Part Code ST1316
R G B WH GR BL Grey Scale #13 C M Y K
DANES-PICTA.COM
A 1 2 3 4 5 6 M 8 9 10 11 12 13 14 15 B 17 18 19

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LOTNICZYCH I OP

Ppłk dr inż. Ryszard SZPYRA

WALKA INFORMACYJNA W PRZYSZŁYCH DZIAŁANIACH SIŁ POWIETRZNYCH

Opracowanie pod kryptonimem CYBERAWIATOR (4.10.0.0)

60991

Nr ewid. II

Biblioteka Główna Akademii Obrony Narodowej
SP 4275
05-004275-001-0

PN 13

WARSZAWA 2000

Colour Chart #13
Blue Cyan Green Yellow Red Magenta White 3/Color Black
Inches Centimetres
DANES-PICTA.COM

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LOTNICZYCH I OBRONY POWIETRZNEJ

BIBLIOTEKA GŁÓWNA – ARCHIWUM
Nr ewid. 60991
II
Akademii Obrony Narodowej

Ppłk dr inż. Ryszard SZPYRA

WALKA INFORMACYJNA W PRZYSZŁYCH DZIAŁANIACH SIŁ POWIETRZNYCH

Opracowanie pod kryptonimem CYBERAWIATOR (4.10.0.0)

BIBLIOTEKA GŁÓWNA
Nr S/4275
Akademii Obrony Narodowej

WARSZAWA **2000**

Spis treści

SPIS TREŚCI **2**

WSTĘP **3**

1. NOWE ŚRODOWISKO, ZAGROŻENIA I MOŻLIWOŚCI **6**

2. WYBRANE PRZYKŁADY POGLĄDÓW NA WYKORZYSTANIE DZIAŁAŃ W OBSZARZE INFORMACYJNYM **30**

2.1. DZIAŁANIA INFORMACYJNE Z PERSPEKTYWY NATO 30

2.2. STANOWISKO SIŁ LĄDOWYCH USA 43

2.3. ROSJA 52

3. POGLĄDY ŚRODOWISK POWIETRZNYCH USA NA WYKORZYSTANIE DZIAŁAŃ W OBSZARZE INFORMACYJNYM **59**

3.1. TREŚĆ DOKTRYNY DZIAŁAŃ INFORMACYJNYCH AMERYKAŃSKICH SIŁ POWIETRZNYCH 60

4. OGÓLNA KONCEPCJA WALKI INFORMACYJNEJ W POLSKICH SIŁACH POWIETRZNYCH W PRZYSZŁOŚCI **98**

ZAKOŃCZENIE **110**

BIBLIOGRAFIA **112**

Wstęp

Obecnie w środowiskach wojskowych i cywilnych toczy się coraz szersza dyskusja nad problemami zagrożeń wynikających z oddziaływań na informację i systemy informacyjne. Wojskowi teoretycy i praktycy pracują nad koncepcjami i doktrynami działań informacyjnych. Pojawiły się już zarysy takich doktryn, a w niektórych przypadkach nawet kompletne doktryny. W formułowaniu doktryn przodują Amerykanie. Już zarówno siły lądowe jak i powietrzne opublikowały swoje doktryny odnoszące się do omawianej problematyki. Również w NATO przyjęto pierwsze dokumenty normatywne. Część z dokumentów odnoszących się do działań w obszarze informacyjnym jest niejawna. Jest to bowiem nowa forma walki i najbardziej efektywne jej formy będą prawdopodobnie utrzymywane w tajemnicy dla zapewnienia sobie zaskoczenia w przyszłych działaniach bojowych. Niemniej jednak opublikowano wystarczająco dużo informacji jawnej na ten temat by można było podejmować próbę określenia tego nowego zjawiska i poszukiwania możliwości stosowania rodzących się nowych form walki w przyszłych działaniach powietrznych.

Biorąc pod uwagę powyższe ustalenia przyjęto, że celem pracy jest określenie przydatności oraz możliwej skali zastosowania walki informacyjnej w przyszłych działaniach powietrznych.

Wiedza ta przyczyni się do adaptowania teorii do nowej rzeczywistości, kształtowania świadomości personelu sił zbrojnych, a w szczególności sił powietrznych, związanej z nową sferą walki, jaką jest walka informacyjna, a także inicjowaniu w Polskich Siłach Powietrznych przedsięwzięć służących adaptacji do potrzeb nowej rzeczywistości. Wiedza ta stanowić ma także podstawę do prowadzenia dalszych szczegółowych badań w tym obszarze.

Z celu pracy wynikły główne problemy badawcze którymi są:

- Jakie są zależności współczesnej walki od informacji i systemów informacyjnych oraz zagrożenia płynące z tych zależności?
- Jakie są poglądy na działania prowadzone w sferze informacyjnej, a w szczególności na działania informacyjne i walkę informacyjną?

- Jak środowisko powietrzne rozumie i zamierza stosować działania informacyjne i walkę informacyjną?
- W jakim kierunku powinien iść rozwój koncepcji działań informacyjnych i walki informacyjnej w Polskich Siłach Powietrznych?

Oczekuje się, że wyniki badań mogą być wykorzystane głównie w dwóch aspektach - teoretycznym i praktycznym.

W aspekcie teoretycznym, jako podstawa dalszych badań nad poszczególnymi aspektami przyszłej wojny powietrznej, a także jako materiał pomocny do opracowania doktryny Polskich Sił Powietrznych, a w tym ich strategii, sztuki operacyjnej i taktyki.

Natomiast w aspekcie praktycznym powinny one służyć merytorycznemu ukierunkowaniu w zakresie jakościowego rozwoju tych sił, z uwzględnieniem podstawowych celów integracji z Siłami Powietrznymi NATO, a także celom dydaktycznym.

Badania prowadzono w oparciu o grupę materiałów źródłowych mających charakter oficjalnych dokumentów takich, jak np. amerykańska doktryna powietrzna i lądowa, czy oficjalnych wypowiedzi, np. przedstawicieli kierownictwa wojskowego NATO. Ze względu na nowość omawianej problematyki grupa oficjalnych dokumentów nie jest zbyt liczna. W wielu państwach toczą się dyskusje i działania, które nie przybrały jeszcze postaci oficjalnych dokumentów lub istnieją w formie niejawnej. W Stanach Zjednoczonych najwcześniej dostrzeżono nowe zagrożenia i możliwości związane z uzależnieniami współczesnej cywilizacji od informacji i systemów informacyjnych. Najwcześniej też podjęto prace nad studiowaniem tej problematyki i praktycznym wdrażaniem rezultatów badań. Dlatego też w amerykańskich źródłach informacji można spotkać najwięcej publikacji na ten temat. Ogólnodostępne publikacje książkowe i w postaci artykułów stanowiły drugą grupę materiałów źródłowych. Wiele z nich traktuje o szerokich aspektach zagrożeń, działań informacyjnych, walki i wojny informacyjnej. Materiały te odnoszą się często do działań organizowanych na poziomie strategicznym i mających charakter niemilitarny. W niniejszym opracowaniu koncentrowano się głównie na wypowiedziach mających związek z działaniami sił powietrznych prowadzonymi współcześnie lub w przyszłości. Niektóre przytoczone

opinie wykraczające poza te kryteria zaprezentowane zostały głównie dla potrzeb przedstawienia nieco innych stanowisk jakie istnieją w tym obszarze.

Dobór teoretycznych materiałów źródłowych służył przede wszystkim sformułowaniu głównych tendencji rozwojowych współczesnych działań i walki informacyjnej dla potrzeb przyszłych działań sił powietrznych.

Rezultaty badań przedstawiono w studium teoretycznym składającym się z wstępu, zakończenia oraz czterech rozdziałów merytorycznych zakończonych wnioskami.

W rozdziale pierwszym omówiono środowisko współczesnych i przyszłych działań militarnych, wskazano na pojawiające się nowe zagrożenia i możliwości ofensywnego eksploatowania nowych możliwości walki.

W rozdziale drugim zaprezentowane zostały najistotniejsze przykłady poglądów na sprawy działań i walki informacyjnej. Są one jedynie ilustracją odmiennych podejść do tej samej problematyki.

Rozdział trzeci prezentuje oficjalne poglądy amerykańskich sił powietrznych w odniesieniu do działań informacyjnych i walki informacyjnej. Jest to już częściowo zweryfikowane w praktyce stanowisko, które zostało ujawnione publicznie. Ponieważ brak jest podobnych stanowisk sił powietrznych innych krajów amerykańskie poglądy stały się podstawą do poszukiwania koncepcji działań informacyjnych dla potrzeb przyszłych działań Polskich Sił Powietrznych. Ogólny zarys tej koncepcji został przedstawiony w rozdziale czwartym niniejszego opracowania.

Prezentowana koncepcja ma swoje źródła w dorobku najwyżej rozwiniętych cywilizacyjnie społeczeństw i ich sił zbrojnych. Stan naszych sił zbrojnych, a w tym i sił powietrznych daleko odbiega od tego poziomu. Niemniej jednak biorąc pod uwagę tempo zmian cywilizacyjnych i czas niezbędny na „dojrzewanie" koncepcji i rozwiązań organizacyjnych wydaje się uzasadnionym podejmowanie prób adaptowania naszych sił powietrznych do nowych wyzwań. Niniejsza praca ma stanowić jedno z przedsięwzięć w rozległym procesie adaptacji i stanowić będzie podstawę do podejmowania kolejnych badań w tym obszarze.

1. Nowe środowisko, zagrożenia i możliwości

Rozpoczyna się XXI wiek. Niesie on ze sobą nie tylko nowy odcinek w chronologii czasu i historii, ale także dramatyczne zmiany cywilizacyjne, które szokują wielkie masy ludzi. Za zmianami tymi nie nadążają przekształcenia świadomościowe i mentalnościowe społeczeństw. W szczególnie trudnej sytuacji są narody wolno adaptujące się do zmian. Wciągane są bowiem przez wir zmian cywilizacyjnych w bezlitosną, zaostrzającą się rywalizację. Globalizacja, powszechny dostęp do informacji i coraz swobodniejsze migracje ludności utrudniają politykę izolacjonizmu. Nawet te społeczeństwa i państwa, które chciałyby pozostać przy swoich wartościach i sposobach życia nieuchronnie poddawane są wielkiej zewnętrznej presji.

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

Tą wrażliwość dostrzegają także zmuszane do rywalizacji i poddawane presji obcej cywilizacji narody i państwa. Dostrzegają ją także różni niepaństwowi aktorzy międzynarodowej sceny politycznej. Co więcej z wrażliwości tej korzystać mogą nawet pojedynczy ludzie dla swoich indywidualnych celów. Oczywiście wielcy i bogaci tego świata również mają świadomość tego stanu rzeczy. Ten bagatelizowany przez długi czas stan rzeczy staje się coraz bardziej groźny. Tworzy bowiem zagrożenie na-

wet dla bytu państw, a także dla organizacji wszelkiego typu i pojedynczych ludzi. Współczesne rywalizacje i wojny przenoszą się w obszar informacyjny. Czy zagrożenia te są groźne i jak są postrzegane? Dla poszukiwania odpowiedzi na to pytanie przytoczyć warto przynajmniej kilka opinii na ten temat.

Kiedy następnym razem[1] jakiś nowoczesny tyran babiloński (na przykład bagdadzki, teherański czy trypolitański) zagrozi sojusznikowi Stanów Zjednoczonych (Rijadowi, Kairowi, Jerozolimie), USA nie wyślą tam natychmiast ani legionów swych żołnierzy, ani eskadry okrętów wojennych. Zamiast tego Waszyngton spuści na tego tyrana serię jak najbardziej nowoczesnych plag roznoszonych przez komputerowe myszy, monitory i klawiatury.

Najpierw wprowadzi się komputerowego wirusa do central telefonicznych agresora, powodując rozległą awarię jego łączności telefonicznej. Następnie komputerowe bomby logiczne nastawione na uaktywnienie się w określonym terminie, zniszczą elektroniczne dyspozytornie kontrolujące koleje i konwoje wojskowe – transportery będą źle kierowane i powstaną gigantyczne korki. Tymczasem zaś nieprzyjacielscy oficerowie frontowi wykonują rozkazy otrzymywane drogą radiową, nie zdając sobie sprawy, że są to rozkazy fałszywe. Podlegli im żołnierze rozsypują się nie efektywnie po pustyni. Wreszcie samoloty USA wyposażone w specjalny sprzęt do operacji psychologicznych, zagłuszają nieprzyjacielskie stacje telewizyjne i nadają na ich częstotliwościach audycje propagandowe, sprawiające, że ludność zwraca się przeciwko swemu władcy. Kiedy zaś despota uruchamia swój PC, dowiaduje się, że miliony dolarów, jakie zgromadził na swych kontach w bankach szwajcarskich, nagle zniknęły. Wszystko to bez jednego wystrzału. (...)

Ta wizja z chronionego przed podsłuchem pomieszczenia w Wirginii jest wizją wojny informatycznej – „infowojny" – najmodniejszej koncepcji Pentagonu. Informatyczni wojownicy mają nadzieję, że uda im się przeobrazić sposób walki żołnierzy. Stawiają sobie za cel wykorzystanie tych wszystkich cudów techniki, jakie przyniosły

---

[1] Waller D. Thompson M. Strach Generałów. Forum Nr 36 (157) z 3 września 1995 r., przedruk artykułu, który 21.VIII 1995 r. opublikowany został w TIME

nam ostatnie lata XX wieku, do przeprowadzenia szybkich, ukradkowych, rozległych i niszczycielskich ataków na wojskowe i cywilne infrastruktury nieprzyjaciela. Przeprowadzając rozmowy z dziesiątkami przedstawicieli wojska, wywiadu i rządu redakcja nasza przekonała się, że Pentagon ma szeroko zakrojone plany zrewolucjonizowania pola bitwy za pomocą techniki informatycznej, tak jak zrewolucjonizowały je czołgi podczas pierwszej i bomba atomowa podczas drugiej wojny światowej. „Jest to podarunek Ameryki dla sztuki wojennej" – mówi admirał William Owens, zastępca przewodniczącego Kolegium Szefów Sztabów USA.

Jednak ta rewolucja cyberwojenna stwarza Stanom Zjednoczonym poważne problemy. Część z nich ma charakter etyczny – czy zniszczenie innemu krajowi jego giełdy papierów wartościowych jest zbrodnią wojenną? Groźniejsze są problemy bezpieczeństwa USA w sytuacji, gdy jakiś tyran może za pomocą niezbyt kosztownego sprzętu technicznego wyłączyć z działania giełdę, lub jakiś pirat komputerowy – terrorysta może zakłócić działanie wieży kontrolnej lotniska. Pełen podniecenia entuzjazm dla infowojny mógłby zostać przerwany przez szok jakiegoś elektronicznego Pearl Harbor. W ubiegłym roku rządowy Wspólny Komitet Bezpieczeństwa nazwał podatność USA na efekty infowojny „największym w tym dziesięcioleciu, a może i w całym przyszłym stuleciu, problemem dotyczącym bezpieczeństwa".

Infowojna ewoluowała z każdym dokonywanym ostatnio, wypadem wojskowym USA. W pierwszych dniach wojny w Zatoce Perskiej, niewidoczne dla radarów samoloty stealth Sił Powietrznych USA uzbrojone w precyzyjne sterowane pociski oślepiły Sadama nokautując jego sieć łączności i sieć elektryczną Bagdadu. Pentagon urzeczywistnił wyrafinowaną operację psychologiczną skierowaną przeciwko wojskowemu reżimowi na Haiti, by przywrócić władzę obalonemu przez ten reżim prezydentowi Jean – Bertrand Aristide`owi. Wykorzystując wyniki badań rynkowych, 4 Grupa Operacji Psychologicznych Sił Lądowych USA podzieliła ludność Haiti na 20 grup i bombardowała każdą z nich setkami tysięcy popierających Ariside'a ulotek redagowanych z uwzględnieniem właściwości danej grupy. Przed interwencją USA, CIA wykonywała anonimowe telefony do haitańskich żołnierzy wzywając ich do poddania się i wysyłała złowieszcze listy pocztą elektroniczną do niektórych członków haitańskiej oligarchii mających komputery osobiste.

Był to tylko początek. Możliwości infowojny rosną w postępie wykładniczym wraz ze wzrostem mocy i powszechności mikroprocesorów komputerowych, urządzeń ultraszybkiej łączności i wyrafinowanych czujników – wszystko to stwarza ogromne możliwości tym, którzy potrafią instrumentami tymi manipulować dla celów wojennych.

W dowództwach Sił Lądowych, Marynarki Wojennej i Sił Powietrznych USA utworzono biura infowojny. W czerwcu br. na Uniwersytecie Obrony Narodowej w Waszyngtonie wręczono bez rozgłosu dyplomy pierwszemu, szesnastoosobowemu rocznikowi oficerów infowojny, specjalnie wyszkolonych we wszystkim co je dotyczy – do obrony przed atakami na komputery po wykorzystywanie rzeczywistości wirtualnej w planowaniu manewrów, jakie będzie się wykonywać na frontach wojny. W lipcu br. Wojenne Kolegium Marynarki w Newport (stan Rhode Island) zakończyło globalną grę wojenną, podczas której specjaliści od wojny informatycznej obmyślali sposoby unieszkodliwienia komputerów nieprzyjaciela. Pod koniec lata br. wyżsi urzędnicy Pentagonu mają zanalizować wyniki kilkunastu tajnych gier infowojennych przeprowadzonych w ciągu ostatnich dwu lat, by ustalić, jak w przyszłości należałoby zmienić taktykę wojskową.

W tej pirackiej wojnie komputerowej maczają też palce agencje wywiadowcze. Agencja Bezpieczeństwa Narodowego (NSA), wraz z ultratajnymi jednostkami wywiadowczymi Sił Lądowych, Marynarki Wojennej i Sił Powietrznych USA bada sposoby wprowadzania do komputerów nieprzyjaciela szczególnie złośliwych odmian wirusów nękających już domowe i biurowe komputery. Inny typ wirusa – bomba logiczna – po wprowadzeniu do systemu nieprzyjaciela będzie bezczynnie czekać do określonego z góry momentu, po którego nadejściu zacznie zjadać dane. Bombami takimi można by na przykład zaatakować komputery kierujące systemem obrony przeciwlotniczej lub komputery banku centralnego. CIA ma tajny program wprowadzania komputerowych kostek – pułapek do systemów broni, które zagraniczni producenci uzbrojenia mogliby dostarczać potencjalnie wrogiemu krajowi. Metoda ta nosi nazwę chipping (łamanie kostek). Inny program prac CIA obejmuje badanie możliwości przekupywania niezależnych poddostawców wynajmowanych przez firmy zbrojeniowe do tworzenia oprogramowania systemów broni, by wprowadzali do tego oprogra-

mowania wirusy. „Dostajesz się do sieci zaopatrzeniowej producenta broni, na chwilę zabierasz daną rzecz z linii zaopatrzenia, wprowadzasz „robaka" i wstawiasz tę rzecz z powrotem na miejsce, by trafiła do danego kraju – tłumaczył nam ktoś związany z CIA i specjalizujący się w technice informatycznej. Podczas wojny ów system broni będzie sprawiał wrażenie całkowicie sprawnego, ale jego głowica bojowa nie wybuchnie".

Bronie infowojny mogą być jeszcze bardziej niezwykłe od wirusów komputerowych. Państwowe Laboratorium Los Alamos w Nowym Meksyku opracowało urządzenie wielkości walizki generujące potężne impulsy elektromagnetyczne. Komandosi mogą przedostać się do stolicy nieprzyjaciela, umieścić taką walizkę w pobliżu banku i uruchomić urządzenie. Wytworzony impuls spowoduje przepalenie się wszystkich elementów elektronicznych w całym budynku. Inne propozycje łączą elektronikę z biologią. Tak na przykład urzędnicy Pentagonu uważają, że można by wyhodować mikroby zjadające elektronikę i materiały izolacyjne wewnątrz komputerów – tak jak wyhodowano mikroby zjadające odpadki. (...)

Infowojna może albo poprzedzać walki, albo je zastąpić, ale jej metody i jej technikę można też wykorzystać do prowadzenia prawdziwej wojny i do nadrabiania słabości konwencjonalnych sił zbrojnych. Kiedy kurczy się budżet Pentagonu i kiedy Siły Lądowe USA liczące 1,1 mln ludzi, zajmują pod względem liczebności ósme miejsce na świecie, wyżsi oficerowie amerykańscy uważają, że Ameryka będzie musiała wykorzystywać w przyszłych wojnach swą przewagę w technice przetwarzania informacji w łączności. W maju br. przeprowadzono w Fort Leavenworth w stanie Kansas symulacyjna grę wojenną: licząca 20 tys. ludzi dywizja piechoty wyposażona w supernowoczesny sprzęt do przetwarzania informacji i w inteligentną broń – to jest w to wszystko, czym według nadziei żywionych przez dowództwo Sił Lądowych USA żołnierze amerykańscy mają rozporządzać w roku 2010 –miała za przeciwnika trzykrotnie od siebie liczniejszy korpus armii północnokoreańskiej. Rozporządzając komputerami szybko przekazującymi rozkazy bitewne i czujnikami umożliwiającymi lepsze dostrzeganie wroga na polu bitwy, ta wyposażona w nowoczesny sprzęt dywizja „po prostu zmiażdżyła przeciwnika" – mówi gen. Keith Kellogg z Dowództwa Szkolenia i Doktryny Sił Lądowych USA.(...)

Konsekwencje infowojny przenikają w dół do zwykłych szeregowych. Dowództwo Sił Lądowych USA ma nadzieję, że „ucyfrowi pole bitwy" podłączając każdego żołnierza i każdą broń do systemu elektronicznego. Zespół badaczy firmy Motorola i Laboratorium Prac Badawczych i Rozwojowych Sił Lądowych USA w Natick w stanie Massachusetts zamierza w przyszłym roku dokonać odsłonięcia prototypu wyposażenia „żołnierza piechoty XXI wieku" Jego hełm będzie wyposażony w mikrofon i słuchawki dla celów łączności, noktowizor i czujniki termiczne umożliwiają widzenie w ciemności. Przed oczyma będzie miał miniaturowy ekran wskazujący mu jego dokładną pozycję i nieustannie dostarczający mu uaktualnianych danych wywiadowczych.

W istocie przyszła wojna może wyglądać jak obecny film fantastyczno – naukowy. „Nadejdą dni, że przywódcy państwa zanim zdecydują się w ogóle prowadzić wojnę, przeprowadzą najpierw wojnę wirtualną" – przewiduje generał porucznik Jay Garner, szef Dowództwa Obrony Kosmicznej i Strategicznej sił Lądowych. Niektórzy futurolodzy idą o krok dalej: kraje zamiast toczyć prawdziwe wojny przeprowadzać będą komputerowe symulacje, by zobaczyć, kto zwycięży. Gen. Garner nie chce posuwać się aż tak daleko: „Trudno mi sobie wyobrazić, by wojna była tylko grą wideo wolną od jakichkolwiek cierpień".

Wszystko to może stanowić zapowiedź zakrojonej na wielką skalę reorganizacji sił zbrojnych. W sytuacji, w której mikroprocesory umożliwiają minaturyzację broni i wytwarzanie kontrolowanych elektronicznie samolotów bezzałogowych zdolnych do śledzenia i atakowania wyznaczonych celów, lotniskowce i bombowce załogowe mogą stać się przestarzałymi narzędziami konfliktów. Podobnie jak komputery spłaszczyły schematy organizacyjne wielkich firm, tak i wojsko może być zmuszone do restrukturyzacji – między generałem i jego żołnierzami na linii ognia mniej będzie potrzebnych warstw oficerów sztabowych. Różnica między żołnierzem i cywilem może ulec zatarciu, ponieważ przy operowaniu skomplikowanym sprzętem na polu bitwy trzeba będzie zatrudniać liczne firmy prywatne. Te nowe formy prowadzenia walk bez wątpienia natrafią wewnątrz sił zbrojnych na biurokratyczne, a nawet kulturowe opory. (...)

Panuje ogólna zgoda, że departament obrony powinien energicznie zajmować się opracowywaniem technik tego typu, jednak istnieje obawa, że nieprzyjaciel mógłby z równą łatwością opracować analogiczną broń i użyć jej przeciwko Stanom Zjednoczonym. (...)

Wojskowe mikroczujniki i wszechwiedzące monitory wideo mogą być bardzo kosztowne, natomiast duża część techniki niezbędnej do atakowania systemów informatycznych jest tania (wystarczy komputer i modem) powszechnie dostępna (wystarczy gotowy do współpracy pirat) również bardzo wydajna (wystarczy jedno połączenie telefoniczne) „To wielki wyrównywacz –mówi futurolog Alvin Toffter.

Nie musi się być ani wielkim, ani bogatym, by stosować ten rodzaj dżudo, jaki potrzebny jest w wojnie informatycznej. Dlatego kraje biedniejsze pójdą w tym kierunku szybciej niż kraje o zaawansowanej technice. Infowojownikiem może być każdy z kolejki do kasy lokalnego sklepu z komputerami.

„Nie wymaga to jakieś ogromnej masy pieniędzy – mówi Donald Latham, niegdyś odpowiedzialny na łączność Pentagonu – paru spryciarzy z komputerami i modemami może zagrozić życiu wielu ludzi i wywołać ogromne zaburzenia gospodarcze".

Wyrządzanie szkód już się zaczęło. Na trzecim piętrze unowocześnionych magazynów Marynarki Wojennej, oddzielonych od Pentagonu tylko Cmentarzem Artington, pracuje Zespół Zapewnienia Bezpieczeństwa Systemom Automatycznym wojska. Jest to techniczne pogotowie Pentagonu, mające reagować na ataki na komputerowy system nerwowy sił zbrojnych. W ciągu osiemnastu miesięcy poprzedzających 1 lipca br. zespół odebrał 28 tys. wezwań o pomoc od operatorów wojskowych sieci komputerowych USA na całym świecie. Zespół izoluje tysiące pirackich programów zwanych criters (stwory) i wsadza je do klatek, by poddać je dalszym badaniom. Programy tego typu mają coraz większy potencjał i są coraz łatwiejsze do stosowania. Intruz nie musi już znać skomplikowanych kodów i nie musi być znawcą informatyki. „Wystarczy, by wybrał odpowiedni punkt, kliknął i zaatakował" – mówi ekspert Pentagonu do spraw bezpieczeństwa komputerów Kenneth Van Wyk.

W październiku ubiegłego roku Rada Nauki departamentu obrony ostrzegła, że istnieje zagrożenie nie tylko ze strony piratów, od lat irytujących Pentagon. Jest to zagrożenie – stwierdziła Rada – ze strony grup terrorystycznych oraz ze strony obcych państw, jest ono dużo bardziej subtelne i dużo trudniejsze do zwalczania niż mniej ustrukturyzowane, ale nasilające się ataki piratów. Pod płaszczykiem nieustrukturyzowanej działalności piratów mógłby zostać przygotowany wielki ustrukturyzowany atak na USA mający charakter strategiczny".

Stany Zjednoczone – kontynuuje swe ostrzeżenie Rada – mogą nawet nie zdawać sobie sprawy, że zostały zaatakowane „Nie istnieje żadna koordynowana na skalę ogólnopaństwową zdolność do przeciwdziałania takiemu ustrukturyzowaniu zagrożenia, a nawet zdolność do jego wykrywania". Uderzenie takie „mogłoby poważnie zaszkodzić gotowości do działań wojskowych i efektywności tych działań", opóźniając rozwinięcie wojsk i skierowując w złą stronę samoloty transportowe, pociągi i okręty.

Piraci mogą się okazać współczesnymi najemnikami gotowymi się sprzedać temu, kto da więcej. Według przedstawicieli Pentagonu, podczas wojny w Zatoce grupa holenderskich piratów zaproponowała, że za milion dolarów zakłóci przerzucanie wojsk amerykańskich na Bliski Wschód. Sadam Husajn zlekceważył tę ofertę. Tymczasem – zdaniem Steve'a Kenta, prywatnego eksperta od spraw bezpieczeństwa komputerów i członka zespołu doradców Pentagonu do spraw obronnej wojny informatycznej – istniały ogromne możliwości wywołania takich zakłóceń: „Podczas wojny w Zatoce wojskowi na duża skalę wykorzystywali do łączności Internet i siły zbrojne poniosłyby znaczne szkody, gdyby Irakijczycy zdecydowali się na odebranie im takiej możliwości".

Tajny raport wywiadowczy przygotowywany przez CIA kończy się wnioskiem, że chociaż nie było jeszcze żadnego wyraźnego ataku na amerykańskie wojskowe instalacje komputerowe, to jednak obce służby wywiadowcze sondują już komputery USA. Wysoki rangą ekspert do spraw bezpieczeństwa komputerów z departamentu sprawiedliwości mówi, że pięciu spośród siedmiu ujawnionych intruzów, którzy dostali się do głównych komputerów Pentagonu, było codzoziemcami. Emerytowany pułkownik sił powietrznych USA Alan D. Campen autor „Frist Information War"

(Pierwsza wojna informatyczna) – wydanej w 1992 r. książki opisującej techniki informatyczne wykorzystywane podczas operacji Pustynna Burza – mówi, że dostał „zamówienia na tę książkę od ambasad z całego świata". Armia chińska posługuje się tą książką przy prowadzeniu zajęć szkoleniowych o infowojnie.

Podczas gdy na ogół uważa się, że wojskowe komputery wykorzystywane do prowadzenia walk są bezpieczne, to obsługę różnych innych kluczowych dziedzin – na przykład płac, spraw kadrowych, transportu i gospodarki częściami zamiennymi – prowadzi się za pomocą kiepsko strzeżonych komputerów Pentagonu połączonych niemal w ogóle niestrzeżonymi kanałami łączności publicznej. Eksperci Pentagonu uważają, że codziennie jest blisko pięćset prób dostania się do wojskowych komputerów przez kogoś z zewnątrz. Wykrywa się jednak tylko około 25 takich prób dziennie, a zaledwie o dwu lub trzech informuje się ludzi odpowiedzialnych za bezpieczeństwo. Ta łatwość dostania się do komputerów Pentagonu jest efektem takiego ich niegdyś projektowania, by były łatwe w użyciu i miały łatwy dostęp do Internetu (sieci, będącej również tworem Pentagonu). Najtrudniej jest się włamać do pierwszego komputera – kiedy jest się już wewnątrz, niemal 90 proc. pozostałych komputerów Pentagonu połączonych z tym do którego się włamano, uzna intruza za uprawnionego użytkownika. „Piraci mówią – informuje Van Wyk – że nasze komputery są twarde z zewnątrz, ale miękkie i łatwe do ugryzienia od środka".

Na zewnątrz wojska poważnie zaniepokojone możliwością, że piraci mogliby z łatwością zniekształcić pracę komputerów kontrolujących banki, giełdy, ruch powietrzny, telefony i sieć elektryczną jest Agencja Bezpieczeństwa Narodowego „Jesteśmy bardziej wrażliwi (na taki atak) niż jakikolwiek inny kraj" – mówi dyrektor NSA, wiceadmirał John Mc Connell. Odpowiednio okablowany przeciwnik mógłby zlikwidować te komputery „nawet nie przyjeżdżając do kraju" – ostrzegł w raporcie przedstawionym w maju br. zespół specjalistów z zewnątrz analizujący przyszłe misje Pentagonu. Według innego raportu Pentagonu opublikowanego w grudniu ubiegłego roku, efekty takiego ataku „mogłyby wywołać powszechną panikę wśród ludności cywilnej".(...)

W istocie pod pewnymi względami infowojna może tylko udoskonalić zwrot współczesnej sztuki wojennej w kierunku atakowania celów cywilnych – począwszy od zrzucania bomb zapalających na Drezno i Tokio podczas II wojny światowej aż po „czystki etniczne" w Bośni. Likwidację kontroli lotów czy systemu telefonicznego danego kraju można przeprowadzić w czysty sposób, posługując się komputerami – ale będzie to jednak atak na cele cywilne. Przykłady stosowania embarga wyraźnie dowiodły, że wojna gospodarcza może być równie brudna jak inne formy wojny. Infowojna ze swą wymyślną techniką może umożliwić uniknięcie pewnych śmierciono-śnych, krwawych i brudnych tradycji pola walki, ale nadal odnosić się do niej będą słowa generała z czasów amerykańskiej Wojny Domowej Wiliama Tecumseha Shermana: „Wojna jest okrucieństwem i tego nie da się poprawić".

Jak mogłaby się zacząć światowa wojna informatyczna, w której żadne chwyty nie byłyby zabronione. W każdym razie tak to sobie ją wyobrażają autorzy „The Day After .. in Cyberspace" (dzień po ... w cyberprzestrzeni), opracowanej przez Rand Corp, grze wojennej, rozegranej przez wyższych urzędników USA. (...)

„4 lutego 2000 Iran próbuje zastraszyć osłabioną Arabię Saudyjską i skłonić ją do zmniejszenia wydobycia ropy w celu pchnięcia w ten sposób w górę jej cen. Waszyngton rozważa wysłanie do tego królestwa swych żołnierzy, by w ten sposób umocnić jego wolę. Iran – pamiętając o losie Sadamma Husajna – postanawiają nie stawiać Ameryce czoła na piaskach pustyni. Zamiast tego postanawiają upokorzyć „wielkiego Szatana" w bardziej podstępny sposób. W istocie nikt jeszcze nie wie, że Stany Zjednoczone są przedmiotem ataku. Nikt nie słyszy lekkiego szmeru nieprzyjacielskich klawiatur, a bezzapalnikowe bomby podróżujące Internetem w ogóle nie wydają żadnego dźwięku. Jednak zaczyna się pojawiać wyraźny wzorzec komputerowego chaosu. Kiedy pracownicy Białego Domu przedstawiają prezydentowi dowody, że Teheran wdaje się w wojnę informatyczną, na kilka godzin ustaje wszelka łączność z Kairem. Nagle do pokoju operacyjnego Białego Domu wpada jeden z współpracowników prezydenta: załamała się sieć telefoniczna północnej Kalifornii i Oregonu, najwyraźniej w wyniku działania „pułapki komputerowej wprowadzonej potajemnie do

komputerowego kodu tych systemów". Dalej na północ pod wpływem „masowego wykręcania odpowiednich numerów" przez Internet na wiele godzin głuchną telefony w ogromnej bazie wojskowej USA w Fort Lewis w stanie Waszyngton.

Wkrótce po zakończeniu się zebrania prezydenckiej Rady Bezpieczeństwa Narodowego (NSC) ultraszybki pociąg pasażerski jadący z szybkością 320 km/godz. zderza się w pobliżu Laurel w stanie Maryland ze skierowanym na niewłaściwy tor pociągiem towarowym. CIA podejrzewa, że winowajcami są agenci Iranu, którzy wprowadzili „bombę logiczną" do systemu komputerowego kolei i że to właśnie taka bomba spowodowała katastrofę. W Arabii Saudyjskiej sabotaż komputerowy powoduje ogromną eksplozję i pożar w rafinerii ropy w pobliżu Dahranu właśnie w chwili, gdy granicom królestwa zagrażają zbliżające się do nich oddziały i okręty Iranu. W Lodynie, Scotland Yard informuje premiera, ze Bank Anglii wykrył w komputerowym oprogramowaniu trzy różne „robaki" – tak zaprojektowane, by sabotowały transfer pieniędzy. I podczas trwania całego tego cyklonu elektronicznego CNN podaje, że Iran najął rosyjskich ekspertów komputerowych i indyjskich programistów, by „by zagrozić całej tkance gospodarczej Stanów Zjednoczonych i Europy Zachodniej". Cała ta seria szoków wywołuje załamanie się kursów akcji na giełdzie nowojorskiej i giełdzie londyńskiej. (...)

Zarówno pracownicy Białego Domu jak i pracownicy Pentagonu przyznają, że jest to denerwujący zestaw zagrożeń. Jeszcze bardziej niepokoi, że nie jest to zestaw nieprawdopodobny – działająca przy Pentagonie Rada Nauki w mrożącym krew raporcie opracowanym pod koniec ubiegłego roku ostrzegała przed możliwością właśnie dokładnie takiego ataku. Ta grupa wysokiego szczebla zwróciła uwagę, że komputery sterujące amerykańskimi elektrowniami, lotniskami, bankami i telefonami dojrzały już do tego, by je zrujnowano „Grupy intruzów elektronicznych, jeśli zostaną zorganizowane i sfinansowane przez zainteresowanego przeciwnika, mają możność przeprowadzenia wyrafinowanego ataku na duża skalę" – stwierdziła Rada.

Państwa „Trzeciego Świata" mogą nabyć wszystko, co potrzebne jest do prowadzenia wojny informatycznej, praktycznie biorąc z "półki". Nawet przed rozegraniem omawianej gry Pentagon zaczął po cichu zmniejszać stopień swej wrażliwości.

Agencja Systemów Informatycznych Obrony (DISA), zajmująca się ochroną komputerów wojskowych, otworzyła w Slidell w stanie Luizjana ośrodek, który określa jako „centrum ciągłości operacyjnej". Jest on przygotowany do usuwania w pracy komputerów i w systemach łączności luk powstałych czy to przypadkowo, czy w efekcie czyjejś świadomej działalności w szesnastu głównych centrach komputerowych sił zbrojnych. DISA zawarła kontrakty na ochronę komputerów, mogące mieć wartość 2 mld dolarów i podpisała największy w swych dziejach kontrakt na programy antywirusowe.

Nie wszyscy eksperci wojskowi widzą sytuację w tak czarnych barwach. Niektórzy przyrównują niebezpieczeństwo stwarzane przez „elektrony trzymetrowego wzrostu" do wyolbrzymianego 10 lat temu zagrożenia ze strony Armii Czerwonej. „Wydaje się, że to przesada przedstawiać jako zagrożenie bezpieczeństwa narodowego coś, co dotychczas było w dużej mierze zaawansowaną techniczną wersją kradzieży samochodu, czy nawet tylko zabrania samochodu po to, by odbyć nim przejażdżkę – mówi Martin Libicki, naukowiec, specjalista od techniki obrony na Uniwersytecie Obrony Narodowej. Admirał William Owens, wiceprzewodniczący Kolegium Szefów Sztabów przyznaje, że USA są w pewnej mierze narażone na taki atak, ale twierdzi w pentagońskim żargonie, że jeśli doszłoby do takiego ataku amerykańskie siły zbrojne „tylko obniżą się z gracją". Gra opracowana przez Rand Corp, wykazuje jednak że to „obniżenie" może mieć rozmiary apokaliptyczne.

10 lutego 2000 Centralne dowództwo Pentagonu zwraca się do prezydenta o zezwolenie na rozpoczęcie operacji „Zielony Szerszeń" – wysłania znacznych sił USA na Bliski Wschód w celu udzielenia pomocy Arabii Saudyjskiej. W NSC panuje różnica zdań na ten temat, a CIA ostrzega, że nowa generacja pocisków rakietowych Patriot, mających zestrzeliwać rakiety Scud, jest szczególnie wrażliwa na atak infowojny. Komitet Pokoju Planetarnego, grupa antymilitarystów amerykańskich podejrzewana o powiązania z irańskimi fundamentalistami, intensywnie korzystając z Internetu oświadcza na konferencji prasowej w Waszyngtonie, że mobilizuje się, by uniemożliwić proponowane użycie wojsk USA.

15 lutego 2000. Siły zbrojne Iranu są w pełni zmobilizowane, w tej sytuacji Wielka Brytania, Francja i Stany Zjednoczone uzgadniają wysłanie wojsk do tego rejonu. Ale w ruchach wojsk amerykańskich przeszkadza skomputeryzowany atak w postaci niezliczonych połączeń z telefonami baz wojskowych, co uniemożliwia korzystanie z tych telefonów. Opracowana przez Pentagon Zsynchronizowana w Czasie Lista Rozlokowania Wojsk, koordynująca transport żołnierzy i niezbędnych im dziesiątków tysięcy ton broni, sprzętu, żywności i paliwa, rozsypuje się, ponieważ wprowadzone do niej „robaki" komputerowe zniekształcają niezbędne dane. Powoduje to powszechny chaos.

Tuż po południu wariują automaty kasowe dwu największych banków Georgii, dodając tysiące dolarów do kont klientów, lub przeciwnie, odejmując z nich tego rzędu sumy. Wszystkie banki Georgii reagują na to zamrożeniem pracy swych automatów. W pięć minut później zanika na 12 minut dźwięk i obraz CNN. Wróciwszy na ekrany sieć ta przekazuje raport o stopniu narażania USA na cyberwojnę. Nie mija godzina, a oddział systemu Rezerw Federalnych w Atlancie powiadamia o runie na banki Georgii. W całym kraju ludzie załamani tym, co dzieje się w Georgii, zaczynają wycofywać pieniądze z banków. Panika ogarnia całe państwo.

17 lutego 2000. 0 7.44 wieczorem w kabinie pilotów brytyjskiego samolotu podchodzącego do lądowania na londyńskim lotnisku Heathtrow gasną wszystkie światła. 20 sekund później samolot uderza w ziemię, wszystkie 402 osoby na jego pokładzie giną. Islamska Organizacja Rewolucyjna powiadamia pocztę elektroniczną Scotland Yard, że to ona odpowiedzialna jest za tę katastrofę – jednocześnie Brytyjczycy uzyskują dowody, że oprogramowanie sterowania tym samolotem zawierało „bombę logiczną". Tymczasem FBI chwyta w San Antonio, w Teksasie dwu podejrzanych pracowników firmy, która przygotowywała oprogramowanie dla tego samolotu. FBI wykrywa, że dwójka ta ostatnio dostała poważną sumę w gotówce wypłaconą przez bank szwajcarski podejrzewany o powiązania z Iranem.

18 lutego 2000, kiedy zapada noc, centralne dowództwo USA zaleca dokonanie uprzedzającego ataku na siły irańskie przygotowane już do pancernego uderzenia na Arabię Saudyjską. Jednocześnie jednak dane wywiadowcze na temat tego, kto kryje

się za atakami informatycznymi na USA, są wciąż niejasne. W Arabii Saudyjskiej znajome twarze prezenterów wieczornych wiadomości telewizyjnych zostają elektronicznie zastąpione przywódcami kampanii na rzecz Islamskiej Odnowy i Demokracji, wzywających do zamachu stanu przeciwko rodzinie królewskiej rządzącej krajem. System telefoniczny Arabii Saudyjskiej zaczyna zawodzić, a jednocześnie nowi prezenterzy komunikują, że władzę w Rijadzie, Dahranie i Mekce przejęła „Tymczasowa Republika Arabska".

Na drugim piętrze Pentagonu, funkcjonariusze wywiadu informują sekretarza obrony, że nieznani cyberprzestępcy wszczęli powszechną dezinformację w USA. Ofiarą ataku padły komputery większości baz wojskowych USA na świecie – pracują wolniej, rozłączają się i załamują. Co gorsza, samoloty JSTARS – grające role ośrodków dowodzenia lotnictwa na linii frontu i przystosowane do zdalnej lokalizacji czołgów i oddziałów wojskowych nieprzyjaciela przygotowującej atak na nie sił sojuszniczych – zaczynają przejawiać oznaki infekcji elektronicznej na przykład migotanie komputerowych monitorów.

19 lutego 2000. Późnym popołudniem przestają działać w Waszyngtonie wszystkie telefony – łącznie z komórkowymi. One również padły ofiarą „pułapek" wprowadzonych do oprogramowania systemów łączności. Prezydent próbuje zwołać nadzwyczajne posiedzenie NSC, ale brak telefonów to uniemożliwia. W końcu jednak Rada zbiera się w Białym Domu. Pentagon opowiada się za potencjalnie długotrwałą i krwawą wojną z Iranem o Arabię Saudyjską. Doradca do spraw Bezpieczeństwa Narodowego ostrzega, że Stany Zjednoczone „znalazły się na krawędzi głębokiej klęski strategicznej, którą mogą im zadać przywódcy wojującego islamu". Wiceprezydent domaga się, by USA dokonały odwetu i również rozpoczęły cyberwojnę. Prezydent patrzy w telewizor na pozbawiony głosu obraz przedstawiciela Komitetu Pokoju Planetarnego. Rzecznik Komitetu podaje, że ugrupowanie to mobilizuje wszystkie swe siły, by uniemożliwić „szaleńczy pęd" USA do wojny.

Kiedy gra wojenna dobiega końca, jej uczestnikom zostaje zadane pytanie: „Jakie – twoim zdaniem działania powinien podjąć naczelny dowódca? Oczekuje on, że w ciągu 50 minut otrzyma twoje memorandum z zaleceniami działań".

Po zakończeniu gry Rand Corporation zestawiła lekcje jakie z niej można wyciągnąć: „Każdy może cię zaatakować ... Możesz nie wiedzieć, kto jest atakowany i kto dowodzi ... Możesz nie wiedzieć co dzieje się naprawdę ... Możesz nie wiedzieć, kto jest twoim przeciwnikiem i jaki jest jego potencjał ... Możesz nie wiedzieć, że jesteś atakowany ani kto atakuje, ani jak dokonuje ataku ... USA przestaną być bezpiecznym schronieniem. „Jeden z uczestników gry powiedział: Wszyscy zdawali sobie sprawę, że jest to nowy typ konfliktu i że nie jesteśmy do niego przygotowani".(...)

Jeszcze inny przykład przytoczony przez tygodnik „Wprost".

Pentagon[2], początek grudnia 1998 r. Na tajny briefing w gabinecie gen. Henry-ego Sheltona, przewodniczącego Kolegium Połączonych Sztabów, przybywają najwyżsi rangą dowódcy wojskowi oraz cywilni pracownicy wywiadu wojskowego. Ostatni do sali konferencyjnej wchodzą nie znani nikomu młodzi ludzie. Jeden z nich podłącza do Internetu przenośny komputer. Odszukuje internetową stronę Departamentu Obrony zawierającą biografię gen. Sheltona i wypisuje z niej kilka danych. Następnie wchodzi do jednej z publicznych baz danych i po kilku sekundach na ekranie laptopa ukazuje się adres i telefon jednego z synów generała, mieszkającego na Florydzie. Dokonujący prezentacji pyta, czy jest on objęty ochroną kontrwywiadowczą lub antyterrorystyczną. Po przeczącej odpowiedzi w sali zapada cisza.

Bohaterami spotkania byli ludzie wchodzący w skład tzw. czerwonych zespołów (red teams). W czasach zimnej wojny mianem "czerwonych zespołów" określano podczas prowadzonych w Pentagonie komputerowych gier wojennych wojska Układu Warszawskiego. Tym razem w skład "drużyn" weszli fachowcy od Internetu - by nie powiedzieć: maniacy komputerowi. Ich zadaniem było ustalenie, jakim zagrożeniem dla bezpieczeństwa państwa mogą być opublikowane w sieci informacje na temat amerykańskich sił zbrojnych. Co takiego udało im się znaleźć, że w wyniku prezentacji w Pentagonie natychmiast wyłączono ponad tysiąc serwerów?

---

[2] Bohenek J. Szpieg online. Wprost nr 11 z 14 marca 1999 s. 84-86.

"Czerwone zespoły" znalazły w Internecie - i to bez włamywania się do zastrzeżonych serwerów - mapy oraz satelitarne i lotnicze zdjęcia amerykańskich instalacji wojskowych, na podstawie których można było zaplanować atak terrorystyczny. Po tym odkryciu jeden z oficerów wywiadu nazwał paranoją fakt, że zdjęcia, które kosztem milionów dolarów Ameryka uzyskiwała ze swych satelitów rozpoznawczych, są teraz za darmo udostępniane w Internecie. Korelując odpowiednio uzyskane dane, można było także określić stan aktualnej gotowości bojowej amerykańskich sił jądrowych oraz czas i miejsce przeprowadzenia ćwiczeń z użyciem broni nuklearnej. Na przykład dane z biografii dowódcy konkretnej jednostki w połączeniu z analizą rozmów telefonicznych pozwoliły ustalić, kiedy wyjeżdża on na poligon atomowy w Nevadzie.

Zagrożenie dla wojskowej sieci komputerowej Milnet istnieje nieprzerwanie właściwie od momentu powstania Internetu. W latach 1985-1987 grupa hakerów z Hanoweru dotarła aż do komputera Dowództwa Obrony Powietrznej w górach Cheyenne w Kolorado, skąd kontrolowane są amerykańskie rakiety międzykontynentalne i system wczesnego ostrzegania. Zachęceni sukcesem odwiedzili komputery Dowództwa Lotnictwa Strategicznego w Omaha, bazy danych Pentagonu - Optimis i Recon - a także serwery centrów badań jądrowych Lawrence Livemore i Los Alamos. Spenetrowali również komputer poligonu rakietowego w Nowym Meksyku. Gdy zabrakło im pieniędzy na sprzęt i narkotyki, nawiązali kontakt z rezydenturą KGB we wschodnim Berlinie. Za dokumenty i oprogramowanie, które przekazali Rosjanom do czasu wpadki w 1988 r., otrzymali łącznie 90 tys. marek.

W Internecie żadna wiadomość nie może być już poufna

Tym razem Pentagon potraktował sprawę poważnie. Specjalnie dla Białego Domu zorganizowano symulację komputerową pod kryptonimem "Cyber Viewer". Prześledzono trzy hipotetyczne scenariusze. W pierwszym z nich 35 hakerom pracującym na zlecenie Korei Północnej udało się za pomocą ogólnie dostępnego sprzętu i oprogramowania sparaliżować całkowicie loty U.S. Air Force nad Półwyspem Koreańskim. Podczas drugiego ćwiczenia ta sama grupa uzyskała - i to nie łamiąc żadnych przepisów - dostęp do urządzeń zasilających i wyłączyła telefony alarmowe w dwuna-

stu miastach USA. Wreszcie podczas trzeciej symulacji hakerzy przejęli kontrolę nad komputerami systemu dowodzenia w Pentagonie, zasypując wojskowych fałszywymi poleceniami. Prezentacja poruszyła prezydenta Clintona do tego stopnia, że postanowił natychmiast wystąpić do Kongresu o dodatkowe 2,8 mld dolarów na walkę z elektronicznym szpiegostwem i terroryzmem.

Dyskusje publiczne zapoczątkowało jednak nie to, że wydatki na ten cel w przyszłorocznym budżecie mają zostać zwiększone aż o 40 proc., lecz fakt, że z serwerów Pentagonu usunięto ze względów bezpieczeństwa większość dostępnych wcześniej informacji. Departament Obrony poinformował, że ma dowody na częste wizyty na swych stronach także osób z państw oficjalnie uznawanych przez USA za wrogie. Przeciw takiemu działaniu zaprotestowała waszyngtońska Federacja Naukowców Amerykańskich (FAS), grupa badawcza zajmująca się problematyką wojskową i wywiadowczą, w tym wieloma aspektami rozszerzenia NATO. John Pike z FAS powiedział: "Mamy do czynienia z polityką informacyjną czasu wojny. Zniknęły wszystkie informacje, dzięki którym można by określić, czym aktualnie zajmuje się Departament Obrony". Federacja, powołując się na ustawę o wolności informacji, zażądała powtórnego udostępnienia danych. Najdobitniej problem nazwał jednak dr Ivan Eland, ekspert do spraw bezpieczeństwa z prestiżowego CATO Institute: "Należy się zastanowić, do jakiego stopnia instytucje rządowe mogą chronić własne bezpieczeństwo, nie ograniczając przy tym wolności obywatelskich użytkowników Internetu".

Pytanie postawione przez Elanda ma swoje uzasadnienie. Już w połowie lat 70. w USA doszło do publicznego skandalu związanego z operacją "Minaret". Jak ujawnił senator Frank Church, kierujący Komisją Śledczą Kongresu w latach 1967 1973, Agencja Bezpieczeństwa Narodowego (NSA), Pentagon i Federalne Biuro Śledcze (FBI) prowadziły elektroniczne rozpoznanie wywiadowcze zarówno pojedynczych osób, jak i organizacji pacyfistycznych protestujących przeciwko wojnie w Wietnamie. Po zakończeniu dochodzenia w marcu 1976 r. senator Church powiedział, że "techniczne możliwości NSA można w każdej chwili wykorzystać przeciwko narodowi amerykańskiemu i trzeba dopilnować, by urząd ten wypełniał swoje zadania w ramach obowiązującego prawa i podlegał odpowiedniej kontroli".

BIBLIOTEKA GŁÓWNA
Nr ewid.
Działu Zbiorów Jawnych Akademii ON

Prezydent Clinton postanowił wystąpić do Kongresu o 2,8 mld dolarów na walkę z elektronicznym szpiegostwem i terroryzmem

W pamięci wielu ekspertów utkwiła tzw. afera INSLAW, ujawniona w wyniku rozpoczętego w 1989 r. dochodzenia Komisji Prawnej Izby Reprezentantów. W 1978 r. firma INSLAW opracowała program komputerowy Promis, najdoskonalsze wówczas narzędzie do elektronicznego przeszukiwania baz danych. Pięć lat później zainteresował się nim Departament Sprawiedliwości. Program okazał się hitem, gdyż doskonale nadawał się do analizy powiązań między poszczególnymi sprawami karnymi, nazwiskami, datami i miejscowościami. Wkrótce po ujawnieniu możliwości programu Departament Sprawiedliwości w wyniku skomplikowanej procedury prawnej doprowadził firmę INSLAW do bankructwa i stał się właścicielem nie tylko praw, lecz także tzw. kodu źródłowego, umożliwiającego wszelkie modyfikacje funkcji programu. W 1983 r. Promis był już w posiadaniu zarówno Agencji Bezpieczeństwa Narodowego (NSA), czyli amerykańskiego wywiadu technologicznego, jak i izraelskiego Mosadu. Służby te swoimi kanałami sprzedały go SHAPE - wojskowemu dowództwu NATO w belgijskim Mons, Interpolowi oraz 88 krajom na całym świecie, w tym Związkowi Radzieckiemu (w 1986 r. wraz ze spreparowanym pakietem komputerów). We wszystkich tych krajach Promis został natychmiast zaadaptowany do potrzeb służb specjalnych. Jednak zarówno Amerykanie, jak i Izraelczycy wbudowali w oprogramowanie tzw. tylne drzwi, dające im możliwość zdalnego dostępu do danych zgromadzonych przez służby innych państw - oczywiście, bez ich wiedzy. Jak ujawnił w swej książce "Profits of War" były izraelski agent Ari Ben-Menashe, aż do 1991 r. Amerykanie byli w stanie kontrolować zasoby elektroniczne radzieckiego wywiadu GRU. Wydawać by się mogło, że wraz z upadkiem muru berlińskiego i związaną z rozwojem Internetu eksplozją informatyczno-komunikacyjną problem wykorzystywania najnowszych technologii informatycznych do orwellowskiego nadzoru nad obywatelami zniknie w sposób naturalny. Stało się jednak inaczej. W nadanym przez biznesowy kanał sieci CNN reportażu poinformowano o usterce występującej we wszystkich wersjach internetowej przeglądarki Netscape Navigator, pozwalającej osobom trzecim podglądać dane na dysku użytkownika. Użytkownicy Navigatora natychmiast zaczęli wydzwaniać do firmy z pytaniem, jak to możliwe, że taka usterka nie została zauwa-

żona przez tyle lat. Odpowiedź była przerażająca: "To nie usterka, lecz cecha tego programu". W wywiadzie dla sieci MS-NBC rzecznik prasowy Netscape James Clarke powiedział: "Musieliśmy to zrobić, by spełnić uzasadnione życzenia organów ścigania".

Podczas gdy międzynarodowe instytucje finansowe zastanawiają się, jak ratować rosyjski budżet, jedyną rządową instytucją, która nie musi się troszczyć o swój budżet (choć ma zredukować swój personel o 40 proc.), jest Federalna Agencja Łączności Rządowej i Informacji (FAPSI), czyli rosyjski wywiad elektroniczny. Wydatki na FAPSI mają bowiem aż do roku 2001 rosnąć o 11 mld rubli (2 mld dolarów) rocznie. Agencja powołana w 1993 r. dekretem prezydenta Jelcyna od pierwszego dnia działalności miała wyjątkową pozycję w rosyjskim systemie władzy. Powstała z połączenia różnych wydziałów techniki operacyjnej KGB - nasłuchu elektronicznego, radiowego i satelitarnego, łamania szyfrów i kodowania. Zasięg działalności FAPSI jest dużo szerszy, gdyż w przeciwieństwie do amerykańskiej NSA nie obowiązuje jej zakaz obserwacji własnych obywateli.

Po raz pierwszy nad realną władzą tej służby opinia publiczna zaczęła się zastanawiać w 1995 r., kiedy Borys Jelcyn dekretem nr 334 zakazał używania do szyfrowania danych sprzętu i oprogramowania bez autoryzacji FAPSI. Stało się jasne, że agencja ta nie zatwierdzi żadnego standardu kodowania, którego nie będzie w stanie złamać. Wprowadzenie dekretu 334 oznacza, że żaden rosyjski bank nie jest w stanie zapewnić klientom tajemnicy bankowej. Do dziś dla zachodnich biznesmenów jest to podstawowa, choć niechętnie ujawniana publicznie, przeszkoda na drodze do inwestowania w Rosji.

Hakerzy potrafią przejąć kontrolę nad komputerami systemu dowodzenia w Pentagonie

Nie mniejsze znaczenie dla Rosjan ma sieć stacji do prowadzenia nasłuchu elektronicznego (SIGINT). Jedną z najważniejszych jest placówka w Lourdes w pobliżu Hawany na Kubie, położona zaledwie 140 km od wybrzeży Florydy. Przez całe lata ok. 2 tys. rosyjskich techników prowadziło nasłuch amerykańskiej łączności wojskowej, satelitów telekomunikacyjnych oraz położonych na Florydzie instalacji kosmicz-

nych NASA. Podsłuchiwano nawet rozmowy prowadzone na statkach handlowych. To właśnie z Lourdes Kreml otrzymał wiadomość o rozpoczęciu przez USA wojny w Zatoce Perskiej.

Prawdziwa eksplozja Internetu, z którego w Rosji korzysta już ponad milion osób, szybko uzmysłowiła szefom służb, że metodami chałupniczymi nie da się kontrolować tej technologii. Liczba Rosjan użytkujących infostradę podwaja się co roku, a ilość informacji przekazanych e-mailem w ciągu pierwszego kwartału 1998 r. była o 26 proc. większa niż w całym 1997 r.! Spadkobierczyni KGB, Federalna Służba Bezpieczeństwa (FSB), wniosła do Dumy projekt ustawy umożliwiającej jej śledzenie całej poczty elektronicznej, łączności internetowej i transakcji dokonywanych w sieci kartami kredytowymi w czasie rzeczywistym. Projekt opatrzony kodem SORM nakłada na dostawców Internetu obowiązek zainstalowania specjalnych "czarnych skrzynek" i szybkiego łącza światłowodowego do transmisji danych pomiędzy swymi komputerami a centralą FSB.

"Z oficjalną argumentacją trudno się spierać. To oczywiste, że musimy łapać przestępców - stwierdził Anatolij Lewienczuk, ekspert komputerowy, który zdecydował się upublicznić projekt SORM. - Jednak mafia i wszyscy pedofile w tym kraju nie mogą uczynić takich szkód jak działające bez żadnej kontroli organa władzy. Zamiast chronić prywatność obywateli, władza szuka nowych sposobów jej naruszenia. Dopiero osiem lat temu zaczęliśmy wypleniać ten absurd, a on znów powraca".

W Rosji nie ma żadnych regulacji prawnych dotyczących Internetu, tajne służby mają więc pole do popisu. Jedno ze źródeł w komisji ds. polityki informacyjnej rosyjskiego parlamentu ujawniło, że pierwotnie FSB w ogóle nie zamierzała kierować projektu SORM do Dumy, ponieważ uważa, że ustawa o czynnościach śledczych już dziś daje jej wystarczające uprawnienia do kontroli prywatnej korespondencji. Problem jednak polega na tym, że - zgodnie z ustawą - przed otwarciem listu lub założeniem podsłuchu konieczne jest uzyskanie nakazu prokuratorskiego. SORM zaś pozwala dokonywać tych czynności bez jakiegokolwiek nakazu - i co ważniejsze - bez śladu.

Od momentu powstania FAPSI miała poważne kłopoty prawne. Wielu wysokich rangą funkcjonariuszy musiało odejść z agencji w wyniku skandali finansowych. Nic dziwnego, skoro oficerowie wywiadu - wbrew prawu - zajmują się interesami. W maju ubiegłego roku FAPSI ogłosiła, że wprowadza na rynek superbezpieczny telefon komórkowy. Według agencji, aparat, mający kosztować 12 tys. dolarów i przesyłać zarówno głos, jak i dane, był zabezpieczony kodem szyfrującym, którego złamanie - jak podano w broszurze reklamowej - zabrałoby sto lat. Pytanie tylko, czy samej FAPSI będzie się chciało czekać tak długo.

Winn Schwartau w swojej książce Cyberterroryzm: Ochrona twojego bezpieczeństwa w elektronicznym wieku (*Cyberterrorism: Protecting Your Personal Security in the Electronic Age*) pisze między innymi:

Fundamenty współczesnego społeczeństwa[3] 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.

Obecnie Stany Zjednoczone przodują w świecie w zakresie rozbudowy globalnie spiętego sieciami informacyjnymi społeczeństwa. Społeczeństwo to wkracza w wiek informacji gdzie informacyjne i ekonomiczne wartości stają się niemal synonimami. Ponad 125 milionów komputerów połączonych ze sobą przez kompleksowe lądowe i kosmiczne systemy łączności, stanowi podstawę ponad $6 trylionowej ekonomii, która zależna jest od ciągłych i pewnych operacji. Walka informacyjna jest elektronicznym konfliktem, w którym informacja jest strategicznym dobrem wartym podboju lub destrukcji. Komputery i inne komunikacyjne i informacyjne systemy stają się atrakcyjnymi obiektami pierwszego uderzenia.

---

[3] Schwartau W. Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age. Thunder's Mouth Press. New York 1996, s. 28 - 32

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

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

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

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

Wyobraźmy sobie rywalizujące ekonomie walczące o poszerzenie strefy globalnego wpływu na elektroniczne, finansowe infostrady nie poświęcając żadnych wydatków dla zapewnienia zwycięstwa. Następnie wyobraźmy sobie świat złożony z firm, które rywalizują i rozwiązują spory za pomocą regularnych wzajemnych najaz-

dów - blitzkriegów na informacyjne infrastruktury. Świat gdzie elektroniczne i rywalizacyjne szpiegostwo są oczekiwaną manierą prowadzenia biznesu.

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

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

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

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

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

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

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

Walka informacyjna dotyczy przeżycia. Francja i Izrael rozwinęły swoje ekonomie i oparły całe gałęzie przemysłu na kradzieży amerykańskich sekretów. Japonia

i Korea z pomocą ich rządów kradną amerykańską technologię jak tylko schodzi ona z desek kreślarskich.

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

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

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

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

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

2. Wybrane przykłady poglądów na wykorzystanie działań w obszarze informacyjnym

Spośród pojawiających się poglądów na działania informacyjne przytoczone zostaną poglądy NATO, główne założenia poglądów sił lądowych USA oraz stanowisko jednego z wojskowych teoretyków rosyjskich.

2.1. Działania informacyjne z perspektywy NATO

Stanowisko NATO w sprawie działań informacyjnych na sympozjum poświęconym tej tematyce[4] prezentował szef pionu operacyjnego Międzynarodowego Sztabu Wojskowego generał major Jose Gardeta. Do najważniejszych tez jego wystąpienia należą przytoczone poniżej stwierdzenia.

Globalna edukacja technologiczna na polu informacji zmieniła świat[5]. Informacja teraz nie tylko integruje większość elementów nowoczesnego życia, włączając w to świat cywilny i wojskowy, ale także przyśpiesza wszystkie procesy. Operacyjny sposób widzenia na systemowe podejście do walki jest ewidentne. Ten sposób widzenia doprowadził NATO do potrzeby sprawdzenia odporności na ataki informacyjne. To z kolei doprowadziło do rozwoju polityki NATO w zakresie działań informacyjnych (Info – Ops) sprecyzowanej w dokumencie MC-422 (15.12.1998) który został zaaprobowany przez Radę Północnoatlantycką 22 Stycznia 1999. Na tej podstawie działania informacyjne należy rozumieć jako przedsięwzięcia podjęte w celu pomocy decydentom w osiągnięciu celów politycznych i militarnych, poprzez wpływ na informację i procesy bazujące na informacji.

---

[4] Było to międzynarodowe sympozjum zatytułowane „Informacja jako środek, obiekt ataku i broń. Działania informacyjne, co to oznacza?", zorganizowane przez holenderską Królewską Akademię Militarną w grudniu 1999 r.

[5] Gardeta J. Information Operations, The NATO Perspective. „NL Arms. Netherlands Annual Review of Mlitary Studies 1999. Bosh J.M.J. Luiijf H.A.M. Mollema A.R. Information Operations". Breda 1999, s. 105-114

Działania informacyjne integrują wojenną kontrolę i dowodzenie z procesem konsultacji politycznej, aparatem podejmowania decyzji i połączonymi polityczno-wojskowymi operacjami Sojuszu. Zapewnia to dowódcy mechanizm potrzebny do stosowania tego nowego podejścia w planowaniu wojskowym.

Problem działań informacyjnych staje się coraz ważniejszy dla narodów Sojuszu. Dotyczy to nie tylko instytucji wojskowych lub cywilnych, ponieważ powiązania działań informacyjnych wychodzą daleko poza pojedynczy aspekt narodowy. Działania informacyjne mogą dosięgać rdzenia narodu, zniszczyć infrastrukturę i wiele innych rzeczy, dzięki którym naród funkcjonuje.

Jedno z największych korzyści osiągniętych dzięki wdrożeniu działań informacyjnych jest zdolność do zapobieżenia kryzysowi rozwijającemu się w konflikt poprzez środki i metody, które demonstrują potencjalnemu przeciwnikowi, że eskalacja kryzysu nie leży w jego interesie. Aktywność w tym względzie musi być podjęta w czasie pokoju i powinna być zrównoważona, zarówno politycznie, jak i wojskowo. Działania w ramach tej aktywności powinny bazować na identyfikacji słabych i silnych punktów, skupiając się na tych obszarach, gdzie mogą być one wykorzystane najefektywniej.

Być może najbardziej niepokojącym efektem rozwoju działań informacyjnych jest fakt, że panuje ogólne niezrozumienie, czym one naprawdę są. (...)

Działania informacyjne nie są nową koncepcją, są one rezultatem ewolucji wysiłków mających na celu rozwinięcie systematycznego podejścia do walki zbrojnej. Ta ewolucja przebiega od momentu, gdy pierwsza grupa ludzi zorganizowała się, by walczyć z drugą. Nowocześniejsze przykłady ewolucji, można znaleźć w koncepcjach Von Clausewitza, w jego książce „O wojnie" gdzie dyskutuje o zasadach wojny. Nowszą jest amerykańska koncepcja „Wspólnej wizji 2010" (*Joint Vision 2010*), w której nowe podejście do definiowania i wprowadzania połączonych wymagań operacyjnych jest podtrzymywane. Te i wiele innych prób podjętych w celu efektywnego zorganizowania sił zbrojnych i ich działań, plus dzisiejsza technologia, doprowadziły Sojusz do obecnej pozycji.

Definicja C2W

Walka o przewagę w dowodzeniu (Command and Control Warfare - C2W) jest zdefiniowana w dokumencie MC- 348 jako: zintegrowane użycie wszystkich możliwości wojskowych, włączając w to bezpieczeństwo działań (OPSEC), dezinformację, działania psychologiczne (PSYOPS), walkę elektroniczną (EW) i niszczenie fizyczne, wspierane przez wszystkie rodzaje rozpoznania oraz systemy łączności i informacyjne (CIS) w celu uniemożliwienia dostępu do informacji, jej modyfikowania oraz uszkadzania lub niszczenia potencjału dowodzenia i kontroli (C2) przeciwnika, przy jednoczesnej ochronie własnego potencjału przeciw podobnym jego akcjom. Innymi słowy walka o przewagę w dowodzeniu oznacza działania zapobiegające uzyskaniu przez przeciwnika informacji potrzebnej do prowadzania działań militarnych i podejmowania decyzji mających na celu kontrolę i użycie własnych sił. (...)

Spektrum konfliktu

Działania informacyjne nie zastępują walki o przewagę w dowodzeniu lecz integrują strategię wojskową z procesami konsultacji politycznej, aparatem decyzyjnym, i połączonymi, polityczno – wojskowymi działaniami Sojuszu. Innymi słowy, walka o przewagę w dowodzeniu C2W to wojskowe zastosowanie działań informacyjnych. NATO ma znaczące doświadczenie w walce o przewagę w dowodzeniu (C2W) i korzysta z niego. Zaaprobowaliśmy politykę zawartą w dokumencie MC- 348 i od 1995 roku niemal każdy opracowywany plan operacyjny zawierał załącznik C2W.

Chociaż Wojna w Zatoce jest traktowana jako pierwsza wojna informacyjna, nie było to pierwsze zastosowanie walki o przewagę w dowodzeniu w walce. Dowódcy przez wieki wiedzieli, że pozbawienie przeciwnika informacji jest doskonałym sposobem na zahamowanie jego kampanii i wzmocnienie swoich możliwości.

Jak w takiej ilości informacji możemy z jednej strony zapobiec „wyciekowi" informacji docierających do przeciwnika, a z drugiej, zatrzymać odwrotny proces - przeładowanie informacjami naszego systemu? Duża część odpowiedzi leży w planowaniu na wszystkich szczeblach. Ale w dzisiejszym otoczeniu, planowanie nie musi być ściśle przywiązane do planowania wojskowego, a to odnosi się szczególnie do NATO. Warto przypomnieć, że przecież działania informacyjne mają potencjał ude-

rzenia na praktycznie każdy komponent struktury narodu i państwa. Jeśli sobie uświadomimy fakt, że wszystkie możliwości wojskowe NATO wywodzą się od dziewiętnastu państw efekt, jaki działania informacyjne mogą wywrzeć na akcje NATO staje się jasny. Byliśmy świadkami efektów dobrze kierowanej i przeprowadzanej kampanii działań informacyjnych podczas operacji Alied Force, której autorem był nasz przeciwnik.

Działania informacyjne dotyczą informacyjnych celów, które dowódca chce osiągnąć przez swoje działania. Jest to fundamentalna strategia dowódcy dla planowania działań. Działania informacyjne przynoszą różne skutki na różnych poziomach wojny, ponieważ na każdym poziomie uwaga skupia się na innych sprawach. Na poziomie strategicznym działania informacyjne są używane jako wsparcie działań NATO. To wsparcie jest osiągane poprzez wpływanie na wszystkie elementy (polityczny, wojskowy, ekonomiczny i informacyjny) potęgi narodowej przeciwnika, oraz osłonę własnych komponentów potęgi. Działania informacyjne na szczeblu operacyjnym koncentrują się na wspieraniu kampanii lub głównych celów operacyjnych. Główne uderzenie na tym poziomie polega na niszczeniu linii komunikacyjnych, logistyki, dowodzenia i kontroli. Działania informacyjne na szczeblu taktycznym wspierają osiąganie poszczególnych celów taktycznych.

W tym miejscu warto wprowadzić definicję działań informacyjnych. Dokument MC 422 pt. „NATO Information Operations Policy" został zaaprobowany przez Komitet Wojskowy 15 grudnia 1999 i przez Radę Północnoatlantycką 22 stycznia 1999. W tym dokumencie działania informacyjne są zdefiniowane jako „**przedsięwzięcia podjęte w celu wywarcia wpływu na decydentów w ramach wsparcia politycznych i militarnych celów poprzez oddziaływanie na informację innych, ich procesy informacyjne oraz systemy dowodzenia, kontroli, łączności i informacyjne, przy wykorzystaniu i ochronie własnej informacji i systemów informacyjnych**". W zależności od natury podjętych akcji są dwie główne kategorie działań informacyjnych: defensywne i ofensywne.

Niektóre możliwości wykorzystywane w defensywnych działaniach informacyjnych zawierają: zabezpieczanie informacji, bezpieczeństwo działań (OPSEC),

ochronę fizyczną, kontrdezinformację, kontrpropagandę, kontrwywiad i walkę elektroniczną (EW). Ofensywne działania informacyjne mogą również wspierać defensywne. Systemy informacyjne umożliwiają stosowanie możliwości bojowych oraz służą ich zwiększaniu, chociaż zwiększająca się zależność NATO do tych systemów stwarza wrażliwości. Niemożliwa jest całkowita ochrona wszystkich systemów. Dlatego też stopień ochrony poszczególnych zasobów zależny być powinien od wartości informacji i ryzyka związanego ze stratą lub deformacją informacji. Jest kilka wzajemnie zależnych procesów i możliwości związanych z defensywnymi działaniami informacyjnymi. Do najważniejszych z nich należą ochrona środowiska informacyjnego, wykrywanie ataków na systemy informacyjne, odtwarzanie niszczonych systemów i odpowiadanie na prowadzone ataki oraz możliwości ich prowadzenia tych procesów.

Ofensywne działania informacyjne zawierają zintegrowane użycie własnych i wspierających zasobów i ich możliwości wspierających się wzajemnie z rozpoznaniem dla wywarcia wpływu na decydentów przeciwnika i osiągnięcia lub promowania konkretnych celów. W ramach działań ofensywnych stosuje się między innymi przedsięwzięcia bezpieczeństwa działań, dezinformacji wojskowej, działań psychologicznych, walki elektronicznej, fizycznego niszczenia i ataku na sieci komputerowe.

NATO w sytuacji kryzysowej prowadzić będzie minimalne działania ofensywne ze względu na naturę Sojuszu, która wymaga konsensusu dziewiętnastu suwerennych państw, aby zaaprobować te akcje. Różne systemy prawne państw, komplikują sytuację jako że niektóre działania informacyjne zostały uznane za nielegalne.

Co to wszystko naprawdę znaczy?

Należy przyjąć, że oznacza to użycie wszystkich środków, jakimi dysponujemy, aby ochronić nasze informacje, systemy informacyjne i procesy bazujące na informacji, próbując jednocześnie zniszczyć te same systemy przeciwnika. Część posiadanego potencjału jest bardziej przydatny do działań informacyjnych niż reszta, ale w żaden sposób nie zmniejsza to możliwości kreatywnego użycia całego potencjału. Analizując go dochodzimy do wniosku, że działania informacyjne na początku można rozpocząć od stosowania walki o przewagę w dowodzeniu (C2W), walki elektronicznej (EW), bezpieczeństwa działań (OPSEC), dezinformacji, fizycznego niszczenia i działań psy-

chologicznych (PSYOPS). Jednakże działania informacyjne zawierają dużo więcej elementów niż te wymienione. Jeden z tych elementów, działania psychologiczne, wart jest szczególnej uwagi, jako że działania te mogą przynieść istotny efekt już w czasie pokoju.

Działania psychologiczne

Od kiedy walka o przewagę w dowodzeniu (C2W) jest stosowana przez wojsko, stało się jasne, że cel tej walki - przywódcy przeciwnika w zależności od zajmowanego szczebla w łańcuchu dowodzenia - prezentują różny stopień wrażliwości i podatności na atak. Ten łańcuch dowodzenia rozciąga się od dowódców wojskowych poszczególnych szczebli dowodzenia aż do stolicy przeciwnika i cywilnego kierownictwa. Konsekwencje zastosowania większości przedsięwzięć walki o przewagę w dowodzeniu przeciwko władzom państwowym stanowiłby akt wojny. W czasie pokoju przywództwo polityczne nie stanowi prawnie uzasadnionego obiektu ataku.

Z kilku przyczyn działania psychologiczne mają specjalne miejsce w walce o przewagę w dowodzeniu i w działaniach informacyjnych. Działania te wpływają na przywództwo przeciwnika, siły zbrojne i nawet na cywilną ludność podczas pokoju. Pomimo tej właściwości, działania te nie mają wielkiego uznania w świecie polityków. Członkowie tych elit muszą rozumieć bardzo ważne relacje między działaniami psychologicznymi a przekazywaniem informacji społeczności. Techniki działań psychologicznych używane są do planowania i prowadzenia perswazyjnej działalności informacyjnej w stosunku do grupy będącej przedmiotem oddziaływania. Celem działań psychologicznych nie jest propaganda lub kłamstwo lecz dostarczenie prawdziwej informacji lub oświadczeń w najlepszym, dla operacyjnych potrzeb, czasie. Właściwie kłamstwo byłoby nieproduktywne, ponieważ po zdemaskowaniu spowodowałoby utratę wiarygodności co uniemożliwiałoby wykonanie misji.

Jeśli prawidłowo zastosowane, działania psychologiczne mogą obniżać morale i redukować skuteczność sił przeciwnika oraz tworzyć niechęć do walki w jego szeregach. Po drugie, działania te oraz publiczne informowanie (PI) muszą być koordynowane. Działania psychologiczne są najbardziej skuteczne wtedy, gdy wpływają na przepływ informacji. Ilość informacji przekazywanych społeczeństwu może być tak

dozowana, aby wzmocnić odczucia społeczne, które chce się wzmocnić. Działania psychologiczne prowadzone podczas pokoju mogą mieć inne cele, niż te w czasie kryzysu lub wojny. W czasie pokoju siły zbrojne prowadzą działania pozawojenne, takie m.in. jak operacje wsparcia pokoju, pomoc humanitarna, pomoc w czasie katastrof. Podczas konfliktu działania psychologiczne są prowadzone tak jak wiele innych działań, aby wspomóc osiągnięcie celów dowódcy. Władze polityczne Sojuszu powinny patrzeć na działania psychologiczne i publiczne informowanie jako partnera a nie przeciwnika, a już na pewno nie jako na maszynę propagandową. Działania psychologiczne są czysto wojskową zdolnością i jako takie nie mogą zastąpić informowania publicznego. Planowanie i skoordynowane użycie działań psychologicznych i publicznego informowania może zapobiec wybuchowi otwartych aktów przemocy. Sam ten fakt czyni działania psychologiczne godnymi włożonego w nie wysiłku, który społeczność polityczna powinna zrozumieć, aby umieć wykorzystać stworzone możliwości. (...)

Jeśli chodzi o działania informacyjne, najważniejszym jest naświetlenie kilku najważniejszych zmian, które pojawiły się w ciągu ostatnich dziesięciu lat i znacząco wpłynęły na sposób, w jaki wojska NATO działają w sytuacjach kryzysowych lub w konflikcie. Na ten sposób wpływ mają: technologia, poziom politycznego zaangażowania w konflikt, wrażliwość narodowa i rozpoznanie.

Globalna ewolucja technologiczna na polu informacji zmieniła świat. Informacja nie tylko integruje większość elementów nowoczesnego życia włączając w to wojsko, ale również przyśpiesza wszystkie procesy. Obecnie dysponujemy środkami i możliwościami przekazywania niemalże nieograniczonej ilości informacji, według naszych potrzeb, w ciągu zaledwie sekund. Miniaturyzacja komputerów uczyniła je wyposażeniem standardowym, nawet na polu bitwy. Daleko zaawansowane są prace nad rozwojem systemów realizujących wyznaczanie obiektów ataku (targeting) w czasie zbliżonym do rzeczywistego, gdzie dane przekazywane będą bezpośrednio do atakującej broni tj. od czujnika do atakującego.

Technologia jest tylko jednym z aspektów działań informacyjnych. O innych była mowa przy charakterystyce działań psychologicznych. Jest to aspekt semantyczny

i poznawczy. Część techniczna, (czyli fizyczna i logiczna) jest prawdopodobnie lepiej rozumiana niż semantyczna, ponieważ zawiera to, do czego jesteśmy przyzwyczajeni, czyli wyposażenie i jego użycie. Podczas gdy działania informacyjne skupiają się na rozwiązaniach nie kinetycznych, należy pamiętać, że niszczenie fizyczne, jeden z głównych elementów C2W, jest także elementem Info-Ops. Aspekt poznawczy odnosi się zaś do informowania publicznego, działań psychologicznych i medialnych.

Zimna wojna zapewniała Sojuszowi „idealną sytuację planistyczną", selektywnie długie okresy narastania napięcia do aktów wrogości, znane obszary zaangażowania, znani i rozumiani przeciwnicy i ich możliwości. Głównym zadaniem aparatu politycznego było decydowanie, czy NATO będzie się angażować, czy nie, a jeśli tak to określenie stopnia tego zaangażowania. Z chwilą gdy konflikt się rozwinął była stosunkowo słaba ingerencja polityków w działania militarne. Dzisiaj jak wiemy warunki się zmieniły. Ale czy my wojskowi, zmieniliśmy się również, by dotrzymać kroku temu nowemu światu? Jak zademonstrowaliśmy to w operacji Allied Force świat NATO jest pełen politycznego zaangażowania podczas kryzysu. Oznacza to fakt, który był zawsze znany w społeczeństwach demokratycznych, że władza cywilna kontroluje wojsko. Wojsko musi funkcjonować w rzeczywistości stworzonej przez polityków. Dobrym przykładem tego była sytuacja zaistniała po stwierdzeniu, że NATO nie użyje wojsk lądowych w Kosowie. Oczywiście, był to czysto polityczny ruch. Użycie wojsk lądowych było punktem spornym i konsensus na szczeblu politycznym był potrzebny, aby utrzymać jedność Sojuszu. Mimo to wpływ, jaki to stwierdzenie miało na działania wojskowe, był poważny. Wpływ działań militarnych na politykę i implikację imperatywów politycznych na prowadzenie operacji militarnych muszą być w pełni rozumiane zarówno przez struktury polityczne, jak i wojskowe.

Kolejną zmianą, o której musimy pamiętać, jest wrażliwość narodowa. Wrażliwości narodowe były zawsze główną sprawą braną pod uwagę w NATO i tak powinno być w Sojuszu, gdzie wszystkie decyzje oparte są na konsensusie. Chociaż, w czasie zimnej wojny, ta sytuacja nie wpływała bezpośrednio na działania w ramach artykułu piątego, lub przekazania zasobów pod dowództwo NATO. Co to, oznacza jest ewidentne. Jak wspomniano wcześniej, wiele z zasobów Sojuszu było przygotowywanych, by spełnić wymagania artykułu piątego, co było planowane od lat.

Przykładem zasobów, które są ściśle chronione przez państwa, to zasoby umożliwiające prowadzenie ofensywnych działań informacyjnych i rozpoznania. Te zasoby nie są przekazywane do NATO w zakresie jaki wynikałby z potrzeb.

Kolejnym ważnym czynnikiem odnoszącym się do narodowych wrażliwości i ich związku z wykorzystaniem zasobów działań informacyjnych jest opinia publiczna. Dzisiaj walka zbrojna jest widoczna w naszych domach niemalże bez opóźnienia. Wojna widziana w perspektywie CNN jest normą. Oczywiście, opinia publiczna jest bardzo ważną dla polityków i będzie wywierać zasadniczy wpływ na ich decyzje dotyczące użycia zasobów działań informacyjnych.

Rozpoznanie

Następną, wartą przedyskutowania zmianą jest rozpoznanie. Łatwiej o tym dyskutować w środowisku wojskowym bo rozpoznanie jest częścią każdej działalności wojska. Planowanie, wykonanie i ocena efektywności działań informacyjnych jest praktycznie niemożliwa bez odpowiedniego rozpoznania. To stwarza dla NATO szczególnie trudny problem do rozwiązania ze względu na to, że Sojusz nie posiada ograniczonych zdolności w zakresie rozpoznania. Dodatkowo, nie ma wspólnego, wojskowo – politycznego aparatu rozpoznawczego w NATO. Na dodatek wymagania działań informacyjnych dla rozpoznania są całkowicie inne niż te, tradycyjnie istniejące w siłach zbrojnych.

Rozpoznanie musi być terminowe, dokładne, użyteczne, kompletne, wiarygodne, obiektywne i wystarczająco szczegółowe, by sprostać szerokim wymaganiom NATO. W wielu wypadkach, rozpoznawcze przygotowanie pola bitwy, które jest najważniejsze w działaniach informacyjnych, będzie wymagało postawienia pytania, którego nie stawialiśmy dotąd rozpoznaniu - dlaczego? W przeszłości potrzebowaliśmy, tylko faktów, np. zidentyfikowania celu, możliwości obronnych itd. W działaniach informacyjnych ta informacja nie jest wystarczająca, aby wykonać zadanie.

Przypuśćmy, że NATO przewiduje operację wspierania pokoju w kraju X. W przygotowaniu do operacji, analiza infrastruktury kraju X koncentruje się na poszukiwaniu słabych i silnych miejsc. Podczas analizy odkryto, że podczas dnia, pijalnia wód mineralnych jest miejscem spotkań setek ludzi w stolicy X. Jeśli byłby to cel działań w

przeszłości, to od rozpoznania wymagano by „tylko faktów": dyslokacji, wymiarów, ochrony. Teraz, jeśli byłby to cel działań informacyjnych potrzebowalibyśmy dodatkowo wiedzieć: dlaczego ludzie spotykają się tam, co dzień? Czy są tam oni z powodów kulturowych czy religijnych? Odpowiedź na to pytanie może zapewnić możliwość użycia kilku możliwości działań informacyjnych. Tak, więc działania informacyjne kładą rozpoznaniu dodatkowe wymagania.

Rozpoznanie przyczynia się także do wykrycia ataku przez zapewnienie ostrzeżenia przed potencjalną aktywnością przeciwnika i zbierania informacji, o jego ruchach.

Obecnie musimy być bardzo dokładni w określaniu wymagań dla rozpoznania. Nie może ono dostarczyć satysfakcjonujących informacji, jeśli nie wie, czego szukać i jak szukać. Pierwszym wymaganiem w stosunku do rozpoznania jest określeniu ewentualnych źródeł i charakteru zagrożeń dla NATO. W następnej kolejności potrzebne jest określenie czy dany kraj lub grupa państw posiada zdolności do stworzenia zagrożenia działaniami informacyjnymi dla NATO.

Reasumując, warunki zmieniły się znacznie w ciągu tych ostatnich dziesięciu lat. Świat wojskowy będzie musiał nie tylko to zaakceptować, ale także dostosować się do nowej sytuacji.

Sytuacja opisana powyżej ma duży wpływ na wszystkie działania militarne, włączając w to informacyjne. Szczególnie jest to prawdziwe na szczeblu strategicznym i wojskowo - politycznym. Działania informacyjne nie powinny być rozpatrywane jako nowa strategia, jednakże szybkość i natężenie, z jakim możemy transmitować informację i szeroki zakres obszaru zastosowań, całkowicie zmieniły wpływ informacji na polityczno – militarne relacje.

Droga w przyszłość

Co to znaczy dla NATO i w jaki sposób może ono czerpać korzyści z nowych możliwości oferowanych, przez działania informacyjne? Oczywiście pierwszym krokiem jest opracowanie planu rozwoju. Z powyższych rozważań wynika, że:

Należy przyzwyczaić liderów i kluczowy personel kierowniczy Sojuszu by myśleli inaczej.

Należy zrozumieć, że dokumenty (polityka i doktryna) nie zawsze zapewniają nam pewność, do której jesteśmy przyzwyczajeni i jakiej oczekujemy. Bieżąca sytuacja i polityczne wytyczne będą decydować o tym jak siły zbrojne reagują i działają w konflikcie. Polityczne decyzje dotyczące działań mogą zapadać w stosunkowo krótkim czasie. Jednym z poważniejszych doświadczeń wyniesionych z działań w Kosowie jest świadomość tego, że wojsko musi działać w środowisku stworzonym przez polityków. Z kolei, politycy muszą myśleć o militarnych skutkach decyzji, które podejmują. Bardzo ważne jest by kierownictwo polityczne i wojsko tworzyły zintegrowany front działań informacyjnych. By spełnić zadość tym wymaganiom potrzebny będzie wojskowy mechanizm kierowania.

Z myślą o przyszłości i potrzebie posiadania odpowiedniego mechanizmu kierowania stworzono grupę roboczą działań informacyjnych. Grupa ta jest kierowana przez oficera generała i ma stałych przedstawicieli z państw, dowództw strategicznych, środowisk prawnych i szefów z obszarów funkcjonalnych zawierających elementy walki o przewagę w dowodzeniu, tj. działań psychologicznych, a także sztabu międzynarodowego i komitetu ochrony informacji NATO.

Podczas udziału NATO w rozwoju działań informacyjnych dla sytuacji związanej z Kosowem, stało się jasne, że nie ma wspólnego dla NATO zrozumienia tych działań i konieczności przygotowania i przeprowadzenia kampanii w tym obszarze. W tych okolicznościach rozwijanie świadomości w tym zakresie jest dla Sojuszu priorytetowe. Przede wszystkim, na najwyższym szczeblu, świadomość pozwala działaniom informacyjnym stać się elementem procesu myślowego kadr kierowniczych, w czasie rozpatrywania sprawy politycznych i wojskowych Sojuszu. Im wcześniej to się stanie, tym bardziej prawdopodobnym jest, że działania informacyjne będą miały wpływ na rezultat operacji. Na wszystkich szczeblach świadomość pozwala na szerszą perspektywę w realizowaniu bieżących zadań.

W zakresie defensywnych działań informacyjnych podjęto szereg przedsięwzięć, szczególnie w zakresie zapewnienia bezpieczeństwa informacji. Opracowywa-

ne są odpowiednie dokumenty oraz powoływane niezbędne organy np. Zespół Reagowania Ratownictwa Komputerowego (Computer Emergency Response Team – CERT). Zespół ten będzie zapewniał użytkownikom systemów informacyjnych i łączności doradztwo i bezpieczeństwo. Ustanowienie CERT będzie miało daleko idące skutki i wpływ zarówno na wojskowe, jak i na cywilne elementy Sojuszu.

Znowu, rozwijanie świadomości jest bardzo ważne. Podstawowe formy, dzięki którym próbuje się rozwinąć tą świadomość to wykłady w szkole NATO - SHAPE, uczestnictwo w kongresach, seminariach i grupach roboczych.

Działania informacyjne muszą stać się stałym elementem procesu planowania operacyjnego. Działania te można stosować przez całe spektrum konfliktu od pokoju poprzez kryzys, wojnę i z powrotem do pokoju. Pojawiają się wyraźne oznaki ze strony Rady Północnoatlantyckiej zrozumienia roli tych działań. Polityczne wytyczne Rady odgrywać będą zasadniczą rolę we wdrażaniu wszystkich aspektów koncepcji działań informacyjnych. Tworzenie planów operacyjnych związanych z sytuacją kryzysową w Kosowie pokazało taką potrzebę. Reagowano wówczas na doraźne potrzeby. Natomiast potrzebne jest skodyfikowanie działań w zakresie planowania i prowadzenia działań informacyjnych w odpowiednich dokumentach.

Teraz kilka słów o zależności NATO od państw, jeśli chodzi o ważne zdolności takie jak rozpoznanie, które są witalne dla planowania i prowadzania działań informacyjnych. Niektóre zdolności ofensywne działań informacyjnych rozwinięte przez niektóre państwa NATO są bardzo delikatnej natury i dosyć drogie, przez to zdolności te nie będą udostępniane dla NATO. Dlatego rozważnym jest rozwinięcie organicznych zdolności ofensywnych działań informacyjnych przez Sojusz. Jest ważnym aby na wypadek konieczności przeprowadzenia kampanii działań informacyjnych zachowany był ich międzynarodowy charakter i wkład odzwierciedlający charakter Sojuszu. Dlatego też wszędzie gdzie to jest możliwe poszczególne państwa powinny wnosić swój wkład w zakresie działań informacyjnych na wszystkich poziomach.

Prowadzenie działań informacyjnych w czasie pokoju, jeśli odkryte jako celowe, może być traktowane jako prowokacja lub wrogi akt i dlatego wymaga wyraźniej

autoryzacji politycznej ze strony Rady Północnoatlantyckiej i określenia reguł reagowania oraz sprecyzowania dyrektyw planistycznych.

Dwa z głównych komponentów działań informacyjnych rozpoznanie oraz systemy informacyjne i łączności będą mocno zaangażowane w określaniu zagrożeń dla naszych systemów i ich odporności na te zagrożenia. Jako minimum na wstępie należy określić najważniejsze systemy, które muszą być chronione by zapewnić sprawne funkcjonowanie NATO.

Wkrótce zostanie zainicjowany proces opracowania doktryny działań informacyjnych. Doktryna jest akumulacją wiedzy i doświadczenia zdobytych w dotychczasowej praktyce. Działania na Bałkanach dostarczą dużej ilości nowej wiedzy i doświadczenia i wywrą wpływ na kształt doktryny. Jednakże doktryna, w odniesieniu do działań informacyjnych, nie może sięgać zbyt głęboko. Działania informacyjne są bardziej sposobem myślenia, a nie czymś co jest łatwo wymierne.

2.2. Stanowisko sił lądowych USA

Siły lądowe USA bardzo poważnie traktują wyzwania przyszłości. Jeszcze pod koniec lat siedemdziesiątych rozpoczęto badania studyjne nad polem przyszłej walki. Wieloletni systematyczny wysiłek zaowocował wizją, która ukierunkowała rozwój uzbrojenia, form organizacji i sposobów prowadzenia walki.

Wojna z Irakiem stała się pierwszym poważnym sprawdzianem obranego kierunku rozwoju. Wojna ta była pod wieloma względami niezwykła. Zdarzyła się tuż po upadku bloku komunistycznego, a więc na początku zupełnie nowej sytuacji geopolitycznej na świecie, gdzie cały aparat militarny Stanów Zjednoczonych i wielu innych państw dostosowany był do dwubiegunowego świata. Siły zbrojne przygotowane były do walki z byłym Związkiem Radzieckim i Układem Warszawskim.

Przygotowanie irackiej kampanii pełne było improwizacji. Prowizorycznie sprzęgano ze sobą systemy, które nie były do tego przystosowane, np. systemy kosmicznego rozpoznania strategicznego, strategiczne systemy ostrzegania, strategiczne systemy łączności itp. Niektóre z tych przedsięwzięć podejmowano już w toku działań bojowych, kierując się nowymi doświadczeniami i potrzebami. Wszyscy uczestnicy przekonali się o kluczowej roli informacji. Była ona podstawowym filarem sukcesu. Bez niej niemożliwe byłoby użycie broni precyzyjnej, niemożliwe byłoby jednoczesne działanie tak dużej ilości samolotów w ograniczonej przestrzeni, niemożliwe byłoby też prowadzenie natarcia w trudnych warunkach pustyni a wiec nie zaistniał by słynny manewr oskrzydlający generała Schwarzkopfa.

Coraz bardziej skomplikowane współczesne i przyszłe działania bojowe stają się nie do pomyślenia bez informacji. Siły lądowe USA po praktycznym, irackim doświadczeniu zrozumiały, że albo szybko dostosują się do nowej sytuacji albo stracą swoje znaczenie i poparcie społeczeństwa. Były oczywiście i inne przyczyny zmian takie, jak zmiana charakteru sił zbrojnych z rozmieszczonych na wysuniętych rubieżach na głównie kontynentalne (rozmieszczone na terytorium USA) z szybką projekcją siły w niezbędne rejony, wielobiegunowa sytuacja polityczna świata, zmniejszanie wydatków budżetowych na obronność itp.

Podejmuje się więc wysiłek by dokonać rzeczywistych nieraz rewolucyjnych, a nie pozorowanych zmian. Promuje się kulturę nagradzania i awansu wszystkich, którzy są niekonwencjonalni i rzucają wyzwania skostnieniu i rutynie. Stworzono wiele instytucjonalnych płaszczyzn w ramach, których prowadzi się badania teoretyczne i praktyczne. Toczy się ponadto niemalże narodowa dyskusja. Szeroko publikowane są problemy i założenia rozwoju. Podstawowe plany i założenia nie tylko nie są utajniane, lecz wręcz szeroko propagowane. Każdy bez trudu może zapoznać się ze wszystkimi najważniejszymi dokumentami opublikowanymi w Internecie, ale również w tradycyjnej formie. W oparciu o ich treści odbywa się szeroka debata w różnych kręgach formalnych i nieformalnych. Spotkać można wiele publicznej krytyki i propozycji. Powoduje to lepsze poznanie i zrozumienie problemów sił lądowych przez społeczeństwo i w rezultacie zacieśnienie więzi i poparcie. Społeczeństwo lepiej się utożsamia z wojskiem i przyjmuje przez to jego problemy jako swoje.

By praktycznie przetransformować to intelektualne wyzwanie wojska lądowe USA stworzyły system prowadzenia szeregu doświadczalnych ćwiczeń na różnych szczeblach, utworzono bitewne laboratoria, zintensyfikowano prace nad nową doktryną i regulaminami, szeroko stosuje się symulacje, opracowano koncepcje i wdrożono do praktyki modelowe formy takie jak: Zaawansowany Eksperyment Bojowy, Zaawansowany Demonstrator Technologii, Zaawansowany Demonstrator Koncepcji Technologicznej i inne. Cały wysiłek koncentruje się na trzech kierunkach: przebudowanie wojsk operacyjnych, przebudowanie infrastruktury wspierającej oraz na rozwoju i dostarczeniu technologii informacyjnego wieku, a więc sprzętu i oprogramowania informacyjnego. Trwa nieustanny ferment wewnątrz i na zewnątrz sił lądowych co stymuluje poszukiwania, przyśpiesza proces i podnosi jego jakość ponieważ jest rezultatem szerokiego wysiłku myślowego i praktyki, a nie tylko wymysłem jakiejś komórki sztabowej.

Siły XXI to w całości przetransformowane siły lądowe XXI wieku. Centralną i zasadniczą cechą tych sił będzie zdolność do wykorzystywania informacji. Informacja i cyfrowe technologie tworzą tak synergiczny efekt pomiędzy działającymi systemami, organizacjami i komponentami, że możliwości wojsk lądowych zostaną wzmocnione o rząd wielkości. (...)

Elektroniczne połączenia pomiędzy wszystkimi rzutami wojsk lądowych i wśród nich zaowocują taką prędkością i precyzją komunikacji, że całościowa, organizacyjna świadomość sytuacji i zwinność wojsk daleko przekroczą dzisiejsze możliwości. (...)

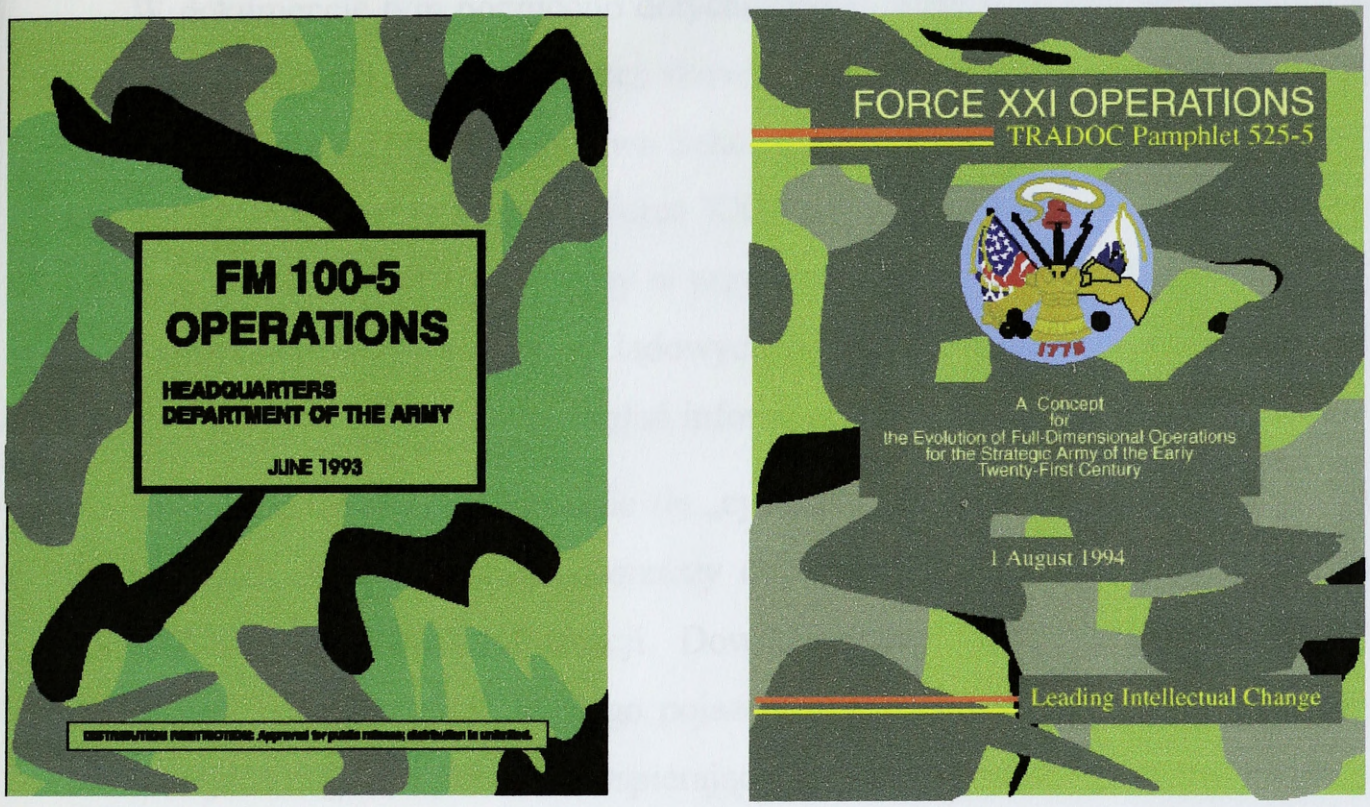
Ponieważ Siły XXI będą modularne z natury, łatwo mogą być z nich komponowane niezbędne dla wykonania konkretnego zadania zgrupowania sił. Modularność ta zapewni elastyczność i umożliwi prowadzenie wszystkich rodzajów operacji militarnych. Siły XXI będą idealnie pasowały do prowadzenia operacji połączonych i będą w pełni kompatybilne z systemami innych rodzajów sił zbrojnych. Informacyjne więzi z innymi elementami sił połączonych będą ich podstawową charakterystyką. Więzi te będą jednym z zasadniczych czynników decydujących o sukcesie działań połączonych.

Jednym z zasadniczych celów stawianych przed Siłami XXI jest wygranie wojny informacyjnej.

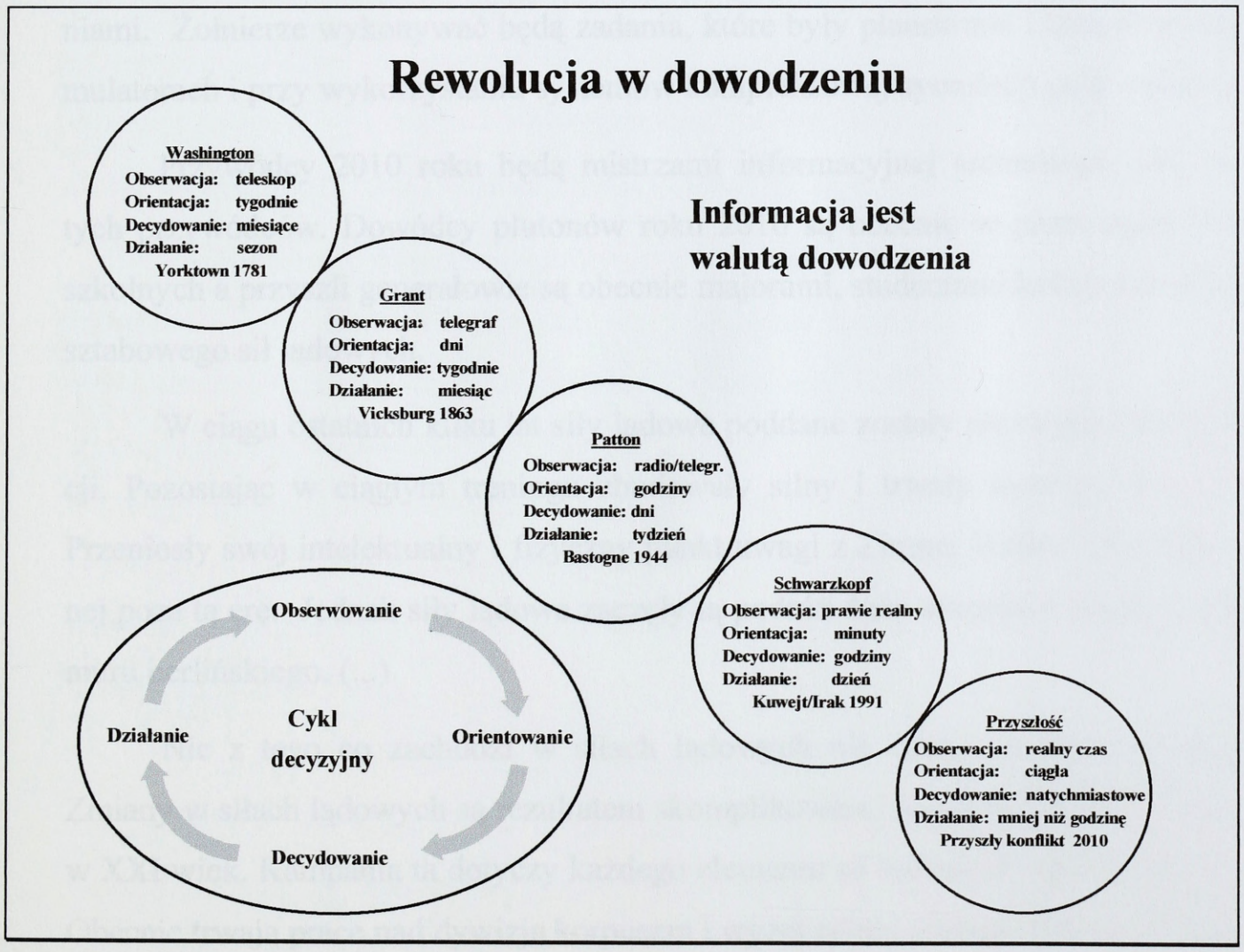
Najsilniejszym argumentem za rozwojem Sił XXI jest to że będą one lepsze. Będą one w stanie generować większą moc bojową przy tej samej wielkości sił. (...)

Wojska lądowe USA osiągnęły wysoki stopień zgodności co do kierunków przyszłych zmian i co do tego, że siły lądowe XXI wieku powinny być organizowane wokół informacyjnej technologii. Siły lądowe Stanów Zjednoczonych, podobnie jak i inne rodzaje sił zbrojnych tego kraju stoją obecnie przed wielkim wyzwaniem, które można streścić w jednym pytaniu: Jak wojska lądowe prowadząc bieżące szkolenie i utrzymując gotowość mają sprostać żądaniu swojego narodu by uzyskiwać większe możliwości przy zmniejszaniu liczebności?

Działania prowadzące do całkowitego przekształcenia prowadzone są na wielu płaszczyznach. Jedną z ważniejszych z nich jest nowa doktryna. Intensywnie zmierza się do opracowania innowacyjnej doktryny XXI wieku, która odzwierciedlałaby sposób myślenia i działania i określałaby czym są wojska lądowe. W tym celu intensywnie rozwijana jest nowa doktryna i uaktualniane są istniejące regulaminy w celu dostosowania ich do nowej rzeczywistości. W ramach tej działalności w 1983 r. został zmieniony jeden z zasadniczych dokumentów jakim jest regulamin FM 100-5.



Rys.1. Doktryna operacyjna sił lądowych USA FM 100-5 oraz koncepcja działań XXI wieku.



Rys. 2. Ilustracja rewolucyjnych zmian w dowodzeniu.

W dokumencie tym porzucono dotychczasowe wąskie spojrzenie skoncentrowane na realia Centralnej Europy na rzecz szerokiej gamy scenariuszy i pełnej gamy operacji. Niezależnie od tego Dowództwo Szkolenia i Doktryny TRADOC opracowało dokument 525-5 Operacje Sił XXI (Force XXI Operations), który jest prekursorem przyszłego regulaminu FM 100-5, który w przyszłości zastąpi jego obecną wersję. Dokument ten podkreśla, że siła wojsk lądowych przyszłości będzie zależała od ich możliwości w zakresie prowadzenia działań informacyjnych.

Do roku 2010 pole walki stanie się „cyfrowe". Wdrożenie cyfrowych technologii do wszelkich systemów walki dostarczy dowódcom bezprecedensowych możliwości zdobywania i dystrybucji informacji. Dowódca grupy, wydzielonej do wykonania zadania, znał będzie pozycję każdego pojazdu swojej jednostki i jednocześnie ta sama informacja dostępna będzie dla wspierających i skrzydłowych elementów ugrupowania, a także wszystkich innych jednostek sektora. W toku walki, pojazdy zaopatrzenia będą ładowały amunicję i prowadziły naprawy zgodnie z bieżącymi zapotrzebowaniami. Żołnierze wykonywać będą zadania, które były planowane i trenowane na symulatorach i przy wykorzystaniu systemów kompleksowej symulacji pola walki. (...)

Przywódcy 2010 roku będą mistrzami informacyjnej technologii. Już znamy tych przywódców. Dowódcy plutonów roku 2010 są obecnie w pierwszych klasach szkolnych a przyszli generałowie są obecnie majorami, studentami koledżu dowódczo-sztabowego sił lądowych.

W ciągu ostatnich kilku lat siły lądowe poddane zostały niezwykłej transformacji. Pozostając w ciągłym treningu zbudowały silny i trwały most do przyszłości. Przeniosły swój intelektualny i fizyczny punkt uwagi z Zimnej Wojny i ery industrialnej poza tą erę. Jednak siły lądowe zaczęły tą podróż dużo wcześniej przed upadkiem muru berlińskiego. (...)

Nic z tego co zachodzi w siłach lądowych nie dzieje się przez przypadek. Zmiany w siłach lądowych są rezultatem skomplikowanej kampanii, która prowadzi je w XXI wiek. Kampania ta dotyczy każdego elementu sił lądowych i daleka jest końca. Obecnie trwają prace nad dywizją korpusem i wyżej co nie oznacza jednak, że batalion

i brygada zostały już całkowicie przebudowane. Siły ery informacyjnej nazwano Siłami XXI (Force XXI). (...)

Chociaż obraz walki ery informacyjnej nie jest jeszcze całkowicie jasny to można już przewidzieć część jego charakterystycznych cech. Dowodzenie i kierowanie opierać się będzie na szerokiej znajomości sytuacji bojowej. Odpowiedzialność pozostanie hierarchiczną, jednak organizacje nie będą hierarchiczne w tradycyjnym sensie. Struktura jednostki będzie bardziej elastyczna i łatwiej dopasowywalna do konkretnej sytuacji i zadania. (...)

Pole przyszłej walki będzie inne i bardziej kompleksowe niż pola walki XX wieku. Zaawansowane technologie przyniosą nowe możliwości bojowe co zrewolucjonizuje przyszłą walkę w pięciu kluczowych obszarach: zabójczości i rozproszenia, skali precyzyjnego ognia, integrującej technologii, masy i efektu oraz niewidzialności i wykrywalności.

Z tym jak uzbrojenie stanie się bardziej zabójcze żołnierze i walczące grupy będą jeszcze bardziej rozproszeni. Z czasem zabójczość wzrośnie o rząd wielkości. Wojna z Irakiem była najświeższym przykładem tego jak wzrost zabójczości spowodował wzrost zagrożenia i skomplikował sytuację na polu walki.

Zwiększone rozproszenie zarówno pojedynczych żołnierzy jak i grup bojowych komplikuje dowodzenie i kierowanie oraz pogarsza koordynację działania. Przyszłe walki charakteryzować się będą również zwiększoną skalą precyzji ognia prowadzonego z większych odległości. Już wojna z Irakiem pokazała możliwości oddziaływania na przeciwnika za pomocą precyzyjnego ognia prowadzonego z dużych odległości. Wyłaniające się nowe technologie spowodują, że ogień prowadzony będzie z jeszcze większą dokładnością i zabójczością w każdych warunkach atmosferycznych w dowolnej porze dnia i roku.

W nowej fali walki, integracyjne technologie mieć będą wielkie znaczenie. Technologie te zastosowane w telekomunikacji, rozpoznaniu, globalnej nawigacji i logistyce zwiększą znajomość sytuacji pola walki przez dowódcę. Dostarczą mu większych możliwości w zakresie efektywniejszego organizowania sił i lepszego ich kontrolowania w toku walki.

Pojawiające się nowe technologie spowodują, że przyszłe siły chociaż mniejsze będą dysponowały większymi możliwościami w zakresie rażenia celów. Będą one miały większe możliwości przenikania pola bitwy dzięki większej mobilności i lepszej łączności. Mniejsze jednostki będą w stanie skupiać wysiłek i ogień swojej broni, ponieważ będą nie tylko lepiej zorganizowane lecz i skuteczniejsze dzięki skoordynowanemu wysiłkowi różnych rodzajów wojsk. Bitwy XXI wieku będą charakteryzować się lepszą koordynacją walczących wojsk z artylerią, wojskami inżynieryjnymi, lotnictwem i innymi rodzajami wojsk. Zwiększy się również koordynacja i współpraca różnych szczebli dowodzenia co możliwe będzie dzięki lepszej łączności, nawigacji i innych technologii zapewniających zwiększenie efektów ognia bezpośredniego i pośredniego.

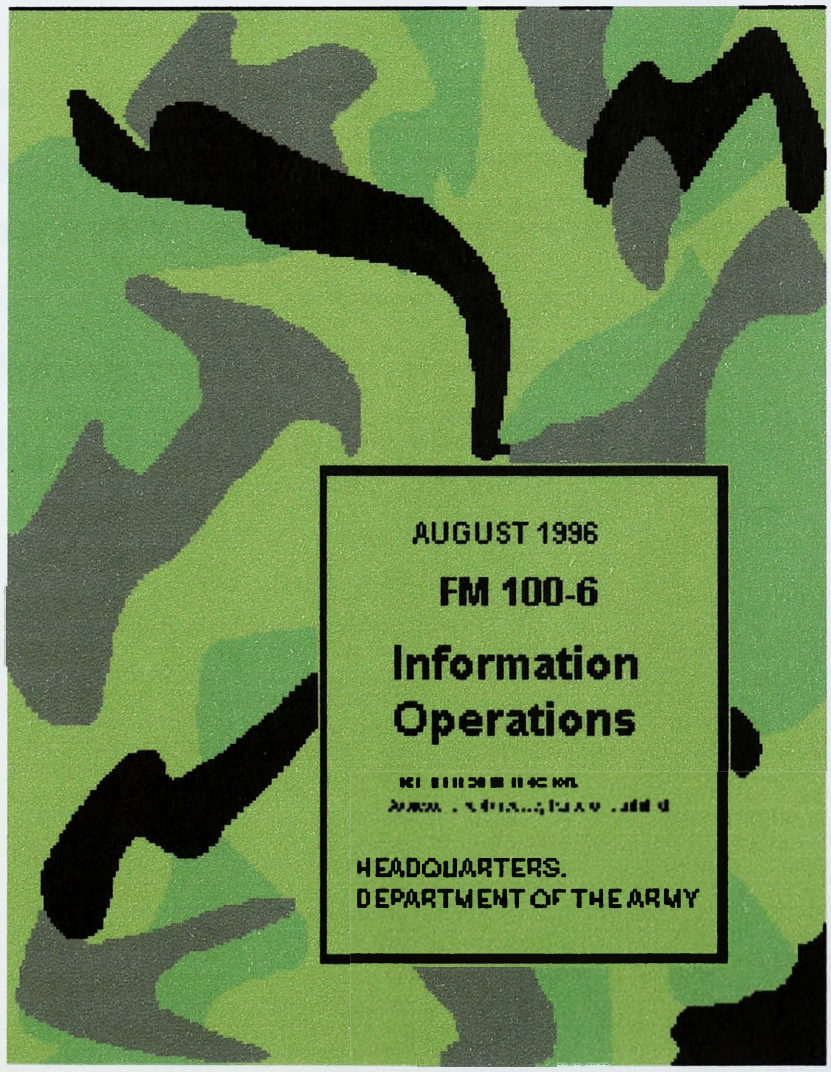
Również manewr w przyszłej walce będzie bardziej efektywny. Nowe technologie zapewnią prowadzenie manewru na duże odległości przy większej kontroli i zdolności przystosowywania się do szybko zmieniającej się sytuacji. Nastąpi pełna integracja jednostek ogólnowojskowych z jednostkami wsparcia bojowego i logistyki. Siły XXI wieku będą więc w stanie maksymalizować korzyści manewru, zwiększać tempo działań i działać w dzień i w nocy we wszystkich warunkach atmosferycznych.

Ponieważ mniejsze jednostki będą w stanie masować wysiłek, działając poza tym w rozproszeniu, istnieć będzie potrzeba obniżenia wykrywalności własnej działalności przez systemy rozpoznania przeciwnika. Z tym jak technologie poprawiają zdolności wykrywania z coraz większych odległości potrzeba bycia niewidzialnym staje się coraz trudniejsza do osiągnięcia lecz jeszcze bardziej niż kiedyś pilniejsza. Przyszły dowódca musi czynić pole walki bardziej przejrzyste dla siebie i bardziej nieznane dla swego oponenta. Wojska nowej ery będą w stanie wykrywać i atakować przeciwnika na polu walki z dużych odległości pozostając samym niewidzialnymi i prowadząc ogień z poza horyzontu. (...)

Informacja do wygrywania wojny wykorzystywana była od dawna. Generał Lee w 1863 roku pokonał dwukrotnie silniejszego przeciwnika mając przewagę informacyjną i odpowiednio ją wykorzystując do kierowania walką. Również w czasie II Wojny Światowej Alianci wykorzystując rozszyfrowane przez siebie tajne informacje

Niemców mogli wielokrotnie paraliżować niemieckie inicjatywy m.in. w Północnej Afryce, Włoszech, Normandii. Takich przykładów jest wiele. Informacja jest walutą dowodzenia.

Informacyjny wiek jest nową erą dla sił lądowych USA. W czasie wojny domowej kurier i telegraf były podstawowymi środkami łączności. To pozwalało dowódcy orientować się w sytuacji w czasie kilkunastu dni, podejmować decyzje w ciągu kilku tygodni i realizować swoje decyzje w ciągu miesiąca. W czasie II Wojny Światowej radio było podstawowym środkiem łączności co pozwalało na orientowanie się w sytuacji w ciągu godzin, decydowania w ciągu dni i wykonywania decyzji w ciągu tygodnia. Generał Schwarzkopf w czasie wojny z Irakiem obserwował sytuacje niemalże w czasie rzeczywistym, orientował się w czasie minut, decydował w czasie godzin i wcielał decyzje w czyn tego samego dnia.



Rys. 3. Doktryna działań informacyjnych sił lądowych USA FM 100-6.

Doktryna działań informacyjnych

Doktryna określa zmiany w siłach lądowych. Dowództwo Szkolenia i Doktryn Sił Lądowych USA (TRADOC) jako pierwsze sformułowało doktrynę walki informacyjnej. Ważność walki informacyjnej jest dobitnie zaakcentowana w opracowanym po raz pierwszy regulaminie FM 100-6 Działania informacyjne (FM 100-6 Information Operations).

Ten nowy dokument definiuje **działania informacyjne jako ciągłą, połączoną działalność, która wzmacnia i chroni cykl decyzyjny dowódcy jednocześnie negatywnie oddziałując na ten cykl u przeciwnika.** Dokument ten jest pierwszym intelektualnym krokiem w kierunku nowego doktrynalnego paradygmatu działań bazujących na wiedzy, zrodzonych przez technologie wieku informacyjnego. Ta nowa doktryna podkreśla ważność przerywania cyklu decyzyjnego przeciwnika. Przerywanie to realizowane jest przez atakowanie jego systemów dowodzenia i kierowania. Takie skoordynowane ataki zawierają elementy walki elektronicznej, fizyczne niszczenie, działania psychologiczne, dezinformację i bezpieczeństwo działań (operational security). Jednocześnie doktryna ta podkreśla konieczność w zakresie zwiększenia szybkości i dokładności własnego cyklu dowodzenia przez jego wsparcie. **Kombinacja atakowania zasilania informacyjnego przeciwnika przy jednoczesnej ochronie i wspieraniu własnej informacji przynosi zdecydowaną przewagę**.

2.3. Rosja

Duże nadzieje w walce zbrojnej przyszłości pokłada się w informacyjnym oddziaływaniu na przeciwnika i w innych rodzajach „nieśmiercionośnej" broni. Uważa się, że współczesne, a tym bardziej armie przyszłości tak silnie są i będą uzależnione od informacji, że można ją zaliczyć do głównych środków oddziaływania na przeciwnika. Są prowadzone badania mające na celu skonstruowanie broni elektromagnetycznej. Nie zabijając ludzi taka broń może sparaliżować pracę urządzeń telefonicznych, radiolokacyjnych, komputerowych i innych środków łączności, naprowadzania, nawigacji, dowodzenia. Myśli się o wynalezieniu takich środków, które powodowały będą unieruchamianie silników, chemikaliów niszczących opony samochodów i samolotów po ich uprzednim rozpyleniu na drogach i lotniskach. Kładzie się duży nacisk na to, żeby przy pomocy takich środków obezwładniać wojska przeciwnika nie niszcząc ich.

W ostatnich latach szczególna uwaga zwracana jest na formę walki, które istnieje od dawna, jednakże obecnie odradza się w nowej postaci. Dotyczy to walki informacyjnej, którą bada m.in. pułkownik Komow.

Według niego opracowanie narodowej teorii wojny informacyjnej napotyka obecnie na obiektywne trudności[6] związane z niejednoznacznym pojmowaniem w różnych kręgach naukowych jej genezy, przedmiotu badania, struktury i treści. Dominują dwa podstawowe podejścia. Pierwsze bazujące na idei informacyjnych środków walki sprowadza problem do tzw. walki komputerowej. Drugie podejście, popierane przez autora, oparte jest na trzech zasadniczych aspektach.

- Po pierwsze, walka informacyjna rozpatrywana jako nieprzemijające zjawisko, towarzyszące ludzkości od momentu jego powstania.
- Po drugie, współczesny fenomen nagłej aktualizacji tego problemu tłumaczy się zwiększeniem znaczenia walki informacyjnej wskutek powstania globalnej, transkontynentalnej przestrzeni informacyjnej.

---

[6] Komow S.A. „O sposobach i formach prowadzenia walki informacyjnej", Wojennaja Myśl 1997 s. 18-22.

- Po trzecie, teorię walki informacyjnej rozpatruje się jako naukę, kumulującą całą zdobytą przez ludzkość wiedzę o prawach, zasadach, formach, sposobach i środkach wywalczania przewagi informacyjnej. Przy czym w jej strukturę i treść powinny być włączone nie tylko empiryczne informacje i teoria tworzenia konstrukcji środków walki informacyjnej i radioelektronicznej, a także sposoby ich zastosowania we współczesnej wojnie, ale również i uogólnione bogatsze wojskowo-historyczne doświadczenia w organizowaniu i prowadzeniu walki informacyjnej.

Do dalszych rozważań przyjmujemy, że sposoby walki informacyjnej to ugrupowanie i metody użycia sił związków operacyjnych (związków taktycznych, oddziałów, pododdziałów) w celu zdobycia i utrzymania przewagi informacyjnej nad przeciwnikiem w czasie przygotowania i prowadzenia działań bojowych.

Sposoby walki informacyjnej zawierają:

- Rodzaj i kolejność oddziaływań informacyjnych na przeciwnika;
- Obiekty oddziaływań;
- Skład sił i środków wydzielonych do prowadzenia walki informacyjnej i ich ugrupowanie.

Treści sposobów wyróżniają się dużą różnorodnością. Skład sił i środków wydzielonych do prowadzenia walki informacyjnej powinien spełniać takie warunki, aby ta sama informacja mogła być opracowana i przekazana do organów kierowania z wykorzystaniem różnych sił i środków.

Wszystkie sposoby walki informacyjnej według tych poglądów dzielą się na trzy podstawowe kategorie: **siłową, intelektualną i kombinowaną**.

Do **kategorii siłowej** odnoszą się sposoby oparte na prowadzeniu walki informacyjnej różnymi rodzajami uzbrojenia (konwencjonalnego, radioelektronicznego, informacyjnego). Zastosowanie sposobów siłowych pozwala osiągnąć przewagę informacyjną w ilości tej informacji niezbędnej do realizacji zadań dowodzenia wojskami (siłami).

Intelektualne polegają na kierowaniu działaniami przeciwnika bez użycia siły. Ich zastosowanie pozwala osiągnąć przewagę informacyjną w jakości informacji wykorzystywanej do dowodzenia wojskami (siłami).

Kombinowane dotyczą sposobów zapewniających osiągnięcie przewagi informacyjnej zarówno w ilości jak i w jakości informacji o sytuacji.

Oprócz tego, w walce informacyjnej (analogicznie do walki zbrojnej) można wyróżnić dwie grupy sposobów: ofensywne i defensywne.

Do grupy ofensywnych zaliczamy następujące sposoby: blokowanie, odwracanie uwagi, wiązanie, nękanie, inscenizacja, dezintegracja, uspokajanie, zastraszanie, prowokowanie, przeciążanie, sugerowanie, wywieranie presji.

Blokowania informacji zawiera się w grupie sposobów siłowych. Istota jego polega na tym, że w etapie przygotowania i prowadzenia działań bojowych, przez przeprowadzenie kompleksu przedsięwzięć przeciwdziałania informacyjnego zupełnie lub częściowo uniemożliwia się zbiór i wymianę informacji w systemach kierowania wojskami i uzbrojeniem przeciwnika. Do realizacji tego sposobu aktywnie stosuje się ogniowe, radioelektroniczne, informacyjne rażenie elementów systemu kierowania wojskami (siłami) i uzbrojeniem przeciwnika.

W skali operacyjnej sposób ten z powodzeniem stosowany był podczas przygotowania i w trakcie przeciwuderzenia i okrążenia niemieckich wojsk pod Stalingradem (listopad 42 rok – luty 43 rok). Informacyjne przeciwdziałanie realizowano głównie poprzez blokowanie zakłóceniami informacji współdziałania. Zakłócenia te emitowane były przez specjalnie przygotowane do tego celu stacje radiolokacyjne. Dzięki temu w znacznym stopniu ograniczono wymianę informacji między okrążoną 6A i grupą armii „Don".

Stosowanie tego sposobu największy rozmach osiągnęło w czasie operacji „Pustynna burza". Wówczas do realizacji tego sposobu masowo stosowano rakiety skrzydlate, lotnicze środki kierowane i środki walki radioelektronicznej. Przypuszcza się, że po raz pierwszy właśnie tam do realizacji zadań bojowych użyto środki walki informacyjnej. Jak wiadomo, zakupione przez Irak we Francji komputery, wchodzące w

skład systemu dowodzenia obroną powietrzną posiadały specjalnie kierowane zastawki, przeznaczone do blokowania informacji dowodzenia. W rezultacie ich uaktywnienia na początku działań bojowych, strona iracka nie była w stanie odpierać ataków ŚNP nad swoim terytorium.

Odwracanie uwagi polega na tym, że na etapie przygotowania działań bojowych, drogą przeprowadzenia kompleksu przedsięwzięć przeciwdziałania informacyjnego, dąży się do stworzenia realnego lub pozornego zagrożenia w stosunku do jednego ze słabych punktów przeciwnika (na skrzydłach, na tyłach itp.) i tym samym wyprzedza się jego zamiar prowadząc działania na jednym z możliwych kierunków w celu odciągnięcia głównych sił przeciwnika do realizacji drugoplanowych zadań.

Stosowanie tego sposobu, dało pozytywne rezultaty wojskom alianckim w Normandii podczas operacji desantowej w 1944 roku. Niemieckie dowództwo było na tyle zdezorientowane co do głównego kierunku uderzenia, że potrzeba było 15 godzin aby opanować sytuację.

Wiązanie sił przeciwnika jest odmianą sposobu odwracania uwagi. Podczas stosowania tego sposobu powoduje się u przeciwnika przekonanie o występowaniu zagrożenia w stosunku do jednego z jego słabych punktów, co prowadzi do zaangażowanie dodatkowych sił i środków. Tak jesienią 1943 roku w czasie Kijowskiej operacji zaczepnej wojska 1 Ukraińskiego frontu częścią sił forsowały Dniepr na północ od Kijowa. Działania te charakteryzowały się dużą uporczywością co spowodowało, że przeciwnik przekonany był, że przełamanie frontu ma nastąpić na tym odcinku. W ten sposób związano tam duże zgrupowanie wojsk niemieckich. W tym czasie radzieckie dowództwo zorganizowało przeprawę przez Dniepr podstawowych sił na odcinku południowym, co pozwoliło wyzwolić Kijów przy stosunkowo niedużych stratach.

Nękanie polega na przeprowadzeniu kompleksu przedsięwzięć oddziaływania informacyjnego w celu zmuszenia przeciwnika do podjęcia bezcelowych lub niekorzystnych działań, co w rezultacie doprowadzi do tego, że przeciwnik przystąpi do walki ze zużytymi środkami i obniżoną zdolnością bojową. W tym celu mogą być prowadzone działania opóźniające lub inne działania prowadzone w ograniczonym zakresie.

Dezintegrację częściej stosuje się w dyplomacji niż w sztuce wojennej. Realizacja tego sposobu polega na przeprowadzeniu kompleksu przedsięwzięć oddziaływania informacyjnego w celu stworzenia warunków, w których przeciwnik będzie uważał za konieczne działać na szkodę koalicji, w ramach której występuje. Do tego celu można wykorzystać dezinformacje opinii publicznej, a także tworzenie pozornego przeświadczenia o trudnej sytuacji polityczno-militarnej w stosunkach pomiędzy państwami uczestniczącymi w konflikcie. Oprócz tego mogą być prowadzone przedsięwzięcia, sprzyjające zaostrzeniu realnie występujących lub sztucznie stworzonych sprzeczności w obozie przeciwnika w celu osłabienia jego wojskowej i ekonomicznej siły. Właśnie taki wariant dezintegracji stosowali Alianci w czasie II Wojny Światowej. Doprowadzili do utworzenia drugiego frontu, wykorzystując w tym celu siły Armii Czerwonej do wyzwolenia krajów europejskich spod faszystowskiej okupacji.

Uspokajanie stosuje się w celu stworzenia wrażenia neutralnego lub pokojowego stosunku do przeciwnika. Istota tego sposobu polega na przeprowadzeniu kompleksu przedsięwzięć oddziaływania informacyjnego, których podstawowym celem jest wywarcie wrażenia u przeciwnika, że zamiast przedsięwzięć przygotowawczych do działań bojowych realizuje się inne działania. Przeciwnik powinien uwierzyć w to i stracić czujność. Dobitnym przykładem takiego działania może być przygotowanie się faszystowskich Niemiec do wojny z ZSRR.

Zastraszanie przeciwnika realizuje się drogą doprowadzenia do niego informacji stwarzającej wrażenie przewagi nad nim, której w rzeczywistości może nie być.

Prowokowanie przeciwnika ma na celu pobudzić go do realizacji działań wygodnych dla przeciwstawnej strony. Tak na przykład w czasie II Wojny Światowej amerykański wywiad wykrył, że w przekazach radiowych Japończyków często powtarza się skrót AF. Istniała hipoteza, że ten kod dotyczy wysp Midway. W celu ujawnienia prawdy postanowiono wysłać telegram w języku angielskim o tym, że niesprawny jest tam system wodociągowy. Wnet amerykański wywiad przechwycił telegram Japończyków o tym, że na AF brakuje wody pitnej. Hipoteza potwierdziła się.

Przeciążanie polega na tym, że w etapie przygotowania do działań bojowych i w trakcie ich prowadzenia doprowadza się do przeciwnika taką ilość sprzecznych in-

formacji, która przeciąża jego systemy kierowania i wymusza podejmowanie decyzji i prowadzenie działań bojowych w warunkach niejasnej sytuacji.

Sugerowanie polega na wytworzeniu, a następnie wykorzystaniu takiego stereotypu informacyjnego, który spowoduje niepowodzenie przeciwstawnej strony. W tym celu, w etapie przygotowania do działań bojowych, a także w trakcie ich prowadzenia, wykonuje się kompleks przedsięwzięć informacyjnego przeciwdziałania polegających na przekazaniu informacji wykorzystując prawną, moralną, ideologiczną lub inną siłę, pobudzającą przeciwnika do realizacji działań wygodnych dla przeciwstawnej strony. Tak, w czasie II Wojny Światowej w Wielkiej Brytanii opublikowano książkę w języku niemieckim pod tytułem „Nostradamus prorokuje o przebiegu wojny". Książka ta w szczególności zawierała informacje o rzekomo istniejącym proroctwie Nostradamusa o nieuniknionym zabójstwie Hitlera. Książkę tę rozpowszechniano w Niemczech, z nadzieją demoralizacji zabobonnych Niemców.

Wywieranie presji oparte jest na doprowadzeniu do opinii publicznej informacji potępiających przeciwnika, wymuszających na krajowych, międzynarodowych, społecznych i innych organizacjach, podejmowanie działania, utrudniającego realizację jego zamiarów. Tym sposobem rząd separatystów prowadził walkę informacyjną w czasie konfliktu czeczeńskiego.

Do grupy sposobów defensywnych można zaliczyć sposoby odblokowywania i identyfikacji.

Odblokowywanie informacji wymaga przeprowadzenia kompleksu przedsięwzięć obrony informacyjnej w celu pozyskania zaszyfrowanej lub zmienionej przez przeciwnika informacji. Przy tym można stosować wszystkie możliwe metody, siły i środki włącznie z przeprowadzeniem działań bojowych na dużą skalę.

Identyfikacja oparta jest na realizacji kompleksu przedsięwzięć obrony informacyjnej, zapewniających zbiór oraz porównanie informacji o tym samym fakcie (zjawisku) z wielu źródeł, co pozwala ujawnić i blokować dezinformację, wprowadzaną przez przeciwnika.

Do podstawowych form prowadzenia walki informacyjnej można zaliczyć:

- Oddziaływanie informacyjne;
- Atak informacyjny;
- Bitwa informacyjna;
- Operacja informacyjna.

Oddziaływanie informacyjne to zorganizowane użycie sił i środków walki informacyjnej do realizacji zadań mających na celu wywalczenie (utrzymanie) przewagi informacyjnej nad przeciwnikiem.

Atak informacyjny to całokształt aktywnych informacyjnych oddziaływań sił i środków samodzielnych pododdziałów na element lub grupę elementów systemów informacyjnych dla realizacji szczególnych zadań taktycznych walki informacyjnej.

Bitwa informacyjna to całokształt różnorodnych informacyjnych oddziaływań i ataków połączonych wspólnym zamiarem, prowadzonych przez specjalnie wydzielone siły i środki ukierunkowane na realizację wspólnego zadania walki informacyjnej.

Operacja informacyjna to całokształt uzgodnionych co do celu, miejsca i czasu oddziaływań informacyjnych, ataków i bitew prowadzonych według wspólnego zamiaru i planu dla realizacji zadań walki informacyjnej na teatrze działań wojennych, strategicznym teatrze lub kierunku operacyjnym.

Do osiągnięcia celów informacyjnych oddziaływań, ataków, bitew i operacji będą stosowane wszystkie sposoby walki informacyjnej.

Na zakończenie należy podkreślić, że globalna informatyzacja już w najbliższej przyszłości może doprowadzić do szerszego zastosowania nowoczesnych środków walki informacyjnej w czasie jej prowadzenia. Ta okoliczność, nie zmieniając istoty rozpatrywanych sposobów, powinna istotnie wzbogacić ich treść i w sposób znaczący podwyższyć efektywność realizacji zadań działań bojowych w ogóle.

3. Poglądy środowisk powietrznych USA na wykorzystanie działań w obszarze informacyjnym

Poglądy środowisk powietrznych na wykorzystanie działań w obszarze informacyjnym są godne zainteresowania ze względu na bardziej niż u innych, aktywne podejście. Ponadto amerykańskie siły powietrzne zainwestowały najwięcej pieniędzy i włożyły wiele wysiłku w zorganizowanie działań informacyjnych.

Dzisiaj, siły powietrzne mają Eskadrę Walki Informacyjnej, która skupia się zwłaszcza na działaniach obronnych informacji i systemów informacyjnych. W przyszłości, forma i możliwości tej organizacji mogą się zmieniać.

Generalnie organizacja ta zapewnia głównym sensorom wszystkich komponentów sił powietrznych, systemom broni, systemom dystrybucji informacji ochronę przed zniszczeniem lub uszkodzeniem mogącym nastąpić w wyniku ataku na informację lub system informacyjny. Reakcją tej komórki na informacyjny atak na taktyczne systemy może być kontratak (przez techniczne lub fizyczne środki), zakłócenie lub wprowadzenie w informacyjne systemy przeciwnika fałszywej informacji. Ponadto eskadra ta może przygotowywać taktyki działania, analizę zagrożenia i ochronę głównych baz danych działań defensywnych, uczestniczenie w usprawnianiu zaatakowanych systemów, szacowanie bezpieczeństwa teatru działań wojennych, ocenianie możliwości obronnych i identyfikację zagrożenia oraz prowadzenie ostrzegania przed możliwością ataku. Eskadra ta włączona została w system organizacji działań informacyjnych. Ponadto siły powietrzne dysponują Zespołami Ratownictwa Komputerowego, które mogą być szybko kierowane w rejony rozmieszczenia sił zagrożenia.

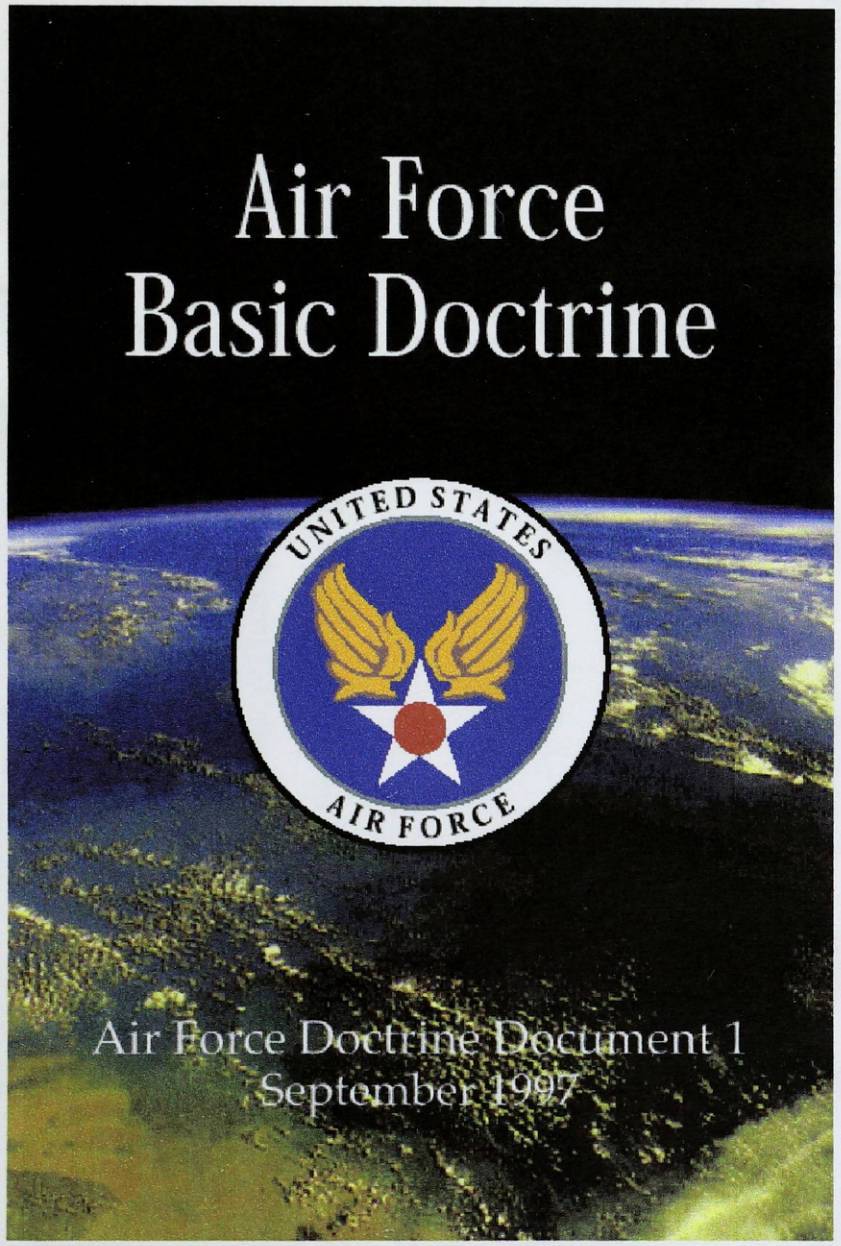
Wcześniej przeprowadzono szereg kompleksowych badań i dyskusji. Weryfikowane były kolejne propozycje doktryny. W 1998 roku z obszernych badań oraz praktyki powstała doktryna działań informacyjnych. Ze względu na nowatorskie treści jest ona godna szczegółowego zaprezentowania.

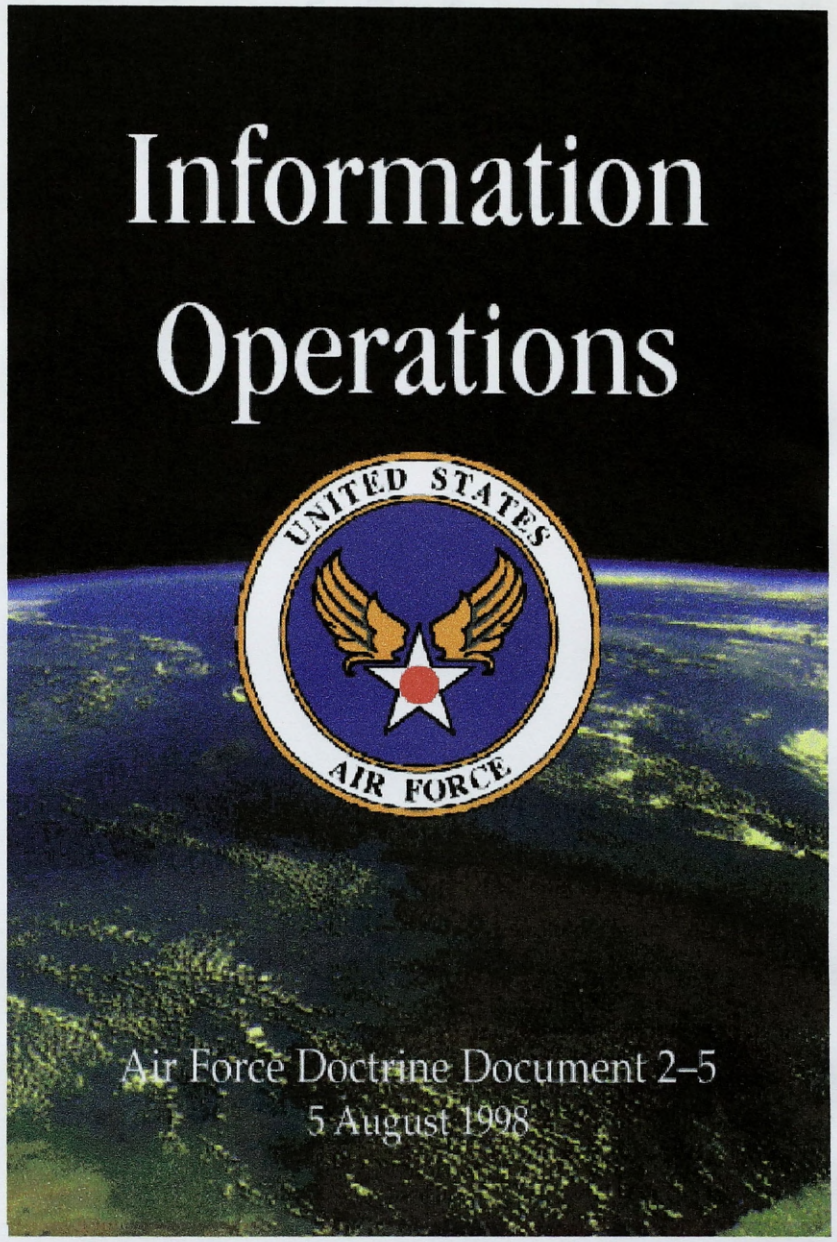
3.1. Treść doktryny działań informacyjnych amerykańskich sił powietrznych

Amerykańskie siły powietrzne w drugiej połowie lat dziewięćdziesiątych podjęły intensywne wysiłki nad opracowaniem nowej doktryny powietrznej przystosowanej do potrzeb warunków XXI wieku. W doktrynie tej duży akcent położono na informację i działania informacyjne. Szersze rozwinięcie tej problematyki zawarte jest w dokumencie doktryny powietrznej, specjalnie poświęconym działaniom informacyjnym. Ze względu na prekursorski charakter treści tej doktryny zostaną zaprezentowane dosyć wiernie.

Informacja od dawna była integralnym składnikiem ludzkiego współzawodnictwa, ci którzy dysponowali doskonałymi możliwościami do jej zbierania, zrozumienia, kontroli i użycia uzyskiwali zdecydowaną przewagę na polu walki. Używając informacji uzyskiwało się znaczną przewagę na polu bitwy. Historia jest pełna przykładów jak informacja wpływała na polityczne i wojskowe starcia – od najwcześniejszych bitew, które zarejestrowała historia do ostatnich działań militarnych w Bośni. Wizja przyszłości sił powietrznych wyłożona w dokumencie „Globalne zaangażowanie: wizja sił powietrznych 21 wieku" *(Global Engagement: A Vision for the 21st Century Air Force)*, uwzględnia to przez uznanie przewagi informacyjnej jako jednej z sześciu podstawowych zdolności sił powietrznych. Dzisiaj, bardziej niż kiedykolwiek, zdobycie i utrzymanie przewagi informacyjnej jest najważniejszym zadaniem dowódców i ważnym warunkiem realizacji pozostałych podstawowych zdolności sił powietrznych. Wykonywanie działań informacyjnych w powietrzu, kosmosie i coraz częściej w cyberprzestrzeni stanowi narzędzia, którymi siły powietrzne realizują swój udział w zabezpieczeniu przewagi informacyjnej swojemu narodowi, połączonemu dowódcy, dowódcy komponentu oraz siłom koalicyjnym.

Siły powietrzne przekonane są co do tego, że działania informacyjne zawierają przedsięwzięcia podejmowane dla pozyskiwania, wykorzystania, obrony lub ataku informacji i systemów informacyjnych. Działania informacyjne odnoszą się do całego spektrum działań militarnych od pokoju do pełnego konfliktu.





Rys. 4. Podstawowy dokument doktryny powietrznej USAF AFDD-1 oraz doktryna działań informacyjnych AFDD 2-5 amerykańskich sił powietrznych.

Siły powietrzne są przekonane, że aby w pełni rozumieć i osiągnąć przewagę informacyjną, rozumienie działań informacyjnych musi wyraźnie zawierać dwa, zasadniczo odmienne konceptualnie, ale niezwykle mocno połączone ze sobą filary: **informacja w walce** – reprezentująca aspekty zdobywania i wykorzystywania lub inne bazujące na informacji procesy oraz **walka informacyjna** – reprezentująca aspekty ataku i obrony.

Ten dokument doktryny koncentruje się głównie na walce informacyjnej, szczególnie na przeciwdziałaniu informacyjnym (Counterinformation) tj. funkcji potęgi powietrznej, przez którą siły powietrzne realizują swój zakres odpowiedzialności wynikający z definicji działań informacyjnych określonej przez Departament Obrony.

Niedawno sformułowana definicja walki informacyjnej uznaje ją za działania informacyjne prowadzone dla obrony własnej informacji i systemów informacyjnych lub atakowania i wpływania na informację przeciwnika oraz jego systemy informacyjne. Defensywny aspekt walki informacyjnej – defensywne przeciwdziałanie informacyjne, podobnie jak strategiczna obrona powietrzna, jest prowadzone ciągle. W przeciwieństwie do tego ofensywna część walki informacyjnej – ofensywne przeciwdziałanie informacyjne jest prowadzone w czasie kryzysu lub konfliktu. Walka informacyjna zawiera różnorodną gamę przedsięwzięć takich jak działania psychologiczne, dezinformacja wojskowa, walka elektroniczna, fizyczny i informacyjny (cyber) atak oraz wiele przedsięwzięć i programów obronnych. Godnym podkreślenia jest fakt, że walka informacyjna jest prowadzona w całym spektrum sytuacji od kryzysu do wojny co ma zabezpieczyć efektywne realizowanie zadań stojących przed siłami powietrznymi.

Doktryna sił powietrznych uznaje całkowite zintegrowanie różnych działań militarnych. Powietrzne i kosmiczne działania mogą wspierać i wzmacniać działania informacyjne i na odwrót. Walka informacyjna wykorzystuje rosnącą wrażliwość informacji i systemów informacyjnych. Walka ta nie jest zależna od typu platform czy od jakiegoś szczególnego stopnia wrogości działań militarnych. Podstawy walki informacyjnej – atakowanie i wpływanie na informację przeciwnika i jego systemy informacyjne i obrona swojej informacji i systemów informacyjnych nie zmieniły się z upły-

wem czasu. To, co się zmieniło to środki i drogi ataku. Ponadto, dzisiejsze własne środowisko informacyjne dysponuje nieznanymi poprzednio własnymi zdolnościami i odpowiedzialnością. Zdolności te muszą być w pełni wykorzystywane a obciążenia skutecznie zarządzane. Dwa filary działań informacyjnych, informacja w walce i walka informacyjna, choć oddzielne i różne muszą być ściśle łączone jedna z drugą i ze wszystkimi funkcjami potęgi powietrznokosmicznej.

Informacja wyłoniła się jako zasadnicza możliwość ale i wrażliwość wszystkich działań militarnych. Musimy być przygotowani do uzyskania przewagi informacyjnej w całym spektrum działań militarnych.

Stany Zjednoczone nie są osamotnione w uznawaniu tych potrzeb – potencjalni przeciwnicy na całym świecie szybko ulepszają i wdrażają swoje własne zdolności do prowadzenia walki informacyjnej. Równocześnie z przekształcaniem się sił powietrznych w siły powietrzne i kosmiczne XXI wieku, musi był zbudowany fundament niezbędny dla rozwoju zdolności koniecznych dla sprostania wyłaniającym się wyzwaniom informacyjnego wieku.

Natura działań informacyjnych

Dominowanie nad informacyjnym spektrum jest tak bardzo ważne dla współczesnego konfliktu jakim było w przeszłości okupowanie terenu lub panowanie w powietrzu.

Gen.Ronald R.Fogleman

Podobnie jak przewaga w powietrzu i przestrzeni kosmicznej umożliwia dowódcy swobodę ataku i bezpieczeństwo przed atakiem tak przewaga informacyjna spełnia również podobną funkcję. Zdolność do wspierania dowódcy kompleksowym, wielozródłowym, zbliżonym do czasu realnego, odzwierciedleniem sytuacji bojowej przy jednoczesnym uniemożliwianiu osiągania tego samego przez przeciwnika jest istotą działań informacyjnych. Możliwość poprawy zdolności dowódcy do obserwacji, orientowania się, decydowania i działania (pętla OODA) szybciej i poprawniej niż przeciwnik, jest tylko częścią sprawy. Przez powstanie działań informacyjnych poja-

wiają się nowe zestawy obiektów działań, stają się dostępne nowe bronie, pojawia się też możliwość bezpośredniego wpływania na decyzje przeciwnika, przez opóźnianie, zakłócenie, czy dezinformację. Jednakże ostatecznie działania informacyjne istnieją dla wsparcia dowódców w ocenie sytuacji, szacowaniu zagrożeń i ryzyka oraz podejmowanie właściwych i terminowych decyzji.

Siły Powietrzne są przekonane, że dominacja w informacyjnym spektrum jest równie ważna w obecnym konflikcie jak w przeszłości było zajmowanie terenu czy panowanie w powietrzu. Dominacja w informacyjnym spektrum jest widziana jako nierozerwalny i synergiczny komponent potęgi powietrznej. Czas pomiędzy zebraniem informacji i jej dostępnością dla użytkowników na wszystkich szczeblach skrócił się obecnie do niewyobrażalnie krótkich wartości. O ile posiadanie, wykorzystanie i manipulacja informacją zawsze była ważną częścią działań wojennych, tak w przyszłości może się to stać głównym czynnikiem wpływającym na wynik konfliktu w przyszłości. Mimo, że tradycyjne zasady wojny mają wciąż zastosowanie są one coraz częściej związane ze zrozumieniem, że posiadanie i manipulacja informacją mogą być kluczowym warunkiem wygrania wojny.

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.

Przewaga informacyjna to stopień dominacji, który daje własnym wojskom zdolność do gromadzenia, kontroli, wykorzystania i obrony informacji bez efektywnego przeciwdziałania. Ta przewaga jest podstawową zdolnością sił powietrznych, na której opierają się pozostałe zdolności tych sił. W żadnej innej dziedzinie nie ma tak wielkiego postępu technicznego, jak w obszarze informacji i systemów informacyjnych. Chociaż przewaga informacyjna nie jest tylko sprawą sił powietrznych, strategiczna perspektywa i globalne doświadczenie uzyskane z działania w przestrzeni, czyni lotników wyjątkowo przygotowanych do zdobywania wykorzystania przewagi informacyjnej. Wykorzystanie to osiągane jest w wyniku dynamicznych działań infor-

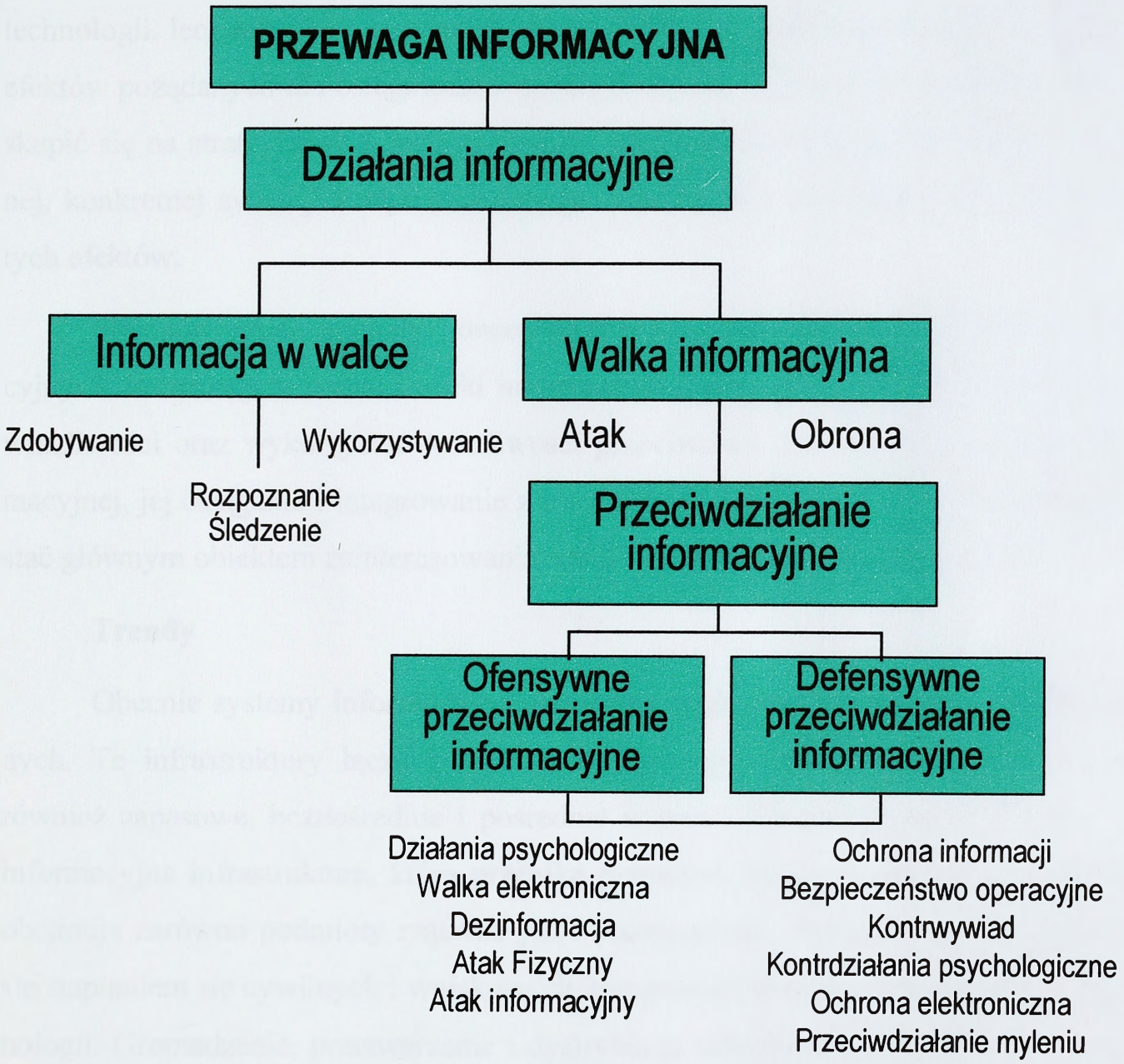
macyjnych (IO-Information Operations) oraz realizowania dwóch głównych aspektów informacji: informacji w walce (IIW- Information-in-warfare) i walki informacyjnej (IW-information warfare).

Działania informacyjne obejmują przedsięwzięcia podejmowane dla zdobycia, wykorzystania, obrony lub ataku na informację lub systemy informacyjne i łączą zarówno aspekt informacji w walce jak i walkę informacyjną. Działania te prowadzone są przez wszystkie fazy operacji i w całym zakresie działań militarnych.

Aspekt informacji w walce to rozległe zdolności sił powietrznych do zabezpieczenia globalnej świadomości w całym zakresie działań militarnych, wynikające z dysponowania zintegrowanymi środkami rozpoznania, śledzenia i rozpoznania pola walki oraz działalności w zakresie gromadzenia i dystrybucji informacji, a także z posiadanych możliwości w zakresie globalnej nawigacji i określania pozycji, rozpoznawania pogody i zabezpieczania łączności.

Walka informacyjna to działania informacyjne prowadzone dla obrony informacji i systemów informacyjnych sił powietrznych lub prowadzone dla atakowania i wywarcia wpływu na informacje lub systemy informacyjne przeciwnika. Ta walka jest prowadzona głównie w czasie kryzysu lub konfliktu. Jednakowoż defensywny komponent tej walki, podobnie jak obrona powietrzna, jest prowadzony w całym spektrum działań militarnych od pokoju do wojny.

Walka informacyjna zawiera się w funkcjach przeciwdziałania informacyjnego (CI - counterinformation), które dekomponuje się na ofensywne (OCI - offensive counterinformation) i defensywne (DCI - defensive counterinformation) przeciwdziałanie informacyjne (rys. 5.)



Rys ..5.. Koncepcja sił powietrznych odnośnie działań informacyjnych.

Siły Powietrzne rozwinęły taktyki, techniki oraz procedury ofensywnego i defensywnego przeciwdziałania informacyjnego dla osiągnięcia przewagi nad przeciwnikami. Walka informacyjna oferuje możliwości bezpośredniego osiągania narodowych celów militarnych. W konsekwencji walka informacyjna jest nie tylko sprawą technologii, lecz także dotyczy integracji środków sfery informacyjnej dla osiągnięcia efektów pożądanych dla osiągnięcia wspólnych celów. Odpowiednio, dowódcy muszą skupić się na strategicznych, operacyjnych i taktycznych efektach, pożądanych w danej, konkretnej sytuacji i użyć właściwego zestawu sił i możliwości dla osiągnięcia tych efektów.

Siły powietrzne przyjęły koncepcję przewagi informacyjnej, działań informacyjnych, informacji w walce i walki informacyjnej, aby ograniczyć swoje potencjalne wrażliwości oraz wykorzystać wrażliwości przeciwnika. Dążenie do przewagi informacyjnej, jej osiąganie i integrowanie z innymi aspektami potęgi powietrznej musi się stać głównym obiektem zainteresowania sztuki operacyjnej sił powietrznych.

Trendy

Obecnie systemy informacyjne są częścią większych infrastruktur informacyjnych. Te infrastruktury łączą poszczególne systemy informacyjne poprzez liczne, również zapasowe, bezpośrednie i pośrednie w tym i kosmiczne łącza. Rozrasta się informacyjna infrastruktura, która przenika przemysł, media, środowisko militarne i obejmuje zarówno podmioty rządowe jak i pozarządowe. Struktura ta charakteryzuje się stapianiem się cywilnych i wojskowych komponentów sieci informacyjnych i technologii. Gromadzenie, przetwarzanie i dystrybucja informacji poprzez ludzi i organizacje stanowi ważną ludzką działalność, która jest integralną częścią infrastruktury informacyjnej. Co równie ważne systemy broni, zdolności i działania są obecnie nierozerwalnie połączone z większą infrastrukturą informacyjną. Działania sił powietrznych były zawsze zależne od tego co dziś nazywane jest obronną infrastrukturą informacyjną (DII-Defense Information Infrastructure). Infrastruktura ta stanowi zbiór wspólnych lub wzajemnie połączonych systemów informacyjnych, które służą lokalnym, narodowym lub globalnym potrzebom informacyjnym resortu obrony.





Rys. 6. Narodowa infrastruktura informacyjna łączy organizacje z prędkością światła.

Ze względu na wzrastającą zależność od systemów komercyjnych obronna infrastruktura informacyjna jest częścią i musi polegać na narodowej strukturze informacyjnej (NII-National Information Infrastructure). Struktura ta jest jeszcze większym zbiorem amerykańskich rządowych i komercyjnych systemów i sieci. Narodowa struktura informacyjna jest powiązana z globalną infrastrukturą informacyjną (GII-Global Information Infrastructure). Ta struktura zaś składa się z rozległych systemów sieci obejmujących cały glob. W rzeczywistości rozpowszechnianie wiadomości, komunikaty dyplomatyczne i wojskowe rozkazy dowodzenia, wszystkie uzależnione są od globalnej infrastruktury informacyjnej.

Zwiększona zdolność sił powietrznych do dostępu, przetwarzania i przechowywania informacji połączona z olbrzymim wzrostem zależności tych sił od systemów i infrastruktury informacyjnej doprowadziły siły powietrzne do ponownego zbadania i przedefiniowania sposobu w jaki siły te integrują działalność informacyjną ze swoimi podstawowymi funkcjami. Zatem jak stwierdzono w AFDD 1 (Podstawowej doktrynie sił powietrznych) dominacja w sferze informacyjnej jest obecnie równie ważna, jak w przeszłości ważna była kontrola przestrzeni powietrznej i kosmicznej czy okupowanie terenu. Dominacja ta jest widziana jest jako nierozerwalny i synergiczny komponent potęgi powietrznej.

Gwałtowny rozwój technologii informacyjnej (komputerów, procesorów i narzędzi wspomagania procesów decyzyjnych) w zasadniczy sposób zmienił zarówno systemy wojskowe sił powietrznych jak i koncepcje ich działań. Obecnie trudno znaleźć jakiś główny system uzbrojenia sił powietrznych czy inny system, który nie uzależniony byłby od zaawansowanej elektroniki i skrajnie precyzyjnej informacji – i zależność ta ciągle wzrasta. W świecie, gdzie procesory komputerowe podwajają swoją prędkość co 18 miesięcy i są natychmiast dostępne na rynku, siły powietrzne muszą być zdolne do adaptacji zarówno swoich technologii jak i koncepcji działań jeszcze szybciej niż czynią to dzisiaj. Rzeczywiście, elastyczność jest jeszcze bardziej znaczącym czynnikiem dla potęgi powietrznej w wieku informacyjnym.

Efektem tego wzrastającego powiązania od zależnych od informacji systemów broni jest wyniesienie rozpoznania, śledzenia i rozpoznania pola walki (ISR) do rangi

podstawy sukcesu wszelkich działań militarnych. Zasoby ISR dążą do uzyskania doskonałego rozumienia informacji przeciwnika oraz jego słabych i mocnych stron dla przeprowadzenia analizy wrażliwości informacyjnej. W niektórych przypadkach trudno jest określić co jest zdolnością rozpoznania, śledzenia i rozpoznania pola walki (ISR) w porównaniu do zdolności walki informacyjnej (IW), faktycznie czasami platforma czy system może być jednym i drugim. Zatem rozpoznanie, śledzenie i rozpoznanie pola walki są równie ważną częścią obronnej infrastruktury informacyjnej i muszą być chronione ponieważ dostarczają kluczowych informacji pozwalających na ochronne, odwetowe i ofensywne działania walki informacyjnej.

Zagrożenie

Zagrożenia, przed którymi stają obecnie Stany Zjednoczone nie mogą być dłużej określane geograficznymi czy politycznymi granicami, jak w czasie zimnej wojny. Z postępem technicznym zdolność społeczeństwa do wymiany informacji i możliwości oddziaływania przeciwnika na informację wzrastają i w niektórych przypadkach mogą osłabić bezpieczeństwo systemów informacyjnych. Tak jak Stany Zjednoczone planują stosowanie działań informacyjnych przeciwko swoim przeciwnikom, tak same mogą oczekiwać, że przeciwnik zrobi to samo. Liczne kraje odkryły korzyści płynące z działań informacyjnych. Stosują działania psychologiczne, walkę elektroniczną, dezinformację wojskową i mylenie a obecnie coraz powszechniej zbierają dostępne dane wywiadowcze poprzez Internet, tworzą złośliwe kody i komórki hakerskie. Terroryści, kryminaliści i hakerzy stają się coraz większym zagrożeniem gdy odkrywają korzyści płynące z wykorzystania środowiska elektronicznego dla osiągania swych celów. Ponieważ socjoekonomiczna i wojskowa infrastruktura jest wysoce zależna od swobodnego przepływu informacji, dobrze poinformowany przeciwnik posiada zdolność do infiltracji i ataku systemów informacyjnych. Pięta Achillesowa Stanów Zjednoczonych może być wielkim czynnikiem wyrównawczym dla słabszego przeciwnika. Działania informacyjne muszą minimalizować zdolność przeciwnika do wpływania na amerykańską informację wojskową, jednocześnie pozwalając USA przeprowadzić działania informacyjne.

Każde z zagrożeń wymienionych na rys 7 przedstawia ryzyko właściwe dla broni i systemów wsparcia, które zależne są od systemów informacyjnych. Ogólne zdolności wyrażają czy zagrożenia są strukturalne czy niestrukturalne. Zagrożenie strukturalne jest zorganizowane, wsparte finansowo ma jasne cele oraz posiada środki do infiltracji i pozyskiwania informacji. Zagrożenie niestrukturalne to te z ograniczoną strukturą wsparcia i ograniczonym motywem. Zagrożenia strukturalne i niestrukturalne mogą być przeprowadzone przez własnych mieszkańców, częściowo pozyskanych przez przeciwnika, częściowo realizujących własne cele. Potencjalne zagrożenia wewnętrzne stają się jednym z największych obszarów troski.

Zagrożenia walki informacyjnej			
Narażanie na szkody	**Dezinformacja/degradacja**	**Uniemożliwienia/ utraty**	**Niszczenie**
Złośliwe kody	Złośliwe kody	Złośliwe kody	Złośliwe kody
Włamania do systemów	Włamania do systemów	Włamania do systemów	Bomby
Działania psychologiczne	Dezinformacja wojskowa	Lasery	Bronie
Rozpoznanie	Zniekształcanie	Atak fizyczny	
Transfer technologii	Imitacja	Nuklearny i konwencjonalny EMP	
Wirusy komputerowe		Wprowadzanie wirusów	
		Przeładowania systemu	
		Zakłócanie radiowe	

Rys. 7. Zagrożenia walki informacyjnej.

Zagrożenia walki informacyjnej mieszczą się w czterech kategoriach: narażania na szkody, dezinformacji/degradacji, uniemożliwienia/utraty, fizycznego zniszczenia. Każde niesie ze sobą ryzyko, zarówno dla samodzielnych jak i włączonych do sieci broni oraz systemów wsparcia, które uzależnione są od systemów informacyjnych.

Działania w ramach tych zagrożeń mogą być stosowane zarówno przez elementy zorganizowane takie jak państwa jak i niestrukturalne, takie jak nieodpowiedzialni hakerzy komputerowi.

Podsumowanie

W dającej się przewidzieć przyszłości dowódcy i przywódcy skupią się na następujących sprawach jako głównych zagadnieniach wysiłku sił powietrznych w działaniach informacyjnych.

- Dwa filary działań informacyjnych, informacja w walce (IIW- Information-in-warfare) i walka informacyjna (IW-information warfare) – mimo, że istnieją niezależnie to są nierozerwalnie połączone i muszą być integrowane w ich stosowaniu dla osiągnięcia przewagi informacyjnej.
- Nawet bardziej niż inne działania powietrzne i kosmiczne, działania przeciwinformacyjne muszą być prowadzone jednocześnie i równolegle. Niektóre działania walki informacyjnej mogą występować na przemian zarówno w ofensywnych jak i w defensywnych działaniach przeciwinformacyjnych w ciągłym cyklu, zmieniając się dosłownie z prędkością światła.
- Siły powietrzne prowadzą walkę informacyjną na poziomie strategicznym, operacyjnym i taktycznym, używając kombinacji różnych zdolności w połączeniu z powietrznymi siłami ekspedycyjnymi.
- Siły powietrzne, gdy otrzymają takie zadanie, będą energicznie wspierać narodową, strategiczną walkę informacyjną jednakże w większości planowaną poza siłami zbrojnymi.
- Defensywne działania przeciwinformacyjne stanowią główny priorytet sił powietrznych w obszarze walki informacyjnej. Dowódcy są odpowiedzialni za kształt i prowadzenie defensywnych działań przeciwinformacyjnych w obrębie ich dowództw.
- Wysiłek walki informacyjnej sił powietrznych skupia się na wprowadzeniu zdolności do wojny informacyjnej dowództw walczących komponentów dla wsparcia dowódców połączonych.

- Działania i przedsięwzięcia walki informacyjnej musza być włączane w proces planowania i wykonania kampanii. Mogą być plany kampanii składające się głównie z działań walki informacyjnej, jednakże nie powinno być samodzielnych kampanii walki informacyjnej.

Przeciwdziałanie informacyjne (Counterinformation)

Walka informacyjna jest szeroko zdefiniowaną koncepcją zawierającą i integrującą wiele rodzajów aktywności i możliwości rozciągających się przez całe widmo konfliktu. Możliwości walki informacyjnej mogą wyjść naprzeciw celom stosowania siły jak i wsparcia. Tak zdefiniowana walka informacyjna wymaga obszernego planowania, zawiera wiele klasycznych funkcji kontrolnych, ta walka obejmuje niezależne uderzenia ofensywne i wymaga także integracji w pełno wymiarową osłonę. Walka ta może być przeprowadzona dla osiągania niemalże wszystkich celów i funkcji, jako wsparcie innych rodzajów sił zbrojnych na danym teatrze, lub jako wsparcie zadań narodowych.

Przeciwdziałanie informacyjne jest funkcją, która ustanawia przewagę informacyjną przez odpowiednie neutralizowanie działalności informacyjnej przeciwnika lub wpływanie na nią w potrzebnej skali. Przeciwdziałanie informacyjne skupia się na zwalczaniu możliwości przeciwnika w zakresie uzyskiwania korzyści informacyjnych. Przeciwdziałanie informacyjne realizowane jest przez wzbranianie dostępu do informacji oraz jej degradację, przerywanie, niszczenie, mylenie i wykorzystanie. Wszystkie te przedsięwzięcia mogą zmylić, opóźnić, zatrzymać akcje ofensywne przeciwnika i zredukować jego czas na podjęcie najważniejszych przedsięwzięć obronnych.

Przeciwdziałanie informacyjne jest prowadzone w całym spektrum konfliktów w niezbędnym i zgodnym z polityką Stanów Zjednoczonych i wymaganiami prawnymi, zakresie. Dlatego też przeciwdziałanie informacyjne może odnosić się do wsparcia działań pozawojennych i obrony sił powietrznych w czasie pokoju, lub sojuszniczego działania i wsparcia. Połączone z walką o panowanie w powietrzu i kosmosie przeciwdziałanie informacyjne tworzy środowisko, w którym własne wojska dysponują

swobodą działania, podczas gdy działalność informacyjna przeciwnika jest w zależności od potrzeb, wzbroniona, neutralizowana lub zniekształcana.

Przeciwdziałanie informacyjne, podobnie jak walka o panowanie w powietrzu i kosmosie, składa się z aspektów ofensywnych i defensywnych.

Przeciwdziałanie informacyjne	
Ofensywne przeciwdziałanie informacyjne	**Defensywne przeciwdziałanie informacyjne**
Działania psychologiczne **Walka elektroniczna** • **Atak elektroniczny** • **Elektroniczna ochrona** • **Wsparcie elektroniczne** **Mylenie** **Atak fizyczny** **Atak informacyjny**	**Ochrona informacji** **Bezpieczeństwo operacyjne** **Przeciwdziałanie myleniu** **Kontrwywiad** **Kontrdziałania psychologiczne** **Ochrona elektroniczna**

Rys. 8. Najważniejsze formy działań przeciwdziałania informacyjnego.

Ofensywne przeciwdziałanie informacyjne (OCI) zawiera akcje podejmowane w celu kontroli środowiska informacyjnego. Działania ofensywnego przeciwdziałania informacyjnego są prowadzone aby ograniczać, degradować, przerywać lub niszczyć możliwości informacyjne przeciwnika. Działania te są zależne od znajomości możliwości informacyjnych przeciwnika.

Defensywne przeciwdziałanie informacyjne (DCI) zawiera działania, które chronią informację, systemy informacyjne i działania informacyjne przed potencjal-

nym przeciwnikiem. Defensywne przeciwdziałanie informacyjne zawiera takie formy jak bezpieczeństwo operacyjne (OPSEC), ochronę informacji i kontrwywiad.

Ofensywne i defensywne przeciwdziałanie informacyjne w swojej konstrukcji są analogiczne do tradycyjnej walki o panowanie w powietrzu, dekomponującej się na ofensywną i defensywną czyli OCA i DCA. Mimo że analogia nie jest doskonała, istnieją znaczne analogie i lotnicy mogą stosować wiele zasad ofensywnej walki o przewagę w powietrzu w odniesieniu do ofensywnego przeciwdziałania informacyjnego oraz defensywnej walki o przewagę w powietrzu w stosunku do defensywnego przeciwdziałania informacyjnego. Tak jak w ofensywnej walce o panowanie w powietrzu (OCA) i defensywnej walce o panowanie w powietrzu (DCA), dowódcy muszą raczej koncentrować się na wymaganych efektach raczej niż na rozróżnianiu rodzaju tego działania. Dzieląca te rodzaje linia może być bardzo cienka i przejścia jednej formy w drugą prawie natychmiastowe.

Działania ofensywnego przeciwdziałania informacyjnego

Działania ofensywnego przeciwdziałania informacyjnego w znacznym stopniu uzależnione są od zrozumienia zdolności informacyjnych przeciwnika, jego uwarunkowań i słabości. Działania ofensywnego przeciwdziałania informacyjnego, które mogą wpływać na zdolności przeciwnika i wykorzystywać jego słabości zawierają: Działania psychologiczne (PSYOP), walkę elektroniczną (EW), mylenie oraz informacyjny i fizyczny atak.

Działania psychologiczne (PSYOPS)

Działania psychologiczne (PSYOPS) są przeznaczone do przekazywania wybranych informacji i sugestii obcym przywódcom i społecznościom, aby wpływać na ich emocje, motywy, rozumowanie i zachowanie na korzyść własnych celów.

Działania psychologiczne mają zastosowanie na szczeblu strategicznym, operacyjnym i taktycznym. 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, zespoły „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.

Prawdziwym celem wojny jest umysł wrogiego dowódcy, nie ciała jego 17 żołnierzy.

Captain Sir Basil Liddell Hart
Myśli o wojnie, 1944

Na szczeblu strategicznym, PSYOP może przybierać formy: politycznego lub dyplomatycznego stanowiska, oświadczeń lub komunikatów. Na szczeblu operacyjnym i taktycznym 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. Stałe ataki działań psychologicznych mogą mieć podwójny efekt, przyspieszając degradację morale i dalsze zachęcanie do dezercji.

Walka elektroniczna

Walka elektroniczna jest akcją militarną zawierającą użycie elektromagnetycznej oraz kierowanej energii do kontroli spektrum elektromagnetycznego lub do ataku przeciwnika. Działanie to jest nie tylko ograniczone do częstotliwości radiowych, ale odnosi się też do widma optycznego i podczerwonego. Walka elektroniczna (EW)

wspomaga siły powietrzne i kosmiczne w uzyskaniu dostępu i operowaniu bez istotnego wpływu ze strony systemów przeciwnika. Podczas operacji „Desert Storm", efektywne grupy lotnicze, zawierające środki osłony działające z dystansu i realizujące zakłócanie oraz ataki antyradiacyjne, przyczyniły się do ekstremalnie niskich strat własnych.

Trzy główne części walki elektronicznej to: atak elektroniczny, ochrona elektroniczna i elektroniczne wsparcie. Wszystkie trzy wspierają działania kosmiczne i powietrzne. Kontrola widma jest osiągana przez ochronę własnych systemów i zwalczanie systemów przeciwnika. Atak elektroniczny ogranicza możliwości użycia przez wrogiego dowódcę spektrum elektronicznego. Ochrona elektroniczna (defensywny aspekt EW) zwiększa możliwości użycia widma przez własne siły. Wsparcie elektroniczne pozwala dowódcy na dokładne określenie sytuacji w rejonie operacyjnym. Atak elektroniczny i wsparcie powinny być zintegrowane z ochroną elektroniczną, by system był efektywny. Rozsądny dowódca, zwykle szczebla komponentu powietrznego (JFACC) musi zapewnić maksimum koordynacji i dekonfliktacji pomiędzy walką elektroniczną, rozpoznaniem i śledzeniem oraz działaniami w zakresie zabezpieczenia łączności.

Walka elektroniczna jest mnożnikiem siły. Kontrola elektromagnetycznego spektrum może mieć główny wpływ na sukces w całym spektrum działań militarnych. Właściwe zastosowanie walki elektronicznej zwiększa zdolności amerykańskich dowódców operacyjnych w zakresie osiągania celu. Gdy działania walki elektronicznej są zintegrowane z operacjami militarnymi, a nie są jedynie dołączone, osiąga się synergię, minimalizowane są straty, a efektywność działań jest zwiększona.

Dezinformacja wojskowa (mylenie)

Wojna jest oparta na myleniu.

Sun Tzu
Sztuka wojny, c. 500 BC

Dezinformacja wojskowa wprowadza przeciwnika w błąd, powodując, że działa on zgodnie z planami organizatora dezinformacji. Działania dezinformacji wojskowej rozciągają się na wszystkie szczeble wojny i zawierają komponenty ofensywne i defensywne. Dezinformacja wojskowa może odwrócić uwagę od, lub zapewnić osłonę dla operacji wojskowych myląc i rozpraszając siły przeciwnika. Kontrdezinformacja zapewnia własnym dowódcom przygotowanie na akcje przeciwnika, co pozwala im uniknąć efektów tego działania. Dezinformacja wymaga głębokiej znajomości kultury, polityki, doktryny, oraz procesu decyzyjnego przeciwnika, które to wiadomości mogą być wykorzystane przez planistów.

Klasycznym przykładem dezinformacji wojskowej jest operacja drugiej wojny światowej „Fortittude North", kiedy alianci, zamiast Normandii, ciężko bombardowali Pas de Calais, powodując przekonanie Niemców o inwazji na Pas de Calais. 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, aby zagrozić przeciwnikowi 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 położona na to jak amerykańscy 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 operacje 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 dowód-

ców i ich sztaby. Działania dezinformacji wojskowej są potężnym narzędziem w operacjach wojskowych. Siły i środki muszą być podporządkowane potrzebom działań dezinformacyjnych aby uczynić je wiarygodnymi i wartymi krótkoterminowych kosztów.

Atak fizyczny

Jako element zintegrowanego wysiłku przeciwdziałania informacyjnego, atak ten odnosi się do użycia broni fizycznie niszczącej, przeciw wyznaczonym obiektom. Celem jest wpływanie na informację lub system informacyjny przeciwnika za pomocą broni fizycznej. Atak fizyczny siłą destrukcyjną przerywa lub niszczy system informacyjny przeciwnika.

Połączenie precyzyjnej amunicji z zaawansowaną platformą, np. „Cruise" 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.

Atak informacyjny

Atak informacyjny odnosi się do tych form aktywności, które mają na celu manipulowanie lub zniszczenie informacji lub systemu informacyjnego bez zmiany fizycznego stanu systemu przeciwnika, w którym dokonywany jest ten atak.

Penetracja systemu informacyjnego przeciwnika ma wielką wartość w walce, ponieważ oferuje zdolność do obezwładnienia przeciwnika bez narażania własnych sił, przy redukcji strat towarzyszących i unikaniu konieczności zadawania dużych strat przeciwnikowi. Dzięki użyciu nowych możliwości i narzędzi, konwencjonalne wyloty bojowe mogą być wykorzystane na inne cele. Manipulacja bazami danych lub parametrami systemów może powodować błędne informacje, które będą wpływały na pro-

ces decyzyjny lub mogą niszczyć zaufanie przeciwnika do jego systemu informacyjnego. Efektywny atak informacyjny może zmusić przeciwnika do używania mniejszej ilości środków technicznych ze względu na nasze włamanie się do jego systemu. Przykładem ataku informacyjnego może być spowodowanie dezinformacji w obiegu danych radarowych, aby doprowadzić do niecelnego ognia pocisków przeciwlotniczych. Atak informacyjny może być postrzegany jako oddziaływanie na „obserwowanie" i „orientowanie" – dwa komponenty zamkniętego cyklu OODA (obserwowanie – orientowanie – decydowanie – działanie), gdyż wówczas zdolność przeciwnika do polegania na „obserwacji" jest obniżona.

Działania defensywnego przeciwdziałania informacyjnego

> ***Mamy dowód, że duża liczba państw na świecie rozwija doktrynę, strategie i narzędzia do prowadzenia ataków informacyjnych na komputery wojskowe.***
>
> *John M. Deutch*
> *Dyrektor, Centralnej agencji Wywiadowczej*
> *The Washington Post, 26 June 1996*

Działania defensywnego przeciwdziałania informacyjnego (DCI) to te akcje, które chronią informacje i systemy informacyjne sił powietrznych przed przeciwnikiem.

Siły powietrzne prowadzą defensywne przeciwdziałanie informacyjnego aby zapewnić potrzebną obronę dla możliwości przeprowadzania własnych działań. Aktualne wypadki włamań do systemów powodowanych przez nastolatków począwszy, kończąc na umyślnym zakłócaniu systemów niezbędnych do tworzenia obrazu sytuacji powietrznej dla połączonych komponentów sił powietrznych demonstruje, jak ważna jest obrona informacji w działaniach militarnych. Ze względu na unikalne zależności Stanów Zjednoczonych od systemów informacyjnych, działania defensywnego prze-

ciwdziałania informacyjnego są priorytetem sił powietrznych, jeśli chodzi o walkę informacyjną. W związku z tym dowódcy są odpowiedzialni za działania defensywnego przeciwdziałania informacyjnego w swoich jednostkach. Celem tych działań jest zapewnienie potrzebnej obrony informacji i systemów informacyjnych, które wspierają działania militarne. Jeśli działania defensywnego przeciwdziałania informacyjnego są połączone z ofensywnym przeciwdziałaniem informacyjnym, rezultatem będzie zwiększona możliwość zastosowania walki informacyjnej dla uzyskania żądanych militarnych i politycznych celów. Formy, które mogą być zastosowane, aby przeprowadzić działania defensywnego przeciwdziałania informacyjnego to: bezpieczeństwo operacyjne (OPSEC), ochrona informacji, kontrdezinformacja, kontrwywiad, kontrdziałania psychologiczne i ochrona elektroniczna. Te różne formy wspólnie się uzupełniają, (tzn. każda z nich może być użyta jako przeciwśrodek w celu wsparcia innej) i mogą wspierać działania ofensywne. Dodatkowo, aby uzyskać lepsze efekty formy te muszą być stosowane wielowarstwowo. Mimo to, jeśli są używane bez koordynacji i integracji może zaistnieć między nimi, jak również z działaniami ofensywnymi, konflikt. Na przykład przedsięwzięcia ochrony informacji mogą dążyć do zminimalizowania skutków włamania do systemu tak szybko jak to możliwe, podczas gdy kontrwywiad może chcieć zezwolić na dalszy dostęp, aby zidentyfikować i wykorzystać przeciwnika.

Bezpieczeństwo operacyjne (OPSEC) i ochrona informacji

Siły powietrzne stosują przedsięwzięcia bezpieczeństwa by chronić i bronić informacje i systemy informacyjne. Przedsięwzięcia te odnoszą się do bezpieczeństwa operacyjnego (OPSEC) i ochrony informacji. Bezpieczeństwo informacyjne (OPSEC) jest procesem identyfikacji najważniejszych informacji i analizowanie własnych akcji, które towarzyszą działaniom militarnym i innym działaniom dla:

- identyfikowania tych akcji, które mogą być obserwowane przez systemy wywiadowcze przeciwnika;

- określania wskaźników, które obce systemy rozpoznania mogą zebrać, zinterpretować i złożyć w całość w celu uzyskania najważniejszych informacji we właściwym czasie;
- wybierania i zastosowania środków, które wyeliminują lub zredukują do akceptowalnego poziomu słabości własnych działań wobec przeciwnika.

Bezpieczeństwo operacyjne to proces. Jest on zbiorem specyficznych zasad i instrukcji, które mogą być zastosowane do działań lub aktywności w celu zablokowania dostępu przeciwnikowi. Bezpieczeństwo operacyjne jest stosowane we wszystkich działaniach wojskowych na wszystkich szczeblach dowodzenia.

Dowódca sił powietrznych powinien wskazać kierunki planowania bezpieczeństwa operacyjnego dla swojego sztabu na początku procesu planistycznego, kiedy określa swój zamiar i następnie dla podległych dowódców w łańcuchu dowodzenia. Poprzez utrzymanie łączności ze wspierającymi dowódcami i koordynowanie planowania bezpieczeństwa operacji dowódca sił powietrznych zapewnia jedność wysiłku w uzyskiwaniu i utrzymywaniu potrzebnego stopnia utajnienia.

Ochrona informacji to przedsięwzięcia podejmowane dla osłony i obrony informacji i systemów informacyjnych dla zapewnienie ich dostępności, integralności, autentyczności, tajności i zdolności do identyfikowania źródła informacji i danych.

Ochrona informacji zawiera także odtworzenie systemów informacyjnych przez utrzymywanie zdolności do osłony, wykrywania zagrożeń i reagowania na nie. Ochrona informacji jest stosowana we wszystkich działaniach militarnych na wszystkich szczeblach. Dowódca sił powietrznych powinien wskazać kierunki planowania dla swojego sztabu, określając swój zamiar oraz dla podległych dowódców w hierarchii dowodzenia. Proces ochrony informacji jest stosowany poprzez działania wykorzystujące nowoczesne technologie.

Ochrona informacji zawiera ochronę systemów informacyjnych przed niepożądanym dostępem do informacji lub jej niszczeniem. Obejmuje to ochronę komputerów, łączności i przedsięwzięcia potrzebne do wykrycia, udokumentowania i przeciwdziałania takim zagrożeniom.

♦ Ochrona komputerów zawiera przedsięwzięcia podejmowane dla ochrony tajności integralności i dostępności informacji przetwarzanej i przechowywanej w komputerze. Składają się na to odpowiednia polityka, procedury, hardwarowe i softwarowe narzędzia potrzebne do ochrony systemów komputerowych i informacji.

♦ Bezpieczeństwo łączności zawiera przedsięwzięcia mające na celu zlikwidowanie dostępu nieautoryzowanych osób do informacji zapewniając jednocześnie autentyczność komunikacji. Ochrona komunikacji zawiera krypto ochronę, ochronę transmisji, emisji i fizyczną ochronę urządzeń komunikacyjnych i informacji.

Kontrdezinformacja

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

Kontrwywiad

Kontrwywiad ochrania działania, systemy, technologię, urządzenia, personel i inne zasoby przed nielegalnymi tajnymi operacjami obcych służb, grup terrorystycznych i innych. Kontrwywiad ocenia możliwe do eksploatacji potencjalne źródła informacji i ich słabości. Ważność kontrwywiadu może być zilustrowana przez przypadek Johny Walkera okresu zimnej wojny. Od lat 60- tych do 80- tych Stany Zjednoczone podejrzewały, że Sowieci znają przebieg przyszłych amerykańskich ćwiczeń morskich. Ujawniło się to w pełni dopiero po wykryciu szajki szpiegowskiej.

Kontrdziałania psychologiczne

Żadne przedsięwzięcie nie jest bardziej skazane na sukces niż to, które zostało ukryte przed wrogiem do momentu wykonania.

Niccolo Machiavelli
The Art. of War

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

Ochrona elektroniczna

Walka elektroniczna jest akcją militarną zawierającą użycie elektromagnetycznej oraz kierowanej energii do manipulacji spektrum elektromagnetycznym lub do ataku przeciwnika. Po stronie defensywnej, ochrona elektroniczna gwarantuje użycie spektrum elektromagnetycznego przez własne siły. Ochrona elektroniczna jest ważna częścią defensywnego przeciwdziałania informacyjnego i musi być skoordynowana i zintegrowana z możliwościami ofensywnego działania oraz z innymi działaniami.

Funkcje Wspierające Działania Informacyjne

Krytyczne funkcje takie jak rozpoznanie i śledzenie, precyzyjna nawigacja i ustalanie położenia, pogoda, wzmacniają efekty użycia przestrzeni powietrznej i

działań informacyjnych. Razem te funkcje dostarczają dowódcom zdolności obserwowania przestrzeni powietrznej i analizy zdarzeń. Zasoby takie jak AWACS; JSTARS (Joint Surveillance Target Attak Radar System); bezzałogowe statki powietrzne; samoloty rozpoznawcze takie jak U-2 i RC-135; platformy meteorologiczne takie jak WC-130 i przestrzenny system wspomagania operacji, daje dowódcom wyższą zdolność oceniania sytuacji i podjęcia stosownego działania.

Środowisko kosmiczne i systemy działające w przestrzeni kosmicznej mają bardzo ważne znaczenie dla sił powietrznych i ich zdolności angażowania się w skali globalnej. Każda z podstawowych zdolności sił powietrznych opiera się na atrybutach systemów kosmicznych w tym szczególnie mocno odnosi się to do przewagi informacyjnej. Wynika to głównie z rosnących wymagań w zakresie nawigacji, pogody, dowodzenia i kontroli, śledzenia i rozpoznania i innych istotnych możliwości. Potęga powietrzna jest niezrównana w zdolnościach i swoich atrybutach systemów powietrznych, a szczególnie przez bycie zdolnym do odpowiedzi niemalże w czasie realnym z dużą szybkością ruchu i siły ognia, zbliżoną do czasu rzeczywistego co jest możliwe do uzyskania dzięki systemom operującym w kosmosie.

Do funkcji wspierających działania informacyjne należą:

Rozpoznanie

Dokładna i aktualna informacja jest ważnym elementem w osiąganiu celów kampanii, włączając w to zadania działań informacyjnych. Ponad utrzymywanie baz danych dla węzłowej analizy możliwości przeciwnika, rozpoznanie dostarcza wiedzy, która tworzy świadomość sytuacji co jest istotne dla kontroli i szacowania globalnych warunków. Działania rozpoznawcze zmierzają do uzyskania doskonałej znajomości silnych i słabych stron w systemie informacyjnym i infrastrukturze przeciwnika oraz dostarczają informacji o miejscach podatnych na atak. Rozpoznanie tworzy okazje dla systematycznej eksploatacji słabości przeciwnika i pomaga w izolowaniu sił od ich przywództwa. Przetwarzanie danych, wspomagane przez technologiczny postęp w zdolnościach komputerów, może tworzyć natychmiastowe globalne wsparcie kryzysu. Gromadzenie i analiza informacji muszą być prowadzone stale, mając szczególnie na

uwadze możliwości i wymagania działań informacyjnych, podobnie jak tradycyjnie rozpoznanie w siłach powietrznych ogniskowało się na prowadzeniu wojny powietrznej. Ponadto, rozpoznawcze wsparcie działań informacyjnych wymaga gromadzenia i analizy informacji w tradycyjnych obszarach (takich jak ugrupowania bojowe i ostrzeżenia), jak również specjalistycznych szczegółów o telekomunikacji i infrastrukturze komputerowej przeciwnika - nie co systemy kraju posiadają, ale szczegóły jak one są instalowane, jak pracują i są używane. Ponadto, analitycy rozpoznania dążą do dokładnego ocenienia prawdopodobnych wariantów działań przeciwnika, włączając w to jego zdolności i zamiary prowadzenia walki informacyjnej. Ten poziom analizy w kilku przypadkach przewyższa aktualne możliwości i będzie wymagać rozwoju nowych technik i systemów gromadzenia informacji albo być może zmianę priorytetów w aktualnym gromadzeniu i zasobach analitycznych.

Śledzenie i rozpoznanie pola walki

Informacyjna preparacja pola bitwy dostarcza walczącym zrozumienia przeciwnika. Integralną częścią tego procesu są śledzenie i rozpoznanie pola walki, które dostarczają dowódcom w czasie rzeczywistym lub bliskim rzeczywistemu informacji o przeciwniku, jego rozmieszczeniu, dyspozycyjności, możliwościach oraz o jego zamiarach. Śledzenie i rozpoznanie pola walki dostarcza oznak i ostrzeżeń o sytuacji zagrożenia dla Stanów Zjednoczonych i ich sprzymierzeńców. Powietrzne, kosmiczne i naziemne systemy i zespoły prowadzą rozpoznanie ugrupowania bojowego sił przeciwnika, rozmieszczenia i ich możliwości. Na przykład: Specjalne Taktyczne Zespoły Sił Powietrznych (Air Force Special Tactics Teams) jako część specjalnego połączonego zespołu operacyjnego, może dostarczyć decydujących informacji w głębokim polu bitwy, przed i po działaniach bojowych. Zespoły te także pomagają w identyfikacji środków ciężkości przeciwnika. Kosmiczne systemy śledzenia i rozpoznania pola walki mają możliwości działania w skali globalnej. Zasoby sił powietrznych oferują dowódcom elastyczne zdolności kolekcji informacji w ramach wspierania procesu decyzyjnego. Śledzenie i rozpoznanie pola walki w praktyce są często prowadzone jed-

nocześnie przez te same zespoły lub platformy. Jednakże funkcje te są rozróżniane przez definicje:

śledzenie jest to ciągłe gromadzenie informacji z powietrza, przestrzeni kosmicznej i powierzchni ziemi; rozpoznanie pola walki jest prowadzone aby uzyskać informacje o zlokalizowanych i konkretnych obiektach w ograniczonym przedziale czasowym.

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

Precyzyjna nawigacja i określanie położenia

Precyzyjna nawigacja i określanie położenia mają polepszyć dokładność broni i dostarczenia platform w określony punkt, w którym broń staje się zdolna do rozróżnienia obiektów uderzeń. Wiele czynników przyczynia się do tego aby broń zwiększała swoje zdolności w zakresie dokładności. Czujniki nowoczesnych samolotów, systemy celowania i precyzyjnego kierowania uzbrojeniem pozwalają dokładniej lokalizować cele i prowadzić ogień. Przestrzenne wsparcie, rozpoznanie i wyposażenie w systemy precyzyjnej nawigacji pozwalają dostarczać uzbrojenie z dużą dokładnością.

Precyzyjna nawigacja i określanie położenia zaspokajają potrzeby powietrznych, kosmicznych i informacyjnych działań w zakresie zdolności atakowania celów we wrażliwych obszarach. Zdolność do zlokalizowania i zapewnienia celnego ognia wielce zmniejsza potrzebną liczbę samolotów oraz ilość misji potrzebnych dla zniszczenia celu.

Powietrzne oraz specjalne naziemne zespoły, a także siły kosmiczne wyposażone w sprzęt precyzyjnej nawigacji i określania położenia są w stanie atakować obiekty ruchome w obszarach wrażliwych. Użytkownicy globalnego systemu nawigacyjnego

mogą przetworzyć sygnały satelitarne i określać pozycję z dokładnością do 10 stóp, szybkość w granicach ułamka mili na godzinę i czas w granicach milionowej części sekundy.

O godz.4.00 16 stycznia 1991, śmigłowce MH-53 Paw Low sił specjalnych ze składu sił powietrznych, jedyne wówczas śmigłowce wyposażone w system GPS, rozpoczęły wojnę w zatoce przez naprowadzenie śmigłowców AH-64 Apache na irackie naziemne środki kontroli. W ten sposób „Apache" utworzyły dziury w Irackim systemie obrony powietrznej co umożliwiło siłom powietrznym atakowanie irackich obiektów.

Zabezpieczenie meteorologiczne

Zabezpieczenie meteorologiczne prowadzone przez siły powietrzne dostarcza aktualnej i dokładnej informacji o pogodzie, dla dowódców osiągających cele i rozwijających plany na strategicznych, operacyjnych i taktycznych poziomach wojny. Zabezpieczenie meteorologiczne to zbieranie, analiza i dostarczanie danych meteorologicznych oraz informacji o środowisku dla planowania misji i jej wykonania. Informacja środowiskowa jest integralną częścią procesu decyzyjnego, ma duży wpływ na użycie sił, planowanie i prowadzenie powietrznych, naziemnych, morskich i kosmicznych działań wspierających działania informacyjne. Informacja meteorologiczna ma wpływ na selekcję celów, tras, systemów broni i taktyki.

Działania informacyjne na teatrze działań wojennych

Przewaga informacyjna

Jednym z priorytetów dowódcy sił powietrznych i dowódcy komponentu powietrznego jest osiąganie przewagi informacyjnej nad przeciwnikiem poprzez kontrolowanie środowiska informacyjnego polepszając tym samym warunki sojuszniczego działania. Ten cel nie neguje potrzeby osiągania przewagi w powietrzu i w kosmosie, ale raczej sprzyja tym wysiłkom w tych obszarach i na odwrót. Celem przewagi informacyjnej jest utrzymanie lepszej orientacji sytuacyjnej i kontroli nad przeciwni-

kiem. Działania informacyjne mogą być środkiem do bezpośredniego osiągnięcia celów dowódcy lub mogą służyć jako mnożnik siły wzmacniający lub uzupełniający inne sposoby walki. Przewaga informacyjna jest osiągana poprzez integrowanie różnych przedsięwzięć dla zdobycia, eksploatacji, wzbraniania, degradowania, przerywania, mylenia oraz niszczenia informacji przeciwnika i jego funkcji informacyjnych przy jednoczesnej ochronie własnej informacji. Wysiłek, aby osiągnąć przewagę informacyjną zależy od trzech zasadniczych komponentów: podejścia bazującego na efektach, zintegrowanego planowania kontrinformacyjnego i organizacji walki informacyjnej.

Podejście bazujące na efektach

Fundamentem sukcesu sił powietrznych w przyszłym wieku jest ich zdolność do ogniskowania pożądanych skutków w osiąganiu celów kampanii, czy to na poziomie strategicznym, operacyjnym czy taktycznym. To ukazuje jak ważny dla działań informacyjnych, jak dla żadnych innych, jest potencjał powietrzny i kosmiczny. Generalnie, zamiar wykonania konkretnego zadania lub akcji determinuje raczej jego stopień wykonalności niż określanie do użycie szczególnej broni czy platform. Planiści powinni jasno definiować pożądane skutki, potem precyzować optymalne możliwości dla osiągnięcia tego skutku.

Efekty strategiczne

Działania informacyjne, szczególnie niektóre akcje ofensywnego przeciwdziałania informacyjnego (OCI) strategicznego szczebla wojny, będą kierowane przez władze narodowe i planowane we współpracy z innymi agencjami lub organizacjami spoza Departamentu Obrony. Takie działania powinny być koordynowane wśród jednostek wsparcia sił powietrznych, dowódcą zespołu działań informacyjnych i innych wspierających elementów tak żeby zapewnić jedność wysiłku i zapobiegać konfliktowi z możliwymi działaniami poziomu operacyjnego. Jakkolwiek, z powodu wrażliwości takich operacji, nie zawsze mogą być one koordynowane z innymi jednostkami, ale raczej dekonfliktowane na możliwie najwyższym poziomie, żeby zapewnić pełny suk-

ces operacji. Niemniej, działania informacyjne mogą być także prowadzone na strategicznym poziomie wojny jako część działań teatru działań wojennych. Szczególnymi efektami jakie działaniami informacyjnymi mogą być osiągnięte są:

* Wpływ na sojusznicze i nieprzyjacielskie zachowania prowadzące ku osiągnięciu celów narodowych przez promocję trwałych więzi i partnerstwa z sojuszniczymi narodami.
* Przerwanie sprzeciwu wrogiego przywódcy przeciwko celom narodowym przez wpływ na siłę woli, zdecydowanie lub zaufanie. Tworzenie atmosfery braku zaufania w siłach zbrojnych przeciwnika, organach dyplomatycznych czy eliminowanie ekonomicznych zdolności do osiągnięcia jego celów lub szkodzenia celom Stanów Zjednoczonych. Uczynienie przeciwnika niezdolnym do kierowania przez spowodowanie braku łączności z jego siłami lub zrozumieniem środowiska działania.
* Odstraszanie agresji, wspieranie nie rozprzestrzeniania broni masowego rażenia i wspieranie działań antyterrorystycznych.

Efekty operacyjne

Działania informacyjne operacyjnego poziomu wojny mogą być kierowane przez dowódcę teatru w granicach przydzielonego obszaru odpowiedzialności lub obszaru działań połączonych przez dowódcę komponentu powietrznego. Działania informacyjne na tym poziomie mogą być także prowadzone w całym spektrum operacji militarnych. Działania informacyjne na tym poziomie będą związane z użyciem zasobów militarnych i ich możliwości dla osiągnięcia operacyjnych skutków przez projektowanie, organizowanie, integrowanie i prowadzenie kampanii i głównych operacji. Szczególnymi skutkami działań informacyjnych jakie mogą być osiągane na tym poziomie są:

* Pozbawianie zdolności przeciwnika do uderzeń. Unieruchamianie pracy jego systemów przetwarzania informacji. Tworzenie zamieszania w środowisku operacyjnym.

* Spowalnianie lub zatrzymywanie operacyjnego tempa działań przeciwnika. Powodowanie niezdecydowania, zamieszania i zagubienia.

* Pozbawianie przeciwnika zdolności do dowodzenia, kontroli, łączności, komputerowego przetwarzania informacji i możliwości rozpoznania przy kierowaniu sytuacji z wojennej w stronę pokojowej. Wykorzystując zamiast fizycznego ataku nie zabójcze techniki walki informacyjnej, zachowuje się fizyczną integralność obiektów pozostających gotowymi dla późniejszego użycia co zapobiega większym kosztom rekonstrukcji podczas przechodzenia od wojny do pokoju.

* Oddziaływanie na percepcję przeciwnika i środowisk neutralnych przez czynienie tej percepcji niezgodnej z celami działań przeciwnika i powodowanie poddania się lub porzucania walki.

* Wspieranie planów działań własnych przez zakłócanie planów działań przeciwnika.

* Zakłócanie zdolności przeciwnika do skupiania wysiłku na swoich celach.

* Wpływanie na ocenę sytuacji przez dowódcę przeciwnika. Przez tworzenie zamieszania i nieścisłości w ocenach dokonywanych przez przeciwnika, można wpływać na kierunek i wynik działań militarnych.

Efekty taktyczne

Dowódcy sił powietrznych lub dowódcy funkcjonalnych komponentów kierują prowadzeniem walki informacyjnej na taktycznym poziomie. Na szczeblu taktycznym walka informacyjna koncentruje się na wzbranianiu, degradowaniu, przerywaniu lub niszczeniu informacji i systemów informacyjnych przeciwnika odnoszących się do dowodzenia i kontroli, rozpoznania i innych ważnych, opartych na informacji procesach bezpośrednio związanych z prowadzeniem działań militarnych. Konkretnymi skutkami mogą być:

* Wzbranianie, degradowanie, przerywanie lub niszczenie informacji o naszych siłach i potencjału informacyjnego przeciwnika.
* Redukowanie rozmiaru lub możliwości sił przeciwnika.
* Uniemożliwianie przeciwnikowi dostępu do wiedzy o siłach.

Planowanie przeciwinformacyjne

Dowódca sił powietrznych utrzymuje wiedzę o informacyjnej infrastrukturze przeciwnika, jego możliwościach i działaniach. Wiedz ta gromadzona jest przez zespół walki informacyjnej pozostający w składzie ośrodka działań powietrznych (AOC). Zespół walki informacyjnej sił powietrznych, szczególnie zespół tego typu w ramach ośrodka działań powietrznych, będzie tworzony podczas kryzysu lub konfliktu (włączając w to działania wojenne) i pracował będzie jako integralna część tego ośrodka. Działalność tego zespołu mieć będzie na celu integrowanie działań walki informacyjnej w plan połączonych działań powietrznych i kosmicznych oraz ujęcie działań walki informacyjnej w rozkaz działań powietrznych (ATO) i kosmicznych. Przedsięwzięcia zespołu walki informacyjnej dowódcy sił powietrznych są w pełni zintegrowane ze strategią, planami walki i manewrowania działań powietrznych i kontrolowane przez centrum operacyjne ośrodka działań powietrznych. Zespół jest złożony z ekspertów reprezentujących różne formy działań informacyjnych. Eksperci ci zebrani są w jednym miejscu aby zbierać i rozdzielać informacje, opracowywać warianty działań walki informacyjnej i określać zadania.

Typowy zespół walki informacyjnej jest złożony ze stałych, głównych i tymczasowych członków. Stali członkowie ponoszą największą odpowiedzialność w ośrodku działań powietrznych, mają doświadczenie na swoich stanowiskach i zwykle przeszli specjalistyczne przeszkolenie. Główni członkowie są ekspertami w granicach swojego obszaru odpowiedzialności, są zobowiązani do pracy w zespole walki informacyjnej i bycia w zespole, ale mają też inne zadania w ośrodku działań powietrznych. Tymczasowi członkowie wnoszą specjalną wiedzę niezbędną w razie pojawienia się doraźnej potrzeby. Kiedy dowódca sił powietrznych dysponuje przydzieloną, orga-

niczną komórką walki informacyjnej to ona wykonuje obowiązki i zakres odpowiedzialności zespołu walki informacyjnej. Podstawą zespołu walki informacyjnej dowódcy sił powietrznych są członkowie biura walki informacyjnej danych sił powietrznych (poszczególne, numerowane siły powietrzne występują jako elementy struktury organizacyjnej) i szef specjalnych działań technicznych oraz zastępca, lub dowódca organizacji walki informacyjnej i szef jego komórki operacyjnej kiedy dowódca sił powietrznych dysponuje etatową strukturą walki informacyjnej.

Zespół walki informacyjnej, na podstawie określonych przez dowódcę sił powietrznych zadań wynikających z celów kampanii dowódcy sił połączonych, opracowuje warianty działań walki informacyjnej. Końcowy plan powinien zawierać zarówno ofensywne jak i defensywne aspekty przeciwdziałania informacyjnego. Udany plan przeciwdziałania informacyjnego zawiera ochronę sił sojuszniczych przez zmuszanie przeciwnika do walki w dogodnym terminie dla sił sojuszniczych, przechwytywanie i utrzymywanie inicjatywy, zapewnienie sprawności, prowadzenie niespodziewanych działań, izolację sił przeciwnika od jego dowódcy i stworzenie warunków do wykorzystania jego słabości. Kluczem do sukcesu walki informacyjnej jest jego pełna integracja przez cały okres planowania, wykonania i finalizowania wszystkich faz działań połączonych i międzynarodowych.

To wymaga koordynacji na całym teatrze działań wojennych, włączając możliwości wsparcia. Przez dowódcę komponentu powietrznego lub dowódcę sił powietrznych zapewniana jest także koordynacja pomiędzy działaniami ofensywnymi i defensywnymi prowadzonymi przez inne organizacje walki informacyjnej sił połączonych.



Rys. 9. Typowy zespół walki informacyjnej.

Ta normalna współpraca i proces integrujący w granicach zadania sił połączonych jest ukazany poniżej:

* Dowódca sił połączonych (JFC) określa cele kampanii i mianuje oficera połączonych działań informacyjnych, który sprawuje ogólny nadzór nad wykonywaniem wszystkich funkcji walki informacyjnej. Oficer działań informacyjnych sił połączonych kieruje zespołem działań informacyjnych jeśli taki jest powołany.

* Zespół działań informacyjnych dowódcy sił połączonych (złożony z wybranych reprezentantów każdego pionu sztabu, rodzajów sił zbrojnych oraz zewnętrznych agencji wspierających odpowiedzialnych za integrację możliwości i dziedzin działań informacyjnych) czerpie cele walki informacyjnej kampanii połączonej z wytycznych połączonego dowódcy (JFC). Te cele zespołu obejmują są bardzo ogólne i nie powinny odnosić się do szczegółów wykonania. Szczegóły te pozostają w zakresie kompetencji komponentów. Jest to zgodne z zasadą sił powietrznych o scentralizowanej kontroli i zdecentralizowanym wykonaniu.

* Komponenty rodzajów sił zbrojnych planują realizację celów walki informacyjnej i efektów niezbędnych dla osiągnięcia tych celów. Wyznaczane są także główne i wspierające elementy walki informacyjnej.

* Zespół walki informacyjnej dowódcy sił powietrznych lub organizacja walki informacyjnej przyjmuje do realizacji zadania wyznaczone siłom powietrznym przez cele połączonego dowódcy i jego zamiar.

* Zespół walki informacyjnej dowódcy sił powietrznych organizuje codzienne bądź gdy potrzeba odprawy, dla opracowania i koordynowania wariantów działań i prezentowania ich dowódcy sił powietrznych do akceptacji. Zespół działań informacyjnych połączonego dowódcy może służyć pomocą w dekonfliktowaniu działań poszczególnych rodzajów sił zbrojnych jeśli zachodzi taka potrzeba.

* Gdy dowódca sił powietrznych zatwierdzi warianty działania zespół walki informacyjnej dowódcy sił powietrznych wprowadza je do rozkazu ATO lub systemu stawiania zadań współpracując z komórkami planowania i kierowania działaniami powietrznymi AOC. Jeżeli wariant działania nie jest zatwierdzony, jest on poprawiany lub odkładany do przyszłego wykorzystania.

* Zespół walki informacyjnej dowódcy sił powietrznych musi opracować zasady walki i wytyczne do walki informacyjnej, także wykazy branych pod uwagę obiektów ataku. Zespół musi koordynować potrzeby i wymagania rozpoznania i być w kontakcie z odpowiednimi strukturami do rozwiązywania problemów i koordynowania wymagań i zadań. Szef zespołu walki informacyjnej musi wyeliminować konflikty w planach atakowania obiektów i zapewniać koordynację z komórką planowania działań powietrznych. Na przykład, jeżeli dany węzeł ma być zachowany dla potrzeb walki informacyjnej to musi być on ujęty w wykazie celi zakazanych do niszczenia. Zespół walki informacyjnej koordynuje użycie zasobów walki informacyjnej sił powietrznych z zespołem planowania dla integracji przedsięwzięć walki informacyjnej w ATO.

Integracja ataku i obrony

Jedną z najważniejszych lekcji sztuki wojennej jest konieczność uzyskania równowagi pomiędzy działaniami zaczepnymi a obronnymi. Udane operacje militarne łączą elementy działań ofensywnych i defensywnych. Równoważne podejście, łączące wszystkie potrzebne i stosowane narzędzia, formy i potencjał walki informacyjnej będą dawać najlepsze efekty w dłuższym okresie czasu. Dowódcy muszą zapewnić swoim sztabom równowagę w planowaniu działań ofensywnych i defensywnych tak żeby uniknąć przeceny możliwości ofensywnych jak również przesadnego polegania jedynie na elektronicznej Linii Maginota.

Ofensywne i defensywne przeciwdziałania informacyjne muszą być zdekonfliktowane i mieć określone priorytety. Na przykład, wysiłki zabezpieczenia informa-

cji zmierzać będą do szybkiego eliminowania ingerencji w systemy informacyjne sił powietrznych, podczas gdy kontrwywiad może życzyć sobie kontynuowania procesu identyfikacji i eksploatowania napastnika czy wprowadzania go w błąd. Działania psychologiczne mogą próbować ujawniać informacje, które normalnie będą nie dopuszczane przez system bezpieczeństwa. Dowódcy są odpowiedzialni za takie decyzje, które są zgodne z planami kampanii i zgodne z decyzjami narodowego dowództwa.

Wyznaczanie obiektów ataku walki informacyjnej

Planiści walki informacyjnej rekomendują obiekty dla walki informacyjnej, które przyczynią się do realizacji planu kampanii. Wyznaczanie celów zaczyna się wraz z określeniem zamiaru dowódcy i ustaleniem strategii działania. Prowadzone ono jest także w oparciu o polityczne i prawne wytyczne. Podążając za tymi instrukcjami, proces wyznaczania celów polega na jasnym określaniu celów szczebla narodowego, teatru działań i określonego dowódcy i ustalaniu pożądanych efektów przy maksymalnej opłacalności każdego wariantu działania. Połączony dowódca określa ogólne cele i wytyczne do ataku na strategiczne i operacyjne środki ciężkości przeciwnika i obronę sojuszniczych, strategicznych i operacyjnych punktów ciężkości jako integralną część kampanii połączonych i głównych operacji. Zespół walki informacyjnej ocenia systemy obiektów informacyjnych, funkcjonalne powiązania i sojusznicze oraz wrogie węzły informacyjne i zaleca odpowiednie ofensywne i defensywne działania walki informacyjnej do ujęcia w plany działań i w ATO. Rodzaj broni i zastosowanych sił zależy od charakterystyki obiektów ataku.

Zespół walki informacyjnej we współpracy z pionem planowania, łączy wyznaczone cele tej walki w plany ataków i rozkazy.

Używając wytycznych połączonego dowódcy, przydziału sił i wykazu obiektów ataku zespół planowania ataku powietrznego planuje szczegóły wykonania ataku używając dostępnych zasobów powietrznych. Zespół kontroli ATO zamienia plan powietrznego ataku w zadania ataku w ATO i dołącza specjalne instrukcje.

4. Ogólna koncepcja walki informacyjnej w Polskich Siłach Powietrznych w przyszłości

Istnieje wiele różnych podejść do działań związanych z oddziaływaniem na sferę informacyjną. Jednakże panuje pewna zgodność w sprawie wyróżniania dwóch obszarów informacyjnego zabezpieczenia różnych procesów i systemów, co nazwać można **informacyjnym zabezpieczeniem walki** oraz sfery atakowania informacji i systemów informacyjnych, atakowania informacją, a także obrony tej sfery. Ten obszar nazwać można ogólnie **działaniami informacyjnymi.** Działania informacyjne odnoszą się do całego spektrum sytuacji od pokoju do wojny. Jednakże działania te w zależności od stojącego przed nimi celu mogą przybrać formę **wojny informacyjnej** lub **walki informacyjnej.**

Wojna informacyjna to działania informacyjne prowadzone na szczeblu strategicznym i mające na celu bezpośrednie osiągnięcie celów strategicznych. **Walka informacyjna** to działania informacyjne, prowadzone w czasie kryzysu lub wojny, mające na celu wsparcie działań militarnych. Działania te prowadzone są dla obrony własnej informacji i systemów informacyjnych lub atakowania informacji i systemów informacyjnych przeciwnika i ingerowania w nie.

Informacyjne zabezpieczenie walki – to rozległe zdolności sił powietrznych do zabezpieczenia świadomości w całym zakresie działań militarnych, wynikające z dysponowania zintegrowanymi środkami rozpoznania oraz działalności w zakresie gromadzenia i dystrybucji informacji, a także w zakresie globalnej nawigacji i określania pozycji, rozpoznawania pogody i zabezpieczania łączności.

Główną kategorią działań informacyjnego zabezpieczenia walki jest **zasilanie informacyjne. Zasilanie informacyjne** dekomponuje się na **zdobywanie informacji, przetwarzanie informacji** i **dostarczanie informacji.** Zasilanie informacyjne dostarcza dowódcom zdolności obserwowania przeciwnika, przestrzeni działań i analizy zdarzeń. Zasoby sił powietrznych mogące realizować informacyjne zabezpieczenie walki umożliwiają dowódcom wyższą zdolność oceniania sytuacji i podjęcia stosow-

nego działania. Funkcje takie jak rozpoznanie, precyzyjna nawigacja i ustalanie położenia wzmacniają efekty użycia przestrzeni powietrznej i działań informacyjnych.

Pojawiające się czwarte środowisko, w którym może być prowadzona walka, umownie nazywane cyberprzestrzenią, przyczynia się do pojawienia się działań prowadzonych w tym środowisku. Ze względu na informacyjny charakter tworzącej się w strefie wysoko rozwiniętych krajów cywilizacji i znaczenie informacji potrzeba dominacji w cyberprzestrzeni staje się warunkiem wstępnym dla podejmowania klasycznych działań. Ponadto istnieje możliwość osiągnięcia celów politycznych czyli wygrania wojny w rezultacie wygrania walki w cyberprzestrzeni. W innych wypadkach osiągniecie dominacji informacyjnej jest niezbędne dla podjęcia klasycznych działań militarnych.

Przewaga informacyjna to stopień dominacji, który daje własnym wojskom zdolność do gromadzenia, kontroli, wykorzystania i obrony informacji bez efektywnego przeciwdziałania. Ta przewaga powinna stać się podstawową zdolnością sił powietrznych, na której opierają się pozostałe zdolności tych sił. W żadnej innej dziedzinie nie ma tak wielkiego postępu technicznego, jak w obszarze informacji i systemów informacyjnych. Chociaż przewaga informacyjna nie jest tylko sprawą sił powietrznych, rozległa perspektywa i doświadczenie uzyskane z działania w przestrzeni, czyni lotników wyjątkowo przygotowanych do zdobywania i wykorzystania przewagi informacyjnej.

Osiągnięcie przewagi informacyjnej jest możliwe w wyniku prowadzonej walki informacyjnej. Podobnie jak przewaga w powietrzu umożliwia dowódcy swobodę ataku i bezpieczeństwo przed atakiem tak przewaga informacyjna spełnia również podobną funkcję. Zdolność do wspierania dowódcy kompleksowym, wielośródłowym, zbliżonym do czasu realnego, odzwierciedleniem sytuacji bojowej przy jednoczesnym uniemożliwianiu tego samego przeciwnikowi jest istotą działań informacyjnych.

Główną kategorią działań współczesnej walki informacyjnej jest **przeciwdziałanie informacyjne. Przeciwdziałanie to ustanawia przewagę informacyjną przez odpowiednie neutralizowanie działalności informacyjnej przeciwnika lub wpły-**

wanie na nią w potrzebnej skali. Przeciwdziałanie informacyjne skupia się na zwalczaniu możliwości przeciwnika w zakresie uzyskiwania korzyści informacyjnych. Przeciwdziałanie informacyjne realizowane jest przez wzbranianie dostępu do informacji oraz jej degradację, przerywanie, niszczenie, mylenie i wykorzystanie. Wszystkie te przedsięwzięcia zmierzają do zmylenia, opóźnienia, zatrzymania ofensywnych akcji przeciwnika i zredukowania jego czasu na podjęcie niezbędnych przedsięwzięć obronnych.

Przeciwdziałanie to dekomponuje się na **ofensywne i defensywne przeciwdziałanie informacyjne.** Połączone z walką o panowanie w powietrzu przeciwdziałanie informacyjne tworzy środowisko, w którym własne wojska dysponują swobodą działania, podczas gdy działalność informacyjna przeciwnika jest w zależności od potrzeb, wzbroniona, neutralizowana lub zniekształcana.

Przeciwdziałanie informacyjne	
Ofensywne przeciwdziałanie informacyjne	**Defensywne przeciwdziałanie informacyjne**
Działania psychologiczne **Walka elektroniczna** • **Atak elektroniczny** • **Elektroniczna ochrona** • **Wsparcie elektroniczne** **Mylenie** **Atak fizyczny** **Atak informacyjny**	**Ochrona informacji** **Bezpieczeństwo operacyjne** **Przeciwdziałanie myleniu** **Kontrwywiad** **Kontrdziałania psychologiczne** **Ochrona elektroniczna**

Rys. 10. Najważniejsze formy działań przeciwdziałania informacyjnego.

Ofensywne przeciwdziałanie informacyjne zawiera przedsięwzięcia podejmowane w celu kontroli środowiska informacyjnego. Działania ofensywnego przeciwdziałania informacyjnego są prowadzone aby ograniczać, degradować, przerywać lub niszczyć możliwości informacyjne przeciwnika. Działania te są zależne od znajomości możliwości informacyjnych przeciwnika.

Defensywne przeciwdziałanie informacyjne zawiera przedsięwzięcia, które chronią informację, systemy informacyjne i działania informacyjne przed potencjalnym przeciwnikiem.

Ofensywne i defensywne przeciwdziałanie informacyjne w swojej konstrukcji są analogiczne do tradycyjnej walki o panowanie w powietrzu, dekomponującej się na ofensywną i defensywną. Mimo że analogia nie jest doskonała, istnieją znaczne analogie i lotnicy mogą stosować wiele zasad ofensywnej walki o przewagę w powietrzu w odniesieniu do ofensywnego przeciwdziałania informacyjnego oraz defensywnej walki o przewagę w powietrzu w stosunku do defensywnego przeciwdziałania informacyjnego. Tak jak w ofensywnej walce o panowanie w powietrzu i defensywnej walce o panowanie w powietrzu, dowódcy muszą raczej koncentrować się na wymaganych efektach raczej niż na rozróżnianiu rodzaju tego działania. Granica dzieląca te rodzaje może być bardzo cienka i przejścia jednej formy w drugą prawie natychmiastowe.

Działania ofensywnego przeciwdziałania informacyjnego

Działania ofensywnego przeciwdziałania informacyjnego w znacznym stopniu uzależnione są od zrozumienia zdolności informacyjnych przeciwnika, jego uwarunkowań i słabości. Działania ofensywnego przeciwdziałania informacyjnego, które mogą wpływać na zdolności przeciwnika i wykorzystywać jego słabości zawierają: Działania psychologiczne, walkę elektroniczną, mylenie oraz informacyjny i fizyczny atak.

Działania psychologiczne

Działania psychologiczne są przeznaczone do przekazywania wybranych informacji i sugestii obcym przywódcom i społecznościom, aby wpływać na ich emocje, motywy, rozumowanie i zachowanie na korzyść własnych celów.

Działania psychologiczne mają zastosowanie na szczeblu strategicznym, operacyjnym i taktycznym. Efekty nowoczesnych działań psychologicznych są potęgowane możliwościami sił powietrznych w zakresie komunikacji. Możliwości te wiążą się z precyzją i różnorodnością oraz dużą ilością informacji, która może być przekazywana dla wywarcia wpływu na wyselekcjonowanych odbiorców 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.

Siły powietrzne mogą prowadzić nowoczesne działania psychologiczne. Na szczeblu operacyjnym i taktycznym działania te mogą zawierać dystrybucję ulotek, użycie głośników i innych środków transmitowania informacji, które mogą zachęcać siły przeciwnika do dezercji, ucieczki, poddania się wzbudzenia strachu, lub buntu. Siły te mogą też prowadzić specjalnie zaplanowane uderzenia dla wywołania efektu psychologicznego. Istnieje wiele przykładów takich działań w praktyce. Stałe ataki działań psychologicznych mogą mieć podwójny efekt, przyspieszając degradację morale i dalsze zachęcanie do dezercji.

Walka elektroniczna

Walka elektroniczna jest działaniem zawierającym użycie elektromagnetycznej oraz kierowanej energii do kontrolowania spektrum elektromagnetycznego lub do ataku przeciwnika. Działanie to jest nie tylko ograniczone do częstotliwości radiowych, ale odnosi się też do widma optycznego i podczerwonego dlatego nie powinno być nazywane walką radioelektroniczną, jak to się zdarza w naszej praktyce.

Trzy główne części walki elektronicznej to: atak elektroniczny, ochrona elektroniczna i wsparcie elektroniczne. Wszystkie trzy wspierają działania powietrzne. Kontrola widma jest osiągana przez ochronę własnych systemów i zwalczanie syste-

mów przeciwnika. Atak elektroniczny ogranicza możliwości użycia przez wrogiego dowódcę spektrum elektronicznego. Ochrona elektroniczna zwiększa możliwości użycia widma przez własne siły. Wsparcie elektroniczne pozwala dowódcy na dokładne określenie sytuacji w rejonie operacyjnym. Atak elektroniczny i wsparcie powinny być zintegrowane z ochroną elektroniczną, by system był efektywny. Rozsądny dowódca, zwykle szczebla operacyjnego musi zapewnić maksimum koordynacji pomiędzy walką elektroniczną, rozpoznaniem i śledzeniem oraz działaniami w zakresie zabezpieczenia łączności.

Walka elektroniczna jest mnożnikiem siły. Kontrola elektromagnetycznego spektrum może mieć główny wpływ na sukces w całym spektrum działań militarnych. Właściwe zastosowanie walki elektronicznej zwiększa zdolności dowódców operacyjnych w zakresie osiągania celu. Gdy działania walki elektronicznej są zintegrowane z operacjami militarnymi, osiąga się synergię, minimalizowane są straty, a efektywność działań jest zwiększona.

Dezinformacja wojskowa (mylenie)

Dezinformacja wojskowa wprowadza przeciwnika w błąd, powodując, że działa on zgodnie z planami organizatora dezinformacji. Działania dezinformacji wojskowej rozciągają się na wszystkie szczeble wojny i zawierają komponenty ofensywne i defensywne. Dezinformacja wojskowa może odwrócić uwagę od, lub zapewnić osłonę dla operacji wojskowych myląc i rozpraszając siły przeciwnika. Kontrdezinformacja zapewnia własnym dowódcom przygotowanie na akcje przeciwnika, co pozwala im uniknąć efektów tego działania. 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 położona 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.

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 broni fizycznej. 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 przekaźni-

kowej lub użycie grupy specjalnej w celu przecięcia lub wykorzystania linii komunikacyjnej.

Atak informacyjny

Atak informacyjny odnosi się do tych form aktywności, które mają na celu manipulowanie lub zniszczenie informacji lub systemu informacyjnego bez zmiany fizycznego stanu systemu przeciwnika, w którym dokonywany jest ten atak.

Penetracja systemu informacyjnego przeciwnika ma wielką wartość w walce, ponieważ oferuje zdolność do obezwładnienia przeciwnika bez narażania własnych sił, przy redukcji strat towarzyszących i unikaniu konieczności zadawania dużych strat przeciwnikowi. Dzięki użyciu nowych możliwości i narzędzi, konwencjonalne wyloty bojowe mogą być wykorzystane na inne cele. Manipulacja bazami danych lub parametrami systemów może powodować błędne informacje, które będą wpływały na proces decyzyjny lub mogą niszczyć zaufanie przeciwnika do jego systemu informacyjnego. Efektywny atak informacyjny może zmusić przeciwnika do używania mniejszej ilości środków technicznych ze względu na nasze włamanie się do jego systemu. Przykładem ataku informacyjnego może być spowodowanie dezinformacji w obiegu danych radarowych, aby doprowadzić do niecelnego ognia pocisków przeciwlotniczych. Atak informacyjny może być postrzegany jako oddziaływanie na „obserwowanie" i „orientowanie" – dwa komponenty zamkniętego cyklu obserwowanie – orientowanie – decydowanie – działanie, gdyż wówczas zdolność przeciwnika do polegania na „obserwacji" jest obniżona.

Działania defensywnego przeciwdziałania informacyjnego

Działania defensywnego przeciwdziałania informacyjnego to te akcje, które chronią informacje i systemy informacyjne sił powietrznych przed przeciwnikiem.

Siły powietrzne powinny prowadzić defensywne przeciwdziałanie informacyjne aby zapewnić potrzebną obronę dla możliwości przeprowadzania własnych działań.

Aktualne wypadki włamań do systemów powodowanych przez nastolatków począwszy, kończąc na umyślnym zakłócaniu systemów niezbędnych do tworzenia obrazu sytuacji powietrznej dla połączonych komponentów sił powietrznych demonstruje, jak ważna jest obrona informacji w działaniach militarnych. Ze względu na rosnące zależności od systemów informacyjnych, defensywne przeciwdziałanie informacyjne powinno być priorytetem sił powietrznych, jeśli chodzi o walkę informacyjną. W związku z tym dowódcy powinni być odpowiedzialni za działania defensywnego przeciwdziałania informacyjnego w swoich jednostkach. Celem tych działań jest zapewnienie potrzebnej obrony informacji i systemów informacyjnych, które wspierają działania militarne. Jeśli działania defensywnego przeciwdziałania informacyjnego są połączone z ofensywnym przeciwdziałaniem informacyjnym, rezultatem będzie zwiększona możliwość zastosowania walki informacyjnej dla uzyskania żądanych militarnych i politycznych celów. Formy, które mogą być zastosowane, aby przeprowadzić działania defensywnego przeciwdziałania informacyjnego to: bezpieczeństwo operacyjne, ochrona informacji, kontrdezinformacja, kontrwywiad, kontrdziałania psychologiczne i ochrona elektroniczna. Te różne formy wspólnie się uzupełniają, (tzn. każda z nich może być użyta jako przeciwśrodek w celu wsparcia innej) i mogą wspierać działania ofensywne. Dodatkowo, aby uzyskać lepsze efekty, formy te muszą być stosowane wielowarstwowo. Mimo to, jeśli są używane bez koordynacji i integracji może zaistnieć między nimi, jak również z działaniami ofensywnymi, konflikt.

Bezpieczeństwo operacyjne i ochrona informacji

Siły powietrzne powinny stosować przedsięwzięcia bezpieczeństwa by chronić i bronić informacje i systemy informacyjne. Przedsięwzięcia te odnoszą się do bezpieczeństwa operacyjnego i ochrony informacji. Bezpieczeństwo informacyjne jest procesem identyfikacji najważniejszych informacji i analizowanie własnych akcji, które towarzyszą działaniom militarnym i innym działaniom dla:

- identyfikowania tych akcji, które mogą być obserwowane przez systemy wywiadowcze przeciwnika;

- określania wskaźników, które obce systemy rozpoznania mogą zebrać, zinterpretować i złożyć w całość w celu uzyskania najważniejszych informacji we właściwym czasie;
- wybierania i zastosowania środków, które wyeliminują lub zredukują do akceptowalnego poziomu słabości własnych działań wobec przeciwnika.

Bezpieczeństwo operacyjne to proces. Jest on zbiorem specyficznych zasad i instrukcji, które powinny być zastosowane do działań lub aktywności w celu zablokowania dostępu przeciwnikowi. Bezpieczeństwo operacyjne jest stosowane we wszystkich działaniach wojskowych na wszystkich szczeblach dowodzenia.

Dowódca sił powietrznych powinien wskazać kierunki planowania bezpieczeństwa operacyjnego dla swojego sztabu na początku procesu planistycznego, kiedy określa swój zamiar i następnie dla podległych dowódców w łańcuchu dowodzenia. Poprzez utrzymanie łączności ze wspierającymi dowódcami i koordynowanie planowania bezpieczeństwa operacji dowódca sił powietrznych zapewnia jedność wysiłku w uzyskiwaniu i utrzymywaniu potrzebnego stopnia utajnienia.

Ochrona informacji to przedsięwzięcia podejmowane dla osłony i obrony informacji i systemów informacyjnych dla zapewnienie ich dostępności, integralności, autentyczności, tajności i zdolności do identyfikowania źródła informacji i danych.

Ochrona informacji zawiera także odtworzenie systemów informacyjnych przez utrzymywanie zdolności do osłony, wykrywania zagrożeń i reagowania na nie. Ochrona informacji powinna być stosowana we wszystkich działaniach militarnych na wszystkich szczeblach. Dowódca sił powietrznych powinien wskazać kierunki planowania dla swojego sztabu, określając swój zamiar oraz dla podległych dowódców w hierarchii dowodzenia. Proces ochrony informacji jest stosowany poprzez działania wykorzystujące nowoczesne technologie.

Ochrona informacji zawiera ochronę systemów informacyjnych przed niepożądanym dostępem do informacji lub jej niszczeniem. Obejmuje to ochronę kompute-

rów, łączności i przedsięwzięcia potrzebne do wykrycia, udokumentowania i przeciwdziałania takim zagrożeniom.

♦ Ochrona komputerów zawiera przedsięwzięcia podejmowane dla ochrony tajności integralności i dostępności informacji przetwarzanej i przechowywanej w komputerze. Składają się na to odpowiednia polityka, procedury, hardwarowe i softwarowe narzędzia potrzebne do ochrony systemów komputerowych i informacji.

♦ Bezpieczeństwo łączności zawiera przedsięwzięcia mające na celu zlikwidowanie dostępu nieautoryzowanych osób do informacji zapewniając jednocześnie autentyczność komunikacji. Ochrona komunikacji zawiera krypto ochronę, ochronę transmisji, emisji i fizyczną ochronę urządzeń komunikacyjnych i informacji.

Kontrdezinformacja

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

Kontrwywiad

Kontrwywiad ochrania działania, systemy, technologię, urządzenia, personel i inne zasoby przed nielegalnymi tajnymi operacjami obcych służb, grup terrorystycznych i innych. Kontrwywiad ocenia możliwe do eksploatacji potencjalne źródła informacji i ich słabości.

Kontrdziałania psychologiczne

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

Ochrona elektroniczna

Walka elektroniczna jest działaniem militarnym zawierającym użycie elektromagnetycznej oraz kierowanej energii do manipulacji spektrum elektromagnetycznym lub do ataku przeciwnika. Defensywny aspekt tej walki, ochrona elektroniczna gwarantuje użycie spektrum elektromagnetycznego przez własne siły. Ochrona elektroniczna jest ważna częścią defensywnego przeciwdziałania informacyjnego i musi być skoordynowana i zintegrowana z możliwościami ofensywnego działania oraz z innymi działaniami.

Zakończenie

Stan rozwoju współczesnej cywilizacji i jej uzależnienie od informacji i systemów informacyjnych sprawiają, że pojawiają się poważne zagrożenia i nowe możliwości walki. Odnoszą się one do działań w nowym wymiarze, roboczo nazwanym cyberprzestrzenią. Obecna sytuacja jest podobna do tej z początków XX wieku kiedy pojawiały się pierwsze aparaty latające i zaistniała możliwość, a później konieczność prowadzenia działań w nowym wówczas środowisku przestrzeni powietrznej. Koncepcja wykorzystania tego nowego wówczas środowiska ulegała zmianom. Początkowo zakładano użycie tej przestrzeni do prowadzenia rozpoznania powietrznego. Szybko jednak odkrywano nowe możliwości w związku z czym pojawiła się walka powietrzna a następnie zadania szturmowe i bombowe w ramach wsparcia wojsk lądowych. Nie upłynęło zbyt wiele lat jak dostrzeżono jeszcze większe możliwości, nazywanego już wówczas potęgą powietrzną, lotnictwa. Gulio Douhet dostrzegł możliwość bezpośredniego wygrania wojny jedynie przy użyciu lotnictwa. W ten sposób potęga powietrzna stała się w niezwykle krótkim czasie jednym z głównych narzędzi przemocy w polityce międzynarodowej.

Podobna sytuacja istnieje obecnie z informacją i cyberprzestrzenią. Informacja była co prawda używana od zarania dziejów jednakże obecna skala tego użycia tworzy nową jakość. Ponadto w cywilizacji, w której informacja staje się głównym dobrem staje się ona także głównym obiektem atakowania, a także środkiem walki. W związku z uzależnieniem informacyjnym współczesnych organizacji obiektem atakowania stają się także systemy informacyjne bo mają one bezpośredni wpływ na informację.

Podobnie jak potęga powietrzna w przeszłości uzyskała zdolności wygrywania wojen tak i obecnie przeprowadzenie wojny informacyjnej może doprowadzić do zwycięstwa. Prowadzenie walki informacyjnej i uzyskanie informacyjnej dominacji staje się warunkiem wstępnym podejmowania jakichkolwiek innych działań militarnych. Siły powietrzne, ze względu na swoje wysokie utechnicznienie, wysoki poziom wykształcenia kadry, szerszą perspektywę, głębokie związki z informacją i systemami informacyjnymi oraz możliwości łączenia działań powietrznych z informacyjnymi

bardzo dobrze nadają się do prowadzenia walki informacyjnej. Ponadto przestrzeń powietrzna ma znaczne podobieństwa z cyberprzestrzenią takie jak np. brak naturalnych ograniczeń w poruszaniu się, duże szybkości ruchu, możliwość szybkiego przenoszenia wysiłku, czy duże zagrożenie spowodowane nieograniczonym zasięgiem i skalą ataku. Sprawia to, że koncepcja wojny powietrznej, a praktycznie działań powietrznych, staje się niezwykle przydatna w konstruowaniu koncepcji wojny informacyjnej, a szczególnie działań i walki inmformacyjnej.

Walka informacyjna jako ta część działań informacyjnych która odnosi się do sfery militarnej jest więc nie tylko przydatna, ale wręcz niezbędna w przyszłych działaniach sił powietrznych. Jeśli te nie podejmą działań i walki informacyjnej przynajmniej w zakresie niezbędnym dla zabezpieczenia własnych działań to ich znaczenie spadnie. Ponadto w każdym swoim działaniu będą zależne od jakiejś innej organizacji, która tworzyć będzie i zabezpieczać warunki ich działań. Tymczasem siły powietrzne lepiej niż inne rodzaje sił zbrojnych nadają się do prowadzenia działań informacyjnych i walki informacyjnej. Jeśli jeszcze nie istnieją właściwe warunki po temu to ze względu na wagę problemu należałoby podjąć wysiłki i systematycznie je tworzyć. Początkowo należałoby uzyskiwać zdolności obronne dla potrzeb zabezpieczenia działań powietrznych, a następnie możliwości ofensywne by przez ich użycie móc osiągać pożądane cele militarne.

Bibliografia

1. Air Force 2025. America`s Vigilant Edge". Air University. Maxwell AFB, 1996.Air Force Basic Doctrine, Headquarters Air Force Doctrine Center, Maxwell AFB, Alabama 1997.
2. Air Force Basic Doctrine. AFDD 1. USAF 1997.
3. Bohenek J. Szpieg online. Wprost nr 11 z 14 marca 1999 s. 84-86.
4. Information Operations. AFDD 2-5. USAF 1998.
5. FM 100-5 Operations. Headquarters Department of the Army. 1993.
6. FM 100-6 Information Operations. Headquarters Department of the Army. 1996.
7. Force XXI Operations. TRADOC Pamphlet 525-5. A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty First Century. US Army TRADOC. 1994.
8. Global Engagement: A Vision for the 21st Century Air Force. USAF.
9. Gulin W.P. „O nowej koncepcji wojny". Wojennaja Myśl Nr 2/1997 r. Tłumacz. por. mar. Przemysław Jastrzębski.
10. Komow S.A. „O sposobach i formach prowadzenia walki informacyjnej", Wojennaja Myśl 1997.
11. NL Arms. Netherlands Annual Review of Mlitary Studies 1999. Bosh J.M.J. Luiijf H.A.M. Mollema A.R. Information Operations. Breda 1999.
12. Schwartau W. Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age. Thunder's Mouth Press. New York 1996.
13. Szpyra R. Środowisko przyszłej walki powietrznej na tle globalnych zmian cywilizacyjnych na progu XXI wieku. AON, Warszawa 1998.
14. Szpyra R. Współczesna wojna powietrzna. AON, Warszawa 1998.
15. Toffler A. i H. Wojna i antywojna. Warszawskie Wydawnictwo Literackie MUZA S.A. Warszawa 1997.

16. Waller D. Thompson M. Strach Generałów. Forum Nr 36 (157) z 3 września 1995, przedruk artykułu, który 21.VIII 1995 r. opublikowany został w TIME

17. Warden III J.A. „Air Theory for the Twenty-first Century" Battlefield of the Future. 21st Century Warfare Issues. Air University, Maxwell AFB 1995.

