednym z wielu rodzajów broni, jakie informacyjny wojownik może stosować.

Złośliwe kody walki informatycznej mogą przybierać głównie formę: wirusów, robaków, bomb logicznych, bomb programowanych czasowo, koni trojańskich lub ich kombinacji odpowiednich do spełnianych funkcji. Różnią się one od hakerskich kodów, jako że służą atakowaniu konkretnych systemów (lub sieci tych systemów) dla osiągnięcia jasno określonych celów w sposób przewidziany przez atakującego.

Atakującym może tu być zarówno militarna, jak i państwowa, ale także i terrorystyczna organizacja czy też międzynarodowa lub prywatna korporacja, a nawet pojedyncza osoba posiadająca wiedzę i zasoby niezbędne do sporządzenia i zainstalowania takiego kodu. Przykłady takiego zastosowania obrazuje poniższa tabela.

Tabela 8. Przykłady walki w sferze przetwarzania danych cyfrowych

Atakujący	Obiekt ataku	Bieżący cel działań	Dalekosiężny cel
Państwo lub organizacja militarna	Sieć C4I przeciwnika	Przerwanie procesu dowodzenia i kontroli podległymi jednostkami przeciwnika	Wygranie wojny
Organizacja terrorystyczna	System komputerowy firmy telekomunikacyjnej AT&T	Przerwanie działalności firmowej, transakcji finansowych i przepływu informacji	Wydanie politycznego oświadczenia
Prywatna korporacja	Baza danych badań i rozwoju konkurenta	Uzyskanie dostępu do zastrzeżonej informacji	Uzyskanie korzyści w walce konkurencyjnej
Rozczarowany lub nieuczciwy pracownik	System księgowości firmy	Transfer pieniędzy na fałszywe konto, długo po rozwiązaniu umowy o pracę	Korzyści finansowe lub „ukaranie" firmy

Atakujący w sferze przetwarzania danych cyfrowych może oddziaływać na atakowany system, przez zastosowanie jednego z następujących sposobów:

- **Wzbranianie – uniemożliwianie atakowanemu obiektowi użycia systemu komputerowego, jego danych lub informacji, której ten system dostarcza. Może to być osiągane przez użycie złośliwego kodu, który spowoduje awarię sprzętu lub destrukcję programów lub danych.**
- **Degradacja – obniżanie wartości atakowanego systemu do stanu, w którym nie może on efektywnie wykonywać swojego zadania. Może to być**

osiągnięte przez zmuszenie przeciwnika do wycofania z użycia zainfekowanej jednostki z sieci, przez zagrożenie rozprzestrzeniania infekcji lub przez wprowadzenie robaka, który przeciąża możliwości przetwarzania danych tego systemu.

- **Dezinformacja (mylenie) – wprowadzenie w błąd atakowanego systemu i spowodowanie generowania fałszywej informacji lub potraktowanie fałszywych danych jako prawdziwe.**
- **Eksploatacja – użycie środków, za pomocą których następuje transmisja informacji z systemu atakowanego do atakującego**.

Przy stosowaniu tej formy walki, w grę może wchodzić szeroka gama celów. Jednakże w każdym wypadku rozważyć należy potrzeby i techniczne możliwości, zanim opracuje się plan zastosowania walki w sferze przetwarzania danych cyfrowych.

Fazy ataku informatycznego

Atak informatyczny składa się z serii kolejnych kroków, następujących w określonej wcześniej kolejności. Jak już wspomniano, w ramach tego ataku użyte mogą być wirusy, robaki, bomby logiczne, bomby programowane czasowo, konie trojańskie lub ich odpowiednie kombinacje. Wszystkie one są formą złośliwych kodów. Atak ten składa się z następujących faz:

- **penetracji – wówczas to następuje wprowadzenie złośliwego kodu do atakowanego systemu zwykle przez jego najsłabiej zabezpieczone połączenie;**
- **rozwoju – wtedy to złośliwy kod przenika przez system w kierunku zaplanowanego obiektu ataku;**
- **uśpienia – w tym okresie wprowadzony kod pozostaje w ukryciu do czasu jego aktywacji;**
- **realizacji – wówczas to następuje aktywacja kodu i wykonanie przezeń zaplanowanego działania;**
- **zakończenia – po wykonaniu swego zadania, złośliwy kod powraca do stanu uśpienia i gotowości do wykonania kolejnego ataku lub ulega samolikwidacji w celu zatarcia śladów swojego działania**.

Faza penetracji

Wprowadzenie kodu komputerowego do atakowanego systemu jest prawdopodobnie najtrudniejszą fazą ataku. Związane są z tym dwa aspekty, które należy rozważyć. Są nimi miejsce oraz metoda penetracji.

Miejsce penetracji. Złośliwy kod może być wprowadzony do atakowanego systemu bezpośrednio (penetracja bezpośrednia) lub może przeniknąć do urządzeń peryferyjnych lub słabiej zabezpieczonych węzłów łączności, a następnie przemieścić się do miejsca docelowego (penetracja pośrednia). Często atakowany system jest dobrze zabezpieczony i odporny na bezpośrednie ataki. Dlatego też atakujący, zmuszany jest do szukania sposobów penetracji pośredniej.

Metoda penetracji. Wyróżnia się przenikanie czołowe i tylne.

Przenikanie czołowe jest określane jako wnikanie do obiektu ataku, przy wykorzystaniu typowych dla danego urządzenia nośników. Przykładem może tu być

włożenie dyskietki do czytnika dyskietek lub skierowanie fal radiowych na antenę odbiorczą. W czasie użycia tej metody penetracji, złośliwy kod przyjmuje zwykle formę ukrytego w legalnym programie konia trojańskiego.

Przenikanie tylne to użycie wszelkich możliwych technik, które umożliwiają przeniknięcie złośliwego kodu przez media nietypowe dla danego systemu. Przenikanie takie, może np. nastąpić przez sieć energetycznego zasilania, urządzenia stabilizujące zasilanie, propagację fal radiowych wysokiej częstotliwości lub starannie kontrolowane impulsy elektromagnetyczne. Możliwe jest także umieszczanie ukrytych, złośliwych kodów w podzespołach dostarczanych przeciwnikowi urządzeń lub w innych wypadkach umożliwiających ich blokadę, gdy dostaną się w niepowołane ręce. Program w formie konia trojańskiego może być uaktywniony przez zakodowany sygnał radiowy. Szczególnie ciekawą metodą jest zaprojektowanie zainfekowanego procesora i umożliwienie jego skopiowania, po to, by został umieszczony w systemie przeciwnika. Przykłady zastosowań różnych miejsc i metod penetracji obrazuje tabela 9.

Tabela 9. Przykłady zastosowań różnych miejsc i metod penetracji

	Penetracja bezpośrednia	**Penetracja pośrednia**
Przenikanie czołowe	Złośliwy kod jest wprowadzany bezpośrednio do programu listy płac przez zaufanego pracownika używającego terminalu.	Złośliwy kod jest transmitowany drogą radiową przez niezabezpieczoną sieć łączności lotniczej. Odbierający go samolot transmituje go do stanowiska dowodzenia (obiekt ataku) w kodowanej sesji łączności.
Przenikanie tylne	Koprocesor z zainstalowanym złośliwym kodem jest umieszczony w zakupionej przez przeciwnika grupie podzespołów i instalowany w głównej sieci systemu pokładowego.	Wyrafinowany terrorysta używa impulsów elektromagnetycznych celem wprowadzenia złośliwych kodów do komputerów firmy energetycznej, doprowadzając do awarii sieci energetycznej w mieście.

Faza rozwoju

Z chwilą przeniknięcia złośliwego kodu do systemu, kod ten musi dotrzeć do planowanego miejsca ataku. Obiektem ataku mogą być wszystkie komponenty systemu lub konkretny zestaw danych. Atak może być dokonywany zarówno na oprogramowanie, jak i na podzespoły (hardware). Może to być zarówno serwer przechowujący najważniejsze dane, jak i węzeł łączności. Najważniejszą sprawą jest tu szczególnie staranne uświadomienie sobie celu ataku i w odniesieniu do tego sprecyzowanie atakowanego obiektu. Jeśli złośliwy kod został wprowadzony bezpośrednio do systemu, musi zlokalizować miejsce przeznaczenia i ukryć się do czasu aktywacji. W wielu sytuacjach błędem byłoby projektowanie kodu, który

miałby atakować wszystkie komponenty systemu, gdy cel mógłby być osiągnięty przez zaatakowanie jednego elementu systemu. Projektując atak, należy brać pod uwagę jego skrytość i dążyć do minimalizacji możliwości jego wykrycia. Kod, który się rozprzestrzenia po całym systemie, jest łatwiejszy do wykrycia, a jeśli zostanie wykryty, prawdopodobieństwo wykonania przez niego zadania jest mniejsze. Chwilowo może być konieczne badanie komponentów systemu, po to, by znaleźć właściwy. Jednakże z chwilą ulokowania się w miejscu przeznaczenia, atakujący kod powinien się skasować w miejscach, w których jest niepotrzebny.

Faza uśpienia

Z chwilą dotarcia do miejsca przeznaczenia, złośliwy kod może się zamaskować i pozostawać w uśpieniu do czasu wyznaczonego ataku. Niekiedy wyczekiwanie nie jest potrzebne i atak będzie następował bezpośrednio po infekcji. Jednakże w większości wypadków czas ataku jest ważny dla osiągnięcia ogólnych celów atakującego. Przykładowo, zgrupowanie militarne dążyć będzie do sparaliżowania sieci dowodzenia i kontroli przeciwnika bezpośrednio przed swoją ofensywą. Grupa terrorystyczna może chcieć powiązać atak z jakimś innym zdarzeniem lub chcieć wykonać atak o określonej porze doby. To znacznie utrudnia identyfikację czasu i miejsca przeniknięcia kodu do systemu. Co jeszcze ważniejsze, zniszczenia mogą zostać dokonane na długo przed wykryciem i odpowiedź może być niemożliwa.

Złośliwy kod ataku w sferze przetwarzania danych cyfrowych może pozostać w systemie w stanie uśpienia w całym okresie eksploatacji i nigdy nie być aktywowany. Pozostając w uśpieniu, może oczekiwać na aktywujący go sygnał z zewnątrz i jeżeli zainfekowany system nie został wybrany na obiekt ataku, może nie być w ogóle aktywowany. W tym wypadku złośliwy kod może stanowić zabezpieczenie przed możliwym zastosowaniem w nieprzyjaznym celu i umożliwiać odpowiednie przeciwdziałanie. Faza uśpienia trwa do czasu aktywacji kodu przez odpowiedni mechanizm.

Faza realizacji

Faza realizacji zaczyna się, gdy odpowiedni mechanizm aktywacji wyprowadza kod ze stanu uśpienia i uruchamia jego działanie. Pozostający w uśpieniu złośliwy kod może się uaktywnić w określonym czasie odmierzonym przez zegar systemowy lub uruchomić się po wykonaniu określonej liczby cykli pracy systemu. Niektóre kody uruchomią się natychmiast po wniknięciu do właściwego komponentu systemu; inne zostaną uruchomione za pomocą mechanizmów, takich jak transmisja odpowiedniego sygnału radiowego, logowanie się określonego odpowiednimi danymi użytkownika lub nawet pojawienie się w systemie odpowiednich danych (np. pojawienie się informacji o prośbie na lądowanie samolotu z określonym znakiem wywoławczym, może uruchomić wirusa w systemie kontroli ruchu lotniczego). Niektóre kody mające postać robaków działają natychmiast i nie potrzebują mechanizmu aktywacji. Jeżeli celem działania robaka będzie paraliż sieci telemonitoringu, to bezpośrednio po wniknięciu będzie się on mnożył w systemie

do czasu przeładowania możliwości przetwarzania danych i zdegradowania systemu do poziomu pożądanego przez atakującego. Uruchomiony złośliwy kod wykonuje działanie prowadzące do osiągnięcia jednego z pożądanych celów, którymi są: wzbranianie, degradacja, dezinformacja i eksploatacja.

Wzbranianie. Złośliwy kod może uniemożliwić atakowanemu obiektowi użycie jego systemu. Może tego dokonać na wiele sposobów. Najskuteczniejszym jest zniszczenie danych i zainstalowanych programów wykonawczych. Innym sposobem będzie atak na komponenty sprzętowe systemu. Na przykład wirus, który może zmienić częstotliwość taktowania zegara głównego procesora, może spowodować jego przegrzanie i samodestrukcję. Złośliwy kod może również atakować dynamiczne komponenty systemu, doprowadzając je do przeciążeń, których nie są w stanie wytrzymać, jak np. ciągłe i nieustanne przemieszczanie głowicy dysku magnetycznego komputera do czasu awarii. Wirus może także znieść ograniczenia programowe sterujące pracą poszczególnych komponentów komputera wprowadzając je w strefę przeciążeń niszczących.

Degradacja. Wprowadzony do systemu wspomniany już robak, może go przeładować i drastycznie obniżyć jego efektywność pracy, co uniemożliwi wykonanie zadania, do którego został przeznaczony. W 1988 r. wprowadzony do Internetu robak zaatakował 6000 komputerów podłączonych do światowej sieci i blokując je, spowodował niemalże paraliż sieci. Wiele firm na całym świecie poniosło już wielkie straty w wyniku takich ataków. Jeżeli nawet w takiej sytuacji system komputerowy nie został całkowicie sparaliżowany, to świadomość częściowego zainfekowania i obawa przed złymi konsekwencjami rozprzestrzeniania się infekcji, zmusza do wycofania tego systemu z eksploatacji. Może to być dla atakującego wystarczającym efektem.

Inną formą degradacji są efekty z obszaru psychoelektroniki. Wprowadzony do systemu wirus może powodować szkodliwą dla operatorów pracę monitorów, wskaźników radarowych i innych urządzeń zobrazowania informacji, wywołując bóle głowy i inne negatywne reakcje organizmu.

Dezinformacja. Jedną z form dezinformacji jest umożliwienie normalnego funkcjonowania systemu, przy jednoczesnym zmuszeniu go do traktowania wprowadzanych fałszywych danych jako prawdziwe. Niewielka modyfikacja programu sprawdzania ważności kart kredytowych może być powodem wielkich strat. Wprowadzenie fałszywych danych w sferze militarnej może mieć jeszcze większe konsekwencje. Możliwość imitowania wykrytych obiektów w przestrzeni powietrznej, w sytuacji gdy one nie istnieją – i odwrotnie – ignorowania rzeczywistych środków napadu powietrznego, może umożliwić uzyskanie zaskoczenia, co jest wartością nie do przecenienia. Niezbędna do uzyskania pożądanego efektu jest modyfikacja programu – prosta zmiana znaku „<„ na „>„ może wystarczyć, aby atakujący osiągnął zamierzony cel. Na przykład system kontroli ognia, którego program został zmodyfikowany przez wirus tak, by zamiast ignorować nadlatujące obiekty o prędkości mniejszej niż dźwiękowa, ignorował obiekty o prędkości

większej niż dźwiękowa, zamiast atakować nadlatujące pociski rakietowe, będzie zwalczał własne samoloty poddźwiękowe, które powinny być bezpieczne.

Eksploatacja. Eksploatacja dotyczy uzyskiwania konkretnej informacji z atakowanego systemu. Zakres, w jakim może to być osiągnięte, zależy od stopnia dostępu atakującego do atakowanego systemu. Jeżeli atakujący ma jakikolwiek dostęp do atakowanego systemu, stosowany złośliwy kod może gromadzić informację w wielu miejscach dostępnych dla atakującego. Jeżeli atakujący pozostaje na zewnątrz systemu, dostęp jest trudniejszy, lecz nie niemożliwy. W tym celu mogą być wykorzystane różne skryte kanały komunikowania do przekazania sygnałów, które ułożone w odpowiednie sekwencje mogą nieść wiadomość dla kogoś, kto wie, jak ją odczytać. Na przykład, jeżeli istnieją zasady postępowania zapobiegające transmisji sygnałów z systemu na zewnątrz, atakujący może zastosować kombinację pogwałceń zasad i braku tych pogwałceń. Kombinacja ta – jak kod Morse'a – może zawierać wiadomość. Atakujący potrzebuje jedynie odwrócić działanie zespołu logowania, by uzyskać mechanizm informowania. Systemy komputerowe stają się coraz bardziej zintegrowane za pomocą coraz rozleglejszych sieci, dlatego też stają się one coraz bardziej podatne na ataki w ramach walki w sferze przetwarzania danych cyfrowych.

Faza zakończenia

Zależnie od ogólnych celów atakującego, użyty kod może być zaprogramowany na całkowite samozniszczenie po wykonaniu zadania. Postępując w ten sposób, osiąga się następujące korzyści:

- **Jeżeli atak nie był oczywisty dla atakowanego obiektu, co może mieć miejsce w wypadku działań skrytych, usunięcie atakującego kodu może uniemożliwić zidentyfikowanie prawdziwej przyczyny awarii lub przesłanki tego, że doszło do ujawnienia tajnej informacji.**
- **W wypadku gdy obiekt ataku jest świadomy zaistnienia tego ataku, jednak nie rozpoznaje natury tego ataku, usunięcie atakującego kodu może utrudnić ocenę szkód i zakresu ataku.**
- **Nawet gdy obiekt ataku jest całkowicie świadomy co do formy i skali ataku, to usunięcie atakującego kodu znacznie utrudni zidentyfikowanie sposobu penetracji i podjęcie właściwych przedsięwzięć zapobiegawczych przyszłym atakom.**
- **Usunięcie atakującego kodu czyni także znacznie trudniejsze dla atakowanego ustalenie źródła ataku i identyfikację napastnika. Ustalenie tych danych może prowadzić do poważnych konsekwencji prawnych lub sankcji militarnych w stosunku do atakującego.**

W niektórych szczególnych wypadkach atakujący może chcieć ponownie wprowadzić atakujący kod w stan uśpienia i gotowości do wykonania kolejnego ataku. Na przykład złośliwy kod zainstalowany w eksportowanym zestawie przeciwlotniczym, może spowodować gwałtowny skręt w prawo i ominięcie celu w sytuacji, gdy transmitowany jest pewien ustalony wcześniej sygnał. Dla zaata-

kowanego zestawu przeciwlotniczego wyglądać to może na przypadkową awarię i może on być dalej eksploatowany, gdyż prawdziwy powód nie został odkryty, wszystkie bowiem testy i przypadki użycia przeciwko samolotom niewysyłającym skrytych sygnałów wypadają pomyślnie. Jednakże atakujący będzie wiedział, że jego samoloty emitujące odpowiednie sygnały pozostaną bezpieczne przed atakiem prowadzonym zainfekowanym zestawem przeciwlotniczym.

Pozostawienie atakującego kodu w stanie uśpienia jest ryzykowne, ponieważ atakujący nie będzie wiedział, czy przy następnym ataku zostanie on wykryty przy następnej aktywacji. Atakowany może przygotować przeciwdziałanie lub wykorzystać wykryty kod do wykonania ataku odwetowego. Dlatego też znacznie rozsądniejszym podejściem jest usuwanie atakującego kodu po wykonaniu przez niego zadania. Jedynie gdy penetracja jest skrajnie trudna, a ryzyko przeciwdziałania mniej ważne, można tę opcję rozważać.

Przewidywalność – wspólny mianownik wszystkich ataków w sferze przetwarzania danych cyfrowych

Jeden aspekt walki w sferze przetwarzania danych cyfrowych musi pozostawać niezmienny. Atakujący powinien dokładnie przewidywać efekt, jaki zastosowany kod ma osiągnąć. Poważnym argumentem przemawiającym za tym jest fakt, że użycie kodu o nieprzewidywalnym działaniu może nie doprowadzić do osiągnięcia pożądanego celu ataku. Podstawy definicji walki w sferze przetwarzania danych cyfrowych opierają się na założeniu, że atak jest skierowany przeciwko wyraźnie określonemu obiektowi i dla osiągnięcia klarownego celu. Zastosowanie kodu, który jest nieprzewidywalny, nie spełnia założeń tej definicji. Dlatego też przewidywalność jest głównym czynnikiem rozpatrywanym przy rozważaniu możliwości użycia ataku w sferze przetwarzania danych cyfrowych.

Inny powód, dla którego przewidywalność jest ważnym czynnikiem, jest wspólny dla wszystkich broni. Stare powiedzenie: „kto mieczem wojuje, ten od miecza ginie", nigdy nie było tak prawdziwe, jak obecnie, gdy rozpatrywane są możliwości prowadzenia walki w sferze przetwarzania danych cyfrowych. Jeżeli wirusy komputerowe mają mieć zastosowanie praktyczne, to muszą mieć przewidywalne działanie. **Każda broń powinna mieć możliwości jej uzbrajania i rozbrajania. Złośliwe kody muszą mieć możliwość celowego rażenia i niestwarzania zagrożenia dla ich użytkowników.** Projektanci takich kodów powinni, jednocześnie z ich konstrukcją, opracować programy wykrywania i neutralizacji tych kodów. **Niepomyślnie przebiegający atak, nie powinien spowodować szkód atakującemu.** Tak więc zarówno użytkownicy, jak i projektanci broni sfery przetwarzania danych cyfrowych, powinni być świadomi ryzyka i konieczności spełnienia wymagania przewidywalności przy opracowywaniu kodów mających zastosowanie w tej walce.

Rodzaje atakowanych systemów

W ramach ataku informatycznego, atakowane mogą być dowolne systemy, które wykorzystują kody cyfrowe do gromadzenia, analizowania, przetwarzania i dystrybucji informacji i umożliwiają skryte wprowadzenie do nich kodu cyfrowego. Rozważając zakres możliwych obiektów ataku, warto zauważyć, iż z polityczno-militarnego punktu widzenia, dla atakującego byłoby najlepiej, gdyby niemal każdy system wrażliwy na atak został skrycie zainfekowany odpowiednim kodem, który byłby kontrolowany przez atakującego. Z przyczyn praktycznych jest to jednak niemożliwe. Dlatego też obiekty ataku muszą być oceniane i wartościowane według hierarchii ich ważności, tak samo, jak to się czyni na potrzeby ataków konwencjonalnych.

Walka w sferze przetwarzania danych cyfrowych może być prowadzona różnymi sposobami. Może ona być bardzo dokładną, precyzyjnie kierowaną bronią, zabójczą jedynie dla obiektu ataku, z nieznacznymi lub żadnymi zniszczeniami towarzyszącymi. Przykładowo, odpowiednia pamięć EPROM zainstalowana w samolocie myśliwskim przed jego eksportem, paraliżująca system kontroli lotu, gdy pojawi się odpowiedni sygnał radiowy lub wirus zainstalowany w sieci łączności przeciwnika, który paraliżuje utajnioną łączność przeciwnika w określonym czasie, może być taką bronią. Użycie jej w cyberprzestrzeni stanowi ekwiwalent pocisku rakietowego kierowanego, czy nawet pocisku typu Cruise.

O tym, że nie jest to tylko teoria, świadczy wiele przykładów. O jednym z nich piszą Egmont R. Koch i Jochen Sperber:

„[...] Sowiecka służba specjalna wyraziła szczególne zainteresowanie prototypowym softwarem systemowym w kodzie źródłowym, kompilatorami i sterowaniem procesami produkcyjnymi, ponadto różnymi programami do wspomaganego komputerowo konstruowania elementów mechanicznych, elektrycznych i elektronicznych w budowie pojazdów, samolotów i przy produkcji chipów, a także informacjami o wojskowym wykorzystaniu amerykańskich komputerów i banków danych. [...] Tak wielkie zainteresowanie KGB kodem źródłowym świadczy o tym, że Sowieci obawiali się zakupów oprogramowania systemowego na Zachodzie. Podejrzewali, że mogą sobie sprowadzić konia trojańskiego, gdyż nie mają żadnej kontroli nad kupowanym softwarem. Być może, mieli już złe doświadczenia z towarami objętymi embargiem, które sprowadzali z Zachodu nielegalnymi kanałami.

Monachijska *MI Group* zajmowała się swego czasu kontrolą sowieckiej misji wojskowej w Berlinie Wschodnim, która miała prawo poruszać się swobodnie w dawnych strefach okupacyjnych aliantów, a więc w Niemczech Zachodnich. Tak samo amerykańskie, brytyjskie i francuskie misje wojskowe miały prawo wjeżdżać do NRD. Sowieci zamówili wówczas swoją flotę samochodów dyplomatycznych u Opla. „Żółte owoce" otrzymały zlecenie umieszczenia w samochodach elektronicznych pluskiew. W tym też celu wprowadzono do Opla agenta jako pracownika firmy, a dodatkowo strażnika, ponieważ akcję zamierzano przeprowadzać nocą. Przed rozpoczęciem operacji grupa ćwiczyła na terenie monachijskich koszar McGraw rozbieranie i fachowe składanie samochodu-atrapy.

Kiedy nadszedł czas, agenci z US Army zjechali z różnych krajów do Frankfurtu, zostali przewiezieni do odpowiedniej hali i zabrali się za rozbieranie pierwszego wozu dyplomatów. W jego ramy wbudowali miniaturowy nadajnik, połączyli go z wieloma pluskwami rozmieszczonymi na „niebie" samochodu, a następnie złożyli całego opla. W przeciągu kilku miesięcy Amerykanie obsłużyli z tuzin samochodów dla sowieckiej misji w Berlinie Wschodnim. Akcja zakończyła się powodzeniem. Podsłuchane rozmowy umożliwiły zdemaskowanie wielu agentów radzieckich w Niemczech Zachodnich"[183].

Z drugiej strony walka w sferze przetwarzania danych cyfrowych stosowana będzie celem wywołania zniszczeń na szeroką skalę. Wirus zainstalowany w komputerze kontrolującym sieć energetyczną regionu, spowodowałby rozległe spustoszenia mające swoje konsekwencje w sferze militarnej i cywilnej. Zaatakowanie sieci finansowej kraju i paraliż głównych węzłów komunikacji finansowej, mogłyby spowodować długoterminowy efekt dewastujący ekonomię tego kraju. Takie lub jeszcze rozleglejsze użycie walki informacyjnej może przynosić skutki porównywalne z użyciem broni jądrowej.

4.2.2. Atak elektroniczny

Atak elektroniczny polega na użyciu energii elektromagnetycznej do atakowania siły żywej, infrastruktury lub sprzętu w celu degradowania, neutralizowania lub niszczenia zdolności bojowych nieprzyjaciela. Atak elektroniczny w obecnych warunkach rozwoju, oparty na kryterium zakresu widma promieniowania elektromagnetycznego, zawiera **atak laserowy** i **atak elektromagnetyczny**[184]. Ze względu na uzyskiwane efekty atakowania, w ramach tego ataku wyróżnić można **zakłócanie**. Zakłócanie wywołuje łagodniejsze skutki, gdyż powoduje czasowe zdegradowanie lub sparaliżowanie funkcjonowania systemów wykorzystujących promieniowanie elektromagnetyczne, zaś **atak w pełnym wymiarze** powoduje destrukcję fizyczną elementów tych systemów, co skutkuje trwałym przerwaniem wykonywanych funkcji.

W dotychczasowej praktyce wykorzystanie energii elektromagnetycznej realizowane było głównie w formie **zakłócania elektromagnetycznego**. Obecnie, ze względu na poziom rozwoju technologicznego, pojawia się możliwość praktycznego wykorzystania energii elektromagnetycznej do rażenia obiektów ataku, wobec czego wyłania się możliwość prowadzenia **ataku elektromagnetycznego**.

---

[183] E.R. Koch, J. Sperber, *Infomafia*... s. 246.

[184] Nazwa „elektromagnetyczny" nie jest tu najbardziej adekwatna, gdyż całe spektrum jest elektromagnetyczne. Jednak trudno znaleźć odpowiedniejszą nazwę, gdyż wykorzystywany zakres fal jest szeroki, a funkcjonujące nazwy zakresów nie pokrywają się z wykorzystywanym pasmem. Najbliższym jest pasmo fal radiowych, lecz nazwanie ataku radiowym, wywoływałoby inne skojarzenia. Dlatego przyjęto taką nazwę.

Zakłócanie laserowe i elektromagnetyczne

Zakłócanie laserowe prowadzone jest w celu oślepienia sensorów optoelektronicznych lub ludzkiego wzroku. Ze względu na różne stopnie wrażliwości, ta sama wiązka energii może stanowić zakłócanie w stosunku do jednego zespołu sensorów, atak zaś w stosunku do innego. Mniej wrażliwe, będą bowiem oślepione, a bardziej wrażliwe zniszczone. Dlatego też decydującym kryterium jest tu zamiar prowadzącego walkę i przeprowadzenie działań zgodnie z tym zamiarem.

Zakłócanie elektromagnetyczne[185] jest celowym emitowaniem, retransmitowaniem lub odbijaniem energii elektromagnetycznej w celu zapobiegania efektywnemu wykorzystaniu przez przeciwnika elektromagnetycznego spektrum lub redukowania efektywności tego wykorzystania i zdegradowania lub neutralizowania możliwości bojowych nieprzyjaciela.

W początkowym okresie stosowania zakłócania jego wysiłek był skierowany przede wszystkim na degradowaniu możliwości wykrywania radarów przeciwnika i maskowaniu obecności własnych samolotów w przestrzeni powietrznej oraz na pogarszaniu celności uzbrojenia kierowanego za pomocą radaru. Obecnie zakłócanie systemu wykrywania przeciwnika ogranicza jego dostęp do informacji o ruchu, składzie i ugrupowaniu środków napadu powietrznego, wprowadzając zamieszanie i niepewność. Skuteczne zakłócanie systemu dowodzenia i kontroli przeciwnika może zdezorganizować jego proces decyzyjny i wykonanie zadań. Współczesne duże uzależnienie od scentralizowanego kierowania, stwarza doskonałą okazję do efektywnego zastosowania ataku elektronicznego.

Atak laserowy

Generatory laserowe będą wykorzystywane do prowadzenia **ataku laserowego**. Promieniowanie laserowe, o odpowiednio dużej mocy, działa tak samo destrukcyjnie, jak materiał wybuchowy. Czynnikami rażenia są tu: wysoka temperatura oraz mogąca się pojawić w związku z nią fala uderzeniowa. Atak polega na wygenerowaniu jak najbardziej skupionej wiązki laserowej i skierowaniu jej na pożądany punkt trafienia atakowanego obiektu. W wyniku pomyślnego ataku, następuje fizyczne zniszczenie podobne do skutków uzyskiwanych za pomocą klasycznej broni.

Atak elektromagnetyczny

Atak elektromagnetyczny[186] jest prowadzony przy wykorzystaniu strumieni energii promieniowania elektromagnetycznego. Źródłem tego promieniowania mogą być generatory różnego typu. Generatory promieniowania w pasmach me-

---

[185] Obszerna dekompozycja zakłócania elektromagnetycznego prowadzonego przez siły powietrzne i jego charakterystyka zawarta jest w pracy Z. Dubrawskiego, *Walka radioelektroniczna...* wyd. cyt.

[186] Opracowano na podstawie: C. Kopp, *The E-Bomb – A Weapon of Electrical Mass Destruction,* http://www.cs.monash.edu. au/carlo/ 04.1997 r.

trowych, decymetrowych, centymetrowych, a nawet milimetrowych zostały odkryte i praktycznie zastosowane na przykład w radiolokacji. Dostrzeżono także możliwości wykorzystania generowanej przez nie energii do destrukcyjnych celów walki. Prace w tym obszarze są prowadzone na szeroką skalę. Ich rezultaty są ujawniane jedynie w niewielkim stopniu. W podrozdziale tym omówiona jest praktyczna możliwość zastosowania dwóch typów generatorów w formie uzbrojenia lotniczego, to jest najbardziej odpowiedniego dla sił powietrznych.

Ogólna charakterystyka środków rażenia ataku elektromagnetycznego

Wysokoenergetyczny impuls elektromagnetyczny został wykryty w czasie próbnych eksplozji jądrowych w latach pięćdziesiątych dwudziestego stulecia. Impulsy elektromagnetyczne małej mocy są powszechnie stosowane w wielu dziedzinach techniki i technologii. Jednakże skonstruowanie niejądrowego urządzenia wytwarzającego odpowiednio silny impuls elektromagnetyczny dla potrzeb militarnych zajmowało dużo czasu. Stopniowo pokonywano bariery technologiczne i psychologiczne, w efekcie czego pojawiła się możliwość militarnego zastosowania tego zjawiska. Ze względu na potencjalne skutki zastosowania tego typu broni zaliczono ją do kategorii broni masowego rażenia. W związku z tym jej rozwój i charakterystyki utrzymywane są w tajemnicy. Jednakże z dostępnych danych wyłania się dosyć klarowny obraz obecnego stanu rozwoju. Zestaw generacji impulsu elektromagnetycznego jest dowolnym urządzeniem jądrowym lub konwencjonalnym, zdolnym do wygenerowania chwilowego bardzo intensywnego, ale krótkiego pola elektromagnetycznego. Dla potrzeb militarnego rażenia, impuls tego pola musi być dostatecznie intensywny, zdolny do wytworzenia takiej gęstości mocy elektromagnetycznej, która jest niszcząca dla sprzętu elektronicznego i elektrycznego.

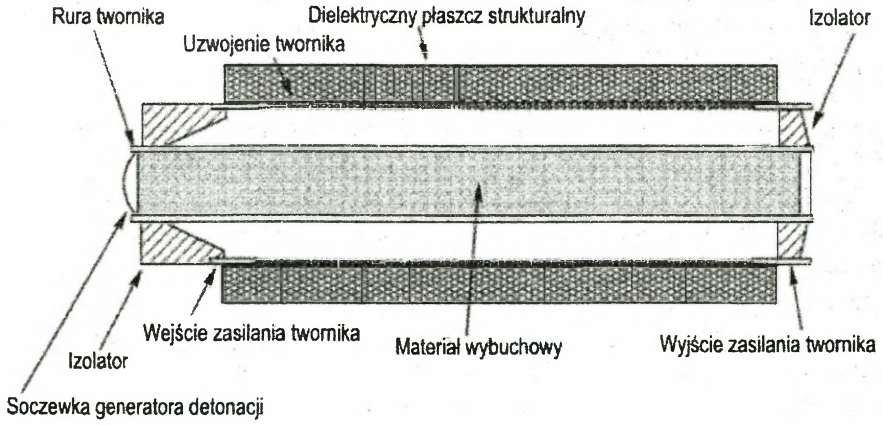
Wytworzony przez generator impuls energii wytwarza silne pole magnetyczne, szczególnie w otoczeniu generatora. Pole to może być na tyle silne, że wytwarza krótkie, ale wysokie napięcia rzędu tysięcy woltów w znajdujących się w jego zasięgu przewodnikach. W rezultacie może to spowodować zniszczenie dużej ilości zróżnicowanych urządzeń elektronicznych i elektrycznych. Zniszczenia mogą być znaczne i mogą wymagać specjalistycznych napraw lub całkowitej wymiany sprzętu. Szczególnie wrażliwe są oczywiście urządzenia cywilne, zupełnie nieodporne na tego typu oddziaływania. Wrażliwość ta gwałtownie się zwiększyła, w wyniku masowego zastosowania półprzewodników oraz ich miniaturyzacji i wytwarzania coraz większych skal integracji. Elementy tego typu są bardzo wrażliwe na niewielkie przepięcia, rzędu nawet kilku czy kilkudziesięciu volt. Takie elementy ulegną całkowitemu zniszczeniu. Inne, bardziej odporne, nie wytrzymają przeciążeń termicznych i jeżeli nie zostaną całkowicie zniszczone, to mogą być znacznie uszkodzone. W rezultacie, jeżeli jakieś urządzenie będzie nadal funkcjonowało, to jego praca może być niewłaściwa i niepewna. Mając na względzie niezwykle szerokie zastosowanie elementów elektronicznych i elektrycznych w każdej niemalże sferze ludzkiej aktywności, należy zagrożenie tego typu trakto-

wać jako bardzo niebezpieczne, mogące prowadzić do paraliżu funkcjonowania wielu sfer społecznej aktywności w rejonie porażenia. Również współczesny sprzęt militarny jest wysoce zelektronizowany i mimo częściowych zabezpieczeń bardzo wrażliwy na takie ataki.

W praktyce stosuje się co najmniej trzy rodzaje niejądrowych generatorów produkujących takie impulsy. Jeden rodzaj obejmuje eksplozyjnie pompowany kompresyjny generator strumieniowy (*explosively pumped flux compression generator – FCG*). Drugim są oparte na materiale wybuchowym lub paliwie sterowane eksplozją generatory magnetohydrodynamiczne (*MHD*). Ponadto stosowana być może grupa urządzeń mikrofalowych wielkiej mocy (*HPM*), a z nich przede wszystkim oscylatory z wirtualną katodą lub vircatory. Wiele różnorodnych konstrukcji tego typu było opracowanych i testowanych. Ślady tej aktywności znaleźć można w jawnej literaturze.

Eksplozyjnie pompowany kompresyjny generator strumieniowy FCG jest najbardziej dojrzałym zestawem przydatnym do stosowania w konstrukcji bomb lotniczych. Urządzenia tego typu były szeroko testowane w Stanach Zjednoczonych, ZSRR oraz WNP. Generator tego typu wykorzystuje energię zainstalowanych źródeł zasilania i eksplozji materiału wybuchowego. Może wytwarzać dziesiątki megadżuli w czasie od dziesiątek do setek mikrosekund. Osiągany w rezultacie tego prąd szczytowy jest tysiąc razy większy od typowego burzowego wyładowania atmosferycznego.

Fizyczna istota generatora FCG. Szybka eksplozja spręża pole magnetyczne. Kompresja ta zamienia energię mechaniczną w pole magnetyczne. Prąd szczytowy rzędu megaamperów był demonstrowany w wielu eksperymentach. Prąd rozruchowy jest dostarczany przez źródło zewnętrzne w postaci: baterii kondensatorów, małego generatora FCG, urządzenia magnetohydrodynamicznego lub prądnicy jednakobiegunowej (rys. 28).

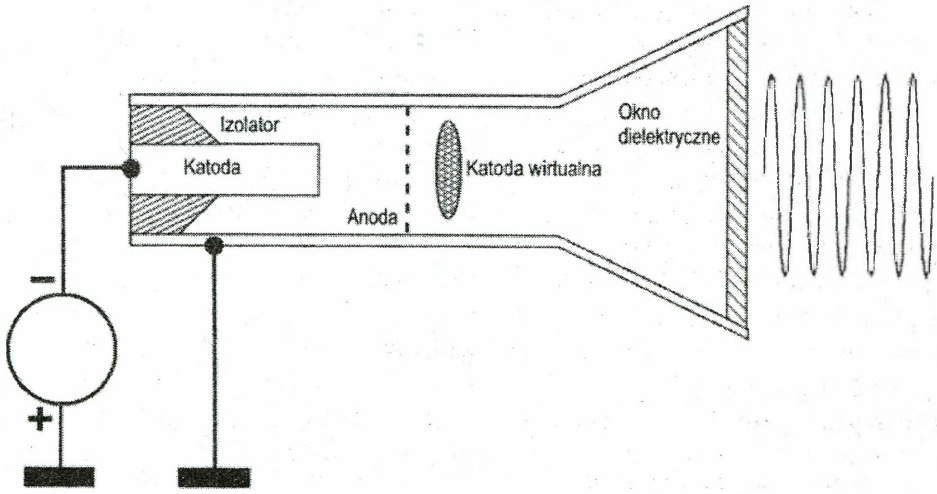


Źródło: C. Kopp, *The E-Bomb – A Weapon of Electrical Mass Destruction*, http://www.cs.monash.edu.au/carlo/ 04.1997 r.

Rys. 28. Eksplozyjnie pompowany kompresyjny generator strumieniowy – FCG

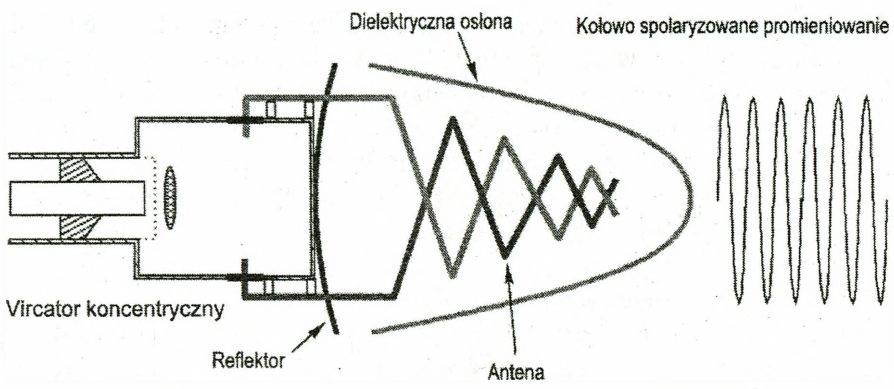
Ze względu na większe problemy technologiczne generatory magnetohydrodynamiczne MHD znajdują mniejsze zastosowanie. W konstrukcji tej wykorzystuje się przemieszczającą się przez pole magnetyczne plazmę, wytworzoną w wyniku eksplozji. Konstrukcja tego typu nadaje się raczej na pociski artyleryjskie do wykonania wielokrotnych ataków na stosunkowo niewielką powierzchnię.

Technologia FCG umożliwia generację wielkich impulsów elektrycznych, ograniczonych jednak do częstotliwości poniżej 1 MHz. Wiele obiektów jest trudnych do atakowania, nawet tak dużymi wielkościami mocy zawartej jednak w drganiach o stosunkowo małej częstotliwości. Ponadto skupienie energii o takiej częstotliwości jest trudne. Urządzenia mikrofalowe wielkiej mocy HPM rozwiązują ten problem, ponieważ generowana energia może zostać skupiona i ma większe możliwości penetracji różnorodnych obiektów ataku. Istnieje spora grupa różnych rozwiązań konstrukcji typu HPM. Należą do nich m.in. klistrony, magnetrony, urządzenia wolnej fali, triody refleksyjne, oscylatory z pozorną katodą (vircatory). Jednak z punktu widzenia potrzeb konstrukcji bomby lotniczej, najlepiej nadaje się do tego celu vircator – urządzenie generujące jeden bardzo silny impuls promieniowania. Impuls ten ma prosty charakter, może jednak mieć częstotliwość mieszczącą się, w zależności od potrzeb, w szerokim spektrum wartości zakresu mikrofalowego (rys. 29 oraz 30).



Źródło: C. Kopp, *The E-Bomb – A Weapon of Electrical Mass Destruction*, http://www.cs.monash.edu.au/carlo/ 04.1997 r.

Rys. 29. Vircator – urządzenie generujące jeden silny impuls promieniowania



Źródło: C. Kopp, *The E-Bomb – A Weapon of Electrical Mass Destruction*, http://www.cs.monash.edu.au/carlo/ 04.1997 r.

Rys. 30. Vircator z zestawem antenowym

Urządzenie to wykorzystuje efekt uderzenia rozpędzonej gęstej wiązki elektronów w siatkową lub foliową anodę. W efekcie przebicia tej anody, w przestrzeni za nią tworzy się naładowana bańka przestrzeni. W odpowiednich warunkach będzie ona oscylować z częstotliwością mikrofalową. Jeżeli ładunek taki zostanie umieszczony w odpowiednio dostrojonej przestrzeni rezonansowej, zostanie uzyskana bardzo duża moc szczytowa takiego impulsu. Normalne techniki formowania energii mikrofalowej umożliwiają wyprowadzenie jej z komory rezonansowej. W zależności od potrzeb, generator taki może uzyskiwać różne częstotliwości. Długość otrzymanego impulsu mieści się w przedziale mikrosekund. Energia takiego impulsu zawierać się może w szerokim zakresie mocy – od 170 kilowatów do 40 gigawatów, przy częstotliwościach rozciągających się w zakresach decymetrowym i centymetrowym.

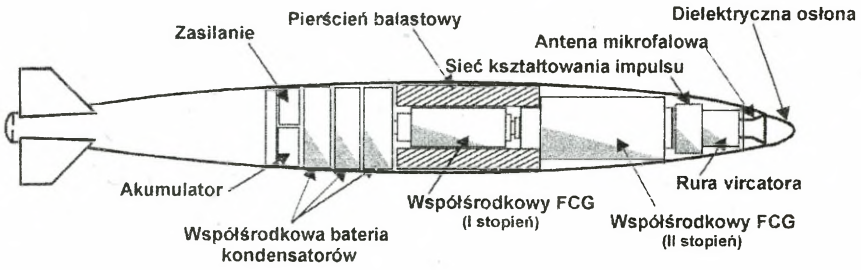
Zdolności rażenia głowic bomb elektromagnetycznych są trudne do jednoznacznego określenia, ze względu na różnorodność obiektów ataku. Jednakże zdolności rażące tego typu broni są duże, a głównym czynnikiem siły rażenia jest efektywność przenikania generowanego promieniowania. Promieniowanie to może wnikać do obiektów ataku w formie przenikania czołowego (*front door coupling*), głównie przez anteny. Penetrujące promieniowanie niszczy wówczas elementy półprzewodnikowe przekaźników i odbiorników. Rażąca energia może wnikać również do atakowanych obiektów przez wszelkiego rodzaju kable energetycznego zasilania i przesyłania danych oraz linie telefoniczne. Impulsy zakresu centymetrowego i milimetrowego wnikać mogą także przez kanały wentylacyjne, szczeliny i słabo zabezpieczone mufy, wywołując przestrzenną falę, stojącą we wnętrzu urządzeń. Energia takich impulsów niszczy wówczas narażone na oddziaływanie urządzenia półprzewodnikowe, przebija izolacje transformatorów i przewody. Tego typu penetracja nazywana jest przenikaniem tylnym (*back door coupling*).

Mechanizm destrukcji bomb elektromagnetycznych polega na tym, że impulsy małej częstotliwości, wytwarzane przez FCG, indukują impulsy wysokiego napięcia w przewodach elektrycznych, a promieniowanie mikrofalowe zestawów HPM tworzy fale stojące wysokiego napięcia w przewodnikach.

Przykładowe możliwości bojowe: 10 Gigawatowa 5 GHz bomba typu HPM zdetonowana na wysokości kilkuset metrów tworzy strefę o średnicy rażenia około 400–500 metrów, z polem o natężeniu rzędu kilowoltów/metr.

Obiekty ataku bombami elektromagnetycznymi

Bombami elektromagnetycznymi (rys. 31) można atakować szerokie spektrum obiektów. Niektóre z nich można łatwo zidentyfikować. Do takich należą z pewnością budynki mieszczące siedziby organów państwowych i samorządowych, a także urządzenia produkcyjne, bazy militarne, posterunki radiolokacyjne, węzły komunikacyjne. Tego typu obiekty mogą być stosunkowo łatwo identyfikowane, za pomocą konwencjonalnych metod rozpoznania. Są zazwyczaj obiektami stałymi, dlatego sposób ataku powietrznego może być wcześniej zaplanowany i uwzględniać zrzut ładunków poza obszarem obiektu ataku i dolot bomb w rejon celu. Jest to możliwe szczególnie teraz, gdy są dostępne bomby precyzyjnie nawigowane i zdalnie sterowane. Umożliwia to zdetonowanie ładunku bojowego i emisję fali elektromagnetycznej w optymalnym miejscu i na pożądanej wysokości.



Źródło: C. Kopp, *The E-Bomb – A Weapon of Electrical Mass Destruction*, http://www.cs.monash.edu.au/carlo/ 04.1997 r.

Rys. 31. Bomba elektromagnetyczna z generatorem typu FCG

Obiekty mobilne i zamaskowane, ale promieniujące energię, mogą być również rozpoznane i zaatakowane. Mobilny sprzęt OP, ruchome węzły łączności czy okręty – reprezentują tę kategorię obiektów ataku. Promieniując, mogą być namierzane i wyznaczane do ataku. Większość obiektów tego typu przemieszcza się raczej powoli i nie są w stanie wykonać uniku przed bombą.

Mobilne i ukryte, a niepromieniujące obiekty mogą sprawiać trudność, szczególnie przy zastosowaniu konwencjonalnych sposobów wpykrywania. Istnieją jed-

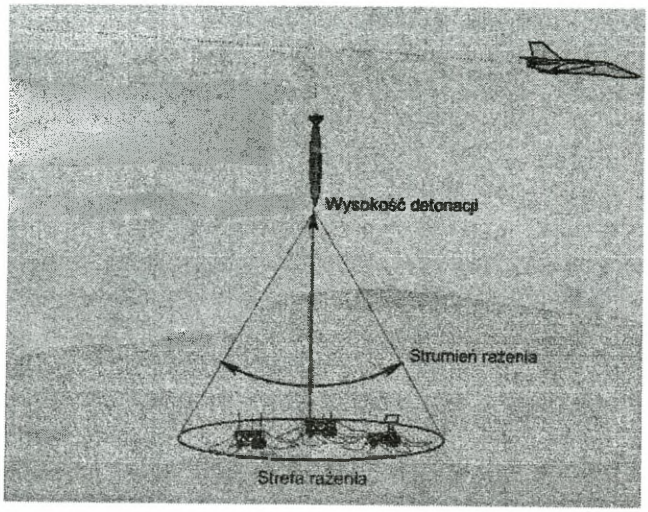
nakże niekonwencjonalne sposoby wykrywania, wykorzystujące różne niezamierzone emisje. Zidentyfikowanie typu emisji i ustalenie czy jest to promieniowanie komputerowego monitora, urządzeń peryferyjnych, jednostki centralnej, energetycznych przełączników, silników elektrycznych, silnikowych urządzeń zapłonowych, innych urządzeń energetycznych, odbiorników superheterodynowych, kabli sieciowych, umożliwi określenie charakterystyki obiektu. Tego typu identyfikacja była stosowana już w czasie wojny w Wietnamie, gdzie zamontowane na samolocie urządzenie wykrywało i namierzało pracę układu zapłonowego silnika, co umożliwiało zidentyfikowanie dyslokacji pojazdu, po czym zniszczenie go za pomocą dział pokładowych.

Sposoby atakowania konwencjonalnymi bombami elektromagnetycznymi

Ze względu na właściwości i technologiczne ograniczenia najbardziej dostępne mogą być bomby lotnicze wypełnione odpowiednimi generatorami impulsów dużej mocy. Bomby tego typu przenoszone przez nosiciela w rejon obiektu ataku mają tę zaletę, że mogą korzystać ze źródła zasilania nosiciela do ładowania baterii inicjujących. Jednak dzięki postępowi technologicznemu również pociski samosterujące, pociski z silnikami rakietowymi i ślizgowe bomby lotnicze mogą być uzbrajane w głowice elektromagnetyczne. Detonacja głowicy nastąpi albo przez automatyczny pokładowy system inicjujący, albo na komendę operatora. W wypadku urządzeń automatycznych, komendę do detonacji może przekazać urządzenie nawigacyjne po osiągnięciu określonej pozycji albo radar pokładowy po wykryciu obiektu ataku i znalezieniu się w jego otoczeniu. Może to być również zapalnik pocisku rakietowego klasy powietrze-powietrze, wykrywający obecność w bezpośrednim sąsiedztwie obiektu ataku. Zapalnik lotniczej bomby elektromagnetycznej może być inicjowany przez radiowysokościomierz, pokładowy system nawigacyjny (np. inercyjny, lub GPS) czy wysokościomierz barometryczny (rys. 32 oraz 33).

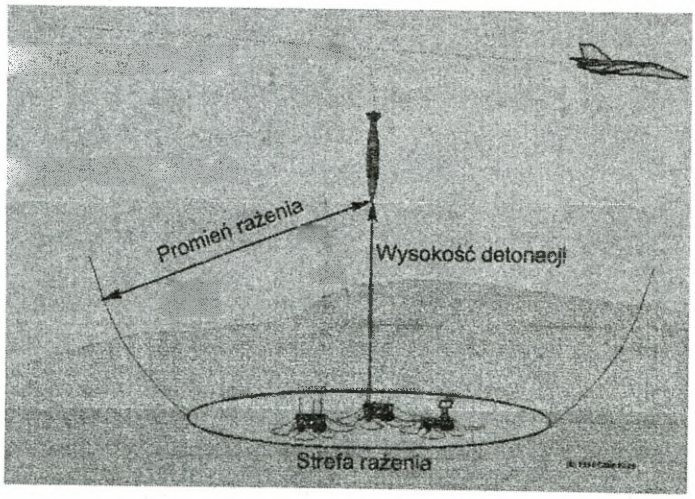
W związku z tym, że promień elektromagnetycznego rażenia będzie zdecydowanie większy w porównaniu do promienia rażenia konwencjonalnej bomby tego samego wagomiaru, to i sposoby atakowania mogą mieć charakter zrzutu dystansowego w stosunku do obiektu ataku bez konieczności pojawiania się nosiciela nad tym obiektem.

Miniaturyzacja oraz postęp technologiczny umożliwiają konstruowanie coraz doskonalszych środków dystansowego ataku, zdolnych do samodzielnego pokonywania coraz większych odległości. Stosowanie tego typu środków do umieszczania na nich głowic elektromagnetycznych, umożliwia bezpieczne pokonanie obrony przeciwlotniczej obiektu, zapobiega oddziaływaniu rażącego impulsu na samolot nosiciel oraz zapewnia dobór optymalnej trajektorii ataku (rys. 34).



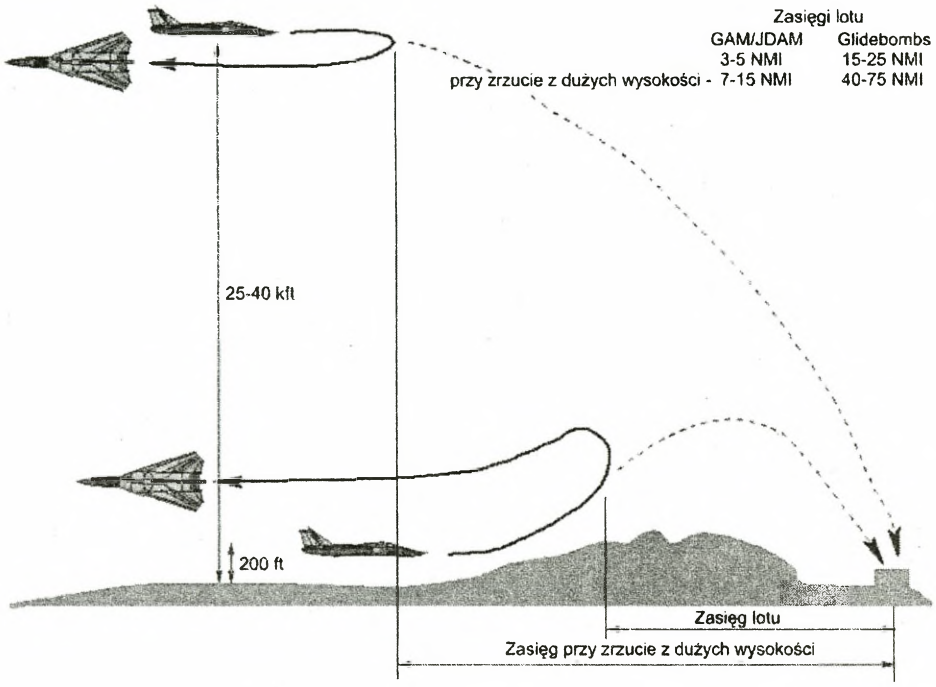
Źródło: C. Kopp, *The E-Bomb – A Weapon of Electrical Mass Destruction* http://www.cs.monash.edu.au/carlo/ 04.1997 r.

Rys. 32. Promień i strefa rażenia bomby elektromagnetycznej



Źródło: C. Kopp, *The E-Bomb – A Weapon of Electrical Mass Destruction*, http://www.cs.monash.edu.au/carlo/ 04.1997 r.

Rys. 33. Strumień rażenia bomby elektromagnetycznej



Źródło: C. Kopp, *The E-Bomb – A Weapon of Electrical Mass Destruction*, http://www.cs.monash.edu.au/carlo/ 04.1997 r.

Rys. 34. Atakowanie bombami elektromagnetycznymi

Główną zaletą bomb elektromagnetycznych jest to, że mogą być stosowane przez dowolny samolot bojowy lotnictwa taktycznego, zdolny do przenoszenia bomb kierowanych nawigacyjnie. Takie samoloty staną się w niedługim czasie standardowym wyposażeniem lotnictwa państw Zachodu i będą mogły być uzbrojone również w bomby elektromagnetyczne.

Ponieważ bomby te będą znacznie prostsze w konstrukcji i obsłudze, i tańsze w produkcji od pocisków przeciwradiolokacyjnych, należy oczekiwać, że znajdą się one w szerokim zakresie w dyspozycji dowódców. Również ze względu na prostotę ich zastosowania i dużą zdolność rażenia, będą coraz powszechniej stosowane we współczesnej walce.

Działania walki elektronicznej z użyciem bomb elektromagnetycznych

Walka elektroniczna może być prowadzona w formie trwałej lub tymczasowej destrukcji. Tymczasowa destrukcja skutkuje zatrzymaniem na określony czas wykonywania funkcji danego zestawu, systemu, komponentu. Całkowite wyeliminowanie atakowanego obiektu z funkcjonowania – jest destrukcją trwałą. Bomby

elektromagnetyczne będą głównie używane do przerywania lub zakłócania przepływu strumieni informacyjnych systemów dowodzenia i kontroli, a także kierowania sprzętem bojowym. Bombami tymi można wykonywać zarówno trwałą, jak i tymczasową destrukcję. Zależy to od siły rażenia bomby, ale też od stopnia odporności obiektu ataku. Trwała destrukcja nastąpi w sytuacji fizycznego zniszczenia całości lub większości zespołów i podzespołów elektronicznych i elektrycznych atakowanego obiektu. Gdy celem walki będzie trwałe eliminowanie elementów ugrupowania bojowego, a szczególnie tych związanych z dowodzeniem i kontrolą, to za atakiem elektromagnetycznym powinien następować atak ogniowy. Atak ten, wykonany konwencjonalną amunicją, zapobiegnie naprawie uszkodzonego sprzętu i utrwali osiągnięte skutki na dłuższy czas.

Bomby elektromagnetyczne mogą być użytecznym narzędziem obezwładniania środków obrony powietrznej. Mogą nawet skutecznie rywalizować z pociskami przeciwradiolokacyjnymi. Szczególnie gdy znana jest dyslokacja atakowanego obiektu, skutki ich rażenia mogą znacznie przekraczać te, które można osiągnąć w wyniku zastosowania pocisków przeciwradiolokacyjnych. Zaletą tego typu bomb jest możliwość ich stosowania na obiekty wstępnie rozpoznane. Możliwość ta wynika z ich stosunkowo dużej powierzchni rażenia. Dzięki temu można ograniczać konieczność stosowania drogich środków precyzyjnego rozpoznania. Kolejną zaletą tego typu bomb jest brak zależności możliwości rażenia od aktywności atakowanego obiektu. Atakowane urządzenia mogą być wyłączone i zupełnie bierne, a mimo to, jeżeli znajdą się w strefie rażenia i nie będą wystarczająco odporne, zostaną zniszczone lub uszkodzone. Masowość rażenia powoduje eliminację różnorodnych obiektów. Na przykład, przy pokonywaniu obrony powietrznej w strefie rażenia zostaną zniszczone nie tylko stacje radiolokacyjne dużych i średnich zestawów przeciwlotniczych, ale także przenośne wyrzutnie w ogóle nie korzystające ze stacji radiolokacyjnych. Zniszczenie elektroniki zestawu uniemożliwi jego użycie. Bomby elektromagnetyczne mogą więc stać się skuteczną bronią przeciwko przenośnym zestawom obrony powietrznej.

Bomby te będą również bardzo przydatne w walce z lotnictwem, mogą bowiem niszczyć nie tylko jego systemy dowodzenia, ale i samoloty. Atak z zaskoczenia na samoloty na lotnisku może całkowicie je sparaliżować i uczynić podatnymi na fizyczne uderzenia bronią konwencjonalną.

Środki rażenia elektromagnetycznego, ze względu na nieobecność zewnętrznych oznak fizycznej destrukcji, są doskonałym środkiem rażenia w operacjach kryzysowych i pokojowych. Ich użycie może wywoływać mniejsze opory polityczne. Wprowadzenie bomb elektromagnetycznych do arsenału współczesnych sił powietrznych znacznie rozszerza możliwości prowadzenia strategicznych kampanii powietrznych. Broń ta stanowi mnożnik siły w wojnie konwencjonalnej. Masowe użycie tej broni może przynieść zdecydowaną przewagę temu, kto będzie miał możliwości dostarczenia jej nad obiekty ataku. Jakościowe zalety tego typu uzbrojenia mogą stworzyć przewagę nawet nad znacznie silniejszym przeciwnikiem, niedysponującym jednak taką bronią.

Elektromagnetyczna broń może stanowić dogodną alternatywę do wykonania ataku strategicznego, powodując wielkie koszty bez widocznych zniszczeń i bez strat towarzyszących, szczególnie w odniesieniu do ofiar w ludziach. Również w odniesieniu do strategii stopniowanego reagowania, broń ta może zapewniać dogodną formę ataku powstrzymującego lub odstraszającego. Ze względu na dużą szybkość osiągania rozległych zniszczeń, efekt odstraszania lub wymuszania może być osiągnięty szybciej. Broń ta może być też dogodnym środkiem oddziaływania na rządy aktywnie wspierające terroryzm, infoterroryzm lub działania zbrojne o małej skali intensywności. Może ona być skutecznym środkiem uderzeń odwetowych i odstraszających, powodując znaczne szkody ekonomiczne, militarne i polityczne bez ofiar w ludziach.

4.2.3. Atak ogniowy

Jako element zintegrowanego wysiłku ataku informacyjnego, atak ogniowy polega na użyciu broni fizycznie niszczącej wyznaczone obiekty. Celem jest wpływanie na informację lub system informacyjny przeciwnika za pomocą fizycznej destrukcji. Atak ogniowy siłą destrukcyjną przerywa lub niszczy system informacyjny przeciwnika.

Połączenie precyzyjnej amunicji z zaawansowaną platformą przenoszenia lub użycie samolotów specjalnych albo też przeniknięcie małej grupy uderzeniowej w celu neutralizacji części systemu, są głównymi przykładami wymagającymi precyzji dla dokładnego ataku, którego celem mogą być elementy systemów dowodzenia i kontroli. Przykładami szczebla taktycznego może być użycie amunicji precyzyjnej przeciw stacji przekaźnikowej lub użycie grupy specjalnej w celu przecięcia, lub wykorzystania linii komunikacyjnej.

Szczególną rolę w prowadzeniu ataku ogniowego odgrywa lotnictwo. Wykonując zadania samodzielnie lub współdziałając z innymi rodzajami sił zbrojnych może – uwzględniając posiadane uzbrojenie i sposób działań – szybko reagować na zaistniałe potrzeby w rejonie konfliktu. Zasadniczą właściwością charakteryzującą lotnictwo jest jego wysoka elastyczność, którą kształtują m.in.:

- duży zasięg samolotów – **który pozwala na wykonanie uderzeń na obiekty położone w znacznej odległości od lotnisk bazowania**;
- duża prędkość samolotów – **dzięki której możliwe jest zyskanie na czasie, osiągnięcie zaskoczenia i zmuszenie przeciwnika do utrzymywania dużych sił w ciągłej gotowości bojowej**;
- wysoka manewrowość – **która umożliwia szybkie przebazowanie samolotów taktycznych pomiędzy poszczególnymi TDW, a możliwość tankowania ich w powietrzu pozwala na głębokie przerzuty w dowolne rejony i obszary geograficzne. Pozwala to na operatywne ześrodkowanie lotnictwa taktycznego i koncentrację jego wysiłku na najważniejszych kierunkach**;
- uniwersalność wyposażenia – **która stwarza możliwość wykonywania zadań bojowych o różnej intensywności, zarówno zaczepnych jak i obronnych, w szerokim zakresie prędkości, wysokości i manewru**;

- dyspozycyjność – **która umożliwia dowództwu szybką reakcję na zaistniałą sytuację bojową w dowolnym rejonie oraz osiągnięcie efektu zaskoczenia co do czasu i miejsca jego użycia, jak również natychmiastowe przeciwdziałanie zagrożeniom ze strony przeciwnika. Stałe utrzymywanie wysokiego stopnia gotowości bojowej lotnictwa, czyni je zdolnym do natychmiastowego użycia. Dla osiągnięcia sukcesu istotne jest jednak jego zastosowanie na głównych kierunkach działania. Czas działania, miejsce, sposób i jego rodzaj muszą być niespodziewane dla przeciwnika, co tym samym pozwala na uzyskanie zaskoczenia i dużej skuteczności przy wykorzystaniu ograniczonych sił.**

4.2.4. Działania psychologiczne (atak psychologiczny)

Działania psychologiczne (PSYOPS)[187] są przeznaczone do przekazywania wybranych informacji i sugestii obcym przywódcom i społecznościom, aby wpływać na ich emocje, motywy, rozumowanie i zachowanie na korzyść własnych celów. Działania psychologiczne, według przyjętej koncepcji, stanowią atak psychologiczny.

Efekty nowoczesnych działań psychologicznych są potęgowane możliwościami sił powietrznych w zakresie komunikacji. Możliwości te wiążą się z precyzją i różnorodnością oraz dużą ilością informacji przekazywanej dla wywarcia wpływu na wyselekcjonowanych odbiorcach w celu zmiany ich percepcji i sterowania procesami decyzyjnymi. Przykłady tych informacji to obietnice, groźby odwetu, warunki poddania się, przepustki dla dezerterów lub wsparcie grup oporu. Jednostki sił powietrznych mogą być użyte do nadawania audycji radiowych i informacji przez głośniki, co może wpływać na społeczeństwo.

W walce stosuje się głównie dwie metody prowadzenia działań psychologicznych: *pośrednią i bezpośrednią.*

Metoda pośrednia stanowi podstawowy sposób oddziaływania na wojska przeciwnika. Realizowana jest za pomocą materiałów drukowanych, audycji radiowych, elektroakustycznych i – w określonych warunkach – telewizyjnych, za pomocą których nadawca (organizator) przenosi określoną informację (sugestię, apel) na odbiorcę, nie będącego z nim w bezpośrednim kontakcie.

Metoda bezpośrednia stanowi pomocniczy sposób oddziaływania w walce na małe grupy i pojedyncze osoby, np. jeńców wojennych, zbiegów i polega na bezpośrednim kontakcie nadawcy i odbiorcy. W działaniach bojowych dominuje metoda pośredniego oddziaływania.

Ze względu na sposób przekazu treści, wyróżnia się następujące sposoby oddziaływań psychologicznych na przeciwnika za pomocą:

- **materiałów drukowanych;**
- **radia;**

---

[187] Opracowano na podstawie: A. Podkowski, *Siły, środki i możliwości oddziaływania psychologicznego armii amerykańskiej podczas konfliktu zbrojnego*, Warszawa 1998; A. Podkowski, A. Laszczkowski, *Ulotki w działaniach bojowych*. Materiał studyjny, Warszawa 2001; AFDD 2-5: *Information Operations*, Washington 1998.

- **rozgłośni elektroakustycznych;**
- **telewizję;**
- **Internetu.**

Dobór sposobów oddziaływań informacyjnych zależy od aktualnej sytuacji polityczno-militarnej, otrzymanego zadania, obiektu oddziaływania oraz technicznych możliwości przekazu.

Oddziaływanie za pomocą materiałów drukowanych

Materiały drukowane stosuje się powszechnie w oddziaływaniu na żołnierzy oraz na ludność we wszystkich rodzajach działań bojowych, niezależnie od warunków terenowych, pory dnia i roku. Ich zaletą jest znaczny stopień wiarygodności, duży zasięg oraz długotrwałość oddziaływania (może ona być czytelna, nawet po kilku dniach rozrzucenia w terenie).

W działaniach psychologicznych najczęściej stosuje się następujące materiały drukowane:

- **ulotki;**
- **materiały poglądowe;**
- **falsyfikaty;**
- **druki zwarte.**

Dla działań psychologicznych szczególną wartość ma apelacyjna część materiału drukowanego, choć część informacyjna zarówno ulotki, jak i innego rodzaju materiału poglądowego czy druku zwartego jest niezbędna, gdyż spełnia istotną rolę w procesie stymulacji zainteresowania odbiorcy.

Ulotki są najbardziej powszechnymi środkami oddziaływania na przeciwnika. Ze względu na ich treść i przeznaczenie dzielą się one na *informacyjne*, *perswazyjne* oraz *nakazujące*. Ulotka informacyjna opiera się na faktach i zawiera odpowiednio dobrane wiadomości polityczne i militarne, ukazujące sytuację według założeń nadawcy. Ulotka perswazyjna osiąga swój cel poprzez argumenty racjonalne. Fakty ukazywane są w taki sposób, aby odbiorcy byli przekonani o słuszności wysuwanych wniosków i byli skłonni do zachowań pożądanych przez nadawcę. Ulotki nakazujące zawierają wezwania i polecenia dowództwa wojsk własnych do zaniechania przez przeciwnika walki lub oporu, poddania się i kapitulacji.

Ze względu na czas przygotowania oraz warunki użycia, ulotki dzielą się na *standardowe* i *specjalne* (sytuacyjne). Ulotki standardowe zawierają ogólne odezwy i są przeznaczone do wielokrotnego użytku we wszystkich, powtarzających się lub podobnych, sytuacjach na polu walki. Są one szczególnie przydatne w szybko zmieniających się sytuacjach taktycznych, w czasie których trudno jest przygotować odpowiednią do sytuacji ulotkę. Ulotki tego typu są jednak, ze względu na ogólnikowy charakter i uniwersalną treść, mniej efektywne niż te, które przygotowuje się na konkretną sytuację. Są z reguły przygotowywane już w okresie pokojowym. Ulotki specjalne (sytuacyjne) przygotowywane są bezpośrednio przed akcją, zawierają specyficzne treści, związane z konkretną sytuacją

bojową. Są one z reguły przeznaczone do jednorazowego użytku. W działaniach psychologicznych prowadzonych na szczeblu taktycznym i taktyczno-operacyjnym osiąga się najlepsze rezultaty, wówczas gdy adresaci otrzymują ulotki o treści najbardziej aktualnej, a proponowany sposób postępowania jest zbliżony do ich obecnych przeżyć i oczekiwań. Tego typu ulotka może być użyta również na szczeblu operacyjnym jako środek do bezpośredniego porozumienia się z odbiorcami. Umożliwia ona precyzyjne dopasowanie treści odezwy do bieżących i konkretnych potrzeb odbiorców (to jest ludności w określonym obszarze, grup etnicznych i religijnych oraz innych wyselekcjonowanych grup ludności i żołnierzy przeciwnika).

Niektórzy specjaliści zachodni dzielą ulotki na *strategiczne, taktyczne i konsolidacyjne*. Ulotka strategiczna jest zwykle adresowana do wojsk i ludności cywilnej przeciwnika na całym jego obszarze. Jej długofalowym celem jest osłabienie woli przeciwnika do stawiania oporu poprzez zwiększanie wewnętrznych niesnasek i napięcia oraz wsparcie ruchu oporu na jego terytorium. Ulotki strategiczne pełnią rolę pomocniczą w przygotowaniu ewentualnej militarnej i politycznej klęski przeciwnika. Ulotki taktyczne mają wpływać na aktualne zachowanie się i postawę żołnierzy przeciwnika i w konsekwencji na przebieg walki na szczeblu taktycznym i operacyjnym; są stosowane łącznie ze wszystkimi innymi środkami walki w celu wykonania zadania bojowego. Ulotki konsolidacyjne stosuje się dla ułatwienia osiągnięcia celów militarnych na terenach wyzwolonych i okupowanych. Ulotki tego typu mogą wskazywać – już po zakończeniu działań militarnych – jakie niezbędne czynności powinny podjąć pozostające na danym obszarze wojska przeciwnika i ludność cywilna.

Materiały poglądowe stosuje się ze względu na ich sugestywność i komunikatywność jako samodzielny lub uzupełniający środek oddziaływania psychologicznego na wojska przeciwnika. Są one z reguły monotematyczne i przedstawiają treści za pomocą ilustracji. Do podstawowych materiałów poglądowych należą *zdjęcia, rysunki, schematy, plany, szkice i wykresy*.

Falsyfikaty stosuje się do prowadzenia działań dezinformacyjnych oraz akcji zakłócających funkcjonowanie zaplecza przeciwnika. Opracowanie falsyfikatów i sposób ich rozpowszechniania wymagają niezwykle starannego i szczegółowego przygotowania w celu wprowadzenia przeciwnika w błąd i wywołania zamierzonych skutków. Do podstawowych materiałów dezinformacyjnych stosowanych przez organy działań psychologicznych należą *falsyfikaty dokumentów bojowych, zarządzeń władz wojskowych i cywilnych, a także podrobione pieniądze, bony towarowe*.

Druki zwarte mają na celu dotarcie do określonych grup przeciwnika z informacjami polityczno-wojskowymi, które mają pogłębiać i utrwalać destrukcyjne nastroje oraz postawy żołnierzy. Do druków zwartych należą *odezwy, broszury, gazety, biuletyny oraz inne materiały, których treść przekracza objętość ulotki*.

Materiały drukowane, by spełnić swój cel jako środek oddziaływania psychologicznego, muszą być, rzecz jasna, dostarczone odbiorcy. Podczas planowa-

nia działań psychologicznych na wojska i ludność cywilną przeciwnika z użyciem materiałów drukowanych, określenie możliwości ich rozpowszechniania należy do najistotniejszych problemów. W działaniach na szczeblu operacyjnym wykorzystuje się do tego przede wszystkim bomby i zasobniki z ulotkami przenoszone przez samoloty oraz w niektórych armiach balony, zaś na szczeblu taktycznym wykorzystuje się przede wszystkim rakietowe pociski z ulotkami bliskiego zasięgu oraz pociski artyleryjskie. Ponadto możliwy jest zrzut ulotek ze śmigłowców, rozpowszechnianie materiałów drukowanych przez patrole rozpoznawcze i grupy wypadowe, korzystanie z pomocy sektora cywilnego lub pozostawianie tych materiałów podczas wycofywania się wojsk.

Oddziaływanie radiowe

Audycje radiowe stanowią jeden ze skuteczniejszych rodzajów oddziaływań psychologicznych, stosowanych w warunkach zagrożenia wojennego oraz we wszystkich rodzajach działań bojowych. Do głównych zalet transmisji radiowych można zaliczyć:

- **szeroki zakres oddziaływania – programy radiowe mogą docierać jednocześnie do masowych i zróżnicowanych grup odbiorców;**
- **wszechstronność – możliwość wykorzystania różnorodnych form wypowiedzi (wywiady, reportaże, apele, wezwania);**
- **łatwość percepcji przez odbiorców;**
- **szybkość przygotowania audycji, także w warunkach polowych.**

W działaniach psychologicznych stosuje się następujące formy przekazu radiowego:

- **codzienne serwisy informacyjne bieżących wydarzeń polityczno-militarnych;**
- **komunikaty wojenne, zawierające opis najważniejszych zdarzeń na różnych kierunkach działań bojowych, zgodne z oficjalną wykładnią dowództwa wojsk własnych;**
- **meldunki nadzwyczajne informujące o szczególnych sukcesach bojowych wojsk własnych oraz niepowodzeniach strony przeciwnej;**
- **apele, wezwania i odezwy zawierające polecenia i nakazy dowództwa wojsk własnych skierowane do żołnierzy przeciwnika, jak również do własnej ludności, członków ruchu oporu na zajętym terenie;**
- **reportaże z frontu, obozu jenieckiego;**
- **komentarze poświęcone sytuacji polityczno-militarnej oraz wydarzeniom wojennym.**

Doświadczenia z zakresu oddziaływania radiowego na żołnierzy i ludność cywilną podczas konfliktu zbrojnego unaoczniają, że zakamuflowane rozgłośnie radiowe, występujące pod innym niż ich właściwej przynależności szyldem, osiągały duże efekty. Działalność ta, zwana czarną propagandą, stawia nadawcę wobec odbiorcy w dużo korzystniejszym położeniu. Nadawca ma możliwość wyboru obiektu działania oraz form i metod dotarcia do niego. Ramami ograniczają-

cymi mogą być jedynie techniczne możliwości dotarcia do odbiorcy, rzadziej z powodu trudności emisyjnych, dużo częściej z prozaicznych przyczyn, jak np. braku odbiorników radiowych wśród odbiorców lub zakłócania przez przeciwnika.

Oddziaływanie elektroakustyczne

Rozgłośnie elektroakustyczne są najskuteczniejszym środkiem przekazu wspierającym działania bojowe prowadzone na szczeblu taktycznym. Stosuje się je w warunkach bezpośredniej styczności z przeciwnikiem. Cechą szczególną oddziaływań elektroakustycznych jest ich ścisłe powiązanie z walką oddziałów i pododdziałów. Akcje te są prowadzone z własnego ugrupowania bojowego i bezpośrednio wspierają działania wojsk. Ich zaletą jest możliwość natychmiastowej reakcji na zmiany w sytuacji bojowej na polu walki. Zastosowanie ich determinują w znacznym stopniu warunki terenowe i meteorologiczne. Audycje elektroakustyczne dzielą się na:

- Audycje słowne o charakterze informacyjnym. **W oddziaływaniu psychologicznym na żołnierzy i ludność przeciwnika stosuje się najczęściej krótkie odezwy zawierające rozkazy, polecenia, wezwania, instrukcje, komunikaty i apele. Transmitowane bezpośrednio bądź odtwarzane z taśmy magnetofonowej audycje, wymagają od spikera doskonałej znajomości języka odbiorców.**
- Audycje dźwiękowe o charakterze nękającym. **Mają na celu zmniejszenie odporności psychicznej i fizycznej żołnierzy przeciwnika poprzez emisję określonych sygnałów dźwiękowych o określonej częstotliwości (2–15 Hz) i poziomie głośności (115–155 dB), wywołujących i podtrzymujących stan stresu, a w skrajnych wypadkach doprowadzających nawet do zaburzeń funkcjonowania organizmu.**
- Audycje mieszane, **które w zależności od charakteru oraz relacji między słowami a sygnałami dźwiękowymi mogą realizować wymienione w poprzednich punktach cele.**

Czas emisji audycji elektroakustycznej nie powinien przekraczać 30 sekund.

Oddziaływanie telewizyjne

Przekaz telewizyjny stanowi jedną z najbardziej sugestywnych form upowszechniania informacji. Jego przydatność w oddziaływaniach psychologicznych wynika z szerokich możliwości zastosowania go jako popularnego środka przekazu. Telewizja do celów czysto militarnych może być wykorzystana już w okresie zagrożenia wojennego. Po wybuchu konfliktu będzie ukierunkowana przede wszystkim na cele obrony terytorialnej i cywilnej oraz na cele konsolidacyjne. Telewizyjne oddziaływanie informacyjne będzie głównie stosowane na ludność, jak również na przeciwnika niezaangażowanego bezpośrednio w walce, jego odwody i jednostki mobilizowane znajdujące się w miejscach stałej dyslokacji. Do emisji programów telewizyjnych na terenie nieobjętym działaniami wojennymi, wykorzysta się stacjonarne urządzenia RTV.

Oddziaływanie przez Internet

Internet staje się stopniowo jednym z najważniejszych mediów komunikacji społecznej. Już obecnie zastępuje pocztę, umożliwia korzystanie z radia, a nawet telewizji. Oddziaływanie przez Internet może być szczególnie efektywne w odniesieniu do tych grup ludności, które z niego masowo korzystają, a nawet stają się od niego uzależnione. Korzystanie to może być formą rozrywki lub też towarzyszyć wykonywaniu obowiązków służbowych. Ponieważ ilość czasu spędzanego w Internecie stale rośnie, możliwości tego oddziaływania stają się również coraz większe. W oddziaływaniu tym mogą być stosowane techniki manipulacji społecznej, marketingu oraz inne, wykorzystywane w oddziaływaniach za pomocą omówionych mediów.

4.2.5. Dezinformacja wojskowa (mylenie)

Dezinformacja wojskowa[188] (*miliatry deception*) wprowadza przeciwnika w błąd, powodując, że działa on zgodnie z planami organizatora dezinformacji. Działania dezinformacji wojskowej rozciągają się na wszystkie szczeble wojny i zawierają komponenty ofensywne i defensywne. Dezinformacja wojskowa może odwrócić uwagę od operacji wojskowych lub zapewnić dla nich osłonę, myląc i rozpraszając siły przeciwnika. Dezinformacja wymaga głębokiej znajomości kultury, polityki, doktryny oraz procesu decyzyjnego przeciwnika – a ta wiedza może być wykorzystana przez planistów.

Od czasu powstania i rozwoju pierwszych form zorganizowanych społeczności, ich przywódcy lub dowódcy formacji zbrojnych w celu wprowadzenia przeciwników w błąd co do swoich zamierzeń, planów i działań, stosowali dezinformację. Nieużywano pojęcia *dezinformacja*, wszelkie natomiast metody wprowadzenia przeciwnika w błąd nazywano fortelem lub podstępem. Najoryginalniejsze i najbardziej pomysłowe przykłady podstępu, kłamstwa w polityce i w walce zbrojnej były zbierane, uogólniane i opisywane przez historyków i teoretyków wojskowych. Pierwszym, który na podstawie doświadczeń wojen z przełomu VI i V w. p.n.e. dokonał analizy przedsięwzięć dezinformacyjnych, był Sun Tzu. Pisał on: „wojna to droga kłamstwa, dlatego jeśli coś możesz – pokazuj, że nie możesz; jeśli korzystasz z czegoś – pokazuj, że nie korzystasz; jeśli jesteś blisko – pokazuj, że daleko, jeśli znajdziesz się daleko – pokazuj, że jesteś blisko; zwabiaj przeciwnika korzyściami, spowoduj u niego dezorganizację i bierz go; przyjąwszy pokorny wygląd, wzbudź w nim pewność siebie; napadaj przeciwnika, kiedy nie jest przygotowany; pojawiaj się tam, gdzie on ciebie nie oczekuje"[189]. W wyniku uogólnień i przeprowadzonej analizy Sun Tzu określił pięć głównych metod stosowania fortelu: działania pozorujące; oddziaływanie na psychikę; dezorganizowanie szeregów; usypia-

[188] Opracowano na podstawie: AFDD 2-5: *Information Operations*, wyd. cyt. oraz A. Podkowski, *Zasady i techniki perswazji w działaniach psychologicznych w walce zbrojnej (na przykładzie armii sowieckiej w latach 1921–1991)*, Warszawa 1998.

[189] Sun Tzu, wyd. cyt.

nie czujności; wykorzystanie błędów, niedoskonałości, nieprzygotowania i nieostrożności przeciwnika.

Najbardziej istotnym z punktu widzenia sił zbrojnych i obronności państwa obszarem dezinformacji jest **dezinformacja wojskowa**. Najogólniej ujmując, obiektami tej dezinformacji są: przeciwnik, wojska własne oraz otoczenie, w którym następuje styczność obu stron. Oddziaływanie na przeciwnika skierowane jest na dwa elementy, to jest **system dowodzenia i kontroli** oraz **system rozpoznania**. Istotą tej dezinformacji jest przekazywanie przez system rozpoznania przeciwnika fałszywych informacji do jego centrum decyzyjnego. Istotą dezinformacji w stosunku do wojsk własnych jest natomiast spowodowanie takiego ich działania, aby umocniło ono przeciwnika w przekonaniu o słuszności jego wniosków z rozpoznania. Taki sam cel ma dezinformacja w stosunku do otoczenia stron, do którego zalicza się ludność cywilną, członków ruchów partyzanckich, jeńców, pracowników wywiadu, obserwatorów i obcokrajowców. Reasumując, **dezinformacja wojskowa to zamierzone przekazywanie poprzez wyżej wymienione kanały fałszywych informacji, pogłosek, dokumentów oraz demonstrowanie działań wojsk, których celem jest wprowadzenie w błąd przeciwnika co do prawdziwych zamierzeń, planów i przeprowadzanych przedsięwzięć o znaczeniu militarnym**.

Dezinformacja wojskowa ze względu na zakres, rolę, charakter i treść **może być prowadzona w skali strategicznej, operacyjnej i taktycznej**. Dezinformację w skali strategicznej organizują i prowadzą centralne organy kierowania państwem. Bezpośrednim organizatorem i koordynatorem wykonania przedsięwzięć dezinformacyjnych jest naczelne dowództwo sił zbrojnych, odpowiedzialne za funkcjonowanie systemu obronnego państwa i wypracowanie strategii użycia sił zbrojnych zgodnie z doktryną wojenną. Swoim zakresem obejmuje ona własne państwo, w tym siły zbrojne, oraz jego otoczenie międzynarodowe. Siły powietrzne mogą uczestniczyć w przedsięwzięciach dezinformacji na tym szczeblu.

W czasie pokoju przedsięwzięcia **dezinformacji wojskowej** w skali strategicznej obejmują zagadnienia dotyczące: szkolenia, struktury organizacyjnej, dyslokacji, stanu gotowości bojowej, sposobów i terminów mobilizacyjnego i operacyjno-strategicznego rozwinięcia sił zbrojnych; zadań strategicznych sił rakietowo-jądrowych; planów i sposobów prowadzenia pierwszej strategicznej operacji powietrzno-lądowej; składu, wyposażenia i gotowości bojowej zgrupowań wojsk rozwiniętych w czasie pokoju; stopnia operacyjnego przygotowania terytorium państwa oraz systemu kierowania i dowodzenia siłami zbrojnymi.

W skali operacyjnej dezinformację organizuje się na szczeblu operacyjnym. Przedsięwzięcia z zakresu dezinformacji wojskowej w skali operacyjnej powinny być potwierdzeniem i logicznym ciągiem fałszywych informacji, przekazywanych przeciwnikowi w skali strategicznej. Dotyczą one sposobu przygotowania i prowadzenia operacji militarnych; wykorzystania w działaniach bojowych związków operacyjnych, taktycznych oraz rodzajów sił zbrojnych; gotowości i zdolności bojowej wojsk; rozmieszczenia punktów dowodzenia i węzłów łączności; zasad organizacji zabezpieczenia operacyjnego i logistycznego. W trakcie bezpośredniego

przygotowania operacji bojowej, główny wysiłek dezinformacji skupia się na ukryciu faktu prowadzenia przygotowań do operacji i planu operacji; stanu gotowości planowanych do użycia wojsk, rejonów ześrodkowania odwodów operacyjno-strategicznych lub prowadzonej mobilizacji; gotowości środków napaści jądrowej i broni precyzyjnego rażenia; rejonów rozwijania stanowisk dowodzenia oraz reżimu pracy środków łączności; kierunków ruchu wojsk i przewozów wsparcia logistycznego. Siły powietrzne mogą zarówno organizować dezinformację tego typu, jak i w niej uczestniczyć.

Przedsięwzięcia z zakresu **dezinformacji wojskowej** w skali taktycznej mogą być realizowane wyłącznie na podstawie zarządzenia przełożonego.

Dezinformacja wojskowa w skali strategicznej, realizowana przez siły i środki sił zbrojnych i państwa zgodnie z opracowanym planem, powinna być organizowana zarówno w czasie pokoju, jak i w czasie wojny. W czasie przygotowania dezinformacji wojskowej powinno się uwzględnić zamierzenia planu maskowania operacyjnego, walki elektronicznej i zwalczania elementów rozpoznawczych przeciwnika. W zależności od metod, sposobów, stosowanych środków i kanałów transmisji i informacji oraz ich treści, a także charakteru działań pozornych, można wyróżnić trzy formy dezinformacji – **przekaz, dokument i działania**. Przekaz może być realizowany dwiema metodami, *ustną i pisemną*. W *metodzie ustnej*, w celu dostarczenia przeciwnikowi dezinformujących danych, wykorzystuje się stan osobowy wojsk własnych, miejscową ludność, dyplomatów, przedstawicieli firm państwowych i prywatnych, a także telewizję, radio oraz wojskowe i cywilne środki łączności. *Metoda pisemna* dezinformacji, polega natomiast na zamierzonym opracowaniu i terminowym dostarczeniu przeciwnikowi dokumentów tekstowych, takich jak: fałszywe dyrektywy, rozkazy, zarządzenia bojowe, meldunki. Dane te uzupełnia się przez publikowanie dezinformacyjnych wiadomości w wojskowych czasopismach, dziennikach, broszurach, ulotkach propagandowych i plakatach.

Formą najpełniej i najdobitniej odzwierciedlającą pozorną sytuację jest dokument. Ta forma dezinformacji polega na dostarczaniu przeciwnikowi fałszywych dokumentów bojowych, np.: map, decyzji, roboczych planów operacji, planów zabezpieczenia działań bojowych, współdziałania, obiektów wojskowych; schematów obrony, łączności, ognia, rozmieszczenia celów, obserwacji pól minowych; harmonogramów uderzeń, przelotów czy przegrupowań wojsk. Ponieważ przeciwnik będzie zawsze dążył do potwierdzenia uzyskanych informacji, ważnym elementem dezinformacji będzie przygotowanie działań pozorujących. Przedsięwzięcia te są formą dezinformacji określaną jako działania. Dezinformacja osiągnie swój cel, gdy przeciwnik, obserwując działania pozorujące, uznaje je za realne.

Sposób dezinformacji wojskowej to wybrany i najbardziej celowy wariant dostarczania fałszywych informacji, dokumentów oraz prowadzenia działań pozorujących, a także wykorzystania sił i środków, żeby wprowadzić przeciwnika w błąd. Jednym z najbardziej popularnych sposobów dezinformacji jest celowe rozpowszechnianie fałszywych informacji (pogłosek) wśród składu osobowego

wojsk i miejscowej ludności. Informacje te poprzez system rozpoznania docierają do dowództwa przeciwnika.

Kolejnym sposobem dezinformacji jest szerzenie fałszywych informacji za pośrednictwem środków masowego przekazu i wojskowych środków łączności. Klasycznym przykładem zastosowania tego sposobu było przygotowanie przez państwa zachodnie desantu w Normandii.

Tabela 10. Elementy dezinformacji wojskowej

<table>
<tr><th>Formy</th><th colspan="2">Przekaz</th><th rowspan="2">Dokument</th><th rowspan="2">Działanie</th></tr>
<tr><th>Metody</th><th>Ustna</th><th>Pisemna</th></tr>
<tr><td>Sposoby</td><td>1. Upowszechnianie fałszywych informacji wśród stanów osobowych wojsk i ludności cywilnej
2. Przekazywanie fałszywych danych poprzez techniczne środki łączności i środki masowego przekazu
3. Fałszywe oświadczenia przywódców</td><td>4. Publikacja fałszywych informacji w prasie wojskowej i cywilnej</td><td>5. Zamierzone zagubienie fałszywych lub odtajnionych dokumentów o znaczeniu operacyjno-strategicznym</td><td>6. Przygotowanie i realizacja działań pozornych</td></tr>
<tr><td>Siły</td><td colspan="4">• Funkcjonariusze wojskowi
• Członkowie misji wojskowych
• Członkowie delegacji sił zbrojnych
• Ludność cywilna współpracująca z siłami zbrojnymi
• Personel informowania publicznego sił zbrojnych
• Obsługa sprzętu łączności sił zbrojnych
• Stany osobowe sił zbrojnych wojsk własnych i przeciwnika
• Dezerterzy i jeńcy
• Agentura, dywersanci, partyzanci i członkowie podziemia współpracujący z siłami zbrojnymi</td></tr>
<tr><td>Środki</td><td>• Sprzęt audiowizualny
• Sprzęt łączności wojskowej</td><td>• Wydawnictwa, prasa plakaty
• Korespondencja pocztowa
• Rakietowe pociski propagandowe
• Środki sił zbrojnych</td><td>• Spreparowane dokumenty wojskowe</td><td>• Technika bojowa i specjalna do imitowania działań pozornych
• Makiety urządzeń wojskowych i uzbrojenia</td></tr>
</table>

Nie mniej ważne znaczenie ma sposób dezinformacji przez publikację fałszywych informacji w prasie cywilnej i wojskowej. Sposób ten jest szczególnie wykorzystywany w celu kształtowania przychylnej dla kierownictwa państwa opinii własnego społeczeństwa, dotyczących np. konieczności zwiększenia wydatków na zbrojenia lub potrzeb związanych z obecnością wojskową w różnych regionach świata, uzasadnianych obroną strategicznych interesów państwa. Z tym sposobem dezinformacji ściśle wiąże się fałszowanie dokumentów, które służą potwierdzeniu rozpowszechnianych w prasie i innych środkach masowego przekazu informacji. Fałszowanie dokumentów łączy się z kolejnym sposobem dezinformacji, to jest zamierzonym „zagubieniem" fałszywych lub odtajnionych dokumentów, zawierających dane szczebla operacyjno-strategicznego. W tym celu organizuje się „nieszczęśliwe wypadki" lub „przypadkowe zapomnienia" dokumentów w torbach polowych, walizkach dyplomatycznych czy niezamkniętych sejfach.

Siły i środki dezinformacji prowadzonej przez siły powietrzne to ludzie – nośnicy informacji – oraz sprzęt, którym się posługują w czasie tej transmisji. W zależności od sytuacji, wykorzystywanych kanałów i środków oraz terminu przeprowadzenia pozorujących przedsięwzięć, w siłach powietrznych mogą być zaangażowane następujące grupy ludzi: funkcjonariusze wojskowi sił powietrznych, członkowie misji wojskowych sił powietrznych, członkowie delegacji sił powietrznych, ludność cywilna współpracująca z siłami powietrznymi, personel informowania publicznego sił powietrznych, obsługa sprzętu łączności sił powietrznych, stany osobowe sił powietrznych wojsk własnych i przeciwnika, dezerterzy i jeńcy, agentura, dywersanci, partyzanci i członkowie podziemia współpracujący z siłami powietrznymi. Podstawą wykorzystania tych sił powinna być zasada szczególnie ścisłego przestrzegania tajności treści przedsięwzięć dezinformacyjnych i przedsięwzięć pozorujących. Osoby rozpowszechniające informacje lub realizujące działania pozorujące nie powinny wiedzieć, że są narzędziem dezinformacji.

Szeroko wykorzystywanym i przydatnym nośnikiem fałszywej informacji jest miejscowa ludność. Zarówno w minionych wojnach, jak i podczas przygotowywania współczesnych operacji wojskowych, każdy wywiad docenia rolę miejscowej ludności przygranicznych rejonów w zdobywaniu informacji, tworząc w tym środowisku agenturę. Zdaniem ekspertów służb specjalnych miejscowa ludność jest jednym z ważniejszych źródeł pozyskiwania przez wywiad informacji. Dlatego należy umiejętnie wykorzystywać to środowisko do prowadzenia dezinformacji. Kolejną grupą ludzi, wykorzystywanych do prowadzenia dezinformacji, są partyzanci i członkowie podziemia. Szczególnie istotną rolę odgrywają oni w czasie konfliktu zbrojnego, gdyż mogą rozpowszechniać fałszywe pogłoski wśród miejscowej ludności zamieszkującej terytorium okupowane przez przeciwnika. W tym środowisku będą pracować agenci wywiadu oraz dywersanci, którzy zbierając informacje wywiadowcze, spotkają się z informacjami dezinformacyjnymi. Aby dezinformacja była skuteczna, należy dążyć do rozpracowania ludzi pracujących dla przeciwnika, a następnie, za ich pośrednictwem, dostarczać mu fałszywych informacji. Kolejną grupą, za której pośrednictwem rozpowszechnia się fałszywe informacje, są zbiegowie i jeńcy wojenni.

Wyżej wymienione grupy ludzi, traktowane jako **siły dezinformacyjne**, korzystają z różnych środków technicznych, zwanych **środkami dezinformacji**. Środki te można podzielić na dwie grupy. **Pierwszą grupę** stanowią *środki masowej informacji*, do których zalicza się: *prasę* – wojskową i cywilną, w tym codzienną i periodyczną; *wydawnictwa* – broszury informacyjne, literaturę techniczną i popularnonaukową, plakaty i ulotki; *filmy* – dokumentalne, popularnonaukowe, o tematyce technicznej i wojskowej oraz reklamowe; *radio, telewizję, sprzęt krótkofalowy, telefony, dyktafony, magnetofony, magnetowidy, korespondencję pocztową, to jest telegramy, listy i karty pocztowe*. Środki masowego przekazu są również wykorzystywane w działaniach dezinformacyjnych przez podawanie informacji tendencyjnych.

Do **drugiej grupy** środków dezinformacji zalicza się środki wojskowe, takie jak: środki łączności telefonicznej, radiowej i telegraficznej naziemnego, powietrznego, morskiego i kosmicznego bazowania. W toku działań wojennych, oprócz wyżej wymienionych środków do rozpowszechniania i dostarczania na tyły przeciwnika lub w rejon działań bojowych ulotek, dokumentów i innych materiałów zawierających fałszywe treści przez siły powietrzne, mogą być wykorzystane: rakiety skrzydlate, kasetowe bomby lotnicze, samoloty bezpilotowe, szybowce oraz makiety techniki i uzbrojenia specjalnego. Syntezę omawianej treści zawiera tabela 10.

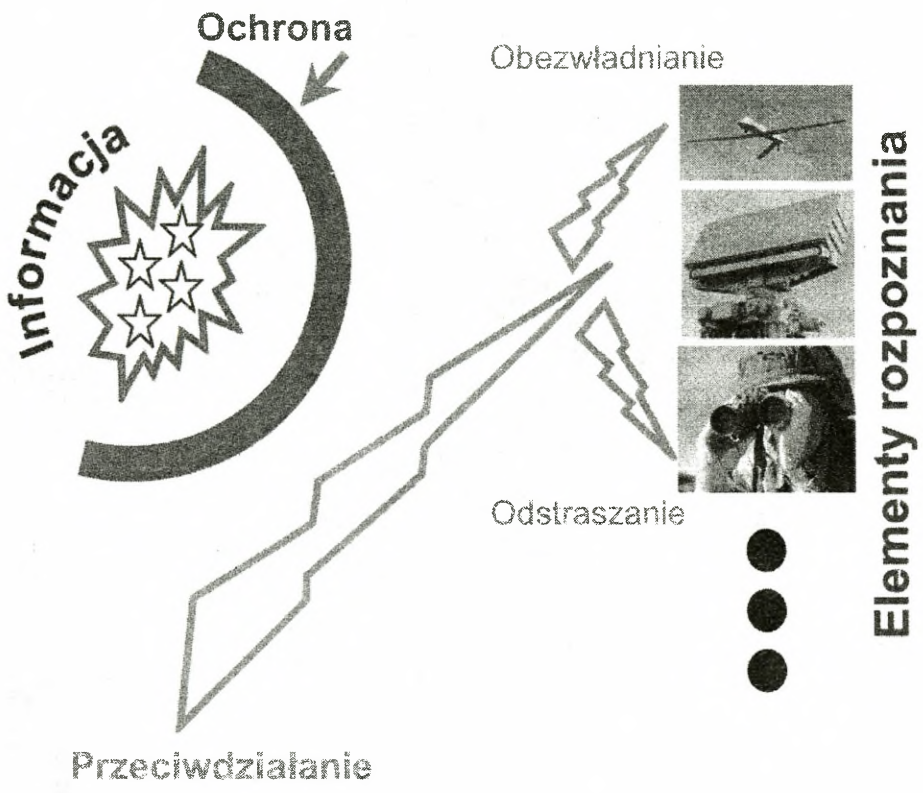
4.3. Formy obrony informacyjnej

Obrona informacyjna obejmuje zapobieganie rozpoznaniu i niedopuszczanie do informacyjnego atakowania lub uzyskiwania pożądanej efektywności tego atakowania przez przeciwnika.

Celem rozpoznania jest uzyskanie informacji o przeciwniku. W aktywności tej wyróżnić można dwa główne elementy: będącą przedmiotem działań informację, która może występować w różnych formach i postaciach, oraz próbujący pozyskać ją element rozpoznania. W tej sytuacji zapobieganie rozpoznaniu może przybierać formę ***przeciwdziałania aktywności rozpoznawczej przeciwnika*** oraz ***ochrony informacji*** przed dostępem elementów rozpoznania (rys. 35).

Przeciwdziałanie aktywności rozpoznawczej przeciwnika polega na odstraszaniu tej aktywności oraz na jej obezwładnianiu, gdy odstraszanie zawiedzie.

Ochrona informacji w rzeczywistości dotyczy zarówno zagrożeń niezwiązanych z działalnością przeciwnika, jak np. wpływ czynników przyrody czy błędy personelu, co może doprowadzić do utraty lub deformacji informacji, jak też zagrożeń wiążących się z działaniami rozpoznawczymi przeciwnika. Niniejsze rozważania koncentrują się przede wszystkim na ochronie przed rozpoznaniem przeciwnika. ***Ochrona informacji*** przed rozpoznaniem osiągana jest głównie w wyniku prowadzenia kontrwywiadu, ochrony technicznej, ochrony informatycznej. Ponadto przedsięwzięciami odnoszącymi się do całej sfery ochrony są: bezpieczeństwo działań i maskowanie.

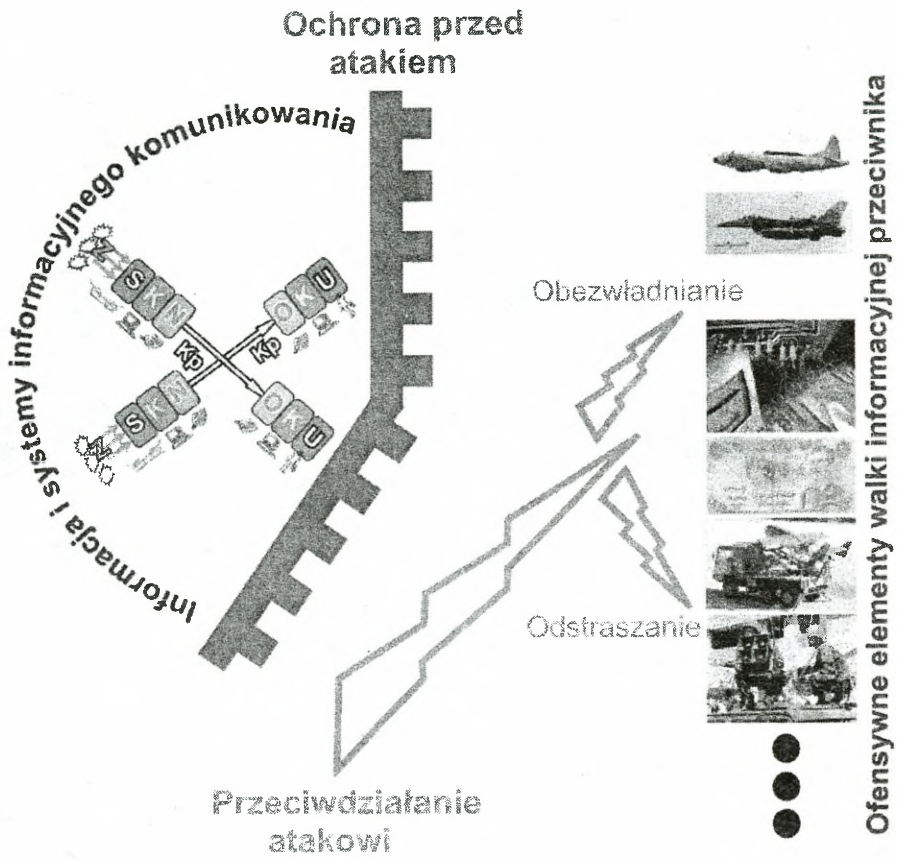


Opracowanie własne.

Rys. 35. Zapobieganie rozpoznaniu

Celem informacyjnego atakowania jest niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji. Podobnie jak w wypadku rozpoznania, informacyjne atakowanie można przedstawić w postaci uproszczonego modelu. Model ten składa się z systemów informacyjnego komunikowania i przepływającej przez nie informacji oraz ofensywnych elementów walki informacyjnej przeciwnika i zachodzących między nimi relacji. Zapobieganie informacyjnym atakom może być prowadzone w dwóch dziedzinach: ***przeciwdziałania informacyjnym atakom*** oraz ***ochrony własnej informacji i systemów informacyjnego komunikowania*** przed atakiem (rys. 36).

Całość tych przedsięwzięć ma na celu niedopuszczenie do informacyjnego atakowania własnej informacji i systemów informacyjnego komunikowania przez przeciwnika. Główną aktywnością w tym względzie jest ***przeciwdziałanie informacyjnym atakom*** przeciwnika. Przeciwdziałanie to może mieć formę odstraszania tych ataków oraz ich obezwładniania, gdy odstraszanie zawodzi.



Opracowanie własne.

Rys. 36. Niedopuszczanie do informacyjnego atakowania lub uzyskiwania pożądanej efektywności tego atakowania przez przeciwnika

Niezależnie od tego podejmuje się przedsięwzięcia, które mają zabezpieczać informację i systemy informacyjnego komunikowania, w sytuacji gdy przeciwdziałanie atakom okaże się nie w pełni skuteczne. Przedsięwzięcia te to ***ochrona własnej informacji i systemów informacyjnego komunikowania.***

Ochronę własnej informacji i systemów informacyjnego komunikowania zapewnia się przez kontrwywiad, ochronę psychologiczną, ochronę elektroniczną, ochronę informatyczną, inżynieryjną rozbudowę i kontrdezinformację. Ponadto przedsięwzięciami odnoszącymi się do całej sfery ochrony są: bezpieczeństwo działań i maskowanie.

4.3.1. Obezwładnianie i odstraszanie rozpoznania i informacyjnych ataków

Obezwładnianie rozpoznania i informacyjnych ataków wiąże się z dysponowaniem skutecznym systemem wykrywania działalności rozpoznawczej i ofensywnej. Jest to jeden z warunków, gdyż brak takiej możliwości może wręcz prowokować do jej podjęcia. Same możliwości wykrywania nie są wystarczającym elementem obezwładniania, gdyż świadomość istnienia wrogiej działalności bez możliwości jej przeciwdziałania ma małą zdolność jej paraliżowania. Obezwładnianie może być zapewnione przy posiadaniu, oprócz sprawnego systemu wykrywania także skutecznego systemu paraliżowania wrogiej działalności. System paraliżowania winien być adekwatny do stanu rozwoju i możliwości potencjału rozpoznania i informacyjnego ataku przeciwnika.

Wiarygodne odstraszanie może być realizowane w warunkach posiadania zdolności obezwładniania rozpoznania i informacyjnych ataków oraz dostatecznego potencjału do prowadzenia efektywnych działań odwetowych. Niezbędna jest także wola jego wykorzystania, jeśli zajdzie taka potrzeba.

Siły zbrojne stosują przedsięwzięcia bezpieczeństwa, by chronić i bronić informacje i systemy informacyjne. Przedsięwzięcia te odnoszą się do odstraszania rozpoznania i informacyjnych ataków. Odstraszanie to jest procesem identyfikacji działań przeciwnika i analizowanie własnych akcji, które towarzyszą działaniom militarnym i innym działaniom w celu:

- identyfikowania tych akcji, które mogą być podjęte przez systemy rozpoznawcze przeciwnika;
- określania kierunków, na które obce systemy rozpoznania mogą koncentrować swoją aktywność, by zebrać, zinterpretować i dokonać syntezy danych celem uzyskania najważniejszych informacji we właściwym czasie;
- wybierania i zastosowania środków, które wyeliminują lub zredukują do aprobowanego poziomu słabości własnych działań wobec przeciwnika.

4.3.2. Ochrona własnej informacji i systemów informacyjnego komunikowania

Ochrona informacji to przedsięwzięcia podejmowane w celu osłony informacji i systemów informacyjnych, zmierzające do zapewnienia ich dostępności, integralności, autentyczności, tajności i zdolności do identyfikowania źródła informacji i danych.

Ochrona informacji zawiera także odtworzenie systemów informacyjnych przez utrzymywanie zdolności do osłony, wykrywania zagrożeń i reagowania na nie. Ochrona informacji jest stosowana we wszystkich działaniach militarnych na wszystkich szczeblach. Dowódca sił powietrznych powinien wskazywać kierunki planowania swojemu sztabowi, określając zamiar, oraz podległym dowódcom. Proces ochrony informacji jest stosowany przez działania wykorzystujące nowoczesne technologie.

Elementami ochrony własnej informacji i systemów informacyjnego komunikowania są: **kontrwywiad, ochrona psychologiczna, ochrona elektroniczna, ochrona informatyczna, inżynieryjna rozbudowa** i **kontrdezinformacja**. Ponadto przedsięwzięciami odnoszącymi się do całej sfery ochrony są: **bezpieczeństwo działań i maskowanie**.

Kontrwywiad

Kontrwywiad ochrania działania, systemy, technologię, urządzenia, personel i inne zasoby przed nielegalnymi, tajnymi operacjami obcych służb, grup terrorystycznych i innych. Kontrwywiad ocenia możliwości wykorzystania potencjalnych źródeł informacji i ich słabości.

Ochrona psychologiczna

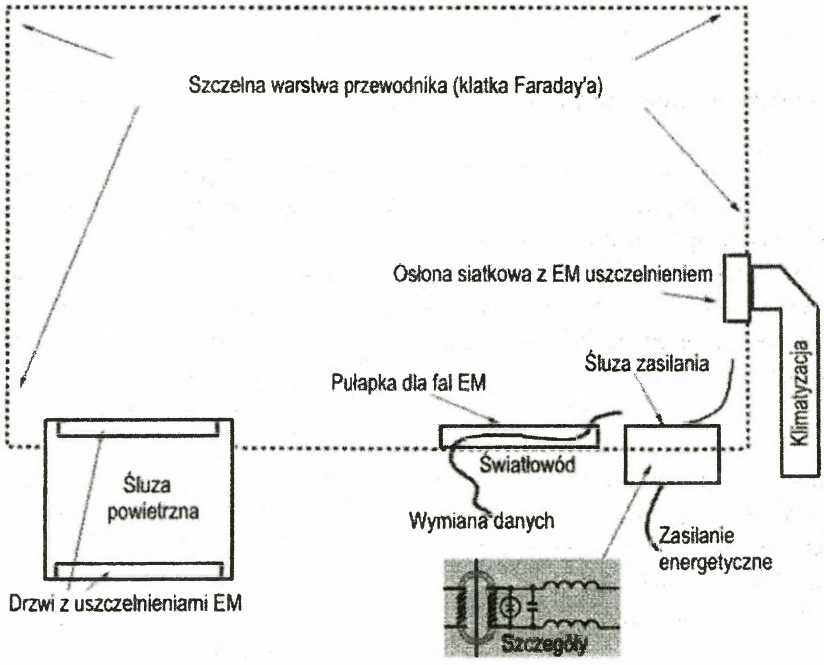
W licznych organizacjach i działaniach można zidentyfikować operacje psychologiczne przeciwnika mające na celu wpływ na społeczeństwo i siły zbrojne. Zwalczanie takich informacji jest bardzo ważne dla powodzenia działań. Dowódcy sił powietrznych muszą rozważyć, jak prowadzić informowanie publiczne o działaniach bojowych i jak osłabiać przewidywane efekty działań psychologicznych przeciwnika. Jeśli zajdzie potrzeba, to ofensywnymi przeciwdziałaniami informacyjnymi, takimi jak atak informacyjny i fizyczny czy walka elektroniczna należy przerwać dystrybucję wiadomości przeciwnika.

Ochrona elektroniczna

Ochrona elektroniczna obejmuje działania mające na celu ochronę personelu, urządzeń i wyposażenia przed przedsięwzięciami rozpoznania i informacyjnego ataku przeciwnika, prowadzonego głównie w formie ataku elektronicznego. Ochrona elektroniczna obejmuje m.in. zmianę częstotliwości pracy i częstotliwości powtarzania impulsów radarowych. Zintegrowanie ochrony elektronicznej i innych przedsięwzięć ochrony i obrony może zapobiec wykryciu, blokadzie, dezorganizacji, zmyleniu i zniszczeniu informacyjnych systemów przez przeciwnika. Zależność własnych sił od zaawansowanej technologii wymaga ochrony elektronicznej. Podejmuje się wiele przedsięwzięć ochrony elektronicznej, możliwych do przeprowadzenia w siłach powietrznych. Nie sposób zidentyfikować wszystkie. Zaprezentowany zostanie jeden, przykładowy, dotyczący ochrony przed atakami elektromagnetycznymi bombami lotniczymi. Jest on na tyle uniwersalny, że może też dotyczyć ochrony przed atakami elektromagnetycznymi prowadzonymi w dowolny sposób.

Ochrona przed atakami elektromagnetycznymi (bombami elektromagnetycznymi)

Najefektywniejszą obroną przed elektromagnetycznymi bombami[190] jest niedopuszczenie do ich użycia albo przez zniszczenie platform ich przenoszenia, albo samych bomb. Jest to jednak trudne i nie zawsze możliwe, dlatego należy poszukiwać także innych sposobów zabezpieczania się przed efektami użycia tego typu ładunków. Sprzęt, który może być narażony na tego typu ataki, powinien być uodporniony na elektromagnetyczne oddziaływania. Najlepszą metodą takiego uodpornienia jest rozmieszczenie urządzeń elektronicznych i elektrycznych w pomieszczeniach zamkniętych od wewnątrz lub zewnątrz szczelną warstwą przewodnika, który tworzy tzw. klatkę Faradaya (rys. 37). Klatka taka, o ile jest szczelna, zapobiega wnikaniu promieniowania elektromagnetycznego do jej wnętrza. Jednakże większość sprzętu elektronicznego musi w jakimś stopniu komunikować się z otoczeniem zewnętrznym. Zwykle także zasilanie energetyczne doprowadzane jest z zewnątrz. Takie połączenia stanowić mogą dogodne kanały wnikania destrukcyjnych impulsów elektrycznych do wnętrza klatki. Jedynym odpornym kanałem komunikowania z otoczeniem są kable światłowodowe.



Źródło: C. Kopp, *The E-Bomb – A Weapon of Electrical Mass Destruction*, http://www.cs.monash.edu.au/carlo/ 04.1997 r.

Rys. 37. Pokój komputerowy zabezpieczony przed atakiem elektromagnetycznym

[190] Opracowano na podstawie: C. Kopp, wyd. cyt.

Ochronę konwencjonalnych połączeń kablowych stanowią filtry. Jednakże filtry te, mimo iż nieskomplikowane w swojej konstrukcji, nie mogą stanowić szerokopasmowej zapory. Filtry, które chronią przed niszczącym impulsem niskiej częstotliwości, mogą się okazać nieskuteczne przy impulsie mikrofalowym.

Uodpornianie jest skuteczniejsze, gdy jest prowadzone kompleksowo. Działanie to powinno się zaczynać na etapie projektowania i być kontynuowane w czasie wykonania i eksploatacji. Uodpornianie nieprzystosowanego sprzętu i pomieszczeń jest trudniejsze, a czasami wręcz niemożliwe. Niestaranne uodpornianie może, mimo poniesionych kosztów, nie zapobiec zniszczeniom, a te, jeśli nawet mają ograniczoną skalę, mogą być przyczyną znacznego obniżenia jakości sprzętu. Takie zniszczenia wymagają żmudnej diagnostyki i odpowiednich napraw, co jest kosztowne. Należy także eliminować wszelkie rodzaje niepożądanych emisji, które mogą być wykorzystane przez rozpoznanie przeciwnika. Sieci telekomunikacyjne powinny zawierać nadmiarowe węzły oraz konstrukcję zapewniającą niezbędną odporność.

Ochrona informatyczna

Ochrona informatyczna zawiera ochronę systemów informacyjnych przed niepożądanym dostępem do znajdującej się w nich informacji lub jej niszczeniem. Obejmuje to ochronę komputerów, łączności i przedsięwzięcia potrzebne do wykrycia, udokumentowania i przeciwdziałania takim zagrożeniom. Ochrona komputerów zawiera przedsięwzięcia podejmowane celem ochrony tajności integralności i dostępności informacji przetwarzanej i przechowywanej w komputerze. Składają się na to: odpowiednia polityka, procedury, hardwarowe i softwarowe narzędzia potrzebne do ochrony systemów komputerowych i informacji. Bezpieczeństwo łączności zawiera przedsięwzięcia mające na celu zlikwidowanie dostępu nieautoryzowanych osób do informacji, zapewniając jednocześnie autentyczność komunikacji. Ochrona komunikacji zawiera kryptoochronę, ochronę transmisji, emisji i fizyczną ochronę urządzeń komunikacyjnych i informacji.

Inżynieryjna rozbudowa

Celem inżynieryjnej rozbudowy jest uodpornienie na atak fizyczny przeciwnika. Rozbudowę tę prowadzi się fortyfikując obiekty i stanowiska oraz budując zapory inżynieryjne i wykonując zniszczenia.

Rozbudowę fortyfikacyjną terenu prowadzi się w celu ochrony ludzi i sprzętu przed środkami rażenia przeciwnika. Obejmuje ona budowę ukryć dla ludzi, dla sprzętu systemów informacyjnych oraz budowę innych obiektów pomocniczych. Rozbudowę fortyfikacyjną terenu prowadzą wszystkie rodzaje wojsk, stosownie do potrzeb i możliwości, wykorzystując naturalne właściwości ochronne terenu.

Kontrdezinformacja

Kontrdezinformacja – to wysiłek mający na celu negowanie, neutralizowanie, zmniejszanie efektów lub zyskanie przewagi nad obcą dezinformacją. Kontrdezinformacja może zapewnić własnym dowódcom przygotowanie się na działanie przeciwnika i podjęcie odpowiedniego przeciwdziałania. Zintegrowane działania kontrdezinformacji zapewniają przygotowanie na postawę lub intencje przeciwnika, a także zidentyfikowanie jego prób mających na celu wprowadzenie w błąd naszych sił. W związku z rozwojem w siłach powietrznych coraz bardziej zintegrowanych systemów czasu rzeczywistego, metody identyfikacji działań dezinformacyjnych przeciwnika muszą rozszerzyć się poza tradycyjne procesy wywiadowcze.

Bezpieczeństwo działań

Siły zbrojne stosują przedsięwzięcia bezpieczeństwa, by informacje i systemy informacyjne chronić oraz bronić. Przedsięwzięcia te odnoszą się do bezpieczeństwa operacyjnego i ochrony informacji. Bezpieczeństwo operacyjne jest procesem identyfikacji najważniejszych informacji i analizowania własnych akcji, które towarzyszą działaniom militarnym i innym działaniom w celu:

- **identyfikowania tych akcji, które mogą być obserwowane przez systemy wywiadowcze przeciwnika;**
- **określania wskaźników, które obce systemy rozpoznania mogą zebrać, zinterpretować i złożyć w całość, aby uzyskać najważniejsze informacje we właściwym czasie;**
- **wybierania i zastosowania środków, które wyeliminują lub zredukują do akceptowalnego poziomu słabości własnych działań wobec przeciwnika.**

Bezpieczeństwo operacyjne to proces. Jest on zbiorem specyficznych działań prowadzonych według zasad i instrukcji w celu zablokowania przeciwnikowi dostępu do informacji. Bezpieczeństwo operacyjne jest stosowane we wszystkich działaniach wojskowych na wszystkich szczeblach dowodzenia.

Dowódcy sił zbrojnych powinni wskazać kierunki planowania bezpieczeństwa operacyjnego swojemu sztabowi na początku procesu planistycznego, kiedy określają swój zamiar i następnie dla podległych dowódców w łańcuchu dowodzenia. Poprzez utrzymanie łączności ze wspierającymi dowódcami i koordynowanie planowania bezpieczeństwa operacji, dowódca zapewnia jedność wysiłku w uzyskiwaniu i utrzymywaniu potrzebnego stopnia utajnienia.

Maskowanie

Za domenę maskowania uważa się przede wszystkim **ukrywanie**, **pozorowanie** i **dezinformowanie**.

Ukrywanie ma na celu[191] uczynienie maskowanego obiektu niewidzialnym. W aspekcie zjawisk psychofizycznych polega ono na dążeniu do uniemożliwienia

[191] G. Nowacki, *Współczesne poglądy...* s. 71–72.

podmiotom rozpoznania dokonania aktu przedstawienia sobie ukrytych przedmiotów. Istnieją dwa podstawowe sposoby osiągania tego celu.

Pierwszy polega 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 powstaje 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 przedstawianie 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 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. Swoją niedoskonałą organizację człowiek poprawia, stosując różnorodne urządzenia techniczne, dzięki którym stosunkowo łatwo radzi sobie z kamuflażem. Lornetka obniża wartość krytycznego progu kontrastu, kamera termowizyjna pozwala spostrzec różnice temperatur obiektu i tła, a jednoczesna obserwacja wielospektralna komplikuje kamuflaż do potęgi równej liczbie pasm spektrum obserwacji. Jednak mimo tych wszelkich utrudnień, ukrywanie nadal odgrywa w maskowaniu rolę szczególną, z uwagi na fakt, że dotyczy bezpośrednio rzeczywistego przedmiotu rozpoznania. Tym też można tłumaczyć priorytet ukrywania w maskowaniu bezpośrednim.

Krótka charakterystyka **dezinformacji** została zawarta w podrozdziale 4.2.5., charakteryzującym przedsięwzięcia informacyjnego ataku. Jednym z elementów dezinformacji jest **pozorowanie**, czyli tworzenie sytuacji nierzeczywistej. Tworzenie to polega na rozmieszczaniu pozornych elementów w infrastrukturze informacyjnej i kreowaniu fałszywej aktywności tej struktury do maskowania stanu rzeczywistego.

W ramach informacyjnej obrony celem dezinformacji jest przede wszystkim ukrycie prawdziwego stanu informacji i organizacji oraz dyslokacji elementów własnych systemów informacyjnych, a także struktury informacyjnej obrony.

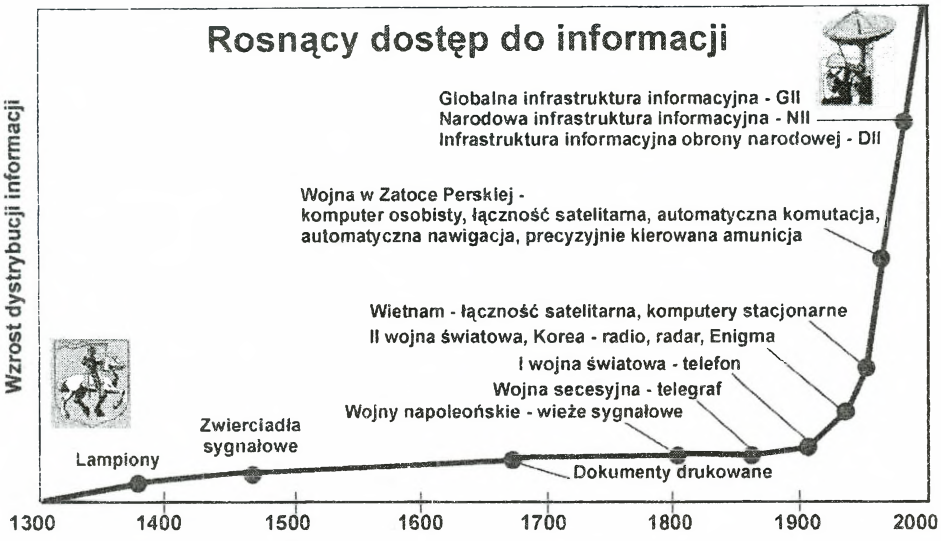
5. INFORMACYJNE ZABEZPIECZENIE

5.1. Ustalenia terminologiczne

Informacja od zarania dziejów była niezwykle pożądanym dobrem. Bardzo wcześnie zrozumiano jej rolę w osiąganiu sukcesu. Już sześć wieków przed naszą erą pisano: „Poznaj dobrze wroga i poznaj dobrze siebie, a w stu bitwach nie doznasz klęski”[192]. Pomimo to dostęp do informacji był ograniczony możliwościami jej przesyłania i dystrybucji, i mimo upływu wieków nie następował radykalny wzrost możliwości w tym zakresie. Praktycznie do końca XIX w. obserwowano bardzo powolny rozwój możliwości dostępu do informacji. Nastanie XX w. zapoczątkowało dynamiczne zmiany w tym zakresie. Zmiany te były rezultatem rewolucji naukowej i technologicznej. Efektem tych zmian było pojawienie się cywilizacji przemysłowej. Upłynął zaledwie wiek, a już stoimy w obliczu nowej cywilizacji informacyjnej. Charakterystyczną cechą minionego wieku był gwałtowny wzrost możliwości przesyłania i przetwarzania informacji (rys. 38). Informacja staje się obecnie głównym dobrem nowej cywilizacji. Jej znaczenie ciągle rośnie, również w sferze militarnej. Informacja jest nie tylko „paliwem” procesów decyzyjnych, lecz także warunkiem precyzyjnego atakowania. Do zaplanowania ataku jądrowego wystarczyły współrzędne centrum miasta. Było to możliwe dzięki dużej powierzchni rażenia. Jednakże taka masowa destrukcja nie jest potrzebna. Wystarczy bowiem zniszczyć węzłowe miejsca danego systemu, by go sparaliżować. Pojawiła się więc broń precyzyjna. W zdecydowanej większości wypadków broń ta nie ma zdolności samodzielnego wyszukania obiektu ataku spośród otoczenia. Potrzebna jest więc informacja o pożądanym miejscu trafienia. Przy dokładnościach trafienia rzędu metra i niżej, nie wystarczy np. określić współrzędne schronu. Należy określić np. miejsce znajdowania się centrum dowodzenia w tym schronie. Również współczesna logistyka dąży do zapewniania systematycznych dostaw, kosztem gromadzenia wielkich zapasów. Zwiększa to jednak zapotrzebowanie na informację. To tyko kilka przykładów ilustrujących zwiększające się zapotrzebowanie na informację. Z tego powodu współcześnie gwałtownie wzrasta rola rozpoznania całej sfery informacyjnego zasilania.

---

[192] Sun Tzu, s. 43.



Źródło: JP 3–13: *Joint Doctrine for Information Operations*, Washington 1998, s. I–12.

Rys. 38. Wzrost prędkości przepływu i przetwarzania informacji

Każde racjonalne działanie wymaga informacji. W kooperacji pozytywnej współpracujące strony przekazują sobie informację o swoich zamiarach i działaniach. W kooperacji negatywnej sytuacja jest odmienna. Informacja jest skrywana, a dostęp do niej broniony. Ponieważ informacja jest podstawą racjonalności działania to mimo obrony musi być zdobywana. Pokonaniu obrony informacji służy wiele różnorodnych zabiegów. Lokują się one zarówno w sferze doskonalenia technologicznego, jak i organizacyjnego.

W sferze militarnej całokształt zabiegów mających na celu zdobycie i oczyszczenie danych oraz przetworzenie ich na informację, nazywane jest w literaturze polskiej rozpoznaniem. Kultura Zachodu wykształciła inne kategorie. Są nimi wywiad, śledzenie i rozpoznanie pola walki (*intelligence, surveillance, and reconnaissance*).

Pod pojęciem „***intelligence***"[193] rozumie się rezultat wszelkich działań gromadzenia, przetwarzania, integracji, oceny i interpretacji dostępnej informacji dotyczącej obcych państw lub obszarów. Jest to informacja i wiedza o przeciwniku osiągnięta drogą obserwacji, gromadzenia danych, analizy i wnioskowania.

Według dosłownego rozumienia jest to **wiedza wywiadowcza**. W sensie czynnościowym może oznaczać wszelkie czynności prowadzące do uzyskania tej wiedzy. Kategoria ta jest często tłumaczona jako wywiad. ***Intelligence*** jest czymś szerszym niż **informacja** (*information*)[194], która w węższym kontekście rozumiana

[193] Joint Pub 1-02: *Dictionary of Military and Associated Terms*, Department of Defense, Washington, D.C. 1999.

[194] Tamże, s. 216.

jest jako nieprzetworzone dane dowolnego typu, które mogą być użyte do wytworzenia (uzyskania) wiedzy wywiadowczej (*intelligence*).

Śledzenie[195] to inna kategoria, oznaczająca systematyczną obserwację wzrokową, słuchową, elektroniczną, fotograficzną lub inną obszarów powierzchni lub przestrzeni naziemnej, podwodnej i podziemnej, a także miejsc, osób lub rzeczy.

Rozpoznanie pola walki (*reconnaissance*)[196] to misja podjęta dla uzyskania, za pomocą obserwacji wzrokowej lub innych metod detekcji, informacji o działaniu i zasobach wroga lub potencjalnego przeciwnika oraz dla zdobycia danych o meteorologicznej, hydrograficznej lub geograficznej charakterystyce pożądanego obszaru.

Według doktryny sił powietrznych[197] dokładna i aktualna informacja jest ważnym elementem w osiąganiu celów kampanii. Elementem tym są także operacje informacyjne. Poza utrzymywaniem baz danych do węzłowej analizy możliwości przeciwnika wywiad dostarcza wiedzy, która tworzy świadomość sytuacji, co jest istotne dla kontroli i szacowania globalnych warunków. Działania wywiadowcze zmierzają do uzyskania doskonałej znajomości silnych i słabych stron w systemie informacyjnym i infrastrukturze przeciwnika oraz dostarczają informacji o miejscach podatnych na atak. Wywiad tworzy okazje do systematycznej eksploatacji słabości przeciwnika i pomaga w izolowaniu sił od ich przywództwa. Przetwarzanie danych, wspomagane przez technologiczny postęp w zdolnościach komputerów, może tworzyć natychmiastowe globalne wsparcie reagowania kryzysowego. Gromadzenie i analiza informacji muszą być prowadzone stale, szczególnie ze względu na możliwości i wymagania operacji informacyjnych, podobnie jak tradycyjne rozpoznanie w siłach powietrznych ogniskowało się na prowadzeniu wojny powietrznej.

Ponadto rozpoznawcze zabezpieczenie operacji informacyjnych wymaga gromadzenia i analizy informacji w tradycyjnych obszarach (takich jak np. o ugrupowaniach bojowych), jak również specjalistycznych szczegółów o telekomunikacji i infrastrukturze komputerowej przeciwnika – nie, co systemy kraju posiadają, ale szczegóły, jak one są instalowane, jak pracują i jak są używane. Analitycy rozpoznania dążą też do dokładnego ocenienia prawdopodobnych wariantów działań przeciwnika, włączając w to jego zdolności i zamiary prowadzenia walki informacyjnej. Ten poziom analizy w kilku wypadkach przewyższa współczesne możliwości i będzie wymagał rozwoju nowych technik i systemów gromadzenia informacji albo być może zmiany priorytetów w obecnym gromadzeniu i zasobach analitycznych.

Informacyjna preparacja pola bitwy daje walczącym możność zrozumienia przeciwnika. Integralną częścią tego procesu jest śledzenie i rozpoznanie pola walki, co dostarcza dowódcom w czasie rzeczywistym lub bliskim rzeczywistemu informacji o przeciwniku, jego rozmieszczeniu, dyspozycyjności, możliwościach oraz o jego zamiarach. Zasoby sił powietrznych zapewniają dowódcom elastyczne zdolności kolekcji informacji w ramach wspierania procesu decyzyjnego. Śledze-

[195] Tamże, s. 432.
[196] Tamże, s. 371.
[197] AFDD 2-5: *Information Operations*, Washington, D.C. 1998, s. 21–22.

nie i rozpoznanie pola walki są w praktyce często prowadzone jednocześnie przez te same zespoły lub platformy. **Jednakże funkcje te są rozróżniane przez definicje: śledzenie jest to ciągłe gromadzenie informacji z powietrza, przestrzeni kosmicznej i powierzchni ziemi; rozpoznanie pola walki jest prowadzone, aby uzyskać informacje o zlokalizowanych i konkretnych obiektach w ściśle ograniczonym czasie.**

Śledzenie i rozpoznanie pola walki są bardzo istotne w jakimkolwiek wojskowym działaniu, włączając w to operacje informacyjne. Na przykład: śledzenie i rozpoznanie pola walki może być wykorzystane do wykrycia i lokalizacji źródeł emisji elektronicznej, a te z kolei do przeprowadzenia ataku informacyjnego lub fizycznego.

Z powyższych treści nietrudno zorientować się w **istnieniu głębokich różnic między podstawowymi kategoriami sfery informacyjnego zasilania procesów decyzyjnych oraz innych potrzeb społecznych w kulturze Zachodu i Polski.** Istniejący w Polsce stan wywodzi się z definicji wypracowanej przez sztukę wojenną Układu Warszawskiego. Każde z tych rozwiązań ma zalety i wady. Nie jest najważniejszym zadaniem dokonywanie ocen. Funkcjonujące kategorie wywodzą się bowiem z tradycji, są głęboko zakorzenione w świadomości środowisk i niełatwo ulegają modyfikacjom. Niewątpliwie przynależność Polski do NATO będzie wywierała coraz większy wpływ na przenikanie sposobów myślenia i elementów kultury do praktyki. Wysiłki teoretyków mające na celu wprowadzenie klarownych podziałów i precyzyjnych kategorii z trudem będą trafiać do praktyki. Ta bowiem jest rezultatem wielonarodowych kompromisów w sferze doktryn. Jeżeli trudno zmienić nawyki środowiska jednego kraju, to tym trudniej dokonać tego wobec tak wielu członków NATO, wśród których jest mocarstwo globalne i potęgi regionalne. Wynika z tego, że w praktyce zakorzeniać się będą raczej standardy nieprecyzyjnych nieraz doktryn NATO, niż racjonalne postulaty badaczy nauk wojskowych. Nie oznacza to, iż nie należy podejmować wysiłków porządkujących w sferze teorii.

Podejście państw Zachodu i ustalenia polskiej sztuki wojennej oraz doktryny, należy stwierdzić, że w podejściu tego pierwszego uwidacznia się wyraźna wada, jaką jest brak jednej nadrzędnej kategorii, która obejmowałaby całą aktywność sfery informacyjnego zasilania. Doraźnym sposobem zapobiegania tej wadzie jest stosowanie sztucznej, zespolonej kategorii w postaci trzech stojących razem nazw: ***intelligence, surveillance, reconnaissance***. W praktyce, dla ułatwienia, stosuje się skrót **ISR**. Ta sztuczna kategoria coraz bardziej utrwala się w piśmiennictwie Zachodu. Tymczasem zarówno w polskiej teorii, jak i praktyce istniejąca kategoria „rozpoznanie" jest jedną, nadrzędną, obejmującą całą aktywność zasilania informacyjnego. Istnieją natomiast różne propozycje dekompozycji, jednakże niewątpliwy jest postulat dążenia do zachowania narodowych ustaleń w tym zakresie. Dlatego też **przyjęto, że podstawową kategorią sfery informacyjnego zasilania jest rozpoznanie.**

Z punktu widzenia operacji informacyjnych, zgodnie z wcześniejszymi ustaleniami, zaspokajanie potrzeb informacyjnych własnych procesów wewnętrznych

państwa jest domeną **informacyjnego zabezpieczenia**. Aktywność ta obejmuje zdobywanie oraz dostarczanie informacji i mieści się w zakresie znaczeniowym rozpoznania. Tak więc **informacyjne zabezpieczenie jest treścią rozpoznania**.

Komponentom państwa odpowiadają przynależne im części rozpoznania, z czego wynika, iż komponentowi militarnemu przynależy **rozpoznanie militarne**.

Niezależnie od tych kategorii wyróżnia się różne podziały sposobów i technik rozpoznania. Na przykład w piśmiennictwie Zachodu wyróżnia się:

IMINT (*imagery intelligence*) – rozpoznanie wizyjne (często nazywane również obrazowym) polegające na uzyskaniu informacji za pomocą zdjęć (obrazu) rozpoznawanego obiektu; ten rodzaj rozpoznania wykorzystuje takie środki, jak: aparaty fotograficzne, czujniki podczerwieni, lasery, czujniki elektrooptyczne, stacje radiolokacyjne z syntetyczną apreturą.

SIGINT (*signals intelligence*) – rozpoznanie sygnałowe; jest to kategoria, której zadaniem jest rozpoznanie wszelkich środków, gdziekolwiek by one były rozmieszczone, emitujących podczas swojej pracy energię elektromagnetyczną; tego typu rozpoznanie polega głównie na rozpoznawaniu pracujących stacji radiolokacyjnych, przechwytywaniu korespondencji radiowej prowadzonej pomiędzy poszczególnymi radiostacjami lub innych form przesyłania danych.

HUMINT (*human intelligence*) – rozpoznanie osobowe, które w działaniach operacyjnych wykorzystuje ludzi jako źródło informacji; opiera się ono na zeznaniach ludzi posiadających daną informację lub tych, którzy mieli z taką informacją osobisty kontakt. Pożyteczne są w tym wypadku raporty załóg wykonujących zadanie, sieć agenturalna, kontrwywiad czy też ludzie dobrze znający dany rejon.

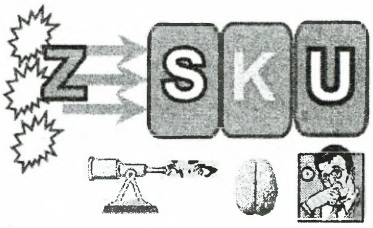
MASINT (*measurement intelligence*) – rozpoznanie pomiarowe i sygnaturowe, zajmuje się pomiarem i analizą szeregu danych z różnego rodzaju źródeł; jego rezultatem są informacje wywiadowcze polegające na wykryciu, śledzeniu, identyfikowaniu lub opisywaniu (określaniu charakterystyk) obiektów; MASINT polega również na zaawansowanej obróbce i wydobywaniu danych dostarczanych przez źródła IMINT i SIGINT; do typowych czujników MASINT zalicza się: radary, systemy optyczne, podczerwone, akustyczne, nuklearne, czujniki promieniowania i sejsmiczne; wspierane są one przez systemy analizujące skład gazów, cieczy i ciał stałych. MASINT jest najnowocześniejszą dyscypliną rozpoznania, najszerszą pod względem zakresu używanych czujników, często łączącą pozostałe kategorie, a więc: IMINT, SIGINT i HUMINT.

OSINT (*open – source intelligence*) – rozpoznanie ze źródeł ogólnodostępnych, tzw. biały wywiad. Wykorzystuje informacje, które są powszechnie dostępne dla opinii publicznej w środkach masowego przekazu, takich jak: prasa, radio, telewizja, Internet.

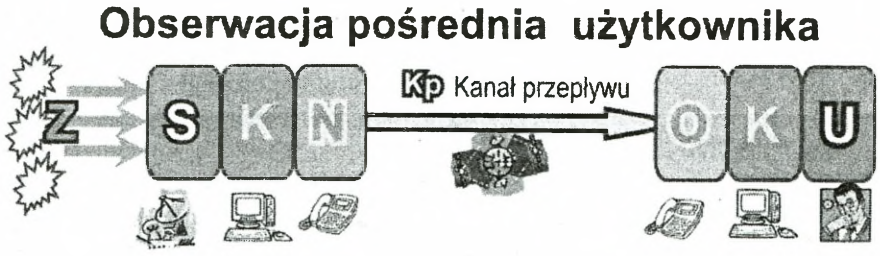
Podział ten ma jednak wady, gdyż brak w nim m.in. wyraźnego kryterium, a elementy podziału nie są rozłączne. W poszukiwaniu klarownych podziałów warto zastanowić się nad istotą procesów rozpoznania. Są one ściśle związane z informacyjnym komunikowaniem społecznym.

Rozpoznanie prowadzi się dla zaspokojenia potrzeb jakiegoś użytkownika lub użytkowników. W najprostszym przypadku użytkownik sam swoimi zmysłami od-

biera wrażenia wywoływane zjawiskami zewnętrznymi, częścią swoich zmysłów i mózgu przetwarza je na postać dogodną dla bezpośrednich potrzeb procesów myślowych. W wysoce skomplikowanym współczesnym świecie takie sytuacje dotyczą jedynie niektórych potrzeb indywidualnego funkcjonowania jednostek. **W zdecydowanej większości użytkownik skazany jest na pośrednie obserwowanie istniejącej rzeczywistości za pomocą mniej lub bardziej rozbudowanych systemów zewnętrznych**. Systemy takie składają się zwykle z zespołu sensorów, modułu przetwarzania i użytkownika. Sytuacja taka ma miejsce, gdy użytkownik sam obserwuje rzeczywistość za pomocą wspomagających go urządzeń. Jednak i taka sytuacja nie jest dominująca. Najczęściej system obserwowania składa się z zespołu sensorów, modułu przetwarzania. Użytkownik zwykle znajduje się poza obszarem zdarzeń, dlatego niezbędne jest przesłanie mu zarejestrowanych zjawisk. Do tego celu jest konieczny jakiś nadajnik, kanał przepływu i odbiornik. Odebrane sygnały muszą być jeszcze dostosowane do możliwości percepcyjnych użytkownika. Niezbędny jest więc kolejny moduł przetwarzania (rys. 39). W rzeczywistości system taki jest jeszcze bardziej rozbudowany, gdyż każdy z tych elementów bywa skomplikowanym zespołem urządzeń lub urządzeń i ludzi.



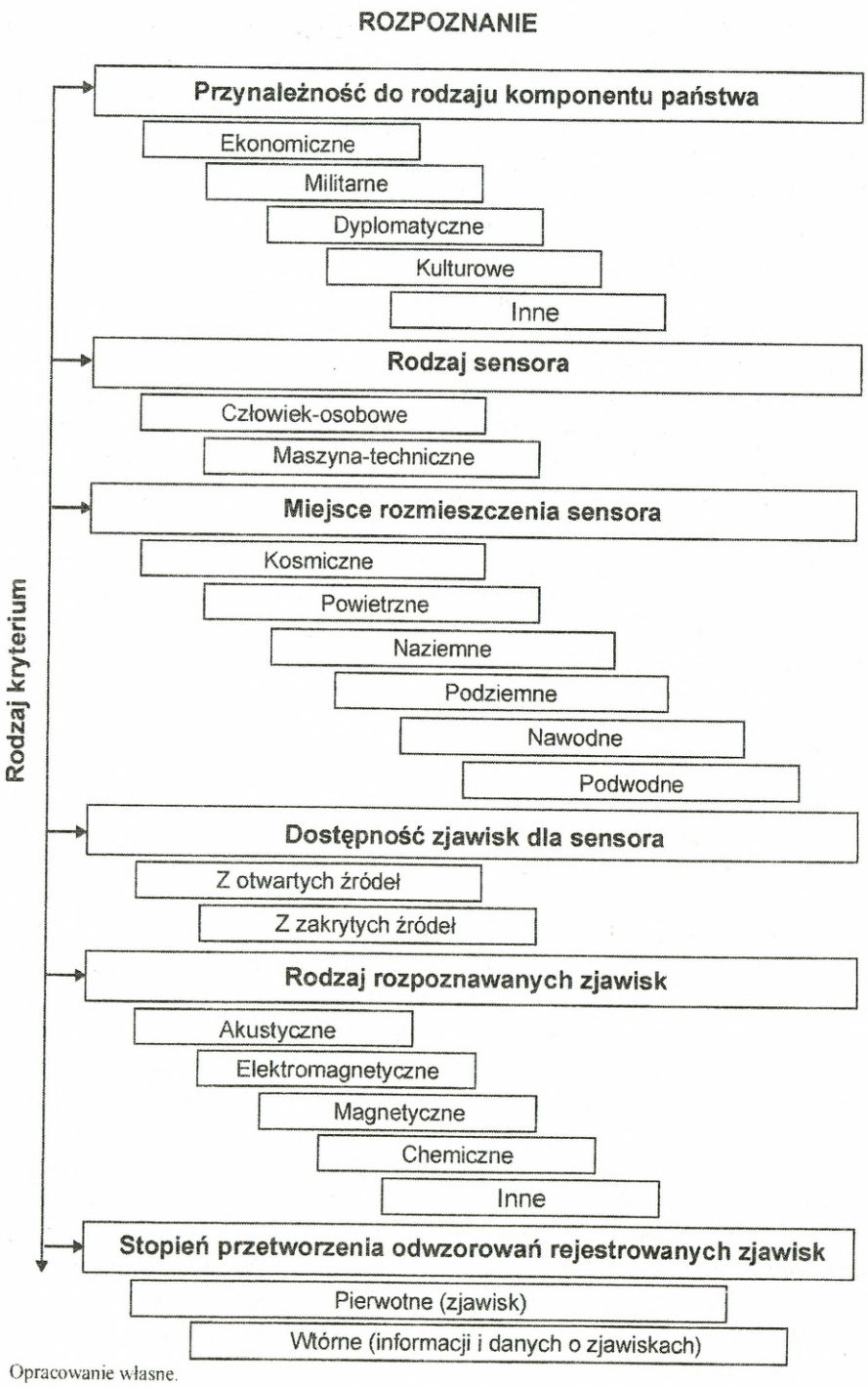
Obserwacja bezpośrednia użytkownika



Z Zjawiska K Moduł przetwarzania O Odbiornik
S Sensory N Nadajnik U Użytkownik

Opracowanie własne.

Rys. 39. Procesy rozpoznania



Opracowanie własne.

Rys.40. Dekompozycja rozpoznania (przykłady)

Wobec takiej sytuacji i potrzeb dokonania dekompozycji należy szukać racjonalnego kryterium podziału sposobów i technik rozpoznania. Kryterium takim może być: rodzaj rozpoznawanych zjawisk, rodzaj sensora, miejsce umieszczenia sensora, wykorzystywane przez sensora zjawisko, dostępność zjawisk dla sensora, sposób przetwarzania. Przykład takiej dekompozycji obrazuje rysunek 40.

W praktyce utrwaliły się jednak wielokryterialne podziały pragmatyczne. Dla potrzeb opisu głównych sposobów i technik prowadzenia rozpoznania, warto wyodrębnić **rozpoznanie osobowe** i **techniczne** (nieosobowe). Kryterium podziału jest tu rodzaj sensora: człowiek lub maszyna. Warto wyodrębnić jeszcze jeden obszar rozpoznania, nie tyle ze względu na rodzaj sensora jako kryterium, lecz ze względu na wykrywane zjawisko, jakim są dane cyfrowe. Wykrywanie i rozpoznawanie danych cyfrowych nazywane jest **rozpoznaniem informatycznym**.

Siły zbrojne mogą stosować wszystkie sposoby rozpoznania. Duże znaczenie, ze względu na możliwości, ma rozpoznanie prowadzone z powietrza (rozpoznanie powietrzne). Nazwa „rozpoznanie powietrzne" może oznaczać, że prowadzone jest ono z powietrza lub że prowadzą je siły powietrzne. Najczęściej jednak używa się go w odniesieniu do rozpoznania prowadzonego z powietrza.

Aktywność rozpoznawcza sił zbrojnych jest ukierunkowana zarówno na zabezpieczenie potrzeb informacyjnego zasilania procesów wewnętrznych tych sił, jak i wspieranych przez nie komponentów państwa.

5.2. Rozpoznanie osobowe

Przestrzeń **rozpoznania osobowego** tworzy człowiek[198] oraz wszelkie narzędzia przystosowane do zdobywania danych w formach bezpośrednio odbieranych przez układ recepcyjny człowieka. Bezpośrednie ludzkie doznania zmysłowe stanowią podstawowe sygnały informacyjne w identyfikowaniu stanu otoczenia. Dla wzmocnienia zasięgu i czułości doznań zmysłowych stosuje się urządzenia wspomagające. W rozpoznaniu tym 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.

Rozpoznanie osobowe jest jednym z najstarszych rodzajów rozpoznania. Rozpoznanie osobowe prowadzi człowiek. Jego bezpośredni kontakt ze zbiorami różnych postaci danych o przeciwniku, może być zapewniony przez: zakonspirowane działania wywiadowcze; fizyczne penetrowanie obszaru przez patrolowanie oraz fizyczne penetrowanie obszaru za pomocą specjalnie przygotowanych działań.

Przestrzeń rozpoznania osobowego należy dzielić na podprzestrzenie:

- **rozpoznania agenturalnego,**

[198] Por. G. Nowacki, *Współczesne poglądy...* s. 46–48.

- **rozpoznania patrolowego,**
- **rozpoznania specjalnego.**

Rozpoznanie agenturalne jest przystosowane do zdobywania i przetwarzania informacji o przeciwniku za pomocą 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.

Rozpoznanie patrolowe może zdobywać dane o przeciwniku przez fizyczną (optyczną i akustyczną) penetrację 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.

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 jest warunkowana możliwościami przerzutu (przenikania) i przetrwania elementów rozpoznawczych. Siły i środki rozpoznania specjalnego mogą pozyskiwać bądź potwierdzać dane zdobyte przez inne źródła bez względu na warunki (pogodę, porę roku, doby) i stopień zamaskowania obiektów. Są one w stanie określić rodzaj, charakter, stan i gotowość bojową przeciwnika, a nade wszystko dokładne współrzędne wykrywanych obiektów.

5.3. Rozpoznanie techniczne

Rozpoznanie techniczne prowadzi się za pomocą systemów wykorzystujących techniczne sensory. Sensory te mogą rejestrować dowolne zjawiska fizyczne, o ile jest to przydatne w osiągnięciu celów rozpoznania. W przeszłości potrafiono rejestrować jedynie niektóre zjawiska, takie jak światło widzialne i fale akustyczne. Później, w miarę postępu, opracowano sensory wykrywające i analizujące parametry fal elektromagnetycznych różnych długości, pola magnetycznego, grawitacyjnego, promieniowania korpuskularnego. Techniczne sensory mogą rejestrować zjawiska zarówno bezpośrednio obserwowalne przez człowieka, jak i pozostające poza zasięgiem rejestracji przez jego zmysły. Sensory te mogą, np. podobnie jak człowiek, rejestrować obrazy w zakresie widzialnym i zapisywać je. Mogą też rejestrować obrazy pozostające poza zasięgiem percepcji człowieka (np. w paśmie podczerwonym). Techniczne sensory obejmują jednakże znacznie szerszy, niż obejmuje człowiek, zakres możliwości rejestracji zjawisk. Dotyczy to zarówno rodzaju tych zjawisk, jak i skali czułości wykrywania. Ponadto techniczne sensory mogą być miniaturowe, ale mogą też być urządzeniami o dużych rozmiarach. Mają one wiele zalet, gdyż mogą np. znajdować się w środowisku niedostępnym dla

człowieka, prowadzić długotrwałą bądź nieustanną rejestrację zaprogramowanych zjawisk. Sensory te mogą wykorzystywać zarówno naturalne emisje obserwowanych obiektów, jak i reakcje otoczenia na obecność obserwowanych obiektów. Mogą też same emitować emisje i rejestrować spowodowane nimi reemisje. Dzieje się tak przy podświetlaniu w paśmie widzialnym, w podczerwieni, podświetlaniu krótkimi falami elektromagnetycznymi (radiolokacja).

Rozpoznanie techniczne, w zależności od przyjętego kryterium, może być różnorodnie dekomponowane. Ze względu jednak na rolę fal elektromagnetycznych większość sensorów jest przystosowana do rejestracji różnych zakresów tych fal. Wobec tego warto rozpoznanie techniczne podzielić na: **elektromagnetyczne** i **pozaelektromagnetyczne**.

Rozpoznanie elektromagnetyczne polega na rejestrowaniu fal elektromagnetycznych. Jednakże ze względu na bardzo szerokie ich spektrum wyróżnia się wiele zakresów i podzakresów fal. Poszczególne sensory tego rozpoznania mają możliwości odbierania tylko wybranych pasm tych fal. W widmie elektromagnetycznym wykorzystywane są głównie[199] 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.

Rozpoznanie radiolokacyjne jest prowadzone za pomocą stacji radiolokacyjnych, które służą do wykrywania powietrznych, naziemnych i nawodnych obiektów 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 powietrznej, systemy rozpoznania powierzchni ziemi SLAR i inne. Prowadzone jest przez samoloty rozpoznawcze wyposażone w stacje radiolokacyjne obserwacji bocznej oraz naziemne, brzegowe, okrętowe stacje radiolokacyjne w różnych zakresach częstotliwości.

Rozpoznanie optoelektroniczne ma na celu zdobywanie oraz przetwarzanie tych informacji o przeciwniku, których nośnikami są fale elektromagnetyczne pasma optycznego. Do pracy w tym paśmie skonstruowano całą rodzinę urządzeń optoelektronicznych, 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 –

[199] Tamże, s. 50–52.

telewizyjne, termowizyjne, noktowizyjne oraz laserowe. 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, w tym funkcjonowania sił i środków przeciwnika.

Rozpoznanie pozaelektromagnetyczne obejmuje aktywność sensorów rejestrujących wszelkie zjawiska zachodzące poza promieniowaniem elektromagnetycznym. Może więc to dotyczyć rejestrowania pól magnetycznych, grawitacyjnych, promieniowań korpuskularnych, fal akustycznych, substancji chemicznych i innych. Rozpoznanie to szybko się rozwija, wkraczając w coraz to nowe obszary możliwości.

Rozpoznanie uwzględniające pomiary pola magnetycznego jest wykorzystywane np. przy wykrywaniu okrętów podwodnych. Poszukiwanie i pomiary substancji chemicznych prowadzi się w celu wykrycia skażeń, ale też np. dla potrzeb określenia składów niebezpiecznych związków chemicznych, wytwórni broni chemicznych lub składników tej broni. W warunkach pokojowych – do monitorowania stanu zanieczyszczenia atmosfery i wód.

Siły zbrojne swoją różnorodną specjalistyczną aparaturą rozpoznawczą mogą prowadzić tego typu rozpoznanie w jego szerokim zakresie możliwości.

5.4. Rozpoznanie informatyczne

Rozpoznanie informatyczne koncentruje się na wykryciu, rejestracji i analizie danych cyfrowych zapisanych na komputerowych nośnikach pamięci oraz na rejestrowaniu ubocznych emisji towarzyszących pracującym elementom sieci komputerowych. Rozpoznanie to obejmuje[200] m.in.:

Nieuprawnione wejście (włamanie) do systemu komputerowego – haking. Polega on na wejściu do systemu po pokonaniu zabezpieczeń w postaci kodów i haseł broniących dostępu do zgromadzonej i przetwarzanej informacji. Penetrowanie przez hakerów systemów informatycznych za pośrednictwem połączeń telekomunikacyjnych jest zjawiskiem o zasięgu międzynarodowym. Nieuprawnione wejście dla potrzeb rozpoznania wiąże sie z dotarciem do danych cyfrowych i ich kopiowaniem.

Według szacunków Departamentu Obrony USA 88% jego komputerów było penetrowanych. Na włamanie są narażone właściwie wszystkie sieci, zarówno mające dostęp z zewnątrz (poprzez Internet), jak i sieci zamknięte (włamania dokonywane przez pracowników niemających wglądu do wszystkich zbiorów informacji). W Internecie można bez trudu odnaleźć specjalistyczne oprogramowanie przełamujące najbardziej wyrafinowane zabezpieczenia lub szukające dziur w sys-

[200] Opracowano na podstawie: J. Hajdukiewicz, *e-Przestępczość*, http://www.it-forum.pl/6/referaty/word/Hajdukiewicz-got.doc.

temie operacyjnym, jak np. program „SATAN", nieodpłatnie rozprowadzany w Internecie od 1995 r.

W Polsce ujawniono sprawców szeregu prób i udanych włamań, zgłaszanych przez polskich administratorów sieci komputerowych, a także próby włamań do systemów komputerowych w Polsce z terenu USA i innych krajów.

Nieuprawnione przechwycenie informacji – podsłuch komputerowy. Współczesne techniki przechwytywania informacji są poważnym zagrożeniem dla systemów informatycznych. Dane komputerowe, można bowiem przejmować zarówno z transmisji teleinformatycznych, jak i w wyniku analizy fal elektromagnetycznych emitowanych przez sprzęt komputerowy (komputery, monitory, przewody) oraz fal akustycznych generowanych przez drukarki; przy tym działania te mogą być zdalne i mogą nie pozostawiać żadnych śladów. Współczesne metody detekcji skrajnie słabych sygnałów obarczonych szumami i zakłóceniami o dużej intensywności, umożliwiają wykrycie sygnałów o poziomach mniejszych o ponad 40 dB od poziomu szumów cieplnych w obwodach elektrycznych.

Bezprawne kopiowanie topografii półprzewodników. Przez topografię półprzewodnika rozumie się rozwiązanie polegające na przestrzennym, wyrażonym w dowolny sposób, rozplanowaniu elementów, z których co najmniej jeden jest elementem aktywnym. W tym wypadku chodzi również o ochronę praw autorskich i patentowych związanych z przestrzennym rozplanowaniem elementów i wszystkich lub części połączeń układu scalonego.

Szpiegostwo komputerowe. W systemach komputerowych na niewielkiej przestrzeni zgromadzone są ogromne ilości danych, które mogą być łatwo i szybko kopiowane za pomocą nowoczesnej techniki, w tym łączy wykorzystywanych do ich przesyłania. Przedmiotami przestępstwa w wypadku szpiegostwa komputerowego są przede wszystkim dane zawarte w systemach informatycznych (kartoteki, wyniki badań, dane handlowe, adresy klientów), dane dotyczące budowy sprzętu i sieci komputerowych, i programy komputerowe. Działanie sprawcy polega przeważnie na nieuprawnionym wejściu do systemu komputerowego po przełamaniu zabezpieczeń i skopiowaniu danych. Może to być także kradzież nośników danych, wykorzystanie „danych resztkowych" pozostałych na dyskietkach lub podsłuch komputerowy.

5.5. Rozpoznanie powietrzne

Rozpoznanie powietrzne może obejmować[201] różne rodzaje rozpoznania, głównie technicznego. Siły powietrzne większych państw, oprócz rozpoznania powietrznego (prowadzonego z powietrza i będącego głównie rozpoznaniem technicznym), prowadzą też niektóre formy rozpoznania osobowego oraz informatycz-

[201] Zob. J. Łazarczyk, *Współczesna technika lotniczego rozpoznania powietrznego*, Referat, Warszawa 2001.

nego. Ostatnio siły powietrzne wielu państw podejmują intensywne wysiłki na rzecz uzyskania zdolności do prowadzenia rozpoznania informatycznego. Wiąże się to z potrzebami i chęciami prowadzenia operacji informacyjnych lub walki informacyjnej przez siły powietrzne. Ponadto poza rozpoznaniem prowadzonym z powietrza, siły powietrzne wielu państw prowadzą naziemne rozpoznanie techniczne, w tym głównie radiolokacyjne. Rozpoznanie to koncentruje się na śledzeniu sytuacji powietrznej w interesie obrony powietrznej. Jednakże i te formy coraz szerzej wkraczają do rozpoznania prowadzonego z powietrza. Na samolotach montuje się bowiem nie tylko stacje radiolokacyjne zabezpieczające bezpośrednie potrzeby nosiciela, lecz także duże radary wczesnego wykrywania i śledzenia. W ten sposób powstały specjalne samoloty wczesnego wykrywania i śledzenia, które przejmują część zadań naziemnego systemu rozpoznania radiolokacyjnego.

Rozpoznanie powietrzne, prowadzone w ścisłym współdziałaniu z innymi rodzajami rozpoznania, uważane jest za najbardziej operatywny sposób pozyskiwania informacji o przeciwniku w warunkach bojowych[202]. Taki stan rzeczy ma miejsce głównie dzięki temu, że lotnictwo rozpoznawcze posiada w wyposażeniu specyficzne środki, o nieporównywalnych z innymi rodzajami rozpoznania możliwościami manewrowymi, przestrzennymi i czasowymi.

Nie należy jednak przy tym zapominać, że do sił rozpoznania powietrznego zalicza się również wyspecjalizowane oddziały i pododdziały przeznaczone do prowadzenia rozpoznania powietrznego, sekcje rozpoznawcze znajdujące się w sztabach kierujących rozpoznaniem powietrznym oraz w sztabach oddziałów i związków taktycznych innych rodzajów sił zbrojnych, wykorzystujących informacje uzyskane z rozpoznania powietrznego. Na szczególną uwagę zasługuje również personel latający, personel kierujący bezpilotowymi aparatami latającymi oraz personel, który opracowuje wyniki z rozpoznania powietrznego.

Do podstawowych rodzajów środków współczesnego systemu rozpoznania powietrznego należą:

- **środki załogowe,**
- **bezpilotowe aparaty latające.**

Środki załogowe, wraz ze swoimi stacjami obróbki naziemnej, stanowią główny element systemu rozpoznania powietrznego. Są zdolne do prowadzenia najtrudniejszych misji i dostarczania informacji w czasie zbliżonym do rzeczywistego. Załogi statków powietrznych są również w stanie reagować na zmieniające się warunki i modyfikować sposób wykonania zadania już w trakcie jego trwania. Posiadają zdolność do przebywania w powietrzu przez długi czas i pokonywania dużych odległości, przez co są w stanie rozpoznać znaczne obszary za pomocą zróżnicowanych czujników.

---

[202] Taką opinię wyrazili: M. Kozub, R. Bartnik, S. Szulc, *Rozpoznanie powietrzne na współczesnym polu walki (według poglądów obowiązujących w NATO)*, „Przegląd Wojsk Lotniczych i Obrony Powietrznej" 1998, nr 12.

Powszechną tendencją we współczesnych środkach załogowych jest wyposażanie ich w systemy przekazujące dane do innych statków powietrznych lub stacji naziemnych w czasie zbliżonym do rzeczywistego.

Bezpilotowe aparaty latające (*unmanned aerial vehicles* – UAV) na obecnym poziomie zaawansowania technicznego posiadają wiele zalet w porównaniu ze środkami załogowymi. Przede wszystkim nie narażają personelu latającego na ryzyko związane z wykonaniem zadania, są generalnie tańsze w eksploatacji, a ich strata zawsze będzie mniej dotkliwa. W planowaniu ich użycia nie należy jednak zapominać o poważnych ograniczeniach. Współczesne systemy bezzałogowe są bowiem w zdecydowanej większości wypadków ograniczone w zastosowaniu do taktycznej strefy działań, a ich zdolność do przenoszenia rozbudowanej i ciężkiej aparatury rozpoznawczej jest bardzo ograniczona.

Znajduje to odzwierciedlenie w stosunkowo małych rejonach rozpoznania, często również bez braku jakiejkolwiek możliwości ingerencji w zmianę trasy lotu już w czasie wykonywania konkretnego zadania.

Być może, w przyszłości rozwój nowych technologii stopniowo wyeliminuje ograniczenia w wykorzystywaniu UAV do zdobywania informacji z powietrza. Jednak współcześnie trzon rozpoznania powietrznego stanowi **rozpoznanie lotnicze**, realizowane przez wyspecjalizowane eskadry, szkolone w wykonywaniu tego rodzaju misji i wyposażone w przystosowane do celów wywiadowczych samoloty oraz szereg innych, zazwyczaj niezwykle zaawansowanych technicznie środków.

Na przestrzeni kilkudziesięciu lat, podczas których wykorzystuje się lotnictwo do prowadzenia działań bojowych, wykształciło się szereg rodzajów lotniczego rozpoznania powietrznego[203]. Różne bowiem były kryteria podziału tego rodzaju lotnictwa, ze względu na czas, sposób wykonania zadania, czy też podporządkowanie organizacyjne danej jednostki lotnictwa rozpoznawczego. Najczęściej jednak przy wszelkiego rodzaju klasyfikacjach przyjmowano, jako pomocnicze, kryterium zakresu oraz charakteru wykonywanych zadań rozpoznawczych.

Wyróżniano więc trzy podstawowe rodzaje rozpoznania: **strategiczne**, **operacyjne** i **taktyczne**. Misje wykonywane w ramach poszczególnych kategorii operacji różniły się zarówno celem prowadzenia rozpoznania, położeniem rejonów zainteresowania, jak i zapotrzebowaniem na szczególny rodzaj informacji. Stąd też brały się różnice w wyposażeniu poszczególnych jednostek w urządzenia rozpoznawcze najlepiej pasujące do charakteru wykonywanych zadań, jak również w odpowiednie statki powietrzne, które byłyby zdolne do ich przenoszenia.

Strategiczne rozpoznanie powietrzne (*strategic air reconnaissance*), jest wkładem sił powietrznych do ogólnego pozyskiwania informacji i prowadzenia rozpoznania na użytek kierownictwa politycznego i wojskowego. Otrzymany za pomocą środków rozpoznania strategicznego obraz stanu rzeczy, służy wczesnemu analizowaniu rozwoju sytuacji kryzysowej, utrzymywaniu inicjatyw polityczno-militarnych oraz elastyczności własnego działania. Sprzęt i środki, za pomocą któ-

[203] Szerzej na temat genezy lotnictwa rozpoznawczego, zob. R. Szymański i in., *Lotnictwo wojskowe*, Warszawa 1998, s. 157–173.

rych prowadzi się strategiczne rozpoznanie powietrzne, posiadają specyficzne właściwości. Ich cechą charakterystyczną jest możliwość prowadzenia rozpoznania i obserwacji zasadniczo bez przekraczania granic, naruszania ustaw międzynarodowych oraz konwencji bilateralnych. Obecnie rozpoznanie takie prowadzi się przede wszystkim za pomocą satelitów i samolotów rozpoznawczych lotnictwa strategicznego oraz w coraz szerszym zakresie przy użyciu bezpilotowych środków rozpoznawczych. Realizowane jest w sposób ciągły, w czasie pokoju, kryzysu i wojny, obejmując nim całe terytorium potencjalnego (realnego) przeciwnika lub regionu, a jego granice wyznaczają głównie możliwości bojowe środków rozpoznania powietrznego.

Operacyjne rozpoznanie powietrzne (*operational air reconnaissance*) realizowane jest na rzecz działań prowadzonych na określonym obszarze w ramach operacji połączonych. Za organizację tego typu rozpoznania odpowiadają organy dowodzenia wojskami szczebla operacyjnego i operacyjno-taktycznego.

Taktyczne rozpoznanie powietrzne (*tactical air reconnaissance*) swoje wysiłki koncentruje przede wszystkim na zdobywaniu i dostarczaniu informacji o przeciwniku, dających podstawę do oceny sytuacji, podjęcia decyzji do działań bojowych oraz ich prowadzeniu[204].

Współcześnie większość zadań zdobywania informacji na korzyść dowództw wszystkich rodzajów wojsk – sił powietrznych, wojsk lądowych i marynarki wojennej – wykonuje się w ramach **taktycznego rozpoznania powietrznego**[205].

Należy przy tym zaznaczyć, że analiza przebiegu ostatnich konfliktów zbrojnych (Zatoka Perska, Bałkany, Czeczenia) wskazuje, że w rozpoznaniu powietrznym coraz częściej zacierają się różnice między poszczególnymi szczeblami dowodzenia. Trudno jest więc dzisiaj jednoznacznie określić, czy dana misja przeprowadzona była na korzyść szczebla strategicznego, operacyjnego, czy taktycznego. Ma to swoje źródła we współczesnym pojmowaniu zakresu (rozmachu) prowadzonej operacji. Obecnie działania Sojuszu są określone jako militarne – strategiczne, operacyjne czy taktyczne – na podstawie ich efektu, czy też wkładu włożonego do osiągnięcia określonych celów i nie są bezpośrednio przyporządkowane do określonego szczebla dowodzenia, wielkości jednostki, jej wyposażenia, czy też typu sił i ich komponentów[206].

Stąd też często samoloty, których początkowym przeznaczeniem było prowadzenie rozpoznania na szczeblu strategicznym, często wykonują rozpoznanie na

---

[204] Zob. M. Kozub, *Rozpoznanie powietrzne w działaniach bojowych*, Warszawa 2001, s. 64–66.

[205] Nazwa ta, funkcjonująca w NATO, w rzeczywistości nie jest adekwatna do kryjących się za nią treści, gdyż wywodzi się od nazw lotnictwa z okresu zimnej wojny. Wówczas w Europie nie wyróżniano poziomu operacyjnego, w związku z czym istniało lotnictwo strategiczne i taktyczne. W rzeczywistości lotnictwo NATO działa w skali operacyjnej i ma znaczenie co najmniej operacyjne, a nietaktyczne. Jednak w praktyce nazwy te funkcjonują nadal i przeniosły się też na obszary pokrewne, takie jak np. „taktyczne rozpoznanie powietrzne".

[206] Szerzej na ten temat zob. S. Zajas i in., *Podstawy użycia rodzajów wojsk sił powietrznych*, Warszawa 1999, s. 231.

korzyść bezpośrednio walczących jednostek i na odwrót, samoloty rozpoznania taktycznego rozpoznają obiekty ważne ze strategicznego punktu widzenia. Co więcej, w planowaniu misji rozpoznawczych łączy się obecnie poszczególne rodzaje obiektów i szczebli rozpoznania, kiedy tylko jest to możliwe, chociażby ze względu na wytyczoną trasę czy przyjęty profil lotu samolotu rozpoznawczego.

6. PRZYSZŁA MILITARNA WALKA INFORMACYJNA

6.1. Wnioski dotyczące identyfikacji trendów i konstrukcji koncepcji militarnej walki informacyjnej przyszłości

W wyznaczaniu kierunków rozwojowych militarnych operacji informacyjnych, skoncentrowano się szczególnie na obszarze walki informacyjnej. W odniesieniu do przyszłej militarnej walki informacyjnej przyjęto, że będą ją kształtować przede wszystkim, wyłaniające się ogólne trendy rozwoju całego zjawiska, jakim jest walka informacyjna. Na te trendy duży wpływ wywrą teorie walki, które są najbliższe ze względu na podobieństwo zjawisk i warunków. **Wobec podobieństwa środowiska powietrznego i informacyjnego oraz zbieżności wielu cech informacji i potęgi powietrznej, a także doświadczenia i dorobku teorii działań powietrznych obejmującej poszczególne koncepcje tych działań, przyjęto, że teoria ta prawdopodobnie wywrze istotny wpływ na kształtowanie się koncepcji militarnej walki informacyjnej w przyszłości.**

We współczesnym działaniu bardziej niż kiedykolwiek potrzebna jest informacja. Informacja stała się z jednej strony najważniejszym dobrem, z drugiej zaś bronią. Ten, kto oczekuje sukcesu w jakimkolwiek działaniu, musi zapewnić sobie dominację informacyjną. Jest to szczególnie ważne w sferze kooperacji negatywnej. Tutaj dominacja informacyjna staje się warunkiem podejmowania innych działań.

Przez analogię do doświadczeń teorii działań powietrznych założyć należy, iż **zdobycie dominacji informacyjnej stanie się głównym celem początkowego etapu każdych działań, a utrzymanie tej dominacji stanowić będzie przedmiot stałej troski organizatorów działań. Problematyce tej powinna być poświęcona koncepcja dominacji informacyjnej.**

Podobnie jak w wypadku potęgi powietrznej, **osiągnięcie pożądanego stopnia dominacji informacyjnej nie jest celem samym w sobie. Stan ten najczęściej umożliwia podjęcie innych działań prowadzących do osiągnięcia głównego celu działań. Wówczas stosowane będą działania mające charakter informacyjnego wspierania innego typu działań, który w danej fazie może być głównym rodzajem tych działań. Do tego typu działań odnosić się powinna koncepcja informacyjnych działań wspierających.**

Należy także założyć, **że w koncepcji walki informacyjnej istnieć będą działania zasadnicze w postaci informacyjnych działań bojowych oraz działania pomocnicze jako informacyjne działania zabezpieczające.**

Jeśli chodzi o samodzielnie osiągane cele działań informacyjnych, to podobnie jak w wypadku potęgi powietrznej, możliwe jest osiąganie celów taktycznych i operacyjnych. Teoretycznie **istnieje także obszar, którego istotą jest samodzielne osiąganie strategicznych celów politycznych przez walkę informacyjną. Problematyce tej powinna być poświęcona koncepcja informacyjnego ataku strategicznego.**

6.2. Walka o przewagę informacyjną

W klasycznym modelu działań sił powietrznych pierwszym celem tych działań jest wywalczenie i utrzymanie przewagi w powietrzu. Pomyślne wykonanie tego zadania nie wyczerpuje jednak misji sił powietrznych. Zdobyta i utrzymywana przewaga, a nawet panowanie w powietrzu, zazwyczaj nie stanowi osiągnięcia politycznego celu walki. Dlatego w praktyce stworzenie przewagi w powietrzu, to wykreowanie warunków do podjęcia działań prowadzących bezpośrednio do osiągnięcia politycznego celu walki. Cel ten może być osiągnięty albo w wyniku wykonania strategicznego ataku powietrznego, albo w wyniku przeprowadzenia strategicznego ataku lądowego lub morskiego. W trudniejszych sytuacjach polityczny cel działań może być osiągnięty dopiero w wyniku serii różnych działań i dopięcia kilku celów pośrednich. Mamy wtedy do czynienia z ciągiem różnych działań, nazywanych w języku teorii i doktryn militarnych kampanią. Poszczególne sekwencje, nazywane fazami kampanii, mają zwykle wyraźny charakter powietrzny, lądowy lub morski. Charakter ten wynika z głównego, w danej fazie kampanii, zadania. W rezultacie najczęściej występuje taka sytuacja, że istnieje główny aktor, zwany wspieranym oraz wspierający go aktorzy, zwani wspierającymi, przy czym stan ten nie jest trwały. W jednej fazie kampanii głównym aktorem (wspieranym) mogą być siły powietrzne. Wówczas inne komponenty podporządkowują swoje działania koncepcji działań wspieranego. W kolejnej fazie rola wspieranego może przypaść siłom lądowym i wówczas siły powietrzne podporządkowują swoje działania potrzebom walki lądowej. W sporadycznych wypadkach może zaistnieć sytuacja wykonywania równie ważnych zadań przez dwa komponenty. Wówczas realizowane będzie współdziałanie. Jednakże sytuacja ta ma miejsce przy wielkim rozmachu kampanii lub na rozległym teatrze w różnych obszarach działań.

Ostatnio mocno akcentuje się koncepcję działań połączonych. Istotą tej koncepcji jest racjonalne, w danej sytuacji, zaprojektowanie sekwencji działań oraz dopasowanie odpowiednich do potrzeb tych sekwencji komponentów militarnych. Jest to więc precyzyjne ustalenie wiodących (wspieranych) aktorów teatru działań oraz włączenie pozostałych uczestników walki we wspieranie wysiłku głównych aktorów. W rezultacie wszyscy mogą prowadzić działania bojowe, ale zawsze jest

wspierany i wspierający. Wynika to z doświadczenia oraz z postulatów wielu zasad sztuki wojennej. Takie podejście przyjęto zarówno w amerykańskiej doktrynie działań połączonych, jak i w doktrynie działań połączonych NATO.

Podobnie jak w klasycznej koncepcji działań powietrznych, **walka informacyjna może mieć na celu osiągnięcie przewagi informacyjnej. Przewaga ta będzie niezbędna dla prowadzenia zasadniczych działań zmierzających do osiągnięcia politycznego celu w danym konflikcie**. Tymi działaniami mogą być zarówno klasyczna walka, jak też walka informacyjna. Obecnie gwałtownie rozwijający się potencjał walki informacyjnej i rosnąca wrażliwość państw na tę walkę, umożliwiają osiąganie celów politycznych konfliktu tylko przez zastosowanie przedsięwzięć walki informacyjnej. Jednakże walka informacyjna jest nowym zjawiskiem, nową przestrzenią z nieukształtowanym samodzielnym podmiotem tej walki. Nie został jeszcze wyodrębniony oddzielny rodzaj sił odpowiedzialny za tę walkę. Jednocześnie z wcześniejszych rozważań wynika, że walka informacyjna jest osobliwym zjawiskiem, obejmującym wszystkie obszary aktywności państwa, w związku z czym **niemożliwe jest utworzenie samodzielnego rodzaju sił odpowiedzialnego za prowadzenie walki informacyjnej, gdyż musiałby się on składać z elementów zaczerpniętych ze wszystkich obszarów aktywności państwa. Możliwe i pożądane jest zaś utworzenie organu koordynującego przedsięwzięcia walki informacyjnej i operacji informacyjnych prowadzonych przez wszystkie komponenty państwa**. Ponadto walka informacyjna, a szczególnie walka mająca osiągać strategiczne cele polityczne, powinna mieć jak największy zasięg. **Dlatego też zarówno poszczególne rodzaje sił zbrojnych, jak i całe siły zbrojne mogą samodzielnie prowadzić walkę informacyjną jedynie w ramach wspierania działań zbrojnych lub wtedy, gdy cel działań ma ograniczony charakter. Mogą więc brać udział w walce o przewagę informacyjną, uczestniczyć w informacyjnym ataku strategicznym państwa lub wspierać działania innych komponentów państwa w zakresie swoich możliwości. Ponadto rola sił zbrojnych w walce informacyjnej państwa zależeć będzie od stopnia rozwoju możliwości prowadzenia tej walki**. Nawet gdyby powstały jakieś siły przeznaczone do prowadzenia tej walki, to i tak nie zwolni to innych komponentów państwa z uczestniczenia w niej. Poziom zdolności do prowadzenia walki informacyjnej w siłach zbrojnych i ich komponentach będzie zależał od wizji przyszłej ich misji oraz determinacji w jej wdrażaniu.

6.2.1. Dominacja powietrzna

Wynalezienie samolotu i jego militarne zastosowanie, w stosunkowo niedługim czasie spowodowało głębokie zmiany sytuacji polityczno-militarnej, jak również sztuki wojennej. Przed jego pojawieniem się zagrożenie atakami ogniowymi ograniczało się do zasięgu artylerii. By jakiś rejon znalazł się w strefie zagrożenia, musiały najpierw dotrzeć w jego otoczenie wojska lądowe lub w strefie przybrzeżnej okręty marynarki wojennej. By zagrozić obiektom położonym na dalekich tyłach państwa przeciwnika, należało najpierw przeprowadzić trudną operację zdo-

bycia i zajęcia terenu. Działania bojowe okresu przedlotniczego toczyły się na stosunkowo niewielkich obszarach bezpośrednich starć wojsk. Przybierały one formy bitew, a w późniejszym okresie wydłużonych linii styczności bojowej wojsk, wzdłuż których rozciągał się pas strefy bojowej. Poza tymi obszarami, nie licząc aktów sabotażu, terroru i dywersji, nie istniało zagrożenie uderzeniami ogniowymi. Wielkie obszary terytoriów położonych z dala od strefy działań bojowych pozostawały bezpieczne. Nawet w czasie wojen toczyło się normalne, niewojenne życie.

Pojawienie się lotnictwa wojskowego, a szczególnie samolotów uderzeniowych dramatycznie zmieniło tę sytuację. Bezpieczne dotychczas obiekty strefy tyłowej znalazły się nagle w zasięgu samolotów uderzeniowych; bezpieczne dotychczas ośrodki władzy, rejony przemysłowe, zasoby infrastruktury, różnego typu zapasy, rejony mobilizacji wojsk, a także miejsca przebywania i aktywności ludności cywilnej mogły zostać w każdej chwili zaatakowane. Te nowe możliwości były pogłębiane przez szybko rozwijające się teorie wojny powietrznej oraz doktryny wyrażające gotowość państw do korzystania z nich. Lotnictwo uderzeniowe, ale i rozpoznawcze, stało się komponentem militarnym stanowiącym największe zagrożenie. Uderzenie lotnicze na obiekty położone nawet w strefie tyłowej mogło zostać wykonane w bardzo krótkim czasie. Gwałtownie wzrosła więc możliwość uzyskania zaskoczenia. Ze względu na właściwości lotnictwa, m.in. takie jak duża prędkość, manewrowość, duży zasięg, trudno zorganizować skuteczną obronę przed jego działaniem. Samoloty mogą swobodnie manewrować, nie mając żadnych barier geograficznych w przestrzeni powietrznej. Mogą w jednym nalocie zaatakować obiekty w jakimś rejonie, a w drugim uderzeniu zaatakować inny odległy obszar. Obecność lotnictwa, mimo że nie jest stała w przestrzeni przeciwnika, to jednak tworzy efekty ciągłego oddziaływania ogniowego na najbardziej niepożądane dla zaatakowanego miejsca. Dlatego też potrzeba neutralizacji zagrożenia lotniczego stała się najwyższą koniecznością. Uderzeniowy potencjał lotniczy przeciwnika miał możliwość skutecznego paraliżowania wszelkich działań militarnych, ale także gospodarczych. Potencjał ten, szczególnie gdy szybko rosły jego możliwości, mógł paraliżować kraj lub narażać go na bardzo dotkliwe koszty.

Doprowadziło to do powszechnego przekonania o konieczności uzyskania panowania lub przewagi w powietrzu na początku jakichkolwiek poważniejszych działań militarnych. Istotą tego dążenia była chęć zneutralizowania zagrożenia powietrznego ze strony lotnictwa uderzeniowego. Dosyć szybko uświadomiono sobie, że najlepszym sposobem walki z lotnictwem jest przeciwstawienie mu również lotnictwa. Dlatego też za głównego wykonawcę walki o przewagę w powietrzu uznano lotnictwo.

W wyniku systematycznego rozwoju obrony powietrznej, stała się ona przeszkodą w walce z lotnictwem uderzeniowym przeciwnika. Stąd kolejnym, wymuszonym obiektem zwalczania w ramach walki o przewagę w powietrzu stał się system obrony powietrznej.

Każda strona zaangażowana w walkę o przewagę w powietrzu dąży do neutralizacji możliwości ofensywnych lotnictwa przeciwnika oraz paraliżu je-

go systemu obrony powietrznej, przy jednoczesnym zachowaniu w jak najlepszym stanie swojego powietrznego potencjału uderzeniowego i sprawnego systemu obrony powietrznej. Osiągnięcie takiego stanu umożliwia jeszcze efektywniejsze wykorzystanie możliwości własnego potencjału powietrznego, nazywanego w państwach Zachodu potęgą powietrzną. Wykorzystanie to ma formę albo szybkiego wykonania działań powietrznych prowadzących do osiągnięcia celu politycznego i wygrania konfliktu, albo radykalnego poprawienia warunków prowadzenia innych form walki. Obecnie „[...] dogodna sytuacja w przestrzeni powietrznej i swoboda działań lotnictwa jest [...] podstawowym warunkiem osiągnięcia zwycięstwa na lądzie i morzu oraz pomyślnego rozstrzygnięcia konfliktu zbrojnego.

Już od drugiej wojny światowej każdą operację, bitwę czy walkę wygrywała w zasadzie ta strona starcia militarnego, która dominowała w przestrzeni powietrznej. Klęskę zaś ponosiła ta strona, która nie była w stanie wywalczyć i utrzymać swobody działań własnego lotnictwa. Wywalczenie dominacji w powietrzu było początkiem sukcesów również na lądzie i morzu, natomiast przegrana w trzecim wymiarze – źródłem porażek i klęsk nie tylko sił powietrznych, ale także lądowych i morskich.

Tę zależność między sytuacją w przestrzeni powietrznej a wynikami walk, bitew, operacji i kampanii wojennych, zgodnie podkreślają teoretycy sztuki wojennej. Przedstawiona jest ona również w regulaminach, doktrynach i innych materiałach normatywnych. Potwierdzają ją także rezultaty współczesnych konfliktów zbrojnych"[207].

Walka o przewagę w powietrzu dzieli się na ofensywną i defensywną. **Siły powietrzne w ramach walki o przewagę w powietrzu mogą prowadzić**:

- **ofensywną walkę o przewagę w powietrzu;**
- **defensywną walkę o przewagę w powietrzu (obronę powietrzną).**

Istotą ofensywnych działań walki o przewagę w powietrzu jest **działanie zmierzające do neutralizacji możliwości ofensywnych lotnictwa przeciwnika oraz paraliżu jego systemu obrony powietrznej**. Sposoby prowadzenia tej walki dostosowane są do aktualnych możliwości posiadanego sprzętu i istniejących nawyków doktrynalnych.

Istotą defensywnych działań walki o przewagę w powietrzu jest **działanie zmierzające do zachowania w jak najlepszym stanie swojego powietrznego potencjału uderzeniowego i sprawnego systemu obrony powietrznej, co tworzy warunki do osiągnięcia celu funkcjonowania tego systemu**. Do powszechnie akceptowanych sposobów działań obrony powietrznej można zaliczyć[208]: obronę strefową, obronę obiektową oraz obronę strefowo-obiektową.

Przewagę w powietrzu osiąga się nie tylko w wyniku działań ofensywnych, ale i defensywnych. Obrona powietrzna[209], jako integralna część operacji zwalczania potencjału powietrznego przeciwnika, ukierunkowana jest na osiągnięcie od-

---

[207] W. Michalak, *Dominacja z powietrza*, Warszawa 1999, s. 13–14.

[208] Przyjęto za: B. Zdrodowski, *Podstawy obrony powietrznej*, Warszawa 1997, s. 48.

[209] B. Zdrodowski, M. Marciniak, *Doktryna powietrzna NATO*, Warszawa, 1999, s. 69.

powiedniego stopnia dominacji w przestrzeni powietrznej, a poprzez to na właściwą ochronę własnych sił. Najlepszym sposobem osiągnięcia tego będzie przygotowanie zintegrowanej obrony powietrznej, która realizowana połączonym wysiłkiem będzie spełniała wymagania każdego komponentu sił.

6.2.2. Dominacja informacyjna

Współczesny rozwój ludzkości wyłania nową formę cywilizacyjną, jaką jest społeczeństwo informacyjne. W formacji tej informacja jest dobrem największym. Jest ona substytutem innych zasobów, takich jak surowce, energia czy kapitał, ale także bytem niezbędnym do podejmowania jakiegokolwiek działania zorganizowanego oraz do istnienia społecznej aktywności. Znaczenie informacji zawsze było duże, ale już obecnie informacja staje się podstawą wszelkiej aktywności i coraz częściej jej celem. W sferze walki staje się także substytutem broni, a nawet najskuteczniejszą bronią przyszłości. Informacja bowiem dociera bezpośrednio do umysłu człowieka i może kształtować jego świadomość skuteczniej niż za pośrednictwem fizycznej presji zewnętrznej.

Badając sferę walki informacyjnej, G. Nowacki zidentyfikował przestrzeń tej walki. Uznał on, że „[...] podstawową strukturę 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"[210].

Kiedyś w historii informacja była tylko zabezpieczeniem głównych systemów broni, a obecnie sama stała się bronią lub obiektem ataku. Ponieważ w środowisku informacyjnym jest niewiele wyraźnych granic, to wojskowe ograniczenia związane z czasem, terenem i odległością, już w tym wieku zredukowane przez rozwój potęgi powietrznej, teraz ograniczone są praktycznie tylko prędkością światła[211]. Teoretycy uznają, iż: „Aby zwyciężyć, należy wygrać walkę informacyjną"[212], oraz że „W dobie powszechnej informatyzacji pokonanie przeciwnika w *infowar* może być czynnikiem decydującym o zwycięstwie w całej operacji wojennej"[213], a także „Walka informacyjna to działania podejmowane dla osiągnięcia przewagi informacyjnej"[214]. Również praktyka w treściach doktryn uznaje, iż: „Podobnie jak przewaga w powietrzu i przestrzeni kosmicznej umożliwia dowódcy swobodę ataku i bezpieczeństwo przed atakiem, tak przewaga informacyjna spełnia również podobną funkcję"[215], a „dominacja w informacyjnym spektrum jest równie ważna

---

[210] G. Nowacki, *Współczesne poglądy...* s. 30.

[211] AFDD 2-5: *Information Operations*, Washington 1998, s. 2.

[212] G. Nowacki, *Walka informacyjna...* s. 61.

[213] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo...* s. 82.

[214] Cyt. za: G. Ivefors, *Information Warfare. Defeat the Enemy Before Battle – A Warfare Revolution in the 21st Century?* http://www.ida.liu.se/~guniv/Infowar/ 26.01.2001 r.

[215] AFDD 2-5, wyd. cyt., s. 1.

w obecnym konflikcie, jak w przeszłości było zajmowanie terenu czy panowanie w powietrzu"[216].

W związku z tym obecnie coraz powszechniej walkę w sferze informacyjnej traktuje się jako najważniejszą formę kooperacji negatywnej, a rezultatem tej walki powinna być dominacja informacyjna. Jak walka o przewagę w powietrzu dzieli się na ofensywną i defensywną, tak i walka o przewagę informacyjną dzieli się na ofensywną i defensywną. **Siły zbrojne w ramach walki o przewagę informacyjną mogą więc prowadzić:**

- **ofensywną walkę informacyjną;**
- **defensywną walkę informacyjną (obronę informacyjną).**

Ofensywna walka o przewagę informacyjną

Tak samo jak w wypadku walki o dominację w powietrzu dąży się do uzyskania panowania w powietrzu, **tak dążeniem prowadzącego walkę o przewagę informacyjną winno być zredukowanie ofensywnego potencjału walki informacyjnej przeciwnika**, bo stanowi on wielkie zagrożenie nie tylko dla działań militarnych, czy nawet funkcjonowania całej sfery militarnej państwa, lecz także dla funkcjonowania innych sfer aktywności państwa. **Ofensywna walka informacyjna może prowadzić do paraliżu państwa lub przynosić niemożliwe do akceptowania koszty.**

Ofensywny potencjał walki informacyjnej przeciwnika jest chroniony systemem obrony informacyjnej, w rezultacie czego system ten stać się musi obiektem ofensywnego oddziaływania. Dlatego też **celem działań walki informacyjnej powinno być obezwładnienie systemu obrony informacyjnej i ofensywnego potencjału walki informacyjnej przeciwnika. Cel ten może być osiągnięty jedynie w wyniku ofensywnych działań walki informacyjnej**. Ponieważ walka jest kooperacją negatywną przynajmniej dwóch podmiotów, a ogólne prawidłowości walki dotyczą wszystkich stron walki, to i przeciwnik będzie dążył do podobnego celu. W rezultacie tego pełnowymiarowa walka informacyjna będzie miała charakter starcia jednorodnego typu, z jednoczesnym udziałem ofensywnych i defensywnych potencjałów informacyjnych przeciwstawnych stron. Ograniczony wymiar walki informacyjnej może zawierać jedynie jedną z form (defensywną lub ofensywną) tej walki. Rozmach walki informacyjnej będzie zaś charakteryzowany skalą zaangażowania poszczególnych stron.

Celem walki o przewagę informacyjną jest uzyskanie pożądanego stopnia dominacji informacyjnej. **Dominacja informacyjna to stopień panowania nad przeciwnikiem w sferze informacyjnej, który daje własnej organizacji zdolność do gromadzenia, kontroli, wykorzystania i obrony informacji bez efektywnego przeciwdziałania ze strony przeciwnika.**

Przedmiotem walki o przewagę informacyjną powinien stać się przede wszystkim ofensywny potencjał walki informacyjnej.

---

[216] Tamże.

Ofensywny potencjał walki o przewagę informacyjną

Do potencjału tego należą zasoby: ofensywnego ataku informatycznego odpowiedzialne za walkę w sferze przetwarzania danych cyfrowych; ofensywnych działań elektronicznych; ofensywnych działań powietrznych oraz częściowo lądowych i morskich; działań psychologicznych oraz dezinformacji.

Zasoby ofensywnego ataku informatycznego składają się z infrastruktury materialnej i intelektualnej. Infrastruktura materialna to przede wszystkim gotowe do użycia narzędzia ataku (złośliwe programy), komputery, sieci komunikacyjne oraz sprzęt i pomieszczenia umożliwiające zasilanie i funkcjonowanie. Infrastruktura intelektualna to specjaliści posiadający wiedzę o możliwościach prowadzenia ataku informatycznego, potrafiący przygotować narzędzia i metody takiego ataku oraz bazy wiedzy w tym zakresie.

Zasoby ofensywnych działań elektronicznych obejmują siły i środki, to jest ofensywną infrastrukturę ataku elektronicznego, potencjał produkcyjny tej infrastruktury oraz odpowiednio zorganizowane zespoły osobowe stosujące te środki. Ofensywna infrastruktura ataku elektronicznego to środki obezwładniania elektronicznego, które dzielą się na środki zakłócania i prowadzenia dywersji oraz środki destrukcji. Środki zakłócania i dywersji nie powodują fizycznego niszczenia atakowanych obiektów, a jedynie paraliż realizowanych przez nie funkcji lub obniżenie jakości ich pracy. Środki niszczenia obejmują grupę urządzeń emitujących silne impulsy promieniowania elektromagnetycznego w różnych zakresach widma, np. mikrofalowym, podczerwonym, widzialnym, nadfioletowym (lasery).

Zasoby ofensywnych działań ogniowych to przede wszystkim lotnictwo uderzeniowe rozumiane jako to, które jest zdolne do wykonywania uderzeń powietrznych. Do zasobów tych zaliczyć można także śmigłowce uderzeniowe i bezzałogowe roboty uderzeniowe (np. pociski manewrujące); również rakiety mogą stanowić powietrzny potencjał uderzeniowy.

Zasoby działań psychologicznych obejmują potencjał intelektualny specjalistów projektujących informacyjne treści przeznaczone do atakowania określonej grupy ludzi oraz infrastrukturę rozsiewczą. Infrastrukturę tę tworzą studia i nadajniki radiowe i telewizyjne, urządzenia elektroakustyczne oraz środki dystrybucji ulotek i materiałów drukowanych. Współcześnie gwałtownie wyłania się nowy kanał społecznej komunikacji, jakim jest Internet. Jako infrastruktura jest siecią komputerową, tzn. wielkim zbiorem komputerów połączonych odpowiednio zorganizowanymi sieciami łączności. Dostęp do bezpośredniego odbiorcy możliwy jest przez różne kanały łączności, np. telefoniczny, kabel telewizyjny, radiowy (telefon komórkowy) i przez różne urządzenia końcowe, takie jak komputer, telewizor, telefon komórkowy.

Zasoby dezinformacji mogą stanowić zarówno wyspecjalizowane siły i środki, jak też takie, dla których zadania te są dodatkowe. Do wyspecjalizowanych sił można zaliczyć wywiad i kontrwywiad, które wykonują inne zadania, jednakże mogą stanowić jedno z narzędzi prowadzenia dezinformacji.

Nawet tak zarysowany ofensywny potencjał walki informacyjnej obrazuje jego rozległość. Dla porównania: ofensywny potencjał walki o przewagę w powietrzu to głównie lotnictwo uderzeniowe i infrastruktura zabezpieczająca jego funkcjonowanie. Również ofensywny potencjał walki informacyjnej korzysta z zabezpieczającej go infrastruktury.

Formy działań ofensywnej walki o przewagę informacyjną

Najefektywniejszym sposobem walki z lotnictwem uderzeniowym przeciwnika jest zniszczenie jego samolotów na ziemi bądź zablokowanie ich na ziemi, z jednoczesnym paraliżem lotniska. W wypadku walki o przewagę informacyjną **zniszczenie ofensywnego potencjału tej walki jest niemalże niemożliwe, gdyż jest on zbyt różnorodny i rozległy**.

Jednak nie cały ten potencjał może być jednocześnie używany. Zależeć to będzie od stanu sytuacji polityczno-militarnej. Walka informacyjna nasilać się będzie w czasie wzrostu sprzeczności interesów między państwami i narastania sytuacji kryzysowej. Siły powietrzne mogą wykonywać wiele zadań w ramach tej walki. Zależeć to będzie od stopnia przygotowania tych sił do prowadzenia zarówno operacji informacyjnych, jak i walki informacyjnej.

Wobec rozległości ofensywnego potencjału walki informacyjnej, walka z nim musi być podjęta i prowadzona przez wszystkie komponenty państwa. Każdy odpowiednio do swoich możliwości. Wobec rozmachu tej walki przerasta to możliwości jakiegokolwiek pojedynczego komponentu państwa.

Siły zbrojne mogą jednakże być istotnym aktorem tej walki. Dysponują bowiem wykwalifikowanym potencjałem intelektualnym, związanym z eksploatowaniem zaawansowanego technologicznie sprzętu wymagającego wysokiej kultury technicznej. Potencjał ten może być zaadaptowany do potrzeb prowadzenia operacji informacyjnych.

W ramach ofensywnej walki o przewagę informacyjną mogą być stosowane wszystkie wcześniej zidentyfikowane (w podrozdziale 4.2.) **formy działań.**

Atak informatyczny może być stosowany w stopniu odpowiednim do rozwiniętych w siłach zbrojnych możliwości w tym zakresie. Do prowadzenia ataku informatycznego niezbędne jest posiadanie przede wszystkim wykwalifikowanych specjalistów informatyków, którzy potrafią zaprojektować i opracować odpowiednie do potrzeb kody komputerowe oraz infrastruktury niezbędnej do użycia tych kodów. Takie projektowanie wymaga wiedzy na temat organizacji i inżynierii podlegających atakowaniu systemów przeciwnika, a więc wymaga rozpoznania. Wiedza ta jest niezbędna nie tylko do zaprojektowania formy rażenia programu, ale także dla znalezienia sposobu dostarczenia atakującego programu do obiektu rażenia i dopasowania tego programu do tych potrzeb. Do wykonania ataku informatycznego w niektórych sytuacjach może być potrzebny sprzęt specjalistyczny. Dotyczyć to będzie sytuacji, w których stosuje się wyrafinowane metody przenikania, np. przez użycie specjalnych impulsów elektromagnetycznych lub przy zastosowaniu komunikacji radiowej. Jednakże wiele form ataku informatycznego może być

stosowanych przy wykorzystaniu klasycznych sieci komputerowych. Potrzebna jest jedynie stosunkowo niewielka grupa wysokiej klasy specjalistów informatyków oraz operatorów, mających wizję odpowiedniego wykorzystania tych informatyków.

Atak elektroniczny jest stosowaną powszechnie przez siły zbrojne formą prowadzenia działań. Jest on bowiem elementem walki elektronicznej, mającej długą historię stosowania. Atak ten służył przede wszystkim zabezpieczeniu własnych działań. Obecnie jednak może być używany na korzyść walki o przewagę informacyjną. Szczególnie efektywną formą tego ataku może być użycie środków trwałej destrukcji, takich jak bomby i pociski z ładunkiem bojowym w postaci generatorów impulsu elektromagnetycznego. Środki te umożliwiają wykonanie ataku elektromagnetycznego. Ta forma ataku może być skuteczna wobec szerokiej gamy obiektów ofensywnej walki informacyjnej przeciwnika. Zakłócanie, jako forma ataku elektronicznego, może być skuteczne jedynie w czasie trwania ataku i dlatego powinno być stosowane raczej do zabezpieczania działań, razem z innymi formami ataku informacyjnego. W ramach ataku elektronicznego stosowane są też destrukcyjne środki przeciwradiolokacyjne. Są to pociski naprowadzające się na źródło promieniowania radiolokacyjnego. Pociski takie mogą naprowadzać się też na inne emitujące promieniowanie elektromagnetyczne urządzenia. Amunicja tego typu może być skutecznym środkiem atakowania wielu elementów infrastruktury ofensywnej walki informacyjnej przeciwnika. Nowymi środkami destrukcyjnymi mającymi zastosowanie w ramach ataku elektronicznego, jest broń laserowa oraz nadajniki mikrofalowe dużej mocy.

Siły zbrojne doskonale nadają się do prowadzenia **ataku ogniowego**. Dysponują bowiem możliwościami przenikania w głąb terytorium przeciwnika i atakowania ważnych, z punktu widzenia walki o przewagę informacyjną, obiektów. Atak ten może być prowadzony za pomocą klasycznych form i sposobów działań zbrojnych. Atak ogniowy może być skutecznym sposobem eliminacji części ofensywnego potencjału walki informacyjnej przeciwnika. Jego zastosowanie jest jednak ograniczone do konfliktu zbrojnego. Powinien być stosowany przede wszystkim wobec obiektów o dużej wartości i znaczeniu w zasobach ofensywnej walki informacyjnej przeciwnika. Jest on użyteczny w sytuacjach oczekiwanego, długotrwałego wyłączenia atakowanego obiektu z walki.

W **działaniach psychologicznych** siły zbrojne uczestniczą od początku. Klasycznym zadaniem było rozrzucanie ulotek. Jednak działania psychologiczne są mniej skutecznym środkiem ataku ofensywnego potencjału walki informacyjnej przeciwnika. Może on być stosowany jako uzupełniająca forma ataku. Obecnie szczególnie przydatne może być prowadzenie działań psychologicznych przy wykorzystaniu Internetu. Jednakże obiektem ataku jest grupa personelu przeciwnika zaangażowana w walkę informacyjną, a więc bardziej świadoma od reszty społeczeństwa, przez co mniej podatna na psychologiczne ataki.

Dezinformacja powinna służyć przede wszystkim obniżeniu efektywności ofensywnych działań informacyjnych przeciwnika. Dezinformacja jest atakiem informacyjnym, gdyż wprowadza nieprzyjacielowi fałszywą informację, stymulując

jego reakcje w pożądanym kierunku. Siły zbrojne w ramach ofensywnej walki o przewagę informacyjną powinny stosować dezinformację, aby uniemożliwić przeciwnikowi rozpoznanie koncepcji działań, ich efektywności i zamiarów.

Defensywna walka o przewagę informacyjną

Nieodłączną formą ofensywnej walki o przewagę informacyjną jest forma defensywna, czyli **obrona informacyjna**. Obrona informacyjna odnosi się zarówno do ofensywnego potencjału walki informacyjnej, jak też do całej infrastruktury państwa. Obrona informacyjna służy neutralizowaniu ofensywnych możliwości walki informacyjnej przeciwnika.

Szerszym celem obrony[217] informacyjnej jest osiągnięcie stanu bezpieczeństwa państwa w jego informacyjnym obszarze. W ujęciu obrony informacyjnej jako części walki państwa, jej cel definiuje się jako niedopuszczenie elementów rozpoznania i ofensywnych elementów walki informacyjnej przeciwnika do osiągnięcia stawianych przed nimi celów, tym samym tworzenie dogodnych warunków stronie własnej do prowadzenia szeroko rozumianej walki w warunkach zagrożenia atakiem informacyjnym.

Działania obrony informacyjnej sił zbrojnych to te akcje, które chronią informacje i systemy informacyjne sił powietrznych oraz inne informacje i systemy informacyjne powierzone ochronie tych sił przed przeciwnikiem.

Informacyjna obrona sił zbrojnych koncentruje się na zapobieganiu rozpoznania i niedopuszczaniu do informacyjnego atakowania lub uzyskiwania pożądanej efektywności tego atakowania przez przeciwnika.

Siły zbrojne prowadzą informacyjną obronę, aby zapewnić możliwości przeprowadzania własnych działań. Ze względu na rosnące zależności sił zbrojnych od systemów informacyjnych, działania informacyjnej obrony są priorytetem sił zbrojnych, jeśli chodzi o walkę informacyjną. Jeśli działania informacyjnej obrony są połączone z atakiem informacyjnym, rezultatem będzie zwiększona możliwość zastosowania walki informacyjnej dla uzyskania pożądanych militarnych i politycznych celów.

(Formy, które mogą być stosowane w ramach obrony informacyjnej, zostały omówione w podrozdziale 4.3.)

Te rozmaite formy wspólnie się uzupełniają (tzn. każda z nich może być użyta jako przeciwśrodek w celu wsparcia innej) i mogą wspierać działania ofensywne. Dodatkowo, aby uzyskać lepsze efekty, formy te muszą być stosowane wielowarstwowo. Jeśli są używane bez koordynacji i integracji, mogą wywołać między nimi, jak również z działaniami ofensywnymi, konflikt. Na przykład przedsięwzięcia ochrony informacji mogą dążyć do zminimalizowania skutków włamania do systemu tak szybko, jak to możliwe, podczas gdy kontrwywiad może chcieć zezwolić na dalszy dostęp, aby zidentyfikować i wykorzystać przeciwnika.

---

[217] Zob. B. Zdrodowski, *Podstawy*... s. 41 oraz B. Zdrodowski, M. Marciniak, *Doktryna*... wyd. cyt.

6.3. Informacyjny atak strategiczny

6.3.1. Powietrzny atak strategiczny

Podłożem każdego konfliktu jest sprzeczność interesów. Gdy sprzeczność ta narasta, następuje eskalacja przemocy. Łagodniejsze formy tej przemocy zastępowane są radykalniejszymi. W zależności od potrzeb projektuje się instrumentarium oddziaływania na przeciwnika. Projekt takiego oddziaływania może zawierać zarówno instrumenty cywilne, jak i militarne. Według tradycyjnych poglądów, aktywne zastosowanie militarnego instrumentu polityki w formie walki zbrojnej w wystarczająco dużej skali tworzy wojnę. Jednakże, jak ustalono we wcześniejszych rozważaniach[218], „wojna" jest pojęciem względnym i niejednoznacznym. Wynika to zarówno ze względności oceny poszczególnych aktorów (jeden może traktować dany konflikt jako wojnę, inny zaś jako incydent zbrojny), jak też z coraz większych trudności z wyznaczeniem granicy tego, co nosi miano „zbrojny" (m.in. z powodu poszerzania się zakresu broni). Dla potrzeb niniejszych rozważań lepsze byłoby posługiwanie się kategorią „konfliktu", w którym zaistniała sprzeczność interesów, w związku z czym strony prowadzą kooperację negatywną (walkę) dla osiągnięcia celów, które zaspokoją ich własne interesy. W literaturze powszechnie przyjęło się jednak używanie pojęcia „wojna" w odniesieniu do odpowiednio ostrych form konfliktu. Klasycy badający zjawisko wojny wnieśli niewątpliwie dużo wiedzy o konflikcie, którego formą jest wojna. Dlatego warto sięgnąć do ich dorobku.

Wojna jest narzędziem polityki i jest prowadzona w celach politycznych[219]. Jeden naród (lub jego część) chce czegoś od drugiego, chce zmusić oponenta do przyjęcia swojej woli. Walka zbrojna może być użyta jako pierwszy, pośredni lub końcowy środek osiągania pożądanego efektu końcowego. **Jeżeli zapada decyzja o wojnie, to wówczas pojawia się problem sposobu jej prowadzenia. Istnieją dwa zasadnicze sposoby myślenia na ten temat.**

Jeden zakłada, że celem walki jest pokonanie wrogich sił zbrojnych i stąd wszystkie środki powinny być skierowane na ten cel. Ten sposób myślenia znajduje szerokie wsparcie w środowisku wojsk lądowych, które utwierdza się ponadto w przekonaniu, że o ostatecznym wyniku decyduje walka lądowa. W tym wypadku efektywność użycia sił powietrznych jest oceniana przez pryzmat ich wkładu w destrukcję wrogich sił zbrojnych oraz jakości wsparcia wojsk lądowych. Wówczas główny wysiłek lotniczy zawsze jest podporządkowany planom działań lądowych i ma charakter szeroko rozumianego wsparcia lotniczego.

Inny sposób myślenia, uznając prymat polityki nad wojną, zakłada, że to polityczne decyzje „produkują" efekt końcowy. Najlepszym wówczas sposobem osiągnięcia zakładanego efektu końcowego jest dokonanie skalkulowanego nacisku na kluczowe miejsca systemu państwa, tzw. środki ciężkości. Taka akcja przekona

---

[218] Zob. rozdział 1.

[219] R. Szpyra, *Współczesna wojna powietrzna. Wybrane problemy*, Warszawa 1998, s. 7.

przywództwo przeciwnika, że opór nie ma sensu, bo koszt oporu jest wyższy niż koszt akceptacji.

Socjoekonomiczny system, a szczególnie infrastruktura produkcyjna społeczeństw przemysłowych, wpływa na perspektywy strategii narodowej i strategii militarnej, które odbijają się w teorii potęgi powietrznej. Podobnie jak Clausewitz, teoretycy potęgi powietrznej podkreślają znaczenie relacji zachodzących między przywódcami wojskowymi i politycznymi oraz społeczeństwem. Dostrzegają oni i podkreślają możliwość wygrywania wojen przez przerwanie spójności tej triady za pomocą odpowiedniego zastosowania przemocy. W myśleniu zwolenników potęgi powietrznej ta przemoc powinna być skierowana zarówno na niszczenie możliwości, to jest infrastruktury produkcyjnej i sił zbrojnych, jak też na złamanie psychologicznej woli przeciwnika, a szczególnie zerwanie morale wojsk i dowódców, narodowych przywódców i całej populacji. Wola przeciwnika rozpoczęcia i kontynuowania wojny jest kluczem bliskiej założeniom potęgi powietrznej – teorii odstraszania.

Niszczenie narodowego systemu socjoekonomicznego w celu wpłynięcia na narodową wolę jest intensywnie eksponowane w teoriach, które identyfikowane są z bombardowaniami strategicznymi. Niektórzy zwolennicy tych bombardowań przekonani byli, że bezpośrednie ataki na ludność cywilną są najskuteczniejszym sposobem wpływania na narodową wolę społeczeństwa. Ta szkoła myślenia stała się symbolem teorii potęgi powietrznej i wywołała debatę nad rolą współczesnego lotnictwa bojowego. Wysiłek związany ze stosowaniem strategicznych bombardowań w czasie drugiej wojny światowej oraz horror broni jądrowej, czasami odciągają dyskusję od istoty teorii potęgi powietrznej i kierują ją w stronę wąskich interpretacji i zastosowań.

Krytycy teorii potęgi powietrznej są skłonni do stawiania znaku równości między strategicznymi bombardowaniami a nieograniczonymi atakami na ludność cywilną. Jakkolwiek miało to miejsce w niektórych poglądach, a miało także miejsce w niektórych operacjach drugiej wojny światowej, nie oznacza, że cała teoria potęgi powietrznej sprowadza się do strategicznych bombardowań ludności cywilnej. Również **termin „strategiczne" nie odnosi się do masowych bombardowań miast ani też do użycia broni jądrowej**. Niestety, takie odniesienia wprowadzają jedynie zamęt w dyskusji na temat strategicznego użycia potęgi powietrznej.

Strategiczne operacje militarne są związane z osiąganiem celów narodowych. Strategiczność nie jest tu definiowana przez rodzaj użytej broni lub systemu uzbrojenia, lecz odnosi się do koncepcyjnego podziału wojny na różne poziomy. ***Poziom strategiczny*** zmierza do osiągania narodowych celów polityki. ***Operacyjny poziom*** wojny, przez określanie celów teatru i organizowanie kampanii zmierzających do realizowania tych celów, prowadzi do osiągania celów strategicznych. ***Działania taktyczne*** są środkami i metodami walki – bitwami i starciami – które prowadzone są dla osiągania celów taktycznych, a pośrednio również operacyjnych i strategicznych. **Teoria potęgi powietrznej koncentruje się na strate-**

gicznym i operacyjnym poziomie wojny i użyciu potęgi powietrznej do bezpośredniego osiągania strategicznych celów wojny.

W kontekście rozpatrywanego zagadnienia, powszechnie uznany dorobek[220] prezentuje John Warden. Wzbogacił on teorię potęgi powietrznej. Jego dorobek jest szczególnie ciekawy i oryginalny w odniesieniu do roli potęgi powietrznej w prowadzeniu ataku strategicznego, dlatego zaprezentowane zostaną najistotniejsze elementy jego rozważań. Koncepcje te najlepiej nadają się[221] do zaadaptowania ich na grunt walki informacyjnej.

Aby wojna miała jakikolwiek sens[222], musi być prowadzona dla jakiegoś powodu. Może on czasami być mało istotny lub błahy, ale doświadczenia historyczne wskazują, że z pewnymi, mało istotnymi wyjątkami, większość władców, wypowiadając wojnę, czyniła to, by coś osiągnąć, np. dodatkowe terytoria, zahamowanie działań przeciwnika, zemstę na wrogach lub wymuszenie zmiany religii. Bardzo niewielu prowadziło wojny dla rozrywki.

Oczywiście nie można powiedzieć, że wszystkie wojny były prowadzone z jasnych i zrozumiałych powodów i dla osiągnięcia ściśle sprecyzowanych celów. W rzeczywistości określenie pożądanych rezultatów i możliwych do użycia środków zależało zarówno dla napastnika, jak i atakowanego od bardzo wielu różnych, niezależnych od siebie czynników. Główną zasadą było i jest: „Jeśli idziesz na wojnę – wiedz, dlaczego to robisz", a co za tym idzie – „zrozum, co chce osiągnąć przeciwnik i jaką cenę każdy z was chce (może) za to zapłacić". „Pamiętaj, że wojna nie polega na walce i zabijaniu, tylko na zdobyciu tego, czego przeciwnik nie chce oddać dobrowolnie". Mówiąc inaczej – wojna to powodowanie, aby przeciwnik zrobił to, co chcesz, aby zrobił, i uniemożliwienie mu wykonywania czynności, które zmusiłyby ciebie do działań niezgodnych z twoją wolą.

Jest wiele różnych sposobów zmuszania przeciwnika do działania zgodnego z naszymi oczekiwaniami. Do podstawowych można zaliczyć trzy następujące: uczynienie przeciwnikowi oporu zbyt kosztownym, przy czym koszty mogą mieć charakter polityczny, militarny lub ekonomiczny; fizyczne uniemożliwienie przeciwnikowi podjęcia jakichś działań przez jego strategiczne lub operacyjne sparaliżowanie; całkowite zniszczenie przeciwnika.

Ostatnia z tych możliwości była rzadko spotykana w historii – z jednej strony z powodu trudności wykonania, a z drugiej z powodu moralnych oporów i w związku z tym można ją w zasadzie pominąć, koncentrując się na dwóch pierwszych.

Kiedy mówimy o uczynieniu oporu przeciwnika na tyle kosztownym dla niego, że decyduje się on przystać na nasze warunki, musimy uwzględnić, że będzie to bardzo trudne do zdefiniowania i przewidzenia. Ponadto organizacje humanitarne

---

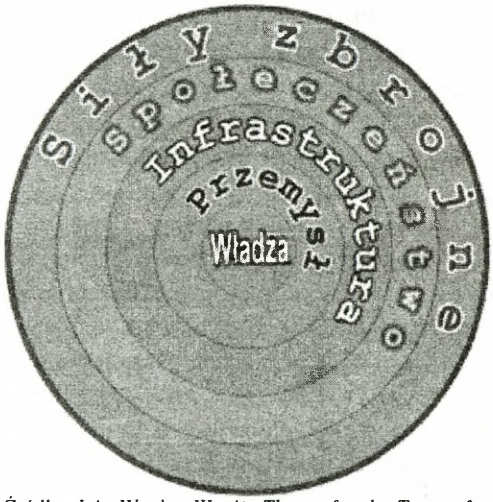
[220] Uznanie to wyraża się wieloma międzynarodowymi opiniami, cytowaniami i adaptacjami oryginalnych pomysłów.

[221] Przydatność różnych teorii oceniano na podstawie charakterystyki walki informacyjnej i działań informacyjnych.

[222] Poglądy te zostały zaprezentowane w J.A. Warden III, *Air Theory for the Twenty-first Century*, [w:] *Battlefield of the Future*... s. 103–124 oraz w R. Szpyra, *Rola sił powietrznych w wojnie przyszłości*, Warszawa 2000, s. 104–124.

mogą poprzez swoje działania uniemożliwić nam osiągnięcie celu. Trudności w ocenie i przewidywaniu nie oznaczają jednak, że sposób ten jest niemożliwy do zrealizowania – jest jedynie nieprecyzyjny.

Z punktu widzenia potęgi powietrznej, naszym zadaniem jest określenie ceny (negatywnej lub pozytywnej), jaką trzeba będzie narzucić przeciwnikowi, aby go nakłonić do przyjęcia naszych warunków. Aby to uczynić, musimy jednak wiedzieć, jak zorganizowani są nasi przeciwnicy. Ktoś mógłby powiedzieć, że zrozumienie tego, jak zorganizowani są nasi przeciwnicy, jest zadaniem niewykonalnym, szczególnie w sytuacji, gdy nie wiemy, kto nimi będzie. Na szczęście nie jest to właściwe podejście, każdy bowiem system żywego organizmu zorganizowany jest w podobny sposób; jedynie szczegóły mogą się różnić. Dla lepszego zobrazowania warto przedstawić model tych systemów w postaci pięciu pierścieni (rys. 41).



Źródło: J.A. Warden III, *Air Theory for the Twenty-first Century*, [w:] *Battlefield of the Future. 21st Century Warfare Issues*, Maxwell AFB 1995, s. 108.

Rys. 41. Model państwa według Wardena

Model ten zawiera pięć współśrodkowych kół. Środkowe, centralne koło reprezentuje narodowe przywództwo kierujące państwem, będące najbardziej krytycznym elementem decydującym o politycznych rezultatach wojny. Jest ono otoczone, wspierane i ochraniane przez inne koła czy raczej pierścienie. Drugie koło obrazuje produkcję, a więc fabryki, elektrownie, rafinerie i inne obiekty wytwarzające najważniejsze dla prowadzenia wojny produkty. Kolejne koło to narodowa infrastruktura w postaci sieci dróg, kolei, a także energetycznych sieci przesyłowych i innych. Czwarte koło to populacja kraju. Piąte reprezentuje narodowe siły zbrojne rozmieszczone w polu.

Celem wojny jest zmuszenie przywództwa przeciwnika, by czyniło to, czego chcemy. Należy mu uświadomić przewidywany skutek mających nastąpić działań,

a także poinformować go o rozmiarach jego strat oraz prawdopodobnych długo- i krótkoterminowych skutkach wynikających z tych działań.

Nie mając możliwości spowodowania nieakceptowalnych dla przeciwnika kosztów, należy być gotowym do narzucenia strategicznego paraliżu. Idea paraliżu jest dość prosta. Jeżeli przeciwnik jest postrzegany jako system, to należy zidentyfikować te części tego systemu, które możemy zdegradować. Zidentyfikowany element musi mieć zasadnicze znaczenie dla wykonywania niepożądanego działania wrogiego systemu, co zapobiegnie temu działaniu. Najlepszym miejscem oddziaływania jest centrum: jeśli potrafimy uniemożliwić systemowi kierowania gromadzenie, obróbkę i wykorzystanie informacji, nie pozwolimy mu działać, osiągniemy paraliż na poziomie strategicznym.

Miejscem oczywistym wywołania paraliżu systemu strategicznego jest poziom kierownictwa lub mózgu. Co się jednak stanie, jeśli mózg nie może być zlokalizowany lub zaatakowany? Mimo że funkcje kierownicze zawsze dostarczają wielu dogodnych miejsc do paraliżu, nie jest to jedyna możliwość.

Warto zastanowić się nad sposobem uzyskania tych efektów. Przedtem należy zauważyć, że prawie nie było mowy o teorii powietrznej, a tym bardziej o szczegółach zastosowania bojowego. Powód jest prosty: **zanim się zacznie myśleć o tym, jak działać, należy sobie dobrze uświadomić, co się chce od przeciwnika. Podejmowanie tej decyzji jest największym wyzwaniem intelektualnym**; gdy zdecydowaliśmy o tym, co chcemy osiągnąć, określenie tego, jak mamy to osiągnąć, jest dużo łatwiejsze, bo ćwiczone jest w codziennej praktyce. Spróbujmy szybko poszukać odpowiedzi na pytanie: jak?

Wojna równoległa poddaje tak wiele systemów przeciwnika pod równoczesny atak, że systemy te nie mogą na te ataki reagować prawidłowo, bronić się lub odnawiać. Jest to podobnie jak ze śmiercią od tysiąca, pojedynczo niegroźnych, cięć. Sto spowolni system, a tysiąc będzie miało fatalny skutek, ponieważ system nie może wytrzymać tak wielu ataków, w tak krótkim czasie. Najlepszym przykładem wojny równoległej jest atak strategiczny na Irak. W ciągu paru minut koalicja zaatakowała przeciwnika w ponad stu kluczowych miejscach. Celami były obiekty w całym Iraku na głębokości strategicznej. Wszystkie ważne funkcje państwa irackiego zostały na długo zatrzymane. Serwis telefoniczny upadł, zabrakło oświetlenia, ośrodki dowodzenia przestały kontrolować obronę powietrzną, podległe im jednostki, kluczowe ośrodki przywództwa były niszczone. Patrząc z perspektywy na problem Iraku, koalicja uderzyła na trzykrotnie więcej celów w tym kraju w pierwszych 24 godzinach, niż siły 8. Armii Powietrznej na Niemcy w czasie całego 1943 r.

Ofensywa bombowa przeciwko Niemcom (aż do samego końca) była operacją seryjną (liniową), jak faktycznie wszystkie wojskowe działania od zarania dziejów. Wszystko to znaczyło, że wojna była sprawą akcji i reakcji, dochodzenia do punktu kulminacyjnego, przegrupowania i zmiany. Istotnie, wojna była wysiłkiem z jednej strony do przełamania się przez linie obrony z atakami seryjnymi, z drugiej zaś próbą przeszkodzenia takim atakom.

W Iraku, w kraju, o podobnym obszarze jak przedwojenne Niemcy, z taką samą ilością kluczowych urządzeń, zniszczeń dokonano tak szybko, że nie było możliwe odtworzenie ich zdolności, gdyż wymagały znacznych napraw. Atak równoległy na Irak był skierowany przeciwko prawdopodobnie najlepiej przygotowanemu do obrony krajowi na świecie. Jeżeli zadziałało to w tym wypadku, prawdopodobnie zadziała wszędzie. Cele niszczone przez ten atak muszą być szczególnie ostrożnie wyselekcjonowane dla osiągnięcia zamierzonego efektu.

Rekapitulując, **zniszczenie sił zbrojnych przeciwnika nie jest istotą wojny; istotą jest przekonanie przeciwnika do zaakceptowania naszej woli, a zwalczanie jego sił zbrojnych jest co najwyżej środkiem jej zakończenia, a w najgorszym wypadku całkowitym zmarnowaniem czasu i energii.**

W działaniu zrozum polityczne i techniczne uwarunkowania; zidentyfikuj cele polityczne; określ, jak chcesz skłonić przeciwnika do tego, by wykonał twoją wolę (narzuć koszt, paraliż lub zniszczenie); używaj pięciopierścieniowego systemu analizy, by otrzymać wystarczającą informację o przeciwniku i aby zidentyfikować stosowne środki ciężkości; atakuj właściwe obiekty uderzeń jednocześnie i tak szybko, jak tylko można.

Kraje są, jak gdyby odwróconymi piramidami, które spoczywają delikatnie na swoich strategicznych podstawach, czyli – przywództwie, komunikacji, najważniejszych sektorach produkcji, infrastrukturze i populacji. Jeżeli kraj jest sparaliżowany strategicznie, to jest pokonany i nie będzie w stanie utrzymać swoich sił, chociaż te pozostaną niemalże nietknięte.

Kiedy kraj traci swoją zdolność do obrony siebie przed atakiem powietrznym, jest na łasce wroga i tylko litość i wyczerpanie przeciwnika może go ocalić. Kiedy państwo będzie tracić strategiczną przewagę powietrzną i nie ma żadnej rozsądnej nadziei na jej szybkie odzyskanie, to powinno tak szybko dążyć do pokojowego rozstrzygnięcia, jak tylko to możliwe. Z ofensywnego punktu widzenia osiągnięcie strategicznej przewagi powietrznej jest najważniejsze dla dowódcy; jeśli ten warunek jest spełniony, reszta jest tylko kwestią czasu.

Strategiczne organizacje, włączając kraje, mają małą liczbę żywotnych obiektów na poziomie strategicznym. Te cele zwykle są małe, bardzo kosztowne, bez obiektów zapasowych i trudne do naprawienia. Jeśli duża liczba z nich jest zniszczona jednocześnie w ataku równoległym, to szkody te stają się nienaprawialne. W przeciwieństwie do tego w ataku seryjnym, gdzie tylko jeden lub dwa cele są atakowane w danym czasie, nieprzyjaciel może złagodzić jego skutki przez: czasowe rozproszenie, powiększenie liczby bronionych celów, które będą prawdopodobnie atakowane, koncentrowanie swojej obrony na obiektach, które mogą być atakowane, i wysiłku na odtworzeniu zdolności obiektu, a także prowadzenie kontrofensywy. Równoległy atak pozbawia go zdolności do skutecznej odpowiedzi; im większy jest procent celów niszczonych w jednym uderzeniu, tym mniej prawdopodobna jest odpowiedź.

Broń precyzyjna pozwala na ekonomiczne niszczenie faktycznie wszystkich, szczególnie strategicznych i operacyjnych celów, którym ciężko się poruszać i ukryć.

Broń ta zmienia naturę wojny w odniesieniu do oczekiwanego rezultatu z prawdopodobnie do pewnie wygranej. Wojny przez tysiąclecia były zjawiskami, w których każda ze stron wysyłała ogromną liczbę pocisków w nadziei, że to skłoni ich przeciwnika do odwrotu lub poddania się. Rezultat był nie do przewidzenia, pełen niespodzianek i rządził nim przypadek. Dzięki broni precyzyjnej nawet logistyka stała się prostsza. Na przykład zniszczenie Iraku na poziomie strategicznym, operacyjnym i taktycznym wymagało zniszczenia dwunastu tysięcy celów. Dlatego nie jest dłużej potrzebne gromadzenie bliżej nieokreślonej liczby amunicji, gdyż mała liczba broni precyzyjnej może wystarczyć do zniszczenia czegoś ważnego.

Siły lądowe na szczeblu operacyjnym są niezwykle wrażliwe. Wspieranie znacznej liczby środków znajdujących się na ziemi jest problemem administracyjnym nawet w czasie pokoju. Sukces zależy od efektywnej dystrybucji informacji, paliwa, jedzenia i amunicji. Wydajna dystrybucja zależy od odwróconej piramidy. Najpierw muszą być zgromadzone zapasy dla całości w jednej lub dwóch bazach operacyjnych, następnie zapasy te rozdzielane są na kolejne dwie lub cztery lokalizacje i tak dalej, aż dotrą do użytkownika. Węzły tego systemu są szczególnie wrażliwe na atak precyzyjny. Logistyka i administracja dominują w walce lądowej, a nie są łatwe do obrony. W przeszłości działalność tego typu miała miejsce na tyle głęboko, że była względnie bezpieczna. Jednak obecnie sytuacja całkowicie się zmieniła, co stawia pod znakiem zapytania użyteczność takich form walki, które wymagają rozległej logistycznej i administracyjnej rozbudowy.

Państwa podporządkowują się woli swoich nieprzyjaciół, gdy kara za niepodporządkowanie się przekracza koszty podporządkowania się. Koszt może być nałożony na kraj przez sparaliżowanie lub zniszczenie jego strategicznej, lub operacyjnej bazy, lub przez okupację wrogiego terytorium. W przeszłości okupacja była dokonywana przez siły lądowe – bo nie było odpowiednio dobrego substytutu. Obecnie koncepcja „okupacji powietrznej" jest rzeczywistością i w wielu wypadkach będzie wystarczająca. Irakijczycy podporządkowali się żądaniom ONZ w takim samym, a może nawet większym stopniu niż Francuzi Niemcom, gdy byli okupowani przez miliony okupantów. Jednakże okupacja lądowa jest niezbędna, gdy istnieje zamiar np. skolonizowania nieprzyjacielskiego terytorium.

Dominacja potęgi powietrznej. Potęga powietrzna (stałopłaty, śmigłowce, pociski samosterujące, satelity), jeżeli niepowstrzymana, zniszczy strategiczne i operacyjne obiekty, które są praktycznie bardzo wrażliwe i trudne do uodpornienia na uderzenia. Potęga powietrzna, jeśli zaistnieje taka potrzeba, może również zniszczyć większość celów taktycznych.

Ważność informacji na strategicznym i operacyjnym poziomie. W wojnie z Irakiem koalicja zdegradowała niemalże całkowicie jego zdolności do zdobywania i wykorzystania informacji. Jednocześnie koalicja była w stanie na dobrym poziomie zarządzać informacją w swoim własnym systemie, mimo że ten zorganizowany był tak, jak za czasów Fryderyka Wielkiego. Wnioski ze sfery wykorzystania informacji, wyciągnięte z wojny z Irakiem, były negatywne; koalicja pomyślnie zdegradowała irackie możliwości zdobywania i przetwarzania informacji, ale nie

udało jej się wypełnić tej luki przez zapewnienie Irakijczykom alternatywnego źródła informacji. To niepowodzenie umożliwiło Saddamowi jego przetrwanie. **Przechwycenie i wykorzystanie infosfery może być najważniejszym wysiłkiem w wielu przyszłych wojnach.**

Szczególną konceptualizacją przekonania o decydującym znaczeniu potęgi powietrznej[223] dla losów wojny jest idea precyzyjnych bombardowań. Przy tym nie odnosi się ona do taktycznej zdolności umieszczenia bomby lub pocisku bezpośrednio w wyznaczonym celu lub obok niego. Jednakże dokładne umieszczenie broni w obiekcie ataku, dostarcza zdolności co do wdrożenia szerszej koncepcji precyzyjnych bombardowań. Koncepcje bombardowań występują w różnych formach, jednakże najlepiej są znane jako produkt Taktycznej Szkoły Korpusu Powietrznego Stanów Zjednoczonych z lat 30. XX w.

Istota precyzyjnych bombardowań zawiera się w idei, że systematyczna analiza politycznych, militarnych i socjoekonomicznych struktur nieprzyjaciela wskaże żywotne punkty, na których powinny się skupić ataki powietrzne. Precyzyjne bombardowania to próba poszukiwania efektywnych i sprawnych działań bojowych, które będą miały istotny wpływ na możliwości i wolę przeciwnika. Skuteczne ataki na żywotne węzły mogą prowadzić do zapaści całego systemu celów, a skumulowany rezultat takich ataków może prowadzić do zwycięstwa. Cele lub grupy celów, które mogą mieć decydujące znaczenie, zostały nazwane środkami ciężkości.

Jakkolwiek precyzyjne bombardowanie jest nakierowane na działania strategiczne, koncepcja wygrania wojny za pomocą potęgi powietrznej zakłada użycie tej potęgi na wszystkich poziomach konfliktu. Precyzyjne ataki mogą dostarczyć również decydujących rezultatów na taktycznym i operacyjnym poziomie, a te możliwości podkreślają ważność elastyczności, co zapewnia maksimum korzyści przy wykorzystaniu ograniczonych środków lotniczych.

Sukcesy na taktycznym i operacyjnym poziomie wojny mogą płynąć z właściwego użycia potęgi powietrznej. Szczególnie ważna jest logiczna selekcja właściwych celów. Analiza przeciwnika powinna uwypuklić i zidentyfikować środki ciężkości i na nich powinien się skoncentrować proces planowania. Środki ciężkości winny stać się celami uderzeń powietrznych. Rozległe zniszczenia nie są przy tym koniecznym celem precyzyjnych ataków, nawet w czasie taktycznych lub operacyjnych działań nakierowanych przeciwko siłom zbrojnym przeciwnika. Raczej **uderzenia powietrzne powinny być specjalnie projektowane na szybkie zdezorganizowanie systemów i uniemożliwienie przeciwnikowi kontynuowania operacji bojowych.** Decydujące kampanie precyzyjnych bombardowań spoczywają na podwalinach zrozumienia możliwości zasobów lotniczych, dopracowanej struktury sił, zastosowaniu najważniejszych operacyjnych zasad i na wykorzystaniu możliwie najlepszego rozpoznania.

W konkluzji należy uznać, iż: **strategiczny atak powietrzny to działania bezpośrednio zmierzające do osiągnięcia efektów strategicznych przez ude-**

[223] Zob.: J.V. Martin, *Victory from Above. Air Power Theory and the Conduct of Operations Desert Shield and Desert Storm*, Maxwell AFB 1994, s. 6; R. Szpyra, *Współczesna wojna...* s. 26–28.

rzanie na środki ciężkości nieprzyjaciela. Działania te są projektowane tak, aby osiągnąć ich cele bez konieczności angażowania innych rodzajów sił zbrojnych i prowadzenia rozległych operacji połączonych. Ta funkcja może być realizowana celem wsparcia dowódcy teatru lub jako samodzielna operacja kierowana przez naczelne dowództwo narodowe. **Strategiczny atak powietrzny powinien przynieść efekty daleko wykraczające poza skalę włożonego wysiłku w jego wykonanie**. Jeśli jest właściwie zastosowany, jest najefektywniejszym sposobem zastosowania potęgi powietrznej. Umożliwia też dowódcy teatru wykorzystanie decydujących efektów przeciwko przeciwnikowi, przy jednoczesnym unikaniu strat ludzkich i materialnych.

6.3.2. Informacyjny atak strategiczny

Współczesne uzależnienie państw od informacyjnej infrastruktury jest powszechne i stale rosnące. Infrastruktura ta jest wrażliwa na atak. To tworzy zagrożenie dla narodowego bezpieczeństwa. Jeśli jednak weźmiemy pod uwagę związki między systemami informacyjnymi a tradycyjnie ważnymi elementami infrastruktury państwa, to się okaże, że zagrożenie walką informacyjną i jej możliwości są jeszcze większe. Z ekonomicznych powodów, takich jak zwiększająca się rywalizacja i konkurencja oraz deregulacja, zwiększają zależność od systemów informacyjnych. Zależność ta wynika z konieczności posługiwania się systemami informacyjnymi dla zapewnienia sprawnego działania, utrzymywania i monitorowania elementów infrastruktury. Ta rosnąca zależność od systemów informacyjnych pogłębia coraz bardziej wrażliwość do stanu niespotykanego wcześniej.

Możliwości stosowania walki informacyjnej[224] rozciągają się od zakłócenia funkcjonowania większych państw przez małe organizacje lub państwa do poważnego sparaliżowania przez nie wielkich państw. Wiele państw lub organizacji znajdują się w przededniu uzyskania zdolności do prowadzenia strategicznej walki informacyjnej, to jest takiej, która może poważnie zagrozić interesom bezpieczeństwa, przy czym strategiczna walka informacyjna może być prowadzona bez deklarowania stanu wojny. Walka ta może być prowadzona przez ludzi nienoszących mundurów i pozostających w swoich domach.

Można uniemożliwić realizację planów działań militarnych w sytuacjach kryzysowych. By to zrealizować, przeciwnik może zaatakować infrastrukturę kraju, jego zagraniczne bazy oraz infrastrukturę państw sojuszników. Kluczowi sojusznicy lub koalicjanci w obliczu takiego ataku mogą odmówić przyłączenia się do koalicji lub – co gorsza – opuścić koalicję w czasie wojny.

Również gospodarka jest zależna od infrastruktury informacyjnej. Wszystko, co celowo zdegraduje możliwości tej infrastruktury, może być uznane za atak. Atak taki może być skierowany na wiele systemów, jak: finansowo-bankowy,

[224] Zob.: R. Szafranski, *Mars Chuckles and Athena in Frustration*, [w:] *Information Operations*, NL ARMS... s. 37; R. Szpyra, *Działania informacyjne i walka informacyjna we współczesnych i przyszłych zastosowaniach sił powietrznych*, „Przegląd Wojsk Lotniczych i Obrony Powietrznej" 2000, nr 9, s. 6.

energetyczny, telekomunikacyjny, hydrologiczny, ratunkowy. Walka informacyjna oferuje nowy rodzaj projekcji siły. Jedną z jej form może być izolacja, która w XXI w. może przybierać różne formy, takie jak zapobieżenie zmasowaniu, funkcjonowaniu na rynku czy poznaniu prawdy. Te nowe, bardziej subtelne środki i sposoby walki nakierowane są na przekonania i wiedzę przeciwnika i wykorzystują jego słabości.

Informacyjni wojownicy mogą prowadzić walkę na wiele sposobów, m.in. mogą blokować systemy komputerowe lub uniemożliwiać ich uruchomienie, zrywać połączenia lub zakłócać systemy łączności, wprowadzać nieznane wirusy komputerowe i inne formy szkodliwych programów, również w sposób zamaskowany, pod szyldem innych produktów, zakłócać sieci radiowe różnego przeznaczenia, wywoływać fałszywe alarmy, zakłócać pracę systemów kierowania energetyką, rozpowszechniać fałszywe informacje, np. o pojawieniu się wirusa *Ebola* lub innych zabójczych mikroorganizmów w wodzie, śmieciach, czy żywności. Mogą też stosować wiele innych tego typu działań, doprowadzając nawet do paraliżu kraju.

Również tzw. miękka wojna[225] (*soft war*) mieści się w zakresie walki informacyjnej, lecz w skali globalnej. Jej celem jest nie tyle osiągnięcie przewagi informacyjnej, co manipulowanie przeciwnikiem (lub własnym społeczeństwem) za pomocą fałszywej lub zmanipulowanej informacji. Zwykle narzędziem tej walki jest telewizja. Używana jest do kształtowania woli innych narodów, co zmienia ich sposób postrzegania rzeczywistości.

Zgodnie z przyjętą wcześniej definicją **walka informacyjna to m.in. zorganizowana w formę przemocy aktywność zewnętrzna państwa** [...] **skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji** [...].

Działania prowadzone w ramach walki informacyjnej mogą prowadzić do osiągania celów taktycznych, operacyjnych lub strategicznych. **Jeżeli aktywność ta umożliwi bezpośrednie osiągnięcie strategicznych celów politycznych, to taką formę walki informacyjnej uznać możemy za informacyjny atak strategiczny**. Ponieważ obiektem takiego ataku jest całe państwo, to przez analogię do teorii powietrznego ataku strategicznego użyteczne będzie zastosowanie zaproponowanego przez Wardena modelu analizy systemowej państwa.

Do przyjęcia takiej analogii upoważniają, oprócz własnych wniosków, również informacje o rezultatach przeprowadzonych badań[226]. Daniel Kuehl, analizując je, stwierdził m.in.: „Dużo konceptualnego myślenia o strategicznym zastosowaniu

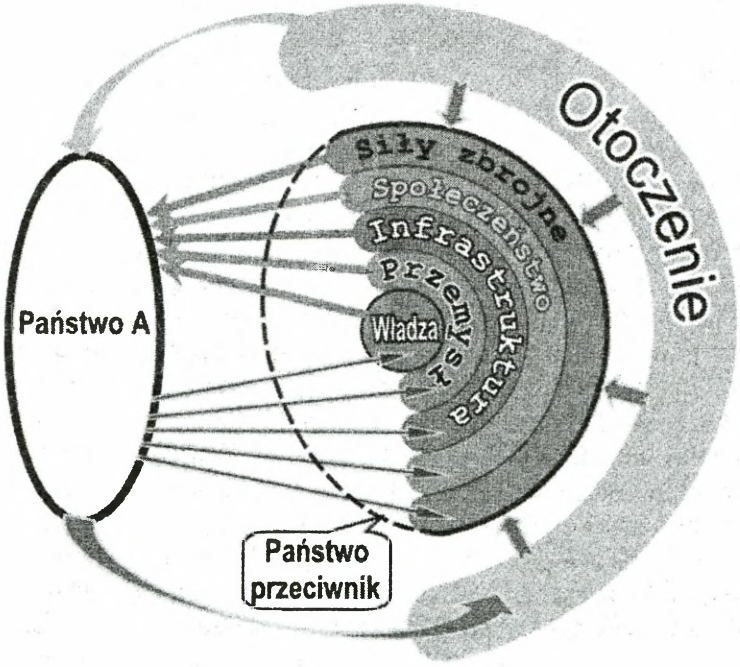
---

[225] Zob. http://www.seas.gwu.edu/~reto/infowar/view.htm 26.01.2001 r.

[226] Przykładem takich prac są: J.B. Barlow, *Strategie Paralysis: An Airpower Theory for the Present*, Maxwell AFB 1994, szczególnie rozdział 5: „The National Elements of Yalue Model", s. 55–78; G.R. Gurst, *Taking Down Telecommunications*, Maxwell AFB 1994, szczególnie rozdział 2: „Telecommunications", s. 5–28; S.M. Rinaldi, *Beyond the Industrial Web: Economic Synergies and Targeting Methodologies*, Maxwell AFB 1995, szczególnie rozdział 3: „Synergies and Infrastructure Elements", s. 25–34; H.D. Arnold, J. Hukill, J. Kennedy, A. Cameron, *Targeting Financial Systems as Centers of Gravity: „Low Intensity" to „No Intensity" Conflict*, „Defense Analysis" 1994, vol. 10, no. 2, s. 181–208.

potęgi powietrznej przeciwko żywotnym narodowym środkom ciężkości zostało przeprowadzone w Uniwersytecie Powietrznym [USA – R.S.] od czasu wojny w Zatoce Perskiej. Większość tego dorobku może być bezpośrednio zastosowana w postulowanej strategicznej walce informacyjnej przeciwko tym samym środkom ciężkości"[227]. Kuehl przytacza także argumenty na rzecz potrzeby prowadzenia strategicznej walki informacyjnej, pisząc: „Potrzeba prowadzenia walki informacyjnej na poziomie strategicznym jest oczywista również dla innych krajów. Chińczycy np. uznali, że głównym celem walki informacyjnej jest osłabienie przeciwnika jego zdolności dowodzenia [...], które zawiera także kierowanie państwem. Rosyjskie publikacje również postulują dezorganizację wszystkich ważnych systemów państwa, jak cywilny i militarny, system kierowania, systemy komunikacji, energetyczne, transportowe"[228].

Do modelu Wardena dodane zostało otoczenie państwa, które jest też uczestnikiem operacji informacyjnych. Można np. przez nie pośrednio oddziaływać na przeciwnika (rys. 42).



Opracowanie własne.

Rys. 42. Model strategicznego ataku informacysjnego

[227] D.T. Kuehl, *Strategic Information Warfare and Comprehensive Situational Awareness*, [w:] A.D. Campen, D.H. Dearth, R.T. Goodden, *Cyberwar: Security, Strategy, and Conflict in the Information Age*, Fairfax 1996, s. 189.

[228] Tamże, s. 189.

Przedmiot informacyjnego ataku strategicznego

Przedmiotem informacyjnego ataku strategicznego są zasoby państwa przeciwnika. Zasoby te, przedstawione w postaci modelu Wardena, zawierają: kierownictwo państwa wraz z systemem kierowania nim; przemysł będący źródłem dochodów państwa; infrastrukturę obejmującą takie elementy, jak: sieć energetyczna, komunikacyjna, gazowa, kolejowa, drogowa; społeczeństwo i siły zbrojne. Zgodnie z sugestiami Wardena informacyjny atak strategiczny powinien prowadzić albo do narzucenia nieakceptowalnych dla państwa kosztów, albo do paraliżu tego państwa.

Jeśli chodzi o **koszty,** to **tworzone mogą** one **być zarówno we wszystkich komponentach państwa, jak też w części z nich.** Praktyczne podejście zależeć będzie od dostępności poszczególnych elementów państwa do wykonania nań informacyjnego ataku oraz od własnych możliwości przeprowadzenia takiego ataku. **Przy planowaniu kosztów należy dążyć do tego, aby miały one jak największe znaczenie dla rządu oraz społeczeństwa. W istocie, chodzi bowiem o zmianę stanu świadomości rządu i społeczeństwa przeciwnika na taki, który zabezpiecza własne interesy i osiągnięcie pożądanych celów politycznych.**

W wypadku dążenia do narzucenia przeciwnikowi **paraliżu,** należy dokonać analizy poszczególnych elementów państwa i zidentyfikować miejsca krytyczne, tzw. środki ciężkości[229], zarówno całego państwa, jak i każdego z jego elementów. Zidentyfikowanie tych miejsc pozwala uniknąć rozpraszania wysiłku oraz umożliwia zwiększanie efektywności podejmowanych działań. W podejściu tym chodzi o znalezienie takich miejsc, które są niezbędne dla funkcjonowania danego organizmu (wyeliminowanie ich powoduje zatrzymanie funkcji organizmu) lub bardzo ważne dla tego organizmu (wyeliminowanie ich spowoduje radykalne ograniczenie funkcji organizmu). Dobrą ilustracją pierwszego przypadku może tu być mityczna pięta Achillesa, a także serce dla człowieka, energia elektryczna dla przemysłu, łączność dla państwa. W drugim przypadku ucięcie człowiekowi nóg i rąk może nieoznaczać końca istnienia, lecz istnienie to będzie wiązało się z bardzo ograniczonym funkcjonowaniem. Podobnie zniszczenie kilku mostów może niesparaliżować całkowicie ruchu, jednakże radykalnie go ograniczy.

Do właściwej identyfikacji środków ciężkości niezbędna jest głęboka wiedza specjalistyczna z danej dziedziny oraz odpowiednia do potrzeb informacja rozpoznawcza. Skuteczność własnych działań jest m.in. funkcją poprawności zidentyfikowania środków ciężkości. Identyfikację tę należy następnie zestawić z własnymi możliwościami i warunkami. Może się bowiem okazać, że co prawda istnieją miejsca krytyczne, których wyeliminowanie sparaliżuje przeciwnika, jednakże są one albo niedostępne, albo mimo dostępności nie dysponujemy zdolnościami do ich

[229] Nazwa ta pochodzi z tłumaczenia z angielskiego wyrażenia „center of gravity". Niektórzy autorzy, jak np. Tadeusz Kardaś, proponują nazywać je „punktami ciężkości" (zob. T. Kardaś, *Punkt ciężkości*, „Myśl Wojskowa" 2000, nr 2, s. 35–48). Jednakże w nazwie „środek" kryje się dodatkowa informacja, że nie chodzi tu o jakiś „punkt ciężkości", lecz o ten, który jest „środkiem ciężkości". W związku z tym przyjęto, że wyrażenie „środek ciężkości" lepiej oddaje istotę tego pojęcia, dlatego będzie używany w niniejszej pracy.

zaatakowania. Gdy istnieje taka sytuacja, należy zastosować podejście pośrednie, zidentyfikować dostępne do zaatakowania obiekty, ważne dla egzystencji środka ciężkości. Główny wysiłek powinien być skupiony na atakowaniu zidentyfikowanych środków ciężkości. **Ważnym postulatem, zgodnym z zaleceniami Wardena, jest dążenie do jednoczesnego atakowania wszystkich lub zdecydowanej większości środków ciężkości, czyli prowadzenie ataku równoległego.**

Formy informacyjnego ataku strategicznego

Informacyjny atak strategiczny będzie prowadzony przez państwo i kierowany przez najwyższe władze państwowe. Siły powietrzne mogą uczestniczyć w wykonywaniu takiego ataku. Atak taki może być prowadzony we wszystkich obszarach walki informacyjnej lub w części z nich, np. dyplomatycznej, ekonomicznej czy militarnej. W zależności od celu politycznego może mieć większy lub mniejszy rozmach, a także być bardziej lub mniej kosztowny dla przeciwnika. Gdy celem działań tego ataku jest paraliż, to rozmach ataku informacyjnego zależeć będzie od zakresu tego paraliżu, tzn. czy dotyczyć ma całego państwa, czy też jakiegoś elementu tego państwa.

W ramach informacyjnego ataku strategicznego, podobnie jak w wypadku ofensywnej walki o przewagę informacyjną, mogą być stosowane wszystkie zidentyfikowane (zob. podrozdział 4.2.) formy działań.

Atak informatyczny może być w niektórych okresach główną formą walki informacyjnego ataku strategicznego. Dotyczyć to będzie takich stadiów konfliktu, w których nie są stosowane uderzenia klasyczną bronią destrukcyjną. Niektóre formy ataku informatycznego wymagają wykonania wcześniejszych przedsięwzięć, np. umieszczenia złośliwych programów w obiektach ataku, umieszczenia spreparowanych podzespołów sprzętu, czy przygotowania odpowiedniej aparatury. W takim wypadku atak informatyczny może polegać na przekazaniu komend uruchamiających zainstalowane programy lub podzespoły sprzętu. Może też mieć formę jednoczesnego instalowania złośliwego oprogramowania i wykonywania przez niego ataku. Atak ten może też mieć formę długotrwałego wprowadzania fałszywych danych do systemów informacyjnych. Najlepszą formą jest zespolenie wielu sposobów, w jedno zespolone uderzenie informatyczne.

Walka w sferze przetwarzania danych cyfrowych prowadzona na poziomie strategicznym może zniszczyć całą cyfrową infrastrukturę państwa, paraliżując narodową sieć finansową, sieci telekomunikacyjne, giełdę papierów wartościowych, system kontroli ruchu powietrznego, handel powodując strach i poczucie niepewności w społeczeństwie. Prowadzić to powinno do ustępstw i akceptacji narzucanej woli bez konieczności używania konwencjonalnego ataku zbrojnego.

Atak elektroniczny w ramach informacyjnego ataku strategicznego dostosowany powinien być do stopnia eskalacji konfliktu. W takich stadiach, w których nie stosuje się uderzeń klasyczną bronią destrukcyjną i nie narusza się przestrzeni powietrznej i lądowej przeciwnika, atak elektroniczny może mieć głównie formę zakłócania znad własnego terytorium. W bardziej zaawansowanym stadium kon-

fliktu atak ten może przybrać formę uderzeń impulsów elektromagnetycznych lub wiązek energii mikrofalowej. Wykonanie ataków powietrznych z użyciem pocisków lub bomb elektromagnetycznych, może całkowicie sparaliżować miejsca ataku. Jeżeli miejsca te zostały starannie wybrane i stanowią krytyczne elementy jakiegoś systemu, to w efekcie ich sparaliżowania zdegradowany może być cały system.

Atak amunicją elektromagnetyczną

Użytecznym środkiem prowadzenia ataku strategicznego może być amunicja elektromagnetyczna, a szczególnie bomby elektromagnetyczne. Środki te bowiem są zabójcze dla sprzętu, a niegroźne dla ludzi. Jest to zasadnicza cecha, która odróżnia ten środek masowego rażenia od innych. Ta selektywność powoduje, że środki ataku elektromagnetycznego będą budzić zdecydowanie mniej oporów przed ich użyciem, aniżeli w stosunku do innych bardziej brutalnych, bo zabójczych środków rażenia. Jednocześnie skutki ataków elektromagnetycznych mogą być bardziej dotkliwe materialnie niż innych ataków.

Strategiczny atak elektromagnetyczny będzie się koncentrował na paraliżu systemów informacyjnych poszczególnych segmentów państwa. Współczesne nawet średnio rozwinięte państwa są bardzo silnie uzależnione od komputerów oraz telekomunikacji. Jednocześnie następuje coraz większe rozproszenie funkcji przetwarzania i dystrybucji informacji. Wiąże się to z powszechnym stosowaniem wielkiej liczby rozproszonych komputerów biurowych. Rozproszenie to oraz powszechność występowania, praktycznie uniemożliwiają uodpornianie na atak elektromagnetyczny, gdyż koszty takiego przedsięwzięcia byłyby większe niż wartość ochranianego sprzętu. Sytuacja ta jest zasadniczo różna od tej z przeszłości, gdy istniały ośrodki przetwarzania danych z dużymi komputerami. Sprzęt takich ośrodków był rozmieszczany w specjalnie przystosowanych pomieszczeniach, a całość łatwiej było uodpornić na zewnętrzne oddziaływania elektromagnetyczne. Współcześnie jest to niemal niemożliwe, gdyż komputery rozlokowane są wszędzie tam, gdzie ludzie przejawiają swoją aktywność. Ponadto rozległe sieci połączeń kablowych między różnymi współpracującymi ze sobą elementami, stanowią miejsce łatwego wzbudzenia wielkich przepięć niszczących podłączone do nich urządzenia. Ta decentralizacja i podatność tworzą niezwykłą wrażliwość na atak elektromagnetyczny, a wykorzystanie tej wrażliwości jest szansą na sukces ataku strategicznego. Zaatakowanie rejonów rozmieszczenia administracji rządowej może doprowadzić do jej paraliżu. Zniszczone mogą zostać nie tylko urządzenia przetwarzania i przesyłania informacji, lecz także przechowywania informacji, co czyni szkody jeszcze dotkliwszymi. Prostota wykonania takiego ataku, brak bezpośrednich ofiar ludzkich oraz zewnętrznych oznak zniszczeń, czyni go bardzo dogodnym i skutecznym.

Również inne komponenty, jak elementy sieci łączności, ich centrale, stacje przekaźnikowe, satelitarne stacje nadawczo-odbiorcze, studia i stacje przekaźnikowe radia i telewizji, rozdzielnie energetyczne, urządzenia sterowania ruchem

kolejowym i wiele innych tego typu, są wrażliwe na atak elektromagnetyczny. W związku z powszechnym uzależnieniem wszystkich aspektów ludzkiej aktywności od elektryczności, a ostatnio od komputerów i innych urządzeń przetwarzania i dystrybucji informacji, wszystkie podsystemy systemu państwa w modelu analizy Wardena są bardzo wrażliwe na atak elektromagnetyczny. Ze względu na powszechność występowania, nie jest możliwe wyeliminowanie wszystkich urządzeń elektronicznych, jednakże właściwa selekcja szczególnie ważnych elementów i ich elektromagnetyczne zniszczenie może doprowadzić do paraliżu państwa, a w najlepszym wypadku do spowodowania nieobliczalnych kosztów.

Główna infrastruktura ekonomiczna jest również wrażliwa na elektromagnetyczny atak. Infrastruktura finansowa, giełda papierów wartościowych są niemalże całkowicie zależne od komputerów i infrastruktury telekomunikacyjnej. Poszczególne gałęzie gospodarki maszynowej i chemicznej są wysoce zautomatyzowane i zrobotyzowane. Możliwe jest to dzięki powszechnemu zastosowaniu programowalnych logicznych układów kontrolnych lub komputerów. Co więcej, większość czujników i elementów telemetrycznych to urządzenia elektroniczne lub elektryczne. Zaatakowanie takich obiektów bronią elektromagnetyczną zatrzyma ich funkcjonowanie na czas ich wymiany lub rekonfiguracji. Niektóre procesy technologiczne mogą być sterowane tylko automatycznie, dlatego zniszczenie elementów elektrycznych i elektronicznych praktycznie je unieruchomi. Przykładem mogą być tu procesy rafineryjne ropy naftowej, wytwarzanie wielu substancji chemicznych, procesy wytopu metali i ich obróbki. Zniszczenie urządzeń automatyki może spowodować wielkie szkody ekonomiczne, a nawet braki materiałów strategicznych. Również przemysł zbrojeniowy jest w nie mniejszym stopniu wrażliwy, uzależniony od elektroniki i urządzeń elektrycznych.

Historyczne doświadczenia drugiej wojny światowej wskazywałyby, iż przemysł jest odporny na ataki powietrzne. Jednakże obecnie istnieją odmienne warunki. Wiążą się one głównie z dokładnością i dużą destrukcyjnością współczesnych środków rażenia. Ponadto współczesny przemysł jest niemalże całkowicie zależny od elektroniki i wysoce zautomatyzowany. Komputer, który był nieznany w czasie drugiej wojny światowej, jest teraz obecny niemalże w każdej maszynie lub linii technologicznej. To tworzy zupełnie odmienną sytuację. Obecnie atak elektromagnetyczny na główne elementy infrastruktury przemysłowej jest potencjalnie bardzo skuteczny, gdyż może spowodować niezwykle wysokie straty paraliżujące lub co najmniej znacznie ograniczające funkcjonowanie przemysłu. Niemniej jednak przy planowaniu tego typu działań, aby zapewnić szybkie osiągnięcie maksymalnego efektu, należy starannie przeanalizować i zidentyfikować środki ciężkości i właściwie określić priorytety ataków.

Infrastruktura komunikacyjna i telekomunikacyjna jest kolejnym elementem systemu państwa. Sieć transportowa jest bardziej odporna niż przemysł, jednakże niektóre elementy systemu transportowego, takie jak centrale sterowania ruchem kolejowym, szczególnie na węzłowych stacjach, stanowią bardzo wrażliwe komponenty. Może to być wykorzystane do blokowania ruchu. Również transport sa-

mochodowy jest oparty na pojazdach uzależnionych od elektroniki. Jednak ze względu na rozproszenie nie jest on łatwym przedmiotem atakowania. Opłacalność takiego ataku może być uzależniona od stopnia koncentracji pojazdów w rejonie ataku.

Kolejnym elementem systemu państwa jest społeczeństwo. Zazwyczaj celem ataku na społeczeństwo jest obniżanie jego morale. To zaś będzie w znacznym stopniu zależało od sprawności rządowej propagandy, a także od warunków życia. Stosując broń elektromagnetyczną, można paraliżować media masowej komunikacji, jak radio i telewizja, niszcząc ich studia produkcyjne oraz stacje przekaźnikowe i rozsiewcze.

Ostatnim elementem systemu państwa, według modelu Wardena, jest zgrupowanie bojowe sił zbrojnych. Współczesne siły zbrojne niemalże w całości są wrażliwe na atak elektromagnetyczny. Jednak ataki te koncentrować się powinny przede wszystkim na ośrodkach i stanowiskach dowodzenia i kontroli, węzłach łączności, stałych bazach logistycznych oraz zgrupowaniach wojsk. W stałych bazach logistycznych znajdują się znaczne ilości sprzętu diagnostycznego i serwisowego, który jest oparty na elektronice, a także komputery wykorzystywane nie tylko przez służby serwisowe, ale także przez administrację i obsługę. Razem ze znajdującym się w rejonie baz sprzętem bojowym, bazy te stanowią niezwykle opłacalny obiekt ataku elektromagnetycznego. Każde miejsce dużej koncentracji sprzętu bojowego stanowi bardzo opłacalny obiekt takiego ataku, gdyż w jego wyniku sprzęt ten zostaje zniszczony lub znacznie ograniczone są jego możliwości bojowe.

Broń elektromagnetyczna może stanowić bardzo efektywny środek rażenia ataku strategicznego. Zmasowane użycie tego typu broni może sparaliżować zarówno funkcjonowanie władzy, jak też infrastruktury przetwarzania i przesyłania informacji oraz ważnych ośrodków przemysłowych. Razem ze skutkami ataku na siły zbrojne, może to stanowić ograniczenie zdolności prowadzenia działań militarnych państwa. Broń elektromagnetyczna tworzy nieistotne w porównaniu do broni konwencjonalnej straty towarzyszące, zapewniając jednocześnie dużą efektywność i wysokie tempo kampanii bez strat w ludziach, typowych dla walk z użyciem broni konwencjonalnych. Z tego powodu kampanie strategicznych bombardowań elektromagnetycznych są dla zachodnich demokracji atrakcyjniejsze niż klasyczne odmiany tych bombardowań. Stosując ataki elektromagnetyczne, unika się bowiem negatywnego efektu obecności w mediach widoków zniszczeń i ofiar towarzyszących atakom konwencjonalnym. Taka obecność rezultatów fizycznej destrukcji i ofiar obniża publiczne poparcie dla prowadzonych działań. Broń elektromagnetyczna nie narusza zewnętrznego kształtu rzeczy, przez co rezultaty jej działań nie są tak widowiskowe i są bardziej akceptowalne przez opinię publiczną. Tymczasem destrukcja wewnętrzna wielkiej liczby urządzeń sterujących oraz przetwarzania i przesyłania informacji spowoduje koszty nieakceptowane przez dobrze rozwinięte cywilizacyjnie państwo. Ponadto, o ile przed atakami złośliwych kodów komputerowych można się skutecznie bronić, to obrona przed bronią elek-

tromagnetyczną jest niezwykle trudna, a szybko uzyskiwane przez atakującego rezultaty mogą odnosić również negatywne dla broniącego się efekty psychologiczne. Przeprowadzenie ataku równoległego bronią elektromagnetyczną, te negatywne dla obrońcy efekty dramatycznie pogłębi, prowadząc do paraliżu państwa.

Inne formy ataku elektronicznego mogą mieć bardziej doraźne znaczenie albo jako forma zabezpieczenia własnych działań sił powietrznych, albo jako uzupełniająca forma ataku. W ramach ataku elektronicznego mogą też być stosowane pociski naprowadzające się na źródło promieniowania radiolokacyjnego. Pociski takie mogą się też naprowadzać na inne emitujące promieniowanie elektromagnetyczne urządzenia. Amunicja tego typu może być skutecznym środkiem atakowania wielu elementów systemów informacyjno-komunikacyjnych.

Atak ogniowy jest klasyczną zdolnością sił zbrojnych. Szczególnie siły powietrzne, które mogą prowadzić powietrzny atak strategiczny – podobny pod względem koncepcji, lecz różniący się formą atakowania – nadają się do prowadzenia ataku ogniowego na dużą głębokość. O ile przy powietrznym ataku strategicznym głównym podmiotem mogą być siły powietrzne, to w wypadku informacyjnego ataku strategicznego siły te mogą być jedynie jednym z uczestników tego ataku. Ponadto w informacyjnym ataku strategicznym ataki koncentrują się na systemach informacyjnych oraz informacji, podczas gdy powietrzne ataki strategiczne skierowane są przeciwko całej infrastrukturze państwa. Atak ogniowy, prowadzony w ramach informacyjnego ataku strategicznego, mimo swojej klasyczności formy działania, wyróżnia się obiektami ataku. Obiektami tymi są bowiem jedynie elementy szeroko rozumianych systemów informacyjnych państwa przeciwnika. Atak ten w wykonaniu sił powietrznych może mieć formę połączonych działań powietrznych (*composite air operations* – COMAO) lub rajdów powietrznych małych grup samolotów. Środkiem rażenia może być każdy rodzaj uzbrojenia dobrany stosownie do charakteru atakowanego obiektu. Atak ten powinien być stosowany przede wszystkim wobec obiektów o dużej wartości i znaczeniu w systemach informacyjnych przeciwnika. Jest on użyteczny w sytuacjach oczekiwanego, długotrwałego wyeliminowania atakowanego obiektu z funkcjonowania.

Działania psychologiczne sił zbrojnych w ramach informacyjnego ataku strategicznego mogą być realizowane w tradycyjny sposób. Klasycznym zadaniem może być rozpowszechnianie ulotek. Przy odpowiednim wyposażeniu siły zbrojne mogą także prowadzić działania psychologiczne, wykorzystując radiowo-telewizyjne powietrzne stacje nadawcze oraz Internet. Obiektem takiego ataku mogą być zarówno kierownicze elity państwa, jak i całe społeczeństwo.

Dezinformacja powinna służyć przede wszystkim obniżeniu efektywności defensywnych działań informacyjnych przeciwnika. Siły zbrojne powinny stosować dezinformację, aby uniemożliwić przeciwnikowi rozpoznanie koncepcji działań, ich efektywności i zamiarów.

6.4. Informacyjne działania wspierające

Wspieranie w działaniach sił powietrznych może mieć formę izolowania i bezpośredniego (bliskiego) wspierania. Formy te zarówno w odniesieniu do klasycznej walki, jak i militarnej walki informacyjnej zostaną kolejno omówione.

6.4.1. Izolacja

Koncepcja izolacji informacyjnej została wywiedziona z istoty izolacji lotniczej. Identyfikacja modelu izolacji informacyjnej została dokonana przede wszystkim przez porównanie i analogię.

Izolacja lotnicza

Izolacja lotnicza[230] to działania powietrzne prowadzone w celu zniszczenia, zneutralizowania lub opóźnienia potencjału militarnego nieprzyjaciela, przed jego zastosowaniem w walce. Działania te prowadzi się na takiej odległości od własnych wojsk, która nie wymaga szczegółowej koordynacji z nimi ognia i manewru.

Izolacja lotnicza, nazywana też izolacją rejonu działań bojowych, pozostaje w polu zainteresowania zarówno teoretyków, jak i praktyków. Ci ostatni[231] koncentrują się głównie na usprawnianiu tego rodzaju działań w przyszłych zastosowaniach potęgi powietrznej.

Założeniem tej izolacji jest panowanie nad ciągłymi zmianami sytuacji. Izolację rejonu działań bojowych najlepiej zdefiniować jako działania lotnicze, prowadzone w celu zniszczenia, zneutralizowania lub opóźnienia działania nieprzyjacielskiego potencjału militarnego, przed jego efektywnym zastosowaniem przeciwko naszym siłom zbrojnym. Działanie to powinno nastąpić w takiej odległości od naszych sił, aby nie trzeba było integrować ognia i ruchu własnych sił w każdej emisji powietrznej. Stąd też izolacja wiąże się z dwoma kluczowymi elementami: oddziaływaniem na potencjał przeciwnika przed jego możliwym użyciem przeciwko naszym siłom oraz wykonaniem tego oddziaływania w takiej odległości, aby niepotrzebna była szczegółowa integracja działania sił własnych.

Odległość przeprowadzenia najbardziej skutecznej izolacji rejonu działań bojowych jest często głównym tematem rozważań. Działania lotnicze w bliskim sąsiedztwie własnych wojsk są tym, co tradycyjnie nazywa się bliskim wsparciem powietrznym i co, do zminimalizowania własnych strat i zapewnienia skuteczności, wymaga szczegółowej integracji planów działań. Tak więc izolacja rejonu działań bojowych obejmuje obiekty działań, które są rozmieszczone poza rejonem bezpośredniej styczności z wojskami własnymi. Do obiektów tych mogą być zali-

---

[230] Przyjęto za: AJP-01: *Allied Joint Doctrine*, Wydanie 1999.

[231] Fragmenty wystąpienia mjr. J.F. Morrisona z sił powietrznych Stanów Zjednoczonych zatytułowanego „Izolacja rejonu działań bojowych; zmienna perspektywa" na Konferencji sił powietrznych (Shephard Conferences) w lutym 1993 r.

czone: magazyny, konwoje, rejony ześrodkowania, linie komunikacyjne, wojska znajdujące się w terenie otwartym, bunkry, stanowiska dowodzenia.

Według amerykańskich założeń doktrynalnych[232] izolacja jest formą manewru powietrznego. Izolacja ta składa się z działań prowadzonych w celu odwrócenia, przerwania, opóźnienia lub zniszczenia naziemnego potencjału militarnego nieprzyjaciela przed jego efektywnym użyciem przeciwko naszym siłom. Walka informacyjna może być również użyta do prowadzenia izolacji przez przechwytywanie lub przerywanie strumienia informacji, lub niszczenie oprogramowania i sprzętu kontrolującego.

Izolacja informacyjna

W toku walki informacyjnej różne komponenty biorące udział w prowadzeniu tej walki mieć będą różne możliwości działania i rażenia. W związku z tym będą istniały obszary możliwości oddziaływania kilku komponentów oraz obszary oddziaływania pojedynczych komponentów. Również siły zbrojne mogą dysponować specyficznymi możliwościami niedostępnymi dla innych. **W sytuacji gdy główny wysiłek walki informacyjnej podejmują inne komponenty państwa, siły zbrojne dysponujące unikalnymi możliwościami mogą wspierać ten wysiłek, atakując pozostające dotąd poza zasięgiem walki elementy.**

Istotą informacyjnej izolacji jest atak informacyjny sił zbrojnych na elementy systemów informacyjnego komunikowania przeciwnika, pozostające poza zasięgiem działania wspieranych komponentów.

Informacyjna izolacja koncentruje się przede wszystkim na: określeniu organizacji systemów informacyjnych przeciwnika, oślepieniu jego sensorów i odcięciu go od informacji rozpoznawczej, zablokowaniu manewrowości jego systemów komunikacyjnych, zablokowaniu jego systemów informacyjnych i wykonaniu ataku pozostającego poza możliwościami wspieranych komponentów. Warto zwrócić uwagę na sprawy najbardziej istotne w informacyjnej izolacji – na proces wyznaczania obiektów ataku.

Identyfikacja obiektów ataku. Lokalizacja i identyfikacja obiektu ataku informacyjnej izolacji posiada duże znaczenie. Potrzeba ukształtowania pola walki na znaczną głębokość, wykorzystania możliwości unikalnych środków rażenia i dużego rozmachu działań walki informacyjnej, zwiększa wymagania w stosunku do systemów rozpoznania. Niezbędne bowiem staje się nie tylko zidentyfikowanie obiektów ataku, lecz także określenie tych spośród nich, które są krytycznie ważne dla funkcjonowania systemów informacyjnego komunikowania. Dotąd polegano na kombinacji pojazdów rozpoznawanych, sterowanych przez ludzi, na bezpilotowych satelitach, stałych lub ruchomych posterunkach rozpoznania oraz na informacjach uzyskiwanych od ludzi. Braki w dokładnościach tych zestawów i brak możliwości adaptacji do szybkiej zmiany warunków informacyjnego pola walki, mogą być poważnym ograniczeniem efektywnego użycia sił walki informacyjnej. Pojawienie

[232] *Air Force Basic Doctrine*, Maxwell AFB 1997.

się nowoczesnych technologii umożliwiających obserwowanie, wykrywanie i przechwycenie celu oraz wykorzystujących te technologie systemów rozpoznania poszerzają zakres obserwacji poza ograniczenia, jakie posiadały starsze systemy. W przyszłości działalność taka będzie ukierunkowana na zlokalizowanie i zidentyfikowanie nieprzyjacielskiego środka ciężkości. Charakter nieprzyjacielskich środków ciężkości będzie inny w każdym przypadku, ale środki te mogą lokalizować się w systemie dowodzenia i kontroli, kluczowych systemach łączności, systemach wykrywania, mogą też dotyczyć elementów cywilnej infrastruktury państwa przeciwnika. Z chwilą gdy obiekty ataku zostaną zidentyfikowane, dowódcy muszą zadecydować, które z nich są najbardziej istotne oraz określić priorytety ich zwalczania.

Stopień zniszczenia celu. Po zidentyfikowaniu potencjalnych obiektów ataku musi być określony stopień ich zniszczenia. Na przykład zakres zniszczenia może zawierać się od okresowej blokady systemu informacyjnego komunikowania do całkowitego zniszczenia jego elementów. Muszą być także wzięte pod uwagę zarówno cele polityczne, jak i cele taktyczne pola walki. Takie czynniki, jak odbudowa po konflikcie, minimalne zniszczenia towarzyszące i straty w ludności cywilnej będą wpływały na kształt ataku przeprowadzanego na określony cel. Po określeniu stopnia zniszczenia obiektu ataku, przychodzi czas na podjęcie decyzji o rodzaju i jakości użycia środków rażenia.

Dobór środków rażenia. Głównym problemem rozważanym podczas doboru środków rażenia są możliwości sił zbrojnych w zakresie walki informacyjnej, dopuszczalność stosowania poszczególnych środków zależna od stopnia eskalacji konfliktu i politycznej zgody na ich użycie. Niektóre środki, jak np. złośliwe programy, mogą zapewniać skrytość ataku, co w określonych sytuacjach może być pożądaną właściwością. Inne, takie jak bomby generujące destrukcyjny impuls elektromagnetyczny, wymagają działania identycznego, jak w wypadku ataku klasycznym uzbrojeniem lotniczym. Nosiciel musi więc wtargnąć w przestrzeń powietrzną przeciwnika i zbliżyć się do atakowanego obiektu. Mimo tej niedogodności, taki atak może być znacznie skuteczniejszy w rażeniu szerokiej gamy urządzeń elektronicznych i elektrycznych. Generowany impuls razi masowo w swojej strefie działania, dlatego jest zaliczany do broni masowego rażenia.

W niektórych wypadkach zalety klasycznego uzbrojenia burząco-destrukcyjnego mogą decydować o jego zastosowaniu. Może to mieć miejsce, gdy urządzenia są dobrze zabezpieczone przed atakiem informatycznym i elektromagnetycznym. Broń ta jest odpowiednia również w sytuacjach pożądanego, trwałego wyeliminowania danego obiektu z użytkowania. Wybór klasycznych środków ataku zależeć będzie od dokładności rażenia obiektu, co będzie również określać wysiłek niezbędny dla uzyskania wymaganego stopnia zniszczenia obiektu ataku. Normalnie do przeprowadzenia klasycznego uderzenia na obiekt ataku mogą być używane środki niekierowane, w tym środki powierzchniowego rażenia, oraz uzbrojenie kierowane. Charakterystyki obiektów rażenia również pomagają dokonać ostatecznego wyboru. Wielkość i stopień obrony obiektu rażenia, jego orientacja i lokalizacja

pozwolą określić nie tylko rodzaj uzbrojenia, ale również sposób dostarczenia uzbrojenia nad cel. Innym istotnym czynnikiem w procesie podejmowania decyzji są warunki w rejonie obiektu ataku.

Sposób dostarczenia środka rażenia nad cel. Po rozpatrzeniu poprzednich punktów, najważniejszą sprawą jest podjęcie decyzji o sposobie dostarczenia środka rażenia do obiektu ataku. W wypadku złośliwego programu komputerowego należy dobrać odpowiedni sposób przenikania oraz dotarcia programu do miejsca przenikania. Istotny jest również czas zainstalowania atakującego programu. Może on bowiem zostać umieszczony w obiekcie ataku lub jego otoczeniu dużo wcześniej przed planowanym atakiem. Ponieważ istnieje wiele różnorodnych sposobów dotarcia programu do obiektu ataku, powinny one być przeanalizowane w kontekście konkretnej sytuacji i dobrane odpowiednio do potrzeb. Jeśli chodzi o środki rażenia wymagające fizycznego umieszczenia ich w obiekcie ataku lub jego bezpośrednim otoczeniu, to nie każdy rodzaj broni ma odpowiednie możliwości dostarczenia wybranego uzbrojenia nad cel w wymaganej liczbie lub dokonania odpowiedniego zrzutu w wymaganym miejscu. Przykładowo, możliwości samolotu, obrona obszaru celu, atak w dzień czy w nocy, wymagany stopień dokładności trafienia, wymagana liczba uzbrojenia do zrzucenia na cel, aby osiągnąć jego pożądany stopień zniszczenia – wszystko to wchodzi w zakres podejmowanej decyzji. Reasumując, proces wyznaczania obiektów ataku jest realizowany w cyklu ciągłym. Począwszy od zbierania informacji i identyfikacji, aż do określenia stopnia zniszczenia, doboru wymaganego uzbrojenia, sposobu dostarczenia go nad cel – proces ten musi pozostać elastyczny z możliwościami adaptacyjnymi do szybko zmieniającej się sytuacji na polu walki.

Informacyjne izolowanie w siłach zbrojnych będzie narzędziem używanym do kształtowania sytuacji na przyszłym polu walki. Możliwości w zakresie izolowania wzmacniane będą posiadaną dominacją informacyjną, precyzyjnym i zabójczym rażeniem, dokładną identyfikacją obiektu ataku i krótkim czasem reakcji. Wiele technologicznych skoków jakościowych usprawni informacyjną izolację w przyszłości. Sensory penetrujące środowisko i urządzenia wskazujące wyposażone w nowe mikrotechnologie uzyskają moc przetwarzania informacji umożliwiającą dokładne trafienie obiektu ataku we właściwym miejscu. Zmienne możliwości rażenia umożliwią wybór wariantów między zniszczeniem, dezorganizacją, opóźnieniem, odstraszeniem lub zakłóceniem obiektów ataku. Synergiczne połączenie tych możliwości z inteligentnymi systemami obróbki logicznej, lepsze możliwości wykrycia obiektu ataku, zmniejszony cykl od wykrycia do ataku oraz ogólne możliwości sił powietrznych sprawią, że siły te będą bardzo ważnym komponentem przyszłej walki informacyjnej.

6.4.2. Bezpośrednie wspieranie informacyjne

Prezentacja koncepcji bezpośredniego wspierania informacyjnego, zgodnie z dominującym w tej części układem, poprzedzona jest omówieniem istoty koncepcji bezpośredniego wspierania lotniczego.

Bezpośrednie wspieranie lotnicze

Bezpośrednie wsparcie lotnicze[233] (CAS – *close air support*) to działanie powietrzne prowadzone zarówno przez stało-, jak i zmiennopłaty przeciwko wrogim obiektom położonym w bezpośredniej styczności bądź w bliskiej odległości od własnych wojsk. Działanie to wymaga szczegółowej koordynacji każdego zadania z ogniem i manewrem tych wojsk. Bezpośrednie wsparcie polega na zaangażowaniu się lotnictwa w walkę w strefie rażenia wojsk lądowych. Teoretycznie nie powinno być powodu dla takiego zaangażowania się, ponieważ wojska lądowe dysponują sprzętem i uzbrojeniem zapewniającym zaspokojenie wszystkich potrzeb bezpośredniej walki lądowej. Jednakże w praktyce bywa inaczej. Wojska lądowe, w sytuacjach gdy przeciwnik dysponuje inicjatywą, znajdują się nieraz w krytycznych warunkach. Lotnicze zaangażowanie jest więc wzmocnieniem walczących sił. Może to być uzasadnione w sytuacjach krytycznych, jednakże środowiska wojsk lądowych oczekują systematycznego angażowania się lotnictwa w walkę lądową. Tymczasem sprzęt lotniczy jest bardzo drogi i opłacalność jego użycia jest zapewniona jedynie wtedy, gdy atakuje on obiekty o dużej wartości, a takie są zwykle położone w głębi ugrupowania przeciwnika. Zniszczenie kilku czołgów czy haubic może mieć niewielką wartość w skali strategicznej, a groźba zniszczenia samolotu w strefie walki jest zdecydowanie większa niż poza nią. Bezpośrednie wspieranie jest więc działaniem awaryjnym i niezbyt racjonalnym.

Ofensywne wspieranie informacyjne

Poszczególni uczestnicy walki informacyjnej państwa prowadzą działania adekwatne do swoich możliwości. Jednoczesne działania walki informacyjnej różnych komponentów państwa w tym samym rejonie lub wobec tych samych obiektów może być niecelowe wobec trudności z koordynacją działań i możliwości wzajemnego zakłócania swoich akcji. Bywają jednak sytuacje, gdy takie działania są niezbędne. Może to być spowodowane uzupełniającymi się możliwościami bojowymi uczestników walki informacyjnej lub innymi podobnymi przyczynami. Dlatego **nie należy wykluczać możliwości prowadzenia ofensywnego wspierania informacyjnego**.

Istotą ofensywnego wspierania informacyjnego jest atak informacyjny sił zbrojnych na elementy systemów informacyjnego komunikowania przeciwnika będące w zasięgu działania wspieranych komponentów. Wspieranie tego typu będzie prowadzone podobnie jak informacyjna izolacja, z różnicą polegającą na ścisłej koordynacji działań wszystkich zaangażowanych w tym samym zadaniu lub rejonie uczestników walki informacyjnej.

W lotniczym wspieraniu „akty bratobójcze" są zrozumiałą przyczyną znacznego zainteresowania. Zapobieżenie atakowaniu swój swego, musi być zabezpieczone przez środki elektroniczne lub procedury albo bezpośrednie kierowanie. Ja-

[233] AJP-01: *Allied Joint Doctrine*, wyd. 1999.

kikolwiek byłby użyty system, musi także zapewnić odpowiedni zakres elastyczności. Podobnie **w wypadku ofensywnego wspierania informacyjnego istnieje niebezpieczeństwo wzajemnej neutralizacji niezbyt dobrze skoordynowanych działań**. Jednocześnie stosowane złośliwe programy ataku informatycznego mogą spowodować ich zdemaskowanie, zakłócenie rażenia. Zaatakowanie jakiegoś obiektu bez dokładnej koordynacji może spowodować zniszczenie bardzo wartościowego źródła informacji. Nieskoordynowane wprowadzenie do systemu informacyjnego komunikowania przeciwnika fałszywej informacji, może wprowadzić nieoczekiwaną dla innych uczestników walki zmianę zachowania przeciwnika i dezorganizację ich planów działania. Wykonanie ataku impulsami elektromagnetycznymi może spowodować obezwładnienie zainstalowanych wcześniej narzędzi ataku informatycznego, gdy sposób tego ataku nie został wcześniej skonsultowany z innymi uczestnikami walki informacyjnej.

W sumie **ofensywne wspieranie informacyjne, jeśli zaistnieje potrzeba jego prowadzenia, powinno być dokładnie skoordynowane z innymi uczestnikami walki informacyjnej oraz stosowane tam, gdzie istnieje uzasadniona potrzeba jego użycia**.

W przyszłości – w wyniku ewolucji systemów kierowania walką informacyjną oraz dalszej ewolucji informacyjnych środków rażenia – zostanie znacznie zwiększona efektywność wykonywania zadań. Uzyskanie zdolności środków rażenia do inteligentnego zachowania się na polu walki, połączone z automatycznym określaniem i przydzielaniem obiektów ataku, zapewni lepsze warunki prowadzenia wspierania. Elementy niezbędne do zbudowania takich systemów, to m.in.: sensory pozaelektromagnetyczne, akustyczne, penetracyjne oraz uzbrojenie z programowanym efektem, sensorowe sieci, bronie energetyczne i cząstkowe oraz wirtualne pętle procesów decyzyjnych. Jądrem tych elementów stają się: nanotechnologia, nieliniowe modelowanie oraz inteligentne systemy wsparcia.

ZAKOŃCZENIE

Obserwowane obecnie przyspieszenie zmian cywilizacyjnych jest źródłem wielu nowych zjawisk, które wzbudzają szerokie zainteresowanie. Podejmuje się więc coraz więcej badań w tym zakresie. Do sfery tego typu zjawisk zaliczyć należy m.in. gwałtowny wzrost roli informacji i oddziaływań w sferze informacyjnej oraz szybkie rozprzestrzenianie się aktywności militarnej niemającej charakteru walki zbrojnej. Problematyka ta stała się przedmiotem coraz szerszego zainteresowania wielu badaczy. W publikowanych rezultatach badań obserwować można jednak głównie podejścia koncentrujące się na analizowaniu istoty tych zjawisk, w oderwaniu od kontekstu, w którym one występują. Szczególnie zjawiska sfery militarnej są bardzo mocno uwarunkowane mechanizmem funkcjonowania państwa w stosunkach z innymi państwami. Dlatego też w niniejszych rozważaniach podjęto wiele wysiłku, by jak najpełniej sięgnąć do istoty i podłoża badanych zjawisk.

Przeprowadzone rozważania dotyczyły złożonego zjawiska, które z jednej strony obecne jest od zarania dziejów w społecznej aktywności, z drugiej zaś, przybierając nową jakość, staje się współczesnym fenomenem rozwoju cywilizacyjnego. Zjawiskiem tym jest informacja i informacyjna sfera oddziaływań. Informacja znalazła szerokie zainteresowanie badaczy, jednakże badanie sfery informacyjnych oddziaływań dopiero nabiera rozmachu.

Szczególnie ważnym aspektem, bo dotyczącym losów państw, jest sfera ich aktywności na arenie międzynarodowej. Całość tej aktywności podejmowanej przez różne komponenty państwa na wielu obszarach to działania państwa. Działania te prowadzone w poszczególnych sferach przez odpowiedzialne za nie komponenty państwa to odpowiednie do rodzaju sfery operacje. Działania państwa zmierzają do osiągnięcia celów państwa i to bezpośrednio wpływa na kształt operacji komponentów państwa. Dlatego charakter zarówno operacji militarnych, jak i operacji informacyjnych jest bardzo silnie powiązany z istotą działań państwa na arenie międzynarodowej. Świadomość tych uzależnień przyczyniła się do określenia istoty działań państwa na arenie międzynarodowej i wpływ tej istoty na operacje informacyjne i operacje militarne państwa.

W toku rozważań zidentyfikowano także militarny obszar walki niezbrojnej, pozostający praktycznie poza zainteresowaniem nauk wojskowych. W obszarze tym lokuje się część operacji informacyjnych. Wobec tego zaproponowano oryginalne rozwiązanie. Jego istotą jest objęcie obszaru militarnej walki niezbrojnej za-

interesowaniem nowej dyscypliny – ***sztuki militarnej***, której częścią pozostawałaby ***sztuka wojenna***. Rozwiązanie takie umożliwi ulokowanie szybko rosnących badań militarnej walki niezbrojnej w obszarze większych zainteresowań badawczych, co odpowiadałoby również obserwowanemu w praktyce wzrostowi militarnej aktywności pozawojennej. Dokonano także obszernej analizy aparatu pojęciowego znajdującego się w sferze prowadzonych rozważań. Wobec ujawnionych słabości, zaproponowano oryginalny zestaw podstawowych kategorii proponowanej *sztuki militarnej*, uwzględniający współczesny charakter i przewidywane zmiany broni, walki i wojny.

Wnikając w istotę informacyjnej aktywności, dokonano identyfikacji podejścia społecznego teorii informacji, jako najpełniej odzwierciedlającego proces informacyjnej komunikacji. Ustalono, że rozbudowały się elementy procesu komunikowania społecznego. Zaproponowano więc zmodyfikowaną wersję modelu procesu komunikowania społecznego. Umożliwiło to wskazanie miejsc możliwego wpływania na procesy informacyjnego komunikowania społecznego.

Rezultatem prowadzonych rozważań jest oryginalna identyfikacja i opis informacyjnej sfery aktywności państwa oraz określenie podstawowych kategorii i relacji zachodzących między nimi. Ustalono, że aktywność komponentów państwa w sferze informacyjnej ma charakter oddziaływań zewnętrznych – w stosunkach z innymi państwami – oraz wewnętrznych. Oddziaływania zewnętrzne mają formę informacyjnej współpracy i walki; oddziaływania wewnętrzne to informacyjne zasilanie procesów wewnętrznych. W związku z tym **dokonano oryginalnego zdefiniowania podstawowych kategorii, takich jak: operacje informacyjne państwa, walka informacyjna państwa, współpraca informacyjna państwa, zabezpieczenie informacyjne państwa**.

Ustalenia te umożliwiły teoretyczne osadzenie pojawiającej się chaotycznie w praktyce kategorii ***operacje informacyjne***, nazywanej niekiedy działaniami informacyjnymi. Dokonywane już były próby konceptualizacji walki informacyjnej, jednakże **nie spotkano zwartej koncepcji *operacji informacyjnych* wynikającej z istoty zjawiska – działań państwa, którego operacje informacyjne są częścią**.

Na tak zbudowanym podłożu konceptualnym zidentyfikowano różne, możliwe komponenty operacji informacyjnych i te przydatne do stosowania w siłach zbrojnych, zestawiono w **uporządkowaną i spójną koncepcję współczesnych militarnych operacji informacyjnych. Stanowi ona oryginalną konstrukcję, szczególnie w sferze kompozycji i dekompozycji jej elementów**. Najistotniejszą dyrektywą, która przyświecała konstrukcji tej koncepcji, była racjonalność i klarowność wyszczególnienia elementów militarnych operacji informacyjnych. **Główny wysiłek poznawczy w tym obszarze skoncentrowano na walce informacyjnej i informacyjnym zabezpieczeniu, gdyż te formy są zasadnicze dla działań militarnych**. Jednakże nie można ignorować istnienia informacyjnej współpracy; w pracy jedynie zasygnalizowano tę problematykę. Stać się ona powinna obszarem dalszej penetracji naukowej.

W wyznaczaniu kierunków rozwojowych militarnych operacji informacyjnych skoncentrowano się przede wszystkim na obszarze walki informacyjnej. W odniesieniu do przyszłej militarnej walki informacyjnej przyjęto, że na ogólne trendy rozwoju walki informacyjnej duży wpływ wywrą teorie walki, które są najbliższe ze względu na podobieństwo zjawisk i warunków. Takim podobieństwem cechują się środowiska powietrzne i informacyjne. Występuje też zbieżność wielu cech informacji i potęgi powietrznej. Wobec tego uznano, że doświadczenie i dorobek teorii działań powietrznych obejmującej poszczególne koncepcje tych działań, prawdopodobnie wywrą istotny wpływ na kształtowanie się koncepcji militarnej walki informacyjnej w przyszłości. W ten sposób ustalono zarys komponentów koncepcji militarnej walki informacyjnej, które prawdopodobnie wyłonią się w wyniku wspominanego wpływu. Zasadniczymi elementami tego zarysu są komponenty odnoszące się do: walki o przewagę informacyjną, informacyjnego ataku strategicznego oraz informacyjnych działań wspierających.

Wobec rosnącego zagrożenia bezpieczeństwa w sferze informacyjnej, opracowane treści mogą służyć zarówno racjonalnemu planowaniu przedsięwzięć poprawy poziomu tego bezpieczeństwa, jak też mogą być inspiracją w poszerzaniu militarnego instrumentarium państwa, służącego wsparciu interesów narodowych w ramach uprawiania polityki międzynarodowej.

BIBLIOGRAFIA

1. *Air Force Basic Doctrine*, Maxwell AFB, 1997.
2. AFDD 2-5: *Information Operations.*, Maxwell AFB 1998.
3. AFDD 2-5.1: *Electronic Warfare*, Washington, D.C. 1999.
4. Air Force Manual 1-1: *Basic Aerospace Doctrine of the United States Air Force*, March 1992.
5. AJP-01: *Allied Joint Doctrine*, NATO 1999.
6. AP 3000: *Royal Air Force Air Power Doctrine*, 2nd edition, Prepared under the direction of the Chief of the Air Staff 1993.
7. Arguilla J. Ronfeldt D., *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica 1997.
8. *Army Focus 94. Force XXI. America's Army in the 21st Century*, Washington, D.C. 1994.
9. Aron R., *Pokój i wojna między narodami*, Warszawa 1984.
10. ATP 33(C) (AJP-3.3): *Joint Air & Space Operations Doctrine*, second study draft, NATO 1997.
11. Balcerowicz B., *Obronność państwa średniego*, Warszawa 1997.
12. Balcerowicz B., *Sojusz a obrona narodowa*, Warszawa 1999.
13. *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, red. D.B. Bobrow, E. Haliżak, R. Zięba, Warszawa 1997.
14. Bosh J.M.J., Luiijf H.A.M., Mollema A.R., *Information Operations*, NL ARMS. Netherlands Annual Review of Mlitary Studies 1999, Breda 1999.
15. Brillouin L., *Science and Information Theory*, wyd. pol. *Nauka a teoria informacji*, Warszawa 1969.
16. Campen A., *The First Information War. The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War*, Fairfax 1992.
17. Campen A.D. Dearth D.H. Goodden R.T., *Cyberwar: Security, Strategy, and Conflct in the Information Age*, Fairfax 1996.
18. Cervera J.A., *Zagrożenia cywilizacji XX wieku. Relacje między kulturą, religią i polityką*, Wrocław 1999.
19. Ciborowski L., *Walka informacyjna*, Toruń 1999.
20. Clausewitz C., *O wojnie*, Warszawa 1958.
21. *Cyber-attacks*, www.infowar.com/mil_c4i/00/mil_c4i_120100a_j.shtml
22. Denning D.E., *Information Warfare and Security*, 1998.
23. Downs L.G. Jr, *Digital Data Warfare: Using Malicious Computer Code as a Weapon*, A Research Report Submitted to the Faculty in Fulfillment of the Curriculum Requirement, Maxwell AFB, 1995.
24. Drucker P.F., *Zarządzanie w XXI wieku*, Warszawa 2000.
25. Dubrawski Z., *Walka radioelektroniczna prowadzona przez siły powietrzne*, Warszawa 2000.
26. *Działania taktyczne wojsk lądowych*, red. S. Koziej, Warszawa 1992.
27. *Działania operacyjne wojsk lądowych*, Warszawa 1992.

28. Eco U., *Cinque scritti morali*, Milano 1997, wyd. pol. *Pięć pism moralnych*, tłum. I. Kania, Kraków 1999.
29. *Encyclopaedia Britannica*, http://www.britannica.com.
30. *Encyklopedia powszechna*, Warszawa 1976.
31. *Encyklopedia prawa*, Warszawa 1999.
32. Feeney M., Grieves M., *The Value and Impact of Information*, London 1994.
33. *Filozofia a nauka. Zarys encyklopedyczny*, Wrocław 1987.
34. FM 100-6: *Information Operations*, Headquarters Department of the Army, Washington 1996.
35. Forno R., Baklarz R., *The Art of Information Warfare: Insight into the Knowledge Warrior Philosophy*, Washington 1999.
36. Fredericks B.E., *Information Warfare at the Crossroads*, „Joint Force Quarterly", Summer 1997.
37. Frezza B., *The Militarization of Cyberspace*, http://techweb.cmp.com/nc/frezza/ frezza.html.
38. *Globalizacja gospodarki światowej a integracja regionalna. Konsekwencje dla świata i Polski*, Warszawa 1998.
39. Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999.
40. Hajdukiewicz J., *e-Przestępczość* http://www.it-forum.pl/6/referaty/word/Hajdukiewicz-got.doc.
41. http://www.seas.gwu.edu/~reto/infowar/view.htm 26.01.2001 r.
42. *Informacyjny wymiar współczesnych działań powietrznych*. Materiały z sympozjum naukowego, red. R. Szpyra, Warszawa 2002.
43. Ivefors G., *Information Warfare. Defeat the Enemy Before Battle – A Warfare Revolution in the 21st Century?* http://www.ida.liu.se/~guniv/Infowar/ 26.01.2001.
44. *Joint Economic Committee Hearing. Radio Frequency Weapons and Proliferation: Potential Impact on the Economy*, 25.02.1998, http://www.house.gov/jec/ hearings/02-25-8h.htm.
45. Joint Pub 1-02: *Dictionary of Military and Associated Terms Department of Defense*, Washington D.C. 1999.
46. Joint Pub 3-13: *Joint Doctrine for Information Operations*, Washington D.C. 1998.
47. Kardaś T., *Punkt ciężkości*, „Myśl Wojskowa" 2000, nr 2.
48. Kennedy P., *Preparing for the Twenty-first Century*, New York 1993.
49. Khalilzad Z.M., White J.P., *Strategic Appraisal. The Changing Role of Information in Warfare*, Santa Monica 1999.
50. Koch E.R., Sperber J., *Infomafia. Szpiegostwo komputerowe, handel informacją, tajne służby*, tłum. R. Ratajski, Gdynia 1999.
51. Kopp C., *The E-Bomb – A Weapon of Electrical Mass Destruction*, http://www.cs. monash.edu.au/carlo/ 04.1997.
52. Koziej S., *Ciągłość oddziaływania na przeciwnika podczas natarcia*, „Myśl Wojskowa" 1978, nr 5.
53. Koziej S., *Teoria sztuki wojennej*, Warszawa 1993.
54. Koziej S., *Współczesna myśl taktyczna*, „Myśl Wojskowa" 1987, nr 10.
55. Koziej S., *Przełom w sztuce wojennej*, [w:] *Sztuka wojenna. Konteksty teoretyczne i praktyczne*, red. M. Krauze, B.M. Szulc, Toruń 2000.
56. Kozub M., Bartnik R., Szulc S., *Rozpoznanie powietrzne na współczesnym polu walki (według poglądów obowiązujących w NATO)*, „Przegląd Wojsk Lotniczych i Obrony Powietrznej" 1998, nr 12.
57. Kozub M., *Rozpoznanie powietrzne w działaniach bojowych*, Warszawa 2001.
58. Łazarczyk J., *Współczesna technika lotniczego rozpoznania powietrznego*. Referat, Warszawa 2001.
59. *Leksykon wiedzy wojskowej*, Warszawa 1979.
60. Lem S., *Bomba megabitowa*, Kraków 1999.

61. Levinson P., *Miękkie ostrze. Naturalna historia i przyszłość rewolucji informacyjnej*, Warszawa 1999.
62. Libicki M.C., *Defending Cyberspace and Other Metaphors*, Washington 1997.
63. Libicki M.C., *What is Information Warfare?* Washington 1995.
64. *Mała encyklopedia wojskowa*, Warszawa 1971.
65. Martin J.V., *Victory from Above. Air Power Theory and the Conduct of Operations Desert Shield and Desert Storm*, Maxwell AFB 1994.
66. Mazur M., *Jakościowa teoria informacji*, Warszawa 1970.
67. McRae H., *Świat w roku 2020. Potęga, kultura i dobrobyt – wizja przyszłości*, Warszawa 1996.
68. Michalak W., *Dominacja z powietrza*, Warszawa 1999.
69. Mitchell W., *Winged Defense: The Development and Possibilities of Modern Power – Economic and Military*, Washington 1971.
70. Molander R.C., Riddile A.S., Wilson P.A., *Strategic Information Warfare. A New Face of War*, Santa Monica 1996.
71. Molander R.C., Wilson P.A., Mussington D.A., Mesic R.F., *Strategic Information Warfare Rising*, Santa Monica 1998.
72. *Nowa encyklopedia powszechna PWN*, Warszawa 1996.
73. Nowacki G., *Walka informacyjna – próba kategoryzacji*, Rozprawa doktorska, Warszawa 1999.
74. Nowacki G., *Współczesne poglądy na prowadzenie walki informacyjnej. Studium teoretyczne*, Warszawa 2001.
75. Nowacki G., *Operacje informacyjne na współczesnym polu walki*, [w:] *Informacyjny wymiar współczesnych działań powietrznych.* Materiały z sympozjum naukowego, red. R. Szpyra, Warszawa 2002.
76. Podkowski A., Laszczkowski A., *Ulotki w działaniach bojowych*, Materiał studyjny, Warszawa 2001.
77. Podkowski A., *Siły, środki i możliwości oddziaływania psychologicznego armii amerykańskiej podczas konfliktu zbrojnego*, Warszawa 1998.
78. Podkowski A., *Zasady i techniki perswazji w działaniach psychologicznych w walce zbrojnej (na przykładzie armii sowieckiej w latach 1921–1991)*, Warszawa 1998.
79. *Polskie Siły Powietrzne w NATO.* Etap II: *Miejsce, rola i zadania Polskich Sił Powietrznych w systemie obronnym RP i NATO oraz kierunki i priorytety ich rozwoju*, Warszawa 2000.
80. Qiao Liang, Wang Xiangsu, *Unrestricted Warfare: Assumptions on War and Tactics in the Age of Globalization*, Beijing 1999, tłum. na j. ang. US CIA's Foreign Broadcast Information Service, http://www.terrorism.com/documents/ unrestricted.pdf lub http://cryptome.org/cuw.zip, 2000.
81. Rutkowski C., *Prakseologiczne aspekty strategii wojskowej*, Rozprawa habilitacyjna, Warszawa 1998.
82. Schwartau W., *Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, New York 1996.
83. Seffers G.I., *Joint Chiefs Inaugurate Information Combat Era*, „Defense News" 1998, November.
84. Sienkiewicz P., *Inżynieria systemów*, Warszawa 1983.
85. Sienkiewicz P., *Wojna informatyczna*, „ComputerWorld" 1997, nr 31.
86. Sienkiewicz P., *Współczesne koncepcje walki informacyjnej*, [w:] *Informacyjny wymiar współczesnych działań powietrznych.* Materiały z sympozjum naukowego, red. R. Szpyra, Warszawa 2002.
87. Skibiński F., *Rozważania o sztuce wojennej*, Warszawa 1978.
88. *Słownik języka polskiego PWN*, Warszawa 1981.
89. *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2002.
90. Stark R., *Future Warfare: Information Superiority through Info War*, http://www. smsu.edu.

91. Stein G., *Information War – Cyberwar – Netwar*, [w:] *Battlefield of the Future. 21st Century Warfare Issues*, Maxwel AFB 1995.
92. Stein G., *Information Warfare*, [w:] *Cyberwar: Security, Strategy, and Conflct in the Information Age*, red. A.D. Campen, D.H. Dearth, R.T. Goodden, Fairfax 1996.
93. Stein G., *Information Warfare. Learning With Sun Tzu*, [w:] *Information Operations*, NL ARMS. Netherlands Annual Review of Military Studies 1999, Breda 1999.
94. *Strategia rozwoju Polski do roku 2020*, t. 1, *Diagnoza ogólnych uwarunkowań rozwojowych*, Komitet Prognoz „Polska 2000 Plus" przy Prezydium PAN, Warszawa 2000.
95. *Strategic Assessment 1996. Instrument of U.S. Power*, National Defence University INSS, Washington D.C. 1996.
96. Sun Tzu, *Sztuka wojny*, Warszawa 1994.
97. *Sztuka wojenna. Konteksty teoretyczne i praktyczne*, red. M. Krauze, M.B. Szulc, Toruń 2000.
98. Szafranski R., *Mars Chuckles And Athena in Frustration*, [w:] *Information Operations*, NL ARMS. Netherlands Annual Review of Military Studies 1999, Breda 1999.
99. Szpyra R., *Operacje informacyjne państwa w działaniach sił powietrznych*, Rozprawa habilitacyjna, „Zeszyty Naukowe AON" (dodatek), Warszawa 2002.
100. Szpyra R., *Przyszła wojna powietrzna*, Praca badawcza pod kryptonimem *WIZJA*, Warszawa 1999.
101. Szpyra R., *Działania informacyjne i walka informacyjna we współczesnych i przyszłych zastosowaniach sił powietrznych*, „Przegląd Wojsk Lotniczych i Obrony Powietrznej" 2000, nr 9.
102. Szpyra R., *Rola sił powietrznych w wojnie przyszłości*, Warszawa 2000.
103. Szpyra R., *Walka informacyjna w przyszłych działaniach sił powietrznych*, Praca badawcza pod kryptonimem *CYBERAWIATOR*, Warszawa 2000.
104. Szpyra R., *Współczesna wojna powietrzna. Wybrane problemy*, Warszawa 1998.
105. Szpyra R., *Współczesne treści powietrznej sztuki operacyjnej*, cz. 1, Praca badawcza pod kryptonimem *OPERATOR 1*, Warszawa 2000.
106. Szpyra R., *Polityczno-militarne i operacyjne aspekty kampanii „Sojusznicza Siła"*, [w:] *Allied Force – współczesny model kampanii powietrznej*, Warszawa 2001.
107. *Sztuka operacyjna wojsk lotniczych*, Warszawa 1988.
108. Szymański R. (zesp.), *Lotnictwo wojskowe*, Warszawa 1998.
109. Świniarski J., *O naturze bezpieczeństwa. Prolegomena do zagadnień ogólnych*, Warszawa–Pruszków, 1997.
110. Świniarski J., *O zasadach, regułach i dyrektywach sztuki wojennej. Próba spojrzenia filozoficznego*, [w:] *Sztuka wojenna. Konteksty teoretyczne i praktyczne*, red. M. Krauze, B.M. Szulc, Toruń 2000.
111. Tedder M., *Air Power in War*, London 1948.
112. *The Global Course of the Information Revolution: Technological Trends.* Proceedings of an International Conference, http://www.rand.org/publications/ CF/CF157/.
113. Toffler A., Toffler H., *Wojna i antywojna. Jak przetrwać na progu XXI wieku*, Warszawa 1997.
114. Vickery B., Vickery A., *Information Science in Theory and Practice*, London 1987.
115. *Walka radioelektroniczna w siłach zbrojnych RP*, Warszawa 1994.
116. Waltz E., *Information Warfare Principles and Operations*, Boston 1998.
117. Warden III J.A., *„Air Theory for the Twenty-first Century" Battlefield of the Future*, [w:] *21st Century Warfare Issues*, Maxwell AFB 1995.
118. Warden III J.A., *The Air Campaign. Planning for Combat*, New York 1998.
119. Wojtaszczyk K.A., *Kompendium wiedzy o państwie współczesnym*, Warszawa 1998.
120. Zacher L.W., *Społeczeństwo informacyjne. W perspektywie człowieka, techniki, gospodarki*, Warszawa 1999.
121. Zajas S. (zesp.), *Podstawy użycia rodzajów wojsk sił powietrznych*, Warszawa 1999.

122. Zdrodowski B., Marciniak M., *Doktryna powietrzna NATO*, Warszawa 1999.
123. Zdrodowski B., *Podstawy obrony powietrznej*, Warszawa 1997.
124. Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego, koncepcje – struktury – funkcjonowanie*, Warszawa 1999.

WITRYNY INTERNETOWE

Witryny cywilne

Network and Computer Security.
URL: http://www.sans.org
Winn Schwartau's InfoWar.com
URL: http://www.infowar.com
Institute for the Advanced Study of Information Warfare
URL: http://www.psycom.net/iwar.1.html
Journal of Infrastructure Warfare
URL: http://www.iwar.org
Federation of American Scientists on IW
URL: http://www.fas.org/irp/wwwinfo.html
The Information Warfare Research Center
URL: http://www.terrorism.com/infowar/index.html

Wybrane witryny wojskowe

Information Operations & Intel
URL: http://www.au.af.mil/au/awc/awcgate/awc-info.htm
US Navy INFOSEC Homepage
URL: http://infosec.nosc.mil/content.html
ACC's Network Operations and Security Center (NOSC)
URL: http://wwwmil.acc.af.mil/nosc/
NASA Automated Systems Incident Response Capability
URL: http://www-nasirc.nasa.gov/nasa/index.html
C4RDP - Command, Control, Communications and Computers Requirements Definition Program
URL: http://www.c4rdp.gordon.army.mil/index.htm
National Counter-Intelligence Center.
URL: http://www.nacic.gov
Naval Computer And Telecommunications Area Master Station, LANT (NCTAMS LANT)
URL: http://www.chips.navy.mil/
DISA Homepage
URL: http://www.disa.mil
Air Intelligence Agency
URL: http://www.aia.af.mil
Defense Technical Information Center
URL: http://www.dtic.mil

Joint Electronic Library
URL: http://www.dtic.mil/doctrine/jel/
USPAWAR (Space and Naval Warfare Systems Command)
URL: http://www.spawar.navy.mil

SPIS RYSUNKÓW

Rys. 1. Obszary aktywności militarnej oraz ich relacje ze sztuką wojenną 28
Rys. 2. Relacje między naukami wojskowymi, sztuką wojskową i sztuką wojenną 44
Rys. 3. Byt, jakość bytu i interes – pierwotne motywy działania 45
Rys. 4. Interesy, pierwotne motywy działania i ich wzajemne relacje 45
Rys. 5. Formy kooperacji 47
Rys. 6. Spektrum aktywności państwa na arenie międzynarodowej 47
Rys. 7. Sfery oddziaływań państwa w relacjach z innymi podmiotami 48
Rys. 8. Pozytywne i negatywne formy sfer oddziaływań 49
Rys. 9. Zewnętrzne sfery oddziaływań oraz sfery zasilania procesów wewnętrznych 50
Rys. 10. Skala zastosowania komponentów potęgi państwa (przykład) 58
Rys. 11. Spektrum działań militarnych 59
Rys. 12. Wybrane kategorie militarnego aspektu walki 63
Rys. 13. Mapa teoretyków, ich poglądów oraz zachodzących między nimi relacji 68
Rys. 14. Podstawowe kategorie opisu infosfery 72
Rys. 15. Społeczne postrzeganie komunikacji informacji 75
Rys. 16. Model informacyjnego transferu 77
Rys. 17. Matematyczno-fizyczne i społeczne podejście teorii informacji 79
Rys. 18. Miejsca możliwego modyfikowania treści informacji 80
Rys. 19. Rewolucyjne zmiany w dowodzeniu 82
Rys. 20. Model cyklu decyzyjnego 83
Rys. 21. Różne cykle decyzyjne 83
Rys. 22. Natura walki informacyjnej 91
Rys. 23. Sfera operacji informacyjnych 93
Rys. 24. Doktryny operacji informacyjnych amerykańskich sił lądowych i powietrznych oraz doktryna połączona 94
Rys. 25. Działania państwa oraz operacje informacyjne państwa 102
Rys. 26. Model systemu informacyjnego komunikowania 102
Rys. 27. Operacje informacyjne państwa w relacjach międzynarodowych 103
Rys. 28. Eksplozyjnie pompowany kompresyjny generator strumieniowy FCG 121
Rys. 29. Vircator – urządzenie generujące jeden silny impuls promieniowania 122
Rys. 30. Vircator z zestawem antenowym 123
Rys. 31. Bomba elektromagnetyczna z generatorem typu FCG 124
Rys. 32. Promień i strefa rażenia bomby elektromagnetycznej 126
Rys. 33. Strumień rażenia bomby elektromagnetycznej 126
Rys. 34. Atakowanie bombami elektromagnetycznymi 127
Rys. 35. Zapobieganie rozpoznaniu 141

Rys. 36. Niedopuszczenie do informacyjnego atakowania lub uzyskiwania pożądanej efektywności tego atakowania przez przeciwnika 142
Rys. 37. Pokój komputerowy zabezpieczony przed atakiem elektromagnetycznym 145
Rys. 38. Wzrost prędkości przepływu i przetwarzania informacji 150
Rys. 39. Procesy rozpoznania 154
Rys. 40. Dekompozycja rozpoznania (przykłady) 155
Rys. 41. Model państwa według Wardena 179
Rys. 42. Model strategicznego ataku informacyjnego 186

SPIS TABEL

Tabela 1. Instrumenty niemilitarne potęgi państwa 55
Tabela 2. Instrumenty polityczno-militarne potęgi państwa 56
Tabela 3. Militarne instrumenty prowadzenia wojny 57
Tabela 4. Definicje informacji 67
Tabela 5. Przegląd definicji walki informacyjnej 97
Tabela 6. Przegląd definicji operacji informacyjnych 99
Tabela 7. Porównanie głównych komponentów walki elektronicznej według poglądów USAF i polskich 109
Tabela 8. Przykłady walki w sferze przetwarzania danych cyfrowych 110
Tabela 9. Przykłady zastosowań różnych miejsc i metod penetracji 112
Tabela 10. Elementy dezinformacji wojskowej 138

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 56910
Akademii Obrony Narodowej

Publikacje
Akademii Obrony Narodowej

do nabycia w Wydziale Wydawniczym AON
al. gen. A. Chruściela 103, bl. 2
00-910 Warszawa,
tel. 681 40 55, tel./faks 681 37 52

- S. Bartosiewicz, M. Mróz – Zaopatrywanie jednostek wojsk lotniczych i obrony powietrznej w techniczne środki materiałowe techniki naziemnej – 7,00 zł
- Bezpieczne niebo. Materiały z konferencji naukowej – 14,00 zł
- J. Bieńkowski, R. Stępień (red.) – Edukacja pedagogiczna w wyższej uczelni wojskowej – 16,00 zł
- H. Binkowski (red.) – OBWE w procesie umacniania bezpieczeństwa europejskiego – 16,00 zł
- A. Bujak – Praca w terenie na szczeblach taktycznych według standardów NATO – 10,00 zł
- W. Chojnacki – Socjologiczne aspekty tendencji instytucjonalno-organizacyjnego rozwoju wojska – 16,00 zł
- R. Chrobak i in. – Działania bojowe dywizji – 15 zł
- M. Cieślarczyk, P. Krawczyk, Z. Korulczyk – Poradnik metodyczny autorów prac kwalifikacyjnych – 8,00 zł
- M. Cieślarczyk, M. Chojnacki, A, Radomyski – Współpraca cywilno-wojskowa (CIMIC) w siłach zbrojnych (SP) RP – 13,00 zł
- M. Cieślarczyk (red.) – Metody, techniki i narzędzia badawcze oraz elementy statystyki – 13,00 zł
- A. Ciupiński, M. Zając (red.) – Wybrane problemy walki z terroryzmem międzynarodowym – 17 zł
- A. Ciupiński (red.) – Dyplomacja wielostronna – 25,00 zł
- A. Ciupiński – Podstawowe elementy polityki bezpieczeństwa i obrony RP – 15,00 zł
- A. Ciupiński, R. Białoskórski – Wczesne ostrzeganie i zapobieganie współczesnym konfliktom zbrojnym w strategii Sojuszu Północnoatlantyckiego – 7,00 zł
- A. Ciupiński, H. Binkowski, A. Legucka – Bezpieczeństwo w stosunkach międzynarodowych – 30,00 zł
- T. Compa – Zarządzanie przestrzenią powietrzną – 10,00 zł
- J. Czaja – Stolica apostolska wobec integracji europejskiej – 15,00 zł
- K. Czajka – Użycie artylerii w obronie oddziału – 8,00 zł
- P. Daniluk – Radiostacje pola walki – 10,00 zł
- A. Dawidczyk – Nowe wyzwania, zagrożenia i szanse dla bezpieczeństwa Polski u progu XXI w. – 9,00 zł
- P. Dela, J. Wołejszo – Wsparcie komputerowe ćwiczeń wojskowych 16 zł
- Dowodzenie lotnictwem sił powietrznych w działaniach wojsk lądowych (praca zbiorowa) – 15,00 zł
- W. Drążczyk – Logistyka sił powietrznych w działaniach wielonarodowych – 9,00 zł
- A. Fellner – Zautomatyzowane systemy kontroli ruchu lotniczego przestrzeni powietrznej – 20,00 zł
- M. Flemming – Międzynarodowe prawo humanitarne konfliktów zbrojnych – 45,00 zł
- P. Gawliczek, J. Pawłowski – Zagrożenia asymetryczne – 14,00 zł
- M. Gąska, A. Ciupiński – Międzynarodowe prawo humanitarne konfliktów zbrojnych – 21,00 zł
- A. Glen, W. Marud – Kontrola przestrzeni powietrznej w czasie kryzysu i wojny – 18,00 zł
- J. Gotowała – Lotnictwo XXI wieku – 11,00 zł
- J. Groskrejc – Antropologiczne i aksjologiczne aspekty edukacji oficerów – 10,00 zł
- J. Halik – Metodyka opracowania pracy magisterskiej i studyjnej – 15,00 zł
- J. Halik, J. Wołejszo – Ćwiczenia wojskowe sił zbrojnych RP w aspekcie interoperacyjności w ramach NATO – 14,00 zł
- M. Huzarski (red.) – Taktyka ogólna wojsk lądowych – 21,00 zł
- K. Jałoszyński – Terroryzm antyizraelski – 12,00 zł
- K. Jałoszyński – Terroryzm czy terror kryminalny w Polsce? – 12,00 zł
- K. Jałoszyński – Zagrożenie terroryzmem w wybranych krajach Europy Zachodniej oraz w Stanach Zjednoczonych – 12,00 zł
- J. Janczak – Zakłócanie informacyjne – 12,00 zł
- Cz. Jarecki – Użycie wojsk rakietowych i artylerii w operacji – 13,00 zł
- T. Jemioło – Globalizacja. Szanse i zagrożenia – 8,00 zł
- T. Jemioło, K. Malak (red.) – Bezpieczeństwo zewnętrzne Rzeczypospolitej Polskiej – 25,00 zł
- A. Jóźwiak, Cz. Marcinkowski – Wybrane problemy współczesnych operacji pokojowych – 18,00 zł
- M. Juszczyk – Wsparcie działań przez państwo gospodarza – 14 zł
- L. Kanarski, P. Gawliczek – Przywództwo w armiach NATO – 9,00 zł
- L. Kanarski, B. Rokicki (red.) – Teoria i praktyka przywództwa wobec wyzwań edukacyjnych – 24,00 zł
- J. Kardas, K. Loranty – Wybrane problemy bezpieczeństwa i obronności państwa w opiniach pracowników administracji publicznej – 12,00 zł
- J. Kardas, K. Loranty – Instytucjonalizacja przygotowania obronnego kadr administracji – 15,00 zł
- J. Karpowicz, Z. Chojnacki – Bezpieczeństwo lotów – 10,00 zł
- J. Karpowicz, E. Cieślak – Lotnictwo wsparcia w sojuszniczych działaniach powietrznych – 17 zł
- J. Karpowicz, K. Kozłowski – Bezzałogowe statki powietrzne i miniaturowe aparaty latające – 18 zł
- J. Karpowicz – Współczesne konstrukcje lotnicze – 20,00 zł

- Cz. Kącki – Siły wielonarodowe do misji pokojowych – 15 zł
- Cz. Kącki – Izrael. Jego wpływ na rozwój sytuacji w regionie Bliskiego Wschodu – 15,00 zł
- Kierowanie mobilnymi systemami łączności wojsk lądowych (praca zbiorowa) cz.I – 14 zł, cz.II – 8 zł, cz.III. – 12 zł
- W. Kitler (red.) – Obrona cywilna (niemilitarna) w obronie narodowej III RP – 25,00 zł
- W. Kitler – Obrona narodowa III RP. Pojęcie. Organizacja. System (rozprawa habilitacyjna) – 24,00 zł
- W. Kitler – Obrona narodowa w wybranych państwach demokratycznych – 14,00 zł
- Z. Klawitter – Rola i zadania zespołu wsparcia personalnego na stanowisku dowodzenia BZ/BPanc – 7,00 zł
- T. Kochański – Logistyka międzynarodowa – 12,00 zł
- T. Kochański – Logistyka jako koncepcja zintegrowanego zarządzania – 18,00 zł
- T. Kochański, S. Kurek – Konkurencyjność przedsiębiorstw – 15 zł
- M. Koziński – Umowa offsetowa i inne formy udziału państwa w międzynarodowym obrocie gospodarczym – 10,00 zł
- M. Kozub – Lotnictwo w operacjach połączonych – 7,00 zł
- M. Kozub – Lotnictwo wojsk lądowych w operacjach połączonych – 8,00 zł
- M. Kozub – Lotnictwo w bojowym poszukiwaniu i ratownictwie – 8,00 zł
- J. Kręcikij – Współczesne kierowanie wojskami. Proces dowodzenia – 12,00 zł
- J. Kręcikij – Metodyka pracy sekcji dowodzenia oddziału i związku taktycznego – 13,00 zł
- J. Kręcikij –Wybrane problemy kierowania zgrupowaniami wielonarodowych sił połączonych – 14,00 zł
- R. Kwećka, M. Gryga – Siły specjalne w kontekście współczesnych zagrożeń – 15,00 zł
- K. Kubiak – Transport wojsk i ładunków wojskowych drogą morską przy użyciu statków handlowych – 12,00 zł
- L. Łukaszuk – Międzynarodowe prawo pokoju i bezpieczeństwa – 20,00 zł
- L. Łukaszuk – Dyplomacja współczesna a problemy prawa i bezpieczeństwa międzynarodowego – 20,00 zł
- L. Łukaszuk – Europejskie prawo pokoju i bezpieczeństwa – 20,00 zł
- T. Majewski – Ankieta i wywiad w badaniach wojskowych – 9,00 zł
- T. Majewski – Kierownik – dowódca w organizacji – 12,00 zł
- T. Majewski – Miejsce celów, problemów i hipotez w procesie badań naukowych – 8 zł
- T. Majewski i in. – Planowanie w organizacji – 9 zł
- K. Malak – Polityka zagraniczna i bezpieczeństwa Białorusi – 18,00 zł
- J. Marczak (red.) – Samoorganizacja społeczeństwa na rzecz bezpie-czeństwa powszechnego. Samoobrona powszechna III RP – 20,00 zł
- M. Marszałek – Siły powietrzne w operacjach ewakuacyjnych (według poglądów amerykańskich) – 13 zł
- M. Marszałek, A. Radomyski – Metodyka pracy zespołów funkcjonalnych na stanowisku dowodzenia brygady rakietowej sił powietrznych – 25,00 zł
- Z. Maślak – Podstawy teorii informacji obrony powietrznej – 10,00 zł
- Z. Maślak (oprac.) – Informacje w obronie powietrznej – potrzeby, wymagania, zagrożenia. Materiały z sympozjum naukowego – 17,00 zł
- M. Michalec (oprac.) – Kierunki rozwoju rosyjskiej myśli teoretycznej i praktyki w zakresie użycia lotnictwa w walce – 14,00 zł
- J. Michniak (red.) – Projektowanie struktury organizacyjnej dowództwa brygady zmechanizowanej (pancernej) – 12,00 zł
- J. Michniak – Stanowiska dowodzenia w wojskach lądowych – 10 zł
- G. Nowacki – Informacja w walce zbrojnej. Materiały z sympozjum naukowego – 17,00 zł
- G. Nowacki – Strategiczne siły jądrowe wybranych państw – 14,00 zł
- G. Nowacki – Rozpoznanie satelitarne USA i Federacji Rosyjskiej – 8,00 zł
- G. Nowacki (red.) – Militaryzacja kosmosu – 17,00 zł
- A. Nowak – Działalność rozpoznawcza na szczeblach taktycznych – 12,00 zł
- E. Nowak – Gospodarowanie zasobami majątkowymi – 15,00 zł
- M. Obrusiewicz – Wielonarodowe połączone siły zadaniowe CJTF – 12,00 zł
- M. Obrusiewicz – Geneza i prognoza kooperatywnych stosunków wojskowych końca XX i początku XXI w. na tle bezpieczeństwa europejskiego – 15 zł
- J. Pawłowski, A. Ciupiński (red.) – Umiędzynarodowiony konflikt wewnętrzny – 20,00 zł
- M. Pelc, M. Juszczyk – Matematyka – 25 zł
- J. Płaczek – Ewolucja polskiej myśli obronno-ekonomicznej w latach 1976–2000 – 20,00 zł
- J. Płaczek (red.) – Gospodarka obronna Polski w końcu lat dziewięćdziesiątych. Szanse i zagrożenia – 25,00 zł
- Podróż studyjna w systemie edukacji oficerów w AON. Materiały z sympozjum naukowego – 17,00 zł
- A. Polak – Wybrane zagadnienia obrony wybrzeża w Polsce (1920–2002) – 16,00 zł
- A. Polak – Teoria grup operacyjnych w polskiej sztuce wojennej okresu międzywojennego – 30,00 zł
- Prawo w stosunkach międzynarodowych. Wybór dokumentów (praca zbiorowa) – 35,00 zł (dwa tomy)
- K. Przeworski – Ewakuacja jako sposób ochrony ludności – 7,00 zł
- Pułk przeciwlotniczy w działaniach operacyjnych (praca zbiorowa) – 20,00 zł
- A. Radomyski – Metody i treść pracy zespołu OPL na stanowisku dowodzenia dywizji zmechanizowanej – 18,00 zł
- A. Skrabacz – Kobiety w obronie narodowej Polski u progu XXI w. – 15,00 zł
- J. Skrzyp (red.) – Informator geograficzny o państwach kandydujących do Sojuszu Północnoatlantyckiego – 14,00 zł

- J. Skrzyp, Z. Lach – Informator geograficzny. Państwa członkowskie NATO – 20,00 zł
- Z. Skwarek – Powietrzne systemy wczesnego wykrywania i powiadamiania – 13,00 zł
- K. Słaboń – Sytuacja jeńców wojennych w konflikcie iracko-irańskim (1980-1988) – 10,00 zł
- Słownik terminów z zakresu bezpieczeństwa narodowego (praca zbiorowa) – 15,00 zł
- Słownik terminów z zakresu psychologii (praca zbiorowa) – 10,00 zł
- Słownik pojęć sojuszniczej obrony powietrznej (praca zbiorowa) – 12,00 zł
- H. Spustek – Wybrane zagadnienia badań operacyjnych i modelowania liniowego – 8,00 zł
- Z. Stachowiak – Metodyka i metodologia pisania prac kwalifikacyjnych (licencjackich, magisterskich i podyplomowych) – 9,00 zł
- Z. Stachowiak, J. Płaczek (red.) – Wybrane problemy ekonomiki bezpieczeństwa – 30,00 zł
- R. Stępień (red.) – Edukacja w wyższych szkołach wojskowych – 21,00 zł
- M. Strzoda (red.) – Wybrane terminy z zakresu dowodzenia i zarządzania – 7,00 zł
- M. Strzoda – Słownik nazw, skrótów i akronimów państw, instytucji, dowództw, jednostek organizacyjnych i osób funkcyjnych – 8 zł
- J. Suwart – Zarys obrony cywilnej w Polsce w latach 1920–1996 – 30,00 zł
- R. Szpyra – Powietrzna sztuka operacyjna wybranych państw – 15,00 zł
- Środki dowodzenia (praca zbiorowa) – 12 zł
- E.A. Wesołowska, A. Szerauc (red.) – Patriotyzm – Obronność – Bezpieczeństwo – 20,00 zł
- J. Wołejszo – Wybrane problemy procesu planowania i rozliczania działalności szkoleniowej na szczeblach taktycznych w SZ RP – 16 zł
- J. Wołejszo – Trening sztabowy dowództw szczebla taktycznego SZ RP – 17,00 zł
- J. Wołejszo – Wybrane aspekty projektowania struktury organizacyjnej zespołu dowodzenia stanowiska dowodzenia brygady zmechanizowanej – 11,00 zł
- J. Wołejszo – Wybrane problemy przygotowania i realizacji ćwiczeń sojuszniczych NATO – 16 zł
- J. Wołejszo, Z. Fiołna – Dowodzenie brygadą zmechanizowaną (pancerną) w obronie – 12,00 zł
- J. Wołejszo, Z. Fiołna – Dowodzenie brygadą zmechanizowaną (pancerną) w marszu – 15,00 zł
- Wojskowe wsparcie władz cywilnych i społeczeństwa. Materiały z seminarium – 20,00 zł
- Wojsko wobec polskiego października'56. Rezolucje, uchwały, listy (wybór, wstęp i opracowanie: E. J. Nalepa) – 30,00 zł
- J. Wojtasik (red.) – Studia z dziejów polskiej techniki wojskowej od XVI do XX wieku – 27,00 zł
- J. Wojtasik (red.) – Od Żółkiewskiego i Kosińskiego do Piłsudskiego i Petlury. Z dziejów stosunków polsko-ukraińskich od XVI do XX wieku – 20,00 zł
- M. Wrzosek – Działania rozpoznawcze na obszarze kraju – 10 zł
- M. Wrzosek – Organizacja pracy taktycznej komórki rozpoznania – 17 zł
- Wsparcie informacyjne obrony powietrznej. Materiały z sympozjum naukowego – 18 zł
- Wydział Lotnictwa i Obrony Powietrznej AON – Ewolucja dla postępu. Materiały z konferencji – 18 zł
- E. Zabłocki – Współczesne siły powietrzne – 13,00 zł
- S. Zalewski – Służby specjalne w państwie demokratycznym – 11,00 zł
- Założenia operacyjne do doktryny zasadniczej sił powietrznych (praca zbiorowa) – 10,00 zł
- L. Zapała – W rembertowskiej Alma Mater. Wspomnienia – 18,00 zł
- B. Zdrodowski, M. Marszałek – Operacje pozawojenne sił powietrznych – 16,00 zł
- J. Zieliński (red.) – Podstawowe założenia dydaktyki sztuki operacyjnej – 14,00 zł
- J. Zieliński – Wojska lądowe jako rodzaj sił zbrojnych – 14 zł
- J. Zuziak – Dzieje Instytutu Józefa Piłsudskiego w Londynie 1947–1997 – 25,00 zł

Zamówienia przyjmujemy telefonicznie lub pisemnie

ISBN 83-89423-40-5

AON Wydział Wydawniczy