AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ LOTNICTWA I OBRONY POWIETRZNEJ

Ppłk dr inż. Ryszard SZPYRA

OFENSYWNA WALKA INFORMACYJNA W DZIAŁANIACH POWIETRZNYCH

Opracowanie pod kryptonimem INFOOFENSYWA

WARSZAWA 2001

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ LOTNICTWA I OBRONY POWIETRZNEJ

Ppłk dr inż. Ryszard SZPYRA

OFENSYWNA WALKA INFORMACYJNA W DZIAŁANIACH POWIETRZNYCH

Opracowanie pod kryptonimem INFOOFENSYWA

WARSZAWA **2001**

Recenzent pracy:

płk dr hab. Marian CIEŚLARCZYK

Spis treści

Wstęp

Współczesna cywilizacja doświadcza niebywałej akceleracji zmian. Zmiany te wyciskają swoje piętno również w sferze rywalizacji i sposobów prowadzenia walki. Szczególnie wyraźnie obserwowanym zjawiskiem jest gwałtowny rozwój badań i praktycznych zastosowań walki informacyjnej.

Fundamenty współczesnego społeczeństwa[1] oparte są na dostępności do informacji, która zabezpiecza prosperującej ekonomii wzrost lub spycha słabą w uzależnienie od silniejszej. W dzisiejszej elektronicznie, wzajemnie połączonym świecie, informacja przemieszcza się z prędkością światła, jest nieuchwytną i niezmiernie wartościową. Dzisiejsza informacja jest ekwiwalentem wczorajszych fabryk, lecz jest dużo bardziej wrażliwa.

Wrażliwość tę wykorzystuje wyłaniająca się walka informacyjna. Nie istnieje powszechnie uzgodniona definicja walki informacyjnej. Jest jednak wspólna treść[2] 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 fizyczną destrukcję infrastruktury, która wykorzystywana jest przez przeciwnika do działań operacyjnych.

Największym zagrożeniem dla bezpieczeństwa informacji i systemów informacyjnych jest ofensywny komponent walki informacyjnej strony przeciwnej. Znajomość tego komponentu ułatwia racjonalne projektowanie przedsięwzięć informacyjnej obrony. Z punktu widzenia zainteresowań badawczych koncentrujących się na działaniach sił powietrznych szczególnie interesującym jest poznanie ofensywnego komponentu walki informacyjnej tych sił.

Biorąc pod uwagę powyższe ustalenia przyjęto, że **celem pracy jest określenie podstawowej charakterystyki ofensywnych działań informacyjnych sił powietrznych we współczesnych warunkach rozwoju cywilizacyjnego**.

---

[1] W. Schwartau, *Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age. Thunder's Mouth Press*, New York 1996, s. 28 – 32.
[2] R. Stark, *Future Warfare: Information Superiority through Info War*, http://www.smsu.edu.

Wiedza ta umożliwi projektowanie koncepcji informacyjnej obrony, jak też wyznaczanie kierunków rozwoju ofensywnych zdolności walki informacyjnej w siłach powietrznych. Wiedza ta stanowić będzie także podstawę do prowadzenia dalszych szczegółowych badań w tym obszarze. Służyć też będzie wsparciu procesu dydaktycznego. Z celu pracy wynikły główne problemy badawcze, którymi są:

- Jaka jest charakterystyka współczesnych działań informacyjnych sił powietrznych?
- Jaki charakter mogą mieć ofensywne działania informacyjne sił powietrznych w przyszłości?

Wyniki badań mogą być wykorzystane głównie w dwóch sferach - teoretycznej i praktycznej. W sferze teoretycznej winny służyć, jako podstawa do badań szczegółowych nad sposobami prowadzenia ofensywnej walki informacyjnej w siłach powietrznych oraz prowadzenia informacyjnej obrony w siłach powietrznych. Umożliwiać, więc powinny identyfikowanie odpowiednich zmian w treściach powietrznej sztuki operacyjnej i taktyki. Wyniki te mogą być także pomocne w formułowaniu doktryny Polskich Sił Powietrznych. W sferze praktycznej wyniki badań powinny służyć przede wszystkim celom dydaktycznym.

Badania prowadzono w oparciu o materiały naukowe stanowiące dorobek krajowych autorów. Odwoływano się także do źródeł zagranicznych zarówno o charakterze naukowym, jak i doktrynalnym. Dobór teoretycznych materiałów źródłowych służył przede wszystkim zidentyfikowaniu charakterystyki współczesnej ofensywnej walki informacyjnej sił powietrznych oraz sformułowaniu zarysu rozwoju tej walki.

Rezultaty badań przedstawiono w studium teoretycznym składającym się z wstępu, zakończenia oraz trzech rozdziałów merytorycznych i bibliografii.

W rozdziale pierwszym omówiono podstawowe uwarunkowania walki informacyjnej w działaniach powietrznych. Rozdział drugi poświęcony jest charakterystyce ofensywnych elementów walki informacyjnej we współczesnych działaniach bojowych. W rozdziale trzecim dokonano próby zarysowania przyszłego kształtu ofensywnej walki informacyjnej w działaniach powietrznych.

1. PODSTAWOWE UWARUNKOWANIA

Rozdział ten poświęcono omówieniu podstawowych uwarunkowań badanego zjawiska oraz identyfikacji najważniejszych założeń przyjętych w tych badaniach. Treści te prezentowane są w kolejnych podrozdziałach niniejszego rozdziału.

Podrozdział pierwszy identyfikuje wyłaniające się w wyniku rozwoju cywilizacyjnego nowe obszary walki.

Podrozdział drugi ujawnia istotę nowej wyłaniającej się cywilizacji i wynikające stąd wnioski.

Podrozdział trzeci zawiera treści założeń przyjętych w niniejszej pracy. Założenia te dotyczą rozumienia podstawowych kategorii walki informacyjnej odnoszących się do obszaru niniejszych badań.

1.1. Militarna eksploracja nowych obszarów walki

Nowe tysiąclecie rozpoczyna się w okresie zachodzącej rewolucji technologicznej i kulturowej. Powszechnie obserwowany jest niebywały ferment intelektualny w wielu obszarach ludzkiego myślenia. Ferment ten widoczny jest również w dyskusjach o sprawach militarnych. Toczy się obecnie wiele dysput dotyczących m.in. istoty wojny, form działań militarnych, militarnych działań pozawojennych, niemilitarnych działań wojennych. Refleksja teoretyczna jest często stymulowana wyprzedzającymi ją działaniami praktycznymi. Czasami można odnieść wrażenie, że nie nadąża ona za praktyką. Przyczyną tego jest obserwowana powszechnie akceleracja rozwoju cywilizacyjnego i pojawianie się w rezultacie tego coraz większej dynamiki zmian. Przeobrażenia, które w przeszłości zajmowały 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 języku wojskowym oznacza szczebel niższy niż taktyczny. Wkrótce jednak objęła swoim zasięgiem również najwyższe poziomy makro docierając do szczebla strategicznego. W

odpowiedzi na obserwowane zjawisko wiele środowisk i myślicieli podjęło wysiłek intelektualny nad badaniem tej sfery walki.

Jednakże nie jest to jedyny przykład nowych zjawisk. Głębokim i dynamicznym zmianom cywilizacyjnym towarzyszy też intelektualne poszukiwanie nowych idei. Nie jest ono obce i środowisku militarnemu. W militarnych kręgach intelektualnych Zachodu popularny jest postulat „*outside box thinking*", co w luźnym 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 też 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"[3]. Ze względu na szeroki rezonans, jaki publikacja ta wywołała w środowiskach militarnych Zachodu i znaczną oryginalność warto przytoczyć najistotniejsze tezy ich wywodu. Mają one ponadto bezpośredni związek z prezentowaną sytuacją problemową.

Ogólnie rzecz biorąc wysoko rozwinięte technologie nie mogą stać się synonimem przyszłej walki. Nawet technologie informacyjne będące ostatnio wizytówką współczesnej walki nie są wystarczające by tworzyły przyszłą wojnę. Nawet, jeżeli w przyszłych wojnach wszystkie bronie będą miały komponenty informacyjnej technologii i będą w pełni skomputeryzowane nie będzie to tworzyło walki informacyjnej. Taką walkę będziemy mogli nazwać, co najwyżej skomputeryzowaną. Bo pocisk Tomahawk dalej pozostaje pociskiem a samolot nawet najnowocześniejszy jak F-22 jest w dalszym ciągu jedynie myśliwcem. Skomputeryzowana walka i informacyjna walka to dwa zupełnie odmienne zjawiska. O ile ta pierwsza odnosi się do wielu form walki, które są wspierane i wzmacniane przez technologie informacyjne o tyle ta druga odnosi się głównie do wojny, w której technologia informacyjna używana jest bądź do uzy-

---

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

skania informacji bądź do jej degradacji.

W porównaniu do broni nowych koncepcji niemalże wszystkie dotychczas znane bronie mogą być traktowane jako bronie starej koncepcji walki. Powodem tego jest fakt, iż podstawowe funkcje tych broni dalej sprowadzają się do mobilności i destrukcyjności. Nawet precyzyjnie kierowane bomby i inne bronie wysoko rozwiniętej technologii w dalszym ciągu wypełniają te same funkcje.

Wszystkie te bronie i platformy ich przenoszenia, które powstały na bazie tradycyjnego myślenia okażą się w ostateczności nie przydatne do współczesnej i przyszłej walki. Założenie oparte na wykorzystaniu magicznej, wysoko rozwiniętej technologii mającej zaadaptować stare bronie do nowych potrzeb okazało się błędne. Wpadło, bowiem w pułapkę niekończącej się spirali wydatków i wyścigu zbrojeń. Jest to paradoks, któremu należy stawić czoła w procesie rozwoju tradycyjnych broni.

Aby zapewnić nowoczesność tych broni należy ciągle zwiększać wydatki, co w ostateczności powoduje, że nikt nie posiada takich pieniędzy by nadążyć za postępem technologicznym. W ostatecznym rachunku bronie takie zamiast zapewniać bezpieczeństwo kraju stają się w ostateczności powodem jego bankructwa.

Ilustruje to dobitnie przykład Związku Radzieckiego gdzie nowe, rozsądne koncepcje marszałka Ogarkowa zostały odrzucone na rzecz intensyfikacji wyścigu zbrojeń ze Stanami Zjednoczonymi w rezultacie, czego ta potęga upadła bez jednego wystrzału.

Obecnie staje się coraz bardziej jasnym, że Amerykanie inwestują coraz więcej i więcej w nowe bronie a ich koszt staje się coraz wyższy i wyższy. Wyprodukowanie samolotów F-14 i F-15 kosztowało miliard dolarów, podczas gdy koszt jednego B-2 wynosi ponad dziesięć miliardów dolarów, a koszt rozwoju F-22 przekroczył już 13 miliardów dolarów. Samolot B-2 jest trzy razy droższy niż porównywalna wagowo ilość złota. To tylko nieliczne przykłady bogatego arsenału Stanów Zjednoczonych i popadania w pułapkę rosnących kosztów nadążania za rozwojem nowych technologii. Jeżeli staje się to coraz trudniejsze dla Stanów Zjednoczonych to tym bardziej problematyczne dla biedniejszych krajów. Jedynym wyjściem z tej pułapki jest poszukiwanie innego podejścia. I tu Amerykanie osiągnęli wiele.

Jednakże Amerykanie nie przewodzą we wszystkim. Nowa koncepcja broni nie opiera się na osiągnięciach nowych technologii, lecz na przytomnym i twórczym myśleniu. Nie osiągnie tego ten, kto jest przywiązany do starego myślenia i jest niewolnikiem technologii. Nie można przecież zaprzeczyć, że sprowokowane przez człowieka trzęsienia ziemi, katastrofy ekologiczne i pogodowe, fale dźwiękowe oraz nowe bronie biologiczne i chemiczne tworzyć będą bronie nowych koncepcji. Jednak mimo istotnej różnicy w skali oddziaływania to są one dalej klasycznymi broniami, które zabijają i niszczą a ponadto są związane ze sprawami militarnymi, wojskiem, amunicją. Także są one nietradycyjnymi broniami o zwielokrotnionej sile rażenia.

Tymczasem bronie nowych koncepcji to przede wszystkim szeroki kontekst ich postrzegania, który jako broń traktuje wszystko, co wykracza poza sferę militarną jednakże, co może być użyte w działaniach militarnych. W tym kontekście wszystko, co może przynosić korzyść człowiekowi może mu także szkodzić. Oznacza to, że praktycznie nie ma niczego takiego na świecie, co nie mogłoby być bronią. Takie rozumienie broni wymaga świadomości, która przekracza wszelkie bariery. Przecież spowodowany przez jednego człowieka kryzys giełdowy, pojedynczy atak wirusowy lub wywołana plotka czy skandal powodujące fluktuacje kursu walutowego to są wszystko bronie nowej koncepcji. W tym ujęciu technologia nie jest już głównym czynnikiem. Jest nią natomiast nowa koncepcja broni.

Ta nowa koncepcja prowadzi do wykreowania broni, które są blisko związane z życiem zwykłych ludzi. Bronie takie ulokują przyszłą walkę na poziomie, który jest trudny do wyobrażenia dla zwykłych ludzi. Bronie te sprawią wielkie zdziwienie i zaskoczenie zwykłych ludzi a także i wojskowych tym, że rzeczy powszechnie występujące wśród zwyczajnych ludzi mogą również stać się broniami, które biorą udział w wojnie. Panuje przekonanie, iż kiedyś nagle ludzie spostrzegą ze zdziwieniem, że do niedawna całkiem przyjemne i miłe rzeczy przybrały nagle inny bardzo dokuczliwy charakter.

Pojawienie się precyzyjnych środków rażenia oraz broni niezabójczych jest punktem zwrotnym w rozwoju broni. Właściwie jest to pierwszy przypadek, gdy bronie rozwijają się w kierunku łagodzenie a nie zaostrzania zabójczości. Bronie precy-

zyjne mogą uderzyć w obiekt ataku z dużą precyzją ograniczając przez to niepotrzebne szkody wyrządzane przypadkowo przy takim uderzeniu. Przykładem, czego może być atak na Dudajewa wykonany pociskiem, który naprowadził się na używany przez niego telefon komórkowy. Bronie niezabójcze mogą efektywnie eliminować zdolności bojowe personelu i sprzętu bez konieczności zabijania ludzi.

Pojawienie się tego typu broni świadczy o tym, że ludzkość zaczyna przełamywać swoje ekstremalne myślenie i zaczyna rozumieć potrzebę ograniczania skali zabójczości, potencjał, której drastycznie się zwiększa. W czasie trwających ponad miesiąc intensywnych bombardowań Iraku straty ludności cywilnej były znacznie niższe niż w czasie jednego zmasowanego bombardowania Drezna w II wojnie światowej. Łagodniejsze bronie są rezultatem świadomych wyborów dokonywanych w ostatnim czasie przez ludzkość. Jednakże tego typu środki pozostają w dalszym ciągu broniami i dążenie do bycia niezabójczą bronią nie oznacza rezygnacja ze wzrostu jej skuteczności bojowej. Aby wyeliminować czołg z walki można go zniszczyć pociskiem lub oślepić jego przyrządy optyczne i załogę promieniem lasera. Na polu walki ranni sprawiają więcej kłopotu niż zabici a bezzałogowe aparaty, czyli bronie roboty mogą pokonywać coraz droższe i lepsze zabezpieczenia obronne. Ci, którzy zaczęli rozwijać niezabójcze bronie na pewno dokonali chłodnej kalkulacji koszt-efekt dla zastosowania tych broni.

Obecnie ludzkość dysponuje bogatą gamą technologii, które mogą wywoływać lęk i strach. Wymaga to jedynie nieco wyobraźni w modyfikacji i zastosowaniu znanych już technologii. Tego typu bronie są intensywnie rozwijane. Czyni się to jednak najczęściej skrycie. Jest jednak wystarczająco dużo sygnałów potwierdzających to zjawisko. Przykładem mogą być bronie informacyjne. Obejmują one zarówno bronie oparte na energii elektromagnetycznej jak i na różnych rodzajach oprogramowania komputerowego, a także na oddziaływaniach medialnych. Cała gama oddziaływań informacyjnych koncentruje się na paraliżowaniu a nie na tworzeniu ofiar ludzkich. Ten kierunek rozwoju broni jest bardzo interesującym i najbardziej obiecującym trendem w rozwoju broni. Przynieść on może trudne do wyobrażenia formy prowadzenia wojny i spowoduje rewolucyjne zmiany w sferze militarnej.

Jednakże wojna w dalszym ciągu pozostaje sprawą przeżycia lub śmierci, przetrwania lub zguby. Jeżeli nawet kiedyś w przyszłości stosować się będzie jedynie bronie humanitarne, czyli niezabójcze a wojny staną się bezkrwawymi to będą one w dalszym ciągu wojnami. Może zaniknąć okrutność procesu wojny jednakże nie zmieni się istota wojny, którą jest przymus i dlatego też nie zmieni to okrutności rezultatów wojny.

W przeszłości wojny toczono dla osiągnięcia różnych stosunkowo jasnych celów. Jeżeli czegoś nie można było osiągnąć pokojową drogą sięgano po przemoc i stosowano przymus. Clausewitz uogólnił historyczne doświadczenia twierdząc, że wojna jest kontynuacją polityki. Nasi przodkowie walczyli jednak zarówno w celach religijnych, dla zdobycia zasobów a nawet z powodu spraw miłosnych między królem a królową. Historia zanotowała przypadki rebelii o rum czy kampanii o dostęp do przypraw. Niemcy pod przywództwem Hitlera prowadzili wojnę o uzyskanie przestrzeni życiowej dla narodu niemieckiego. Japończycy z kolei chcieli budować większą sferę wpływów w Azji. Mimo większego rozmachu to cele wojny sprowadzały się do poszerzenia swojej sfery wpływów oraz czerpania korzyści z opanowanych terytoriów.

Dzisiaj odpowiedź na pytanie, o co się toczą walki i kto jest wrogiem nie jest w wielu wypadkach łatwa. Upadł komunizm nie toczą się, więc wojny o ekspansję komunizmu. Kraj, który był sojusznikiem może się stać w krótkim czasie wrogiem. Jest na to wiele przykładów. Stosunki między Irakiem, Iranem czy Afganistanem a Stanami Zjednoczonymi, ilustrują dobitnie ową zmienność podobnych przykładów znaleźć można więcej. Potwierdza to znaną prawdę, że przyjaźnie są zmienne stałe są tylko interesy.

Ponieważ kalejdoskop interesów ulega rozmyciu w procesach globalizacji i zmian cywilizacyjnych. Pojawiają się też nowe interesy. Powodem przyszłej wojny może być zarówno spór o terytoria czy zasoby, spory ideologiczne, spory o rynki zbytu, konflikty religijne, etniczne, spory o władzę, sankcje handlowe czy konflikty rodzące się z zakłóceń finansowych. Bezpośrednie cele walki mogą być ponadto maskowane innymi publicznie deklarowanymi.

Współcześnie największa różnica między wojnami przeszłości a teraźniejszości polega na tym, że publicznie głoszony i rzeczywisty, ukryty cel współczesnych wojen to dwie różne sprawy.

Przez długi okres czasu 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.

Jest oczywistym, że mechaniczne rozszerzanie istniejących przestrzeni walki nie jest perspektywą przyszłych zmian. Nawet przeniesienie walki w głębiny oceanu czy w otwartą przestrzeń kosmiczną nie zmieni faktu dalszego pozostawania w sferze ograniczeń praw fizyki.

Prawdziwie rewolucyjną zmianą jest przeniesienie pola walki do nienaturalnych przestrzeni. Trudno na przykład uznać przestrzeń elektromagnetyczną za naturalną przestrzeń fizyczną w dotychczasowym jej rozumieniu. Przestrzeń elektromagnetyczna jest sztuczną, stworzoną przez człowieka przestrzenią. W przestrzeni tej takie wymiary jak długość, szerokość, wysokość nie mają sensu.

Należy zgodzić się, co do tego, że każde przyszłe rozszerzenie przestrzeni walki zależeć będzie od nowych odkryć i wynalazków, które tworzyć będą nową, technologiczną przestrzeń. Przestrzeń sieciowa obecnie skupia uwagę współczesnych żołnierzy. Przestrzeń ta jest wytworem człowieka powstałym przez połączenie elektroniki, technologii informacyjnych i zastosowania specyficznych konstrukcji i organizacji. Kolejną bardziej "egzotyczną" może być nanoprzestrzeń. Umożliwi ona prowadzenie wojny bez bezpośredniego udziału ludzi w niej. Niewielkie grona najbardziej twórczych i wykształconych żołnierzy intensywnie i bez rozgłosu pracuje nad otwarciem tej przestrzeni dla walki przyszłości.

Czas fundamentalnych zmian przestrzeni walki nie jest odległym. W przeszłości walka w przestrzeni sieci informacyjnych czy walka w przestrzeni nano była trudna do wyobrażenia, a tymczasem na naszych oczach stawać się będzie rzeczywistością.

Prawdopodobnie walka ta będzie miała bardzo intensywny charakter jednakże będzie zasadniczo bezkrwawą. Będzie jednakże rozpoznawalny wynik. Można będzie zidentyfikować, kto jest zwycięzcą a kto pokonanym w ogólnej wojnie. Coraz częściej nowe, tego typu 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 stosowane w nich zjawiska. Tworzyć to będzie niezwykle bogate, nieznane w historii ludzkości pole walki.

Jednocześnie, wraz z postępującym zacieraniem różnic pomiędzy technologią wojskową i cywilną oraz między profesjonalnym żołnierzem i nieprofesjonalnym wojownikiem przestrzeń walki coraz bardziej będzie się mieszać z innymi przestrzeniami, w których nie toczy się walka. Granice ograniczające przestrzenie walki będą zanikać. Walka obejmować będzie przestrzenie cywilnej sfery działalności. Stopniowo walka obejmie wszystkie przestrzenie ludzkiej aktywności. Wszystko, czego będzie potrzeba to posiadania pewnych zdolności do wykonania ataku w określonej sferze, przy użyciu odpowiednich środków dla osiągnięcia niezbędnego celu. Przestrzeń walki staje się, więc wszechobecna. Stopniowo pole walki będzie wszędzie, obejmując wszystkie sfery ludzkiej aktywności.

Obecnie świat jest widownią wielkich redukcji liczebności sił zbrojnych. Wielu komentatorów uznaje, że społeczeństwa po zakończeniu zimnej wojny konsumują dywidendę pokoju. Jednakże jest to tylko wierzchołek góry lodowej. Głównym powodem tych redukcji jest, bowiem gwałtownie narastająca fala rozwoju technologii walki informacyjnej. Wymaga ona zbyt wiele wysiłku, aby jednocześnie można było utrzymywać wielkie profesjonalne armie uzbrojone odpowiednio do potrzeb walki zmechanizowanej. Dokładnie z tego powodu w czasie redukcji sił zbrojnych niektóre dalekowzroczne kraje zamiast mechanicznej redukcji personelu koncentrują się raczej na podnoszeniu jego jakości kosztem ilości, oraz na zwiększaniu udziału nowych generacji uzbrojenia w swoich arsenałach a także na rozwoju myśli i teorii walki.

Era silnych i dzielnych żołnierzy, którzy są heroicznymi obrońcami ojczyzny już minęła. W świecie gdzie nawet pojęcie walka jądrowa stanie się zbędnym żargo-

nem militarnym jest prawdopodobnym, że blado wyglądający uczeń noszący grube okulary lepiej pasuje na współczesnego żołnierza niż silny młodzieniec z rozbudowanymi bicepsami. Najlepszym potwierdzeniem tego jest historia przytaczana w wojskowych środowiskach Zachodu o tym jak młody porucznik używając modemu rzucił dywizję marynarki na kolana.

Kontrast między dzisiejszym żołnierzem a żołnierzem poprzednich generacji jest podobny do tego, jaki występuje pomiędzy współczesną bronią a jej poprzednikami. Kontrast ten uwidacznia się w sposobie oceny żołnierza kiedyś głównie fizycznej a obecnie intelektualnej. Mimo iż nowa generacja amerykańskich żołnierzy urodzonych w latach 70-tych i 80-tych szkolona była według najlepszych wzorców akademii West Point to jest dla niej trudno porzucić ich łagodną i delikatną naturę zakorzenioną w duchu współczesnego społeczeństwa. Ponadto nowoczesne systemy broni umożliwiły im przebywanie z dala od konwencjonalnego pola walki. Mogą oni atakować nieprzyjaciela z dystansu nie będąc skazanymi na walkę z widokiem krwi u niszczonego przeciwnika. Obecnie cyfrowy wojownik przejmuje rolę niegdysiejszego wojownika krwi i stali, rolę, która nie zmieniała się przez tysiąclecia.

Obecnie tradycyjne podziały ról w społeczeństwie, charakterystyczne dla społeczeństwa epoki przemysłowej zanikają. Również walka przestaje być domeną jedynie żołnierzy. Tendencja w kierunku ucywilniania walki jest wyraźnie widoczna. Nie oznacza to potrzeby rozległej mobilizacji ludzi. Czasami wprost przeciwnie technologiczne elity społeczeństwa przełamały bariery i wdarły się w obszar zastrzeżony do tej pory dla żołnierzy stawiając wojsko w kłopotliwej sytuacji. Kto będzie głównym przeciwnikiem nieznanej krainy następnej wojny? Pierwszym, który się wyłania i najsławniejszym staje się haker komputerowy. Ten ktoś, kto zwykle nie przeszedł żadnego przeszkolenia wojskowego i nie wykonuje żadnej pracy związanej ze sferą militarną może łatwo osłabić bezpieczeństwo sił zbrojnych a nawet państwa. Może tego dokonać wykorzystując jedynie swoje osobiste umiejętności i wiedzę informatyczną. Amerykańska doktryna sił lądowych w zakresie działań informacyjnych przytacza wiele przykładów tego typu.

W dekadzie lat dziewięćdziesiątych, wraz z serią działań militarnych przeprowadzonych przez niewojskowych wojowników i pozarządowe organizacje zaczęliśmy wchodzić w okres wojen typu niemilitarnego. Wojny te prowadzone są również przez jeszcze inny typ ludzi spoza wojska. Ludzie ci nie są hakerami ani też nie są członkami organizacji paramilitarnych. Mogą być specjalistami analizy systemów, inżynierami programistami czy finansowcami lub maklerami giełdowymi dysponującymi dużą ilością wolnego kapitału. Mogą też być magnatami dysponującymi wielkimi wydawnictwami prasowymi i stacjami telewizyjnymi czy też sławnymi komentatorami czy felietonistami. Jego czy jej filozofia życia jest inna od ślepej i niehumanitarnej, jaką wyznają terroryści. Często ludzie ci wyznają i realizują twardą i stanowczą filozofię życia i ich przekonania w sferze fanatyzmu nie różnią się od fanatyzmu Osama bin Ladin`a. Co więcej nie brakuje im motywacji i odwagi by rozpocząć walkę, jeśli zaistnieje taka potrzeba. W oparciu o takie kryteria oceny, kto może zaprzeczyć, że George Soros jest finansowym terrorystą.

Tak samo jak współczesna technologia zmienia bronie i pole walki tak samo zamazuje obraz tego, kto prowadzi i bierze udział w wojnie a kto nie. Już teraz żołnierz stracił monopol na prowadzenie wojny. Globalna działalność terrorystyczna jest jednym z produktów globalizacji. Trend ten nie został wprowadzony w wyniku rozwoju technologicznego. Nieprofesjonalni wojownicy i organizacje pozarządowe niosą coraz większe zagrożenie dla suwerennych państw i stają się coraz poważniejszymi przeciwnikami każdych profesjonalnych sił zbrojnych. W porównaniu z tymi przeciwnikami profesjonalne siły zbrojne wyglądają jak gigantyczne dinozaury, które brak odpowiedniej zdolności i siły rekompensują swoją wielkością. Ich przeciwnicy zachowują się, więc jak gryzonie z wielką wolą przetrwania, które mogą używać swoich ostrych zębów by dręczyć lepszą część świata.

Jeśli chodzi o środki i metody, jakie będą używane w przyszłych wojnach warto sięgnąć po amerykański dorobek gdyż w porównaniu do teoretycznego dorobku środowisk militarnych innych państw amerykański jest rzeczywiście najlepszy. Amerykanie zidentyfikowali cztery główne formy prowadzenia wojny, czyli rodzaje walki. Należą do nich: walka informacyjna, walka precyzyjna, działania połączone i militarne działania pozawojenne. Szczególnie ta ostatnia forma świadczy o dużej wyobraźni i

bardzo praktycznym podejściu Amerykanów. Oprócz działań połączonych, które ewoluowały z tradycyjnych działań prowadzonych w ramach współdziałania różnych rodzajów sił zbrojnych pozostałe trzy formy prowadzenia wojny mogą być uznane za produkt nowego myślenia militarnego.

Generał Gordon R. Sullivan uznaje, że walka informacyjna będzie podstawową formą prowadzenia wojny w przyszłości. Dlatego też zorganizował on najlepsze na świecie cyfrowe wojska. Ponadto zaproponował on koncepcję walki precyzyjnej zakładając, że nastąpi ogólny zwrot w kierunku przetwarzania informacji oraz niewidzialnych ataków na duże odległości, co stanie się fundamentem przyszłej walki.

Pojawienie się nowego, wykorzystującego nowoczesne technologie uzbrojenia takiego jak precyzyjnie kierowane uzbrojenie, system precyzyjnej nawigacji GPS, systemy C4I, samoloty niewidzialne umożliwi Amerykanom rozproszenie żołnierzy i uniknięcia koszmaru walki na wyniszczenie. Precyzyjna walka, która nazwana została przez Amerykanów "atakiem bez kontaktu" oraz "zdalną walką" przez Rosjan, charakteryzowana jest przez takie cechy jak skrytość, prędkość, dokładność, wysoki stopień efektywności i niewielkie straty towarzyszące. W wojnach przyszłości ich wynik znany będzie dosyć często w krótkim czasie po ich rozpoczęciu a stosowane sposoby walki w wojnie z Irakiem będą tymi, po które amerykańscy generałowie będą często sięgali.

Jednakże formą, która jest produktem szczególnie bogatego w wyobraźnię myślenia są militarne działania pozawojenne. Koncepcja ta jest w szczególny sposób oparta na globalnych interesach, na które Amerykanie nieustannie się powołują.

Niezależnie od tego znaczenie tej koncepcji jest znaczne gdyż po raz pierwszy kompleksowo podchodzi do problemów XX i XXI wieku. Umieszczone one zostały w przedziale zwanym militarne działania pozawojenne, co wskazuje drogę postępowania siłom zbrojnym we wszelkich sytuacjach nie związanych z polem walki. Jednakże koncepcja ta nie obejmuje pozamilitarnych działań wojennych (non-military war operations). Dopiero koncepcja tych działań w swojej istocie poszerza rozumienie wojny i jest niezwykle ważna, bo zmienia istniejącą percepcję wojny.

Różnica pomiędzy koncepcją "pozamilitarnych działań wojennych" a "pozawojennych działań militarnych" (military operations other than war) jest dużo większa niżby na to wskazywały pobieżne analizy. Koncepcja "pozawojennych działań militarnych" to szyld, pod którym w warunkach braku stanu wojny mogą być prowadzone wszelkie działania militarne i wykonywane przez siły zbrojne różne misje. Koncepcja "pozamilitarnych działań wojennych" rozszerza rozumienie tego, co dotychczas było uznawane za wojnę. Koncepcja wojny w nowym rozumieniu wkracza niemalże w każdy obszar ludzkiej aktywności i obejmuje obszary położone daleko poza tym, co do tej pory rozumiano pod nazwą działania militarne. Rozszerzenie tego typu jest w istocie naturalnym rezultatem tego, że ludzie użyją wszelkich możliwych środków i sposobów by osiągnąć swoje cele.

Jakie więc są to przedsięwzięcia, które wydawałoby się, iż bezpośrednio nie związane z wojną stają się jednak ulubioną bronią wojen nowego typu – "pozamilitarnych działań wojennych?. Która broń jest często i coraz częściej stosowana na całym świecie?

Wojna handlowa. Warto zauważyć, że jeszcze kilkadziesiąt lat temu "wojna handlowa" była głównie kategorią opisową a obecnie stała się rzeczywistym narzędziem prowadzenia niemilitarnej walki przez wiele państw. Szczególnie skutecznie używają jej Amerykanie, którzy doprowadzili ją niemalże do mistrzostwa. Do niektórych form jej prowadzenia należą: użycie wewnętrznego prawa handlowego na arenie międzynarodowej. Arbitralne tworzenie i demontowanie barier celnych, używanie pośpiesznie montowanych sankcji handlowych, nakładanie embarga na eksport technologii, wykorzystywanie Sekcji Specjalnej 301 prawa, stosowanie klauzuli najwyższego uprzywilejowania itp. Całkowite wieloletnie embargo przeciwko Irakowi jest tu klasycznym podręcznikowym przykładem w tym względzie.

Wojna finansowa. W czasie, gdy Azjaci doświadczyli finansowego kryzysu w południowo-wschodniej Azji nikt nie był bardziej dotknięty "wojną finansową" niż oni. Właściwie to nie tylko dotknięci, lecz dotknięci do żywego. Niespodziewany atak wojny finansowej, który został celowo zaplanowany i wykonany przez właścicieli międzynarodowego ruchomego kapitału rzucając na ziemię jedno państwo za drugim.

Dotyczyło to państw, które jeszcze nie tak dawno nazywane były "Azjatyckimi Tygrysami" lub "Małymi Smokami". Ekonomiczny rozwój, który jeszcze nie tak dawno wzbudzał podziw zachodniego świata zamienił się w depresję. Państwa te w krótkiej chwili padły jak wielkie drzewo w czasie jesiennego sztormu. Po jednej rundzie walki ekonomie wielu krajów zostały cofnięte w rozwoju o dziesięć lat. Co więcej taka klęska na ekonomicznym froncie spowodowała niemalże rozpad porządku społecznego i politycznego. Skala ofiar tego chaosu jest nie mniejsza niż spowodowana wojną regionalną a rany zadane żywym organizmom społecznym nawet przekraczają poziom, jaki mogłaby pociągnąć za sobą taka wojna.

Organizacje pozarządowe w tej ich pierwszej wojnie bez użycia siły militarnej używają niemilitarnych środków do zaatakowania suwerennych krajów. Dlatego też wojna finansowa jest formą niemilitarnej walki, która jednakże jest tak samo destrukcyjna jak krwawa wojna, jednakże, w której krew nie jest w niej przelewana. Walka finansowa stała się obecnie główną areną wojny, areną, która dotychczas przez tysiąclecia była miejscem zarezerwowanym dla żołnierzy i broni, na której masowo obecna była krew i śmierć. Jesteśmy przekonani, że niedługo „walka finansowa" stanie się jedną z podstawowych kategorii sfery militarnej.

W przyszłości, gdy sięgniemy do historii końca XX i początku XXI wieku to się okaże, że głównym protagonistą walki finansowej był nie jakiś strateg militarny, lecz George Soros. Oczywiście Soros nie ma monopolu na używanie finansowej broni do prowadzenia wojen. Jeszcze przed Soros`em Helmut Kohl użył marki niemieckiej do przełamania Berlińskiego Muru, muru którego nikt nie był w stanie obalić artyleryjskimi pociskami. Podobnej broni w Azji użył także Li Denghui do przeprowadzenia ataku na walutę Hong Kongu. Ponadto należy także odnotować tłum mniejszych i większych spekulantów, włączając w to Morgan Stanley oraz Moody`s, słynące ze swoich raportów wskazujących obiecujące obiekty ataku dla zdobycia korzyści przez grube ryby finansowego świata. Te dwie firmy są typowymi przedstawicielami aktorów, którzy biorą bezpośredni udział w tej wielkiej uczcie i zbieraniu korzyści.

Latem w 1998 roku po rozpoczęciu ponad rocznej walki finansowej wojny bitwy drugiej rundy tej wojny zaczęły się rozwijać na jeszcze większą skalę. Dwa gigan-

ty Rosja i Japonia zostały również najechane. Zachwiało to jeszcze bardziej ekonomiczną sytuacją świata. Tym razem "ślepe ognie spaliły mało warte czeki tych, którzy posługiwali się ogniem". Jak się okazało Soros i jego "Quantum Fund" jedynie w Rosji i Hong Kongu utracili, co najmniej kilka miliardów dolarów. Obrazuje to skalę i rozmach destrukcyjnej potęgi finansowej wojny.

Obecnie, gdy broń jądrowa stała się jedynie przerażająca dekoracją, która z każdym dniem traci swoje realne znaczenie operacyjne, wojna finansowa stała się "hiperstrategiczną" bronią, która rodzi zainteresowanie świata. Dzieje się tak, bo wojna finansowa jest łatwa do manipulowania i umożliwia skryte działania. Jest także wielce destrukcyjna. Analizując chaos w Albanii, jaki tam niedawno zapanował jasno widać rolę, jaka odegrały różne typy fundacji ustanowionych przez międzynarodowe grupy milionerów z dochodami porównywalnymi do niektórych państw. Fundacje te kontrolują media, subsydia dla politycznych organizacji i minimalizują opór władz prowadząc przez to do zapaści społecznego porządku i upadku legalnie wybranych władz. Coraz większa częstotliwość i intensywność tego typu wojen oraz to, że coraz więcej krajów i organizacji pozarządowych celowo je prowadzi budzi niepokój. Sprawia także, że musimy im coraz częściej stawiać czoła.

Nowy i tradycyjny terroryzm formą współczesnej wojny. Z powodu ograniczonej skali tradycyjnej wojny terrorystycznej skala jej ofiar bywa z reguły dużo mniejsza niż wojny konwencjonalnej. Jednakże tradycyjna wojna terrorystyczna niesie za sobą znaczny ładunek przemocy, bo nie liczy się z żadnymi regułami życia społecznego. Z militarnego punktu widzenia tradycyjna wojna terrorystyczna jest charakteryzowana przez użycie ograniczonych zasobów do prowadzenia nieograniczonej wojny. Ta cecha stawia narodowe siły w bardzo niekorzystnej sytuacji, bo siły te zawsze muszą przestrzegać pewnych praw i dlatego też nawet używając nieograniczonych środków mogą prowadzić jedynie ograniczona wojnę. To tłumaczy, dlaczego terrorystyczne organizacje używając nawet ograniczonej ilości niedoświadczonych terrorystów mogą sprawić wiele problemów nawet takim krajom jak Stany Zjednoczone oraz dlaczego używanie "ciężkiego młota" dla zabicia mrówki często okazuje się być nieefektywne. Niedawne przypadki dwóch eksplozji w rejonie amerykańskich ambasad w

Nairobi i Dar es Salaam są tego przykładem. Pojawienie się terroryzmu w stylu bin Ladin`a sprawia, że trudno jest wygrywać w grze, która nie ma reguł.

Jednakże, gdy wszyscy terroryści ograniczą swoje działania do klasycznych metod to będziemy mieli do czynienia jedynie z wielkim natężeniem terroru. Co rzeczywiście uderzyć może w serca społeczeństw jest połączenie terrorystów z całą gamą nowych technologii. Taki mariaż niesie ze sobą nową superbroń. Próbą tego, co może być stosowane było użycie przez sektę Aum Shinrikyo sarinu w tokijskim metrze. Tylko częściowe zadziałanie ładunków przyniosło przerażające rezultaty. Przypadek ten zwraca uwagę na osiągnięcia nowoczesnej biochemii, które odpowiednio wykorzystane przez terrorystów stanowić będą zabójczą broń zdolną do masowego niszczenia ludności. Inne grupy terrorystów poruszają się w zupełnie odmiennej sferze. Atakują oni informacyjną infrastrukturę współczesnej cywilizacji wprowadzając chaos i zamęt. Te nowe formy terroryzmu rodzą wojnę nowego terroryzmu.

Wojna ekologiczna odnosi się do nowego typu niemilitarnej walki, w której nowoczesne technologie są stosowane dla wywarcia wpływu na stan rzek, oceanów, skorupy ziemskiej, polarnych czap lodowych, cyrkulacji powietrza w atmosferze, czy warstwy ozonowej. Wywołując trzęsienia ziemi, nienaturalne opady deszczu, niezwykłe zmiany temperatur i inne podobne zjawiska niszczy się naturalne środowisko fizyczne i tworzy sztuczne sfery ekologiczne. Być może niedługo wywołany przez człowieka efekt El Nino czy La Nina stanie się nową superbronią w rękach niektórych państw lub organizacji pozarządowych. Jest bardziej prawdopodobnym, że organizacje pozarządowe staną się głównym inicjatorem wojny ekologicznej. Organizacje te często cechuje terrorystyczna natura, nie ponoszą one odpowiedzialności przed społeczeństwami a praktyka wskazuje, że nie są one skłonne do przestrzegania istniejących reguł. Z powodu dążenia wielu państw do jak najszybszego rozwoju ekonomicznego samo środowisko coraz bardziej znajdować się będzie na skraju równowagi. W tym stanie nawet niewielkie zmiany czynników tego środowiska mogą powodować ekologiczny holocaust.

Ponadto pojawia się jeszcze wiele innych środków i metod prowadzenia niemilitarnej wojny. Niektóre z nich już istnieją inne pojawią się w przyszłości. Należą

do nich m.in. walka psychologiczna, walka przemytnicza (prowadząca do zachwiania rynku i ekonomicznego porządku), walka medialna (manipulowanie tym, co ludzie widzą i słyszą dla kierowania nimi), walka narkotykowa (uzyskiwanie szybkich i znacznych nielegalnych profitów z rozprzestrzeniania katastrofy w innych krajach), walka sieciowa (w sieciach informacyjnych), walka technologiczna (tworzenie monopolu przez niezależne ustanawianie standardów), walka surowcowa (grabież zasobów i dóbr innych), walka pomocą ekonomiczną (jawne obdarowywanie kogoś przy skrytym zdobywaniu kontroli), walka kulturowa (kreowanie i narzucanie trendów kulturowych w celu asymilowania tych, którzy reprezentują inny punkt widzenia), walka prawem międzynarodowym i inne temu podobne. Paleta form niemilitarnej wojny jest tak obszerna, 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. Ponadto możliwe jest także twórcze stosowanie różnych mieszanych form walki, co jeszcze bardziej wzbogaca arsenał walki.

Co ważniejsze wszystkie te formy prowadzenia walki z korespondującymi z nimi praktycznymi działaniami, które weszły, wchodzą bądź wejdą do arsenału środków walki służących do prowadzenia wojny, już zaczęły niezauważalnie zmieniać wyobrażenie o walce prowadzonej w ludzkiej cywilizacji. Mając do wyboru niemalże nieograniczone możliwości wyboru dogodnej formy prowadzenia walki, dlaczego ludzie mieliby się ograniczać do wyboru form, które ograniczają się do sfery sił zbrojnych i potęgi militarnej. Przecież formy, które nie charakteryzują się użyciem sił zbrojnych i potęgi militarnej, a nawet nie związane są z obecnością przelewu krwi i ofiar, tak samo gwarantują pomyślne osiąganie celów wojny a nawet osiąganie większych korzyści niż przy użyciu potęgi militarnej.

Automatycznie prowadzi to do rewizji tezy, że „wojna jest krwawą formą polityki" oraz zmiany dotychczasowego postrzegania walki prowadzonej przez siły zbrojne jako ostatecznego środka rozwiązywania konfliktów. To różnorodność środków i form możliwych do skutecznego stosowania dla prowadzenia walki poszerzyła współczesną koncepcję tej walki. Poszerzenie koncepcji walki zwiększyło zakres przedsięwzięć i działań związanych z prowadzeniem wojny. **Jeśli ograniczymy się jedynie do**

walki rozumianej w wąskim, militarnym sensie prowadzonej na tradycyjnym polu walki zbrojnej będzie bardzo trudnym odzyskanie punktu zaczepienia w przyszłości. 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.

Cel takiej walki będzie obejmował więcej niż jedynie" użycie środków przemocy militarnej do zmuszenia przeciwnika zaakceptowania naszej woli". Cel taki powinien się raczej zasadzać na "użyciu wszelkich dostępnych środków militarnych i niemilitarnych, krwawych i bezkrwawych by zmusić przeciwnika by służył naszym interesom." (Akcent R.S.)

Pod ogólnym hasłem realpolitik według, którego jedynie narodowe interesy są stałe, jakikolwiek sojusz może jedynie koncentrować się bardziej jawnie na interesach. Bez wątpienia fenomen sojuszów będzie dalej istniał, jednakże częściej będzie on przybierał formę krótkoterminowych koalicji skupionej wokół krótkoterminowych koalicji. Co więcej nie należy oczekiwać jakiegokolwiek sojuszu gdzie jedynie moralność a nie interesy byłyby jego spoiwem. Różne okresy mogą być związane z innymi interesami i celami i to determinuje powstanie sojuszu lub jego rozpad. Coraz bardziej pragmatyczne i niezwiązane jakimikolwiek moralnymi ograniczeniami to charakterystyczne cechy współczesnych i przyszłych sojuszy.

Mimo iż granice pomiędzy żołnierzami i nie żołnierzami zostały obecnie zatarte a przepaść miedzy walką i nie walką niemalże zanikła, globalizacja uczyniła wszystkie problemy współzależnymi i wzajemnie powiązanymi to należy znaleźć klucz do stawienia czoła tym zjawiskom. Klucz, który powinien otworzyć wszystkie zamki, które zamykają 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 mieć zastosowanie dla jednostek zarówno polityków i generałów jak i zwykłych żołnierzy. Trudno sobie wyobrazić bardziej odpowiedni klucz niż "nieograniczona walka" (unrestricted warfare).

* * *

Mimo kontrowersyjności postulatu nieograniczonej walki dokonana diagnoza obecnej sytuacji jest niezwykle trafna, sama zaś sytuacja zachęca do podejmowania poszukiwań badawczych w wyłaniających się obszarach aktywności militarnej. Jednym z takich obszarów jest nowa jakość wykorzystania sfery informacyjnej.

1.2. Informacyjny charakter współczesnej cywilizacji

Współczesne procesy rozwojowe można sprowadzić do trzech współzależnych kategorii. Są to przede wszystkim procesy związane z rozwojem nauki, techniki i technologii, które stwarzają zarówno nowe możliwości; jak też potencjalne nowe zagrożenia. Równocześnie te nowe możliwości nie zawsze są wykorzystywane w rozumny sposób, a potencjalne zagrożenia coraz częściej stają się zagrożeniami realnymi. Procesy rozwoju nauki, techniki i technologii dynamizują jednak gospodarkę. Prowadzi to do kolejnej, gospodarczej kategorii przemian, czyli do procesów rozwoju gospodarczego pojmowanych najczęściej nadal jako wzrost gospodarczy, Wzrost ten napotyka jednak granice, pozwalające się zidentyfikować. Wysoka dynamika wzrostu powodowana poprzez rozwój nauki i techniki z jednej strony, a jej granice o charakterze fizycznym, instytucjonalnym oraz intelektualnym z drugiej strony, określałyby z tego punktu widzenia charakter zachodzących przeobrażeń. Prowadzi to jednak do kolejnej kategorii zjawisk i procesów rozwojowych, a mianowicie do zjawisk i procesów kulturowych. Zarysowane tendencje rozwojowe przebiegają, bowiem w obrębie pewnych tradycyjnych wzorców myślenia, działania i ładu społecznego. Pojawiające się coraz częściej bariery i granice tradycyjnie pojmowanego rozwoju sprawiły, że zaczęłyby się rodzić nowe wzorce o charakterze kulturowym. W związku z tym coraz częściej mówi się o pewnego rodzaju „punkcie zwrotnym", poprzez który przechodzi cywilizacja zachodnia, jednak sam sposób pojmowania tego przełomu także ewoluuje w czasie.

Przełom ten pojmowano najpierw jako wyzwanie rozwojowe związane ze zderzeniem nowej, masowej kultury amerykańskiej ze starą, elitarna kulturą europejską. Nieco później zaczęto go postrzegać jako konfrontację „cywilizacji Atlantyku" z ro-

dzącą się „cywilizacją Pacyfiku". Wreszcie ostatnio zaczęto go pojmować jako kres globalnej cywilizacji konsumpcyjno-przemysłowej oraz początek nowej cywilizacji i kultury globalnej, której ostateczny kształt nie został jeszcze do końca przesądzony[4].

W poglądach wielu myślicieli panuje powszechna zgodność co do tego, że **wyłaniająca się nowa forma cywilizacji ludzkiej ma charakter informacyjny** a organizacja ludności rozwiniętych obszarów świata przyjmuje postać społeczeństwa informacyjnego. Informacja staje się głównym dobrem. Wysoko rozwinięte obszary świata coraz szybciej zaczynają tworzyć przyczółki nowej cywilizacji informacyjnej. Interesy zarówno państw jak i coraz większej liczby organizacji ponadnarodowych a także pojedynczych ludzi wiążą się z informacją. Informacja staje się, więc głównym dobrem oraz „miejscem" gdzie krzyżują się różne interesy.

Powstanie nowej cywilizacji stymulowane było przez wiele czynników. Do najważniejszych z nich zaliczyć jednak należy gwałtowny rozwój elektroniki.

W 1947 r. trzech amerykańskich uczonych: W. Shockley, J. Bardeen i W. Brattain dokonało odkrycia nowego półprzewodnikowego elementu elektronicznego - tranzystora bipolarnego. On to, po upływie kolejnych 10 lat stał się podstawowym elementem układów komputerowych (II generacja komputerów). W 1958 r. w laboratoriach firmy Texas Instruments skonstruowano pierwszy układ scalony, czyli umieszczono na jednym krysztale półprzewodnika więcej niż jeden z współpracujących z sobą elementów. Wytwarzany od 1961 r. na skalę przemysłową układ scalony był przerzutnikiem i składał się z czterech tranzystorów bipolarnych i dwóch rezystorów.

Rozwój technologiczny przynosił stały wzrost skali integracji układów, od małej (SSI) do bardzo wielkiej (VHLSI). I znów po 10 latach, u schyłku lat 60-tych, układy scalone zastosowano w konstrukcji układów komputerowych (komputery III generacji). Od tej pory stosowanie układów coraz większej skali integracji przynosiło komputery, nie tylko mniejsze i lżejsze, ale przede wszystkim szybsze, tańsze i bardziej niezawodne.

---

[4] J. Stacewicz, *Cywilizacyjno-kulturowy wymiar globalizacji integracji oraz transformacji*, [w:] *Globalizacja gospodarki światowej a integracja regionalna. Konsekwencje dla świata i Polski*, Warszawa 1998, s. 120-121.

Bez tych zmian technologicznych z pewnością nie dokonałyby się zmiany organizacji procesów przetwarzania danych w systemach komputerowych. I tak, jeszcze na początku lat 60 komputer mógł być wykorzystywany przez tylko jednego użytkownika z tylko jednym programem napisanym, jeśli nie w języku wewnętrznym maszyny („Strings"), to w tzw. assemblerze („Expressions").

Pod koniec lat 60-tych komputery wyposażono już w kompilatory języka symbolicznego, co znacznie zwiększało efektywność programowania i użytkowania systemów liczących. Te zaś dzięki powstaniu i rozwojowi systemów operacyjnych zyskały właściwości wieloprogramowości (użytkownik mógł już uruchamiać cały „wsad" programów nie troszcząc się o to, jak będzie organizowany ich proces realizacji w komputerze) i wielodostępności (z zasobów komputera może korzystać wielu użytkowników i to bez troski o to, jak ich żądania będą przez komputer realizowane).

Kolejną rewolucję, coraz częściej określaną jako nowy przełom informatyczny, rozpoczął w 1971 roku w firmie Intel wynalazek pierwszego mikroprocesora. Składał się on z czterech bloków funkcjonalnych (sterowania, jednostki arytmetyczno-logicznej, rejestrów, wewnętrznych szyn przesyłowych). Od pierwszego mikroprocesora Intel 4004 o architekturze czterobitowej rozpoczął się trwający do dziś proces nieustannego rozwoju mikroprocesorów; w 1980 r. powstał pierwszy mikroprocesor trzydziestodwubitowy. Stanowił on zapowiedź istnej eksplozji informatycznej: w ciągu 30 lat objętość całego pokoju pełnego lamp elektronowych i innych elementów zmalała do rozmiarów płatka owsianego! Już u schyłku lat 70-tych stwierdzono, że gdyby w ciągu ostatnich 30 lat w przemyśle samochodowym dokonał się taki postęp jak w elektronice, to samochód Rolls-Royce można byłoby kupić za 2,5 dolara i przejechać nim dwa miliony mil zużywając na to galon benzyny[5].

Kolejny skok technologiczny będzie związany raczej z zastosowaniem w technologii komputerowej sygnałów świetlnych niż elektronicznych. W praktyce moc komputerów następnej generacji będzie tak duża, by wykonywać większość operacji wymaganych w działalności gospodarczej. Już obecnie osprzęt jest tak dobry, że wartość użytkowa komputerów jest uzależniona właściwie tylko od zastosowanego oprogra-

---

[5] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999, s. 15-16.

mowania, przy czym większa moc obliczeniowa umożliwia zastosowanie oprogramowania dla użytkownika bardziej przyjaznego. W pewnym momencie na pewnym etapie, w przyszłym ćwierćwieczu, osiągnięty zostanie taki poziom rozwoju, na którym nie będzie sensu produkowania silniejszych komputerów, tak jak nie ma sensu produkowanie jeszcze silniejszych samochodów. Nie znajdujemy się jeszcze na tym etapie, lecz nietrudno sobie wyobrazić skutki sytuacji, w której każde gospodarstwo domowe lub małe przedsiębiorstwo będzie mogło dysponować mocą obliczeniową umożliwiającą im konkurowanie z przedsiębiorstwami wielonarodowymi, ponieważ nie będzie miała dłużej znaczenia konkurencyjność w skali gromadzenia, składowania i opracowywania informacji. Po prostu - duże maszyny liczące odejdą do lamusa, podobnie jak to miało miejsce w przypadku okrętu liniowego[6].

Współcześnie różne odmiany komputerów stanowią wszechobecny element tworzącej się cywilizacji. Są bowiem zarówno elementem sterowania nowoczesnych automatycznych procesów produkcji, jak też komponentem większości współczesnych urządzeń. Odnosi się to do wszelkich aspektów aktywności społecznej. Ponadto komputery doprowadziły do zasadniczych zmian w organizacji pracy, komputer stał się podstawą automatyzacji pracy umysłowej w sferach:

- inżynierii obliczeń: komputer jako środek do obliczeń *(computer as a computer);*
- inżynierii rozwiązywania problemów: komputer jako środek do rozwiązywania problemów *(computer as a problem solver);*
- Inżynierii informacji: komputer jako środek do gromadzenia i przetwarzania informacji *(computer as an Information collector and processor);*
- Inżynierii wiedzy: komputer jako ekspert *(computer as an expert).*

Obecnie na całym świecie wykorzystywane są miliony komputerów osobistych: od desktopów („na biurko"), poprzez laptopy („do torby"), notebooki i subnotebooki, do palmtopów („do ręki"). Rzecz jasna, oprócz PC funkcjonują komputery o większej mocy oblicze-

---

[6] H. McRae, *Świat w roku 2020. Potęga, kultura i dobrobyt – wizja przyszłości*, Warszawa 1996, s. 254.

niowej: stacje robocze *(workstation)*, minikomputery, komputery (mainframe) i superkomputery (np. CRAY)[7].

Podobne zmiany zajdą w dziedzinie łączności. Łatwo założyć, że telefon komórkowy zastąpi zwykły. Jeśli prawie każdy będzie posiadał przy sobie przenośny telefon, to jest oczywiste, że nie będzie trzeba wiedzieć, gdzie się kto znajduje. Bez wątpienia pozostaną telefony domowe i biurowe, lecz zapewne będą w większym zakresie wykorzystywane dla transmisji danych i połączeń wideo niż dla zwykłych rozmów[8].

W latach 60-tych rozwój techniczny komputerów, a także środków telekomunikacji, uczynił możliwym połączenie odległych od siebie komputerów w celu bezpośredniego przesyłania danych między nimi. Jeśli coś staje się możliwym, to zapewne - prędzej czy później - zostanie przez ludzi praktycznie wykonane (...). Tak też się stało z łączeniem komputerów - w latach 60-tych powstały pierwsze sieci komputerowe. Jedną z nich była sieć, przeznaczona dla Departamentu Obrony USA, o nazwie ARPAnet.

Siecią komputerową jest system, który tworzą wzajemnie połączone autonomiczne komputery zdolne do wymiany informacji między sobą. Połączenia w sieci mogą być realizowane za pomocą łączy przewodowych, radiowych, radioliniowych, mikrofalowych, światłowodowych i satelitarnych. Sieci komputerowe budowane są w celu zapewnienia użytkownikom dostępu do wszystkich programów, danych i innych zasobów obliczeniowych niezależnie od przestrzennej lokalizacji użytkowników i tych zasobów, a także dla łatwości aktualizacji informacji w odległych bazach danych i uzyskania wysokiej niezawodności przez stworzenie alternatywnych dróg sięgania do zasobów komputerowych. Ze względu na zasięg terytorialny przyjmuje się podział sieci teleinformatycznych na: lokalne (LAN - do kilku kilometrów), miejskie (MAN - do kilkudziesięciu kilometrów) i rozległe (WAN - rozwinięte na dowolnym obszarze).

---

[7] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999, s. 16.
[8] H. McRae, *Świat w roku 2020. Potęga, kultura i dobrobyt – wizja przyszłości*, Warszawa 1996, s. 254.

Obecnie w świecie trwa „boom sieciowy" budowane są sieci zarówno ograniczone do użytkowników określonej organizacji, jak i sieci o powszechnym dostępie, a tempo sprzedaży technologii sieciowych wzrasta z roku na rok. Rosną także wymagania stawiane sieciom, dotyczące funkcjonalności i niezawodności, ochrony zasobów i bezpieczeństwa sieci, a przede wszystkim - zakresu oferowanych usług informacyjnych. Ostatnio rośnie zainteresowanie sieciami multimedialnymi integrującymi, w celu efektywnego oddziaływania na odbiorcę, kilka typów informacji: VIDEO (pełny ruch) - AUDIO (głos, dźwięk) - DATA (dane, tekst - grafika)[9].

Dzięki wzajemnym połączeniom tych różnych odmian sieci i podłączonych do nich komputerów oraz innych urządzeń stworzona została globalna sieć informacyjna. Dzięki temu teoretycznie każdy, kto podłączony jest do takiej sieci może mieć dostęp do wszystkich użytkowników globalnej sieci. Sieci telefoniczne istnieją od dawna, jednakże to, co jest nowe to niezmierne zagęszczanie owej sieci oraz łączenie w niej wszystkich nowych i najnowszych wynalazków w dziedzinie komunikowania i przetwarzania informacji. Stąd, pojęcie sieci obejmuje coś więcej niż fizyczne urządzenia do transmisji, gromadzenia, przetwarzania oraz odtwarzania głosu, danych oraz obrazów. Obejmuje także (...) **„szeroką skalę oraz stale wzrastający zasób instrumentów, włączając aparaty fotograficzne i wideo, skanery, klawiatury, telefony, faksy, komputery, przełączniki, płyty kompaktowe, taśmy audio i wideo, kable i światłowody, satelity, połączenia mikrofalowe, telewizory, monitory, drukarki i wiele, wiele innych."** (...)

Sieci globalne nie są już hierarchiczne, zarządzane odgórnie, nadzorowane ściśle przez państwa, ale horyzontalne, oddolne, samorozwijające się. Nie są jedynie narzędziami określonych organizacji (tak jak początkowo były systemy łączności, np. usług bankowych, itp.), ale - jak to ujmuje metafora sieci drogowej - autostradami (do przyszłości)[10].

---

[9] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999, s. 17.
[10] Tamże, s. 90- 91.

Jeśli mieszkania i miejsca pracy zostaną wyposażone w kable światłowodowe, to możliwość transmisji danych zwielokrotni się tysiąckrotnie. Zestaw dokumentacji formatu A4 będzie mógł zostać przekazany na drugą półkulę w ciągu ułamka sekundy przy jednocześnie znacznie wyższej jakości. Co istotne z punktu widzenia połączeń między komputerami, to fakt, że sygnały nie będą musiały być dłużej przekształcane na postać analogową, by odpowiadać standardom sieci telefonicznej, lecz będą przesyłane wyłącznie w formie cyfrowej. Jest również całkowicie możliwe, że kompresja danych osiągnie taki stopień rozwoju, że zwykły kabel telefoniczny, wytworzony zgodnie ze stuletnią technologią, będzie wystarczał do zaspokojenia potrzeb zwykłego gospodarstwa domowego jeszcze przez następne dwadzieścia pięć lat. Jednocześnie technologia ta wyprzedzając epokę może zmniejszyć wymagania stawiane rozwojowi innej równie szybko rozwijającej się technologii, czyli światłowodom.

Dalszy wzrost liczby kanałów telewizyjnych będzie trwał, co doprowadzi do sytuacji, w której struktura rynku mediów zbliży się do struktury rynku wydawniczego, czyli mała liczba produkcji narodowych oraz międzynarodowych przy wielości stacji wyspecjalizowanych — odpowiedników wyspecjalizowanych czasopism. Postęp zachodzący w zakresie kompresji danych umożliwi w końcu, by wideofon stał się alternatywnym rozwiązaniem dla istniejących połączeń telefonicznych[11].

W tej sytuacji dokonuje się masowe ucyfrowienie form informacji. W rezultacie tego powszechnym standardem przesyłanej informacji staje się forma cyfrowa. Odnosi się to zarówno do dźwięków obrazów i pisma, jak też i różnych bodźców rejestrowanych przez mechaniczne sensory. Taki stan rozwoju elektroniki zasadniczo zmienia komunikowanie społeczne – główny element życia społecznego.

W efekcie obserwowanych zmian w rozwiniętych gospodarczo krajach wyłania się społeczeństwo informacyjne rozumiane, jako „**społeczeństwo, które nie tylko posiada rozwinięte środki przetwarzania informacji i komunikowania, lecz prze-**

---

[11] H. McRae, *Świat w roku 2020. Potęga, kultura i dobrobyt – wizja przyszłości*, Warszawa 1996, s. 255.

twarzanie informacji jest podstawą tworzenia dochodu narodowego i dostarcza źródła utrzymania większości społeczeństwa"[12].

W cywilizacji współczesnej, zdominowanej przez rewolucję w elektronice i komunikacji społecznej zachodzi wiele procesów. Obserwuje się m.in.:

- Gwałtowny wzrost ilości informacji „zalewającej" świat;
- Systematyczny wzrost znaczenia informacji i wiedzy;
- Wzrost roli sektora usług w tworzeniu dochodu narodowego;
- Znaczne poszerzenie zakresu sfery usług;
- Zmiany w organizacji procesów wytwarzania;
- Wzrost znaczenia mediów społecznego komunikowania się;
- Gwałtowne zmiany kulturowe w całych narodach;
- Cyfrową rewolucję kulturalną i ekspansję kultury;
- Jednoczesną integrację (globalizacja) i dezintegrację;
- Erozję państwa narodowego;
- Wzrost roli aktorów niepaństwowych;
- Decentralizację władzy;
- Likwidację bariery odległości;
- Fragmentaryzację kontaktów międzyludzkich i zerwanie więzi międzypokoleniowej;
- Rozwój wirtualnego biznesu;
- Dalszy rozwój automatyzacji i robotyzacji;
- Częste zmiany pracy i kariery zawodowej;
- Wzrost rozwarstwienia społecznego;

---

[12] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999, s. 43.

- Wzrost migracji ludności;
- Wzrost możliwości manipulacji informacją;
- Zanik znaczenia granic;
- Wzrost napięć i konfliktów między cywilizacjami;
- Wzrost wrażliwości na infoterroryzm.

Wspólnym mianownikiem wszystkich tych procesów jest przede wszystkim głębokie uzależnienie od informacji i systemów informacyjnych. Uzależnienie to staje się główną wrażliwością nie tylko systemów militarnych, ale także i całych systemów państwa. Wrażliwość ta stymuluję coraz szybszy rozwój walki informacyjnej.

1.3. Główne założenia

Walka informacyjna jest formą kooperacji negatywnej działań informacyjnych. Ponieważ istotą walki jest przemoc, 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.**

Jest niewątpliwym istnienie rozległych obszarów walki informacyjnej, jednakże ze względu na ukierunkowanie niniejszych badań, przedmiotem zainteresowania jest ofensywna część walki informacyjnej. Ogólnym przedmiotem badań jest, więc walka informacyjna, a szczegółowym ofensywna walka informacyjna w działaniach powietrznych.

Działania powietrzne prowadzone są głównie przez siły powietrzne, gdyż to jest głównym przeznaczeniem i specjalizacją tych sił. Dla innych komponentów sfery mili-

tarnej działania powietrzne stanowią jedynie drugorzędne znaczenie. Dlatego też istota walki informacyjnej w działaniach powietrznych zawiera się w kategorii walka informacyjna sił powietrznych. Działania powietrzne mogą być rozumiane, jako działania w powietrzu lub, jako działania prowadzone przez siły powietrzne. Dla potrzeb niniejszych badań przyjęto, że działania powietrzne to działania prowadzone przez siły powietrzne. Działania powietrzne zawierają działania w powietrzu i inne formy aktywności. Jednakże w zależności od przyjmowanych kryteriów podziały działań sił powietrznych mogą przybierać różne formy. Nie wdając się w szersze rozważania na ten temat przyjęto, że walka informacyjna w działaniach powietrznych stanowi część działań sił powietrznych.

Przyjęto także, że **walka informacyjna sił powietrznych to zorganizowana w formę przemocy, militarna 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.**

Podstawowymi kategoriami jakiejkolwiek walki są „atak" i „obrona". Jeżeli przyjmuje się powszechnie istnienie **walki** informacyjnej to konsekwencją tego powinno być uznanie istnienia „**informacyjnego ataku**" i „**informacyjnej obrony**". Tymczasem niektórzy badacze[13] 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", itp. 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 kla-

---

[13] L. Ciborowski, *Walka informacyjna*, Toruń 1999 oraz G. Nowacki, *Walka informacyjna – próba kategoryzacji*, Warszawa 1999.

rowności należałoby uznać kategorię „**informacyjny atak**" za odpowiedniejszą niż *informacyjne zakłócanie*, dlatego też tak zostało przyjęte do dalszych badań.

Ofensywna walka informacyjna w działaniach powietrznych to informacyjny atak sił powietrznych.

2. OFENSYWNE ELEMENTY WALKI INFORMACYJNEJ WE WSPÓŁCZESNYCH DZIAŁANIACH POWIETRZNYCH

Walka informacyjna sił powietrznych dzieli się na **informacyjny atak** i **informacyjną obronę**.

Odpowiednio do przyjętego rozumienia walki informacyjnej uznano, iż: **informacyjny atak sił powietrznych to zorganizowana w formę przemocy, militarna aktywność zewnętrzna sił powietrznych prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji.**

Przed dokonaniem charakterystyki ofensywnych form walki informacyjnej sił powietrznych należy zwrócić uwagę na istnienie w koncepcjach i doktrynach kategorii „walka elektroniczna" nazywanej w części polskiego piśmiennictwa „walką radioelektroniczną".

2.1. Walka informacyjna a walka elektroniczna (radioelektroniczna)

Zbigniew Dubrawski w wyniku przeprowadzonych badań[14] 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:

---

[14] Z. Dubrawski, *Walka radioelektroniczna prowadzona przez siły powietrzne*, Warszawa 2000, s. 39 i 56.

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 to 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."

Według niego „**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)"[15].

---

[15] Tamże, s. 45.

Podobna definicja[16] oraz identyczne komponenty składowe walki radioelektronicznej prezentowane są także w podręczniku „Walka radioelektroniczna w Siłach Zbrojnych RP" wydanym przez Wydział Wojsk Lądowych AON w 1994 r.

Według poglądów Sił Powietrznych USA[17] 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 wykorzystywanym 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 zakresów spektrum. 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

---

[16] 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. [W:] *Walka radioelektroniczna w Siłach Zbrojnych RP*, Warszawa 1994, s. 11.

[17] *Electronic Warfare*, *Air Force Doctrine Document 2-5.1*, Washington, D.C. 1999.

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 stanowią reprezentatywne odzwierciedlenie poglądów panujących 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 1).

Tabela - 1. Porównanie głównych komponentów walki elektronicznej wg 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 środowisku polskim w dalszym ciągu obserwuje się wahania nad zmianą nazwy „radioelektroniczna" na „elektroniczna". Niektórzy uznają[18] 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 Zbigniewa Dubrawskiego, któ-

---

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

ry w definicji stosuje nazwę „elektroniczna" a dalszej treści pracy używa nazwy „radioelektroniczna" umieszczając czasami drugą nazwę „elektroniczna" w nawiasach.

W wielu ustaleniach doktrynalnych komponuje się zarówno działania 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 działań i walki informacyjnej. Z punktu widzenia działań informacyjnych wsparcie elektroniczne jest częścią informacyjnego wsparcia zaś elektroniczny atak i obrona są 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.

2.2. Formy informacyjnego ataku

W ramach **informacyjnego ataku** mogą być stosowane następujące formy działań:

- **Atak informatyczny (w sferze przetwarzania danych cyfrowych);**
- **Atak elektroniczny;**
- **Atak fizyczny;**
- **Działania psychologiczne;**
- **Dezinformacja (mylenie).**

2.2.1. Atak informatyczny (w sferze przetwarzania danych cyfrowych)

Atak informatyczny[19] jest formą walki 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.

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 hackerskich 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 - 2. 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 jednostkami przeciwnika	Wygranie wojny
Organizacja terrorystyczna	System komputerowy firmy telekomunika-	Przerwanie działalności firmowej,	Wydanie politycznego oświadczenia

[19] Opracowane treści oparto na: L.G. Jr. Downs, *Digital Data Warfare: Using Malicious Computer Code as a Weapon. A Research Report Submitted to the Faculty in Fulfillment of the Curriculum Requirement. Air War College Air University*, Maxwell AFB 1995.

	cyjnej AT&T	transakcji finanso-wych i przepływu informacji	
Prywatna korporacja	Baza danych badań i rozwoju konkurenta	Uzyskanie dostępu do zastrzeżonej in-formacji	Uzyskanie korzyści w walce konkuren-cyjnej
Rozczarowany lub nieuczciwy pracow-nik	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 przy zastosowaniu 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 – degradowanie 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 za prawdziwe.
- Eksploatacja – użycie środków za pomocą, których następuje transmisja informacji z atakowanego systemu do atakującego.

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

2.2.1.1. Fazy ataku w sferze przetwarzania danych cyfrowych

Atak w sferze przetwarzania danych cyfrowych składa się z serii kolejnych kroków następujących w określonej wcześniej kolejności. Jak wspomniano wcześniej w ramach tego ataku użyte mogą być wirusy, robaki, bomby logiczne, bomb programowane czasowo, konie trojańskie lub ich odpowiednie kombinacje. Wszystkie one są formą złośliwych kodów. Atak w sferze przetwarzania danych cyfrowych 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 przez niego 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.

2.2.1.1.1. 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 docelowego miejsca (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 (front-door coupling) i tylne.

Przenikanie czołowe określane jest 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 na przykład 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 przypadkach 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 umieszczony został w systemie przeciwnika.

Przykłady zastosowań różnych miejsc i metod penetracji obrazuje tabela 3.

Tabela - 3. 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 terminala.	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	Wyrafinowany terrorysta używa impulsów elektromagnetycznych dla

	zakupionej przez przeciwnika grupie podzespołów i instalowany w głównej sieci systemu pokładowego	wprowadzenia złośliwych kodów do komputerów firmy energetycznej doprowadzając do awarii sieci energetycznej w mieście.

2.2.1.1.2. 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 jest mniejsze prawdopodobieństwo wykonania przez niego zadania. Chwilowo może być koniecznym 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.

2.2.1.1.3. 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 następował będzie bezpośrednio po infekcji. Jednakże w większości przypadków 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 mo-

że 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 umożliwia odpowiednie przeciwdziałanie. Faza uśpienia trwa do czasu aktywacji kodu przez odpowiedni mechanizm.

2.2.1.1.4. 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 ilości 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 (na przykład 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, jakimi są: wzbranianie, degradacja, dezinformacja i eksploatacja.

- **Wzbranianie**. Złośliwy kod może uniemożliwić atakowanemu obiektowi użycie jego systemu. Może tego dokonać na wiele sposobów. Wśród nich najskuteczniejszym jest zniszczenie danych i zainstalowanych programów wykonawczych. Innym sposobem będzie atak na komponenty sprzętowe systemu. Przykładowo wirus, który może zmienić częstotliwość taktowania zegara głównego procesora może spowodować jego przegranie i samo destrukcję. Złośliwy kod może również atakować dynamiczne komponenty systemu wprowadzając je w przeciążenia, których nie są w stanie wytrzymać, jak na przykład 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 roku wprowadzony do Internetu robak zaatakował 6000 komputerów podłączonych do światowej sieci i blokując je powodując 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 wystarczającym efektem dla atakującego.

Inną formą degradacji są efektu z obszaru „psycho-elektroniki". 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 wprowadza-

nych fałszywych danych jako prawdziwe. Niewielka modyfikacja programy 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 modyfikacja programu nie musi być wielka. Prosta zmiana znaku „<" na „>" może wystarczyć dla osiągnięcia celu atakującego. Przykładowo system kontroli ognia, którego program został zmodyfikowany przez wirusa tak by zamiast ignorować nadlatujące obiekty o prędkości mniejszej niż dźwiękowa ignorował obiekty o prędkości większej niż dźwiękowa zamiast atakować nadlatujące pociski rakietowe zwalczał będzie 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 wykorzystane mogą być różne skryte kanały komunikowania do przekazania sygnałów, które ułożone w odpowiednie sekwencje mogą nieść wiadomość dla kogoś, kto wie jak ją odczytać. Przykładowo, 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.

2.2.1.1.5. 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 oczywistym dla atakowanego obiektu, co może mieć miejsce w wypadku skrytych działań usunięcie atakującego kodu może uniemożliwić zidentyfikowanie prawdziwej przyczyny awarii lub przesłanki tego, że doszło do ujawnienia tajnej informacji.
- W przypadku, 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 przeciwko przyszłym atakom.
- Usunięcie atakującego kodu czyni także znacznie trudniejszym dla atakowanego ustalenie źródła ataku i identyfikacji napastnika. Ustalenie tych danych może prowadzić do poważnych konsekwencji prawnych lub sankcji militarnych w stosunku do atakującego.

W niektórych, szczególnych przypadkach atakujący może chcieć ponownie wprowadzić atakujący kod w stan uśpienia i gotowości do wykonania kolejnego ataku. Przykładowo 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 zaatakowanego zestawu przeciwlotniczego wyglądać to może na przypadkową awarię i może on być dalej utrzymywany w eksploatacji gdyż prawdziwy powód nie został odkryty. Wszystkie, bowiem testy i przypadki użycia przeciwko samolotom nie wysyłającym skrytych sygnałów wypadają pomyślnie. Jednakże atakujący będzie wiedział, że jego samoloty

emitujące odpowiednie sygnały pozostaną bezpieczne przed atakiem dostarczonym 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 sfery przetwarzania danych cyfrowych musi pozostawać niezmiennym. Atakujący musi 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 nieprzewidywalnym 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. Gdy siły lądowe USA zamówiły badania mające określić wykonalność wirusów przeznaczenia militarnego wielu zaangażowanych w sprawę wyrażało obawy, które wyrażało stwierdzenie znanego specjalisty Gary'ego Chapmana, iż „uwalnianie tego typu rzeczy jest niebezpieczne", bo „jeśliby wirus wydostałby się spod kontroli to stanowiłby niebezpieczeństwo dla najbardziej zagrożonych krajów na czele, których znajdują się same Stany

Zjednoczone, które osiągnęły największy stopień zintegrowania swoich komputerów w sieć". Uznano, że jeżeli wirusy komputerowe mają mieć praktyczne zastosowanie to muszą mieć przewidywalne działanie. Każda broń powinna mieć możliwości jej uzbrajania i rozbrajania. Złośliwe kody muszą mieć możliwość celowego rażenia i nie stwarzania 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.

2.2.1.2. Rodzaje atakowanych systemów

W ramach walki w sferze przetwarzania danych cyfrowych 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 zauważyć warto, iż z polityczno-militarnego punktu widzenia dla atakującego byłoby najlepiej gdyby niemalże 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 jest czynione dla potrzeb ataków konwencjonalnych. Wyłanianie i klasyfikowanie obiektów uderzeń poprzedzać powinna intensywna analiza:

Atakowanego systemu, a w nim, jaki typ danych jest przetwarzany? Jaki jest stopień znajomości tego procesu i czy istnieje możliwość zbudowania lub znalezienia odpowiedniego kodu, który mógłby być zastosowany? W jaki sposób atakujący kod może być umieszczony i jakie jest prawdopodobieństwo wykrycia go zanim wykona on swoje zadanie?

Cel ataku, tzn., co należy osiągnąć, jaki efekt i jakie jest prawdopodobieństwo sukcesu? Jakie są polityczne i ogólne cele konfliktu?

Konkretne silne i słabe strony przeciwnika? Jak atak w sferze przetwarzania danych cyfrowych będzie je wykorzystywał? Czy przeciwnik będzie dysponował zapasowymi komponentami, które może użyć by zastąpić zaatakowane elementy? Czy przeciwnik może osiągnąć swój cel bez użycia zautomatyzowanych systemów, które mają być obiektem ataku?

Przypuszczalny sposób działania od góry do poziomu taktycznego. Jak atak w sferze przetwarzania danych cyfrowych wpłynie na sposób wykonywania zadania przeciwnika? Czy dowodzenie i kontrola są zcentralizowane czy zdecentralizowane? Jak wykonanie ataku w sferze przetwarzania danych cyfrowych wpłynie na ogólny wysiłek w konflikcie?

Należy pamiętać o tym, że walka w sferze przetwarzania danych cyfrowych powinna być stosowana w koordynacji z innymi formami działań militarnych po to by osiągać najlepsze efekty w zakresie pożądanego celu działań. Walka ta nie jest jedynym narzędziem sił zbrojnych, ale jednym z tych, które powinny być użyte w skoordynowany sposób z innymi formami walki zbrojnej.

W jakich okolicznościach walki w sferze przetwarzania danych cyfrowych powinna być stosowana? Walka w sferze przetwarzania danych cyfrowych może być stosowana na znacznie zróżnicowane sposoby. Może ona być wysoce 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 kierowanego czy nawet pocisku typu Cruise Missile.

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, elek-

trycznych 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 Zachodnich Niemczech"[20].

Z drugiej strony walka w sferze przetwarzania danych cyfrowych stosowana będzie dla wywołania zniszczeń na szeroką skalę. Wirus zainstalowany w komputerze kontrolującym sieć energetyczną regionu spowodowałby rozległe spustoszenia mające

---

[20] E. R. Koch , J. Sperber, *Infomafia. Szpiegostwo komputerowe, handel informacją tajne służby*, tłum. R. Ratajski, Gdynia 1999, s. 246.

swoje konsekwencje w sferze militarnej i cywilnej. Zaatakowanie sieci finansowej kraju i paraliż głównych węzłów komunikacji finansowej mogłoby spowodować długoterminowy efekt dewastujący ekonomię tego kraju. Takie lub jeszcze rozleglejsze użycie walki informacyjnej może przynosić skutki porównywalne z użyciem broni jądrowej.

2.2.2. 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, dekomponowany w stosunku do kryterium zakresu widma promieniowania elektromagnetycznego, zawiera **atak laserowy** i **atak elektromagnetyczny**[21]. 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**.

---

[21] Nazwa „elektromagnetyczny" nie jest tu najbardziej adekwatna, gdyż całe spektrum jest elektromagnetyczne. Jednak trudno znaleźć adekwatną 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.

2.2.2.1. Zakłócanie laserowe i elektromagnetyczne.

Zakłócanie laserowe prowadzone jest dla 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 zaś atak w stosunku do innego. Mniej wrażliwe będą, bowiem oślepione zaś bardziej wrażliwe zniszczone. Dlatego też decydującym kryterium jest tu zamiar prowadzącego walkę i przeprowadzenie działań zgodnie z tym zamiarem.

Zakłócanie elektromagnetyczne[22] jest celowym emitowaniem, retransmitowaniem lub odbijaniem energii elektromagnetycznej w celu zapobiegania efektywnemu wykorzystaniu przez nieprzyjaciela elektromagnetycznego spektrum lub redukowania efektywności tego wykorzystania i zdegradowania lub neutralizowania możliwości bojowych nieprzyjaciela.

W początkowym okresie stosowania zakłócania jego wysiłek skierowany był przede wszystkim na degradowanie możliwości wykrywania radarów przeciwnika i maskowaniu obecności własnych samolotów w przestrzeni powietrznej oraz na pogarszaniu celności kierowanego radarowo uzbrojenia. 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 wysokie uzależnienie od scentralizowanego kierowania stwarza doskonałą okazję do efektywnego zastosowania ataku elektronicznego.

2.2.2.2. Atak laserowy

Generatory laserowe wykorzystywane będą do prowadzenia **ataku laserowego**. Promieniowanie laserowe w odpowiednio dużej mocy działa tak samo destrukcyjnie, jak materiał wybuchowy. Czynnikami rażenia są tu wysoka temperatura oraz mogąca

---

[22] Obszerna dekompozycja zakłócania elektromagnetycznego prowadzonego przez siły powietrzne i jego charakterystyka zawarta jest w pracy: Z. Dubrawski, *Walka radioelektroniczna prowadzona przez siły powietrzne. Studium operacyjne*, Warszawa 2000.

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.

2.2.2.3. Atak elektromagnetyczny

Atak elektromagnetyczny[23] prowadzony jest przy wykorzystaniu strumieni energii promieniowania elektromagnetycznego. Źródłem tego promieniowania mogą być generatory różnego typu. Generatory promieniowania w pasmach metrowych, decymetrowych, centymetrowych a nawet milimetrowych zostały odkryte i praktycznie zastosowane np. w radiolokacji. Dostrzeżono także możliwości wykorzystania generowanej przez nich energii dla destrukcyjnych celów walki. Prace w tym obszarze są szeroko prowadzone. Ich rezultaty są jedynie w niewielkim stopniu ujawniane.

W podrozdziale tym omówiona jest praktyczna możliwość zastosowania dwóch typów generatorów w formie uzbrojenia lotniczego, tj. najbardziej adekwatnego dla sił powietrznych. W treści podrozdziału kolejno zaprezentowano: ogólną charakterystykę środków rażenia ataku elektromagnetycznego; obiekty ataku bombami elektromagnetycznymi; sposoby atakowania konwencjonalnymi bombami elektromagnetycznymi oraz działania ataku elektromagnetycznego z użyciem bomb elektromagnetycznych.

2.2.2.3.1. 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

---

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

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 aktualnego 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 niszczącą dla sprzętu elektronicznego i elektrycznego.

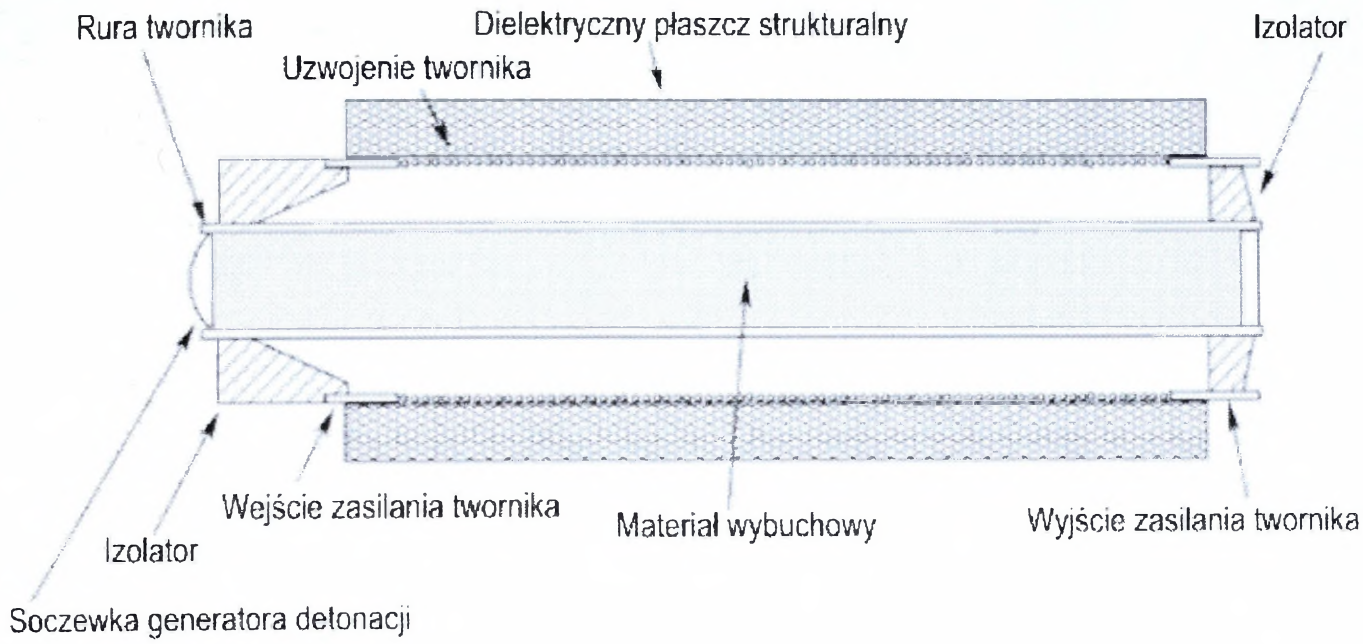
Wytworzony przez generator impuls energii wytwarza silne pole magnetyczne, szczególnie w otoczeniu generatora. Pole to może być na tyle silne, że wytwarza krótkie, ale wysokie napięcia rzędu tysięcy Volt w znajdujących się w jego zasięgu przewodnikach. W rezultacie spowodować to może zniszczenie szerokiej gamy urządzeń elektronicznych i elektrycznych. Zniszczenia mogą być znaczne i wymagać rozległych napraw lub całkowitej wymiany sprzętu. Szczególnie wrażliwe są oczywiście urządzenia cywilne, zupełnie nie odporne na tego typu oddziaływania. Wrażliwość ta się gwałtownie 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 traktować 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 stosowane są przynajmniej 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. Generator ten może wytwarzać dziesiątki megadżuli w czasie od dziesiątek do setek mikrosekund. Osiągany w rezultacie tego prąd szczytowy jest 1000 razy większy od typowego burzowego wyładowania atmosferycznego.

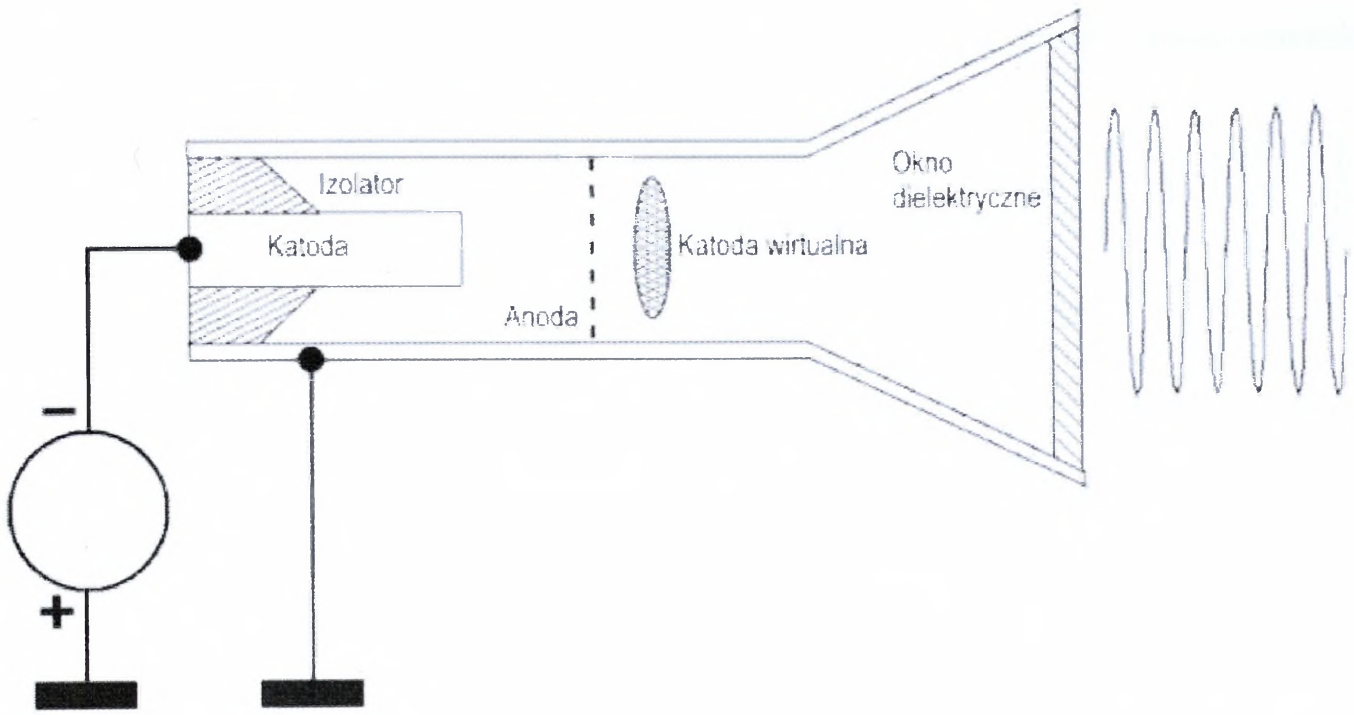
Fizyczna istota generatora FCG: szybka eksplozja spręża pole magnetyczne. Kompresja ta zamienia energię mechaniczną w pole magnetyczne. Prąd szczytowy rzędu megaamperów demonstrowany był w wielu eksperymentach. Prąd rozruchowy jest dostarczany przez źródło zewnętrzne w postaci baterii kondensatorów, mały generator FCG, urządzenie magnetohydrodynamiczne lub prądnicę (rys.1).

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



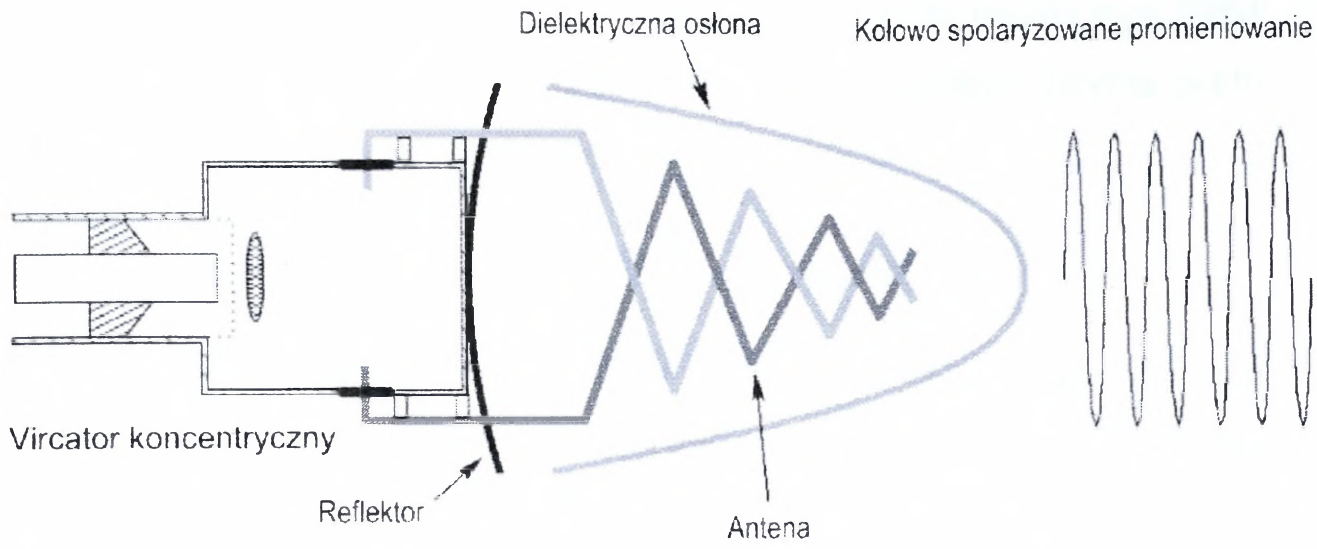
Rys. 1. Eksplozyjnie pompowany kompresyjny generator strumieniowy – FCG. (Źródło: Kopp C. The E-Bomb - A Weapon of Electrical Mass Destruction http://www.cs.monash.edu.au/carlo/ 04.1997 r.).

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. 2 oraz 3).



Rys. 2. Vircator – urządzenie generujące jeden bardzo silny impuls promieniowania. (Źródło: Kopp C. The E-Bomb - A Weapon of Electrical Mass Destruction http://www.cs.monash.edu.au/carlo/ 04.1997 r.)

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 oscylować ona będzie z częstotliwością mikrofalową. Jeżeli ładunek taki umieszczony zostanie w odpowiednio dostrojonej przestrzeni rezonansowej uzyskany zostanie 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 uzyskiwanego impulsu mieści się w przedziale mikrosekund. Energia uzyskiwana w takim impulsie zawierać się może w szerokim zakresie mocy od 170 kilowatów do 40 gigawatów przy częstotliwościach rozciągających się w zakresach decymetrowym i centymetrowym.



Rys. 3. Vircator z zestawem antenowym. (Źródło: Kopp C. The E-Bomb - A Weapon of Electrical Mass Destruction http://www.cs.monash.edu.au/carlo/ 04.1997 r.)

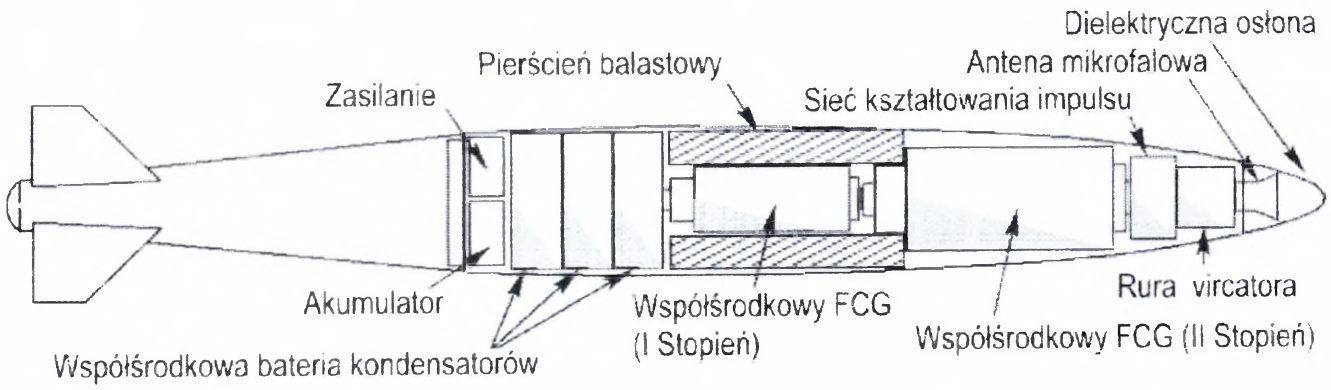
Zdolności rażenia głowic bomb elektromagnetycznych są trudne do jednoznacznego określenia ze względu na różnorodność obiektów ataku. Jednakże zdolności rażące tego typu broni są znaczne a głównym czynnikiem siły rażenia jest efektywność przenikania generowanego promieniowania. Promieniowanie to może 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 również przez kanały wentylacyjne, szczeliny i słabo zabezpieczone mufy wywołując przestrzenną falę stojącą we wnętrzu urządzeń. 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 GigaWattowa 5 GHz bomba typu HPM zdetonowana na wysokości kilkuset metrów tworzy strefę o średnicy rażenia około 400 - 500 metrów z polem o natężeniu kiloVoltów/metr.

2.2.2.3.2. Obiekty ataku bombami elektromagnetycznymi

Bombami elektromagnetycznymi (rys. 4) 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 rozpoznawane konwencjonalnymi metodami rozpoznania. Tego typu obiekty są zazwyczaj stałymi, dlatego sposób ataku powietrznego może być wcześniej zaplanowany i uwzględniać może zrzut ładunków poza obszarem obiektu ataku i dolot bomb w rejon celu. Jest to możliwe szczególnie teraz, gdy dostępne są bomby precyzyjnie nawigowane i zdalnie sterowane. Umożliwia to zdetonowanie ładunku bojowego i emisję fali elektromagnetycznej w optymalnym miejscu i na pożądanej wysokości.



Rys. 4. Bomba elektromagnetyczna z generatorem typu FCG. (Źródło: Kopp C. The E-Bomb - A Weapon of Electrical Mass Destruction http://www.cs.monash.edu.au/carlo/ 04.1997 r.)

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 one w stanie wykonać uniku w czasie lotu bomby.

Mobilne i ukryte a nie promieniujące obiekty mogą sprawiać trudność, szczególnie przy zastosowaniu konwencjonalnych sposobów wykrywania. Istnieją jednakże 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 był on niszczony za pomocą dział pokładowych.

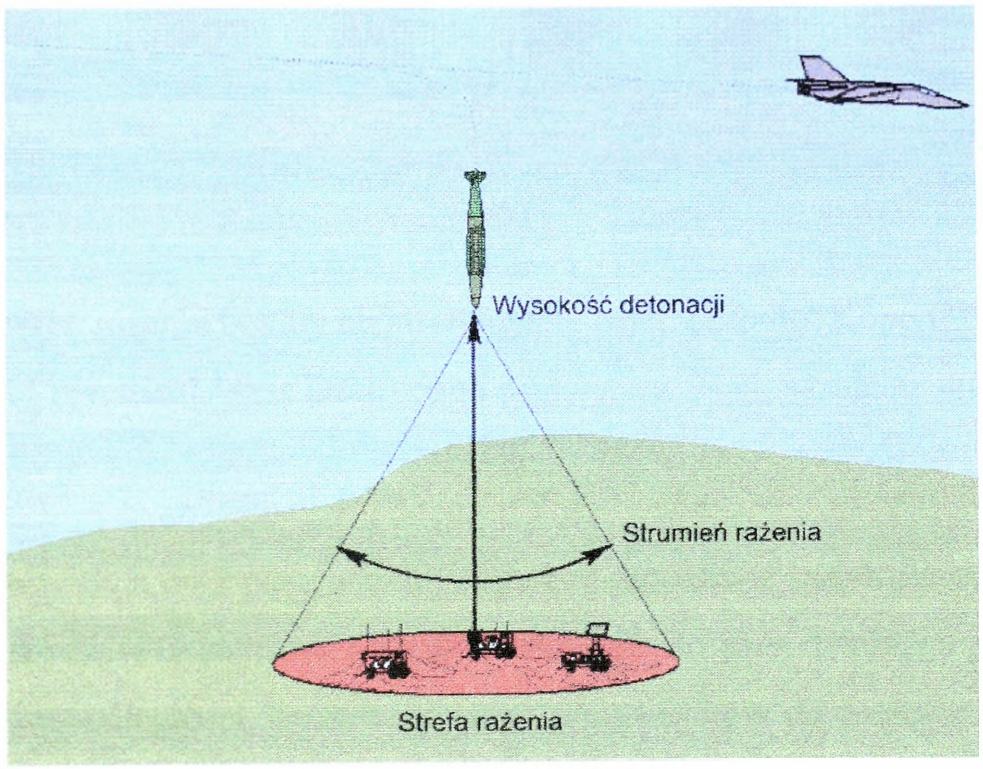
2.2.2.3.3. Sposoby atakowania konwencjonalnymi bombami elektromagnetycznymi

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 lub na komendę operatora.

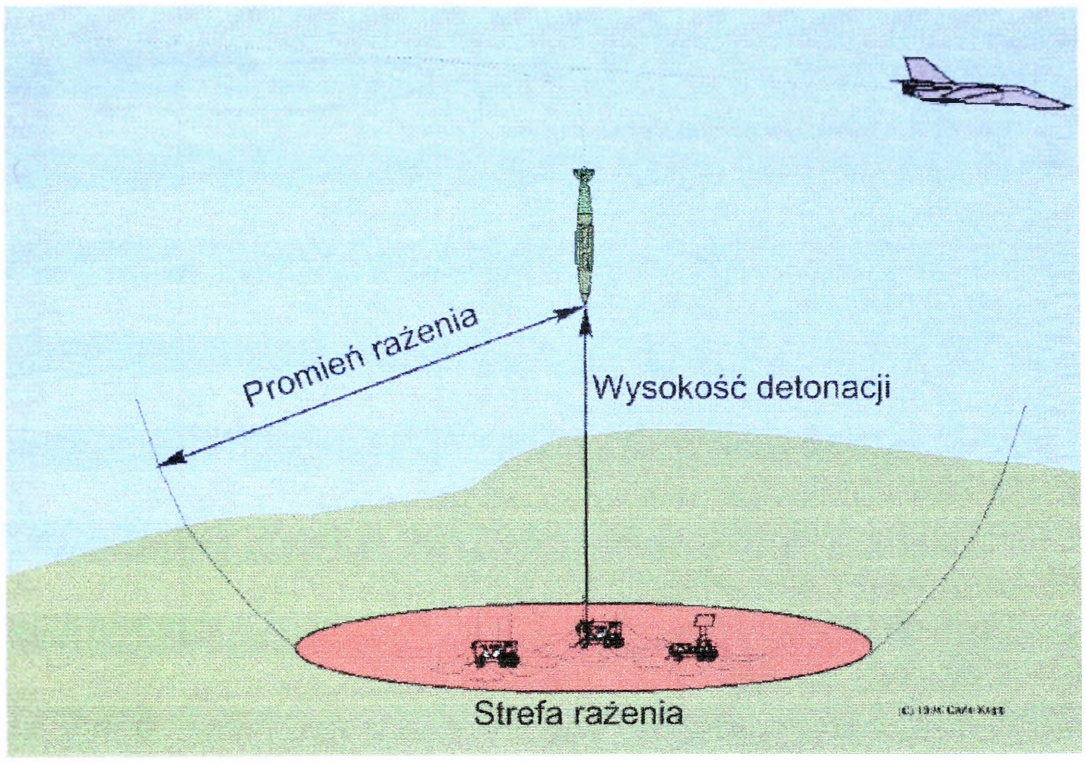
W wypadku urządzeń automatycznych komendę do detonacji może przekazać urządzenie nawigacyjne po osiągnięciu określonej pozycji albo radar pokładowy po wykryciu obiektu ataku i znalezieniu się w jego otoczeniu. Może to być również zapalnik pocisku powietrze-powietrze wykrywający obecność w bezpośrednim sąsiedztwie obiektu ataku. Zapalnik lotniczej bomby elektromagnetycznej może być inicjo-

wany przez radiowysokościomierz, pokładowy system nawigacyjny (np. inercyjny, lub GPS) czy wysokościomierz barometryczny (rys. 5 oraz 6).

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 na tym obiektem.



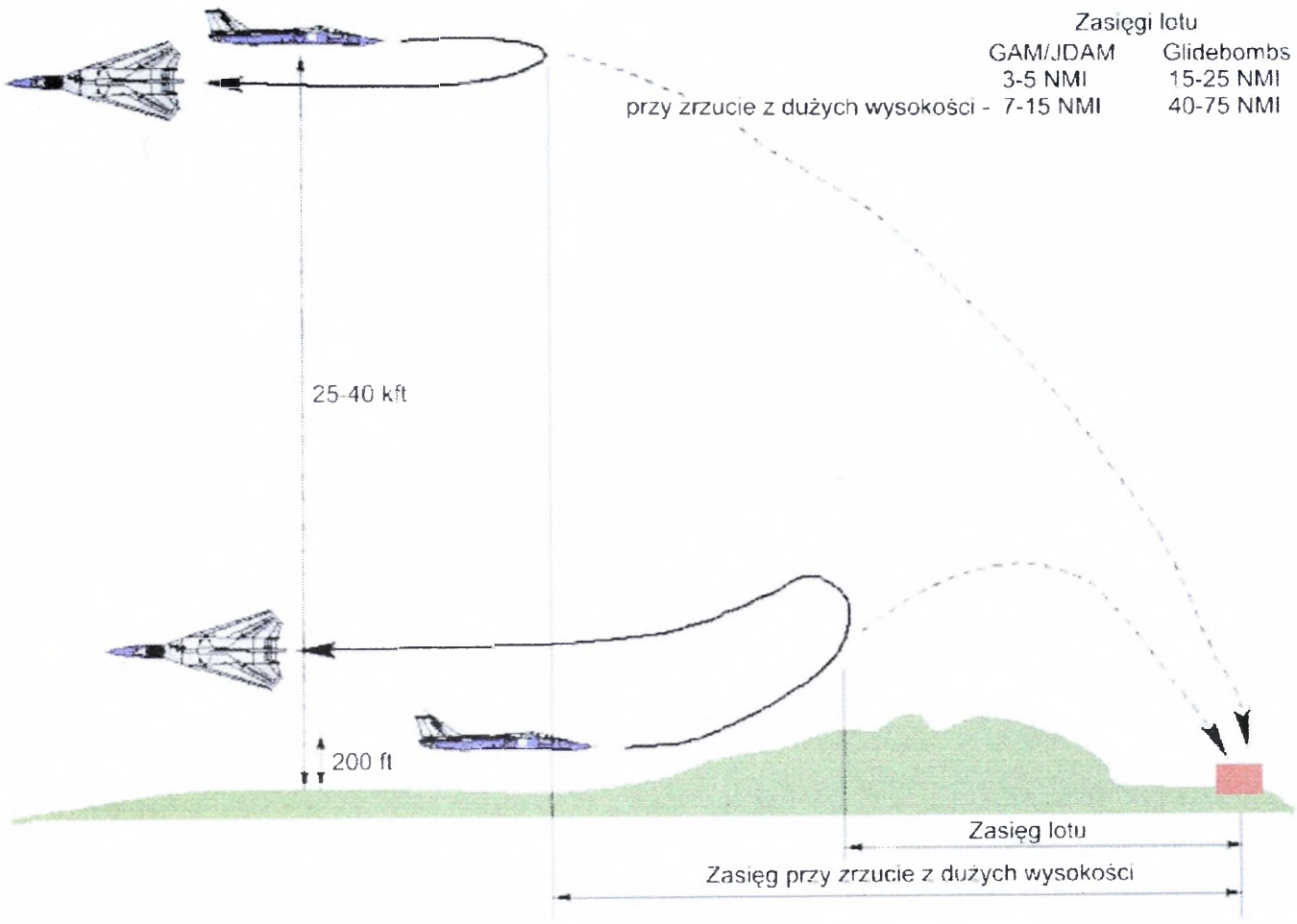
Rys. 5. Promień i strefa rażenia bomby elektromagnetycznej. (Źródło: Kopp C. The E-Bomb - A Weapon of Electrical Mass Destruction http://www.cs.monash.edu.au/carlo/ 04.1997 r.)



Rys. 6. Strumień rażenia bomby elektromagnetycznej. (Źródło: Kopp C. The E-Bomb - A Weapon of Electrical Mass Destruction http://www.cs.monash.edu.au/carlo/ 04.1997 r.)

Miniaturyzacja oraz postęp technologiczny umożliwia 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 optymalny dobór trajektorii ataku (rys. 7).

Główną zaletą bomb elektromagnetycznych jest to, że mogą one być przenoszone 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 one mogły przenosić również i bomby elektromagnetyczne.



Rys. 7. Atakowanie bombami elektromagnetycznymi. (Źródło: Kopp C. The E-Bomb - A Weapon of Electrical Mass Destruction http://www.cs.monash.edu.au/carlo/ 04.1997 r.)

Ponieważ bomby te będą znacznie prostsze w konstrukcji i obsłudze i tańsze w produkcji od pocisków przeciwradiolokacyjnych to 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.

2.2.2.3.4. 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 trwałą destrukcją. Bomby elektromagnetyczne używane będą głównie dla 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 zarówno od siły rażenia bomby, ale też i 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 następować powinien atak fizyczny. Atak ten wykonany konwencjonalną amunicją zapobiegnie naprawie uszkodzonego sprzętu i utrwali osiągnięte skutki na dłuższy okres czasu.

Bomby elektromagnetyczne mogą być użytecznym narzędziem obezwładniania środków obrony powietrznej. Mogą nawet skutecznie rywalizować z pociskami przeciwradiolokacyjnymi. Szczególnie, gdy znana jest dyslokacja atakowanego obiektu ich skutki rażenia mogą znacznie przekraczać te, które można osiągnąć w wyniku zastosowania pocisków przeciwradiolokacyjnych.

Zaletą tego typu bomb jest możliwość ich stosowania w stosunku do obiektów wstępnie rozpoznanych. Możliwość ta wynika z ich stosunkowo dużej powierzchni rażenia. Dzięki temu można ograniczać konieczność stosowania drogich środków precyzyjnego rozpoznania.

Ponadto koleją 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 przy walce z lotnictwem. Mogą, bowiem niszczyć nie tylko jego systemy dowodzenia, ale także 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 przynieść może 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, nie dysponującym jednak taką bronią.

Elektromagnetyczna broń stanowić może dogodną alternatywę dla wykonania ataku strategicznego powodując wielkie koszty bez widocznych zniszczeń i 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.

2.2.3. Atak fizyczny

Jako element zintegrowanego wysiłku przeciwdziałania informacyjnego, atak ten polega na użyciu broni fizycznie niszczącej wyznaczone obiekty. Celem jest wpływanie na informację lub system informacyjny przeciwnika za pomocą fizycznej destrukcji. Atak fizyczny 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 może być dowodzenie i kontrola. Przykładami szczebla taktycznego mogą być; użycie amunicji precyzyjnej przeciw stacji przekaźnikowej lub użycie grupy specjalnej w celu przecięcia lub wykorzystania linii komunikacyjnej.

2.2.4. Działania psychologiczne (PSYOPS) (atak psychologiczny)

Działania psychologiczne (PSYOPS)[24] 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.

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. Podczas operacji na Haiti, ze-

---

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

społy „Comando Solo" sił powietrznych nadawały dwie informacje radiowe dziennie, informując społeczeństwo, że „Syn Demokracji" prezydent Jean-Bertrand Aristide, wkrótce wróci. Prezydent Jean-Bertrand Aristide mógł wkrótce wrócić. Podczas operacji „Just Couse", siły lądowe używały głośników, aby wywabić Manuela Noriegę z ukrycia i przekonać do poddania się tysiące panamskich żołnierzy. W podobnych sytuacjach jednostki sił powietrznych mogą być użyte do nadawania audycji radiowych i informacji przez głośniki, co może wpływać na społeczeństwo.

Plan użycia jednostek działań psychologicznych zakłada trzy, wzajemnie ze sobą powiązane typy zadań:

1. Zadania o charakterze strategicznym;
2. Zadania na szczeblu operacyjnym;
3. Zadania konsolidacyjne.

Istotę i zadania o charakterze strategicznym określa się następująco: **Bojowe działania psychologiczne o wymiarze strategicznym** są kierowane przeciwko całości sił zbrojnych z jednoczesnym oddziaływaniem na jego ludność. Prowadzi się je łącznie z operacjami bojowymi lub niezależnie od nich. Nie oczekuje się od nich natychmiastowych wyników tych działań Ich efekty mogą być widoczne dopiero po upływie dłuższego czasu. Działania te prowadzą do obniżania, osłabiania, zachwiania odporności psychicznej przeciwnika, dezintegracji jego morale i wyeliminowania z walki. Na szczeblu strategicznym, PSYOP może przybierać formy: politycznego lub dyplomatycznego stanowiska, oświadczeń lub komunikatów.

Działania psychologiczne o wymiarze operacyjnym. Na szczeblu operacyjnym planowanie działań psychologicznych może zawierać dystrybucję ulotek, użycie głośników i inne środki transmitowania informacji, które mogą zachęcać siły przeciwnika do dezercji, ucieczki, poddania się wzbudzenia strachu, lub buntu.

Działania psychologiczne o wymiarze taktycznym są prowadzone przeciwko oddziałom i pododdziałom przeciwnika na polu walki w pasach i na kierunkach działania związków taktycznych i operacyjnych. Planują je oficerowie specjaliści wyższych sztabów, a realizują organiczne i przydzielone pododdziały ds. akcji psy-

chologiczno-propagandowych. Głównym zadaniem działań psychologicznych na tym szczeblu jest przygotowywanie, wspieranie, a w sprzyjających warunkach nawet zastępowanie działań bojowych środkami i metodami psychologicznymi, psychotechnicznymi, informacyjnymi czy dezinformacyjno-manipulacyjnymi. Są, więc działania tego rodzaju organiczną bronią wsparcia, gdyż ułatwiają wykonanie zadań taktycznych i operacyjnych wojsk własnych.

Działania psychologiczno o charakterze konsolidacyjnym są prowadzone głównie wśród własnej ludności. Ciężar tych działań spoczywa w zasadzie na instytucjach cywilnych odpowiedzialnych za porządek i bezpieczeństwo w czasie wojny. Wojsko włącza się do tych działań, ponieważ ich efekty dotyczą bezpośrednio potrzeb, interesów i sytuacji sił zbrojnych. Dlatego też podstawowym zadaniem działań konsolidacyjnych jest bezwzględne zapewnienie dyscypliny zaplecza, neutralizowanie i opanowanie żywiołowych reakcji ludności (paniki), otworzenie warunków do przeprowadzenia mobilizacji i przedsięwzięć alarmowych, zapewnienie swobody manewru sił własnych.

W działaniach bojowych stosuje się głównie dwie metody prowadzenia działań psychologicznych: *pośrednia i bezpośrednią.*

Metoda pośrednia stanowi podstawowy sposób oddziaływania na wojska przeciwnika. Realizowana ona jest przy pomocy materiałów drukowanych, audycji radiowych, elektroakustycznych i w określonych warunkach także 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 na polu walki w odniesieniu do małych grup i pojedynczych osób np., jeńców wojennych, zbiegów itp. i polega ona na bezpośrednim kontakcie nadawcy i odbiorcy. W działaniach bojowych dominuje metoda pośredniego oddziaływania.

2.2.4.1. Sposoby oddziaływań psychologicznych na wojska i ludność przeciwnika

Ze względu na sposób przekazu treści wyróżnia się następujące rodzaje oddziaływań psychologicznych na przeciwnika:

- **Przy użyciu materiałów drukowanych;**
- **Za pomocą radia;**
- **Poprzez rozgłośnie elektroakustyczne;**
- **Z wykorzystaniem telewizji;**
- **Z wykorzystaniem Internetu.**

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

2.2.4.2. Oddziaływanie przy użyciu 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 stosowane są najczęściej następujące materiały drukowane:

- **Ulotki;**
- **Materiały poglądowe;**
- **Falsyfikaty;**
- **Druki zwarte.**

Dla działań psychologicznych szczególną, można rzec priorytetową wartość ma apelacyjna część materiału drukowanego, choć prawdą jest - i występuje tu

zgodność wśród teoretyków - że 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 wg 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, kapitulacji i poddania się.

Ulotki ze względu na czas przygotowania oraz warunki użycia 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 jednakże, ze względu na ogólnikowy charakter i uniwersalną treść, mniej efektywne niż te, które przygotowuje się na konkretną sytuację. Są one z reguły przygotowywane już w okresie pokojowym. Ulotki sytuacyjne przygotowywane są bezpośrednio przed akcją, zawierają specyficzne treści, związane z konkretną sytuacją bojową. Są one przeznaczone z reguły 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 aktualnych przeżyć i oczekiwań. Np. rozsądne będzie nawoływanie do poddania się, gdy w danej sytuacji przeciwnika wojska nie mają innej, alternatywnej możliwości działania. 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 (tj. ludności w określonym obszarze, grup etnicz-

nych i religijnych oraz innych wyselekcjonowanych grup ludności i żołnierzy przeciwnika).

Niektórzy specjaliści zachodni dzielą ulotki na *strategiczne, taktyczne i konsolidacyjne*. Ulotka strategiczna adresowana jest zwykle do wojsk i ludności cywilnej przeciwnika na całym obszarze przeciwnika. Jej długofalowym celem jest osłabienie woli nieprzyjaciela do stawiania oporu poprzez zwiększanie wewnętrznych niesnasek i napięcia oraz wsparcie ruchu oporu na terytorium przeciwnika. 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 one 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 wojska przeciwnika i ludność cywilna pozostające na danym obszarze.

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* itp.

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 planowania działań psychologicznych na wojska i ludność cywilną przeciwnika z wykorzystaniem 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.

2.2.4.2.1. 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 zaliczyć można:

a) szeroki zakres oddziaływania - programy radiowe mogą docierać jednocześnie do masowych i zróżnicowanych grup odbiorców;

b) wszechstronność - możliwość wykorzystania różnorodnych form wypowiedzi (wywiady, reportaże, apele, wezwania itp.);

c) łatwość percepcji przez odbiorców;

d) szybkość przygotowania audycji, także w warunkach polowych.

W działaniach psychologicznych stosuje się następujące formy przekazu radiowego:

- **Codzienne serwisy informacyjne z 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 itp.;**
- **Komentarze poświęcone sytuacji polityczno-militarnej oraz wydarzeniom wojennym**.

Do emisji określonych audycji mogą być wykorzystywane środki walki radioelektronicznej w ramach zakłócania i dywersji radiowej.

Doświadczenia z zakresu oddziaływania radiowego na żołnierzy i ludność cywilną podczas konfliktu zbrojnego unaoczniają, że zakamuflowane rozgłośnie radiowe/występujące pod innym szyldem niż jest ich właściwa przynależność, 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 ograniczającymi 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 dla wsparcia działań bojowych prowadzonych 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 prowadzone są z własnego ugrupowania bojowego i bezpośrednio wspierają działania wojsk własnych. Ich zaletą jest możliwość natychmiastowej reakcji na zmiany w sytuacji bojowej na polu walki. Ich zastosowanie determinują w znacznym stopniu warunki terenowe i meteorologiczne. Audycje elektroakustyczne dzielą się na:

a) **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;

b) **Audycje dźwiękowe o charakterze nękającym**. Mają one na celu zmniejszenie odporności psychicznej i fizycznej żołnierzy przeciwnika poprzez emisję określonych sygnałów dźwiękowych ó określonej częstotliwości (2-15 Hz) i poziomie głośności (115-155 dB), wywołujących i podtrzymujących stan stresu, a w skrajnych przypadkach doprowadzających nawet do zaburzeń funkcjonowania organizmu;

c) **Audycje mieszane**, które w zależności od charakteru oraz relacji między słowami a sygnałami dźwiękowymi realizować mogą wymienione w pkt. a i b cele.

Czas emisji audycji elektroakustycznej nie powinien przekraczać 30 sekund. Rozgłośnie elektroakustyczne dzielą się na mobilne, które montowane są na pojazdach kołowych, gąsienicowych, środkach latających oraz przenośno-plecakowe, przenoszone przez żołnierzy.

Oddziaływanie telewizyjne

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

2.2.4.2.2. Oddziaływanie przez Internet

Współcześnie 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 wynikać może z przyjemności lub towarzyszyć wykonywaniu obowiązków służbowych. Ponieważ długość czasu spędzanego przy Internecie stale rośnie, więc możliwości tego oddziaływania stają się również coraz większe. W oddziaływaniu tym stosowane mogą być techniki manipulacji społecznej, marketingu oraz stosowane w oddziaływaniach przez inne, omawiane media.

2.2.5. Dezinformacja wojskowa (mylenie)

Dezinformacja wojskowa[25] wprowadza przeciwnika w błąd, powodując, że działa on zgodnie z planami organizatora dezinformacji. Działania dezinformacji

---

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

wojskowej rozciągają się na wszystkie szczeble wojny i zawierają komponenty ofensywne i defensywne. Dezinformacja wojskowa może odwrócić uwagę od, lub zapewnić osłonę dla operacji wojskowych myląc i rozpraszając siły przeciwnika. Dezinformacja wymaga głębokiej znajomości kultury, polityki, doktryny, oraz procesu decyzyjnego przeciwnika, które to wiadomości mogą być wykorzystane przez planistów.

Nowoczesne możliwości dezinformacji można zilustrować na przykładzie przeciwnika nie dysponującego samolotami tankowanymi w powietrzu. Jeśli siły powietrzne mogą spowodować, że wrogi dowódca wyśle swoje myśliwce zbyt wcześnie, to tak jakby ich w ogóle nie wysłał.

Działania dezinformacji są zależne od dokładnego i wiarygodnego rozpoznania, śledzenia, a także od ścisłej współpracy z kontrwywiadem. Kluczem jest przewidzenie motywów przeciwnika i jego akcji. Kiedy formułowana jest koncepcja dezinformacji, szczególna uwaga musi być zwrócona na to jak dowódcy chcieliby, aby przeciwnik działał w krytycznych okresach. Te pożądane działania stają się później celem działań dezinformacyjnych.

Działania dezinformacyjne muszą być planowane z góry na dół, a plany podrzędne muszą wspierać plan nadrzędny. Plany mogą zawierać użycie jednostek niższego szczebla, chociaż podwładni mogą nie znać ogólnej koncepcji. Dowódcy na wszystkich szczeblach mogą planować działania dezinformacji, ale muszą skoordynować swoje plany z przełożonymi w celu osiągnięcia skupienia wysiłku. Z powodu bezpieczeństwa działań tylko wybrana grupa starszych dowódców i oficerów sztabu może wiedzieć, które akcje są jedynie dezinformacjami. Mimo to limitowanie detali tych działań może powodować zamęt i musi być ściśle monitorowane przez dowódców i ich sztaby. Działania dezinformacji wojskowej są potężnym narzędziem w działaniach militarnych. Siły i środki muszą być podporządkowane potrzebom działań dezinformacyjnych, aby uczynić je wiarygodnymi i wartymi krótkoterminowych kosztów.

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. Nie używano pojęcia dezinformacja, natomiast wszelkie 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 wieku 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". W wyniku uogólnień i przeprowadzonej analizy, Sun-Tzu określił pięć głównych metod stosowania fortelu: działania pozorujące; oddziaływanie na psychikę; dezorganizowanie szeregów; usypianie czujności; wykorzystanie błędów, niedoskonałości, nieprzygotowania i nieostrożności przeciwnika.

Obszarem dezinformacji najbardziej istotnym z punktu widzenia sił zbrojnych i obronności państwa 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, tj. **system dowodzenia i kontroli** oraz **system rozpoznania**. Istotą tej dezinformacji jest przekazywanie przez system rozpoznania przeciwnika fałszywych informacji do jego centrum decyzyjnego. Natomiast istotą dezinformacji w stosunku do wojsk własnych jest 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 odnośnie prawdziwych zamierzeń, planów i przeprowadzanych przedsięwzięć o znaczeniu militarnym**.

W trakcie przygotowania i prowadzenia operacji bojowej dezinformacja wojskowa będzie jednym z elementów uzyskania zaskoczenia, a tym samym osiągania powodzenia w walce. Pod względem treści w obecnej dobie staje się ona wyjątkowo rozgałęzioną i wielostronną dziedziną strategii wojennej i wojskowej państwa, będącej w ścisłym związku z polityką, gospodarką oraz nauką i techniką.

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.

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 dezinformacyjne realizowane są zgodnie z planem dezinformacji naczelnego dowództwa, pod bezpośrednim kierownictwem sztabu generalnego. 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 zabezpiecze-

nia 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 operacyjho-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 zabezpieczenia logistycznego.

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

Dezinformacja wojskowa w skali strategicznej, realizowana przez siły i środki sił zbrojnych i państwa zgodnie z opracowanym przez sztab generalny planem, powinna być organizowana zarówno w czasie pokoju, jak i w czasie wojny. Potwierdzeniem działań pozornych i fałszywych informacji organizowanych na szczeblu strategicznym, powinny być działania dezinformacyjne w skali operacyjnej i taktycznej. 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, tj.: **przekaz, dokument i działania**. Przekaz może być realizowany dwiema metodami, tj. *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 również telewizję, radio oraz wojskowe i cywilne środki łączności. Natomiast *metoda pisemna* dezinformacji polega na zamierzonym opracowaniu i terminowym dostarczeniu przeciwnikowi dokumentów tekstowych, takich jak: fałszywe dyrektywy, rozkazy, zarządzenia bojowe, meldunki. Uzupełnia się te dane poprzez publikowanie dezinformacyjnych danych 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, 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 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 dla wprowadzenia 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.

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, tj. zamierzonym „zagubieniem" fałszy-

wych 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 nie zamkniętych sejfach.

Do prowadzenia dezinformacji mogą być użyte różne siły i środki będące w dyspozycji organów państwowych i wojskowych. Skala ich użycia będzie zależna od sytuacji polityczno-wojskowej, siły przeciwnika, głównego kierunku zainteresowania wywiadu i rozpoznania przeciwnika oraz ich możliwości, jak również od zakresu i treści głównych przedsięwzięć dezinformacyjnych.

Siły i środki dezinformacji 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 mogą być zaangażowane następujące grupy ludzi: działacze państwowi i wojskowi; pracownicy ambasad i misji; przedstawiciele różnych delegacji; ludność miejscowa; korespondenci prasy, radia i telewizji; telefoniści i radiotelegrafiści węzłów łączności; skład osobowy wojsk własnych i przeciwnika; zbiegowie i jeńcy wojenni; agenci i dywersanci; partyzanci. 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 dla zdobywania 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 dla 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 pośrednictwem, której 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 cywilna, w tym codzienną i periodyczną; *wydawnictwa* - broszury informacyjne, literaturę techniczną i popularnonaukową, plakaty i ulotki, *filmy* - dokumentalne, popularnonaukowe, o tematyce technicznej i wojskowej oraz reklamowo; *radio, telewizje, sprzęt krótkofalowy, telefony, dyktafony, magnetofony, magnetowidy, korespondencję pocztową, tj. telegramy, listy i karty pocztowe*.

Środki masowego przekazu są również wykorzystywane w działaniach dezinformacyjnych poprzez 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 mogą być wykorzystane: środki wojsk rakietowych i artylerii, tj. rakiety kasetowe, pociski artyleryjskie; środki sił powietrznych, tj. rakiety skrzydlate, kasetowe bomby lotnicze, samoloty bezpilotowe, szybowce; środki sił morskich, technika bojowa i specjalna, wykorzystywana do imitacji i demonstracji działań pozornych oraz makiety techniki i uzbrojenia specjalnego.

Tabela - 4. Formy, metody, sposoby, siły i środki dezinformacji wojskowej

Formy	**Przekaz**		**Dokument**	**Działanie**
Metody	**Ustna**	**Pisemna**		
Sposoby	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	4. Publikacja fałszywych informacji w prasie wojskowej i cywilnej	5. Zamierzone zagubienie fałszywych lub odtajnionych dokumentów o znaczeniu operacyjno-strategicznym.	6. Przygotowanie i realizacja działań pozornych
Siły	▪ 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.			
Środki	▪ Radio, sprzęt audio telewizyjny; ▪ Środki łączności wojskowej.	▪ Wydawnictwa, prasa plakaty; ▪ Korespondencja pocztowa; ▪ Rakietowe pociski propagandowe; ▪ Środki sił powietrznych.	▪ Spreparowane dokumenty wojskowe	▪ Technika bojowa i specjalna do imitowania działań pozornych; ▪ Makiety urządzeń wojskowych i uzbrojenia

3. PERSPEKTYWY ROZWOJU OFENSYWNEJ WALKI INFORMACYJNEJ W DZIAŁANIACH POWIETRZNYCH

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 osiągnięty może być dopiero w wyniku serii różnych działań i osiągnięciu kilku celów pośrednich. Mamy wtedy do czynienia z sekwencją różnych działań nazywaną 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 podporządkowuję 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 jednakże zawsze jest wspierany i wspierający. Wynika to z doświadczenia oraz z postulatów wielu zasad sztuki wojennej. Takie podejście przyjmowane jest w amerykańskiej doktrynie działań połączonych jak również i w doktrynie działań połączonych NATO.

W rezultacie siły powietrzne mogą prowadzić walkę o przewagę w powietrzu i walkę o bezpośrednie osiągnięcie celu politycznego (powietrzny atak strategiczny) lub wspieranie działań innego komponentu. Ponadto, niezależnie od tego prowadzić będą działania zabezpieczające własną aktywność.

Podobnie, jak w klasycznej koncepcji działań powietrznych walka informacyjna sił powietrznych może mieć na celu osiągnięcie przewagi informacyjnej. Przewaga ta będzie niezbędna dla prowadzenia zasadniczych działań zmierzających do osiągnięcia politycznego celu w danym konflikcie. Tymi zasadniczymi działaniami mogą być zarówno działania klasycznej walki, jak też i działania walki informacyjnej. Obecnie gwałtownie rozwijający się potencjał walki informacyjnej i rosnąca wrażliwość państw na tę walkę umożliwia 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 samodzielny rodzaj sił odpowiedzialny za tę walkę. Jednocześnie z wcześniejszych rozważań wynika, że walka informacyjna jest rozległym zjawiskiem obejmującym wszystkie obszary aktywności państwa w związku, z czym niemożliwe jest utworzenie samodzielnego rodzaju sił, gdyż musiałby się on składać z elementów zaczerpniętych ze wszystkich obszarów aktywności państwa. Możliwe i pożądane zaś jest utworzenie organu koordynującego przedsięwzięcia walki informacyjnej i działań informacyjnych prowadzonych przez wszystkie komponenty państwa. Ponadto walka informacyjna, a szczególnie mająca osiągać strategiczne cele polityczne powinna mieć jak najszerszy zasięg. Dlatego też siły powietrzne samodzielnie walkę informacyjną mogą prowadzić jedynie w ramach wspierania działań powietrznych lub, 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 powietrznych w walce informacyjnej państwa zależeć będzie od stopnia rozwoju możliwości prowadzenia tej walki. Ponieważ nawet gdyby powstały jakieś siły tej walki to i tak nie zwolni to innych komponentów państwa z uczestniczenia w tej walce. Poziom zdolności do prowadzenia walki informacyjnej w siłach powietrznych zależał będzie od wizji przyszłej misji sił powietrznych oraz determinacji w jej wdrażaniu.

3.1. Walka o przewagę informacyjną

Wynalezienie lotnictwa i jego militarne zastosowanie w stosunkowo niedługim czasie spowodowało głębokie zmiany zarówno sytuacji polityczno militarnej jak i sztuki wojennej. Przed pojawieniem się lotnictwa zagrożenie atakami ogniowymi rozpościerało się na płytki obszar 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 dużych głębokościach państwa przeciwnika należało najpierw przeprowadzić trudną operację zdobycia i zajęcia terenu. Działania bojowe okresu przedlotniczego toczyły się w stosunkowo niewielkich obszarach bezpośrednich starć wojsk. Przybierały one formy bitew a w późniejszym okresie wydłużonych linii styczności bojowej wojsk wzdłuż, których rozciągały się pasy 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. Dotychczas bezpieczne obiekty strefy tyłowej znalazły się nagle w zasięgu samolotów uderzeniowych. Bezpieczne dotychczas ośrodki władzy, rejony rozmieszczenia przemysłu, zasoby infrastruktury, różnego typu zapasy, rejony mobilizacji wojsk a także miejsca przebywania i aktywności ludności cywilnej mogły zostać w każdej chwili zaatakowane. Te potencjalne możliwości pogłębiane były przez szybko rozwijające się teorie wojny powietrznej oraz doktryny wyrażające gotowość państw do korzystania z tych nowych możliwości. Lotnictwo uderzeniowe,

ale również 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 jakichkolwiek działań militarnych, ale też i 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 głównym wykonawcą 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 jego 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 lub 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 je także rezultaty współczesnych konfliktów zbrojnych"[26].

Współczesny rozwój ludzkości wyłania nową formę cywilizacyjną, jaką jest społeczeństwo informacyjne. W formacji tej największym dobrem jest informacja. Jest ona zarówno 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 jednakże obecnie informacja staje się podstawą wszelkiej aktywności i coraz częściej jej celem. W sferze walki informacja staje się także substytutem broni a nawet najskuteczniejszą bronią przyszłości. Informacja dociera, bowiem bezpośrednio do umysłu

---

[26] W. Michalak, *Dominacja z powietrza*, Warszawa 1999, s. 13-14.

człowieka i może kształtować jego świadomość skutecznej niż za pośrednictwem fizycznej presji zewnętrznej.

Badając sferę walki informacyjnej Gabriel 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”[27].

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**. 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[28]. Teoretycy uznają, iż: „Aby zwyciężyć należy wygrać walkę informacyjną”[29], oraz „W dobie powszechnej informatyzacji pokonanie przeciwnika w *Infowar* może być czynnikiem decydującym o zwycięstwie w całej operacji wojennej”[30], a także „Walka informacyjna to działania podejmowane dla osiągnięcia przewagi informacyjnej”[31]. Również praktyka treściami 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

---

[27] G. Nowacki, *Współczesne poglądy na prowadzenie walki informacyjnej*, Warszawa 2001, s. 30.
[28] *Information Operations. AFDD 2-5*, USAF 1998, s.2.
[29] G. Nowacki, *Walka informacyjna – próba kategoryzacji. Rozprawa doktorska*, Warszawa 1999, s. 61.
[30] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999, s. 82.
[31] 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.

funkcję"[32] a „ dominacja w informacyjnym spektrum jest równie ważna w obecnym konflikcie jak w przeszłości było zajmowanie terenu czy panowanie w powietrzu."[33]

Podobnie jak walka o przewagę w powietrzu dzieli się na ofensywną i defensywną, **tak i** walka o przewagę informacyjną sił powietrznych dzieli się na ofensywną i defensywną. **Siły powietrzne w ramach walki o panowanie informacyjne mogą, więc prowadzić:**

- Ofensywną walkę informacyjną;
- Defensywną walkę informacyjną (obronę informacyjną).

Tak samo jak w przypadku dominacji w powietrzu **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 ofensywnej walki informacyjnej powinno być również 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 pełno wymiarowa 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

---

[32] *Information Operations. AFDD 2-5*, USAF 1998, s.1.
[33] Tamże, s. 1.

walki informacyjnej charakteryzowany zaś będzie skalą zaangażowania poszczególnych stron.

Celem walki o panowanie informacyjne jest uzyskanie przewagi informacyjnej. **Przewaga informacyjna** to stopień dominacji 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 panowanie informacyjne powinien stać się przede wszystkim ofensywny potencjał walki informacyjnej.

3.1.1. Ofensywny potencjał walki informacyjnej

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 oraz potrafiący przygotować narzędzia i metody takiego ataku oraz bazy wiedzy w tym zakresie.

Zasoby ofensywnych działań elektronicznych obejmują siły i środki tj. 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 elek-

tromagnetycznego w różnych zakresach widma, np. mikrofalowym, podczerwonym, widzialnym, nadfioletowym (lasery).

Zasoby ofensywnych działań powietrznych to 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 złożony ze specjalistów projektujących informacyjne treści przeznaczone dla 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, którym 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 itp.

Zasoby dezinformacji stanowić mogą zarówno wyspecjalizowane siły i środki, jak też takie, dla których zadania te są dodatkowymi. Do wyspecjalizowanych sił zaliczyć można wywiad i kontrwywiad, które wykonują inne zadania, jednakże mogą stanowić jedno z narzędzi prowadzenia dezinformacji.

Nawet tak w zarysie przedstawiony 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. 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 prze-

wagę informacyjną zniszczenie ofensywnego potencjału tej walki jest niemalże niemożliwe gdyż jest on zbyt różnorodny i rozległy.

Jednakże 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 działań 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 powietrzne jednakże mogą być istotnym aktorem tej walki. Dysponują, bowiem wysokim potencjałem intelektualnym związanym z eksploatowaniem zaawansowanego technologicznie sprzętu, wymagającego wysokiej kultury technicznej. Potencjał ten może być zaadaptowany do potrzeb prowadzenia działań informacyjnych.

W ramach ofensywnej walki informacyjnej stosowane mogą być następujące formy działań:

- Atak informatyczny (w sferze przetwarzania danych cyfrowych);
- Atak elektroniczny;
- Atak fizyczny;
- Działania psychologiczne;
- Dezinformacja (mylenie)

Atak informatyczny może być stosowany w stopniu odpowiednim do rozwiniętych w siłach powietrznych możliwości w tym zakresie. Do prowadzenia ataku informatycznego niezbędne jest posiadanie przede wszystkim wykwalifikowanych specjalistów informatyków, którzy będą umieli zaprojektować i opracować odpowiednie do

potrzeb kody komputerowe oraz infrastruktury niezbędnej do użycia tych kodów. Takie zaprojektowanie wymaga wiedzy na temat organizacji i inżynierii podlegających atakowaniu systemów przeciwnika, a więc wymaga rozpoznania. Wiedza ta jest niezbędna nie tylko dla 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 specjalistyczny sprzęt. Dotyczyć to będzie sytuacji, w których stosuje się wyrafinowane metody przenikania, np. przez użycie specjalnych impulsów elektromagnetycznych lub przy zastosowaniu komunikacji radiowej itp. Jednakże wiele form ataku informatycznego może być stosowanych przy wykorzystaniu klasycznych sieci komputerowych. Potrzebna jest jedynie stosunkowo niewielka grupa wysokiej klasy specjalistów informatyków i operatorów mających wizję odpowiedniego wykorzystania tych informatyków.

Atak elektroniczny jest stosowaną powszechnie przez siły powietrzne formą prowadzenia działań. Jest on, bowiem elementem walki elektronicznej, mającej w siłach powietrznych długą historię stosowania. Atak ten w wykonaniu sił powietrznych 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 skuteczna jedynie w czasie trwania ataku i dlatego powinna być stosowana raczej do zabezpieczania działań w zestawieniu 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 destrukcyj-

nymi mającymi zastosowanie w ramach ataku elektronicznego jest broń laserowa oraz nadajniki mikrofalowe dużej mocy.

Siły powietrzne doskonale nadają się do prowadzenia ataku fizycznego. Dysponują, bowiem możliwościami przenikania w głąb terytorium przeciwnika i atakowania ważnych, z punktu widzenia walki o przewagę informacyjną, obiektów. Atak ten prowadzony może być przy zastosowaniu klasycznych form i sposobów działań powietrznych. Atak fizyczny może być skutecznym sposobem eliminacji części ofensywnego potencjału walki informacyjnej przeciwnika. Jego zastosowanie ograniczone jest jednak do konfliktu zbrojnego. Atak ten 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 wyeliminowania atakowanego obiektu z funkcjonowania.

W działaniach psychologicznych siły powietrzne uczestniczą od swojego początku. Klasycznym zadaniem było rozsiewanie ulotek. Jednakże działania psychologiczne są mniej skutecznym środkiem ataku ofensywnego potencjału walki informacyjnej przeciwnika. Może on być stosowany jako uzupełniająca forma ataku. Obecnie szczególnie przydatnym 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 służyć powinna przede wszystkim obniżeniu efektywności ofensywnych działań informacyjnych przeciwnika. Dezinformacja jest atakiem informacyjnym gdyż wprowadza nieprzyjacielowi fałszywą informację stymulując reakcje nieprzyjaciela w pożądanym kierunku. Siły powietrzne w ramach ofensywnej walki o przewagę informacyjną powinny stosować dezinformację, aby uniemożliwić przeciwnikowi rozpoznanie koncepcji działań, ich efektywności i zamiarów.

Nieodłączną od ofensywnej jest defensywna forma walki o przewagę informacyjną, 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.

3.2. Informacyjny atak strategiczny

Informacyjny atak strategiczny jest inspirowany koncepcją powietrznego ataku strategicznego, dlatego też koncepcja ta jest scharakteryzowana w treści pierwszego podrozdziału. Prezentacji tej koncepcji poświęcono więcej miejsca niż innym gdyż jest ona nową i nie zawsze właściwie rozumianą.

Analogią do niej jest koncepcja informacyjnego ataku strategicznego. Jest ona przedstawiona w podrozdziale drugim. Jej prezentacja koncentruje się w dwu modułach przedmiot i formy informacyjnego ataku strategicznego. Stanowią one treści podrozdziałów wewnętrznych.

3.2.1. 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 „wojna" jest pojęciem względnym i niejednoznacznym. Wynika to zarówno z względności oceny poszczególnych aktorów (jeden może traktować dany konflikt, jako wojnę inny zaś, jako incydent zbrojny), jak też z coraz większymi trudnościami z wyznaczeniem granicy tego, co się nazywa zbrojny (m.in. z powodu poszerzania się zakresu broni). Dla potrzeb niniejszych rozważań lepszym byłoby posługiwanie się kategorią „konfliktu", w którym zaistniała sprzeczność interesów w związku z czym strony prowadzą kooperację negatywną (walkę) dla osiągnięcia celów, które zaspokoją własne interesy. W literaturze jednak powszechnie przyjęło się używanie pojęcia „wojna" w odniesieniu do odpowiednio ostrych form konfliktu. Kla-

sycy badający zjawisko wojny niewątpliwie wnieśli dużo wiedzy o konflikcie, którego formą jest wojna. Dlatego warto sięgnąć do ich dorobku.

Wojna jest narzędziem polityki i jest prowadzona w celach politycznych[34]. 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 skierowane być powinny na ten cel. Ten sposób myślenia znajduje szerokie wsparcie w środowisku wojsk lądowych, które skłania się ponadto do przekonania, że walka lądowa jest decydującą w rozstrzygnięciu ostatecznego wyniku. W tym wypadku efektywność użycia sił powietrznych jest mierzona 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.

Inna sposób myślenia uznając prymat polityki nad wojną zakłada, że to polityczne decyzje „produkują" końcowy efekt. Najlepszym wówczas sposobem osiągnięcia zakładanego efektu końcowego jest dokonanie skalkulowanego nacisku na kluczowe miejsca systemu państwa, tzw. środki ciężkości. Taka akcja przekona przywództwo przeciwnika, że opór nie ma sensu, bo koszt oporu jest wyższy niż 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 i podkreślają oni możliwość wygrania wojen przez przerwanie spójności tej triady za pomocą odpo-

---

[34] R. Szpyra, *Współczesna wojna powietrzna. Wybrane problemy*, Warszawa 1998, s. 7.

wiedniego zastosowania przemocy. W myśleniu zwolenników potęgi powietrznej ta przemoc powinna być skierowana zarówno na niszczenie możliwości, tj. infrastruktury produkcyjnej i sił zbrojnych jak również na zerwanie psychologicznej woli przeciwnika a szczególnie 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 najszybszym 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 II wojny światowej oraz horror broni jądrowej czasem 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 pomiędzy strategicznymi bombardowaniami a nieograniczonymi atakami na ludność cywilną. Jakkolwiek miało to miejsce w niektórych poglądach a także miało miejsce w niektórych operacjach II wojny światowej nie oznacza to, 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 związane są 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 prowa-

dzone są dla osiągania celów taktycznych a pośrednio również operacyjnych i strategicznych. **Teoria potęgi powietrznej koncentruje się na strategicznym i operacyjnym poziomie wojny i użyciu potęgi powietrznej do bezpośredniego osiągania strategicznych celów wojny.**

W kontekście rozpatrywanego zagadnienia powszechnie uznany dorobek[35] 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[36] do zaadoptowania ich na grunt walki informacyjnej.

Aby wojna miała jakikolwiek sens[37] musi być prowadzona dla jakiegoś powodu. Może on czasami być błahy lub mało istotny, ale doświadczenia historyczne wskazują, że z pewnymi, mało istotnymi wyjątkami, większość władców wypowiadając wojnę czyniła to by coś osiągnąć na przykład dodatkowe terytoria, zahamowania działań przeciwnika, zemstę na wrogach lub wymuszenie zmiany religii. Bardzo niewielu prowadziło wojny dla zabawy.

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".

---

[35] Uznanie to wyraża się wieloma międzynarodowymi opiniami, cytowaniami i adaptacjami oryginalnych pomysłów.

[36] Badanie przydatności różnych teorii badano w oparciu o charakterystyki walki informacyjnej i działań informacyjnych.

[37] Poglądy te zostały zaprezentowane w: J.A. Warden III, *Air Theory for the Twenty-first Centur*, [w:] *Battlefield of the Future. 21st Century Warfare Issues*, Maxwell AFB 1995, s. 103-124 oraz R. Szpyra, *Rola sił powietrznych w wojnie przyszłości*, Warszawa 2000, s. 104-124.

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**. Jednakże do podstawowych można zaliczyć następujące trzy: **uczynienie przeciwnikowi oporu zbyt kosztownym, przy czym koszty mogą mieć charakter polityczny, militarny lub ekonomiczny; fizyczne uniemożliwienie przeciwnikowi podjęcie jakichś działań przez jego strategiczne lub operacyjne sparaliżowanie; całkowite zniszczenie przeciwnika**.

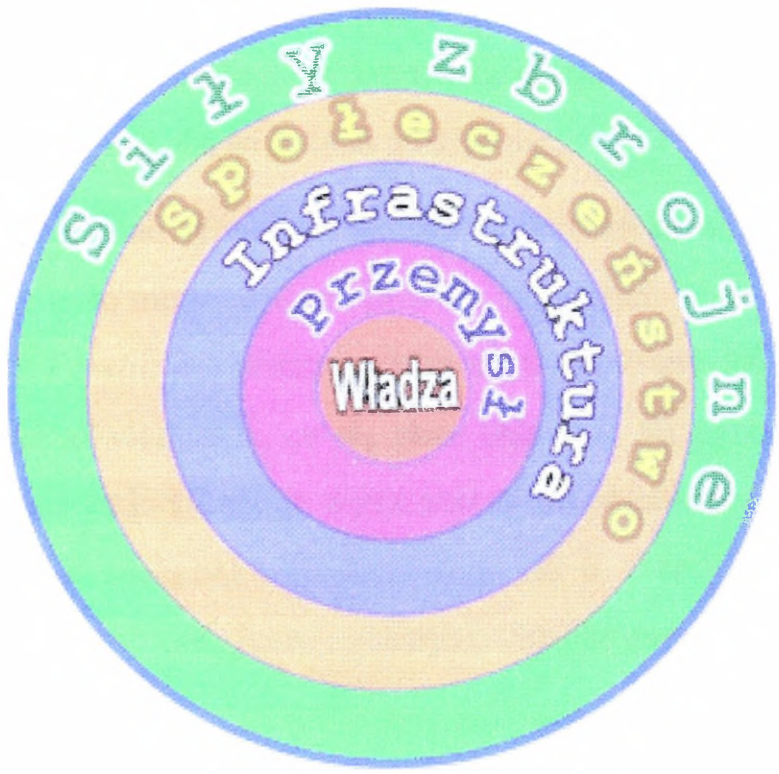
Ostatnia z tych możliwości była rzadko spotykana w historii z powodu, z jednej strony trudności wykonania, a z drugiej moralnych oporów i w związku z tym można ją w zasadzie pominąć, koncentrując się na dwóch pierwszych.

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 mogą poprzez swoje działania uniemożliwić nam osiągnięcie celu. Trudności w ocenie i przewidywaniu nie oznaczają jednak, że sposób ten jest niemożliwy do zrealizowania, a jedynie nie precyzyjny.

Z punktu widzenia potęgi powietrznej, naszym zadaniem jest określenie ceny (negatywnej lub pozytywnej), jaką trzeba będzie narzucić przeciwnikowi, aby nakłonić go do przyjęcia naszych warunków. Aby to uczynić musimy jednakże 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, bowiem każdy system oparty na życiu, zorganizowany jest w podobny sposób. Jedynie szczegóły mogą się różnić. Dla lepszego zobrazowania warto przedstawić model tych systemów w postaci pięciu pierścieni (rys. 8).

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 wspie-

rane 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 oraz piąte reprezentuje narodowe siły zbrojne rozmieszczone w polu.



Rys. 8. Model państwa według Wardena (źródło: Warden III J.A. „Air Theory for the Twenty-first Century" Battlefield of the Future. 21st Century Warfare Issues. Air University, Maxwell AFB 1995, s. 108).

Celem wojny jest zmuszenie przywództwa przeciwnika by czyniło, to czego chcemy. Należy uświadomić nieprzyjacielowi prawdopodobny skutek mających nastąpić działań, a także poinformować go o rozmiarach jego strat oraz prawdopodobnych długo i krótko terminowych skutkach wynikających z tych działań.

Nie mając możliwości spowodowania nie akceptowanych dla przeciwnika kosztów, należy być gotowym do narzucenia strategicznego paraliżu. Idea paraliżu jest dość prosta. Jeżeli nieprzyjaciel jest postrzegamy 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.

Oczywistym miejscem wywołania paraliżu systemu strategicznego jest poziom kierownictwa lub mózgu. Jednakże, co się 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. Przed tym, 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 osiągnąć na przeciwniku. Podejmowanie tej decyzji jest największym wyzwaniem intelektualnym**; gdy zdecydowaliśmy o tym, co chcemy osiągnąć określenie tego jak to mamy 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 takie 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. Naszym najlepszym przykładem wojny równoległej jest atak strategiczny na Irak. W granicach minut koalicja zaatakowała przeciwnika w ponad stu kluczowych miejscach. Celami były obiekty w całym Iraku na głębokości strategicznej. Wszystkie ważne funkcje państwa Irackiego zostały zatrzymane na długo. Serwis telefoniczny upadł, brak 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 Iraku w pierwszych 24 godzinach jak siły 8A powietrznej na Niemcy w czasie całego 1943 roku.

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, dochodzeniu do punktu kulminacyjnego, przegrupowaniu i zmiany. Istotnie, wojna była wysiłkiem z jednej strony do przełamania się przez linie obrony z atakami seryjnymi lub była to próba do przeszkodzenia takim atakom.

W Iraku, w kraju o podobnym obszarze, jak przedwojenne Niemcy, z taką samą ilością kluczowych urządzeń, które uległy zniszczeniu tak szybko, że nie było możliwe odtworzenie ich zdolności gdyż wymagały znacznych napraw. Atak równoległy przeciw Irakowi był skierowany przeciwko prawdopodobnie najlepiej przygotowanemu do obrony krajowi na świecie. Jeżeli zadziałało to w tym przypadku 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 przypadku 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; oraz atakuj właściwe obiekty uderzeń jednocześnie i tak szybko jak to jest tylko możliwe.

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 będą niemalże nie tknięte.

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 szybkie odzyskanie tego 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 kwestia czasu.

Strategiczne organizacje, włączając kraje, mają małą liczbę żywotnych obiektów na poziomie strategicznym. Te cele zwykle są małe, bardzo kosztowne, bez obiektów zapasowych i są trudnymi 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 jego zdolności do skutecznej odpowiedzi, im większy procent celów jest niszczonych w jednym uderzeniu, tym mniej prawdopodobna jest odpowiedź.

Broń precyzyjna pozwala na ekonomiczne niszczenie, faktycznie wszystkich szczególnie strategicznych i operacyjnych celi, 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 taka liczba pocisków skłoni ich przeciwnika do odwrotu lub poddania się. Rezultat był nie do przewidzenia, pełny niespodzianek i rządzony przypadkiem. Dzięki broni precyzyjnej nawet logistyka stała się prosta, zniszczenie Iraku na poziomie strategicznym, operacyjnym i taktycznym wymagało zniszczenia dwunastu tysięcy celi. Przez to nie jest dłużej potrzebne gromadzenie, bliżej nie określonej liczby amunicji, ze względu na to, że mała liczba broni precyzyjnej może zniszczyć coś ważnego.

Siły lądowe na szczeblu operacyjnym są niezwykle wrażliwe. Wspieranie znacznej ilości środków znajdujących się na ziemi jest problemem administracyjnym

nawet w czasie pokoju. Sukces zależy od efektownej dystrybucji informacji, paliwa jedzenia i amunicji. Wydajna dystrybucja zależy od odwróconej piramidy. Najpierw zgromadzone muszą być 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 realizowana przez siły lądowe – bo nie było odpowiednio dobrego substytutu. Obecnie koncepcja „okupacji powietrznej" jest rzeczywistością i w wielu przypadkach będzie wystarczającą. Irakijczycy podporządkowali się żądaniom ONZ w takim samym, a może nawet większym stopniu niż Francuzi Niemcom, gdy zostali 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 nie powstrzymana, 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 ta 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 wy-

ciągnięte 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 w przyszłości najważniejszym wysiłkiem w wielu przyszłych wojnach**.

Szczególną konceptualizacją przekonania o decydującym znaczeniu potęgi powietrznej[38] dla losów wojny jest idea precyzyjnych bombardowań. Przy tym nie odnosi się ona do taktycznej zdolności umieszczenia bomby lub pocisku bezpośrednio w lub obok wyznaczonego celu. Jednakże precyzyjne umieszczenie broni w celu dostarcza ważnej zdolności do wdrożenia szerszej koncepcji precyzyjnych bombardowań. Koncepcje bombardowań istnieją w różnych formach, jednakże najlepiej znane są jako produkt Taktycznej Szkoły Korpusu Powietrznego Stanów Zjednoczonych z lat 1930-tych.

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

---

[38] J.V. Martin, *Victory from Above. Air Power Theory and the Conduct of Operations Desert Shield and Desert Storm*, Maxwell AFB 1994, s. 6 oraz R. Szpyra, *Współczesna wojna powietrzna. Wybrane problemy*, Warszawa 1998, s. 26-28.

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 ważnym 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 i zastosowaniu najważniejszych operacyjnych zasad i wykorzystaniu możliwie najlepszego rozpoznania.

W konkluzji należy uznać, iż: **strategiczny atak powietrzny to działania bezpośrednio zmierzające do osiągnięcia efektów strategicznych przez uderzanie na środki ciężkości nieprzyjaciela.** Działania te są projektowane tak, aby osiągnąć ich cele bez konieczności wcześniejszego angażowania obszernymi działaniami militarnymi na operacyjnym i taktycznym szczeblu wojny, rozwiniętych w polu sił zbrojnych nieprzyjaciela. Ta funkcja może być realizowana dla 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 właściwie zastosowany, atak ten jest najefektywniejszym sposobem zastosowania potęgi powietrznej. Atak ten dostarcza dowódcy teatru możliwości stworzenia decydujących efektów przeciwko przeciwnikowi przy unikaniu strat ludzkich i materialnych.

3.2.2. Koncepcja informacyjnego ataku strategicznego

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 okaże się, że zagrożenie walką informacyjną i jej potencjalne 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[39] rozciągają się od do zakłócenia funkcjonowania większych państw przez małe organizacje lub państwa do poważnego sparaliżowania przez nie wielkich państw. Wiele państw lub organizacji jest w przededniu uzyskania zdolności do prowadzenia strategicznej walki informacyjnej, tj. takiej, która może poważnie zagrozić interesom bezpieczeństwa. Przy tym strategiczna walka informacyjna może być prowadzona bez deklarowania stanu wojny. Walka ta może być prowadzona przez ludzi nie noszących 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.

---

[39] R. Szafranski, *Mars Chuckles And Athena In Frustration* [w:] *NL Arms. Netherlands Annual Reviev of Military Studies 1999. Information Operations*, Breda 1999, s.37 oraz R. Szpyra, *Działania informacyjne i walka informacyjna we współczesnych i przyszłych zastosowaniach sił powietrznych*, [w:] „Przegląd Wojsk Lotniczych i Obrony Powietrznej" nr 9/2000, s. 6.

Również gospodarka zależna jest od infrastruktury informacyjnej. Wszystko, co celowo zdegraduje możliwości tej infrastruktury może być uznane za atak. Atak taki może być skierowany na wiele systemów takich jak finansowo-bankowy, energetyczny, telekomunikacyjny, hydrologiczny, ratunkowy, itp. Walka informacyjna oferuje nowy rodzaj projekcji siły. Jedną z jej form może być izolacja, która w XXI wieku 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 uruchomieniu, 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 prowadząc nawet do paraliżu kraju.

Również tzw. „miękka wojna”[40] (Soft War) mieści się w zakresie walki informacyjnej, lecz w globalnej skali. Jej celem jest nie tyle osiągnięcie przewagi informacyjnej, co manipulowanie przeciwnikiem (lub własnym społeczeństwem) za pomocą fałszywej lub zmanipulowanej informacji. Telewizja jest zwykle narzędziem tej walki. Używana jest ona 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 (...).**

---

[40] http://www.seas.gwu.edu/~reto/infowar/view.htm 26.01.2001.

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**.

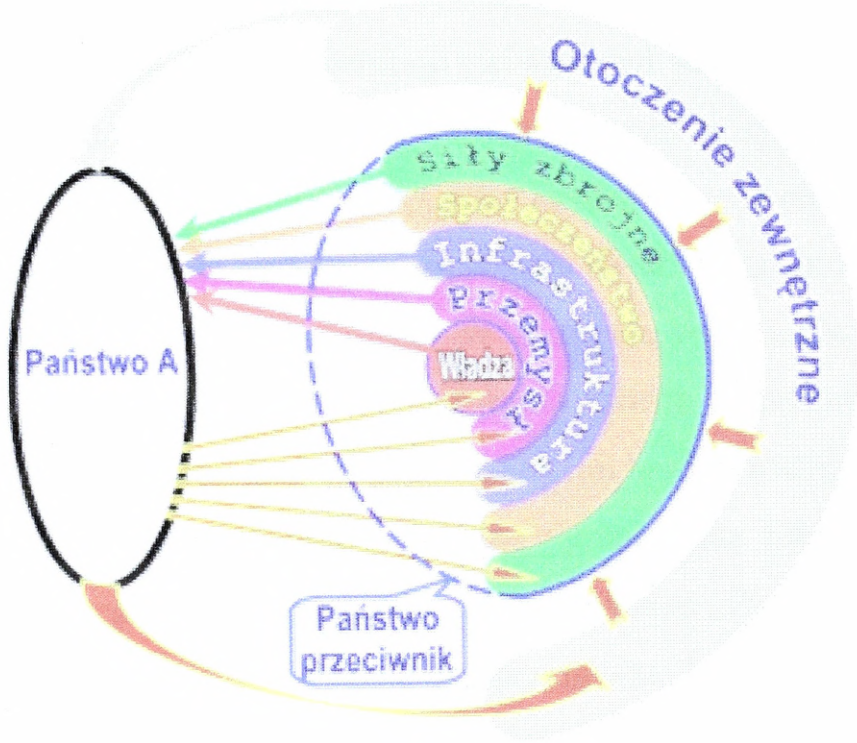
Ponieważ obiektem takiego ataku jest całe państwo to przez analogię do teorii powietrznego ataku strategicznego użytecznym będzie zastosowanie zaproponowanej przez Wardena modelu analizy systemowej państwa.

Do przyjęcia takiej analogii upoważniają oprócz własnych wniosków również informacje o rezultatach przeprowadzonych badań[41]. Daniel Kuehl analizujący je stwierdził m.in. „Dużo konceptualnego myślenia o strategicznym zastosowaniu potęgi powietrznej przeciwko żywotnym narodowym środkom ciężkości zostało przeprowadzone w Uniwersytecie Powietrznym (USA przy. R.S.) od czasu wojny w Zatoce Perskiej. Większość z tego dorobku może być bezpośrednio zastosowana w postulowanej strategicznej walce informacyjnej przeciwko tym samym środkom ciężkości"[42]. 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 przeciwnikowi jego zdolności dowodzenia (...), które zawiera także kierowanie państwem. Rosyjskie publikacje również postulują dezorganizację wszystkich ważnych systemów państwa takich, jak cywilny i militarny system kierowania, systemy komunikacji, energetyczne, transportowe, itp."[43].

---

[41] 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 Value Model" s. 55-78; G.R. Gurst, *Taking Down Telecommunications. Air University Press*, 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 i in. *Targeting Financial Systems as Centers of Gravity: "Low Intensity" to "No Intensity" Conflict*, [w:] "Defense Analysis", Vol. 10, No. 2, 1994, s. 181-208.
[42] D.T. Kuehl, *Strategic Information Warfare and Comprehensive Situational Awareness*, [w:] A.D. Campen, D.H. Dearth, R.T. Goodden, *Cyberwar: Security, Strategy, and Conflct in the Information Age*, Fairfax 1996, s. 189.
[43] Tamże, s. 189.

Do modelu Wardena dodane zostało otoczenie zewnętrzne, które jest też uczestnikiem działań informacyjnych. Można np. przez nie pośrednio oddziaływać na przeciwnika (rys. 9).



Rys. 9. Model strategicznego ataku informacyjnego.

3.2.2.1. 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; infrastruktura obejmująca takie elementy, jak: sieci energetyczna, komunikacyjna, gazowa, kolejowa drogowa, itp.; społeczeństwo i siły zbrojne.

Zgodnie z sugestiami Wardena **informacyjny atak strategiczny prowadzić powinien 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 dla informacyjnego ataku oraz od własnych możliwości w zakresie prowadzenia takiego ataku. **Przy planowa-**

niu 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 zapewnia zabezpieczenie własnych interesów i osiągnięcie pożądanych celów politycznych.

W przypadku dążenia do narzucenia przeciwnikowi **paraliżu** należy dokonać analizy poszczególnych elementów państwa i zidentyfikować miejsca krytyczne, tzw. „środki ciężkości"[44] 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 nie oznaczać końca istnienia, lecz istnienie to będzie wiązało się z bardzo ograniczonym funkcjonowaniem. Podobnie zniszczenie kilku mostów może nie sparaliżować całkowicie ruchu, jednakże radykalnie go ograniczyć.

Dla dokonania 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 tą należy następnie zestawić z własnymi możliwościami i warunkami. Może się, bowiem okazać, że co prawda istnieją miejsca krytyczne, wyeliminowanie, których sparaliżuje przeciwnika jednakże albo są one niedostępne, albo mimo dostępności nie dysponujemy zdolnościami do ich zaatakowania. Gdy istnieje taka sy-

---

[44] Nazwa ta pochodzi z tłumaczenia z angielskiego "center of gravity". Niektórzy autorzy tak, jak np. Tadeusz Kardaś proponują nazywać je „punktami ciężkości" (T. Kardaś, *Punkt ciężkości*,[w:] „Myśl Wojskowa" Nr 2/2000, Warszawa 2000, 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 „środek ciężkości" lepiej oddaje istotę tego pojęcia przez co będzie używany w niniejszych badaniach.

tuacja należy zastosować podejście pośrednie, zidentyfikować dostępne dla ataku 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.**

3.2.2.2. Formy informacyjnego ataku strategicznego

Informacyjny atak strategiczny prowadzony będzie 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 i 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 stosowane mogą być następujące formy działań:

- **Atak informatyczny (w sferze przetwarzania danych cyfrowych);**
- **Atak elektroniczny;**
- **Atak fizyczny;**
- **Działania psychologiczne;**
- **Dezinformacja (mylenie).**

Podobnie, jak w przypadku walki o przewagę informacyjną siły powietrzne mogą prowadzić **atak informatyczny**. Atak ten może być w niektórych okresach główną formą walki informacyjnego ataku strategicznego. Dotyczyć to będzie takich stadiów konfliktu, w których nie stosowane są 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 przypadku 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 i 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 z nad własnego terytorium. W bardziej zaawansowanym stadium konfliktu atak ten może przybrać formę uderzeń impulsów elektromagnetycznych lub wiązek energii mikrofalowej. Wykonanie ataków powietrznych z użyciem pocisków lub bomb elektromagnetycznych może sparaliżować całkowicie 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 w tym szczególnie bomby elektromagnetyczne. Środki te są, bowiem 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 uży-

ciem aniżeli w stosunku do innych bardziej „brutalnych" bo zabójczych w stosunku do ludzi środków rażenia. Jednocześnie skutki elektromagnetycznych ataków mogą być bardziej dotkliwe materialnie niż innych.

Strategiczny atak elektromagnetyczny koncentrował się będzie 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 wielkich ilości rozproszonych komputerów biurowych. Rozproszenie to i powszechność występowania praktycznie uniemożliwia uodparnianie na atak elektromagnetyczny gdyż koszty takiego przedsięwzięcia byłyby większe niż wartość ochranianego sprzętu. Sytuacja ta jest zasadniczo różna w stosunku do tej z przeszłości, gdy istniały ośrodki przetwarzania danych z dużymi komputerami. Sprzęt takich ośrodków rozmieszczany był w specjalnie przystosowanych pomieszczeniach a całość łatwiej było uodpornić na zewnętrzne oddziaływania elektromagnetyczne. Współcześnie jest to niemalże niemożliwe gdyż komputery rozlokowane są wszędzie tam gdzie ludzie prowadzą 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 elektromagnetyczny atak 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 takie 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 po-

wszechnym uzależnieniem wszystkich aspektów ludzkiej aktywności od elektryczności a ostatnio od komputerów i innych urządzeń przetwarzania i dystrybucji informacji to wszystkie podsystemy systemu państwa w modelu analizy Wardena są bardzo wrażliwe na atak elektromagnetyczny. Ze względu na powszechność występowania nie jest możliwym wyeliminowanie wszystkich urządzeń elektronicznym jednakże właściwa selekcja krytycznie ważnych elementów i ich elektromagnetyczne zniszczenie może doprowadzić do paraliżu państwa a w najlepszym przypadku do wytworzenia 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 mocno 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 elektromagnetyczną bronią 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, itp. Zniszczenie urządzeń automatyki może spowodować wielkie szkody ekonomiczne a nawet braki materiałów strategicznych. Również przemysł zbrojeniowy jest w nie mniejszym stopniu uzależniony od elektroniki i urządzeń elektrycznych i wrażliwy.

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

spowodować może niezwykle wysokie straty paraliżujące lub, co najmniej znacznie ograniczające funkcjonowanie przemysłu. Niemniej jednak przy planowaniu tego typu działań by 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 samochodowy 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 degradacja jego morale. To zaś zależne będzie w znacznym stopniu od sprawności rządowej propagandy a także od warunków życia. Stosując broń elektromagnetyczną można paraliżować media masowej komunikacji takie, 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 polu. Stałe bazy logistyczne zawierają znaczne ilości sprzętu diagnostycznego i serwisowego, który jest oparty na elektronice. W bazach takich istnieje też znaczna koncentracja komputerów wykorzystywanych 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 znacznej koncentracji sprzętu bojowego stanowi bardzo opłacalny obiekt takiego ataku gdyż w jego wy-

niku sprzęt ten staje się 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 zdegradować funkcjonowanie infrastruktury przetwarzania i przesyłania informacji oraz ważnych ośrodków przemysłowych. Razem ze sutkami 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 atrakcyjniejsze dla zachodnich demokracji niż klasyczne odmiany tych bombardowań. Stosując ataki elektromagnetyczne unika się, bowiem negatywnego efektu obecności w mediach widoków zniszczeń i ofiar towarzyszących konwencjonalnym atakom. 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 elektromagnetyczną jest niezwykle trudna a szybko uzyskiwane przez atakującego rezultaty mogą odnosić również negatywne dla broniącego się psychologiczne efekty. 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 lub, jako uzupełniająca forma ataku.

W ramach ataku elektronicznego stosowane mogą być też 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 systemów informacyjno-komunikacyjnych.

Atak fizyczny jest klasyczną zdolnością sił powietrznych. Siły powietrzne mogą prowadzić przecież powietrzny atak strategiczny, który jest podobny pod względem koncepcji, jednakże różni się formą atakowania. 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 fizyczny 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 (COMAO) lub rajdów powietrznych małych grup samolotów. Środkami rażenia może być każdy rodzaj uzbrojenia lotniczego 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 powietrznych w ramach informacyjnego ataku strategicznego mogą być realizowane w różny sposób. Klasycznym zadaniem może być rozsiewanie ulotek. Przy odpowiednim wyposażeniu siły powietrzne mogą także prowadzić działania psychologiczne przy wykorzystaniu radiowo-telewizyjnych powietrznych stacji nadawczych oraz przy wykorzystaniu Internetu. Obiektem takiego ataku mogą być zarówno kierownicze elity państwa, jak również całe społeczeństwo

Dezinformacja służyć powinna przede wszystkim obniżeniu efektywności defensywnych działań informacyjnych przeciwnika. Siły powietrzne powinny stosować dezinformację, aby uniemożliwić przeciwnikowi rozpoznanie koncepcji działań, ich efektywności i zamiarów.

3.3. Informacyjne wspieranie działań powietrznych, lądowych i morskich

Wspieranie sił lądowych i morskich w działaniach sił powietrznych może mieć formę izolowania i bezpośredniego (bliskiego) wspierania.

3.3.1. Izolacja

Izolacja lotnicza[45] (AI – *Air Interdiction*) to działania powietrzne prowadzone dla 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[46] 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 dla zniszczenia, zneutralizowania lub opóźnienia działania nieprzyjacielskiego potencjału militarnego przed jego efektywnym zastosowaniu 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 misji powietrznej. Stąd też izolacja wiąże się z dwoma kluczowymi elementami: oddziaływaniem na potencjał przeciwni-

---

[45] *Allied Joint Publications, AJP-01,* NATO 1999.
[46] Fragmenty wystąpienia „Izolacja rejonu działań bojowych; zmienna perspektywa" wygłoszonego na Konferencji Sił Powietrznych (Shephard Conferences) w lutym 1993 r. przez majora Johna F. Morrisona z Sił Powietrznych Stanów Zjednoczonych.

ka przed jego możliwym użyciem przeciwko naszym siłom oraz wykonaniem tego oddziaływania w takiej odległości, aby nie potrzebna 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, dla 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 zaliczone: magazyny, konwoje, rejony ześrodkowania, linie komunikacyjne, wojska znajdujące się w otwartym terenie, bunkry, stanowiska dowodzenia, itd.

Według amerykańskich założeń doktrynalnych[47] 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. Jakkolwiek nie tradycyjnie w klasycznym sensie, walka informacyjna może również być użyta do prowadzenia izolacji przez przechwytywanie lub przerywanie strumienia informacji lub niszczenie oprogramowania i sprzętu kontrolującego.

3.3.2. 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 istnieć będą obszary możliwości oddziaływania kilku komponentów oraz obszary oddziaływania pojedynczych komponentów. Również siły powietrzne mogą dysponować specyficznymi możliwościami niedostępnymi dla innych. W sytuacji, gdy główny wysiłek walki informacyjnej podejmowany jest przez inne komponenty państwa siły powietrz-

---

[47] *Air Force Basic Doctrine*, Maxwell AFB, 1997.

ne dysponujące unikalnymi możliwościami mogą wspierać ten wysiłek atakując pozostające dotychczas poza zasięgiem walki elementy.

Istotą informacyjnej izolacji jest atak informacyjny sił powietrznych 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 wykonania ataku pozostającego poza możliwościami wspieranych sił.

Warto zwrócić uwagę na sprawy najbardziej istotne w informacyjnej izolacji na proces wyznaczania obiektów ataku.

Wyznaczanie celów - obiektów ataku. W procesie wyznaczania obiektów ataku dla potrzeb informacyjnej izolacji istnieją cztery główne przypadki. Pierwszy, gdy potencjalne cele są znane i określony jest wymagany poziom ich zniszczenia. To powoduje, że planujący działanie mogą wybrać odpowiednie środki ataku i odpowiednio dopasować je do szeroko rozumianych platform przenoszenia, aby osiągnąć wymagany skutek.

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 staje się, bowiem 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 braku możliwości adaptacji do szybkiej zmiany warunków informacyjnego pola walki

mogą być poważnym ograniczeniem efektywnego użycia sił walki informacyjnej. Pojawienie się nowoczesnych technologii umożliwiających obserwowanie, wykrywanie i przechwycenie celu oraz wykorzystujących te technologie systemy 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 muszą określić priorytety ich zwalczania.

Stopień zniszczenia celu. Po zidentyfikowaniu potencjalnych obiektów ataku, musi być określony stopień ich zniszczenia. Na przykład, zakres zniszczenia może obejmować 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 wpływać na kształt ataku przeprowadzanego na określony cel. Mając tak określony stopień zniszczenia obiektu ataku przychodzi czas na podjęcie decyzji o rodzaju i jakości użytych środków rażenia.

Dobór środków rażenia. Głównym problemem rozważanym podczas doboru środków rażenia, są możliwości sił powietrznych w zakresie walki informacyjnej, dopuszczalność stosowania poszczególnych środków zależna od stopnia eskalacji konfliktu i politycznej zgody na ich użycie. Niektóre środki takie, 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 przypadku 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 zaliczany jest do broni masowego rażenia.

W niektórych przypadkach 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 odpowiednią również w sytuacjach pożądanego trwałego wyeliminowania danego obiektu z użytkowania. Wybór klasycznych środków ataku zależeć będzie od dokładności rażenia obiektu, co będzie również określać ilość wymaganych wylotów dla uzyskania wymaganego stopnia zniszczenia obiektu ataku. Normalnie do przeprowadzenia klasycznego uderzenia na obiekt ataku mogą być używane zarówno środki niekierowane, w tym środki powierzchniowego rażenia oraz uzbrojenie kierowane. Charakterystyki obiektów rażenia również pomagają dokonać ostatecznego doboru. 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 procesu 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 przypadku złośliwego programu komputerowego należy dobrać odpowiedni sposób przenikania oraz dotarcia programu do miejsca przenikania. Ponadto istotnym jest również czas zainstalowania atakującego programu. Może on, bowiem zostać umieszczony w obiekcie ataku lub jego otoczeniu dużo wcześniej przez planowanym atakiem. Ponieważ istnieje całe bogactwo sposobów dotarcia programu do obiektu ataku to 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 istnieje wiele samolotów myśliwskich i bombowych, ale nie każdy z nich ma odpowiednie możliwości dostarczenia

wybranego uzbrojenia nad cel w wymaganej ilości lub dokonania odpowiedniego zrzutu w wymaganym miejscu.

Możliwości samolotu, obrona obszaru celu, atak w dzień czy w nocy, wymagany stopień dokładności trafienia, wymagana ilość 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 elastycznym z możliwościami adaptacyjnymi do szybko zmieniającej się sytuacji na polu walki.

Informacyjne izolowanie w siłach powietrznych 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 lotniczą w przyszłości. Sensory penetrujące środowisko i urządzenia wskazujące wyposażone w nowe mikrotechnologie uzyskają moc przetwarzania informacji umożliwiającą dokładne "dotknięcie" 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.

3.3.3. Bezpośrednie (bliskie) wspieranie

Bezpośrednie wsparcie lotnicze[48] (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 do 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 krytycznych sytuacjach, jednakże środowiska wojsk lądowych oczekują systematycznego angażowania się lotnictwa w walkę lądową. Tymczasem sprzęt lotniczy jest niezwykle drogi i opłacalność jego użycia jest zapewniona jedynie, 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.

3.3.4. Informacyjne wspieranie ofensywne

Poszczególni uczestnicy walki informacyjnej państwa prowadzą działania adekwatne w stosunku 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 nie-

---

[48] *Allied Joint Publications, AJP-01,* NATO 1999.

zbędne. Może to być spowodowane uzupełniającymi się możliwościami bojowymi uczestników walki informacyjnej lub innymi podobnymi przyczynami. Dlatego nie należy wykluczać możliwości prowadzenia informacyjnego wspierania ofensywnego.

Istotą informacyjnego wspierania ofensywnego jest atak informacyjny sił powietrznych 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. Podczas konfliktu na Falklandach, działań Stanów Zjednoczonych w Grenadzie i w Panamie oraz w konflikcie w Zatoce Perskiej poziom strat, ogólnie był tak niski, że „akty bratobójcze" stały się jedną z głównych przyczyn ponoszonych strat. Oczekiwanie, że można podjąć takie środki, które zapobiegną ryzyku „aktów bratobójczych" są nierealistyczne. Mimo wszystko, istnieją poważne powody, aby doskonalić wzajemną identyfikację. Od niej, bowiem zależą możliwości skutecznego użycia ognia dalekiego zasięgu i zastosowania systemów uzbrojenia „odpal i zapomnij". Jakiekolwiek by nie było ostateczne rozwiązanie, to można wiele osiągnąć, przez zapewnienie szkolenia i zaostrzenie dyscypliny procedur kierowania oraz jasnego określenia sytuacji na polu walki. Nowe środki nawigacyjne również bardzo pomagają w rozwiązaniu tego problemu. Wizualna identyfikacja pojazdów opancerzonych, wciąż jest wyjątkowo trudna, szczególnie w rejonach swobodnego stosowania nowoczesnego uzbrojenia. Zapobieżenie atakowaniu swój-swego musi być zabezpieczone przez środki elektroniczne lub poprzez procedury albo bezpośrednie kierowanie. Jakikolwiek system nie byłby użyty, musi on także zapewnić odpowiedni zakres elastyczności.

Podobnie w przypadku informacyjnego wspierania ofensywnego istnieje niebezpieczeństwo wzajemnej neutralizacji niezbyt dobrze skoordynowanych działań. Jednocześnie stosowane złośliwe programy ataku informatycznego mogą spowodować ich zdemaskowanie, zakłócenie rażenia itp. Zaatakowanie jakiegoś obiektu bez do-

kładnej 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 informacyjne wspieranie ofensywne, jeśli zaistnieje potrzeba jego prowadzenia powinno być dokładnie skoordynowane z innymi uczestnikami walki informacyjnej oraz stosowane tam gdzie istnieje uzasadniona potrzeba jego stosowania.

W przyszłości w wyniku ewolucji systemów kierowania walką informacyjną oraz dalszej ewolucji informacyjnych środków rażenia znacznie zwiększą 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 trzy wyłaniające się technologie. Do technologii tych należą nanotechnologia dla wewnętrznych jednostek pomiarowych, sensorów, transmiterów, procesorów i nieliniowe modelowanie oraz inteligentne systemy wsparcia wirtualnych pętli procesów decyzyjnych.

Zakończenie

Głównym celem prowadzonych badań było poszukiwanie charakterystyki ofensywnych działań informacyjnych sił powietrznych we współczesnych warunkach rozwoju cywilizacyjnego.

Badania ujawniły podstawowy kształt ofensywnej walki informacyjnej możliwy do stosowania w warunkach wyłaniania się cywilizacji informacyjnej. Sformułowaniu tego kształtu sprzyjało zidentyfikowanie najistotniejszych czynników, stymulujących jego rozwój. Czynnikami tymi są przede wszystkim zmiany zachodzące w koncepcjach walki oraz charakter tworzącej się nowej cywilizacji informacyjnej. Opierając się na rezultatach wcześniejszych badań oraz dokonując przeglądu możliwych form ofensywnej walki informacyjnej. W rezultacie ustalono, że w działaniach informacyjnych sił powietrznych mogą być stosowane następujące formy ofensywne tych działań: atak informatyczny, atak elektroniczny, atak fizyczny, działania psychologiczne, dezinformacja wojskowa.

Próbując określić charakter ofensywnej walki informacyjnej w przyszłych działaniach powietrznych uznano, iż na charakter ten wpływ wywrą teorie działań powietrznych. Dokonując porównań i posługując się analogią zidentyfikowano zarys koncepcji przyszłej, ofensywnej walki informacyjnej w działaniach powietrznych. W tej sytuacji kolejnym zadaniem badawczym powinno być zidentyfikowanie charakteru defensywnej walki informacyjnej w działaniach powietrznych.

Bibliografia

1. *Air Force Basic Doctrine*, Maxwell AFB, 1997
2. *Allied Joint Publications, AJP-01,* NATO 1999
3. Arnold H.D. i in. *Targeting Financial Systems as Centers of Gravity: "Low Intensity" to "No Intensity" Conflict*, [w:] "Defense Analysis", Vol. 10, No. 2, 1994
4. Barlow J.B., *Strategie Paralysis: An Airpower Theory for the Present*, Maxwell AFB 1994
5. Ciborowski L., *Walka informacyjna*, Toruń 1999
6. 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. Air War College Air University*, Maxwell AFB 1995
7. Dubrawski Z., *Walka radioelektroniczna prowadzona przez siły powietrzne. Studium operacyjne*, Warszawa 2000
8. *Electronic Warfare, Air Force Doctrine Document 2-5.1*, Washington, D.C. 1999
9. Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999
10. Gurst G.R., *Taking Down Telecommunications. Air University Press*, Maxwell AFB 1994
11. http://www.seas.gwu.edu/~reto/infowar/view.htm 26.01.2001
12. *Information Operations. AFDD 2-5*, USAF 1998
13. 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
14. Kardaś T., *Punkt ciężkości*,[w:] „Myśl Wojskowa" Nr 2/2000, Warszawa 2000
15. Koch E. R., Sperber J., *Infomafia. Szpiegostwo komputerowe, handel informacją tajne służby*, tłum. R. Ratajski, Gdynia 1999

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

17. Kuehl D.T., *Strategic Information Warfare and Comprehensive Situational Awareness*, [w:] A.D. Campen, D.H. Dearth, R.T. Goodden, *Cyberwar: Security, Strategy, and Conflct in the Information Age*, Fairfax 1996

18. Martin J.V., *Victory from Above. Air Power Theory and the Conduct of Operations Desert Shield and Desert Storm*, Maxwell AFB 1994

19. McRae H., *Świat w roku 2020. Potęga, kultura i dobrobyt – wizja przyszłości*, Warszawa 1996

20. Michalak W., *Dominacja z powietrza*, Warszawa 1999

21. Nowacki G., *Walka informacyjna – próba kategoryzacji. Rozprawa doktorska*, Warszawa 1999

22. Nowacki G., *Współczesne poglądy na prowadzenie walki informacyjnej*, Warszawa 2001

23. Podkowski A., Laszczkowski A., *Ulotki w działaniach bojowych. Materiał Studyjny*, Warszawa 2001

24. Podkowski A., *Siły, środki i możliwości oddziaływania psychologicznego armii amerykańskiej podczas konfliktu zbrojnego*, Warszawa 1998

25. Podkowski A., *Zasady i techniki perswazji w działaniach psychologicznych w walce zbrojnej (na przykładzie armii sowieckiej w latach 1921-1991)*, Warszawa 1998

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

27. Rinaldi S.M., *Beyond the Industrial Web: Economic Synergies and Targeting Methodologies*, Maxwell AFB 1995

28. Schwartau W., *Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age. Thunder's Mouth Press*, New York 1996

29. Stacewicz J., *Cywilizacyjno-kulturowy wymiar globalizacji integracji oraz transformacji*, [w:] *Globalizacja gospodarki światowej a integracja regionalna. Konsekwencje dla świata i Polski*, Warszawa 1998

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

31. Szafranski R., *Mars Chuckles And Athena In Frustration* [w:] *NL Arms. Netherlands Annual Reviev of Military Studies 1999. Information Operations*, Breda 1999

32. Szpyra R., *Działania informacyjne i walka informacyjna we współczesnych i przyszłych zastosowaniach sił powietrznych,* [w:] „Przegląd Wojsk Lotniczych i Obrony Powietrznej" nr 9/2000

33. Szpyra R., *Rola sił powietrznych w wojnie przyszłości*, Warszawa 2000

34. Szpyra R., *Współczesna wojna powietrzna. Wybrane problemy*, Warszawa 1998

35. *Walka radioelektroniczna w Siłach Zbrojnych RP*, Warszawa 1994

36. Warden J.A. III, *Air Theory for the Twenty-first Centur,* [w:] *Battlefield of the Future. 21st Century Warfare Issues*, Maxwell AFB 1995