AKADEMIA OBRONY NARODOWEJ

WARTOŚĆ INFORMACJI W DOWODZENIU I ZARZĄDZANIU

MODEL PRZEWAGI INFORMACYJNEJ

WARSZAWA 2002

AKADEMIA OBRONY NARODOWEJ

WARTOŚĆ INFORMACJI W DOWODZENIU I ZARZĄDZANIU

MODEL PRZEWAGI INFORMACYJNEJ

Zespół autorski:

płk prof. dr hab. Inż. Piotr SIENKIEWICZ – kierownik
dr Henryk SPUSTEK
por. mgr inż. Jerzy GRZYB
mgr inż. Maciej KOZYRA
lic. Halina ŚWIEBODA
Barbara ROGOWIEC

Warszawa **listopad 2002**

SPIS TREŚCI

WPROWADZENIE

Wojna (i walka cybernetyczna) i informacja są jak stare wino w nowych bukłakach. O wojnie w Zatoce Perskiej napisano, że była „I wojną informacyjną" (The First Information War), zaś o „wojnie z terroryzmem" mówi się tylko o wojnie „nowej generacji". To opinie nie pozbawione pewnej przesady. O wojnie peloponeskiej, genialnie opisanej przez Tukidydesa można również powiedzieć, że była „wojną informacyjną". Z kolei, swoistą innowacją „Wojny z terroryzmem jest to, że nie jest prowadzona „z kimś", jak bywało dotychczas, lecz „z czymś". każda ze znanych wojen zawierała elementy walki informacyjnej. Ale dopiero lata 90 ubiegłego wieku uświadomiły, że „zmasowane" użycie różnorodnych technologii i systemów informacyjnych może mieć wpływ na przebieg i rezultaty walki zbrojnej porównywalny do wpływu środków materialno-energetycznego rażenia. Opierając się na znanych elementach „wojny w Zatoce" można skonstruować następujący scenariusz: faza pierwsza – systemy walki informacyjnej paraliżują „system nerwowy" (tj. systemy dowodzenia, łączności, rozpoznania i wre) przeciwnika, faza druga – uderzenie sił powietrznych powoduje „przetrącenie kręgosłupa" (tj. obezwładnienie obiektów aktywnych i elementów infrastruktury), faza trzecia – siły lądowe powodują „opanowanie" terenu i obezwładnienie sił i środków przeciwnika. Gdyby cele polityczno-wojskowe zostały osiągnięte już w wyróżnionej fazie pierwszej, to przedstawiony scenariusz można byłoby przyjąć za scenariusz „wojny informacyjnej" (INFOWAR). Aktualne możliwości techniczne USA pozwalają uznać ten scenariusz za możliwy i prawdopodobny.

„Wojna z terroryzmem" przypomniała (bo nie stworzyła, bynajmniej) pojęcie asymetrii w walce Należy jednak zauważyć, że w odróżnieniu od niektórych autorów na ten temat, nie chodzi wszak o „asymetrię siły", czyli „miażdżącą" przewagę wyrażoną chociażby za pomocą „stosunku siły", lecz o „asymetrię informacyjną", czyli nierównomierny dostęp do istotnych, z punktu widzenia celu działań, informacji. Dodajmy, że za prace poświęcone asymetrii informacji na rynku (realiach: producent – nabywca) w roku 2000 J. Stiglitz (Columbia University) otrzymał Nagrodę Nobla w dziedzinie ekonomii.

Po roku trwania „wojny z terroryzmem" można dostrzec swoistą asymetrię informacji: pomimo posiadania trudnej do wyrażenia „przewagi informacyjnej" nie uzyskano dostatecznej „przewagi wiedzy". Wyrazem zaś tego są wypowiedzi typu: „na podstawie posiadających informacji można stwierdzić, że bin Laden znajduje się w Pakistanie lub innym kraju".

W dokumentach takich, jak Joint Vision 2010 i 2020 oraz najnowszych publikacjach RAND Corporation w centrum uwagi znajdują się pojęcia PRZEWAGI INFORMACYJNEJ oraz PRZEWAGI WIEDZY jako wyrażające czynniki decydujące o zwycięstwie na współczesnym polu walki (w hipotetycznej przyszłej wojnie?). Imperatywem współczesnych badań systemowych nad zjawiskiem wojny (walki) jest analiza, a przede wszystkim operacjonalizacja powyższych kategorii. Stosowne instrumentarium badawcze obejmuje niejako klasyczne metody i modele takie, jak:

- matematyczna teoria informacji (z jej wariantem pierwotnym stworzonym przez C.E.Shannona),
- matematyczne teoria walki (z jej wariantem wyjściowym stworzonym przez W.Lanchestera).

Dodatkowym urządzeniem są z pewnością modele symulacyjne (typu JTLS, JANUS czy projektowany ZŁOCIEŃ), które niebawem znajdą się na wyposażeniu Centrum Symulacji i Komputerowych Gier Wojennych AON.

Warto zwrócić uwagę na obserwowane w najbliższym otoczeniu zjawisko, które trudno nie oceniać negatywnie. Otóż, nader często podkreśla się jakiś „brak definicji informacji", zaś przytacza się różnorodne określenia, nie zawsze zresztą poprawnie interpretowane. Tymczasem, cybernetyka Norberta Wienera (a także Mariana Mazura), teoria informacji Claude'a Shannona, a także prace Johna von Neumanna, Allana Turinga i wielu innych (np. Juliusza L. Kulikowskiego i Jerzego Seidlera) nie pozostawiają żadnych wątpliwości co do istoty informacji i komunikowania. A to przecież „klasyka" nauki XX wieku, którą należy po prostu znać.

Schyłek XX wieku przyniósł, oprócz przytoczonego wcześniej pojęcia INFOWAR (i INFOWARFARE) także inne, np. CYBERWAR i NETWAR. Pierwsze oznacza walkę (wojnę) w przestrzeni cybernetycznej (CYBERSPACE) drugie wskazuje na globalną sieć (np. INTERNET) jako środowisko przyszłej walki. Pojęcia te niejako otwierają dopiero niezwykle interesujący obszar badań systemowych.

Niniejszy raport z badań obejmuje rezultaty mające przede wszystkim charakter przeglądowy. Siłą rzeczy skłaniają do wstępnej konceptualizacji oraz propozycji pewnego modelu matematycznego walki informacyjnej. Chcąc tworzyć pewne projekcje należałoby zapewne zwrócić uwagę na wartości tkwiące w teorii nieliniowych dynamicznych systemów i związanej z nią teorii chaosu. Jednakże badanie zjawisk nieliniowych oznacza wkraczanie w obszar badań wielce złożonych i trudnych. Trudności sprawia matematyczne modelowanie nieliniowych procesów fizycznych, chemicznych, czy biologicznych. Ale walka zbrojna,

w tym walka informacyjna należą do klasy zjawisk społecznych, te zaś nadal należy uznać za „mało podatne" na „matematyzację". Należy zatem szukać pewnego kompromisu między ścisłością (i elegancją) modeli matematycznych a „publicystyczną nieprecyzyjnością" (i „filozofią") badań społecznych. Dążenie do tak rozumianego kompromisu przyświecało autorom niniejszego raportu.

1. WSPÓŁCZESNE KONCEPCJE WALKI INFORMACYJNEJ

Gdy podsumowywano wpływ nowoczesnych technologii na rezultat wojny w Zatoce Perskiej, posłużono się skrótem: „4S" , co miało oznaczać: niewidzialne samoloty *(Stealth),* manewrujące rakiety wystrzeliwane z okrętów *(Sea Launched C'ruise Missiles),* obronę zorganizowaną zgodnie z założeniami Strategicznej Inicjatywy Obronnej *(SDI Like Defense)* oraz systemy rozpoznania kosmicznego *(Sperce System Spy Satelites).* Następnie dodano piąte S - *Semiconductors* , czyli po prostu półprzewodniki, słusznie podkreślając podstawę rozwoju technologii informacyjnych, od których zależał rozwój pozostałych czterech „S". Słynny publicysta Alvin Toffler pisał, nie bez pewnej przesady, że wojnę w Zatoce wygrała inteligencja ukryta w mikroprocesorach systemów uzbrojenia oraz w systemach dowodzenia, łączności i rozpoznania.

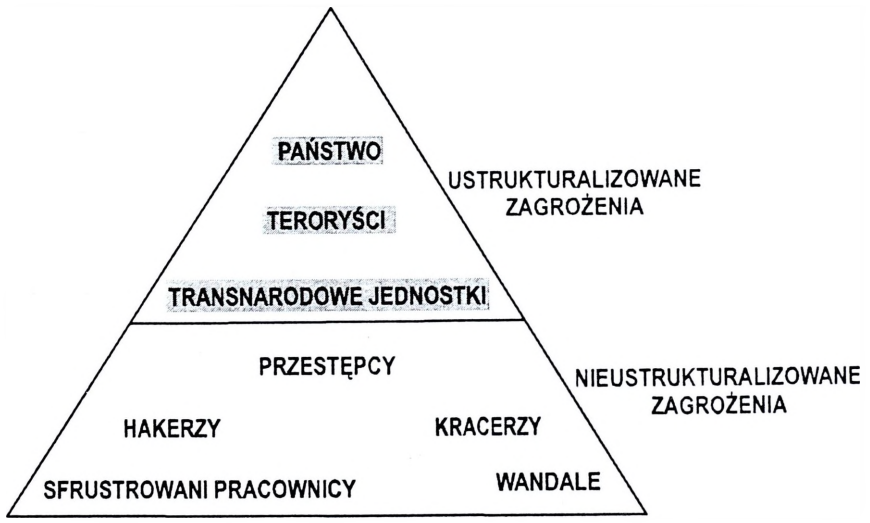
Wśród głównych przyczyn klęski armii irackiej, której potencjał był oceniany jako czwarty na świecie, uznano przestarzałą elektronikę. Była ona bowiem mało wydajna, oparta na łatwo zakłócanej technice analogowej, uniemożliwiającej efektywną, kompleksową automatyzację systemów dowodzenia, łączności, rozpoznania i sterowania środkami walki. Na przegranej Irakijczyków zaważył również zbyt mały i przestarzały potencjał systemów informacyjnych, które nie były w stanie dostarczyć danych niezbędnych do planowania i wykonania uderzeń na obiekty przeciwnika. Obrazu przyczyn klęski dopełnił mało elastyczny system kierowania i dowodzenia (o sztywnej hierarchicznej strukturze). W tych obszarach wyraża się druzgocąca wprost przewaga aliantów, co można wyrazić jako konfrontację systemów należących do dwóch różnych generacji technologicznych.

Wojna w Zatoce Perskiej stanowiła przykład wojny, o rezultatach której zadecydowała „przewaga technologiczna", której następstwem była „przewaga informacyjna".
Dlatego słusznie zapewne A. Campen nazwał ją „I wojną informacyjną" *(The First Information War).*

1.1. WSPÓŁCZESNA WALKA INFORMACYJNA

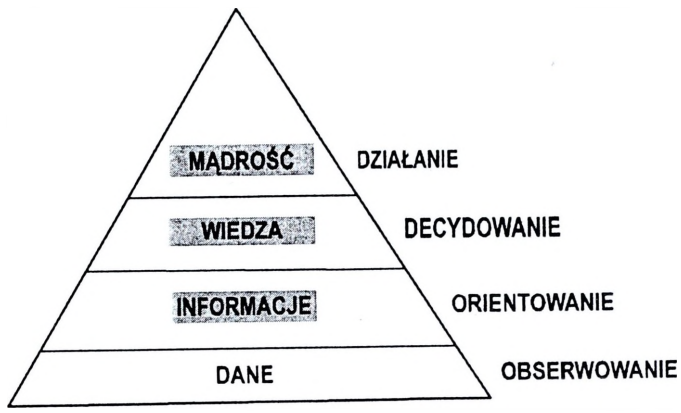
W dokumentach z serii Joint Publication Hierarchy Departamentu Obrony USA dostrzec można koncepcję tworzenia wieloczynnikowej przewagi militarnej *(multifactor military superiority)* w oparciu o kontrolowaną, rozstrzygającą przewagę informacyjną *(information superiority)* i technologiczną *(technological superiority).* We wszystkich współczesnych koncepcjach walki informacyjnej *(infórmation warfare)* kluczową rolę odgrywa potencjał informacyjny jako istotny element potencjale militarnego (bojowego) zarówno w działaniach (operacjach) ofensywnych, jak i defensywnych.

Od czasów Wojny w Zatoce, którą uznano za „I wojnę informacyjną" (A. Campen: *„The First Information War")* rozstrzygająca przewaga informacyjna traktowana jest jako istota współczesnych koncepcji prowadzenia działań (operacji) informacyjnych typu *„Infowar"* i *„Cyberwar".*



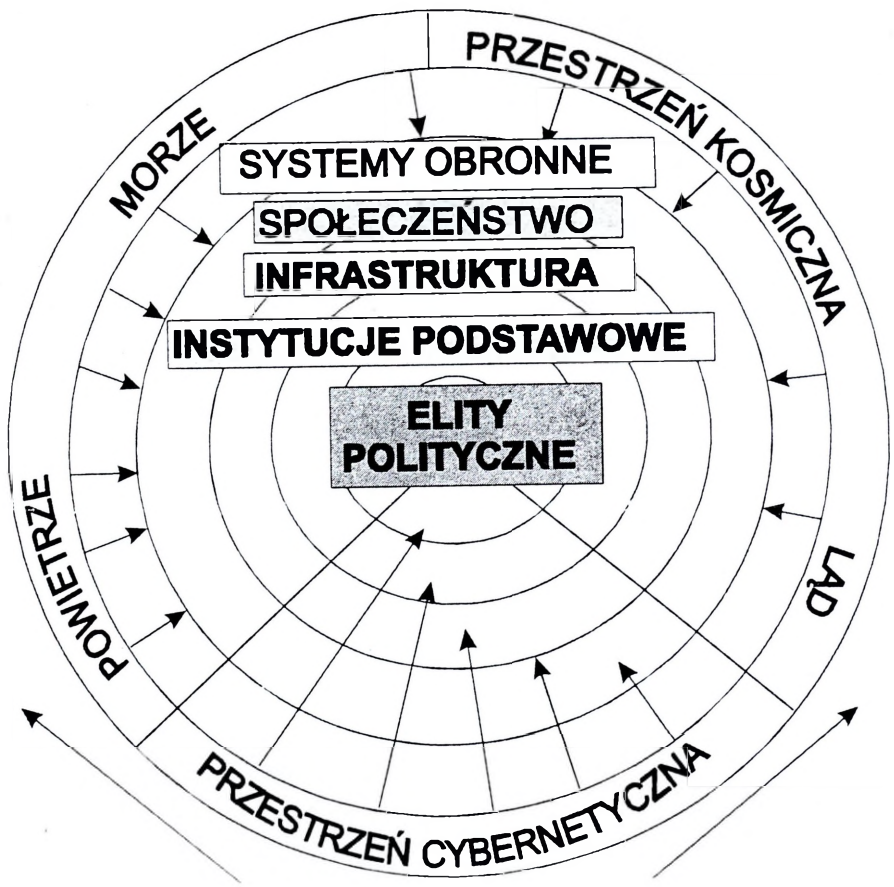
Rys.1.1. Hierarchia zagrożeń

Za punkt wyjścia należy przyjąć pojęcie bezpieczeństwa informacyjnego jako inteligentnej części bezpieczeństwa narodowego, a następnie zagrożeń informacyjnych (rys.l.1). Infosfera, czyli całokształt informacyjnych elementów tworzących społeczne otoczenie wszelkich działań (indywidualnych i zbiorowych) obejmuje: dane *(data),* informacje *(information),* wiedzę *(knowledge)* i mądrość *(wisdom).*



Rys.1.2. Hierarchia informacji

Warto zauważyć związek Hierarchii informacji z ogólnym modelem „ODDA" *(Observe – Orient - Decide - ACT ;* rys. 2). Innym nowym, bo sformułowanym w latach 90, ujęciem współczesnej walki jest tzw. Model Wardena, w którym piątym „wymiarem" walki jest „przestrzeń cybernetyczna" *(Cyberspace).*

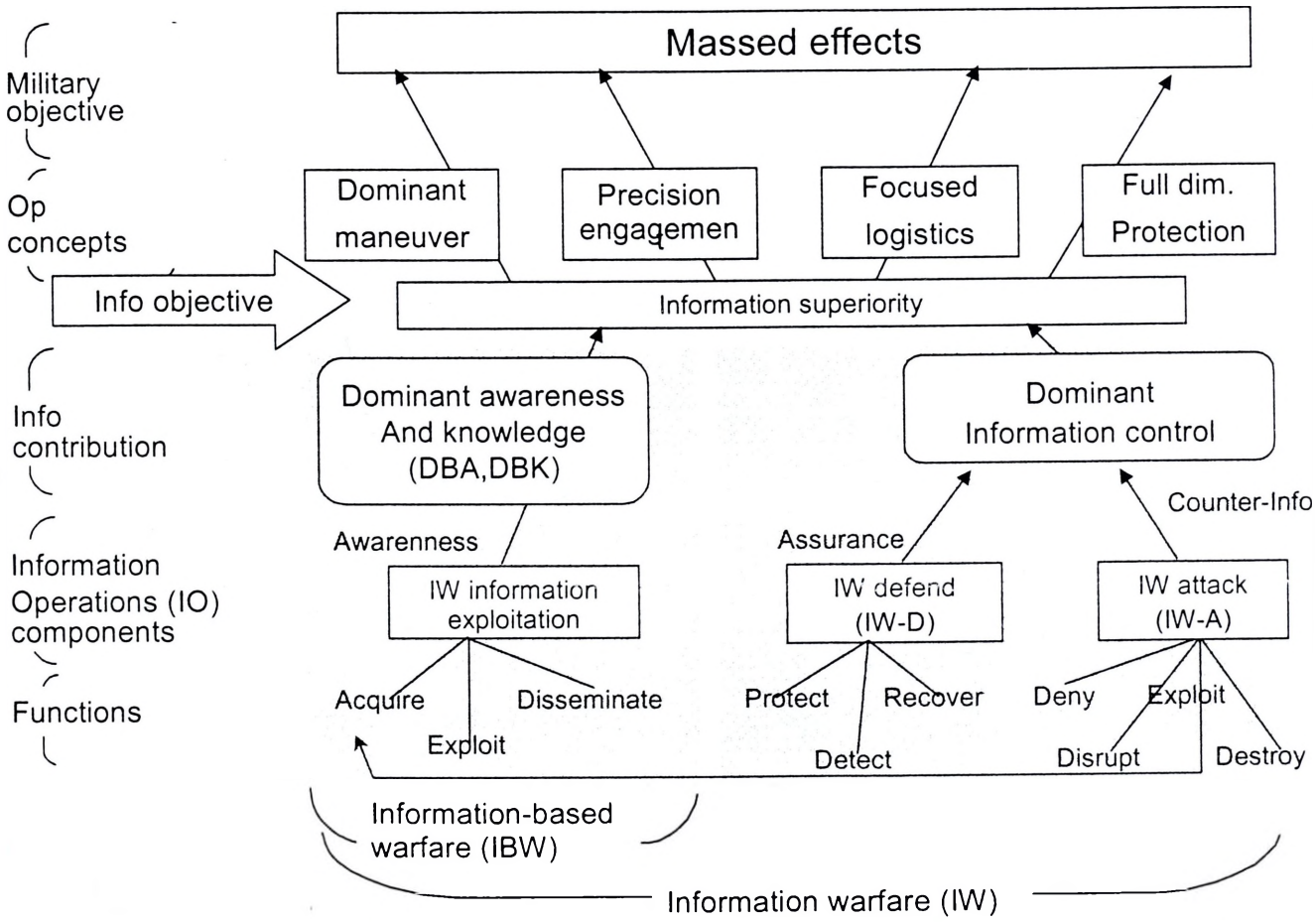


Rys.1.3. Model „pięciu wymiarów" walki Wardena

W opracowaniu Joint Wision 2010 wprowadzono nowe elementy działań (operacji):

- manewr dominujący *(dominant maneuvre)* ,
- uderzenie precyzyjne *(precision engagement),*
- ochrona pełnowymiarowa (*fulldimension protection*),
- logistyka zogniskowana *(focused logistics).*

Warunkiem powodzenia powyższych działań jest uzyskanie przewagi informacyjnej rozumianej jako: *„zdolność do zbierania, przetwarzania i udostępniania informacji przy wykorzystaniu (lub deprecjonowaniu) zdolności przeciwnika do wykonania tego samego"* (RAND, 2001. Z kolei, dominacja informacyjna obejmuje zarówno wysiłki ofensywne, jak i defensywne, których celem jest stworzenia dystansu *„między tym, co my wiemy o naszej przestrzeni bojowej i operacjach w niej prowadzonych, a tym, co nieprzyjaciel wie o swojej przestrzeni bojowej"* (rys. 1.4).



Rys.1.4. Model przewagi informacyjnej.

Konsekwencją analizy systemowej procesów informacyjnych na współczesnym polu walki jest wprowadzenie „stosunku wiedzy" (relative knowledge) stron walczących, jako czynnika decydującego w rezultatach walki.

Walką informacyjną (information warfare, infowar) nazywamy całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych).

Istotą tak rozumianej walki informacyjnej jest:

(1) zniszczenie (lub degradacja wartości) zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych;

(2) zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystanych systemów informacyjnych.

1.2. OPERACJE INFORMACYJNE

Nowoczesne koncepcje walki zbrojnej bazują na tworzeniu wieloczynnikowej przewagi militarnej *(multifactor mulitary superiority)* w oparciu o kontrolowaną, rozstrzygającą przewagę informacyjna *(information superiority)* i technologiczną *(technological superiority).* Aczkolwiek potencjał informacyjny stanowił zawsze istotny czynnik potencjału bojowego, to w rozważaniach dotyczących sposobów tworzenia przewagi na polu walki był on raczej pomijany. W szczególności w matematycznych modelach walki (typu modele Lanchestera) uwaga koncentrowała się na *„stosunku sil"* uwzględniającym przede wszystkim *„potencjały rażenia"* stron walczących.

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

W ostatnich latach wyróżniono informacyjne operacje (działania) ofensywne i defensywne.

Do operacji ofensywnych zalicza się takie działania, jak:

- osłona operacji *(operations security),*
- operacje psychologiczne *(psychological operations),*
- pozoracja *(military deception),*
- destrukcja *(physical attack),*
- walka elektroniczna *(electronic warfare).*

Warunkiem powodzenia powyższych działań jest uzyskanie przewagi informacyjnej *(information superiority),* rozumianej jako: *„zdolność do zbierania, przetwarzania i udostępniania informacji przy wykorzystaniu (lub deprecjonowaniu zdolności przeciwnika do wykonania tego sameg"* (BAND , 2001). Z kolei, dominacja informacyjną *(information dominance)* obejmuje zarówno wysiłki ofensywne, jak i defensywne, których celem jest stworzenie różnicy *„między tym, co my wiemy o naszej przestrzeni bojowej i operacjach w niej prowadzonych, a tym, co nieprzyjaciel wie o swojej przestrzeni bojowej".*

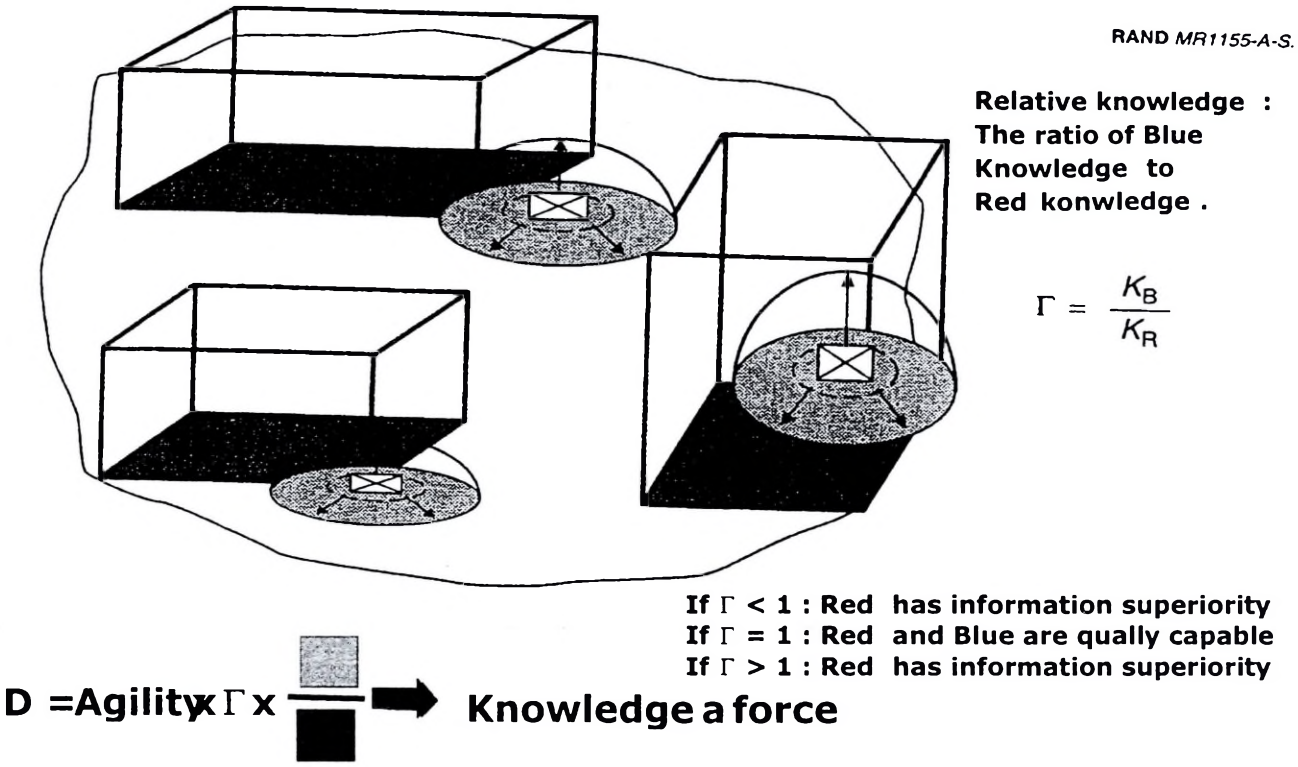
Przyjęcie powyższych koncepcji prowadzenia działań zmusza do poszukiwania nowych miar (kryteriów) oceny efektywności. Jedną z nich jest tzw. Stosunek wiedzy, określony dla następujących założeń (rys. 1.6):

(1) dowolna jednostka kontroluje dowolny obszar, gdy jest ona zdolna do działania „wewnątrz" tego obszaru w sposób dowolny;

(2) promień kontrolowanego przez daną jednostkę obszaru jest równy najmniejszej z trzech wielkości: maksymalnego, skutecznego zasięgu systemów ognia pośredniego jednostki, maksymalnego skutecznego zasięgu jej systemów rozpoznania („sensorów"), promienia przydzielonego obszaru operacji;

(3) wiedza to stopień posiadanej przez dowódcę jednostki znajomości dyspozycji sił własnych i nieprzyjaciela wewnątrz obszaru wyznaczonego przez promień kontroli tej jednostki (tzw. Stopień posiadanej „świadomości sytuacyjnej").

Rys.1.5. Dowodzenie i działania militarne



Rys.1.6. Koncepcja oceny efektów i przewagi informacyjnej

Niech wiedzę jednostki Niebieskich i jednostki Czerwonych oznaczają odpowiednio wielkości: K_B i K_R . Względną wiedzę (lub względną świadomość sytuacyjną) określa „stosunek wiedzy":

$$\Gamma = \frac{K_B}{K_R}, \quad 0 \leq \Gamma < \infty$$

taki, że:

Jeśli	**to**	**i**
$K_B > K_R$	$\Gamma > 1$	**Niebiescy mają przewagę informacyjną**
$K_B < K_R$	$\Gamma < 1$	**Czerwoni mają przewagę informacyjną**
$K_B = K_R$	$\Gamma = 1$	**Brak przewagi informacyjnej**

Załóżmy, że **O < β < 1** jest wymaganą „luką" zapewniającą dominację informacyjną. Aby niebiescy osiągnęli dominację informacyjną należy przyjąć, że $K_B > K_R$ (warunek przewagi informacyjnej) oraz

$$1 \geq K_B - K_R \geq \beta$$

stąd warunek:

$$1 + \frac{\beta}{K_R} \leq \Gamma \leq 1 + \frac{1}{K_R}$$

CYBERWAR – ZAGROŻENIE OCENY

Zważywszy na różnorodność występujących konfliktów, mamy do czynienia z diametralnie różnymi przeciwnikami i typami prowadzenia potencjalnych konfliktów.

Tablica 1.1. Typy konfliktów

Wojny partyzanckie

		Wysoka technologia	**Niska technologia**	
Gospodarka oparta na wojnach	**Konflikt fizyczny**	C1. kampania militarna C2W o dużej intensywności C2. nacisk ekonomiczny i militarny C3. precyzyjne cele C4. fizyczne maskowanie C5. technologia C4I	C6. partyzanckie działania wojenne C7. niska intensywność kampanii militarnych C8. bezwzględność C9. przypadkowy dobór celów C10. środowisko naturalne C11. sieci społeczne	**Terroryzm**
	Konflikt abstrakcyjny	D1. Wojna sieciowa, CyberWar D2. konflikt przestrzeni kosmicznej D3. wiedza siłą sprawczą D4. ustalanie celów oparte na informacji D5. technologia sieci globalnych	D6. wojna ideologiczna D7. cele społeczne D8. ideologiczna sieć społeczna	

Wojny kulturowe

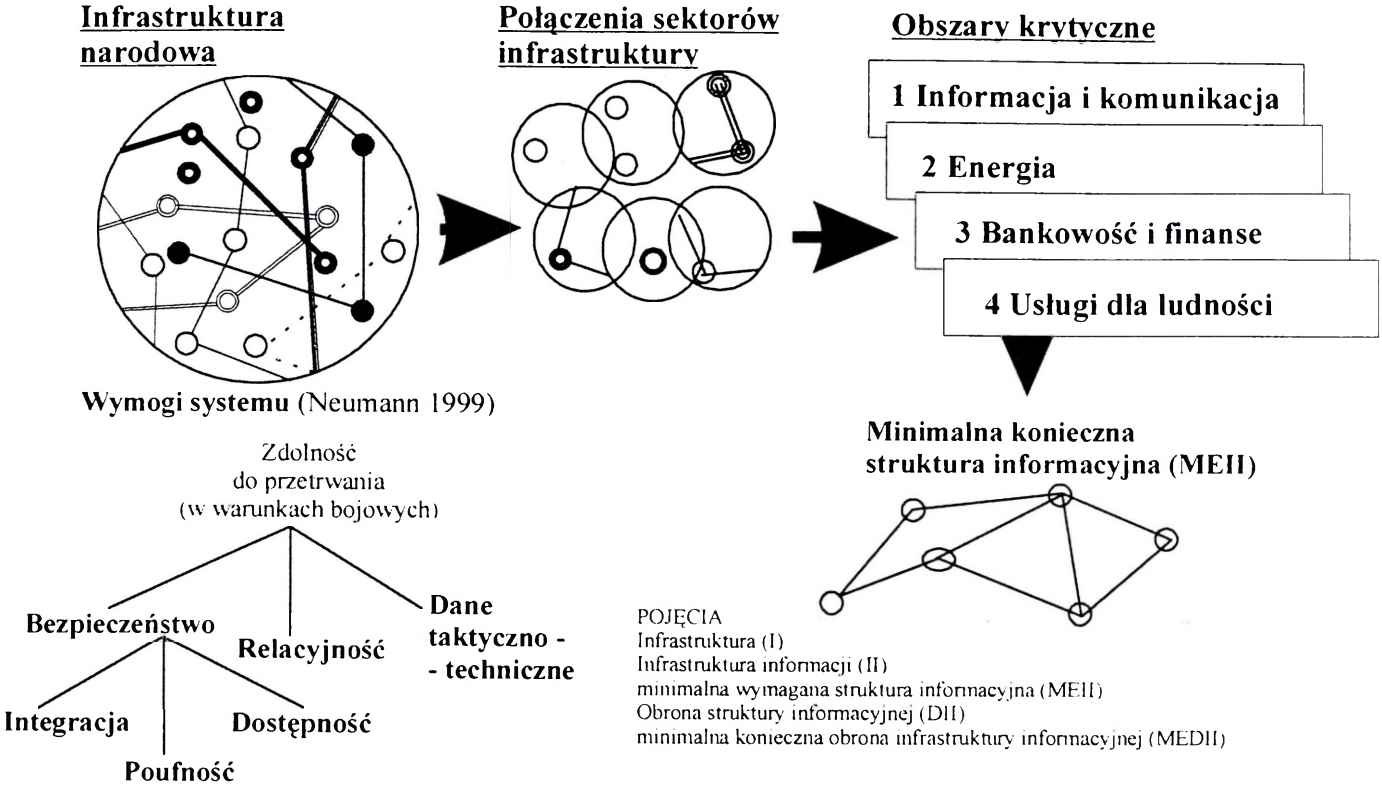
Źródło: Waltz E. , Information Warfare, Artech H. , Boston 1998.

EWOLUCJA CYBERATAKÓW

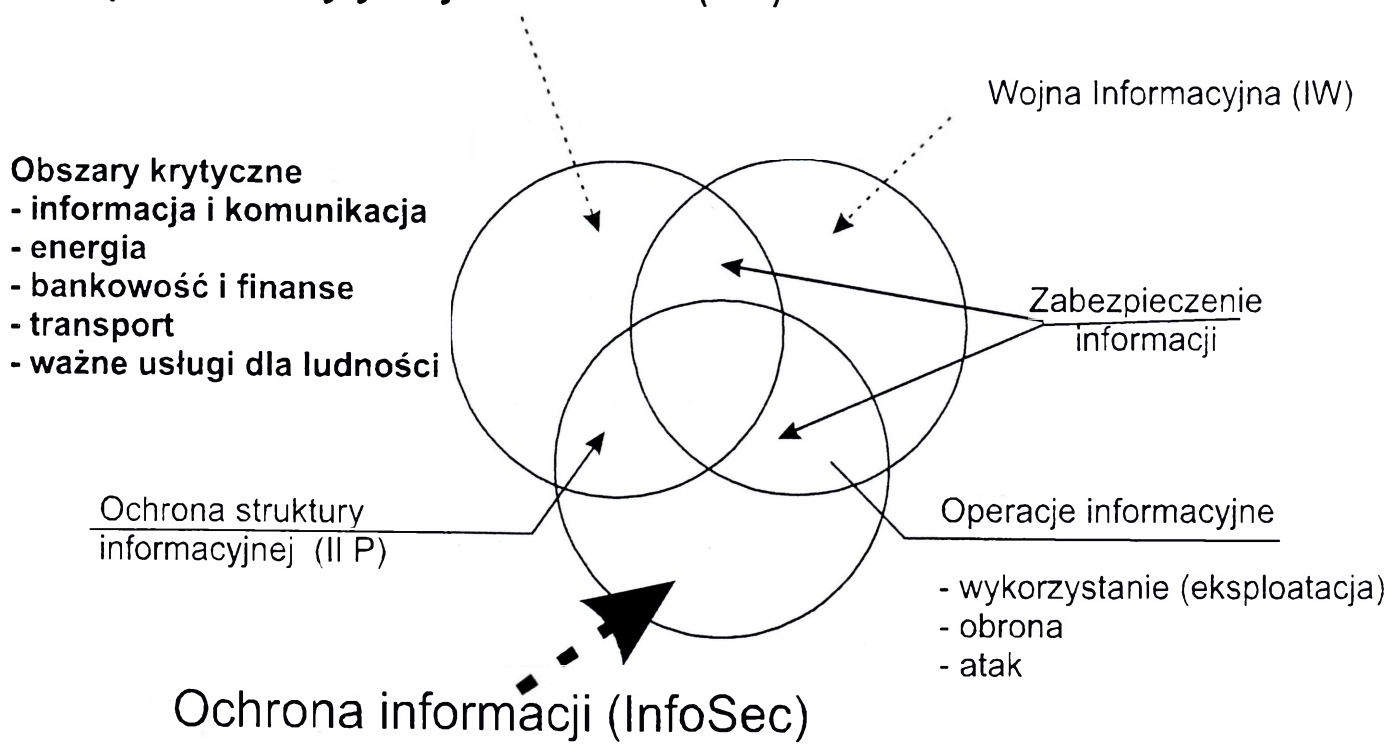
Tablica 1.2 zawiera cechy cyberataków służące oszacowaniu prawdopodobieństwa celów i motywów.

Cyberataki	Odnotowane ważne ataki	Cele				
		Informacja	Systemy Małe Sieci	Organizacje Przemysł	Rząd	Infrastruktura i społeczeństwo
Niekompetencja niedbalstwo	Powszechny	Główny cel	Główny cel			
Wewnętrzna odmowa usług	Powszechny	Główny cel	Ograniczony	Główny cel		
Hakerstwo rekreacyjne	Powszechny	Główny cel	Główny cel			
Elektroniczne Nieposłuszeństwo	Ograniczony		Cel	Główny cel		
Publiczne Hakerstwo	Powszechny	Główny cel	Ograniczony			
Poparcie prawne	Ograniczony	Główny cel	Ograniczony			
Występowanie Wywiadu Gospodarczego	Ograniczony Szybki wzrost	Główny cel				
Atak Ekonomiczny	Ograniczony Szybki wzrost	Główny cel	Główny cel	Główny cel		Ograniczony
Wywiad Narodowy	Wiadomo że wystąpił	Główny cel		Ograniczony?	Cel?	
Grupy działania/ hakerzy	Ograniczony wzrost	Ograniczony	Główny cel	Główny cel	Główny cel	Ograniczony
wandalizm	Ograniczony		Główny cel	Cel		Ograniczony
Przestępstwa Proste	Ograniczony	Główny cel		Cel		
Przestępstwa finansowe	Wysoki, szybki wzrost	Główny cel		Cel		
Przestępczość zorganizowana	Nieznane	Główny cel		Główny cel	cel	
Cyber terroryzm	PIRA: ograniczony				cel	Główny cel
	Ograniczony	Główny cel	cel	cel	cel	Główny cel

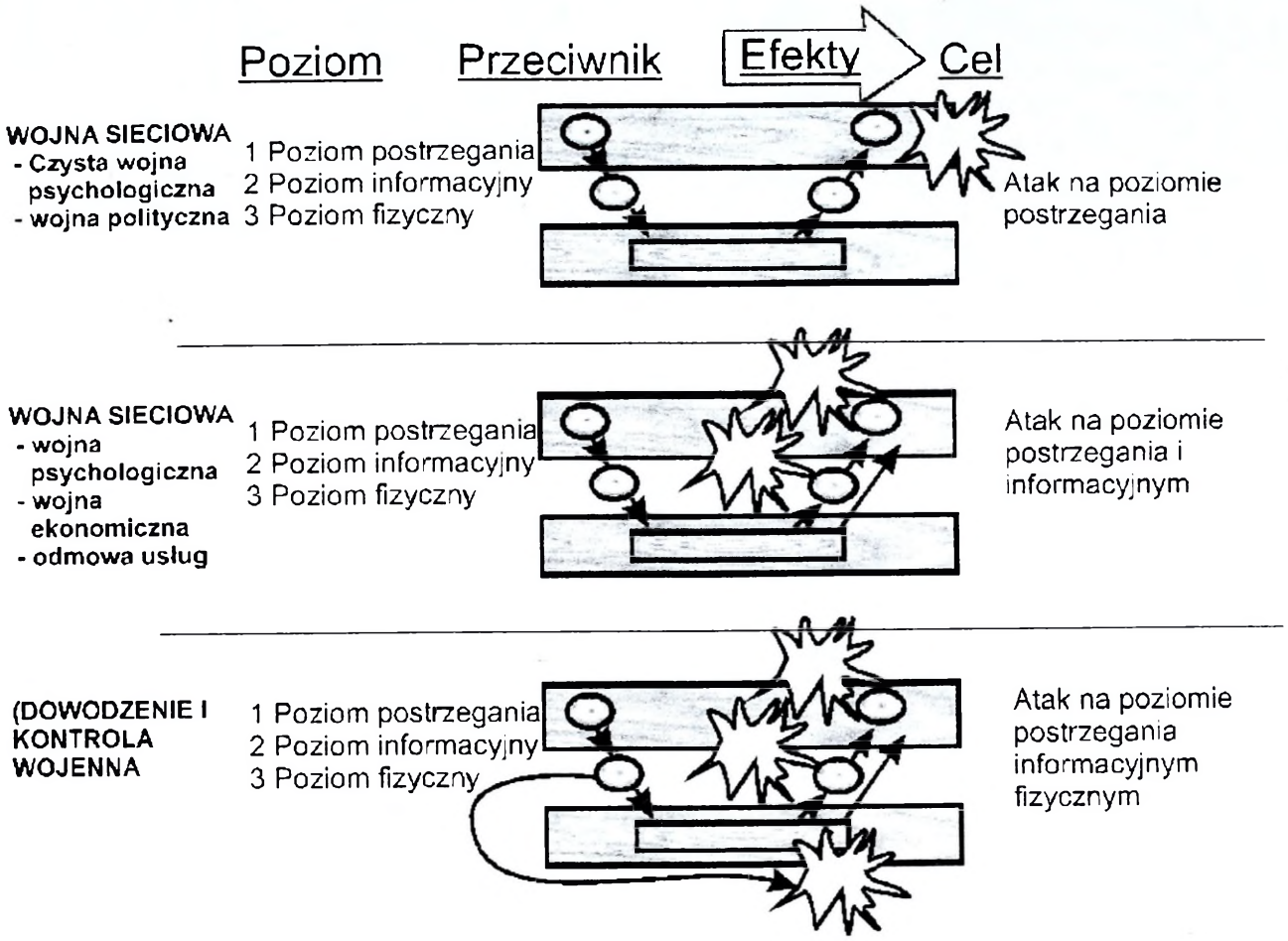
A.



B.



Rys.1.7. Informacja w strukturach społecznych.



Rys.1.8. Wojna sieciowa i jej poziomy.

1.3. PODSUMOWANIE

Współczesne koncepcje walki informacyjnej, obejmujące nowe modele operacji, w których kluczową rolę spełniają pojęcia „przewagi informacyjnej" i „przewagi wiedzy" nie wyczerpują pojęcia wojny cybernetycznej, czyli różnych form walki prowadzonej w „przestrzeni cybernetycznej" . Aczkolwiek pojęcie „cyberprzestrzeni" W. Gibson w powieści „Neuroromancer", to obecnie najczęściej określa ono globalną informacyjną (teleinformatyczną) infrastrukturę. A zatem istotą wojny cybernetycznej jest realizacja określonych celów politycznych dzięki działaniom podejmowanym w przestrzeni cybernetycznej.

Do swoistych cech wojny cybernetycznej należy zaliczyć następujące:

- misją jest uzyskanie przewagi informacyjnej,
- przeciwnik jest „niewidzialny",
- terenem działań jest cyberprzestrzeń,
- czynnikiem krytycznym jest czas.

Istnieje kilka poziomów wojny cybernetycznej, z których można wyróżnić trzy:

- wojna cybernetyczna towarzysząca operacjom wojskowym
- ograniczona wojna cybernetyczna,
- nieograniczona wojna cybernetyczna.

W ograniczonej wojnie cybernetycznej teleinformatyczna infrastruktura państwa jest środkiem i celem działań towarzyszących realnemu atakowi. Może być prowadzona w celu np. opóźniania przygotowań przeciwnika do interwencji zbrojnych.

Nieograniczoną wojnę cybernetyczną charakteryzuje rozległy zasięg, zarówno wojskowe jak i cywilne obiekty, wreszcie destrukcyjne konsekwencje potencjalnie w każdej sferze życia społecznego.

Współczesne myślenie o pokoju, bezpieczeństwie narodowym, musi obejmować analizy systemowe zjawiska wojny cybernetycznej oraz związane z nim zagrożenia i szanse bezpiecznego rozwoju.

LITERATURA DO ROZDZIAŁU PIERWSZEGO

1. Argnilla I. , Ronfeldt D. , Cyberwar is Coming" , Comparative Strategy, 12, 1993.
2. Bracken I. , Combat Models, J. Wiley, 1995.
3. Campen A. , Dearth D. , Gooden R. (ed.) , Cyberwar: Security, Strategy and Conflict in the Information Age, AFCEA 1996.
4. Campen S.A. (ed.) ,The First Information War, AFCEA 1992.
5. Concept for Future Joint Operations: Expanding Joint Vision 2010, Department of Defense, May 1997.
6. Darilek R. , Perry W. , Bracken J. , Gordon J. , Nichiporuk B. , Measures of Effectiveness for the Information - Age Army, RAND 2001.
7. Sienkiewicz P. , Inżynieria systemów , MON 1983.
8. Sienkiewicz P. , Współczesne koncepcje wojny informatycznej, „Computerworld" , nr 35, 1995.S
9. Sienkiewicz P. Inżynieria informacji (w przg .).
10. Stokalski A. , Amerykańska doktryna operacji informacyjnych, „Myśl Wojskowa", nr 11, 200.
11. Waltz E. , Information Warfare, Artech H. , Boston 1998

2. MODELOWANIE PROCESU WALKI INFORMACYJNEJ

Wojna informacyjna obok wojny nuklearnej, chemicznej czy biologicznej, stanowi swoisty rodzaj wojny w której specyficznym narzędziem stanowiącym broń, jest informacja. Dokładne przyjrzenie się uwarunkowaniom jakie spowodowały, że wojna informacyjna stała się obecnie tak powszechnym zjawiskiem, pozwala na sformułowanie tezy, że kierunek rozwoju i ewolucji broni odbył się w zupełnie naturalny sposób. Informacja stała się bronią tak samo efektywną jak inne, konwencjonalne metody prowadzenia walki. Jednocześnie, posługiwanie się informacją jako bronią pozwala na rozwiązanie konfliktów w odmienny sposób, diametralnie różny od metod konwencjonalnych. Przede wszystkim, możliwym staje się uniknięcie strat typowych dla metod konwencjonalnych. Niekiedy możliwym staje się całkowita eliminacja strat. Dzieje się tak dlatego, że wielu konfliktów można uniknąć, właśnie dzięki odpowiedniemu użyciu zdobytej a następnie przetworzonej informacji. Zdolność do zdobywania, przetwarzania, manipulowania i wymiany informacji ma, i będzie miała, zdecydowany wpływ na podstawową działalność człowieka, w tym i przyszłą wojnę. Mimo oczywistego faktu, wiodącego wpływu informacji, jej kwantyfikowanie i pomiar, nie jest zadowalający. Rozwiązanie tego zagadnienia jest ważne dla armii, szczególnie w czasie, gdy przeznacza ona znaczną część swojego, z trudem wystarczającego, kapitału inwestycyjnego na tworzenie połączeń Wieku Informacyjnego wewnątrz swoich sił i struktur (tzw. „ucyfrowienie armii"). Ze względu na procesy transformacji w samej Armii, potrzebuje ona narzędzi analitycznych, godnych Wieku Informacyjnego, zapewniających pomoc w dokonywaniu najlepszych możliwych wyborów.

W niniejszym rozdziale zostanie przedstawiona propozycja modelowania procesu tworzenia przewagi ze szczególnym uwzględnieniem czynników niematerialnych, w tym informacji. Zaprezentowano dwojakie podejście do zagadnień tworzenia przewagi informacyjnej: traktując zagadnienie w sposób probabilistyczny i deterministyczny.

2.1. PRZEWAGA I METODY JEJ TWORZENIA

Po drugiej wojnie światowej wybuchła ogromna ilość wojen i konfliktów zbrojnych. Z bardziej znaczących wymienić można: Koreę, Wietnam, Bliski Wschód, Pakistan, Iran, Irak, Afganistan, Zatoka Perska, wojna w byłej Jugosławii, Czeczenia. Konflikty zbrojne o podłożu etnicznym przeniosły się również na terytorium Europy, kontynent na którym przez długi czas panował pokój.[1]

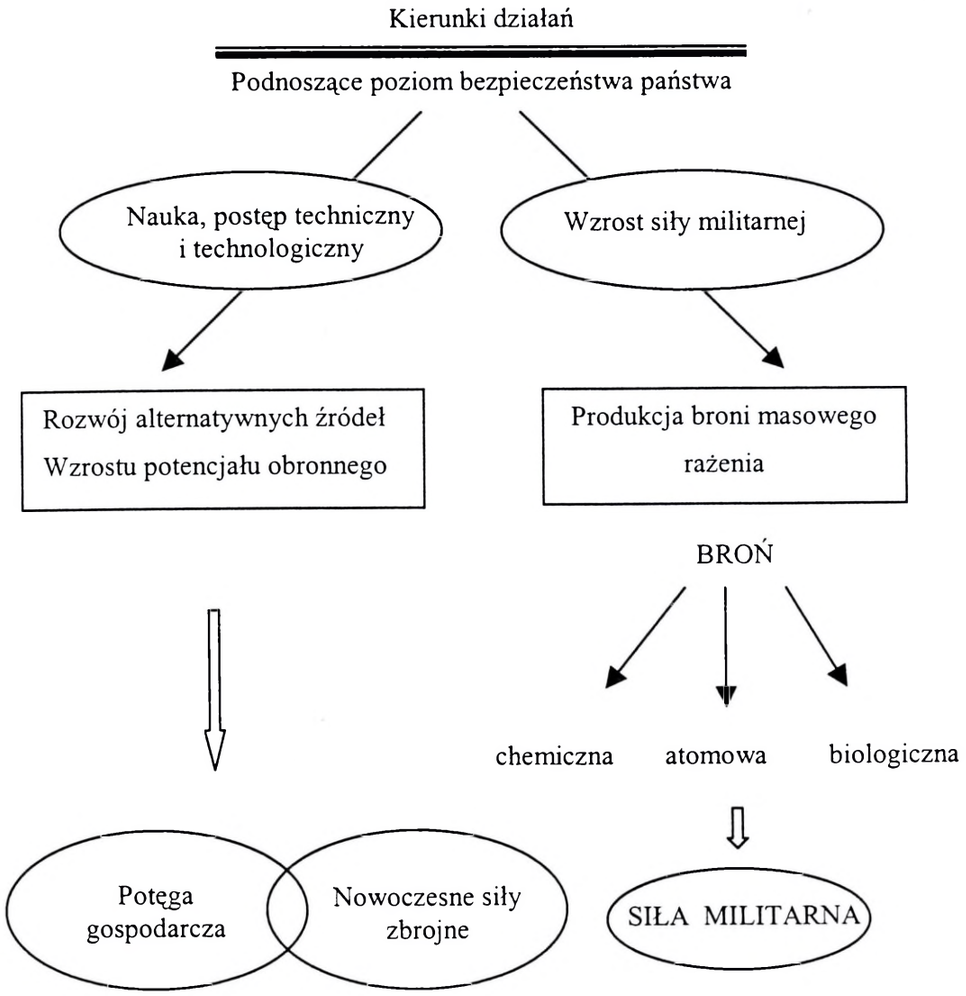
Znaczne zmniejszenie stanów osobowych wojsk oraz uzbrojenia i sprzętu technicznego, powoduje konieczność poszukiwania nowych rozwiązań pozwalających na zapewnienie przewagi w potencjalnym konflikcie zbrojnym. Państwa wysoko rozwinięte kładą główny nacisk na rozwój technologiczny swoich systemów uzbrojenia. Sukcesywna modernizacja i wymiana posiadanego uzbrojenia na sprzęt coraz nowszej generacji, pozwala zachować im posiadany potencjał bojowy w stosunku do innych państw, pomimo znacznego zredukowania części systemów uzbrojenia.

W przypadku państw rozwijających się, problem zapewnienia nawet podstawowego poziomu bezpieczeństwa narodowego jest bardziej złożony. Z powodu niedoboru środków finansowych na modernizowanie i rozwój sił zbrojnych, część z nich, większą wagę przykłada do rozwoju innych, niewymagających dużych nakładów, procesów na utrzymanie wymaganego poziomu potencjału obronnego. Są to działania kładące większy nacisk na rozwój intelektualny - wyszkolenie armii. Inny kierunek działań w tym zakresie polega na próbach uzyskania i wyprodukowania broni masowego rażenia, najczęściej chemicznej lub biologicznej.

Każde państwo próbuje zapewnić sobie pewien minimalny poziom bezpieczeństwa poprzez wybór i rozwój takich systemów uzbrojenia, na które je stać i które w maksymalnym stopniu zapewnią realizację celów zawartych w doktrynach wojennych oraz możliwość uzyskania przewagi podczas ewentualnego konfliktu zbrojnego. Kierunki podejmowanych działań, których celem jest podnoszenie bezpieczeństwa państwa przedstawia rys. 2.1.

---

[1] Z.Ścibiorek, Wojna czy pokój?, Ossolineum, Wrocław 1999 s.96 – 99.



Rys.2.1. Metody podnoszenia bezpieczeństwa państwa.

Źródło: opracowanie własne.

Różne podejście do problemu podnoszenia poziomu bezpieczeństwa państwa ma bezpośredni wpływ na przebieg przyszłego konfliktu zbrojnego. Konflikt ten należy rozpatrywać w wielu wymiarach. Jest rzeczą oczywistą, że nie będzie to klasyczne starcie dwóch wielkich armii, tak jak odbywało się to w przeszłości. Precyzując ten pogląd, należałoby powiedzieć, że jest rzeczą niezmiernie mało prawdopodobną aby w przyszłości zaistniał konflikt zbrojny klasycznego typu.[2]

[2] J.Stefanowicz, Rzeczypospolitej pole bezpieczeństwa, Wyd. Adam Marszałek, Warszawa 1993, s.144.

2.2. KLASYFIKACJA METOD TWORZENIA PRRZEWAGI

W większości konfliktów na świecie jakie wybuchły w latach 90-tych ubiegłego wieku, dużą rolę odgrywały formacje nieregularne, partyzanckie oraz narodowo-wyzwoleńcze. Formacje te występowały przeciwko regularnym siłom zbrojnym. Przyczynę takiego układu sił w wielu minionych konfliktach należy upatrywać w tym, że ich podłoże stanowiły waśnie etniczne. To właśnie tego typu konflikty uzmysławiają wagę czynników trudno mierzalnych w kształtowaniu przewagi na polu walki.

Przewagę należy rozpatrywać w wielu wymiarach, a samo jej tworzenie jest zjawiskiem złożonym.[3] Elementów tworzenia przewagi nie można traktować rozłącznie, ponieważ wzajemnie się przenikają i uzupełniają.[4]

Przewagę należy traktować w kategoriach procesu. Proces tworzenie przewagi jest procesem ciągłym. Rozpoczyna się on w czasie pokoju we wszystkich sferach działalności państwa, w tym w sferze militarnej.

Pojęcie przewagi jest nierozerwalnie związane z pojęciem potencjału bojowego. Wszelkie rozważania dotyczące przewagi, jej tworzenia oraz utrzymania muszą być prowadzone w kontekście oddziaływań na siebie przeciwstawnych stron. Zatem, przewaga może być rozumiana dwojako:

- statycznie, jako przewaga w potencjale wojsk operacyjnych i obrony terytorialnej,
- dynamicznie, jako efekt wykorzystania różnego rodzaju oddziaływań.[5]

Warunki środowiska walki postrzegane jako „coś niemierzalnego", stają się często czynnikiem decydującym o powodzeniu lub niepowodzeniu działań bojowych.

Do zasadniczych elementów potencjału bojowego wojsk (oprócz czynników wymiernych) będących podstawą tworzenia wymaganej przewagi na czas konfliktu zbrojnego zalicza się:

- gotowość i zdolność wojsk do działania,
- kadry dowódcze i sztabowe, w tym ich wykształcenie i przygotowanie do dowodzenia i działania w różnych, nawet najbardziej skomplikowanych warunkach,
- odpowiednio wyszkolone i przygotowane siły i środki wojsk operacyjnych, zdolne do współdziałania w ramach struktur sojuszniczych,
- sprawny i niezawodny system dowodzenia.

---

[3] Rozważania dotyczące przewagi wypada rozpocząć stwierdzeniem Clausewitza: „Zarówno w taktyce jak i w strategii jest przewaga najpoważniejszą zasadą zwycięstwa" – Clausewitz, O wojnie, Wyd. Test, Lublin 1995, s.187.

[4] Przewaga, jej formy i sposoby tworzenia wraz z poglądami teoretyków wojskowych można znaleźć m. in. w zwięzłym opracowaniu akademickim: B.Sikorski, Tworzenie i wykorzystanie przewagi w walce i operacji, AON, Warszawa 1990.

[5] Z. Ścibiorek, Wojna czy pokój?, Ossolineum, Wrocław 1999, s.116.

Jednocześnie, aby utrzymać zdolność do stworzenia przewagi podczas ewentualnego konfliktu nie można dopuścić do obniżania potencjału bojowego poprzez:

- przyjmowanie nieodpowiednich koncepcji i założeń operacyjno – taktycznych,
- obniżanie poziomu kształcenia i szkolenia kadr dowódczo – sztabowych,
- utrzymywanie wadliwych i skostniałych struktur organizacyjnych.[6]

W istotny sposób na możliwość utworzenia przewagi na współczesnym polu walki wpływają również inne czynniki, takie jak poziom zaawansowania technicznego uzbrojenia i środków walki, systemów dowodzenia oraz rozpoznania i łączności.

Warto zauważyć, że na skutek ogromnego postępu w dziedzinie rozwoju techniki i zaawansowaniu technologicznemu, dużemu zróżnicowaniu uległo uzbrojenie. Pojawiły się nowe jego rodzaje a ich możliwości w znacznie większym niż dotychczas zakresie decydują o skuteczności bojowej. Stąd, należy poszukiwać takich współczynników jakości, które w sposób obiektywny pozwoliłyby na ustalenie wpływu czynników trudno mierzalnych na potencjał bojowy zgrupowań wojsk, co w efekcie umożliwiłoby porównanie sił walczących stron.

Przewaga występuje w dwóch kategoriach wartości. Pierwsza, którą można jednoznacznie i łatwo ocenić, policzyć czy zmierzyć to przewaga materialna, wymierna. Druga kategoria, to przewaga niematerialna.[7] Zatem, można mówić o przewadze ilościowej i jakościowej. Pod pojęciem przewagi jakościowej rozumie się przewagę wytworzoną poprzez wykorzystanie czynników trudno mierzalnych.[8] W celu zdobycia przewagi ogólnej należy w planowaniu i prowadzeniu walki uwzględniać i umiejętnie łączyć te dwie kategorie przewagi.

Wartości wymierne, materialne, obejmują czynniki ilościowe. Do zasadniczych czynników materialnych decydujących o wartości bojowej wojsk należy liczebność żołnierzy, uzbrojenia, wyposażenia itp. Ustalenie liczby żołnierzy, ilości związków taktycznych czy operacyjnych, liczby poszczególnych rodzajów uzbrojenia, składów i baz zaopatrzenia pozwala łatwo wyliczyć przewagę według obowiązujących procedur obliczeniowych.[9] Daje to określone pojęcie o sile bojowej wojsk własnych i przeciwnika.

Jednakże, uzyskane wyniki nie w każdym przypadku stanowią o przewadze ogólnej,

---

O problemie tworzenia przewagi w warunkach przyszłego pola walki traktuje praca Z.Ścibiorek, W.Kaczmarek, Przyszłe pole walki, AON, Warszawa 1995, s.54 – 69.

[6] K. Nożko, Sztuka tworzenia przewagi w systemie obronnym RP, Bellona, Warszawa 1994, s.111-116.

[7] J. Zubek, Rozprawa habilitacyjna, dodatek C/8300,AON, Warszawa 1990, s.42-43.

[8] Z. Galewski, Czynniki powodzenia we współczesnej walce, Wyd. MON, Warszawa 1986, s.11 – 12.

[9] patrz: J. Wołejszo, Sposoby obliczania potencjału bojowego pododdziału, oddziału i związku taktycznego, AON, Warszawa 2002.

chociaż pozornie mogłoby się tak wydawać, studiując literaturę na ten temat.[10]

Pomimo tego, że znaczenie przewagi w walce jest ogólnie zrozumiałe to przykłady z minionych i nam współczesnych konfliktów oraz wojen wskazują, że wielokrotnie zdarzało się, że strona która nie dysponowała przewagą ilościową wygrywała lub zadawała przeciwnikowi ciężkie straty. Przykładem jest wojna wietnamska, afgańska czy też konflikt w Czeczenii, w których angażowano ogromne siły, (czołgi, lotnictwo, artylerię) przeciwko siłom niewspółmiernie mniejszym i słabiej wyposażonym, a mimo to nie osiągnięto zakładanych celów. Przykłady te wskazują, że oprócz czynników wymiernych, o sukcesie w walce (bitwie) decydowało wytworzenie oraz wykorzystanie przewagi w wyniku doskonałego przygotowania dowódców i wyszkolenia wojsk, karności i zdyscyplinowania, należytego opracowania planów bitwy i konsekwentnej ich realizacji, umiejętnego wykorzystania terenu, stosowania śmiałych i niekonwencjonalnych form manewru, dążenia do uzyskania zaskoczenia a także utrzymywania wysokiego morale żołnierzy. Współcześnie coraz częściej mamy do czynienia z konfliktami zbrojnymi, gdzie jedna ze stron konfliktu dysponuje ogromną przewagą materialną, setkami tysięcy żołnierzy, nowoczesnym uzbrojeniem i środkami rażenia, potężnym zabezpieczeniem logistycznym, natomiast druga strona posiada kilkunastotysięczną armię słabo uzbrojonych i wyposażonych ochotników, praktycznie bez zaplecza logistycznego. Jednakże, armia ta stawia skuteczny opór wielokrotnie silniejszemu przeciwnikowi, bądź też odwrotnie, słaby przeciwnik odnosi zwycięstwa zadając dotkliwe straty wielokrotnie silniejszej stronie. Z pewnością, o takim stanie rzeczy nie stanowi przewaga materialna. Przyczyn należy raczej poszukiwać w niewykorzystanej (lub źle wykorzystywanej) przewadze materialnej i praktycznie zlekceważonych elementach przewagi niematerialnej. O braku powodzenia, pomimo posiadania przewagi ilościowej zdecydować może, między innymi:

- niski poziom wykształcenia kadry dowódczej, co skutkuje złym wykorzystaniem posiadanych sił w walce,
- brak wyobraźni oraz źle pojmowany a przez to wykorzystywany czynnik świadomego ryzyka,
- rutynowe planowanie operacji i działań bojowych, nie liczenie się ze stratami własnymi oraz bezkrytyczna wiara w posiadaną przewagę liczebną i techniczną,
- brak motywacji żołnierzy do walki oraz ich niskie morale,
- bardzo niski poziom wyszkolenia i przygotowania żołnierzy do działań bojowych,

[10] Przewaga ogólna rozumiana jest tak jak u Z. Galewskiego w książce „Czynniki powodzenia we współczesnej walce", jako „przewaga przewag", tj. zawierająca w sobie wszystkie rodzaje przewag (por. str.11), nie zaś jako przeciwieństwo przewagi lokalnej.

- słabo zorganizowane i nie przystosowane do charakteru działań systemy dowodzenia i zabezpieczenia logistycznego.

Z drugiej strony, na sukces składają się przede wszystkim:

- wysoka wręcz fanatyczna chęć obrony własnej suwerenności i niezależności w połączeniu z fanatyzmem religijnym,
- doskonałe przygotowanie dowódców i żołnierzy (bojowników) do charakteru prowadzonej walki,
- elastyczność w dowodzeniu i prowadzonych działaniach, a przez to częste zaskakiwanie przeciwnika.

Nikt obecnie nie neguje wpływu jaki wywiera nowoczesna technika na osiąganie przewagi na polu walki. Jednakże, w przypadku współczesnych konfliktów militarnych, o przewadze decydują nie tylko systemy broni strategicznych, lecz wpływają na nią bezpośrednie działania bojowe prowadzone przez pododdziały, oddziały i związki taktyczne.

Pomimo ogromnej roli i znaczenia przypisywanego współczesnym środkom walki, wydaje się słusznym stwierdzenie, że o przebiegu walki w równym stopniu decydować będzie dobrze uzbrojony i wyszkolony żołnierz. Stopień przygotowania żołnierzy może mieć zasadniczy wpływ na wielkość przewagi militarnej, szczególnie w przypadku względnie wyrównanych sił przeciwstawnych stron. Wówczas to, możliwym jest osiągniecie przewagi w wyniku pojedynczego uderzenia. Źródła osiągnięcia przewagi w takim przypadku należy upatrywać w nieustannych bezpośrednich działaniach na szczeblach dowódczych i sztabowych.

Przewaga niematerialna wywiera i będzie wywierała w przyszłości ogromny wpływ na tworzenie przewagi ogólnej, a co za tym idzie powodzenie w walce.

Inne spojrzenie na problem przewagi polega na jej podziale na przewagę względną i bezwzględną.[11] Gdy jedna ze stron (nie mając przewagi bezwzględnej) wytworzy przewagę w określonym miejscu (kierunku) lub czasie, zapewniając sobie swobodę manewru i skuteczność działania mówimy o przewadze względnej.[12]

---

[11] S.Mossor, Sztuka wojenna w warunkach nowoczesnej wojny, Wyd. MON, Warszawa 1986, s.208-209.

[12] W ten sposób określają przewagę dwie, spośród pięciu tzw. „zasad napoleońskich" – szerzej w pracy: M.Kukiel, Wojny napoleońskie, Warszawa 1964, s.209.

„Przewaga kierunku", określana jako szczególny rodzaj przewagi uzyskanej w wybranym kierunku działań, pochodzi od analogii siły i kierunku jej działania, tak jak ma to miejsce w mechanice klasycznej.[13]

Analiza doświadczeń historycznych oraz współczesnych bitew i wojen dobitnie potwierdza rolę i znaczenie przewagi uzyskanej przede wszystkim w sferze niematerialnej, która potęguje efekt wartości materialnych. Przewagę w walce, bitwie czy operacji uzyskiwać będzie strona lepiej przygotowana i wyszkolona, mająca lepszych dowódców, dobrze przygotowane sztaby i reprezentująca wyższe morale.[14]

Wartość bojowa współczesnych wojsk w znacznym stopniu polega na wytwarzaniu, przyswajaniu, dystrybuowaniu i stosowaniu wiedzy do celów strategicznych, operacyjnych i taktycznych.

Na współczesnym polu walki czynniki materialne są nośnikami wartości trudno mierzalnych, będących wyrazem jakościowej przewagi nad przeciwnikiem, jak również, wartości trudno mierzalne potęgują i zwielokrotniają siłę elementów materialnych, stanowiąc w sumie o przewadze ogólnej nad przeciwnikiem.

W powyższym stwierdzeniu zawarty jest sens pojęcia wzajemnej substytucji wartości wymiernych i niewymiernych. Wspomniana substytucja stała się podstawą budowy dynamicznego modelu przewagi opisanego w rozdziale siódmym niniejszej rozprawy.

Przewaga ilościowa – jest wielkością wymierną, określana jest zwykle stosunkiem sił własnych do sił przeciwnika lub porównaniem parametrów uzbrojenia przeciwstawnych stron.

Przewagę jakościową rozpatruje się w kategoriach:

- intelektualnej,
- lepszego i skuteczniejszego niż przeciwnik przygotowania i wyszkolenia żołnierzy,
- wyższego poziomu dyscypliny i morale,
- przygotowania psychologicznego (woli walki),
- lepszego wykorzystania w walce posiadanych zasobów.

Przewaga w taktyce polega na lepszymi, skuteczniejszym wykorzystaniu warunków terenowych, pogodowych (również pory dnia), sprawniejszym dowodzeniu oraz umiejętnym stosowaniu zasad sztuki wojennej.

---

[13] Przy okazji warto dodać, że w literaturze przedmiotu, bardzo często można spotkać teorie dotyczące elementów walki zbrojnej, bazujące na analogiach fizycznych. Autorzy tych publikacji starają się, niekiedy za „wszelką cenę" znaleźć tego typu analogie, polegając całkowite na swojej intuicji.
Interesujący, chociaż matematycznie skomplikowany model walki, oparty na kinetycznej teorii płynów oraz równaniach Lanchestera, można znaleźć w książce: P.S.Krasnoszczekow, A.A.Pietrow, Princypy postrojenia modelej, Moskwa 1983, s.233-262.

Do niematerialnych czynników mających wpływ na możliwości bojowe wojsk, zalicza się:

- poziom wyszkolenia wojsk i dowództw,
- stopień gotowości bojowej,
- struktury organizacyjne,
- dyscyplinę,
- umiejętność wykorzystania środowiska walki.

Rzeczywistą wartość bojową jednostek wojskowych w coraz wyższym stopniu kształtuje:

- wiedza dowódców i żołnierzy,
- ich przygotowanie psychologiczne i motywacja,
- ich zdolność do elastycznego reagowania.

Czynniki te mają zasadniczy wpływ na kształtowanie faktycznej wartości bojowej wojsk, a co za tym idzie także możliwości zdobywania przewagi, w przeciwieństwie do ilości posiadanych żołnierzy, czołgów, samolotów i innego sprzętu wojskowego.

Wraz ze zmieniającymi się środkami walki, rośnie rola przygotowania człowieka do ich odpowiedniego użytkowania i właściwego zastosowania w ewentualnej walce. Oczywiście, nawet największa przewaga intelektualna dowódców i żołnierzy będzie nieskuteczna, przy przestarzałym technicznie, niesprawnym uzbrojeniu wojsk, zacofanym systemie dowodzenia.

W realiach współczesnych, armia potrzebuje żołnierzy z „otwartym umysłem", potrafiących porozumiewać się z przedstawicielami innych narodów i kultur, którzy przejmując inicjatywę, wykazują twórczą wyobraźnię pozwalającą na wyjście poza wytyczone dotychczas ramy.

W wojsku, wraz z postępem technicznym i wprowadzeniem do uzbrojenia nowoczesnych (inteligentnych) systemów uzbrojenia, wzrosło zapotrzebowanie na inteligentnych i doskonale wykształconych żołnierzy. Żołnierz niewykształcony mógł wzorowo posługiwać się i walczyć prostą bronią, a jego wyszkolenie i przygotowanie do walki nie pochłaniało dużo czasu i nie było skomplikowane.

Poziom, a co za tym idzie i koszt, wyszkolenia współczesnych żołnierzy jest znacznie wyższy niż w okresach wcześniejszych. Podczas drugiej wojny światowej młodych żołnierzy włączano do walki niejednokrotnie po kilku godzinach czy dniach ćwiczeń. Obecnie czas trwania szkolenia, w zależności od specjalności trwa od kilkunastu miesięcy do kilkunastu lat i wymaga poniesienia ogromnych nakładów.

W kształceniu kadr dowódczych zwraca się obecnie uwagę na podnoszenie poziomu wiedzy specjalistycznej i ogólnej, w tym umiejętności samodzielnego myślenia,

---

[14] Z. Galewski, Czynniki powodzenia we współczesnej walce, Wyd. MON, Warszawa 1986, s.62 - 65.

a także kształtuje się takie zdolności jak wyobraźnię, podejmowanie ryzyka, umiejętność przewidywania.[15] Jak widać, są to wartości trudno mierzalne, pozostające w sferze psychiki i kształtujące osobowość każdego człowieka. Już w okresie drugiej wojny światowej dużą wagę przywiązywano do zbierania, analizowania informacji o osobowości poszczególnych dowódców, ich przyzwyczajeniach i innych cechach charakteru. Pozwalało to z większym prawdopodobieństwem przewidzieć sposoby ich działania, a co za tym idzie, znaleźć skuteczne metody przeciwdziałania.

Właściwe wykorzystanie i kształtowanie przewagi na polu walki zależy od tego jak dużą rolę przypisuje się wyobraźni taktycznej dowódców i żołnierzy, gdyż jej brak staje się często przyczyną nieskutecznego działania. Aby wyobraźnia była twórcza musi być poparta rzetelną wiedzą o przedmiocie, o celu przygotowywanych i prowadzonych działań. Bez tego jest ona złudna, może prowadzić do błędnych ocen oraz realizacji walki w sposób szablonowy. Posiadanie wyobraźni przez dowódców, oficerów sztabów warunkuje podjęcie optymalnych decyzji i wyboru takich sposobów prowadzenia walki, których nie przewidzi przeciwnik. Wyobraźnia pozwala również uniknąć zaskoczenia ze strony przeciwnika, utworzyć spójny obraz całości z drobnych, często oderwanych elementów oraz daje jasność i możliwość elastycznego oddziaływania podczas prowadzenia walki.

W ocenach i procesach decyzyjnych potrzebne są obiektywizm i rozwaga, umiejętność właściwej oceny sytuacji własnej i przeciwnika. Żadna zasada sama w sobie nie jest „przepisem" na uzyskanie przewagi, jeżeli dowódca (żołnierz) nie potrafi przetworzyć w swojej wyobraźni całego splotu zdarzeń i czynników związanych z konkretną lub przewidywaną sytuacją taktyczną. Wynika stąd, że im bardziej jest rozwinięta wyobraźnia dowódcy tym większe jest prawdopodobieństwo stworzenia przewagi nad przeciwnikiem i racjonalnego jej wykorzystania w danej sytuacji taktycznej.

Podczas drugiej wojny światowej niemal każdy dowódca, w mniejszym lub większym stopniu mógł obserwować i wpływać na przebieg rozgrywającej się walki. We współczesnych realiach nie zawsze jest to możliwe, gdyż charakter prowadzenia działań bojowych staje się wielowymiarowy. Obecnie, dowódcy i oficerowie sztabu „obserwują" przebieg działań i obraz pola walki za pomocą kamer, ekranów komputerów, bądź analizując wyniki obserwacji zebrane np. w postaci wykresów. Dowódcy planujący walkę powinni umieć odtwarzać w swojej wyobraźni jej przebieg na podstawie niepełnych, często fragmentarycznych danych, przedstawianych na mapie (coraz częściej mapie cyfrowej) za

---

[15] K. Nożko, Walka o przewagę, Wyd. MON, Warszawa 1985, s.55-103.

pomocą znaków taktycznych.[16] Powinni oni również zdawać sobie sprawę, że każdy znak czy symbol taktyczny na mapie, w terenie przedstawia rzeczywistych ludzi i sprzęt bojowy, a od właściwego użycia tych znaków zależy życie i zdrowie żołnierzy.

Na podstawie znaków taktycznych w wyobraźni odtwarzany jest dynamizm działań bojowych na określonym obszarze. W zależności od zarysu sytuacyjnego wyrażonego umownymi znakami, dowódca wczuwa się w sytuację już istniejącą lub tę, która może dopiero zaistnieć. Rola wyobraźni taktycznej jest nieoceniona. Wyobraźnia służy do plastycznego i wyrazistego przedstawienia istniejących lub przewidywanych warunków pola walki oraz sposobów tworzenia własnej przewagi a pozbawiania jej przeciwnika. Obejmuje ona kompleks wyobrażeń o różnorodnych zjawiskach współczesnego pola walki, a także możliwości skutecznego wpływania na przebieg wydarzeń. W rozwijaniu wyobraźni coraz większą rolę odgrywa rzetelna wiedza, wszechstronna znajomość obiektywnie działających praw wojny, zasad jej prowadzenia, rozwoju techniki i technologii oraz umiejętność wykorzystania wszelkiego typu symulacji do badania przyjętych koncepcji operacyjno – taktycznych.[17]

Prowadzenie walki związane jest z podejmowaniem ogromnego ryzyka. Każda decyzja dowódcy, oceny, przedsięwzięcia organizacyjne i planistyczne sztabu zawierają elementy ryzyka. Jest to ogromna odpowiedzialność za życie i zdrowie podwładnych, ludności cywilnej zamieszkującej w obszarze prowadzonych walk, straty w sprzęcie uzbrojenia, zniszczenia środowiska naturalnego, a w rezultacie za wynik prowadzonych działań bojowych.

W przeszłości, wielu dowódców podejmowało ryzyko, często graniczące z brawurą, które prowadziło do spektakularnych sukcesów, niekiedy kończyło się również dotkliwymi porażkami.

Dlatego, podczas podejmowania ryzyka w walce należy uwzględnić, że:

- zostanie ono podjęte z całą świadomością, a opierać się musi nie tylko na wyczuciu, wiedzy i doświadczeniu ale i na wszechstronnych kalkulacjach możliwości wojsk własnych i przeciwnika,
- podejmując określone ryzyko, przynajmniej w przybliżeniu, musimy zdawać sobie sprawę z jego konsekwencji zarówno w razie sukcesu jak i braku powodzenia.

Ze zjawiskiem podejmowania ryzyka wiąże się trudny problem ustalenia dopuszczalnej jego granicy. Granica ta powinna być wynikiem chłodnej kalkulacji zysków i strat związanych z podjęciem konkretnych decyzji.

---

[16] Z. Ścibiorek, Wojna czy pokój?, Ossolineum, Wrocław 1999, s.64.
[17] K. Nożko, Sztuka tworzenia przewagi w systemie obronnym RP, Warszawa 1994, s.118 – 136.

W celu uzyskania przewagi w walce, ważną rolę odgrywają przewidywania operacyjno – taktyczne. Nie sposób bowiem uzyskać przewagę nad przeciwnikiem i to we wszystkich jej kategoriach, bez trafnego przewidzenia właściwości, charakteru i sposobu przeprowadzenia przygotowywanych przez niego działań. Przewidywania operacyjno – taktyczne odgrywają ważną rolę w ocenie skutków podjętych decyzji, w jaki sposób dana decyzja wpłynie na osiągnięcie celu walki oraz skutków jakie wywrze na działanie lub przeciwdziałanie przeciwnika. Przewidywanie to można sprowadzić do znalezienia odpowiedzi na następujące pytania:

- Jaki może być skład organizacyjny, rzeczywiste ugrupowanie, siły, możliwości oraz sposoby działania przeciwnika.
- Jakie mogą być silne i słabe strony w jego ugrupowaniu, siłach, położeniu lub sposobie działania wojsk.
- Jaki może być cel i zamiar działania przeciwnika oraz w jaki sposób może rozwinąć
  się w czasie dana sytuacja taktyczna.
- Jakie mogą być skutki podjętych obustronnie decyzji, kiedy, gdzie i jakie mogą wyniknąć sytuacje kryzysowe oraz w jaki sposób im zapobiegać.
- Jak na przebieg walki wpływać będzie infrastruktura i właściwości terenu, pora roku lub doby.[18]

Przewidywania operacyjno – taktyczne są niezbędnie i mają zasadniczy wpływ na szybkość działania (przeciwdziałania) wojsk w walce.

Koncentracja sił i środków oraz skupienie wysiłków na wykonaniu zadań decydujących o powodzeniu, bądź też rozstrzygających o osiągnięciu celu walki, stanowi istotny element tworzenia i racjonalnego wykorzystania przewagi. W przeszłości realizowano to poprzez gromadzenie dużych sił na wybranym kierunku działania. Przy współczesnych środkach rozpoznania trudno jest zamaskować ogromne zgrupowanie wojsk w jednym rejonie. Koncentrację sił realizuje się raczej poprzez wykorzystanie ich dużej mobilności, która zapewnia skierowanie w określony rejon wymaganej ilości sił w krótkim czasie. Zasadę koncentracji sił na wybranych kierunkach stosują przede wszystkim te strony konfliktu które nie będą posiadały przewagi ogólnej. Skumulowanie działań w celu uzyskania przewagi na określonym, taktycznym odcinku walki pozwala, w wielu wypadkach, na późniejsze osiągnięcie przewagi bezwzględnej.

Większość z wymienionych czynników zapewniających osiągnięcie przewagi w walce zależy od przygotowania dowódców i sztabów do właściwego planowania i prowadzenia

---

[18] tamże s.155 – 156.

walki a także umiejętności szybkiego dostosowywania się do zmieniających się warunków i odpowiedniego na nie reagowania.

Wpływ czynników niematerialnych na kształtowanie przewagi jest zagadnieniem złożonym. Wielu autorów publikacji na ten temat, widzi ten problem odmiennie. Przykładowo, Alvin i Heidi Toffler, rozwój środków i sposobów prowadzenia walki porównują z rozwojem nowego światowego porządku gospodarczego. Do zasadniczych cech prowadzenia nowych wojen zaliczają:

- czynniki zniszczenia,
- wartości niematerialne,
- odmasowienie,
- pracę,
- innowację,
- skalę,
- organizację,
- infrastrukturę,
- integrację systemów,
- przyspieszenie.

Pisząc o wartościach niematerialnych podkreślają oni ich znaczenie w prowadzeniu wojen, jednak nie dokonują ich wyszczególnienia. Omawiając czynniki zniszczenia, nie negują roli środków walki lecz podkreślają znaczenie wiedzy w prowadzeniu walki. *„Rewolucją staje się umiejscowienie różnych postaci wiedzy jako rdzenia siły militarnej"*[19] . Powołując się na wypowiedź Alana D. Campena, że „Wojna w Zatoce Perskiej była wojną w której uncja krzemu w komputerze przynosiła większe efekty niż tona uranu", wysuwają tezę że, wiedza znacznie zmniejsza potrzebę innych czynników, a jednym ze wskaźników rosnącego znaczenia wiedzy w sposobie prowadzenia wojen jest komputeryzacja. W rzeczywistości, wojna w Zatoce Perskiej była pierwszą wojną informacyjną.[20] Opisując czynniki niematerialne generalnie A.H. Toffler potwierdzają ich rosnące znaczenie dla osiągnięcia przewagi militarnej, szczególną uwagę zwracając na inicjatywę, lepszy wywiad i rozpoznanie, lepsze systemy porozumiewania się i łączności, lepsze wyszkolenie żołnierzy o silniejszej motywacji, czyli czynniki wymienione wcześniej. Podkreślają również

---

[19] A i H. Toffler, Wojna i antywojna, Warszawa 1997, s.100 - 101.

[20] O znaczeniu informacji w wojnie w Zatoce Perskiej piszą: T.Goban-Klas, P.Sienkiewicz, Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania, Wyd. Fundacji Postępu Telekomunikacji, Kraków 1999, s.79.
W tym miejscu trzeba jednak zwrócić uwagę na fakt, że zdania teoretyków wojskowych (także amerykańskich) co do wagi doświadczeń z wojny w Zatoce Perskiej są mocno podzielone. „ ... nie należy traktować wojny w Zatoce Perskiej jako prototypu wszystkich wojen przyszłości ..." – B. Balcerowicz, Wybrane problemy obronności państwa, materiał studyjny, AON, Warszawa 1999, s.38 za S.Metz i inni, The Future of American Landpower SSI, Carlise Barrack 1996, s.16.

fakt, że w chwili obecnej brak jest wiarygodnych opracowań uwzględniających czynniki trudno mierzalne, a najbardziej autorytatywne z nich, „The Military Balance" skupia się na podawaniu „suchych wskaźników" dotyczących liczby i rodzaju posiadanego przez dane państwo uzbrojenia. Sposoby jakimi mierzy się współcześnie wartość nie przystają już do nowych warunków. W odmasowieniu natomiast upatrują pole do rozwoju „inteligentnych" środków walki, gdzie do zniszczenia indywidualnego celu będzie dobierany indywidualny środek zniszczenia. Przemysł zbrojeniowy konstruuje pociski samosterujące które potrafią zidentyfikować i zniszczyć dowolny cel. Celem rozwojowym jest coraz większa precyzja i selektywność produkowanych systemów uzbrojenia.

We współczesnej walce, od dowódców, sztabów a nawet pojedynczych żołnierzy wymaga się przejawiania wysokiego stopnia inicjatywy własnej w rozwiązywaniu problemów. Związane jest to z niekonwencjonalnym podchodzeniem do określonych już zasad oraz szukaniem nowych sposobów wykonania postawionych zadań. Wymaga to jednak umiejętności połączenia i wykorzystania wielu czynników oraz znajomości sposobów prowadzenia nowoczesnej walki. Inwencja dowódców i żołnierzy pozwoli wykorzystać środki podręczne do prowadzenia lub skutecznego wsparcia walki.

Zmienia się również organizacja. Dużą wagę przykłada się do stworzenia określonych struktur organizacyjnych i ich przystosowanie do aktualnych uwarunkowań pola walki. Rośnie znaczenie umiejętności wykorzystania posiadanych sił i środków stosownie do otrzymanego zadania.

Zmianie ulega także skala prowadzenia współczesnych działań bojowych. Zmiany te zachodzą wskutek odmiennego podejścia do charakteru i sposobów prowadzenia przyszłych wojen. Coraz częściej słyszy się, że bardziej skuteczne w przyszłej walce będą pododdziały małe ale za to doskonale wyposażone i uzbrojone.

Ogólna tendencja zmierza ku takim rozwiązaniom systemów uzbrojenia, które dysponowałyby większą siłą rażenia przy mniejszej liczbie ludzi obsługujących te systemy.

W przeszłości wojna sprowadzała się do przeprowadzenia jednej lub kilku bitew, które decydowały o przegranej lub zwycięstwie jednej ze stron.

Współcześnie prowadzone są wojny w wielu równoległych wymiarach, dostrzeżonych dopiero po drugiej wojnie światowej. Prowadzone są wojny radioelektroniczne i coraz bardziej prawdopodobne jest zwiększenie ich nasilenia i znaczenia w przyszłości ze względu na ogromne nasycenie współczesnych środków walki elektroniką, zniszczenie czy zakłócenie której powoduje że staną się one bezużyteczne. Nasycenie środków walki wyposażeniem elektronicznym oraz postępująca ich automatyzacja i autonomiczność powoduje, że wielu

dowódców mówi wręcz o automatyzacji pola walki. Współczesne środki walki są tak nasycone podzespołami elektronicznymi że często mamy do czynienia z zastosowaniem robotów do prowadzenia walki.

W wielu wypadkach uwaga dowódców skupiała się na gromadzeniu wielokrotnie liczebniejszych sił w stosunku do przeciwnika, przy jednoczesnym ignorowaniu innych czynników jak wyszkolenie żołnierzy oraz ich wartości moralno – bojowe. Nie zawsze też brano pod uwagę stan psychiczny żołnierzy. Zakłada się, że po okresie trzydziestu dni intensywnych działań z użyciem konwencjonalnych środków rażenia, stosunek strat psychicznych do strat fizycznych w sile żywej (zabitych i rannych) wynosi 1 : 4. Często, mniejsze liczebnie siły odnosiły zwycięstwa dzięki lepszemu ich wykorzystaniu, w wyniku zastosowania przez dowódców skuteczniejszej taktyki działania, sposobów walki, fortelu, szybkości działania lub innych zabiegów zapewniających uzyskanie przewagi. [21]

Niskie morale i słaba odporność psychiczna są bez wątpienia czynnikami, które utrudniają skuteczne prowadzenie działań bojowych i często wręcz uniemożliwiają pokonanie przeciwnika. Stąd, jedną z podstawowych czynności walki zbrojnej powinno być dążenie do podnoszenia odporności psychicznej walczących żołnierzy oraz ich dowódców.

Współczesne działania bojowe charakteryzuje przede wszystkim duża dynamika przejawiająca się różnymi formami ruchu fizycznego którego podstawową formą na polu walki jest manewr. Manewr jest zorganizowanym przemieszczeniem wojsk na polu walki w celu zajęcia dogodniejszego położenia względem przeciwnika, uzyskania i wykorzystania przewagi.[22]

Największy manewr wykonany został przez Armię Radziecką w 1945 r. w celu zgrupowaniu sił i środków do walki z japońską Armią Kwantuńską[23]. Manewr tego typu stanowi obecnie historię i raczej nigdy się nie powtórzy. Inny przykład manewru obserwowano w operacji wojsk sprzymierzonych w Zatoce Perskiej w lutym 1991r. Głównym założeniem planu gen. N.H. Schwarzkopfa było unieruchomienie armii irackiej atakiem frontalnym jednej armii Sprzymierzonych, przy jednoczesnym wykonaniu przez jeszcze większa armię manewru oskrzydlenia, okrążenia, a w rezultacie przyparcia do morza. Manewr stanowi wyjątkowo ważny, niekiedy decydujący czynnik uzyskiwania przewagi nad przeciwnikiem i racjonalnego jej wykorzystania. Istota manewru polega na zdobyciu przewagi nad przeciwnikiem, głównie przez zorganizowany ruch, w celu stworzenia dogodnych warunków do skuteczniejszego użycia posiadanych sił i środków, wykonania

---

[21] Z. Ścibiorek, Wojna czy pokój, Ossolineum, Wrocław 1999, s.11.
[22] J. Zieliński , Teoretyczne podstawy walki zbrojnej, W-wa 1995, s.39.
[23] K. Nożko, Walka o przewagę, W-wa 1985, s. 165.

nieoczekiwanego uderzenia lub celowego wykorzystania warunków topograficzno-geograficznych terenu, a przez to postawienia przeciwnika w niekorzystnej dla niego sytuacji i w efekcie – rozstrzygnięcia walki lub bitwy na swoją korzyść przy jednocześnie minimalnych stratach własnych. W literaturze przedmiotu czytamy na ten temat między innymi: *„We wszystkich zaczepnych formach starcia zbrojnego celem zastosowania manewru jest osiągnięcie jakiegoś rodzaju przewagi nad przeciwnikiem. Nie oznacza to przy tym zawsze konieczności doprowadzenia do koncentracji w określonym czasie i w określonym punkcie terenu większej niż po stronie przeciwnika liczby pocisków, żołnierzy, sprzętu. Moment przewagi, do której prowadzi manewr, polega m.in. na zaskoczeniu, a przede wszystkim na zajęciu, w stosunku do przeciwnika takiego położenia w terenie, które by (rozpatrywane w sensie geometrycznym) stawiało go – zarówno w znaczeniu fizycznym, jak i psychicznym – w możliwie najtrudniejszych warunkach".*[24]

Zatem, przez celowe wykonanie manewru można spotęgować siłę uderzenia, zaskoczyć przeciwnika, uchwycić inicjatywę i narzucić mu własny sposób działania, jak również w wielu sytuacjach można poprzez manewr uniknąć zniszczenia własnych sił głównych. Można to osiągnąć wyprowadzając umiejętnie własne siły spod uderzenia ogniowego lub uderzeń zgrupowań przeciwnika a następnie wykorzystać je w dogodniejszych warunkach, w innym czasie, gdzie istnieje możliwość uzyskania przewagi nad przeciwnikiem.

K. Nożko pisze o przemieszczaniu się punktu ciężkości przewagi, a wszystko to za sprawą manewru.[25] Przytoczony wyżej opis manewru i celowości jego stosowania świadczy o powiązaniu kierunku działań z przewagą, a co za tym idzie, wielkością potencjału bojowego. Możliwe zatem staje się wyznaczenie kierunku maksymalnego potencjału bojowego. Współgra to z koncepcją postrzegania potencjału bojowego przez pryzmat pola skalarnego. Wyznaczenie właściwych (przynoszących sukces) kierunków działań bojowych, to nic innego jak określenie „powierzchni ekwipotencjalnych" (analogia do fizycznego pola skalarnego). Określenie kierunku działań to określenie maksymalnego gradientu potencjału bojowego.[26] Jest to jednocześnie, określenie sposobu kreowania przewagi ogólnej nad przeciwnikiem[27]. Pole skalarne stanowiące odzwierciedlenie danej sytuacji bojowej ma

---

[24] F. Skibiński, Rozważania o sztuce wojennej, Warszawa 1972, s.270.

[25] K. Nożko, Sztuka tworzenia przewagi w systemie obronnym RP, Bellona, Warszawa 1994, s.223.

[26] próbę takiego ujęcia potencjału bojowego przedstawił autor niniejszego opracowania w swojej pracy Metodyka Oceny Potencjału Bojowego Sił Zbrojnych RP problem naukowy „Doskonalenie II", AON, Warszawa 1992. W tym miejscu, należy się pewne wyjaśnienie, otóż podobnie jak wielu innych autorów, tak i piszący te słowa, próbował zastosować, „elegancki", model fizyczny do opisu zjawisk pola walki. Z koncepcji tej jednak w następnych latach zrezygnowano głównie z powodu trudności obliczeniowych, adaptacyjnych i interpretacyjnych.

[27] Przewaga ogólna – jest to przewaga występująca na całym obszarze działania danej jednostki organizacyjnej Z.Galewski, Czynniki powodzenia we współczesnej walce, Warszawa 1986, s.11.

również swoje uzasadnienie w istocie aktywności na polu walki. Aktywność (inicjatywa) oznacza nieustanne dążenie do narzucenia przeciwnikowi swojej woli i swoistego sterowania jego działaniami w myśl własnych celów i zamierzeń.[28]

Nie sposób w tym miejscu nie odnieść się również do szeregu stwierdzeń, zaczynających się słowami: „Na podstawie analiz przeszłych wojen i konfliktów zbrojnych można stwierdzić, że ...".[29] Panuje raczej powszechna zgodność, że konflikty I i II wojny światowej nie stanowią dobrych wzorów do naśladowania, doświadczenia tamtego okresu, w dzisiejszych działaniach bojowych są nieprzydatne. Współcześnie, najbardziej prawdopodobny jest wariant konfliktu małej i średniej intensywności o zasięgu lokalnym. Przed nami stają nowe wyzwania i jakościowo inne zagrożenia. Istnieje potrzeba budowy nieklasycznych modeli.[30]

Współczesną walkę zbrojną cechuje niespotykany rozmach, dynamika działań oraz nagłe i gwałtowne zmiany sytuacji operacyjno-taktycznej na lądzie, w powietrzu i na morzu. Wynika to z intensywności i zdecydowanego charakteru działań prowadzonych przez różne rodzaje wojsk i sił zbrojnych. W ich wyniku można stosunkowo szybko wywalczyć przewagę nad przeciwnikiem, zaskoczyć go, uprzedzić w działaniu, zmusić do prowadzenia walki w niekorzystnych dla niego warunkach. Aktywne i zdecydowane działania nie tylko zapewniają zdobycie przewagi, lecz przyczyniają się do jej utrzymania oraz potęgowania. Szczególnym wyrazem aktywności w tworzeniu przewagi nad przeciwnikiem jest walka o uzyskanie inicjatywy i ciągłe dążenie do jej utrzymania oraz narzucenia przeciwnikowi swojej woli i sposobu działania. Wyraża się ona m.in. w umiejętności wyboru ekonomicznych form oraz sposobów działania operacyjno-taktycznego, a także we właściwym ich stosowaniu.[31]

Innym elementem stymulującym przewagę jest zaskoczenie. Zaskoczenie wyraża się w nieoczekiwanym, nagłym i gwałtowanym dla przeciwnika działaniu, wskutek którego zostaje on pozbawiony inicjatywy bojowej oraz możliwości zorganizowanego prowadzenia walki.[32] Zaskoczenie zawsze stanowiło niezwykle ważny czynnik tworzenia ogólnej przewagi

---

[28] Regulamin działań wojsk lądowych, Warszawa 1999, s.82.

[29] Kilka przykładów historycznych można znaleźć w opracowaniu akademickim: E.Gwóźdź, Pojęcie przewagi i jej tworzenie na przykładach historycznych, AON, Warszawa 1972.

[30] B. Balcerowicz, Wybrane problemy obronności państwa, materiał studyjny, AON, Warszawa 1999, s.39.

[31] *„Rola przewagi wynika z potrzeby przeciwdziałania powietrzno-lądowemu charakterowi działań zaczepnych, a tym samym konieczności prowadzenia aktywnych działań w całym operacyjnym obszarze odpowiedzialności obronnej – w wymiarze przestrzennym. Wymusza to przygotowanie operacji obronnej głęboko urzutowanej, prowadzonej ze względu na znaczny obszar sposobem ogniskowym, kierunkowym lub kombinowanym. Jednak, głębokie urzutowanie wojsk dla utrzymania trwałości operacji obronnej, to nie liczba rozbudowanych rubieży (rejonów). To przede wszystkim ekonomiczne gospodarowanie siłami, powietrzno-lądowy i przestrzenny charakter operacji obronnej, manewrowość sił i środków, możliwość precyzyjnego oddziaływania ogniowo-elektronicznego oraz integralne połączenie statycznych i dynamicznych form jej prowadzenia."* – R.Bojarski, Operacja obronna, AON, Warszawa 1999, s.22.

[32] Regulamin działań wojsk lądowych, Warszawa 1999, s.12.

nad przeciwnikiem. *Celem zaskoczenia jest uzyskanie przewagi nawet nad liczebnie silniejszym przeciwnikiem przez sparaliżowanie woli jego działania i tym samym pozbawienie go zdolności do stawiania zorganizowanego oporu podczas realizacji własnych zamierzeń. W wyniku zaskoczenia zwiększa się siłę własnego uderzenia, zwłaszcza w początkowym okresie działań od 1,5 do 2 razy, a niekiedy znacznie więcej.*[33]

Zaskoczenie wydaje się być najlepszym przykładem wagi czynników niematerialnych w procesie tworzenia przewagi. Zaskoczenie osiągane jest w sposób różnorodny. Jego źródłem może być zarówno manewr jak i ekonomia sił. Trzy zasady walki: zaskoczenie, manewr i ekonomia sił, wzajemnie się przenikają i uzupełniają. Stąd, można powiedzieć, że efektem manewru winno być zajęcie zaskakującego, korzystnego położenia w stosunku do przeciwnika, umożliwiającego ekonomiczne użycie własnych wojsk. Zaskoczenie jest działaniem pozamaterialnym, dającym efekty w postaci przewagi materialnej. Historia bitew wskazuje, że zaskoczenie to jedna z najstarszych i najczęściej stosowanych zasad walki. Jednakże, nie zawsze zasada ta znajdowała zastosowanie. Działo się tak z wielu powodów. Między innymi, z jednej strony zmianom ulegały poglądy dowódców zaś z drugiej strony, zmieniały się środki walki. W czasach starożytnych, w podstępach i fortelach dominowały ludy azjatyckie, natomiast w Europie (zwłaszcza w Grecji) dobre uzbrojenie i wyćwiczone reguły walki. Postępujący stopniowo rozwój w dziedzinie sztuki wojennej zmierzał w kierunku zwiększenia manewrowości z jednej strony oraz wzrostu możliwości rażenia, z drugiej strony. Niestety, wielu dowódców dostrzegało tylko drugi aspekt i preferowało rozwiązania siłowe nad kunszt walki.

Racjonalnie działać i odnosić zwycięstwo w każdej walce zbrojnej, oznacza, że kosztem jak najmniejszych strat własnych, trzeba poznać istotę przewagi zarówno własnej, jak i przeciwnika, określić kryteria jej oceny i znaczenie dla obu przeciwstawnych stron, ustalić mechanizmy, które pozytywnie i negatywnie wpływają na procesy jej kształtowania, zbadać zmienne wartości przewagi, zwłaszcza te, które warunkują powodzenie w działaniach wojennych, a następnie podjąć zabiegi w celu odpowiedniego jej wykorzystania.
Tego typu „przepisy" na uzyskanie przewagi dostarcza nam literatura przedmiotu. Pozostaje jedynie problem analitycznego (jeśli to tylko możliwe!) ujęcia tych kategorii w postaci modelu matematycznego.

---

[33] K.Nożko, Walka o przewagę, Bellona, Warszawa 1985, s.131.

2.3. INFORMACJA W PROCESIE TWORZENIA PRZEWAGI

Analiza czynników mających wpływ na wielkość przewagi wskazuje jednoznacznie na potrzebę wyodrębnienia dwóch kategorii:

- czynników stymulujących przewagę (wpływających na wzrost przewagi),
- czynników wpływających destrukcyjnie (obniżających wartość przewagi).

Wyróżnione wyżej kategorie czynników reprezentowane są w proponowanym modelu przewagi odpowiednio przez współczynniki α i β. Na oba rodzaje współczynników α i β składają się czynniki wymierne (ilościowe) i niewymierne bądź trudno mierzalne (jakościowe). Wzrost przewagi nad przeciwnikiem można jednoznacznie określić poprzez obliczenie stosunku sił walczących stron w kolejnych fazach konfliktu. Stosunek sił walczących stron jest zmienny w czasie, a jego wartość odzwierciedla wpływ współczynników α i β na przebieg walki. Od właściwego określenia tych współczynników zależy wiarygodność otrzymanych wyników.

Rozpatrując walkę zbrojną nie sposób pominąć głównych jej czynników. Przypomnijmy te czynniki wskazując jednocześnie na wyraźny ich podział na dwie grupy.
Do elementarnych czynników walki zbrojnej na szczeblu taktycznym zaliczamy:

- rażenie,
- ruch,
- informację.[34]

Według zasad obowiązujących w NATO, klasyfikacja czynników walki jest nieco inna: do głównych elementów walki zalicza się rażenie i ruch, zaś czynnikami walki są siły, obszar i czas.[35] Regulamin działań wojsk lądowych podaje elementarne czynniki operacyjne, są to: siły, obszar, czas i informacja. Czynniki te mają zgoła inny charakter niż w działaniach taktycznych. Wynika to z odmiennej roli jaką w obu rodzajach działań spełnia cel, czas i miejsce działania sił. Większość decyzji do działań operacyjnych będzie podejmowanych na podstawie niepełnych informacji, stąd miejsce informacji w elementarnych czynnikach operacyjnych.[36]

Oprócz podstawowych czynników walki występują czynniki złożone. Złożone czynniki walki powstają poprzez łączenie czynników podstawowych. Oznacza to, że w rzeczywistości

---

[34] S.Koziej, Podstawy i zasady sztuki wojennej, Warszawa 1993, s.100.
[35] M.Wiatr, Działania operacyjne według poglądów NATO, Warszawa 1988, s.21.
[36] Regulamin działań wojsk lądowych, Warszawa 1999 s.11.

nigdy nie mamy do czynienia tylko z jednym „czystym" czynnikiem walki. Jest to dodatkowy powód poszukiwania zagregowanych współczynników α i β, o których jest mowa wyżej.

Rażenie jest to bezpośrednie destrukcyjne, fizyczne, psychologiczne lub informacyjne oddziaływanie na siły i środki przeciwnika.

Rażenie dzielimy na :

- rażenie ogniowe,[37]
- rażenie elektroniczne,
- rażenie psychologiczne.

Rażenie ogniowe jest całkowicie pozbawione trudno wymiernego czynnika jakościowego.[38]

W przypadku rażenia elektronicznego czynnik ten zarysowuje się na tyle intensywnie na ile intensywne będą działania tego typu. Rażenie psychologiczne zawiera w sobie całkowicie czynnik jakościowy, zupełnie przeciwnie do rażenia ogniowego.

Rażenie elektroniczne jest to działalność prowadzona za pomocą sił i środków radiowych oraz radiolokacyjnych, której celem jest paraliżowanie systemów informacyjnych przeciwnika, zwłaszcza jego elementów rozpoznania i dowodzenia.

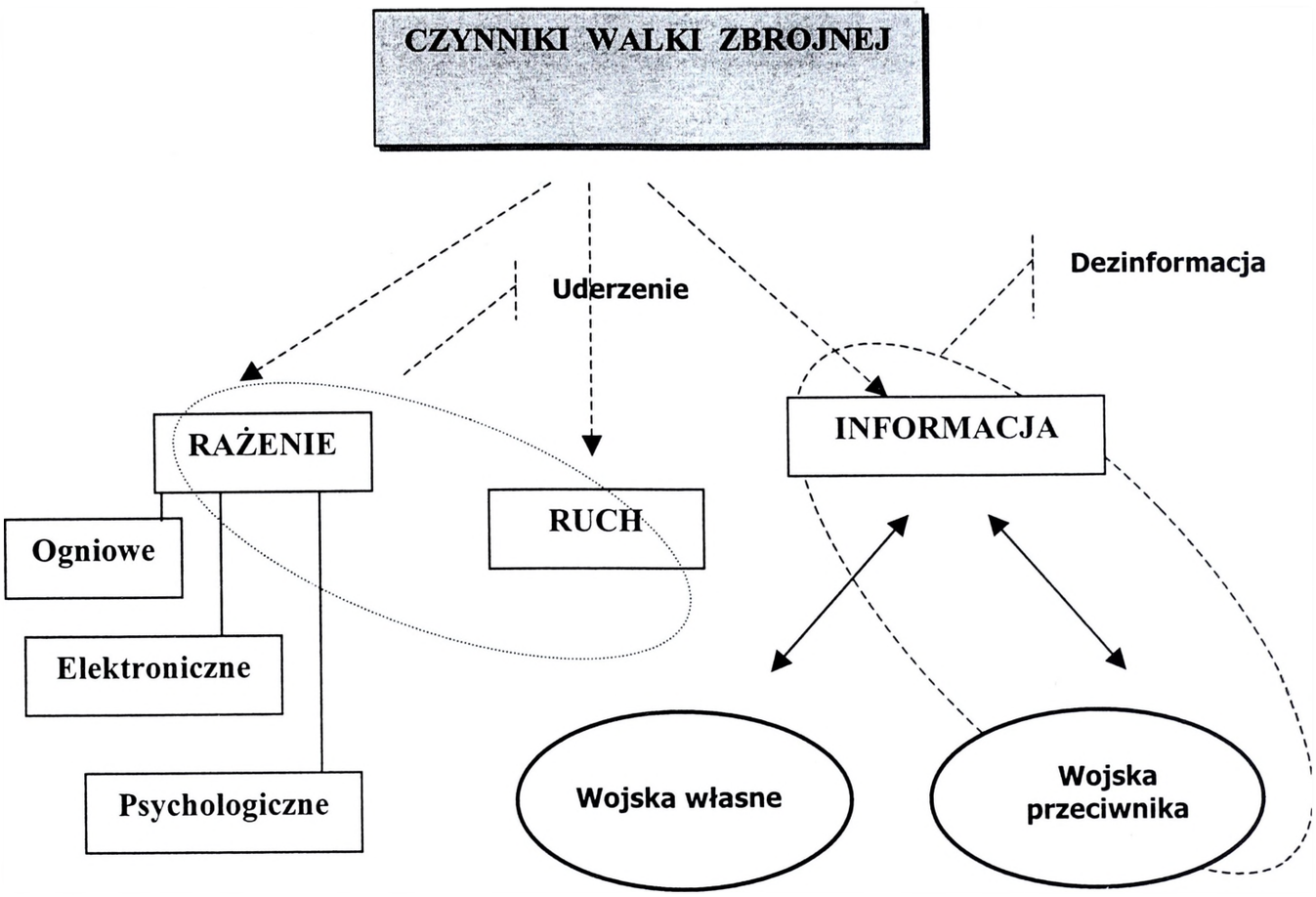
Rażenie psychologiczne jest to oddziaływanie na przeciwnika w taki sposób aby osłabić jego wolę walki i utwierdzić go w przekonaniu, że działania zbrojne które prowadzi są bezcelowe i nie przyniosą pożądanego efektu.

---

[37] O przewadze ogniowej traktuje między innymi opracowanie: Cz. Jarecki, Przewaga ogniowa warunkiem powodzenia działań zaczepnych. Sposoby jej uzyskania i utrzymania, AON, Warszawa 1992.

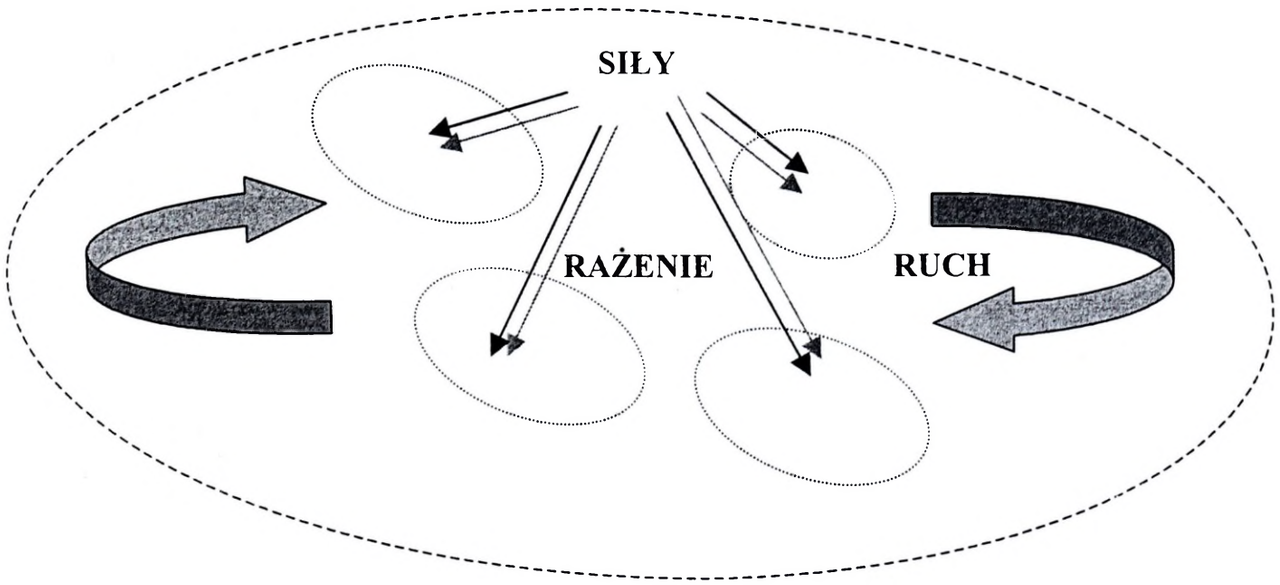
[38] Rażenie ogniowe to :

- ogień bezpośredni pododdziałów piechoty i czołgów
  - umożliwia realizację zadań taktycznych,
  - zapewnia zniszczenie lub obezwładnienie sił żywych i środków walki przeciwnika znajdujących się bezpośrednio w zasięgu obserwacji i ognia,
  - mocno powiązany jest z właściwościami terenu,
- ogień środków wsparcia
  - ogień artylerii,
  - uderzenia rakietowe i lotnicze,
  - działalność innych środków rażenia np. inżynieryjnych (ze względu na zakres zadań i cel działalności ogniowej wsparcie ogniowe dzielimy na: bezpośrednie i ogólne),
- ogień środków obrony powietrznej
  - ciągłe rozpoznanie przestrzeni powietrznej,
  - działalność ogniowa wojsk lotniczych i obrony powietrznej,
  - działalność specjalistycznych oddziałów i pododdziałów obrony plot. wojsk lądowych i MW,



Rys.2.2. Czynniki walki zbrojnej.

Źródło: opracowanie własne.



Rys.2.3. Elementy i czynniki walki wg poglądów NATO.

Źródło: opracowanie własne.

Ruch stanowi wszelkie przesunięcia, zmiany rozmieszczenia sił i środków. Ruch może być wykonywany bezpośrednio przed lub po starciu w celu zajęcia dogodnego położenia i uzyskania oraz wykorzystania przewagi sytuacyjnej.[39]

Informacja jest czynnikiem sterujący przygotowaniem i prowadzeniem walki zbrojnej, powinna ona cechować się przede wszystkim dużą wiarygodnością, dokładnością i aktualnością. Informacja zawiera :

- informacyjne oddziaływanie na wojska własne (dowodzenie),
- informacyjne oddziaływanie na przeciwnika:
  - dezinformacja,
  - walka radioelektroniczna,
  - maskowanie.

Informacja i jej logiczne zaprzeczenie – dezinformacja, są tymi czynnikami walki zbrojnej, które najwydatniej odzwierciedlają wpływ trudno wymiernego czynnika jakościowego na walkę. Ma to swoje uzasadnienie w tym, że działalność człowieka we współczesnym świecie wymaga korzystania z wielu informacji. Informacja stała się nieodzownym atrybutem wszelkich poczynań za sprawą przeobrażeń niemal we wszystkich dziedzinach życia, jakich świadkami wciąż jesteśmy. Oprócz zasobów demograficznych, surowcowych i energetycznych, zasoby informacyjne obejmujące osiągnięcia nauki, kultury i sztuki stanowią najistotniejszy czynnik potencjału cywilizacyjnego.[40]

Bez racjonalnie ukształtowanej sfery informacyjnej nie może efektywnie funkcjonować współczesne społeczeństwo, państwo - jego administracja, nauka i szkolnictwo, kultura, gospodarka narodowa i wreszcie siły zbrojne. Informacja stanowi potężną siłę, zdolną zmienić podjęte przez przeciwnika decyzje wielkiej wagi. Tak charakterystyczny dla okresu „trzeciej fali" gwałtowny rozwój elektroniki i znaczny wzrost intensywności obiegu informacji znalazł swoje odbicie w sposobie prowadzenia wojen.[41] Na polu walki pojawiła się nowa technika zdobywania, przekazywania i przetwarzania danych. „Wchłonięto" elektronikę do procesów rozpoznawania, systemów uzbrojenia oraz procedur planowania, organizowania

---

[39] Podstawową formą ruchu jest manewr. Rodzajami manewru są:
- podejście,
- oskrzydlenie,
- obejście,
- przenikanie,
- odejście.

[40] Świat „globalną wioską", ludzkość powiązana siecią „elektronicznej wioski" społeczeństwa trzeciej fali – znajdujemy w książce A.Toffler, Trzecia fala, PIW, Warszawa 1997, s.313.

[41] L.Ciborowski, R.Polko, Planowanie i organizowanie walki zbrojnej według poglądów NATO, cz.II, Informacyjna preparacja pola walki, AON, Warszawa 1996, s.8-9.

i nadzorowania walki. Stworzono nowe rodzaje amunicji o cechach „inteligentnych". Udoskonalono też środki przenoszenia broni. Skrócono w sposób zasadniczy czas reakcji ogniowej, znacznie zwiększono stopień manewrowości wojsk. Wszystko to sprawiło, że dostrzeżono rosnącą rolę walki informacyjnej. W walce zbrojnej układy informacyjne są systemami służącymi do zdobywania informacji o przeciwniku i obszarze zmagań zbrojnych oraz do przekazywania informacji o własnych procesach dowodzenia i kierowania uzbrojeniem. Istotą walki informacyjnej jest zatem stwarzanie sytuacji utrudniających przeciwnikowi podejmowanie trafnych decyzji, wykonywanie sprawnych ruchów wojskami i precyzyjnych uderzeń ogniowych przy jednoczesnej obronie przed tym samym własnych wojsk Jest to nic innego, jak dezorientowanie przeciwnika w sytuacji pola walki, komplikowanie jego warunków działania i w efekcie tego zmuszanie go do podejmowania błędnych decyzji. Podstawą sukcesu w walce zbrojnej jest zawsze precyzja rażenia i czas reakcji ogniowej.[42]

Wielu teoretyków wojskowych wypowiada się, że przyszłą walkę zbrojną cechować będzie bardzo duża manewrowość, ukierunkowana na ciągłe i szybkie zajmowanie dogodniejszego położenia w stosunku do przeciwnika.[43] Do osiągnięcia tego niezbędna będzie znajomość sytuacji po stronie przeciwnika, tak w przedniej strefie, jak i w głębi ugrupowania. Wykonujący manewr musi dysponować stosownymi środkami wykrywania, lokalizacji i zwalczania elementów ugrupowania przeciwnika, a dowódca musi mieć stworzone warunki do szybkiego podejmowania trafnych decyzji oraz sprawnego i skrytego wdrażania ich do realizacji. Warunki ku temu stwarza właściwie i pomyślnie przeprowadzona walka informacyjna. Stąd też, wymogi przyszłego pola walki nadają walce informacyjnej nową jakość. Doświadczenia ostatnich konfliktów zbrojnych wraz z rozwojem techniki komputerowej, skłaniają do traktowania sił i środków przeznaczonych do prowadzenia walki informacyjnej jako specjalistycznej służby, funkcjonującej pod jednolitym dowództwem.

O wadze informacji mówią doświadczenia z wojen jakie miały miejsce w drugiej połowy XX wieku. Każdy konflikt zbrojny poprzedzała walka informacyjna w myśl tezy, że nie jest możliwe odniesienie zwycięstwa zbrojnego bez wcześniejszego pokonania systemów informacyjnych przeciwnika. Konflikty lokalne ostatnich łat dowodzą również, że w walce zbrojnej znaczącą przewagę odniesie ten, kto uzyska informacje o punktach, które w danej sytuacji są punktami kluczowymi. Współcześnie mówi się, że wszelkie działania związane z walką informacyjną sprowadzają się do oszukania przeciwnika, głównie przez

[42] B.Balcerowicz, Pokój i „nie-pokój", Bellona, Warszawa 2001, s.173-174.
[43] Z.Ścibiorek, Rozważania o obronie, Bellona, Warszawa 1993, s.51.

dostarczenie mu nieprawdziwych wiadomości i wytworzenia błędnego obrazu położenia i zamiarów własnych wojsk. To zaś, powinno doprowadzić do podejmowania przez przeciwnika nietrafnych decyzji, co zapewne nie pozostanie bez wpływu na wynik końcowy starcia zbrojnego. Przykładem wykorzystania informacji jako broni był konflikt w Zatoce Perskiej. Podczas tego konfliktu mogliśmy śledzić działania wojenne niemal na żywo z tym, że niestety nieprawdziwe. Wszystko to co obecnie obserwujemy, stanowi postęp myśli w sferze militarnej znacznie wykraczający poza wczesne koncepcje wojny elektronicznej.[44]

„Pulsacyjność" działań taktycznych, manewrowość, ruch i jego istota, dynamika pola walki, walka informacyjna, elektroniczny wymiar pola walki – to tylko niektóre terminy, które coraz częściej pojawiają się w opracowaniach dotyczących przyszłych działań wojennych. Stosunkowo łatwo jest pisać o tych elementach, trudniej natomiast je modelować (patrz powyższy opis walki informacyjnej). Tego typu sytuację dobrze oddają myśli zawarte w publikacji PAN dotyczącej wspomagania decyzji[45]. Czytamy tam, że w wielu zagadnieniach optymalizacyjnych, jakie występują między innymi w badaniach operacyjnych, teorii sterowania itp. udaje się przedstawić z zadowalającą dokładnością, funkcję opisującą cel działalności. Funkcję tę nazywa się zwykle funkcją celu. Udaje się też sformułować problem optymalizacyjny, zadając wraz z funkcją celu ograniczenia charakteryzujące dopuszczalny obszar rozwiązań. Następnie, stosując jedną z dobrze znanych technik optymalizacyjnych uzyskuje się rozwiązanie w formie jawnej (explicite) lub w formie numerycznej. Dzieje się tak w przypadku dobrze sformułowanych, a raczej „elegancko" opisanych klasycznych problemów. Istnieją jednak problemy optymalizacyjne w których cele działania są uzależnione od subiektywnych cech decydenta. Tak jest między innymi w psychologii, socjologii, naukach społecznych jak również w grupie problemów których dotyczy niniejsze opracowanie. W takich przypadkach mówi się nie o funkcji celu, lecz o funkcji użyteczności decydenta. Od trafnego zadania postaci funkcji użyteczności zależeć będzie poprawność opisu rozważanego procesu. Jaką zatem postać powinna mieć funkcja użyteczności? Czy są ogólne reguły budowy tej funkcji? Odpowiedź jest twierdząca a dostarcza ją lektura literatury ekonomicznej – omawiane tam zagadnienia dotyczą procesów

---

[44] Informacja może być też szkodliwa, dobitnych przykładów dostarczyła wojna falklandzka w 1982 roku, kiedy to jedna informacja podana przez BBC mogła zadecydować o wyniku całej wojny. Informacja dotyczyła niewypałów, jakie znaleziono na okrętach brytyjskich po nalotach argentyńskich. Okazało się, że prawie połowa bomb zrzuconych przez Argentynę, nie wybuchało. Samoloty latały zbyt nisko i nie wystarczało czasu na zapalenie się ładunku wybuchowego. Informacja ta nie powinna była nigdy ukazać się w środkach masowego przekazu. Obszerny opis znajdziemy w Regan G., The Guinness Book of Military Blunders, Guinness Publishing, London 1991, p.169 – 170.

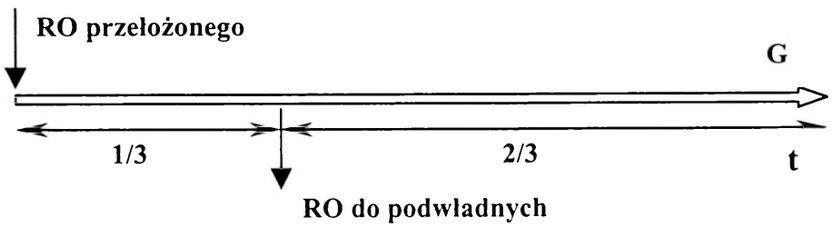
[45] R.Kulikowski, M.Libura, L.Słomiński, Wspomaganie decyzji inwestycyjnych, IBS PAN, Warszawa 1998, s.27.

decyzyjnych dających się przenieść na zagadnienia zastosowań wojskowych. Funkcja użyteczności powinna być rosnąca oraz ściśle wklęsła[46].

Przykład

ZNACZENIE INFORMACJI W PROCESIE DOWODZENIA.

Porównanie wariantów działania jest jedną z najważniejszych czynności w pracy sztabu. Czynność ta powinna być przeprowadzona w sposób obiektywny przez uczestników tak, aby uniknąć stronniczości (np. najlepszy jest wariant zaproponowany przeze mnie). Czas przewidywany na pracę sztabu wynosi 1/3 czasu przeznaczonego na przygotowanie walki. Po tym czasie podwładni otrzymują Rozkaz Operacyjny (RO), gdy wymaga tego sytuacja, Wstępne Zarządzenie Operacyjne (WZO) i przystępują do realizacji zadań (rys.2.4).



Rys.2.4. Podział czasu przeznaczonego na przygotowanie działań.
Źródło: opracowanie własne.

Na działalność koncepcyjno-organizacyjną powinna być przeznaczona znaczna część dostępnego czasu, a tylko nieznaczna jego część, na przedsięwzięcia kalkulacyjne czy redakcyjne.

Pełna kontrola dowództw i sztabów nad potokiem informacji, zapewnienie ich szybkiego przetworzenia, dokonanie niezbędnych prognoz oraz sporządzenie różnorodnych dokumentów, przy jednoczesnym zapewnieniu wysokiego stopnia ich wiarygodności, bez wspomagania informatycznego stało się wręcz niemożliwe. Dynamicznemu rozwojowi techniki towarzyszą rosnące wymagania osób wykorzystujących jej osiągnięcia. Żądane jest zapewnienie możliwości przekazywania danych w sposób wiarygodny, precyzyjny i aktualny. Uczestnicy tego procesu chcą mieć pewność co do poprawności przetwarzanych danych i rzetelności otrzymanych wyników. Stosując narzędzia informatyczne oczekują oni lepszych efektów swojej pracy w ograniczeniach czasowych, czy wręcz przy braku znajomości złożonych metod matematycznych ograniczając się jedynie do obsługi programu.

[46] Optimization of survival strategy by application of safety dependent utility model by R.Kulikowski, Control and Cybernetics vol. 29 (2000) No. 1.

Warunkiem informatycznego wspomożenia omawianych zagadnień jest zbudowanie ścisłego w sensie matematycznym algorytmu opartego na wybranej metodzie analitycznej.[47]

Do analiz wybrano metodę taksonomii numerycznej opartej na algorytmie opracowanym przez Hugo Steinhausa.[48] Wykonano stosowne obliczenia wykorzystując dane zaczerpnięte z literatury.[49]

Jednym z istotnych kryteriów w przeprowadzonej analizie porównawczej jest informacja a raczej stopień jej posiadania. Stąd kryterium to mieści się w kategorii stymulant.

Wyniki obliczeń przedstawiono poniżej. Informacyjnie podano również wyniki pośrednie. W rzeczywistości, użytkownik wprowadza jedynie dane wejściowe i otrzymuje końcowy wynik analizy. Pozostałe, wymienione kryteria mieszczą się w kategorii stymulant.

Ocena wariantów B i C okazała się w tym przypadku zbliżona (z lekką przewagą na korzyść wariantu C). Powodem takiego stanu rzeczy jest narzucony w przykładzie układ wag.

Sytuacja ulega radykalnej zmianie, wraz ze zmianą wartości poszczególnych wag. Wówczas to, lepszy okazuje się wariant B (patrz tablica 2.6). Warto też zaobserwować zmiany wyniku analizy porównawczej w przypadku, gdy pod uwagę zostanie wzięte dodatkowe kryterium (tablica 2.7).

Przy okazji warto zauważyć, że wprowadzone dodatkowo kryterium mieści się w kategorii destymulant, co w żadnym wypadku nie utrudnia analizy.

Inny problem, na który warto zwrócić uwagę związany jest z systemem nadawania wag, tzn. chodzi tu o subiektywizm w ocenach wartości poszczególnych wag.[50]

---

[47] prezentowana tutaj koncepcja wparcia procesu podejmowania decyzji została zaprezentowana przez autora na 13-tej międzynarodowej konferencji naukowej ITEC 2002 w Lille (Francja).

[48] Metoda taksonomii numerycznej została na nowo „odkryta" i przeniesiona na grunt badań akademickich w AON przez Pana Profesora Piotra Sienkiewicza w 1989 r. Wtedy używając tej i innych metod taksonomii numerycznej wykonano szereg prac naukowo-badawczych, których celem było miedzy innymi określenie współczynników jakości taktyczno - technicznej sprzętu będącego na wyposażeniu WP, jak i metodologii określania potencjałów bojowych zgrupowań wojsk własnych i przeciwnika.
W tym miejscu, trzeba też wspomnieć o postaci Profesora Hugo Steinhausa, człowieka o wielkim umyśle wykraczającym poza przyjęte ramy i standardy wyznaczone przez reguły matematyczne. „... Hugo Steinhaus uważał, że matematyka jest uniwersalna, nie ma rzeczy, która by była dla niej obca ..." R. Rabczuk, fragment z artykułu „Matematyka" nr 4/1992.

[49] J.Michniak, Metody i treści pracy zespołów funkcjonalnych na SD WLąd, AON Warszawa 2000, s.68.

[50] E. Gatnar, Symboliczne metody klasyfikacji danych PWN, Warszawa 1998, s.35.

Tablica 2.1. Rozważane warianty działania.

Kryterium	Znaczenie kryterium	Wariant „A”	Wariant „B”	Wariant „C”
Prostota	**2**	2 / **4**	1 / **2**	3 / **6**
Zaskoczenie	**3**	1 / **3**	3 / **9**	2 / **6**
Czas	**5**	1 / **5**	2 / **10**	3 / **15**
Ekonomia sił	**1**	1 / **1**	2 / **2**	1 / **1**
Wsparcie logistyczne	**2**	1 / **2**	3 / **6**	2 / **4**
Działania połączone	**1**	1 / **1**	2 / **2**	1 / **1**
Suma/Suma po uwzględnieniu kryterium		1 / **16**	13 / **31**	12 / **33**

Źródło: Praca zespołowa pod kier. J. Michniak, Metody i treść pracy zespołów funkcjonalnych na SD WLąd , AON, Warszawa 2000, s.68.

Tablica 2.2. Dane do porównania wariantów działania.

	Prostota	Zaskoczenie	Czas	Ekonomia sił	Wsparcie logistyczne	informacja
Wariant „A”	**4**	**3**	**5**	**1**	**2**	**1**
Wariant „B”	**2**	**9**	**10**	**2**	**6**	**2**
Wariant „C”	**6**	**6**	**15**	**1**	**4**	**1**
Rodzaj cechy	**S**	**S**	**S**	**S**	**S**	**S**
Wagi	**0,15**	**0,2**	**0,36**	**0,07**	**0,15**	**0,07**

Źródło: opracowanie własne.

Tablica 2.3. Macierz ustandaryzowanych cech

	Prostota	Zaskoczenie	Czas	Ekonomia sił	Wsparcie logistyczne	Informacja
Wariant „A”	**0,000**	**-1,225**	**-1,225**	**-0,707**	**-1,225**	**-0,707**
Wariant „B”	**-1,225**	**1,225**	**0,000**	**1,414**	**1,225**	**1,414**
Wariant „C”	**1,225**	**0,000**	**1,225**	**-0,707**	**0,000**	**-0,707**

Źródło: opracowanie własne.

Tablica 2.4. Macierz dyspersji.

	Prostota	Zaskoczenie	Czas	Ekonomia sił	Wsparcie logistyczne	Informacja
Wariant „A”	**1,500**	**-6,000**	**6,000**	**4,500**	**6,000**	**4,500**
Wariant „B”	**6,000**	**0,000**	**1,500**	**0,000**	**0,000**	**0,000**
Wariant „C”	**0,000**	**1,500**	**0,000**	**4,500**	**1,500**	**4,500**

Źródło: opracowanie własne.

Tablica 2.5. Wektor średniej odległości (d_{on}) z wynikami oceny globalnej.

	Wariant „A”	Wariant „B”	Wariant „C”
d_{on}	**2,262**	**1,200**	**1,075**
Wynik globalny	**0,273**	**0,614**	**0,654**

Źródło: opracowanie własne.

Tablica 2.6. Tabela danych do porównania wariantów działania. Przykład drugi, uwzględniający zmianę wag.

	Prostota	Zaskoczenie	Czas	Ekonomia sił	Wsparcie logistyczne	Informacja	Wynik globalny
Wariant „A”	4	3	5	1	2	1	0,320
Wariant „B”	2	9	10	2	6	2	0,729
Wariant „C”	6	6	15	1	4	1	0,472
Rodzaj cechy	S	S	S	S	S	S	
Wagi	0,1	0,1	0,1	0,3	0,15	0,25	

Źródło: opracowanie własne.

Tablica 2.7. Tabela danych do porównania wariantów działania. Przykład trzeci, uwzględniający zmianę wag i dodatkowe kryterium.

	Prostota	Zaskoczenie	Czas	Ekonomia sił	Wsparcie logistyczne	Informacja	Oddziaływa -nie p-ka	Wynik globalny
Wariant „A”	4	3	5	1	2	1	6	0,392
Wariant „B”	2	9	10	2	6	2	6	0,404
Wariant „C”	6	6	15	1	4	1	4	0,766
Rodzaj cechy	S	S	S	S	S	S	D	
Wagi	0,2	0	0	0	0,1	0,1	0,6	

Źródło: opracowanie własne.

2.4. DYNAMICZNY MODEL PRZEWAGI INFORMACYJNEJ

2.4.1. PODEJŚCIE PROBABILISTYCZNE

W podejściu probabilistycznym, w pierwszym etapie, stworzono pewien model prawdopodobieństwa wiedzy. Przy pomocy tego modelu, który służył jako podstawa rozważań teoretycznych, odwołano się do teorii gier i równań Lanchester'a. Do dalszych rozważań wykorzystano model prawdopodobieństwa wiedzy wraz ze zdefiniowanymi miarami informacji, celem stworzenia zależności analitycznych opisujących przewagę informacyjną nad przeciwnikiem.[51] Zdefiniowano pewną nową Miarę Efektywności (MOE) opartą na wiedzy, jaką jest kontrola przestrzeni bojowej dla koncepcji manewru dominującego. Zbadano także możliwość opracowania nowych Miar Efektywności dla poszczególnych rodzajów operacji.

Do oceny wartości przewagi informacyjnej wykorzystano teorię gier, a następnie równania Lanchester'a, w tym także możliwość dominacji informacyjnej - tzn. przewagi informacyjnej (na tyle kompletnej, że będzie ona wpływała na wiedzę posiadaną przez przeciwnika).

Prace nad miarami efektywności i związanymi z nimi wielkościami wymiernymi zdecydowanie sugeruje, że informacja - w szczególności przewaga informacyjna, może mieć silny wpływ na wyniki operacji militarnych. Pomiar stopnia przewagi informacyjnej, jaki mogłaby osiągnąć, jedna strona nad drugą, jest czymś najbardziej pożądanym w „Wieku Informacyjnym". W raporcie, o którym tu mowa, skupiono się na miarach relatywnych, poczynając od wiedzy względnej, dla której opracowano jednostkę miary wiedzy.

Ta wymierna wielkość, wyraża zależność między wiedzą idealną i rzeczywistą w operacjach militarnych, dla obu stron. Skupiono się także na potrzebie posiadania nowych miar efektywności do oceny nowych koncepcji operacji aktualnie przyjmowanych przez armię, jak również na wpływie, jaki na te operacje może wywierać informacja.

Tradycyjne miary efektywności (wciąż „zakorzenione" w modelach opracowywanych dla każdego indywidualnego układu sił), wyliczają efektywność na bazie wskaźników zmian zdominowanych przez główne systemy uzbrojenia. Mierzą one jedynie pewną część zdolności bojowej dowolnej jednostki wojskowej. Ponadto, tradycyjne miary efektywności nie spełniają

---

[51] R. Darilek i inni, Miary efektywności dla armii wieku informacyjnego, Centrum Rand Arroyo, 2002 – tłumaczenie z języka angielskiego, źródło: http//www.rand.org/organization/ard/

swojego zadania, gdy dochodzi do przygotowywania operacji stabilizujących i zachowania bezpieczeństwa - operacji znanych wcześniej jako operacje militarne inne niż wojna (MOOTW), które mogą zdominować przyszłe operacje militarne.

Dwa warianty prawa Lanchestera (wariant liniowy i kwadratowy) o których mowa w rozdziale 2.4.2 zostały uzupełnione przez tzw. wariant mieszany, tzn. prawo Lanchestera zmodyfikowane wiedzą.

W omawianym tu podejściu probabilistycznym, widoczny staje się pewien mechanizm zwany „fizykalizacją zjawisk".[52] Mechanizm ten jest naturalną konsekwencją stosowania aparatu matematycznego do opisu różnych zjawisk analogicznie do tych, występujących w fizyce klasycznej. Tego typu podejście wynika z chęci zastosowania „eleganckich" w sensie analitycznym metod analiz zjawisk z jakimi mamy do czynienia w fizyce. Stąd zastosowanie „hamiltonianów" i koncepcji entropowego modelu informacji w połączeniu z prawem Lanchestera zmodyfikowanym wiedzą.

Kolejne modyfikacje równań Lanchestera dowodzą, ograniczonej ich przydatności do opisu rzeczywistych zjawisk pola walki. Nie można odmówić tym równaniom „elegancji" w zapisie, jednakże pozostaną one jedynie narzędziem dociekań akademickich. Prawdziwych rozwiązań należy poszukiwać w symulacjach komputerowych.

TEORIA GIER W ZASTOSOWANIACH MILITARNYCH

Teoria gier jest szeroko wykorzystywana do analizy efektów wyboru strategii alternatywnych celem osiągnięcia założonych celów militarnych. W przypadku dwuosobowych gier z zerową sumą, tzn. gdy wygrana jednego gracza jest stratą gracza drugiego, obaj gracze mają kilka alternatywnych strategii, które mogą realizować, a chociaż każdy jest świadom strategii dostępnych swojemu przeciwnikowi, żaden z nich nie jest pewny, jaką strategię wybierze przeciwnik. Każdy gracz wybiera taką strategię, która maksymalizuje jego zysk. Jednocześnie każdy gracz zabezpiecza się przed wyborem takiej strategii jego przeciwnika, która może przyczynić się do zmniejszenia zysku. W działaniach obu graczy widać siłę oddziaływania informacji na wynik walki. Każdy z graczy reprezentuje stronę w walce.

Wszystkie gry mają strukturę taką, jak widzimy na rys.2.5. Strony: 1 i 2, mogą wybrać odpowiednio strategie i = 1, 2, 3, ..., m oraz j = 1, 2, 3, ..., n. Dla każdej pary strategii istnieje pewien zysk a_{ij}. Zysk a_{ij} jednej strony, jest jednocześnie stratą a_{ij} strony drugiej.

---

[52] patrz H. Spustek, Przewaga w walce i operacji, rozprawa habilitacyjna AON, Warszawa 2002 r.

Podczas gdy strona pierwsza maksymalizuje swój zysk, strona druga minimalizuje swoje straty.

Strategie (j) Strony 2

Strategie (i) Strony 1	1	2	. . .	n
1	a_{11}	a_{12}	.....	a_{1n}
2	a_{21}	a_{21}	.....	a_{2n}
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
m	a_{m1}	a_{m1}	.....	a_{mn}

Rys. 2.5. Macierz gry.

PRZYPADKI ZMIENNEJ WIEDZY

O wojnie moglibyśmy myśleć abstrakcyjnie w następujący sposób: W dowolnej walce wybór strategii Strony 1 będzie miał zasadniczy wpływ na wynik, podobnie jak dla Strony 2. W zależności od warunków walki (stosunki sił, teren, itp.), możliwe strategie mogą powodować większe lub mniejsze różnice.

Podobnie do powszechnie uwzględnianych (wyżej wymienionych) warunków walki, należy uwzględnić wartość informacji. Można rozważyć pewne abstrakcyjne przypadki, w których wybór strategii ma bardzo zróżnicowane konsekwencje w odniesieniu do uzyskanych wyników.

Możliwe są cztery przypadki:

- Gra 1: dla armii współczesnej – przypadek klasyczny (obie strony posiadają prawidłową wiedzę). Strona pierwsza i Strona druga mają wspólną i prawidłową wiedzę w postaci wszystkich wartości z macierzy zysków **A** (macierz **A** ma postać taką jak na rys.2.5. Obie strony mają tę samą informację o zyskach, ale nie są świadome, jakich wyborów dokonuje przeciwnik. Żadna ze stron nie posiada przewagi wiedzy.

- Gra 2: Armia XXI wieku (Strona pierwsza posiada prawidłową informację, a Strona druga informację nieprawidłową). Strona pierwsza posiada prawidłową wiedzę o wszystkich wartościach $\mathbf{A} = \mathbf{A}_1$, a Strona druga dysponuje całkowicie *nieprawidłowym* rozumieniem macierzy zysków. Symulacja tego stanu odbywa się poprzez dostarczenie Stronie drugiej macierzy zysków $\mathbf{A} = \mathbf{A}_2$ złożonej z pewnego zestawu liczb losowych z przedziału od 0 do 100. Dlatego też Strona druga podejmować będzie decyzje oparte na informacji fałszywej. Mimo całkowitej abstrakcji, pozwala to na opis pewnej sytuacji, w której Armia XXI wieku posiadająca luksusową informację walczy z przeciwnikiem, który nie tylko nie posiada ważnej informacji, ale także jest całkowicie wprowadzony w błąd. Sytuacja ta może być traktowana jako przypadek, w którym Niebiescy (Stroma pierwsza) posiadają przewagę informacyjną.

- Gra 3: AAN (Strona pierwsza posiada prawidłową informację. Strona druga posiada prawidłową informację. Strona pierwsza zna wybór Strony drugiej). Strona pierwsza i Strona druga posiadają prawidłową wiedzę o wartościach **A**, podobnie jak w Grze 1. Strona druga wybiera swoją strategię minimax j^* z prawidłowej macierzy **A**. Jednakże, Strona pierwsza zna wybór Strony drugiej, i zamiast dokonywać wyboru swojej strategii maximin (i), skupia się raczej, jedynie na zyskach odpowiadających wyborowi minimax Strony drugiej i maksymalizuje swój zysk. Symuluje to przypadek, w którym Strona pierwsza posiada perfekcyjny wywiad, a w wyniku, inny rodzaj lub wyższy poziom przewagi informacyjnej. Mimo, że informacja bazowa Strony drugiej w tym przypadku (w przeciwieństwie do Gry 2) nie jest zła, to jest ona wyraźnie gorsza w porównaniu do Strony pierwszej.

- Gra 4: AAN (Strona pierwsza posiada informację prawidłową. Strona druga posiada informację nieprawidłową, Strona pierwsza zna wybór Strony drugiej). W grze czwartej Strona pierwsza posiada prawidłową wiedzę o wszystkich wartościach $A = A_1$, a Strona druga dysponuje całkowicie niepoprawną macierzą zysków $A = A_2$, złożoną z drugiego zestawu liczb losowych z przedziału między 0 i 100, jak w Grze 2. Strona druga wybiera swoją strategię minimax.j* w oparciu o nieprawidłową informację z A_2. Strona pierwsza zna wybór Strony drugiej. Zamiast wykorzystywać swoją strategię maximin, skupia się ona jedynie na zyskach odpowiadających wyborowi minimax Strony drugiej dokonanym w oparciu o nieprawidłową informację i dokonuje swojego wyboru z prawidłowej macierzy

A_1. Strona posiada informację perfekcyjną (wiedza maksymalna). Może ona nawet tworzyć swoją pozycję (wykorzystując ofensywne operacje informacyjne) przez aktywną znajomość faktu, że Strona druga posiada złą informację. Zatem Strona pierwsza posiada nie tylko przewagę informacyjną ale także dominację informacyjną.

Z gier tych wynika wyraźny wniosek, że przewaga i dominacja informacyjna pochodzi z dynamicznych interakcji między obu stronami. Mogą się one zmieniać w czasie - np. w trakcie trwania konfliktu. Stąd też powinniśmy myśleć o przewadze i dominacji informacyjnej w kategoriach dynamicznych.

Przykład

INFORMACJA W WOJNIE W ZATOCE PERSKIEJ.

Gry omówione powyżej, reprezentują stosunkowo proste, abstrakcyjne kalkulacje opracowane w celu stymulacji podejścia jakościowego. Gry te, zamiast trudnych i dodatkowo, niedostępnych danych o wyborach dokonywanych przez Armię XXI wieku, pokazują potencjalny udział przewagi informacyjnej i dominacji informacyjnej w zwycięstwie. Pomimo tego, że są one pouczające, to prawdziwym testem modeli budowanych na gruncie teorii gier jest to, czy oferują nam one coś więcej ponad jakościową ocenę wartości informacji.

Przykładowo, zdrowy rozsądek może doprowadzić nas do hipotezy, że wartość informacji zależy od stopnia zależności wyniku walki od wyborów uczestników tej walki. W przypadku, gdy istnieje ogromna różnica sił, otwarty teren i brak możliwości zaskoczenia czy maskowania, wybory dostępne stronom przeciwnym są relatywnie bez znaczenia. Dla kontrastu, jeśli stronom przeciwnym dostępne są wybory o dużym znaczeniu, np. wybór między zaskoczeniem przeciwnika, a zyskaniem czasu na przygotowanie się lub między skoncentrowaniem sił w jednym sektorze, a ich rozłożeniem w sposób równomierny, wówczas informacja może mieć znaczenie decydujące.

Wojna w Zatoce stanowi dobry przykład do badania wyżej poruszanych zagadnień.

Zarówno Generał Schwarzkopf, jak i Saddam Hussein, rozważali szereg wariantów działania dla osiągnięcia swoich celów. Koalicja dowodzona przez USA (Strona 1) jako swój cel przyjęła wycofanie sił irackich z Kuwejtu. Irakijczycy (Strona 2) ze swojej strony byli zdeterminowani pozostać. Dlatego też wynik tego konfliktu jest binarny: wojska irackie opuszczają Kuwejt (wynik pożądany dla Strony 1 i niepożądany dla Strony 2 lub wojska

irackie pozostają (wynik pożądany dla Strony 2 i niepożądany dla Strony 1). Można łatwo wypełnić macierz gry za pomocą wyników opartych na strategiach wybranych przez przeciwników. Jednakże, koalicja kierowana przez USA może także być zainteresowana odpowiedzią na pytania: Ile czasu potrzeba na wyparcie Irakijczyków z. Kuwejtu? W jakim stopniu koalicja jest zdolna to wykonać?

Poniżej opisano wybory dostępne każdej ze stron.

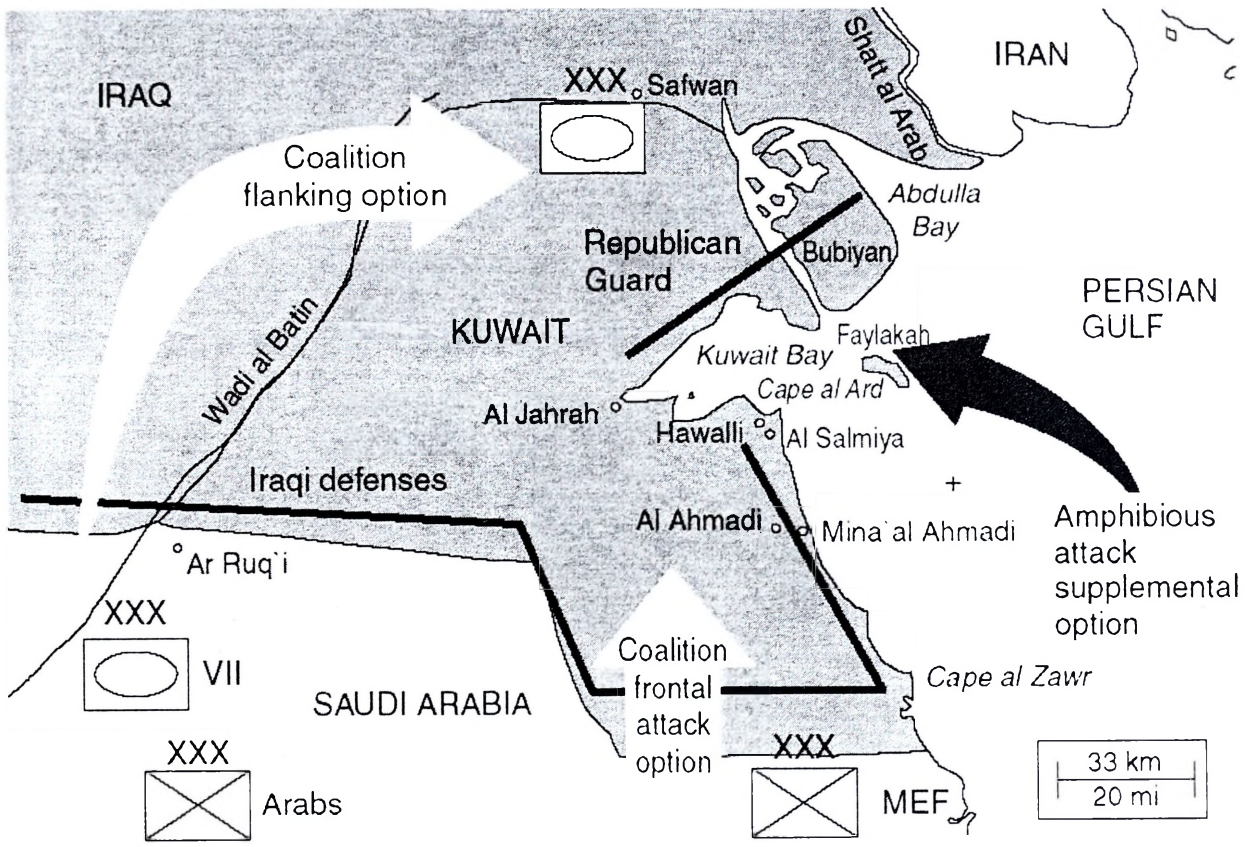
Opcje rozważane przez Koalicję.

1. Atak oskrzydlający. Jest to opcja rzeczywiście wybrana przez koalicję. Głównym naziemnym działaniem ofensywnym był zakrojony na olbrzymią skalę atak oskrzydlający, którego zamiarem było zaatakowanie celów naziemnych od zachodniej części Kuwejtu w kierunku kluczowych pozycji jednostek Irackiej Gwardii Republikańskiej, które były rozlokowane na linii północna część Kuwejtu - południowa część Iraku. Po pokonaniu Gwardii Republikańskiej, główne siły Iraku w Kuwejcie zostałyby okrążone. Świadomość przewagi sytuacyjnej koalicji, w połączeniu z możliwością poruszania się w otwartej pustyni zachodniego Kuwejtu (ze względu na posiadanie GPS), ułatwiły szybkie poruszanie się na lądzie w tej historycznej operacji.

2. Atak frontalny. Jest to opcja, w której koalicja w celu uzyskania zwycięstwa atakowałaby bezpośrednio wojska irackie, które zajęłyby Kuwejt, polegając na przewadze w wyszkoleniu i sile ognia. Mimo, że opcja ta nie została zrealizowana, większość wysiłków koalicji w zakresie maskowania przekonała Irakijczyków, że jest to rzeczywisty plan ataku koalicji.

3. Atak oskrzydlający ze wsparciem desantu sił lądowo-morskich. Opcja ta zakładała, że w uzupełnieniu do zakrojonego na szeroką skalę manewru VII Korpusu oskrzydlającego zachodnią część Kuwejtu siły Piechoty Morskiej (Marines) przeprowadzą desant lądowa-morski w pobliżu Zatoki. Operacja ta była rzeczywiście planowana, ale nie została zrealizowana. Zaletą tego manewru było to, że mógł on pokazać dowódcom irackim dodatkowe zagrożenie na północno-wschodnim teatrze operacji.

4. Frontalny atak ze wsparciem desantu sił lądowo-morskich. Opcja ta zakładała, że niezależnie od silnego ataku wyprowadzonego bezpośrednio z Arabii Saudyjskiej na Kuwejt, nastąpi desant lądowa-morskich sił Piechoty Morskiej. Atak ten wywarłby pewną presję na północna-wschodnią część sił irackich w Kuwejcie jednocześnie z atakiem głównym od południa.



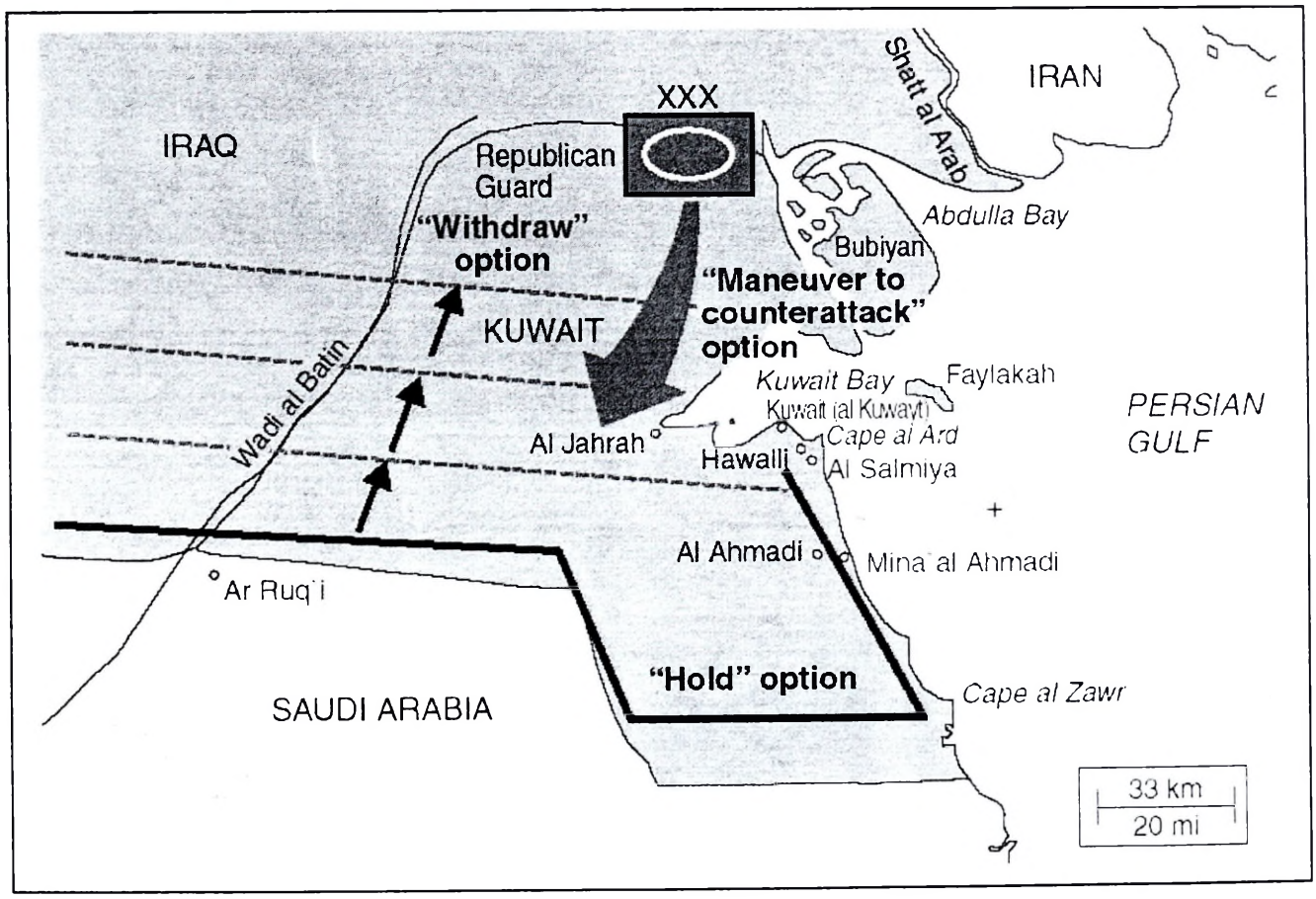
Rys.2.6. Opcje Ofensywne Koalicji.

Opcje rozważane przez Irak

1. Wycofanie. Opcja ta zakłada, że Irakijczycy zajmą pozycję wewnątrz Kuwejtu, w szczególności w celu przeprowadzenia manewru wycofania w walce w przypadku lądowego natarcia koalicji, którego celem będzie wyzwolenie Kuwejtu. Wojska irackie zajmą głębokie pozycje w Kuwejcie w celu zadania strat nacierającym wojskom koalicji, w szczególności, gdy wojska te będą nacierały z połurdnia, jak to zakładano w opcji „ataku frontalnego" koalicji.

2. Utrzymanie pozycji. Opcja ta reprezentuje plan, który Irakijczycy rzeczywiście usiłowali zrealizować. Duża liczba irackich dywizji piechoty została przesunięta w kierunku południowego Iraku i Kuwejtu i okopała się na tzw. Linii Saddama. Intencją Iraku było zadanie maksymalnych strat nacierającym wojskom koalicji poprzez zwalczanie pododdziałów z pozycji ufortyfikowanych. Z perspektywy Iraku strategia ta była najlepiej przygotowana na frontalny atak koalicji z południa. Dodatkowo, opcja ta przewidywała podjęcie próby zachowania kontroli nad Kuwejtem.

3. Przejście do kontrataku. Opcja ta zakładali możliwość stworzenia wystarczająco silnej obrony, która umożliwiałaby Gwardii Republikańskiej i innym regularnym siłom pancernym przeprowadzenie swobodnego manewru wewnątrz kuwejckiego teatru działań. W zależności od wyboru koalicji, natarcie z flanki lub atak frontalny, (z / lub) bez wsparcia desantu morskiego. Irakijczycy mogliby wykorzystać swoje duże formacje pancerne dla przeprowadzenia manewru agresywnego przegrupowania i kontrataku.



Rys.2.7. Opcje Defensywne Iraku.

2.4.2. PODEJŚCIE DETERMINISTYCZNE

MODEL WALKI LANCHESTERA

Przypomnijmy, postać równań Lanchestera jest następująca:

$$\begin{cases} \dfrac{dR(t)}{dt} = -bB(t)^{c_1} R(t)^{c_2} \\ \dfrac{dB(t)}{dt} = -rR(t)^{c_3} B(t)^{c_4} \end{cases}, \qquad (2.1)$$

gdzie: r i b są liczbami rzeczywistymi z przedziału (0, 1) i są to tzw. współczynniki efektywności Lanchestera. Współczynniki te są niekiedy interpretowane jako prawdopodobieństwo strat każdej z walczących stron w ciągu jednego dnia walki (dzienne prawdopodobieństwo strat),

$c_1, \ldots, c_4$ są wykładnikami potęg przy B(t) i R(t) i mogą przyjmować wartości liczbowe 0 lub 1.

Po stosownych przekształceniach matematycznych otrzymujemy cztery rodzaje rozwiązań, zależnie od wartości współczynników $c_1, \ldots, c_4$ (patrz tablica 2.1).[53]

Tablica 2.1. Możliwe warianty rozwiązania układu równań Lanchestera.

Rodzaj rozwiązania	c_1	c_2	c_3	c_4	Rozwiązanie
Liniowe	1	1	1	1	$b[B(0) - B(t)] = r[R(0) - R(t)]$
kwadratowe	1	0	1	0	$b[B(0)^2 - B(t)^2] = r[R(0)^2 - R(t)^2]$
logarytmiczne	0	1	0	1	$b\ln[B(0)/B(t)] = r\ln[R(0)/R(t)]$
Zasadzka (ang. ambush)[54]	1	1	1	0	$b/2[B(0)^2-B(t)^2] = r[R(0) - R(t)]$

Źródło: Joshua M. Epstein, The Calculus of Conventional War Dynamic Analysis without Lanchester Theory, Studies in Defence Policy, The Brookings Institution, Washington 1985, p.147.

[53] dokładną analizę przedstawionych tu rozważań można znaleźć w pracy Joshua M. Epstein, The Calculus of Conventional War Dynamic Analysis without Lanchester Theory, Studies in Defence Policy, The Brookings Institution, Washington 1985, p.146 – 156.

[54] Wariant zasadzki pozwala na modelowanie walk partyzanckich. Zostało dowiedzione, że oddziały partyzanckie, stosując odpowiednią taktykę, mogą prowadzić skuteczną walkę z siłami regularnymi. Ten rodzaj walk określa przypadek rozwiązania równań Lanchestera zwany wariantem „zasadzki".

Pierwszy, najprostszy wariant – wariant liniowy, opisuje walkę przy następujących warunkach początkowych:

- Dwie strony, biorące udział w walce, atakują jedna drugą. Każda ze stron jest w zasięgu działania broni przeciwnika,
- Walczące strony składają się z jednorodnych jednostek bojowych (posiadają jednakowe uzbrojenie). Przez jednostkę bojową rozumie się tutaj jednostkę uzbrojenia, przykładowo: karabin, działo, czołg, samolot itp.
- Każda ze stron, znając obszar zajmowany przez przeciwnika, prowadzi ogień bez znajomości jego skutków.
- Ogień jest równomiernie rozkładany na cały obszar rozmieszczenia przeciwnika.
- Walczące strony nie posiadają strat nie bojowych.
- W czasie walki siły stron nie są uzupełniane.

Walka rozpatrywana jest jako ciąg następujących po sobie starć (zdarzeń), stanowiący proces ciągły, o zmieniającej się ilości jednostek bojowych. Zakłada się ponadto, że wszystkie starcia zachodzą w jednakowych przedziałach czasowych, o pewnej wartości średniej, co pozwala na stosowanie metod rachunku różniczkowego.

Rozpatrzmy wariant równania kwadratowego (model walki o zależności kwadratowej). W modelu walki Lanchestera o zależności kwadratowej przyjmuje się następujące założenia:

- Każda jednostka bojowa dowolnej strony, dopóki nie jest zniszczona, oddaje ciąg strzałów z pewną średnią szybkostrzelnością; ciąg ten (dokładnie lub w przybliżeniu jest poissonowski).
- Każda jednostka bojowa jednej strony może prowadzić ogień do dowolnej jednostki drugiej strony i odwrotnie. Ogień jest celowany, tj. skierowany na zniszczenie ściśle określonej jednostki bojowej przeciwnika.
- Jednym strzałem nie można razić więcej niż jedną jednostkę bojową.
- Jeżeli jednostka bojowa została rażona, ogień natychmiast zostaje przenoszony na inną, a jednostka rażona nie bierze dalszego udziału w działaniach bojowych.
- Nie bierze się pod uwagę czasu lotu pocisku do celu, gdyż jest on bardzo mały w porównaniu z ogólnym czasem trwania walki.
- W dowolnej chwili czasu ogólna efektywność bojowa każdej strony jest proporcjonalna do wartości średniej przypadkowo nie zniszczonych jednostek bojowych. Jest to szczególnie ważne dla bardzo licznych zgrupowań wojsk.[55]

[55] M. Ciechanowicz i inni, Wybrane metody optymalizacji decyzji, MON, Warszawa 1969, s.128.

W przypadku modelu walki o zależności kwadratowej, równania Lanchestera przyjmują postać:

$$\begin{cases} \dfrac{dR(t)}{dt} = -bB(t) \\ \dfrac{dB(t)}{dt} = -rR(t) \end{cases} . \qquad (2.2)$$

Postulując rozwiązanie w postaci:

$$B(t) = Ae^{\alpha t} + Be^{-\alpha t} \qquad (2.3)$$

i korzystając z tablicy 6.1 celem określenia postaci rozwiązania $R(t)$ otrzymujemy:

$$B(t) = \frac{1}{2}\left\{\left[B(0) - \sqrt{r/b}R(0)\right]e^{\sqrt{rb}t} + \left[B(0) + \sqrt{r/b}R(0)\right]e^{-\sqrt{rb}t}\right\} \qquad (2.4)$$

oraz

$$R(t) = \frac{1}{2}\left\{\left[B(0) - \sqrt{b/r}B(0)\right]e^{\sqrt{rb}t} + \left[R(0) + \sqrt{b/r}B(0)\right]e^{-\sqrt{rb}t}\right\}. \qquad (2.5)$$

Powyższe rozwiązanie uzyskano przy założeniu stałych w czasie współczynników efektywności działań r i b. Z zależności (2.4) i (2.5) widać, że siły walczących stron zależą jedynie od czasu i wielkości sił początkowych. W zależnościach tych nie uwzględniono prędkości wycofywania. Innymi słowy, według równań Lanchestera prędkość wycofania nie wpływa na wielkość poniesionych strat. Zatem, powyższe zależności nie nadają się do opisu prędkości przesuwania się frontu jako funkcji zmian stosunku strat określonych równaniami (2.1). Rozwiązania równań Lanchestera dają te same wyniki zarówno w obronie z elementami wycofywania jak i bez wycofywania. Dzieje się tak, z powodu tego, że nie ma tu sprzężenia zwrotnego pomiędzy prędkościami natarcia i prędkościami cofania.

Obliczymy jeszcze czas jaki upłynie od momentu rozpoczęcia walki do jej zakończenia. W tym celu należy przyrównać do zera równanie (2.5) i obliczyć czas t_k. Dokonując stosownych przekształceń otrzymujemy:

$$t_k = \left(\frac{1}{rb}\ln\frac{R(0) + \sqrt{b/r}B(0)}{\sqrt{b/r}B(0) - B(0)}\right)^{1/2} . \qquad (2.6)$$

Na podstawie zależności (2.6) widać, że czas trwania walki zależy tu jedynie od stałych współczynników r i b i początkowej liczebności walczących stron.

Równania Lanchestera mają zastosowanie jedynie do walki na pewnym obszarze w określonym z góry czasie. W przypadku gdy czas walki „przesunie się", to wówczas staniemy przed problemem „przesunięcia" funkcji strat obu stron, a na pytanie jak to wykonać, niestety równania Lanchestera odpowiedzi nie dają.

Na uwagę zasługuje też przypadek równych sił początkowych obu stron. Wówczas, strony pozostają w sytuacji patowej (bez wyjścia). Odpowiada to równości:

$$b \cdot R(0)^2 = r \cdot R(0)^2 . \tag{2.7}$$

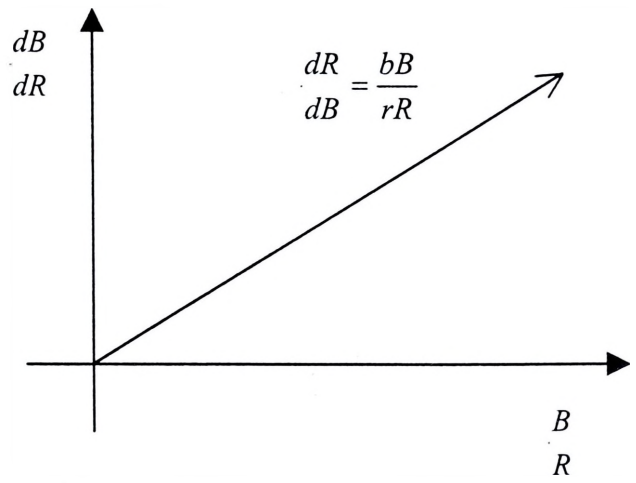
Innymi słowy, można powiedzieć, że stosunek efektywności b/r jest wówczas równy kwadratowi stosunku liczbowego sił $R(0)/B(0)$:

$$\frac{b}{r} = \left(\frac{R(0)}{B(0)}\right)^2 . \tag{2.8}$$

Dzieląc równania (6.2) stronami otrzymujemy następującą zależność:

$$\frac{dR}{dB} = \frac{bB}{rR} . \tag{2.9}$$

Powyższy przypadek „sytuacji bez wyjścia", można zilustrować graficznie (rys.2.8).



Rys. 2.8. Przypadek „sytuacji bez wyjścia".
Źródło: Joshua M. Epstain, The Calculus of Conventional War Dynamic Analysis without Lanchester Theory, Studies in Defence Policy, Washington 1985, p.154.

Zależność (2.9) ma sens jedynie dla $r > b$. Na podstawie zależności (2.9) i rys. 2.8 można napisać, że:

$$\frac{\partial}{\partial(B/R)}\left(\frac{dR}{dB}\right) = \frac{b}{r} > 0 . \tag{2.10}$$

Przypadek „zasadzki" – walki partyzanckiej (por. tablica 2.1) charakteryzuje poniższy układ równań:

$$\begin{cases} \dfrac{dR(t)}{dt} = -bB(t)R(t) \\ \dfrac{dB(t)}{dt} = -rR(t) \end{cases} \tag{2.11}$$

W tym przypadku, ubytek sił partyzantów następuje według równań Dinera[56], a ubytek sił wojsk regularnych – według równań Lanchestera.

Wychodząc z układu równań Lanchestera o zależności kwadratowe, różniczkując powtórnie po czasie pierwsze równanie układu (2.2), otrzymujemy:

$$\frac{d^2R(t)}{dt^2} = -b\frac{dB(t)}{dt}. \qquad (2.12)$$

Korzystając z drugiego równania układu (2.2) otrzymujemy następującą zależność:

$$\frac{d^2R(t)}{dt^2} - brR(t) = 0. \qquad (2.13)$$

Biorąc pod uwagę warunki początkowe: $R(0) = R_0$ i $B(0) = B_0$ dostajemy rozwiązanie układu w innej niż (2.4) i (2.5) postaci:

$$R(t) = R_0 \cosh\sqrt{brt} - B_0\sqrt{\frac{b}{r}}\sinh\sqrt{brt}, \qquad (2.14)$$

$$B(t) = B_0 \cosh\sqrt{brt} - R_0\sqrt{\frac{r}{b}}\sinh\sqrt{brt}. \qquad (2.15)$$

Dzieląc równania (2.14) i (2.15) odpowiednio przez R_0 i B_0 oraz oznaczając:

$$\mu_R = \frac{R(t)}{R_0} \quad \text{siły „czerwonych" (jednostki umowne),} \qquad (2.16)$$

$$\mu_B = \frac{B(t)}{B_0} \quad \text{siły „niebieskich" (jednostki umowne),} \qquad (2.17)$$

$$\tau = \sqrt{brt} \quad \text{czas (jednostki umowne),} \qquad (2.18)$$

$$\Phi_0 = \frac{R_0}{B_0}\sqrt{\frac{b}{r}} \quad \text{przewaga początkowa,} \qquad (2.19)$$

otrzymujemy równoważną postać rozwiązania układu równań Lanchestera o zależności kwadratowej:

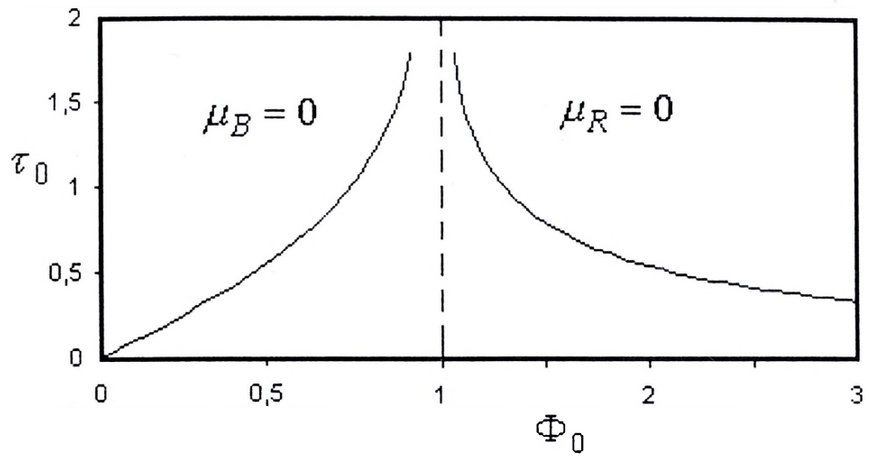
$$R(t) = \cosh\tau - \Phi_0^{-1}\sinh\tau, \qquad (2.20)$$

$$R(t) = \cosh\tau - \Phi_0\sinh\tau. \qquad (2.21)$$

Interpretacja przewagi początkowej Φ_0 została pokazana na rys. 2.9.

---

[56] Model Dinera został opracowany dla przypadku, kiedy walka jest słabo zorganizowana, nie uzyskuje się informacji o stanie przeciwnika i nie dokonuje się przenoszenia ognia. Przypadek ten jest przeciwstawny do sytuacji opisywanych równaniami Lanchestera, zobacz M.Rybár i inni, Modelovanie a simulácia vo vojenstve, Ministerstvo Obrany Slovenskiej Republiky, Bratislava 2000, s.204 – 208.



Rys.2.9. Interpretacja przewagi początkowej Φ_0 w modelu Lanchestera o zależności kwadratowej.

Źródło: Opracowano na podstawie: Przemieniecki J.S., Mathematical Methods in Defence Analyses, Air Force Institute of Technology, Washington, 1994, s.94.

Model walki Lanchestera (i jego liczne modyfikacje) pozwala na modelowanie walki w jej „starej" formie, gdzie dwie przeciwstawne strony walczą ze sobą na określonym z góry obszarze, w jasno określonej sytuacji bojowej. Przy pomocy równań różniczkowych można opisać różnorodne działania bojowe, gorzej jest z ich rozwiązaniem. Nierzadko, równań tych nie można rozwiązać w sposób ścisły. Pozostaje wówczas zadowolić się rozwiązaniem przybliżonym, którego uzyskanie należy powierzyć maszynie liczącej. Trzeba również zauważyć, że wybór rodzaju modelu, do konkretnych działań bojowych wcale nie jest łatwy, wymaga sporej wiedzy i doświadczenia z zakresu matematycznego modelowania zjawisk.

MODEL WALKI EPSTEINA[57]

Omówione wyżej mankamenty modelu Lanchestera stały się powodem poszukiwań nowych rozwiązań w tym zakresie. W trakcie walki, atakujący wymusza duże tempo działań w wyniku których jego siły maleją (ponosi straty). Jednakże, straty te są niekiedy mniejsze niż w przypadku zaniechania ataku. Atakujący stara się wywrzeć ekstremalnie duży nacisk na stronę przeciwną, czego powodem mogą być przyczyny strategiczne, operacyjne lub polityczne. Z kolei, tempo obrony narzucane jest przez (często przypadkowe) zmiany stosunku strat obrony do ataku. Atakujący może wybrać pozycję utrzymując tempo ataku lub może zmniejszyć tempo natarcia przez wycofanie – zmniejszenie prędkości. Czynniki operacyjne, taktyczne lub polityczne mogą uniemożliwić obronę na pewnym obszarze

[57] Opisany tutaj model pochodzi z publikacji Joshua M.Epstein, The Calculus of Conventional War, Studies in Defense Policy, The Brookings Institution, Washington 1985.

w ciągu określonego czasu. Zamiast liniowej zależności stosunku strat stron do stosunku ich sił w czasie trwania walki (patrz rys.6.1), generowanej przez model Lanchestera, należy wprowadzić przebieg nieliniowy, będący odzwierciedleniem kolejno następujących po sobie bitew i zatrzymań, charakterystycznych dla współczesnej wojny.

Modyfikacja równań Lanchestera[58]

Dokonano zatem modyfikacji równań Lanchestera. Całkowite siły atakującego w chwili czasu t, wyrażono poprzez siły w chwili $(t-1)$ poprzedzającą chwilę t o jednostkę umowną:

$$A_g(t) = A_g(t-1) - \alpha(t-1)\cdot A_g(t-1), \qquad (2.22)$$

gdzie: $A_g(t)$ - bieżące siły strony atakującej,

$A_g(t-1)$ - siły strony atakującej w chwili $t-1$,

$\alpha(t-1)$ - tempo strat atakującego w chwili $t-1$.

Równanie (2.12) można przedstawić w postaci:

$$A_g(t) = A_g(t-1)\cdot[1-\alpha(t-1)]. \qquad (2.23)$$

Dla strony broniącej się można zapisać:

$$D_g(t) = D_g(t-1) - \frac{\alpha(t-1)}{\rho} A_g(t-1), \qquad (2.24)$$

oznaczając: $D_g(t)$ - bieżące siły strony broniącej się,

$D_g(t-1)$ - siły strony broniącej się w chwili $t-1$,

ρ - stosunek strat strony atakującej do broniącej się w chwili $t-1$.

Dla strony atakującej można teraz napisać:

$$\alpha(t-1)\cdot A_g(t-1) = \frac{\alpha(t-1)}{\rho} A_g(t). \qquad (2.25)$$

Przyjmując wartość początkową ρ dla $t=1$ i znając zależność czasową współczynnika α - strat strony atakującej, możemy w sposób dynamiczny opisać walkę.

---

[58] Od momentu powstania klasycznej postaci modelu Lanchestera, wykonano szereg jego modyfikacji. Kolejni autorzy starali się w taki sposób „poprawić" równania Lanchestera, by dostosować je do wymogów zmieniającego się pola walki. Przykładowo: model „mieszany" (patrz: H.Brackney, The Dynamics of Military Combat, Operations Research, Vol.7, Jan.-Feb. 1959, pp.30-49, P.M.Morse, and G.E.Kimball, Methods of Operations Research, MIT Press

Oznaczając tempo wycofywania przez $W(t)$, maksymalne tempo wycofywania przez $W_{\max}$ oraz przyjmując $W(1)=0$ (dla początkowej chwili czasu), możemy napisać:

$$\alpha(t)=\alpha_g(t)\cdot\left[1-\frac{W(t)}{W_{\max}}\right], \qquad (2.26)$$

przy warunku $0 \le W(t) \le W_{\max}$.

W przypadku gdy strona broniąca się, nie będzie się wycofywać lub nie będzie mogła się wycofywać, to wówczas $W(t)=0$ i tempo walki zostanie zasadniczo zależne od strony atakującej. Wycofywanie rozpoczyna się dopiero wtedy, gdy tempo strat przewyższa pewien próg α_{dT}. Stąd, tempo obrony z wycofywaniem w chwili czasu t, jest funkcją tempa strat w chwili $(t-1)$, tj. $\alpha_d(t-1)$. Różnica tempa wycofywania obrony w dwóch kolejno po sobie następujących chwilach czasu, zależy od różnicy pomiędzy aktualnym tempem strat i progową wartością tempa strat α_{dT}, przemnożonej przez pewną funkcję tempa wycofywania $f(t)$, co można zapisać w postaci następującej zależności:

$$W(t)-W(t-1)=f(t)\cdot[\alpha_d(t-1)-\alpha_{dT}], \qquad (2.27)$$

gdzie: $$f(x)=\frac{W_{\max}-W(t-1)}{1-\alpha_{dT}}.$$

Tempo strat dziennych strony atakującej $\alpha(t)$ jest odwrotnością „czynnika wymiany" ρ strat obrony przypadających na daną chwilę czasu $\alpha_d(t)$. W przypadku gdy, tempo strat strony broniącej się przewyższa wartość progową α_{dT}, wówczas w następnym przedziale czasowym tempo wycofywania będzie równe $W(t+1)$. Mamy wówczas do czynienia z ujemnym sprzężeniem zwrotnym – tempo strat atakującego wynosi $\alpha(t+1)$. Jeżeli w chwili czasu $(t-1)$ odnotowane tempo strat atakującego przekracza α_{aT}, atakujący zmniejsza prędkość prowadzenia działań bojowych $\alpha_g(t)$, zmniejsza tempo prowadzenia ataku. Jeżeli natomiast, tempo strat jest niższe niż α_{aT}, to atakujący przyspiesza poprzez zwiększenie α_{gT} - rys.2.10.

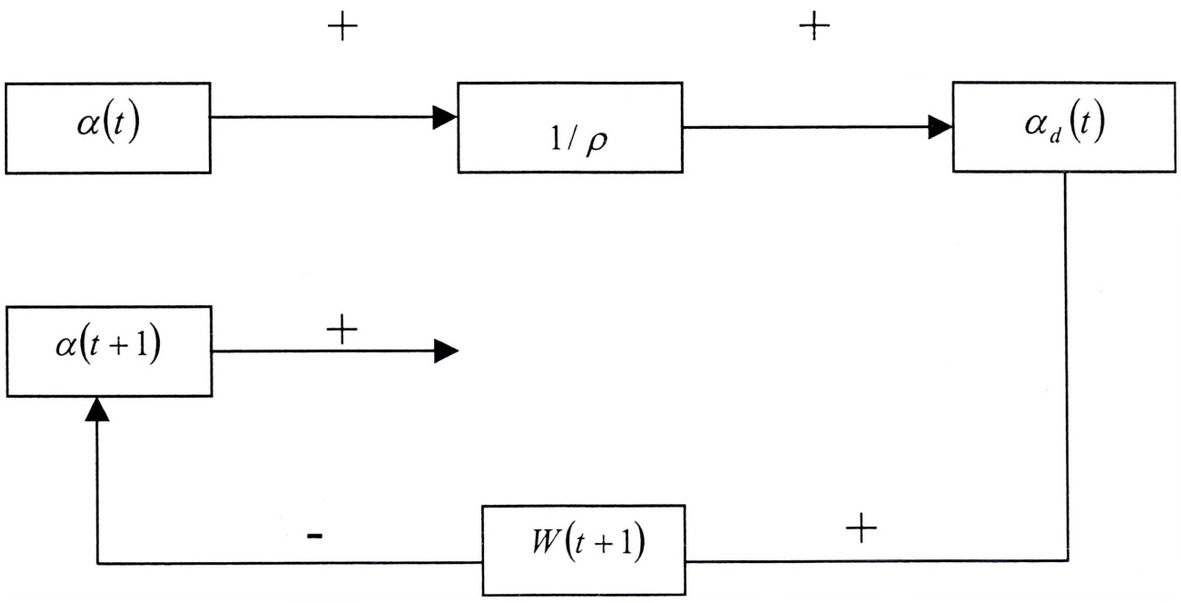
---

and Wiley, New York, 1951, pp. 71-73), model Helmbold'a (patrz: R.L.Helmbold, Decision in Battle: Breakpoint Hypotheses and Engagement Termination Data, Rand Corp., Santa Monica, CA, Rept. R-772-PR, June 1971).

Zmiana współczynnika α_{gT} dąży do zera, gdy tempo strat atakującego zbliża się do α_{aT}, wówczas równanie tempa ataku można zapisać w postaci:

$$\alpha(t) = \alpha_g(t-1) - \left[\frac{\alpha_{aT} - \alpha_g(t-1)}{\alpha_{aT}}\right] \cdot [\alpha_a(t-1) - \alpha_{aT}]. \qquad (2.28)$$

W ten oto sposób, stosując połączenie klasycznego modelu Lanchestera oraz jego modyfikacji otrzymaliśmy dynamiczny model w którym możliwym stała się aproksymacja strat każdej ze stron.



Rys. 2.10. Mechanizm zmian tempa strat dziennych strony atakującej $\alpha(t)$.
Źródło: Joshua M. Epstain, The Calculus of Conventional War Dynamic Analysis without Lanchester Theory, Studies in Defense Policy, The Brookings Institution, Washington 1985, p. 123.

Model walki Epsteina definiuje następujące zmienne:

$A_g(t)$ - siły atakującego w kolejnych umownych jednostkach czasu,

$\alpha_g(t)$ - współczynnik tempa prowadzenia ataku w danej chwili czasu t,

$\alpha(t)$ - dzienny współczynnik tempa strat,

α_{aT} - progowa wartość współczynnika strat,

$D_g(t)$ - współczynnik strat obrony w kolejnych umownych okresach czasu,

ρ - stosunek strat strony atakującej w stosunku do strony broniącej się,[59]

α_{dT} - progowa wartość współczynnika strat, zależna od sposobu wycofywania,

$\alpha_d(t)$ - bieżący współczynnik strat obrony,

$W(t)$ - tempo wycofywania (jednostki prędkości),

$W_{\max}$ - maksymalne tempo wycofywania (jednostki prędkości),

t - czas (jednostki umowne), $t = 1,2,3,...$

Uwzględniając wsparcie sił powietrznych, wprowadza się:

$D_a(t)$ - siły strony broniącej się w danej chwili czasu t,

$A_a(t)$ - siły strony atakującej w danej chwili czasu t,

K_a - straty obrony w pojazdach pancernych, w stosunku do strony atakującej,

K_d - straty w pojazdach pancernych, w stosunku do strat obrony przypadających na pojedynczą operację bojową,

S_a - bieżący współczynnik strat strony atakującej,

S_d - tempo operacji lotniczej w danej chwili t,

V - straty w pojazdach pancernych (przypadające na dywizję),

L - straty bezpowrotne (przypadające na dywizję),

α_{da} - współczynnik strat obrony w pojedynczym locie bojowym,

α_{aa} - współczynnik strat strony atakującej w pojedynczej operacji lotniczej,

$ACAS(t)$ - straty bezpowrotne poniesione w jednostkowym (umownym) przedziale czasu przez stronę broniącą się,

$DCAS(t)$ - straty bezpowrotne poniesione w jednostkowym (umownym) przedziale czasu przez stronę atakującą.

---

[59] W tym modelu ρ jest interpretowane jako stała uśredniona, zależna od czasu, w przeciwieństwie do modelu Lanchestera, gdzie mimo, że pochodne dR(t) i dB(t) są funkcją czasu, to stosunek b/r pozostaje stały.

Równania:

$$A_g(t) = A_g(t-1)\cdot[1-\alpha(t-1)] - DCAS(t-1), \tag{2.29}$$

$$D_g(t) = D_g(t-1) - \frac{\alpha(t-1)}{\rho}\cdot A_g(t-1) - ACAS(t-1), \tag{2.30}$$

gdzie: $\alpha(t) = \alpha_g(t)\cdot\left[1-\frac{W(t)}{W_{\max}}\right]$. (2.31)

Tempo wycofywania dane jest funkcją:

$$\begin{cases} 0 & ; \quad \alpha_d(t-1) \le \alpha_{dT} \\ W(t-1) + \left[\frac{W_{\max} - W(t-1)}{1-\alpha_{dT}}\right]\cdot[\alpha_d(t-1) - \alpha_{dT}] & ; \quad \alpha_d(t-1) > \alpha_{dT} \end{cases}, \tag{2.32}$$

przy czym:

$$\alpha_d(t) = \frac{D_g(t) - D_g(t+1)}{D_g(t)}\ . \tag{2.33}$$

Podstawiając $W(1) = 0$, dla strony atakującej można napisać, że:

$$\alpha_g(t) = \alpha_g(t-1) - \left[\frac{\alpha_{aT} - \alpha_g(t-1)}{\alpha_{aT}}\right]\cdot[\alpha_a(t-1) - \alpha_{aT}], \tag{2.34}$$

gdzie:

$$\alpha_a(t) = \frac{A_g(t) - A_g(t+1)}{A_g(t)}\ . \tag{2.35}$$

Wyrażenia na współczynniki $DCAS(t)$ i $ACAS(t)$ są zupełnie symetryczne:

$$DCAS(t) = \frac{L}{V}\cdot D_a(1)\cdot(1-\alpha_{da})^{S_d(t-1)}\cdot\left[K_d\sum_{i=1}^{S_d}(1-\alpha_{da})^i\right], \tag{2.36}$$

oraz

$$ACAS(t) = \frac{L}{V} \cdot A_a(1) \cdot (1-\alpha_{aa})^{S_d(t-1)} \cdot \left[K_a \sum_{i=1}^{S_a} (1-\alpha_{aa})^i \right]. \tag{2.37}$$

Przy czym:

$$D_a(t) = D_a(1) \cdot (1-\alpha_{da})^{S_d(t-1)}, \tag{2.38}$$

oraz

$$A_a(t) = A_a(1) \cdot (1-\alpha_{aa})^{S_a(t-1)}. \tag{2.39}$$

Uwzględniając postęp geometryczny, równania (2.26) i (2.27) można zapisać następująco:

$$DCAS(t) = \frac{L}{V} \cdot D_a(1) \cdot (1-\alpha_{da})^{S_d(t-1)} \cdot K_d \left[\frac{1-(1-\alpha_{da})^{S_d+1}}{\alpha_{da}} - 1 \right], \tag{2.40}$$

oraz

$$ACAS(t) = \frac{L}{V} \cdot A_a(1) \cdot (1-\alpha_{aa})^{S_a(t-1)} \cdot K_a \left[\frac{1-(1-\alpha_{aa})^{S_a+1}}{\alpha_{aa}} - 1 \right]. \tag{2.41}$$

DYNAMICZNY MODEL PRZEWAGI

Dane są początkowe siły dwóch stron: R i B, których wielkość oznaczono przez R_0 oraz B_0. Pojęcie sił początkowych jest rozumiane szeroko i stanowi o potencjalnych możliwościach każdej ze stron. To od nich zależy w głównej mierze powodzenie bądź porażka przyszłych działań zbrojnych. Zatem, siły początkowe o których tu mowa są wielkościami całkowitego początkowego potencjału bojowego stron konfliktu zbrojnego. Proponuje się, stosunek sił podawać w postaci:[60]

$$\frac{R}{B}(t) = A \cdot f[\alpha(t), \beta(t)], \tag{2.42}$$

gdzie $\alpha(t)$ i $\beta(t)$ są współczynnikami zmiennymi w czasie wprowadzonymi do modelu celem określenia czynników stymulujących i utrudniających działania strony R w odniesieniu do strony B,

A - stała,

t - czas.

Pomiędzy współczynnikami $\alpha(t)$ i $\beta(t)$ zachodzi zależność:

$$\alpha(t)+\beta(t)=1, \qquad \text{dla} \qquad t=1,2,3,...,t_{max}, \tag{2.43}$$

przy spełnionych warunkach: $0 \le \alpha(t) \le 1$ oraz $0 \le \beta(t) \le 1$.

Zależnie od wartości $\frac{R}{B}(t)$ w danym czasie, można mówić o przewadze nad przeciwnikiem (wartość powyżej jedności) lub jej braku.

Wartość stałej A jest łatwa do obliczenia (przy znanej postaci funkcji $f[\alpha(t),\beta(t)]$), z zależności: $\frac{R}{B}(t_0=0)=\frac{R_0}{B_0}=A\cdot f[\alpha(t_0),\beta(t_0)]$,

$$A=\frac{R_0}{B_0\cdot f[\alpha(t_0),\beta(t_0)]}. \tag{2.44}$$

Funkcję $f[\alpha(t),\beta(t)]$, określono tak aby jak najlepiej opisać proces tworzenia przewagi. Funkcja ta powinna przyjmować wartość równą jedności dla $\alpha=1$ i $\beta=0$ (strona przeciwna nie stawia oporu - wariant zaskoczenia). W przypadku $\alpha=0$ i $\beta=1$ wartość funkcji powinna być nieokreślona – absurdalne warunki początkowe, walka pozbawiona jest sensu przy współczynniku stymulującym równym zeru. Do dalszych rozważań użyto funkcji logistycznej.

Rozważmy problem prognozowania na podstawie tendencji rozwojowych, występujący w ekonometrii. Jest to przykład modelu interdyscyplinarnego. Interdyscyplinarność modelu wynika między innymi z faktu zastosowania w modelu funkcji logistycznej. Wśród tej klasy modeli najczęściej są wykorzystywane funkcje trendu. Mimo pewnych zalet, funkcje te mają ograniczony zasięg wykorzystywania. Niewiele jest takich zjawisk rzeczywistych, które dają się dobrze opisać tylko za pomocą zmiennej czasowej. Związki przyczynowo-skutkowe są bardziej stabilne od modeli, w których zmienną objaśniającą jest czas. Praktyczne postępowanie przy wykorzystaniu do celów prognozowania funkcji trendu polega

---

[60] Analityczna postać modelu tworzenia przewagi została zasygnalizowana w pracy H.Spustek, Analizy

na oszacowaniu parametrów kilku lub kilkunastu wariantów takiej funkcji a następnie, na podstawie otrzymanych statystyk, wybraniu wariantu najlepszego. Podstawą oceny, są wartości współczynnika determinacji, wielkości ocen średnich błędów estymatorów, statystyka Durbina-Watsona itp.

Funkcja logistyczna jest jedną z podstawowych funkcji trendu i zajmuje wyjątkowo uprzywilejowane miejsce wśród bardzo wielu różnych postaci funkcji używanych do opisu zjawisk ekonomicznych i przyrodniczych. Wynika to stąd, że wzrost organizmów zwierzęcych i roślinnych, liczebność organizmów żywych bytujących w określonych warunkach, jak i produkcja całych gałęzi przemysłu, przebiegają w sposób dający się opisać krzywą logistyczną. Jej równanie można uzyskać na drodze dedukcyjnej wychodząc z rozważań fizykalnych. Równaniem krzywej logistycznej możemy opisać wszystkie zjawiska, których prędkość rozwoju jest wprost proporcjonalna do iloczynu osiągniętego wzrostu nazywanego czynnikiem rozpędu, oraz do odległości tego wzrostu od poziomu nasycenia (a-y), który możemy nazwać czynnikiem hamowania, gdyż z upływem czasu wartość tego czynnika maleje.

Otrzymujemy równanie różniczkowe noszące nazwę prawa wzrostu Robertsona:

$$\frac{dy}{dx} = ky(a - y), \qquad (2.45)$$

gdzie: $k > 0$ jest współczynnikiem proporcjonalności,

a jest poziomem nasycenia (rzędną asymptoty krzywej logistycznej).

Postać funkcji logistycznej (zależna od wartości jej parametrów) wykorzystywana jest między innymi w ekonometrii do wyznaczania trendu logistycznego.[61]

---

porównawcze potencjałów bojowych zgrupowań wojsk w konflikcie zbrojnym, AON, Warszawa 2002 s.41-56.

[61] Zainteresowanie krzywą logistyczną sięga końca XIX wieku. Pionierem był P. F. Verhulst, a pierwszym propagatorem jej wykorzystania R. F. Pearl. To on nadał jej ostateczną postać stosowaną z dużym powodzeniem do dzisiaj. Demografowie (np. A.J. Lotka) i biolodzy jako pierwsi próbowali posłużyć się krzywą logistyczną do wyrażenia prawa rozwoju populacji. Krzywą logistyczną można dobrze dopasować do szeregu czasowego obrazującego ilościowy wzrost organizmów żywych w ustalonych warunkach (określony zapas żywności lub określony dopływ żywności). Krzywa ta może również dobrze opisywać wzrost ilościowy organizmów żywych wszędzie tam, gdzie nie nastąpiła jeszcze ingerencja człowieka w ich życie, np. w rezerwatach ścisłych czy niedostępnych obszarach. Wzrost populacji ludzkiej nie rozwija się dokładnie według tej krzywej. Wpływa na to wiele warunków społeczno-ekonomicznych oddziałujących na zasoby żywności. Podważyło to możliwość wykorzystania krzywej logistycznej jako uniwersalnego prawa rozwoju populacji. Wykazano, że rozwój ludności Szwecji przebiegał zgodnie z krzywą logistyczną. Rozwój ten w ciągu ostatnich dwóch stuleci odbywał się prawie w izolacji (nie oddziaływały na niego w znacznym stopniu czynniki zewnętrzne).Funkcja logistyczna dobrze opisuje popyt na dobra trwałego użytku, np. na samochody w krajach wysoko rozwiniętych, na telewizory , na motocykle i motorowery, na motocykle i skutery, na radioodbiorniki; dobrze obrazuje również wzrost liczby abonentów telefonicznych w Polsce. W Polsce zastosowano funkcję logistyczną do badania popytu na dobra trwałego użytku. Na podstawie danych dotyczących stanu posiadania motocykli i rowerów w gospodarstwach wiejskich w Polsce w latach 1951-1962 dokonano ekstrapolacji powstałej funkcji na lata 1963-1966. Podkreślono przy tym, że funkcja logistyczna może dawać dobre prognozy krótkoterminowe i średnioterminowe, natomiast prognozy długoterminowe są ryzykowne. Za pomocą funkcji logistycznej

Rozdzielając zmienne w równaniu (1.1) otrzymujemy:

$$\left(\frac{1}{y}+\frac{1}{a-y}\right)dy = akdx, \qquad (2.46)$$

co po rozwiązaniu względem y prowadzi do wzoru:

$$y = \frac{a}{1+e^{-akx-C_1}}, \qquad (2.47)$$

gdzie C_1 jest dowolną stałą.[62]

Podstawiając $c = ak$ oraz $b = e^{-C_1}$ otrzymujemy równoważną postać krzywej logistycznej:

$$y = \frac{a}{1+be^{-cx}}, \qquad (2.48)$$

wykorzystaną w dalszej części dysertacji.[63]

Powyższa funkcja jest nieliniową funkcją trzech parametrów a, b, c. Można wykazać, że funkcja jest stale rosnąca, najpierw w tempie coraz bardziej przyspieszonym $(y'' > 0)$, a następnie w tempie malejącym $(y'' < 0)$, aż do niemal całkowitego zahamowania wzrostu, o czym świadczy fakt, że krzywa zbliża się asymptotycznie do prostej $y = a$, co określa się stwierdzeniem, że z biegiem czasu krzywa logistyczna gaśnie. Wynika stąd, że obserwowany gasnący wzrost badanego procesu zmierza do stanu stagnacji.[64]

Funkcja logistyczna (opisana wyżej) została wykorzystana w proponowanym modelu przewagi.[65]

Znaczenie parametru a łatwo wynika z charakteru zjawiska przewagi.

---

możemy opisać zależność wydajności pracy od stażu pracy na ustalonym stanowisku w przypadku pracowników, którzy nie przekroczyli wieku 50 lat (po przekroczeniu tej granicy wieku wydajność spada). Warto podkreślić, że przy powyższej aproksymacji pomijamy wpływ postępu technologicznego. Krzywa logistyczna dobrze opisuje zmiany szybkości pewnych zjawisk chemicznych, np. szybkości rozpuszczania się soli w wodzie. Podobnie, zależność wielu reakcji od czasu ich trwania, zwłaszcza reakcji syntezy, np. reakcji wody z karbidem, w wyniku której otrzymujemy acetylen. W. Winkler zaproponował użycie krzywej logistycznej do opisu zmian gęstości sieci dróg kolejowych na określonym terenie. Funkcję logistyczną zastosowano w medycynie (np. rozwój pewnych chorób w organizmie) i farmakologii (sposób dawkowania niektórych leków). Podjęto również próby wykorzystania krzywej logistycznej w rehabilitacji i antropologii.

[62] S. Smolik, Wyznaczanie parametrów krzywej logistycznej, Przegląd statystyczny R.XXXII- zeszyt 4-1985, s.365 – 373.

[63] H.Hotelling, Differential Equations Subject to Errors and Population Estimates, Journal of the American Statistical Association, 1927 s. 283 –292.

[64] L.Fahrmeir, G.Tutz, Multivariate Statistical Modelling Based on Generalized Linear Models, Springer, New York 2001, s.403-404.

[65] patrz: H. Spustek, Przewaga w walce i operacji, rozprawa habilitacyjna, AON, Warszawa 2002r.

Punkt kulminacyjny następuje przy $\frac{R}{B}=1$, co praktycznie oznacza przerwanie walki.[66] Współczynnik k określający prędkość zbliżania się do punktu kulminacyjnego (tzn. prędkość z jaka następuje wyrównanie sił walczących stron) jest równy współczynnikowi utrudniającemu walkę - β. Pozostaje jeszcze obliczenie współczynnika b występującego w równaniu (2.48). Wykonano to w sposób prosty, podobnie jak w opisanym wcześniej modelu Epsteina:

$$\begin{aligned} & t=0 \Rightarrow \frac{R}{B}(0)=\frac{R_0}{B_0}=\frac{1}{1+be^0} \\ & R_0(1+b)=B_0 \\ & b=\frac{B_0}{R_0}-1 \end{aligned} \qquad (2.49)$$

Teraz, wystarczy wstawić zależność (2.49) do (2.48) i wykonać elementarne przekształcenia algebraicznych otrzymując:

$$\begin{aligned} \frac{R}{B}(t) &= \frac{1}{1+\left(\frac{B_0}{R_0}-1\right)\cdot e^{-\beta t}}=\frac{R_0 e^{\beta t}}{R_0\left(e^{\beta t}-1\right)+B_0}= \\ &= \frac{B_0\cdot\frac{R_0}{B_0}e^{\beta t}}{B_0\cdot\left[\frac{R_0}{B_0}\left(e^{\beta t}-1\right)+1\right]}=\frac{k'\cdot e^{\beta t}}{k'\cdot\left(e^{\beta t}-1\right)+1}= \\ &= \frac{e^{\beta t}}{e^{\beta t}-1+\left(k'\right)^{-1}} \end{aligned} \qquad (2.50)$$

Zatem, proponuje się wyrażenie stosunku sił walczących stron poprzez następującą zależność:

$$\frac{R}{B}(t)=\begin{cases} \frac{R_0}{B_0} & dla \quad \alpha=1,\beta=0 \\ \frac{e^{\beta t}}{e^{\beta t}-1+k'} & dla \quad \beta\in(0,1) \\ nieokreslony & dla \quad \alpha=0,\beta=1 \end{cases}, \qquad (2.51)$$

[66] „Punkt kulminacyjny traktuje się w natarciu jako okres w czasie i przestrzeni, gdy potencjał bojowy (siła bojowa) strony prowadzącej natarcie przestaje być wieksza niż możliwości obrońcy. Natomiast strona broniąca się osiąga punkt kulminacyjny, gdy nie jest już w stanie wykonać zwrotu zaczepnego lub kontynuować skutecznej obrony." - patrz: praca zbiorowa pod kier. M.Huzarski, Taktyka ogólna wojsk lądowych, AON, Warszawa 2001, s.8.

gdzie: $k' = \left(\frac{R_0}{B_0}\right)^{-1}$ określa odwrotność początkowego stosunku potencjałów bojowych strony R do strony B.

Stosunek sił początkowych stanowi w głównej mierze o powodzeniu, bądź porażce działań zbrojnych w ich początkowej fazie. Zatem, siły początkowe o których tu mowa są wielkościami całkowitego początkowego potencjału bojowego stron konfliktu zbrojnego R_0 oraz B_0. Wielkości te można interpretować, tylko wówczas, gdy rozważamy ich wzajemne stosunki, nigdy wartości bezwzględne.

Zadaniem współczynników α i β jest odzwierciedlenie mechanizmów wpływających pozytywnie i negatywnie na wynik walki a tym samym na przewagę nad przeciwnikiem. W celu określenia wartości liczbowych tych współczynników, należy rozpoznać czynniki tworzenia przewagi w danych warunkach operacyjnych lub taktycznych oraz określić wymierne sposoby jej oceny.

LITERATURA DO ROZDZIAŁU DRUGIEGO

1. Balcerowicz B, Wybrane problemy obronności państwa, materiał studyjny, AON, Warszawa 1999.
2. Balcerowicz, Pokój i „nie-pokój", Bellona, Warszawa 2001.
3. Ciechanowicz M. i inni, Wybrane metody optymalizacji decyzji, MON, Warszawa 1969.
4. Galewski Z., Czynniki powodzenia we współczesnej walce, Wyd. MON, Warszawa 1986.
5. Ciborowski L., Polko R., Planowanie i organizowanie walki zbrojnej według poglądów NATO, cz.II, Informacyjna preparacja pola walki, AON, Warszawa 1996.
6. Goban-Klas T., Sienkiewicz P., Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania, Wyd. Fundacji Postępu Telekomunikacji, Kraków 1999.
7. Gwóźdź E., Pojęcie przewagi i jej tworzenie na przykładach historycznych, AON, Warszawa 1972.
8. Huzarski M., Taktyka ogólna wojsk lądowych, AON, Warszawa 2001.
9. Jarecki Cz., Przewaga ogniowa warunkiem powodzenia działań zaczepnych. Sposoby jej uzyskania i utrzymania, AON, Warszawa 1992.
10. Joshua M. Epstein, The Calculus of Conventional War Dynamic Analysis without Lanchester Theory, Studies in Defence Policy, The Brookings Institution, Washington 1985.
11. Koziej S., Podstawy i zasady sztuki wojennej, Warszawa 1993.
12. Kulikowski R., Libura M., Słomiński L., Wspomaganie decyzji inwestycyjnych, IBS PAN, Warszawa 1998.
13. Nożko K., Sztuka tworzenia przewagi w systemie obronnym RP, Bellona, Warszawa1994.
14. Nożko K., Walka o przewagę, Wyd. MON, Warszawa 1985.
15. Mossor S., Sztuka wojenna w warunkach nowoczesnej wojny, Wyd. MON, Warszawa 1986.
16. Krasnoszczekow P.S,.Pietrow A.A, Princypy postrojenia modelej, Moskwa 1983.
17. Regan G., The Guinness Book of Military Blunders, Guinness Publishing, London 1991.
18. Regulamin działań wojsk lądowych, Warszawa 1999.
19. Rybár M. i inni, Modelovanie a simulácia vo vojenstve, Ministerstvo Obrany Slovenskiej Republiky, Bratislava 2000.
20. Ścibiorek Z., Rozważania o obronie, Bellona, Warszawa 1993.
21. Ścibiorek Z., Wojna czy pokój?, Ossolineum, Wrocław 1999.
22. Ścibiorek Z., W.Kaczmarek, Przyszle pole walki, AON, Warszawa 1995.
23. Sikorski B., Tworzenie i wykorzystanie przewagi w walce i operacji, AON, Warszawa 1990.
24. Skibiński F., Rozważania o sztuce wojennej, Warszawa 1972.

25. Spustek H., Analizy porównawcze potencjałów bojowych zgrupowań wojsk w konflikcie zbrojnym, AON, Warszawa 2002.

26. Spustek H., Analizy porównawcze potencjałów bojowych zgrupowań wojsk w konflikcie zbrojnym, AON, Warszawa 2002.

27. Spustek H. Przewaga w walce i operacji – rozprawa habilitacyjna, Warszawa AON 2002.

28. Stefanowicz J., Rzeczypospolitej pole bezpieczeństwa, Wyd. Adam Marszałek, Warszawa 1993.

29. The Dynamics of Military Combat, Operations Research, Vol.7, Jan.-Feb. 1959, pp.30-49, P.M.Morse, and G.E.Kimball, Methods of Operations Research, MIT Press and Wiley, New York, 1951, pp. 71-73), model Helmbold'a (patrz: R.L.Helmbold, Decision in Battle: Breakpoint Hypotheses and Engagement Termination Data, Rand Corp., Santa Monica, CA, Rept. R-772-PR, June 1971).

30. Toffler A.H., Wojna i antywojna, Warszawa 1997.

31. Toffler A., Trzecia fala, PIW, Warszawa 1997.

32. Wiatr M., Działania operacyjne według poglądów NATO, Warszawa 1988.

33. Wołejszo J., Sposoby obliczania potencjału bojowego pododdziału, oddziału i związku taktycznego, AON, Warszawa 2002.

34. Zieliński J., Teoretyczne podstawy walki zbrojnej, W-wa 1995.

35. Zubek J., Rozprawa habilitacyjna, dodatek C/8300,AON, Warszawa 1990.

3. ASYMETRIA INFORMACJI W SYTUACJACH DECYZYJNYCH

3.1. PRZEWAGA INFORMACYJNA W DZIAŁANIU

Obecnie odnotowujemy zjawisko tzw. Kompresji czasu i przestrzeni. Zjawiska te niosą ze sobą bardzo daleko idące konsekwencje dla efektywnego funkcjonowania instytucji. W przypadku działań na arenie rynkowej firmy muszą uzyskiwać przewagę w najróżniejszych obszarach swojej działalności. Obserwując wykorzystanie znajomość najróżniejszych technik zarządzania firmami nastąpiła dzisiaj daleko idąca standaryzacja metod i technik zarządzania. Przenikanie się metod zarządzania powoduje proces tworzenia coraz lepszych podręczników pozwalających na racjonalne wykorzystanie powszechnie stosowanych metod zarządzania. Obserwujemy więc zjawisko jasnego definiowania metod postępowania umożliwiającego przewidywanie zachowania się naszego przeciwnika rynkowego. Pozwala to również na takie planowanie naszej działalności, aby możliwym stało się jak najefektywniejsze zarządzanie pozwalające na realizację naszych celów biznesowych. Należy podkreślić fakt, że nasze cele biznesowe powinny być dla nas jasno zdefiniowane, ale jednocześnie trudne do odkrycia dla przeciwnika. Nie należy dzisiaj mówić, że naszym jedynym celem jest zysk, albowiem może on mieć charakter krótkotrwały. Konieczne jest przyjmowanie bardzo szerokich strategii działania pozwalających na przewidywanie i planowanie zysków naszej firmy w szerokiej perspektywie czasu, co jest jawnie sprzecznie z tezą o kompresji czasu.

Planowanie długoterminowe jest możliwe przy wypracowaniu technik pozwalających na zdobycie przewagi informacyjnej, a najlepiej dominacji informacyjnej nad wszystkimi uczestnikami gry rynkowe. Należy przy tym podkreślić fakt trudności zdobycia przewagi informacyjnej nad konkurencją. Spowodowane jest to powszechną standaryzacją metod zarządzania. Nietrudno przewidzieć jak postąpi konkurencja w danych warunkach rynkowych, jeśli stosuje znaną nam metodologie zarządzania i analizy ryzyka związanych z decyzjami operacji pomocniczych.

Wydaje się więc koniecznym uprzedzanie i przewidywanie działań konkurencji w oparciu o skrócenie analiz koniecznych do podjęcia decyzji z jednej strony, a także na podstawie lepszej wiedzy jaka towarzyszy podejmowanej decyzji. Przewagę uzyskamy więc wówczas gdy będziemy lepiej poinformowani i gdy będziemy wiedzieli co w danej sytuacji jest w stanie uczynić przeciwnik. Powstaje pytanie: Na jakiej wiedzy jesteśmy w stanie oprzeć nasze decyzje. Tu zaczyna się problem, ponieważ nasza wiedza składa się z co najmniej dwóch głównych czynników: wiedzy użytecznej i wiedzy bezwartościowej lub

o niewielkiej przydatności. Wiedza użyteczna, to taka wiedza jaka jest nam najbardziej przydatna do podjęcia decyzji w danych okolicznościach. Nie jest to pełna wiedza, ale jedynie ta jaką w danych okolicznościach posiadamy. Stąd, musimy dbać o to by nasza wiedza była najlepszej jakości. Załóżmy, że posiadamy ogromną wiedzę wysokiej jakości. Niestety, sytuacja ta zaczyna nam utrudniać podejmowanie decyzji ponieważ, wydłuża się analiza informacji konieczna do podjęcia właściwej decyzji. Wynika to z faktu posiadania w bazie, informacji o wysokiej jakości, lecz w danych warunkach nieodpowiedniej. Wobec tego, przed każdorazowym podjęciem decyzji, osoba podejmująca decyzję musi dokonać odpowiedniej selekcji już otrzymanych informacji z posiadanego źródła wysokiej jakości i ponownie ocenić jej jakość. Należy podkreślić, konieczność selekcji informacji i stosowania takiej jaka jest nam w danej chwili potrzebna, wystarczająca, być może niepełna ale pewna i odpowiednia do podjęcia rozważanych decyzji.

Rosnący krąg firm stara się uzyskać certyfikację ISO dotyczącą zarządzania. Obok prestiżowych powodów istnieje również ten, interesujący nas najbardziej, aby uzyskać przewagę informacyjną, zarząd firmy zaczyna coraz chętniej wdrażać systemy komputerowe do wspomagania zarządzania swej firmy.

Wiąże się to z rosnącymi kosztami jakie niesie ze sobą stosowanie metod informatycznych w zarządzaniu. Jest to bardzo korzystne jeśli chodzi o czas dostępu do informacji jak i o stale zwiększającą się jakość informacji uzyskiwanych ze skomputeryzowanych systemów zarządzania. Daleko posunięta obecnie standaryzacja tego typu metod zarządzania powoduje obniżenie kosztów inwestycji z jednej strony, ale jednocześnie utrudnia uzyskanie przewagi informacyjnej nad konkurencją z drugiej strony. Czym ten problem jest spowodowany? Odpowiedź na to pytanie wydaje się dość prosta. Nie jest trudno jest zbudować dzisiaj system w którym oprócz informacji o naszej sprzedaży i asortymencie, będziemy również gromadzić podobne informacje o produktach konkurencji. Przykładem tego typu systemów są systemy CRM wspomagające zarządzanie relacjami z klientami. Systemy tego typu starają się nam umożliwić odpowiedź na pytania: "Czego oczekuje od nas nasz klient?", "Jakiego typu naszymi usługami są zainteresowani nasi klienci?", "Co powinniśmy zmienić, aby zaadresować nasze usługi do nie obsługiwanej części naszych przyszłych klientów?" itd. itp.

Jest to z pewnością prawda, ale konkurencja ma już tego typu systemy - takie same (bo standaryzowane, wykorzystujące te same algorytmy przetwarzania, analizy i wnioskowania) i posiada doświadczonych pracowników w ich wykorzystywaniu. Uzyskanie przewagi nad konkurencją wydaje się trudne, ale jest to możliwe. Należy między innymi,

korzystać z doświadczeń innych, ale i nie tylko. Rdzeniem wokół którego możliwe jest wybudowanie przewagi informacyjnej są własne procedury oparte na doświadczeniach firmy i doświadczeniach innych, ale stanowiące integralną własność firmy nieujawnioną konkurencji. Stanowi to jakby trzon decyzyjny opleciony siecią informacyjną firmy. Sprawne funkcjonowanie tego organizmu jest możliwe jeśli przepływy informacyjne wewnątrz firmy zachodzą w sposób płynny bez żadnych zahamowań, jeśli zapewniona jest szczelność w przepływie informacji o charakterze newralgicznym dla działalności firmy.

Co można i należy uczynić aby uzyskać przewagę informacyjną? Przyglądając się systemom informacyjnym należy podkreślić konieczność ich rozbudowy o jak najlepsze moduły pozyskiwania informacji. Przykładem mogą tu być systemy gromadzenia zamówień. Dziś koszt wyposażenia przedstawicieli handlowych (PH) w przenośne komputery czy też różnego rodzaju i-PAQi pozwala na zaoszczędzenie ogromnej ilości czasu koniecznego na wielokrotne przepisywanie danych przez nich wprowadzonych do naszego systemu informacyjnego. Zaoszczędzony czas można przeznaczyć na zlecenie im innych zadań pozwalających na lepsze obserwowanie działań konkurencji. Dodatkową korzyścią z tego typu działań jest to, że wywiad uzyskiwany w trakcie zwyczajnej wizyty handlowej nie budzi niczyich podejrzeń co do pozyskiwania cennych informacji na temat konkurencji. W trakcie dokonywania zamówienia zazwyczaj dokonuje się inwentaryzacji towarów posiadanych przez naszego klienta. Nic nie stoi na przeszkodzie, aby w trakcie tego przeglądu zanotować produkty konkurencji, ich cenę zarówno hurtową jak i detaliczną jak i szacunkową ich ilość. Informacje uzyskane w ten sposób stanowią dobre źródło informacji o tym jak bardzo konkurencja depcze nam po piętach, a także co klienci by kupili i czego brakuje w naszej ofercie. Tak uzyskane cyfrowe źródła informacji stanowią wiarygodne dane umożliwiające szybkie zasilanie danymi naszych systemów przetwarzania wiedzy / informacji. Uzyskujemy przy tym możliwość wprowadzania danych w formacie akceptowanym przez nie ze sprawdzoną ich integralnością i jakością. Zyskujemy też łatwą możliwość oceny pracy naszych PH.

Obserwacja rozwoju technologii wspomagających systemy informacyjne pozwala na stwierdzenie, że obok zapewnienia dostępności do tych systemów konieczne jest zwiększenie bezpieczeństwa usług ponieważ rozwój usług opartych o ww. technologie prowadzi jednocześnie do uzależnienia się od nich. Niestety odporność tego typu systemów na różnego rodzaju zakłócenia jest ciągle trudna do zapewnienia, jednak korzyści wynikające ze stosowania tego typu rozwiązań pozwalają na zwiększenie przewagi informacyjnej nad przeciwnikiem.

Odmienny problem stanowi kreowanie wizerunku przyszłego klienta. W tym obszarze działań, firmy mają bardzo duże osiągnięcia pozwalające na szybki zwrot nakładów finansowych pozwalających na lepsze zrozumienie potrzeb klienta. Obok działań analitycznych z zakresu potrzeb, przeprowadzane są również badania nad zwiększeniem sprzedaży, czy zwiększeniem zapotrzebowania z zakresu już istniejących usług, jak i przekonaniem klienta o naszej „niezastępowalności" w tym zakresie. Rozważając problematykę przewagi informacyjnej i porównując informacje jakie jest w stanie zdobyć nasz obecny lub przyszły klient obserwujemy występowanie zjawiska asymetrii informacyjnej. Jako firma, która poniosła już nakłady finansowe na zdobycie informacji o klienci,e stoimy na twardym gruncie i doskonale zdajemy sobie z tego sprawę na co stać klienta korzystającego z naszego produktu, czy usługi.

Rozwój technik informacyjnych w latach 90-tych XX wieku spowodował głębokie utrwalenie pojęcia wejścia w wiek ery informacyjnej (Information Age). Jasnym jest, że osiągnęliśmy zdolność do gromadzenia, pozyskiwania, manipulowania i wymiany informacji w sposób od którego zaczyna zależeć wszelka działalność. Piętno świadomości faktu, że zaczynamy się coraz bardziej uzależniać od konieczności posiadania informacji zaczyna coraz bardziej skłaniać nas do budowania systemów informacyjnych, których celem jest zapewnienie naszej dominacji nad innymi (w przypadku businessu innymi uczestnikami rynku). Natychmiastowo nasuwa się chęć wykorzystania posiadanych informacji do zwalczania przeciwników.

Aby odpowiedzieć sobie na pytanie, jakie są warunki konieczne do uzyskania przewagi informacyjnej powinniśmy sobie uzmysłowić, dlaczego chcemy uzyskać przewagę informacyjną, jakie korzyści wynikają z faktu uzyskania przewagi informacyjnej. Odpowiedź na pierwsze pytanie wydaje się prosta, bo prowadzi nas do uzmysłowienia sobie chęci uzyskania dominacji informacyjnej. Dominacja informacyjna pozwoliłaby nam na sparaliżowanie wszelkich działań przeciwnika w takim zakresie, w jakim uzyskalibyśmy dominację.

Przykładem przewagi informacyjnej lub wręcz asymetrii informacyjnej może być wszelka działalność firm mających na celu wprowadzenie nowych wyrobów na rynek.

Firmy decydujące się na wprowadzenia nowego wyrobu prowadzą głębokie badania rynku, na który opracowywany jest dany produkt .

Nie jest to obecnie proces prosty i składa się z kilku etapów. W pierwszej fazie odbywa się

badanie rynku, gdzie gromadzimy informację o potencjalnych klientach, staramy się określić przedziały do których kwalifikujemy klientów ze względu na ich zdolności finansowe, a także gromadzimy dane na temat metod jakimi będą badani kienci w trakcie przyszłych kampanii reklamowych. W trakcie tego badania odbywają się wywiady dotyczące kształtu hipotetycznych produktów jakie byłyby najbardziej pożądane przez badanych. Na podstawie wstępnych badań możliwe jest określenie oczekiwanych cech i właściwości produkowanych przez firmę produktów. Historia uczy, że wykorzystanie tej wiedzy pozwala na obniżenie nakładów na wprowadzenie na rynek produktów nowych, bowiem tworzony jest dobry produkt, który nie wymaga reklamy.

Do uzyskania przewagi informacyjnej konieczne jest zapewnienie spełnienia wielu czynników zależnych od stanu w jakim znajdują się podmioty będące przedmiotem rywalizacji.

Jeżeli przewagę informacyjną chcą uzyskać nad sobą dwie firmy rywalizujące o tego samego klienta, konieczne jest zapewnienie odpowiednich warunków w jednej z firm, które umożliwią realizację powyższego zadania.

Ciekawy problem stanowi asymetria informacyjnej, jaka występuje pomiędzy klientem, a sprzedawcą. Sprzedawca dysponuje zazwyczaj dużo większą wiedzą na temat oferowanego przez siebie towaru. Klient chcąc nabyć produkt o jasno przez siebie sprecyzowanych wymaganiach musi rozstrzygnąć, czy prezentowany produkt posiada ww. wymagania, czy tylko sprzedawca upewnia go w słuszności decyzji klienta, nie dbając o spełnienie stawianych wymagań.

Amerykańscy analitycy wojskowi skłaniają się do opinii, że najbardziej zawodnym ogniwem w łańcuchu decyzyjnym jest człowiek. Przekonanie to nie wydaje się zbyt przesadzane, ponieważ człowiek nie kieruje się wyłącznie racjonalną oceną sytuacji, ale w procesie decyzyjnym w jakim bierze udział człowiek występuje również czynnik związany z jego subiektywnymi odczuciami i przekonaniami. Obok tego, możliwy jest czynnik związany z odmową wykonania zadania przez człowieka, a spowodowaną przez różnorodne zabiegi przeciwnika.

Uzyskanie przewagi informacyjnej nabiera coraz większego znaczenia w zastosowaniach militarnych. Dysponując przewagą informacyjną możemy uprzedzić działania przeciwnika lub też lepiej się zabezpieczyć przed jego następstwami. Przykładem mogą być różnego rodzaju inteligentne czujniki wykorzystywane do wykrywania działań przeciwnika. Obecnie czujniki wykorzystywane są na różnych poziomach od zabezpieczania

działań piechoty, aż po rozpoznanie lotnicze i satelitarne. Największym problemem w uzyskaniu przewagi informacyjnej przy stosowaniu ww. środków jest konieczność przestrzegania podstawowych zasad w projektowaniu takich środków, a później znajomość mocnych i słabych cech zastosowanych rozwiązań technicznych w tych środkach technicznych.

"... Zastosowanie nowych rozwiązań technicznych w wielu systemach wojskowych połączonych z nowatorskimi pomysłami i adaptacją organizacyjną w sposób, który zasadniczo zmienia charakter i przebieg konfliktu. Rozwiązania te powodują gwałtowny wzrost efektywności militarnej sił zbrojnych.[67]

W trakcie wojny w Zatoce Perskiej na podkreślenie zasługuje fakt uzyskania przewagi informacyjnej nad przeciwnikiem przez wojska Armii Stanów Zjednoczonych. Przewaga ta wynikała z doskonale zorganizowanej łączności pomiędzy siedzibą głównodowodzącego w USA i wojskami prowadzącymi działania w Zatoce Perskiej. Mimo tego, że system TROJAN SPIRIT zapewniał doskonałą wizualizację działań, to nie zapewniał pełnego sprzężenia zwrotnego pomiędzy sztabem w USA, a oddziałami prowadzącymi działania na pustyni. W pełni zrealizowano śledzenie głównego teatru działań na poziomie sztabów, co z pewnością przyczyniło się do sukcesu działań. Niestety, w systemie tym zabrakło możliwości bezpośredniego wydawania rozkazów przez dowództwo oddziałom realizującym poszczególne działania. Dyspozycje dla oddziałów realizujących plan przychodziły ciągle przez kurierów, co dzisiaj wydaje się być niepotrzebną zwłoką czasu. Jednak rozwiązanie to na pewno miało też i wiele zalet, przy niewydolności informacyjnej na jaką cierpiały wojska irackie. Wydawanie tego typu dyspozycji, pomimo wydłużenia czasu reakcji jest jednocześnie mniej podatne na tzw. zakłócenia informacyjne. Ponieważ częstotliwość wydawania rozkazów w tym trybie sterowania przypomina sterowanie układem dynamicznym w pętli otwartej to należy podkreślić konieczność wydawania rozkazów kompletnych przemyślanych, ponieważ korekcja działań jest możliwa dopiero w następnym cyklu sterowania, który ma miejsce po wysłaniu następnej grupy kurierów z dyspozycjami do poszczególnych oddziałów realizujących operację.

---

[67] Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," The National Interest, No. 37(Fall) 1994, p.30.

3.2. SYSTEMY KOMPUTEROWEGO WSPOMAGANIA DOWODZENIA

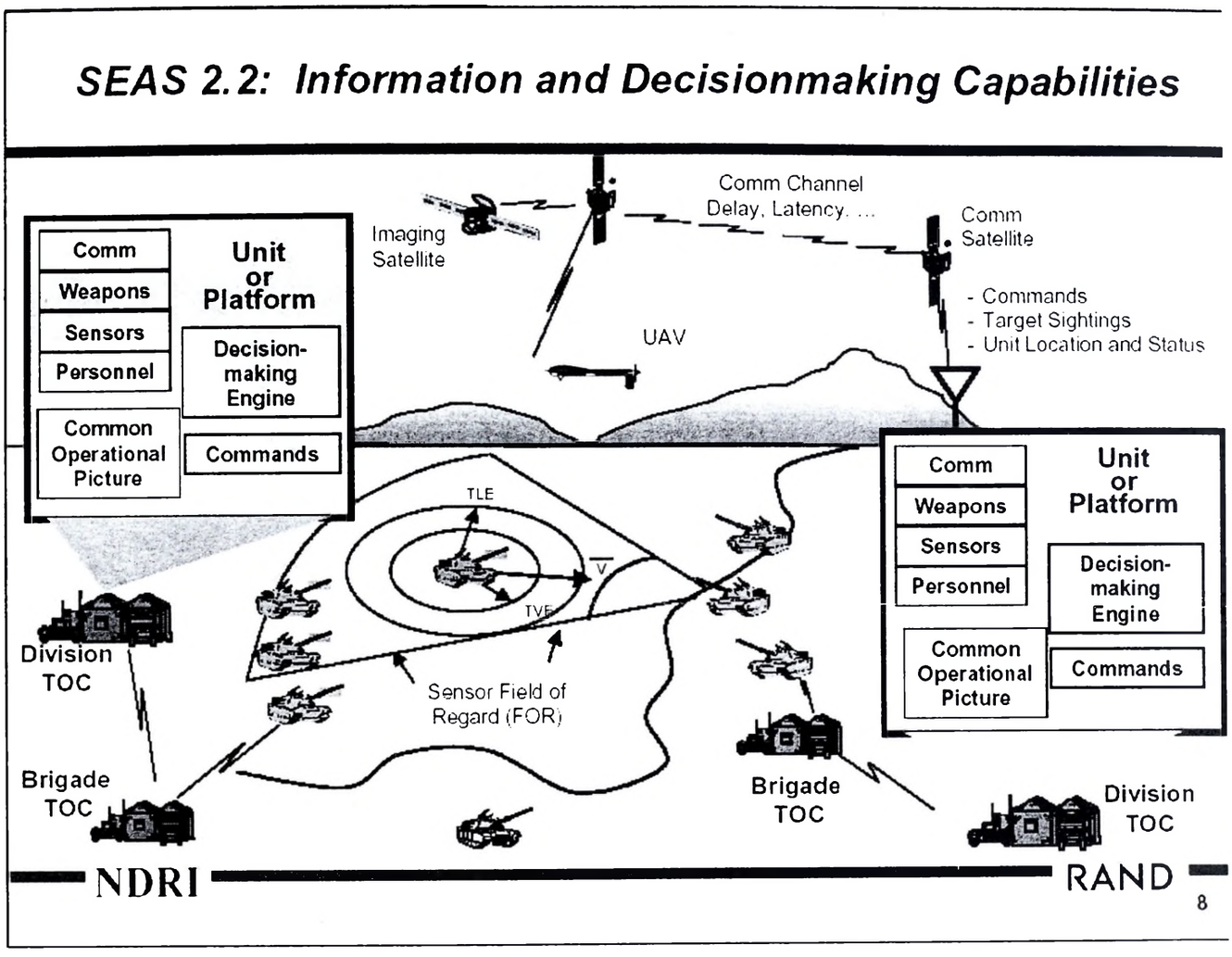
Systemy Commannd, Control, Communcations, Computers, Intelligence, Surveillance, and Reconnaissance (C4IRS) stanowią wojskowy odpowiednik systemów klasy CRM w przypadku sprzedaży. Systemy C4IRS powstały w celu uzyskania przewagi informacyjnej (Information Superiority) nad przeciwnikiem, jak również aby umożliwić gromadzenie, przetwarzanie i rozpowszechnianie nieprzerwanego strumienia informacji, przy jednoczesnym uniemożliwianiu realizacji tych samych celów przeciwnikowi.[68] Przewaga informacyjna jest definiowana jako zdolność do krótszego czasu reagowania, podejmowania lepszych decyzji, ich szybszego wykonania niż nasz oponent. Przewaga informacyjna jest postrzegana jako istota lub pożądany wynik uzyskiwany z systemów IS.[69]

RAND Corporation zaproponowało tego typu system rozbudowując już istniejący system: System Effectivness Analysis Simulation (SEAS) o nowe funkcjonalności i modyfikując zastosowane w nim już istniejące algorytmy. SEAS powstał aby umożliwić szacowanie i ocenę użyteczności systemów kosmicznych, ale został zaadoptowany przez RAND do oceny wartości szerokiego zakresu systemów typu C4ISR. System który posłużył do analizy możliwości uzyskania przewagi informacyjnej jest wersją, która umożliwia modelowanie i integrację adaptacyjnych zachowań w pojedyncze jednostek naziemnych wykorzystywanych w tym modelu.

W proponowanym systemie dowódca dywizji ma dostęp do wywiadu, systemów przetrwania i rozpoznania (ISR) jakie dają bezzałogowe samoloty rozpoznawcze dalekiego zasięgu (UVAs- unmanned areal vehicles). Dowódcy brygad dysponują dostępem do bliższych im systemów (ISR) (bezzałogowe samoloty rozpoznawcze krótkiego zasięgu). Doródcy dywizji i brygad są połączeni ze sobą siecią komunikacyjną, która przekazuje informacje C2 i sygnały ostrzegawcze. W modelu tym czołgi są wyposażone w ich własne systemy i czujniki rozpoznania w podczerwieni (FLIR – Forward Looking Inftared) i są w stanie dzielić się informacją i sygnałami ostrzegawczymi, ze swego poziomu działań, z innymi czołgami na poziomie internetu taktycznego. Opóźnienia jakie występują w dostarczaniu wiadomości w tych systemach mogą być parametrycznie regulowane.

---

[68] DoD Dictionary of Military and Associated Terms, Joint Publications 1-2, Joint Chiefs of Staff, 12 April 2001.
[69] Joint Vision 2020, Joint Chiefs of Staff, November 2000.



Rys.3.1. System Effectivness Analysis Simulation (SEAS).

Algorytm decyzyjny zastosowany w proponowanym modelu jest oparty na korelacji sił i sposobów (COFM – the Correlacjon of Forces and Means). COFM estymuje zdolności naszych sił na podstawie informacji i statusów otrzymywanych z symulowanego pola walki. Estymuje również oddziały wroga kreowane dla specyficznych obszarów pola walki, a oparty na powszechnym (typowym) obrazie operacyjnym (COP – Common Operational Picture) dostępnym dla tych dowódców. Silnik decyzyjny COFM przetwarza uzyskane estymacje w czasie, przestrzeni z uwzględnieniem czynników terenowych aby obliczyć prawdopodobieństwo sukcesu operacji. Algorytmy te pozwalają na porównywanie własnych pozycji i określanie celów i podcelów planowanych operacji. Dowódcy jednostek mogą modyfikować swoje plany manewrowe, operacyjne i stosowane uzbrojenie, korzystając z analiz sytuacji wizualizowanej w ich lokalnym COP.

3.3. PROBABILISTYCZNY MODEL WIEDZY

Dowódcy zawsze poświęcali znaczne zasoby aby doskonalić wywiad i rozpoznanie, a jednocześnie starali się chronić informacje o swoich siłach przed wrogiem, stosując różnego typu wybiegi i kamuflaż. Postępowanie takie wynikało z założenia, że im więcej wiedzy posiadają dowódcy o sytuacji na polu bitwy, a zwłaszcza o siłach przeciwnika, tym lepiej są w stanie wykorzystać swoje siły i łatwej im będzie uzyskać nad nim dominację. Rzeczywiście, jest wiele przykładów w historii, które pozwalają na dowiedzenie tej tezy.

Niestety niewiele jak dotąd zrobiono, aby określić jasne relacje pomiędzy informacją, a tym jaki ma ona wpływ na wynik operacji militarnej. Spowodowane jest to problemem jaki niesie ze sobą określenie sposobów w jaki informacja wpływa na operacje militarne. Załóżmy, że dowódca zna położenie 30 procent wrogich sił. Możemy rozpatrzyć kilka wariantów jakie może on podjąć w zależności od sytuacji:

- Jeżeli posiada on duży wachlarz różnych rodzajów uzbrojenia, z różnorodną amunicją, może potraktować pozycje przeciwnik jako cele i zaatakować jak najbardziej dopasowaną amunicją do charaktery celów jakie planuje zniszczyć. W tym przypadku ograniczona wiedza pozwala mu na zniszczenie 30 procent celów lub więcej i ten wynik potraktowany zostanie jako wynik "dobry".
- Jeśli uważa on, że przeciwnik posiada przewagę lub też nie posiada wystarczającego uzbrojenia aby zagwarantować sobie zniszczenie 30 procent znanych pozycji przeciwnika to może zadecydować o unikaniu starcia z przeciwnikiem, do momentu aż otrzyma wymagane wsparcie lub więcej informacji o przeciwniku, albo też otrzyma inne cele taktyczne. Ten wynik może być korzystny dla przeciwnika, ponieważ występuje opóźnienie, które pozwala przeciwnikowi na przygotowanie i przeprowadzenie własnego ataku.
- Nawet jeśli ma wystarczająco dużo siły, aby podjąć walkę i zniszczyć wszystkie znane pozycje przeciwnika, może uznać za stosowane poczekać na dalsze informacje o położenie pozostałych 70 procent wrogich sił mając nadzieję że informacje te wkrótce nadejdą. Tak, jak w powyższym przypadku może to doprowadzić do przewagi przeciwnika.

Jeśli dodamy to, co wie nasz przeciwnik to uzyskamy kilka dalszych możliwości, jakie opisana sytuacja niesie ze sobą. Problem stanowi to, że nie istnieje prosta relacja pozwalająca na wyznaczenie zależności pomiędzy dostępną informacją jaką posiada dowódca, a najlepszą możliwą realizacją postawionego zadania. Poza tym, należy uwzględnić udział jeszcze wielu innych czynników. Nie oznacza to jednak, że nic nie możemy zrobić. Istnieją zasady jakie otrzymano w wyniku analizy kilku szczególnych przypadków.

3.4. WIEDZA ORAZ NIEWIEDZA I ICH WARTOŚCI

Informacja ma dwa istotne atrybuty: wartość i jakość. Informacja przedstawia sobą wartość jeśli informuje dowódcę i dodaje nowe elementy do wiedzy posiadanej przez niego o sytuacji bojowej. Konsekwencją tego jest to, że jeżeli odwołuje się on do "wiedzy" to oznacza to, że jest ona istotna i dlatego jest "wartościową" informacją. Jakość informacji zależy od jej precyzji, dokładności, aktualności i kompletności. Jakość informacji może przedstawiać sobą małą wartość lub też być kompletnie bezwartościowa (np.: nadaje informacji inne uboczne znaczenie) i dlatego może zostać odrzucona z posiadanej wiedzy.

W trakcie gromadzenia informacji z różnych sensorów i różnorakich źródeł, dowódca poszukuje informacji, które posiadają wartość, a są określane terminem (CEI – critical elements of information). Problem polega na tym, że rzadko jesteśmy w stanie trafnie ocenić jakość informacji jaką właśnie otrzymujemy. W konsekwencji tego, dowódca musi zdawać sobie sprawę z tego, że część "wiedzy" może być zbyteczna. Przypuśćmy, że przeciwnik używając zaawansowanych technik maskowania i imitacji spowodował, że nasz dowódca zna rzeczywiście położenie połowy obiektów, spośród tych których sądzi, że zna. Powoduje to powstanie kilku dodatkowych kwestii, które musi uwzględnić dowódca w trakcie podejmowania decyzji. Jeśli podejrzewa, że jest wprowadzony w błąd, może poczekać do momentu w którym dotrą do niego pewniejsze informacje. Jeśli zaś nic nie podejrzewa, to może postąpić ponownie jak przedtem, otrzymując inny i prawdopodobnie mniej imponujący wynik. Powyższe rozważanie sugeruje konieczność zastosowania użytecznej metody oceny informacji. Niech **K** będzie miarą wartości informacji lub wiedzy dostępnej dla dowódcy. W niektórych przypadkach **K** może być wartością liczbową, przykładowo: jeśli przeciwnik posiada **N** oddziałów (jednostek), wówczas **K=0.3 N**.

Oznacza to, że dowódca zna położenia **0.3N** wrogich oddziałów. Dla obu stron **K** zawiera

dwa komponenty : wiedzę o informacjach wysokiej jakości i wiedzę o informacjach niskiej jakości lub bezwartościowej wiedzy $\mathbf{K} = \mathbf{K_C} + \mathbf{K_i}$. W przykładzie: $\mathbf{K_C} = \mathbf{K_i} = \mathbf{0,15\ N}$. W typowych przypadkach **K** jest wielowymiarowe, zawiera wiele informacji takich jak wolę walki przeciwnika, identyfikację jednostek itp. Warto odnotować fakt, że w większości przypadków dowódcy nie wiedzą że są wprowadzeni w błąd przez działania przeciwnika.

3.5. OCENA WIEDZY

W walce, obszar działania (AO- area of operation), wiedza i manewr rywalizują ze sobą, aby zapewnić efektywne wykorzystanie siły ognia. Kiedy jednostka pojawia się w obszarze działań możemy oczekiwać że będzie zorientowana na działania ofensywne bądź też defensywne. Przeciwnik jest wówczas graczem, chcącym w aktywny sposób osiągnąć postawione sobie cele, w tym samym czasie stara się uniemożliwić realizację i osiągnięcie naszych celów.

Definicja 1: Oddział kontroluje obszar jeśli jest w stanie operować w nim bez przeszkód. Nie oznacza to, że przeciwnik jest wyeliminowany z tego obszaru, a jedynie że sprzymierzone oddziały są w stanie wywierać wpływ na wszystkie punkty w danym obszarze przez cały czas.

Definicja 2: Promień kontroli oddziału jest to minimum z: maksymalnego efektywnego zasięgu ognia danego oddziału i ognia systemów broni wsparcia w_i, maksymalny efektywny zasięg lokalnych systemów rozpoznania s_i i promienia operacji c_i.

$$r_i = \min\{w_i, s_i, c_i\} \qquad (3.1)$$

Definicja 3: Wiedza jest to stopień w jakim dowódca jednostki zna położenie jednostek przeciwnika i naszych w swoim promieniu działania.

Oznaczmy wiedzę jednostek niebieskich i oraz czerwonych j jako $K_{B,i}$ oraz $K_{R,j}$.

Świadomość sytuacyjna według definicji 3 może zostać porównana do wiedzy o CEI i może zawierać tak trudne elementy jak ocena postawy bojowej przeciwnika i jego intencje. CEI lub istotny element informacji są składnikami informacji koniecznymi do wyznaczenia wspólnego obrazu przestrzeni bojowej i stopnia w jakim ten obraz jest jasny dla dowódcy jednostki, oceniającego swoją świadomość sytuacyjną lub wiedzę.

W naszych rozważaniach, bardziej istotnym jest liczba obcych celi w j – tym celu zainteresowania (TAI – target area of interest), niż wiedza o położeniu n celi w obszarze promienia kontroli. Rys. 3.2. przedstawia trzy TAI w danym, kontrolowanym obszarze.

W przypadku gdy, liczba obcych celi w każdym kontrolowanym obszarze jest równa μ_j, wówczas mamy $\sum_j \mu_j \le n$. Dla uproszczenia zakładamy, że TAIs nie nakładają się na siebie, wobec czego suma wiedzy walczących ze sobą dowódców jest w przybliżeniu równa całkowitej liczbie celów przeciwnika w TAIs. W tym przypadku $K = \sum_{j=1}^{3} \omega_j K_j$, gdzie K_j jest wiedzą o lokalizacji celi w TAI_j i ω_j jest względną ważnością TAI_j obu dowódców $\left(\sum_{j=1}^{3} \omega_j = 1\right)$. Średnia wiedza wynosi $K = \frac{1}{3} \cdot \sum_{j=1}^{3} K_j$. Metryka wiedzy w tym przypadku jest średnią wiedzą ważoną nad TAIs i przedstawia poziom sytuacyjnej świadomości dowódcy.

WIEDZA RELATYWNA

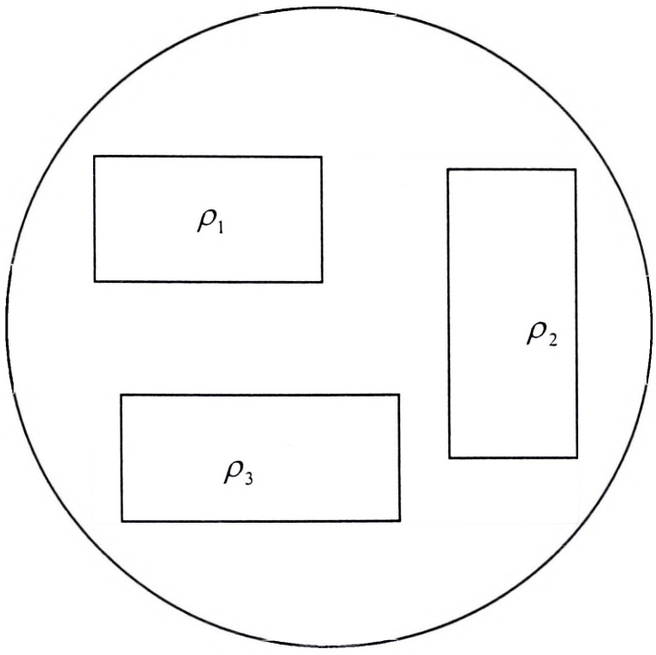
Wiedza jest wartością średnią wiedzy oddziału $K_B = \frac{1}{m} \sum_{i=1}^{m} K_{B,i}$ i $K_R = \frac{1}{s} \sum_{i=1}^{s} K_{R,i}$.

Wiedza relatywna lub relatywna świadomość sytuacyjna jest definiowana jako iloraz:

$$\Gamma = \frac{K_B}{K_R}, \; K_R \neq 0. \qquad (3.2)$$

Uwaga.

K_B jest nieograniczone z góry, zaś K_R jest ograniczone z dołu przez 0.



Rys. 3.2. Cele zainteresowań (TAIs) w obszarze kontrolowanym.

PRZEWAGA INFORMACYJNA

Oczekuje się, że armia wieku informacyjnego będzie w stanie w pełni wykorzystać możliwości jakie drzemią w przewadze informacyjnej. Rodzi się nowe pytanie – jaki wpływ może wywołać przewaga informacyjna na sposób dowodzenia w przyszłości? Amerykańska wizja armii (dokument Army Vision 2010) opiera się na pojęciu przewagi informacyjnej. Przewaga informacyjna definiowana jest jako zdolność do gromadzenia, przetwarzania i rozpowszechniania nieprzerwanego potoku informacji, przy pozbawieniu tych samych możliwości przeciwnika. Zdefiniowanie pojęcia wiedzy relatywnej umożliwia nam dokonanie oceny przewagi informacyjnej pomiędzy Czerwonymi (R) i Niebieskimi (B).

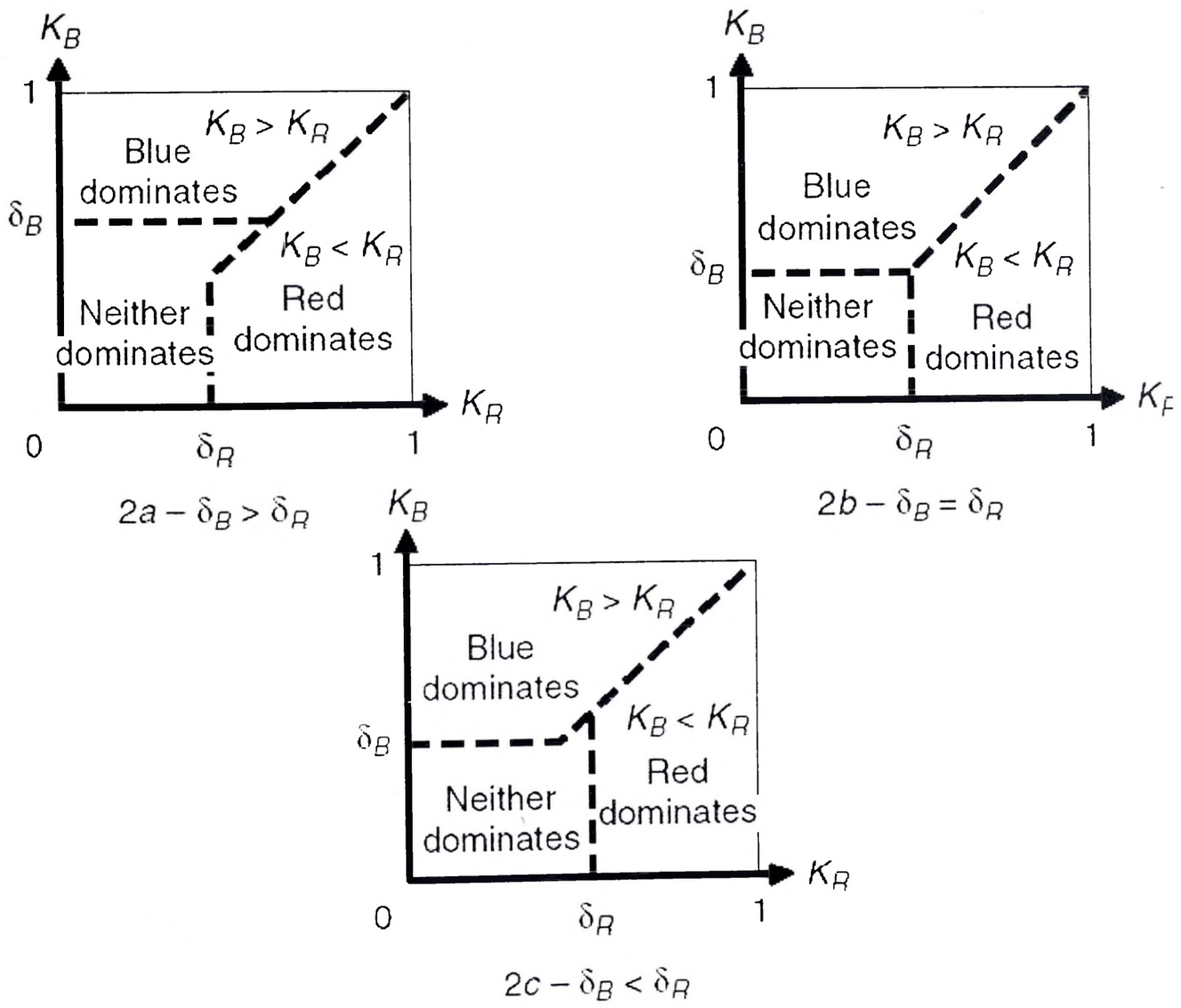
Tablica 3.1.

Możliwe reakcje.

Jeśli	***Wtedy***	***I***
$K_B > K_R$	$\Gamma > 1$	Niebiescy posiadają przewagę informacyjną
$K_B < K_R$	$\Gamma < 1$	Czerwoni posiadają przewagę informacyjną
$K_B = K_R$	$\Gamma = 1$	Brak przewagi informacyjnej

DOMINACJA INFORMACYJNA

Pojęcie dominacji informacyjnej jest już mniej jasne. Wygląda na to, że „dominacja informacyjna" jest osiągana wtedy, kiedy „różnica" pomiędzy Niebieskimi i Czerwonymi jest wystarczająco duża. Z definicji tej wynika, że dominacja informacyjna jest osiągana wówczas, gdy przekraczana jest pewna wartość progowa. Metryka wiedzy relatywnej może też być uzyta do definiowania dominacji informacyjnej poprzez określenie wartości Γ.



Rys. 3.3. Dominacja informacyjna.

Rozpatrzmy przedział $0 < \beta < 1$ w którym będziemy mieli dominację informacyjną. Niebiescy posiadają przewagę informacyjną, kiedy $K_B > K_R$ (K_R musi być wartością na tyle dużą aby można było uznać, że przeciwnik jest w stanie osiągnąć przewagę informacyjną)[70], wtedy $1 \geq K_B - K_R \geq \beta$. Dzieląc obie strony przez K_R otrzymujemy:

$$\frac{1}{K_R} \geq \Gamma - 1 \geq \frac{\beta}{K_R}. \qquad (3.3)$$

Daje to ograniczenie Γ do przedziału:

$$1 + \frac{\beta}{K_R} \leq \Gamma \leq 1 + \frac{1}{K_R}. \qquad (3.4)$$

Jeśli interesowałyby nas warunki przy których czerwoni uzyskaliby przewagę informacyjną, konieczne byłoby przeprowadzenie podobnego rozumowania.

Graficzne zobrazowanie dominacji informacyjnej przedstawia rys.3.3. Zobrazowanie to pozwala zrozumieć różnicę pomiędzy przewagą informacyjną a dominacja informacyjną.

Na uwagę zasługuje fakt, że pomimo dominacji jednej ze stron, możliwa jest nadal przewaga informacyjna drugiej strony. Wszystko zależy od okoliczności i charakteru dominacji informacyjnej, bądź przewagi informacyjnej. Sytuacja taka może powstać w różnych regionach. Oznacza to, że można mówić o jednoczesnej dominacji niebieskich i czerwonych, ale dla dwóch różnych regionów.

[70] Jeśli K_R jest bardzo małe, to nie można mówić o przewadze informacyjnej a w konsekwencji nie można mówić o uzyskaniu dominacji informacyjnej.

LITERATURA DO ROZDZIAŁU TRZECIEGO

1. Alan D. Capmen, The First Information War, October 1992.
2. DoD Dictionary of Military and Associated Terms, Joint Publications 1-2, Joint Chiefs of Staff, 12 April 2001.
3. Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," The National Interest, No. 37(Fall) 1994, p.30.
4. Joint Vision 2020, Joint Chiefs of Staff, November 2000.
5. The Dynamics of Military Combat, Operations Research, Vol.7, Jan.-Feb. 1959, pp.30-49, P.M.Morse, and G.E.Kimball, Methods of Operations Research, MIT Press and Wiley, New York, 1951, pp. 71-73).
6. R.L.Helmbold, Decision in Battle: Breakpoint Hypotheses and Engagement Termination Data, Rand Corp., Santa Monica, CA, Rept. R-772-PR, June 1971.
7. R. Darilek, Walter Perry, Jerome Bracken, John Gordon, Braian Nichiporuk, Measures of effectiveness for the Information – Age Army, RAND 2001,
8. Dan Gonzales, Lou Moore, Chris Pernin, David Matonick, Paul Dreyer, Assessing the Value of Information Superiority for Ground Forces – Proof of Concept, RAND 2001.

ZAŁĄCZNIKI

CSIS

Asymmetric Warfare versus Counterterrorism:
Rethinking CBRN and CIP Defense and Response
Background Briefing to the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information

Anthony H. Cordesman
Arleigh A. Burke Chair for Strategy
March 2001[71]
Asymmetric Warfare and Homeland Defense 3/30/01 Page 2

ASYMMETRIC WARFARE VS. "TERRORISM"

Asymmetric State or Efficient Terrorist Attacks versus the Conventional Picture of "Terrorism"

- Threats involve different levels of sophistication and intensity, and probably very different methods of attack and technologies.
- The problems of warning, defense and response differ sharply by level of attack and threat.
- The rules change for all responders as attacks escalate from conventional lowlevel terrorism ("crooks and crazies") to major levels of damage and casualties:
  - National emergency forces DoD into critical role.
  - Law enforcement must operate in state of national emergency. Issue of state of war becomes real prospect.
  - Public health and emergency services saturated and face reality can only half-anticipate.
  - Possible threats to basic structure of commerce, economic infrastructure, continuity of government.
  - May well be linked to a serious theater-driven crisis or war.

The Problem of Probability

- Low level terrorist attacks are indeed more probable, and in fact are constantly occurring at the cyber and false alarm level.
- Seen over a 25 year period, however, the probability of some sophisticated form

---

[71] Center for Strategic and International Studies, 1800 K Street N.W.,Washington, DC 20006, (202) 775-3270 Web: CSIS.ORG Acordesman@aol.com

of major asymmetric attack is high.

- Not only on US, but our allies.

- We have a "Non-Gaussian" reality. There is no standard distribution curve.
- The cumulative probability over time of a low to moderate probability event actually be the highest priority for planning is much higher than the probability the most probable events will actually be the highest priority for planning.
- We cannot deal with the problem by adding analytic and technological elegance to the classic American solution to all critical problems: "Simple, quick, and wrong."

The "Theater" Aspects of Asymmetric Warfare and Homeland Defense

- Threat is not directed at US per se, but at US as extension of regional/theater/foreign nation objectives.
- Allied targets, US forces and businesses overseas, and critical economic facilities can be targeted, not just US.
- Multiple and sequential attacks more likely, as are mixes of methods of attack.
- Availability of sophisticated biological and nuclear weapons more likely.
- CIP offers a low cost adjunct to virtually all forms of asymmetric and theater warfare.
- Crisis/war driven intentions and escalation extremely difficult to predict.
  - History is irrational and is often made out of worst cases. Intelligent, prudent, "business as usual" intentions usually means crisis never occurs in the first place.
  - Asymmetric values and perceptions are as real as asymmetric warfare.

Do Asymmetric and Terrorist Attack Have Important Elements in Common?

- All threats relate to other national security activities.
- All compete for limited resources and federal emergency management capabilities.
- "Squeezing the balloon:" Defending in one area while failing in the others pushes attackers to attack the less defended area.
- Many common problems in law enforcement.

- Many common problems in public health and emergency services.
- All depend on the relative vulnerability of commerce, economic infrastructure, continuity of government.
- All create the risks of attacks with effects so costly that response may prove unaffordable, and where it is unclear that technology and systems are available for effective response.

Do Asymmetric and Terrorist Attack Differ in Important Elements?

- Natural difference in priority between Defense and Law Enforcement/Responder communities. Each focuses on business as usual.
- Responders/defenders do not focus on "mission impossible."
- Linkage to foreign threats and wars largely ignored outside the Department of Defense and national security community.
- Intelligence and law enforcement efforts decoupled. Serious legal barriers to effective action.
- Asymmetric warfare can push US rapidly towards Presidential state of emergency, most terrorism is business as usual.
- Defense/response has priority over normal legal procedures and civil rights.
- Breakdown/collapse of local defense and response efforts is a much higher priority.
- Risks of attacks with effects so costly that response may prove unaffordable is much higher, as is uncertainty that technology and systems are available for effective response.

If cannot defend, must respond as well as retaliate.

ASYMMETRIC WARFARE: RECONSIDERING OFFENSE, DEFENSE, AND RESPONSE

Federal Government Does Not Currently Respond Effectively to the Threat of Large-Scale and Asymmetric Attacks

- Really have not conducted systematic threat evaluation of who can really use different kinds of CBRN weapons and methods of attack, and how technology will evolve over next 25 years.
- Legalistic approach prevents effective action. Much of law and human rights discussion fails to distinguish between the need to respond differently to a critical attack/existential threat and a lower level incident.

- Failure to integrate theater and homeland offensive/defense issues.
- "C," "B," "R," and "N" threats and poorly defined. Warning, intelligence, defense, and response tend to be compartmented.
- Effects models dubious at best and unsuited for response planning.
- Failure to realistically address major nuclear and biological attacks, examine limits of what response can and cannot do.
- Defense and response programs tend to be compartmented. Create open-ended programs with no clear picture of what deployed system will look like and cost.
- Major problems in biological side with proposed solutions decoupled from massive public health cost problems and reduction in hospital and emergency care capabilities for cost-effectiveness reasons.
- Lack of Net Technical Assessment and realistic evaluation of cost to defeat proposed programs and solutions.
- Failure to explicitly consider offensive and retaliatory options against foreign attack.

Asymmetric Warfare: Finding Solutions

- Re-evaluate the threat in terms of warfighting and not just "terrorism."
- Force common intelligence/defense/response planning for high level "C," "B," "R," and "N" attacks.
- Re-examine theater and homeland offensive/defense issues: Consider post Cold-War strategic and theater offensive/retaliatory options, including nuclear.
- Look honestly at the critical threshold where existing federal, state, and local response options fail: The nuclear and critical biological attack.
- Examine the real-world limits of intelligence, warning, and defense.
- Create a "zero-based" review of the real-world impact of CBRN weapons on critical targets and urban environments. Look at the reactor problem.
- Require Net Technical Assessment and realistic evaluation of "cost-to0defeat" proposed programs and solutions.
- Conduct a "zero-based" review of legislation to clearly define how intelligence and law enforcement can be made more effective, and the trade-offs involved.
- Treat CBRN response in the full context of national public health requirements. Determine what is really practical and affordable.
- Create an effective program budget, not simply an annual budget.
- Evolve the right solution to real problems.

Reconsidering the Sophistication and Level of Attack

- All attacks are not created equal. Limited CBR attacks at the terrorist and extremist level are fundamentally different from nuclear and highly lethal nuclear and biological attacks.
- Covert and proxy attacks by foreign governments are acts of war. Truly sophisticated terrorists will not operate under the limits currently assumed in most studies.
- Such attacks sharply raise the probability of "cocktails" of different agents, mixes of CBRN and cyber attacks, and the use of such attacks to supplement theater conflicts. NMD + CBRN + CIP is then credible.
- The current and perhaps any affordable response effort will collapse at finite and limited levels, forcing federal/state/local governments and the private sector to improvise radically.
- Bioattacks with immune or genetically engineered strains that have unpredictable delays, persistence, symptoms, ability to defeat treatment and vaccines, and lethality become a real possibility.
- The "balloon effect" means that attacker will respond to US defensive measures by (a) shifting their methods of attack to strike at the least defended areas, and (b) developing countermeasures to exploit the weaknesses in any defense.
- This makes "cost to defeat" and net technical assessment of all defensive programs and options critical.
- There does not seem to be any current prospect of dramatic changes in the ability to build a nuclear bomb in the basement and in domestic/foreign terrorist ability to acquire nuclear weapons.
- The situation with biological technology *may* be radically different. Bioattacks with immune or genetically engineered strains that have unpredictable delays, persistence, symptoms, ability to defeat treatment and vaccines, and lethality then become a real possibility.

The Need for an Unambiguous Strategic Offensive Doctrine

- We are drifting towards a response-oriented approach that does not even have a Maginot Line-like emphasis on defense.
- Major attacks must be firmly deterred, preempted or reduced in size, and firmly retaliated to.
- It must be clear that attacking states, and states that deliberately host terrorist

movements, will be the target of US strikes directed at the nation and not simply at the leadership.

- The US needs to give its theater and strategic forces this option.

Asymmetric Warfare: Offensive Defense

- What changes to deterrence, offensive strike capability, and retaliation really matter if states and foreign movements are involved?
- What can be done to aid defenders in securing US borders and territory?
- What can be done in terms of intelligence/technology to rapidly and conclusively identify the attacker?
- What can be done to accelerate and improve warning time for offensive/counterattack/deterrent purposes?
- When is the threat/attack one that justifies "war?" When is "legalism" over?

Asymmetric Warfare: Intelligence, Threat Assessment, Offense, Defense, and Response

- When is the threat/attack one that justifies decisive defensive action?
- When does a true state of emergency begin and when is "legalism" over?
- What can be done to improve or replace HUMINT?
- Can data-mining and AI provide a new technological approach?
- Probable number, sequence, and mix of attacks.

Asymmetric Warfare: Defensive Defense

- Does new technology and a systems approach really offer any significant statistical/actuarial help to the defender in detecting CBRN attacks in ways that allow a defensive response?
- Is improved border coverage possible and cost-effective? Only NR or CB as well? National or localized, emergency capability with warning?
- 21st Century NEST: If you zero-base the concept, can you really do more to protect borders or find the weapon? If you have an attack, can you improve the search for additional weapons?
- Is there any credible form of "Bio-NEST"? Is there any hope of search technology to find biological (chemical) weapons?
- Is any kind of distributed detection and diagnostic system technically credible and cost effective?
- What operational research is needed into search and detection options

- What can be done to give defenders rapid capability to secure/sterilize/decontaminate an area with suspected CBRN weapons with minimum collateral damage?
- When is the threat/attack one that justifies decisive defensive action? When does a true state of emergency begin and when is "legalism" over?

Asymmetric Warfare: Net Technical Assessment

- GIGO: Critical effectiveness and lethality data are very uncertain and modeling is becoming more sophisticated rather than more accurate.
- Attack models are weak, and cannot be rapidly tailored to simulate specific types of attacks on specific cites and targets.
- Technology and effectiveness of different means of attack and defense are poorly assessed. Assumptions about the effectiveness of weaponization and delivery methods often have weak technical and empirical rationale.
- Lack of Net Technical Assessment means that we are selling and buying too many ideas with:
  - Uncertain analysis of probable trends in related defensive and offensive technology.
  - No clear technology base for overall prioritization.
  - Little or no assessment of the cost to by pass or defeat a given program.
  - No assessment of the "end state" in terms of a description of a deployed system and capability and is procurement and life-cycle cost?
- Parochial cost/time/effectiveness models designed to sell the program.

Asymmetric Warfare: Attack Characterization is Critical to Defense and Response

- Defensive concepts are now generally stovepiped and oriented to a single attack by one type of weapon.
- There are no rules that say we do not face multiple or sequential attacks by mixes of weapons.
- If national specialized intelligence, counterterrorism, and law enforcement assets cannot handle this burden, the vulnerability is obvious.
- Today's ability to assess the impact of given types of weapons, simulate their actual use in real-world urban environments, and discuss uses of mixes of weapons is based on tenuous and inadequate models that may do more to misinform responders and waste resources than help.

- The cheapest way to reduce the burden on local (and federal and state) responders may be to provide the most accurate possible picture of what an attack can do and what response is really required. Since the burden will still fall largely on local responders, intergovernmental coordination and organization is not the key priority.
- There is no point in developing individual types of high technology detectors that cannot be used in effective C,B, R & N systems that can characterize the nature of the attack, the area of the attack, and identify the proper response.
- At the same time, the cheapest way to make the response effort efficient and reduce the response burden would be distributed or rapidly deployable tools that would provide this information and monitor developments like plumes and fall out.

Asymmetric Warfare: Decentralized and Distributed Response

- Response needs rethinking to consider truly large-scale and/or multiple attacks.
- Most federal and a great deal of state and regional response may come too late to fit the critical time windows for biotreatment. And dealing with the prompt effects of nuclear explosions and fall out.
- Some form of decentralized and distributed local/civil defense may be the only answer. The questions then become prompt attack characterization, instructions to flee or stay, proper guidance to responders, and options for very low-cost distributed defensive aids like masks, medicines, etc.
- The key limiting factor in terms of capability and expense will be medical treatment. Is any kind of distributed system technically credible and cost effective?
- The issue of *live or let die triage* must be addressed now to guide local responders and determine whether new diagnostic and detection technology can reduce the medical burden.
- It is far from clear that response training today really prepares anyone for anything other than relatively small and easily characterized events.
- Much of the non-medical response effort seems to be focused around obtaining equipment and facilities to "get well" from past underfunding or provide equipment for small events. It is unclear that creating standard packages of such equipment, or responding to responder's priorities, really deals with the problem of homeland defense.
- Fixing the firehouse is pork, not homeland defense.
- The question is what kinds of training and equipment really help.

Asymmetric Warfare: Rethinking Civil Defense

- Many cheap solutions do exist.
- Cannot suboptimize on C, B, R, or N.
- *Must look beyond asymmetric warfare and terrorism, consider broader national public health priorities, and NMD "leakage" problems.*
- Real-time warning, characterization, and guidance can cover widest area most cheaply:
- Use of media?
- Flee or stay advice. Detailed in the office, home, and car advice.
- Real time linkage between responder and media.
- Credible and affordable low cost options:
  - What can citizens, corporations, local, state, and federal governments really afford.
  - Masks, tape, home detectors, etc. If cost is low enough, make purchase voluntary.
- Ecological and agricultural civil defense?

Asymmetric Warfare: Unthinking the Thinkable About Nuclear Attacks - I

- There are no reliable models of nuclear weapons effects in major urban areas involving massive complexes of high rise steel and glass buildings. The containment effects of modern cities are extremely difficult to model. Military studies indicate, for example, that modern buildings can reduce the effect of blast, thermal, and radiation by 40-60%, but they do not specifically address modern heating and air conditioning systems, and the sheltering effects are not designed to take glass into account and the internal impact on the building.
- Nuclear explosions create a wide range of different effects that can interact on the human body. The recent literature on military models for predicting casualties indicates that such models are not reliable, and states that, "The US Army Office of the Surgeon General is developing a system of casualty estimation that will provide rapid and reasonably accurate estimates of the number of types of casualties produced by a given enemy nuclear attack." This system, however, is not yet available.ii The military handbook on the subject acknowledges that medical facilities will probably be saturated or collapse in the event of a major attack, but effectively dodges the problem of diagnosis and triage, and assumes that adequate medical professionals and facilities are available to allow extended triage and preventive medical treatment.

- The Defense Threat Reduction Agency (DTRA) is working on more sophisticated models tailored to attacks on the US but it again is unclear when any unclassified results will be available.
- The impact of prompt radiation is extremely difficult to estimate, and lethal and serious does can vary sharply according to exposure even in the same areas. Even personnel equipped with dosimeters present major problems in triage because dosimeter readings cannot be used to judge whole body radiation, and a mix of physical symptoms have to be used to judged the seriousness of exposure. The impact of radiation poisoning also changes sharply if the body has experienced burns or physical trauma.
- In the case of treatable patients, significant medical treatment may be required for more than two months after exposure.
- Fall out can very sharply according to the size and nature of a weapon and its placement, and in the size and lethality of articles and water vapor. While most fall out settles within 24 hours, this varies according to wind pattern and movement through the affected area. The drop in actual radiation of the affected material is much slower, but logarithmic. Radiation at the first hour after the explosion is down about 90%, and radiation is only about one percent of the original level after two days. Radiation only drops to trace levels, however, after 300 hours.

Asymmetric Warfare: Unthinking the Thinkable About Nuclear Attacks - II

- The test data on the longer-term (after 24 hours) effects of radiation are highly uncertain and the longer term impacts of radiation are so speculative as to be impossible to estimate. As a result, virtually all estimates of the impact of nuclear weapons ignore the long-term casualties (96 hours to 70+ years) caused by radiation, such as cancer, and the impact of a weapon on the environment in terms of the poisoning of water and food supplies. The data on treatment of exposures from zero to 530 cGy of exposure do not even seem to call for recording the probable level of exposure.
- There is little data on the steadily growing seriousness of EMP on urban areas filled with computers and solid-state communications and control devices.
- Most models of fall out assume relatively neat patterns of distribution or plumes that give state and local responders a relatively clear picture of probable lethality and casualty effects. It is uncertain how realistic these models really are.
- Weather patterns could produce far more erratic patterns of distribution, and some estimates indicate that the "worst case" area covered by the overall plume could easily be

twice the area used as the reference case. There is little detailed or parametric modeling of these uncertainties, and of the burden they place on response teams. These uncertainties also are much greater for the much larger areas covered by low levels of radiation over time.

- The problem is further complicated by trying to estimate the specific mix of radioisotopes and radionuclides that will be produced and then become induced in the soil. The hazard prediction models used by the Department of Defense are under review, and it is not clear when new models will be available.
- There is often a gap between generic data on radiation, burn, and physical effects and the assumed level of treatment required. Much of the federal, state, and local response literature effectively dodges around the issue of triage, and the problem of choosing who will receive limited medical treatment and how these victims will be selected. It does not describe what is done with the assumed dying and untreatable. The broader issue, however, is what indicators will be used for triage and deciding treatment and what treatment should actually be employed.
- Food and water contamination can be a serious problem, and add to the response burden in any major attack. Fallout presents special problems since sheltered civilians may not have access to safe water, and urban water systems may be affected.
- Corpse disposal may be a major problem as may disposal of dead animals and birds. This aspect of response seems to be largely ignored.
- Even military medical handbooks fail to address the psychological impacts of prompt and longer-term effects.

Asymmetric Warfare: How Can Technology Deal with The Nuclear Risk?

- Improved modeling of real-world urban effects. Modeling of fallout and "rain out" plumes in ways tailored to improve response planning.
- Near real time fallout corridor modeling and data mining. Modeling for needed level of state,

  regional, and federal response.
- Detection and diagnostic systems – either distributed or rapidly deployable (e.g. the public transportation sensor grid).
- Monitoring of actual distribution of fallout and weapons effects to give local responders a more precise picture of short and long term response requirements. Real-time

transmission to responders, and state, regional, and federal actors. (Often 12-48 hour time window for critical response actions).

- Systems for instant detection and diagnostics, guidance for response and triage. Dosimeters are useless for this purpose. Need clearly defined stay or flee guidance.
- Cheap portable systems for real-time triage analysis.
- Improved detection and characterization of residual threats, decontamination technologies and decon effectiveness measuring systems.
- Hospital technology solutions, rapidly deployable care technology.
- Cheap, simple civil defense options: Masks, no cost what to do technology and advice, media
  warning and advice alert systems.

Unthinking the Thinkable About Asymmetric Biological Warfare - I

- It may not be possible to detect and characterize a biological attack (or attacks) until it is too late to provide effective treatment, to determine what levels of medical resources are required, or know how many response and treatment capabilities have been attacked and what level of patient flow will result.
- Much of the current response planning tacitly assumes that either incidents will be small and familiar enough to allow existing response capabilities to work or that attacks will be detected and characterized in ways that allow effective response planning. CDC/USAMIRID, etc. are sized at this level.
- Attacks by multiple agents, sequential attacks, attacks designed to create national infectious disease patterns, and mixing these attacks with CIP and cyber attacks is an unthinkable worst case, particularly at the law enforcement and responder level.
- Much of the response planning assumes that it is possible to predict the required medical treatment based on limited experience with civil incidents and epidemics. It is not clear that the "scaling" involved in estimating the effect of terrorist, extremist or covert use of more sophisticated weapons is more than speculative, and many studies do not cite the special evidence and method used to scale up civil cases into estimates of how biological weapons would behave.
- The uncertainty created by the ability to modify or engineer new weapons or forms of existing weapons greatly compounds these problems. There do not seem to be net assessments of the balance between changes in offensive and defensive biotechnology that

allow the US to predict future lethalities or the effectiveness of many proposed response measures.

- Most of the measures the US takes to provide homeland defense against biological weapons immediately become part of the open literature, and many take years of lead-time to become effective. While this can act as a deterrent, it can also act as a road map for states and sophisticated extremists in finding the weaknesses in US defenses.
- There are a number of detailed problems in detection, characteristics, and effects analysis. For example, reliable models of biological weapons effects do not seem to exist which cover attacks in major urban areas involving massive complexes of high rise steel and glass buildings. The containment and transmission effects of modern cities are extremely difficult to model.
- Most effects estimates only apply to the use of one biological weapon, but attacks using "cocktails" of several biological weapons were found to be the most effective method of mass attack during the Cold War.

Unthinking the Thinkable About Asymmetric Biological Warfare - II

- There is often a gap between generic data on the treatment needed for a given biological weapon and the assumed level of treatment required.
- There is the tacit or explicit assumption that a weapon can be treated as a conventional disease, and that enough will be known about effects and exposure for treatment to be applied.
- Much of the federal, state, and local response literature effectively dodges around the issue of triage, and the problem of choosing who will receive limited medical treatment and how these victims will be selected.
- Corpse disposal may be a major problem, as may disposal of dead animals and birds. This aspect of response seems to be ignored.
- Even military medical handbooks fail to properly address the psychological impacts of prompt and longer-term effects.
- Little or no practical planning to deal with longer-term physiological effects and mass decontamination and recovery problems.

Asymmetric Warfare: Militarized and Infectious Biological Attacks

- Much of the present approach seems to assume that biological attacks will be limited to non-contagious agents or "crooks and crazies".

- Other work assumes that it will follow containable patterns of normal disease outbreaks.
- The use of militarized and genetically modified strains needs explicit analysis.
- There seems to be a major decoupling of defensive and response planning from any net technical assessment of the advances taking place in biological weapons.

Asymmetric Warfare: Advances in Biological Weapons - I

- *Safer handling and deployment,* including the elimination of risks from accidents or misuse – the "boomerang effect".
- *Easier propagation and/or distribution* eliminating the need for a normally-hydrated bioagent or any use of aerosols. Microorganisms with enhanced aerosol and environmental stability.
- *Improved ability to target the host,* including the possible targeting of specific races or ethnic groups with given genetic characteristics.
- *Greater transmissivity and infectivity:* Engineering a disease like Ebola to be as communicable as measles.
- Microorganisms resistant to antibiotics, standard vaccines, and therapeutics.
- *New weapons:* Benign microorganisms, genetically altered to produce a toxin, venom, or bioregulator.
- *Increased problems in detection:* Immunologically altered microorganisms able to defeat standard identification, detection, and diagnostic methods. Problems in diagnosis, false diagnosis, lack of detection by existing detectors, long latency, binary initiation.
- *Greater toxicity, more difficult to treat:* Very high morbidity or mortality, resistant to know antibacterial or antiviral agents; defeats existing vaccines; produces symptoms designed to saturate available specialized medical treatment facilities.
- *Combinations of some or all of the above.*
- *Binary biological weapons* that use two safe to handle elements that can be assembled before use. This could be a virus and helper virus like Hepatitis D or a bacterial virulence plasmid like E. coli, plague, anthrax, and dysentery.
- *Designer genes and life forms,* which could include synthetic genes and gene networks, synthetic viruses, and synthetic organisms. These weapons include DNA shuffling, synthetic forms of the flu – which killed more people in 1918 than died in all of World War I and which still kills about 30,000 Americans a year – and synthetic microorganisms.

- *"Gene therapy" weapons* that use transforming viruses or similar DNA vectors carrying Trojan horse genes (retrovirus, adenovirus, poxvirus, HSV-1). Such weapons can produce single individual (somatic cell) or inheritable (germline) changes. It can also remove immunities and wound healing capabilities.
- *Stealth viruses* can be transforming or conditionally inducible. They exploit the fact that humans normally carry a substantial viral load, and examples are the herpesvirus, cytomegalovirus, Epstein - Barr, and SV40 contamination which are normally dormant or limited in infect but can be transformed nto far more lethal diseases. They can be introduced over years and then used to blackmail a population.
- *Host-swapping diseases:* Viral parasites normally have narrow host ranges and develop an evolutionary equilibrium with their hosts. Disruption of this equilibrium normally produces no results, but it can be xtremely lethal. Natural examples include AIDS, hantavirus, Marburg, and Ebola. Tailoring the disruption for attack purposes can produce weapons that are extremely lethal and for which there is no treatment. A tailored disease like AIDS could combine serious initial lethality with crippling long-term effects lasting decades.
- *Designer diseases* involve using molecular biology to create the disease first and then constructing a pathogen to produce it. It could eliminate immunity, target normally dormant genes, or instruct cells to commit suicide. Apoptosis is programmed cell death, and specific apoptosis can be used to kill any mix of cells.

Asymmetric Warfare: How Can Biotechnology Deal with This Risk?

- Detection and diagnostic systems – either distributed or rapidly deployable. (e.g. the public
  transportation sensor grid).
- Systems for instant detection and diagnostics, guidance for response and triage.
- Cheap portable systems for real-time triage analysis.
- Near real time infection corridor modeling and data mining. Containment modeling.
- Modeling for needed level of state, regional, and federal response.
- Finding the cure: Multivalent vaccines, replicon vaccines, broad spectrum antibiotics, immune system boosters, new antivirals. (*Now being oversold. Needs much more challenging peer group review of project proposals.*)
- Improved detection and characterization of residual threats, decontamination technologies and decon effectiveness measuring systems.

- Hospital technology solutions, rapidly deployable care technology.
- Cheap, simple civil defense options: Masks, no cost what to do technology and advice, media warning and advice alert systems.

Asymmetric Warfare: Implications for Public Health Services and Hospitals

- Vague, generalized recommendations to strengthen public health systems, hospitals, and private care must be rethought. Tend to focus on low to mid level B and C attacks, not major BRN attacks.
- Symbolic and half-measures may simply increase cost with marginal increases in capability.
- The present emphasis on vaccines, respirators, and more specialized public health and treatment facilities threatens to be purposeless in terms of cost to defeat, cost to procure, dual-use, value and real world distribution times.
- The actuarial chance a given apparently low cost-fix may actually be required on a national level can be extremely low and the cumulative cost can be extremely high.
- The nation has many ongoing day-to-day health priorities that will increase as the population ages.
- In most large-scale events the real world answer is that effective response in terms of major medical facilities is neither predictable enough to provide or afford. *But*, there may be low-cost distributed health measures that can reduce casualties.

Note that improving triage and (a) avoiding treatment of those who do not need it, (b) delaying

treatment for those not needing urgent treatment, and (c) letting the "walking dead" die may ultimately be the only way to do this.

Current warning and detection technology is not designed to support this kind of triage, and often will not support effective diagnostics.

Improved diagnostics is the second area where efficiency seems improvable at the least cost.

Asymmetric Warfare: Must Also Deal with Agricultural and Ecological Warfare

- Don't get mad get even – revenge is a dish best eaten cold.
- Already have many inadvertent cases to show this threat is real.
- If state-driven or well-organized attack, can be highly sophisticated, longdelayed, very hard to detect, and very hard to attribute. Advances in bioattack and biodefense technology are just as important here.

- Syndromic surveillance and improved detection?
- Response technology?

CYBERWARFARE VS. CYBERTERRORSM

Asymmetric Warfare: What Does Cyberwar Really Mean?

- We need a clear picture of current and projected cyberwar options for attackers.
- Effective defense and response requires a full-scale net technical assessment of what attackers can really do, key vulnerabilities, and requirements for defense and response.
- Exercising responses to assumptions about such attacks is not analysis or adequate Planning Cyberwar can occur at a number of levels and in conjunction with other means of attack.
- A covert cyberwar may be possible where the attacker cannot be identified quickly or at all. Larger-scale cyberwar may involve clearly identifiable attackers.
- Given the low cost of cyberwar, is a missile or CBRN attack without cyberwar credible?

Asymmetric Warfare and Attacks on CIP/Information Systems

- Cyberwar is *not* cybercrime or cyberterrorism
- Refocus on critical threats, leave normal defense to private sector, state/local, and federal agencies.
- Identify true critical risks. Look at cases where basic reductions in technological vulnerability may be the only solution
- Examine the full range of legal changes necessary for effective defense, including the "laws of war."
- Conduct a Zero-based reexamination retaliatory and offensive options.
- Force the creation of a common future year program with honest deployment and life-cycle costs.
- Examine the real-world limits of intelligence, warning, and defense.
- Require Net Technical Assessment and realistic evaluation of cost to defeat proposed programs and solutions as part of this zero-based options.
- Conduct a "zero-based" review of legislation to clearly define how intelligence and law enforcement can be made more effective, and the trade-offs involved.
- Evolve the right solution to real problems.

Asymmetric Warfare and CIP/Information Systems: Is There an Offensive Option?

"Technology 101" at the defender level says you really cannot identify the attacker and respond:

- Can a 21st Century approach change this?
- If so, in time to actually defend or in time to retaliate?
- What is the difference between "cyberattack" and "cyberwar"? When does the level of attack become wide or critical enough to merit decisive federal action?
- Is some form of national cyberwarning possible? Can you characterize attacks well enough to know the difference? Is some form of cyber damage assessment in near realtime possible? Can you build a warning system and net into critical national networks?

CIP/Information Systems: the Need for Degenerative, Non-Vulnerable, and Replaceable Systems

- There is far too much emphasis on trying to shield entry to highly distributed fragile or vulnerable systems.
- The only workable solution at many levels may be to avoid over-dependence on systems that

  cannot function in a degenerative form, are not sealed off, and do not have some workable human alternative.
- Alternatively systems must be designed to survive prolonged crashes, and be reconstitutable.
- Current diagnostics overemphasize guarding the portal, rather than measuring broad systematic attack patterns. Integrated and systems-wide warning and diagnostics are needed.

Asymmetric Warfare: Timelines and Responsibility

- Must have strong DoD Element: Offensive and theater focus equally important, foreign intelligence critical
- Need effective 5 and 10 year programs based on realistic threats, not short-term half-measures in response to artificial crises.
- Some kind of central planning and programming is critical, but the issue is not strategy, masterminding today's defense/response, or allocating one rear of budget funds. Must develop and manage a coherent program in detail.
- Who and where the Czar is, is important. What the Czar does is far more important.

- Must be central managers for intelligence, defense, and *response with individual programming and review authority and adequate resources*. Putting some one in charge at the top is of limited practical value unless this is done.
- Need to understand that no affordable system is likely to be capable of dealing with worst cases, and no one will pay for worst cases until the threat is far more tangible.
- Congressional review cannot be improved until the Executive Branch presents a program worth reviewing.

DND Photo JTF2 Ba

The blurring of traditional lines of responsibility between law enforcement and the military, coupled with ambiguities surrounding the very meaning of 'criminal activity', point to a future demand for joint and combined responses.

ASYMMETRIC WARFARE AND THE USE OF SPECIAL OPERATIONS FORCES IN NORTH AMERICAN LAW ENFORCEMENT

by Lieutenant-Colonel Donald A. La Carte

The devastation and attendant loss of life wrought by the terrorist assaults of 11 September on the World Trade Center and Pentagon completely demolished our sense of invulnerability to foreign hostile action, and shook the complacency of North American societies. Such was the gravity of these attacks, that it paralyzed the New York financial markets for days, closed down the air transport system for a similar time span, and degraded the US economy both by its direct effect and by its substantial impact on public confidence. Terrorist operations cut to the very bone of our vital national interests. If the world after that date has changed forever, has our perception and strategic awareness evolved in consonance with the new dangers and the need for reform?

At both the strategic and operational levels, the transnational nature of 'post-modern' asymmetric threats such as information warfare, terrorism, organized crime, and weapons of mass destruction (WMD) has placed increasingly varied and more complex demands on both Canadian and American armed forces and law enforcement agencies. In today's world of technological specialization, perpetrators and techniques alike have attained a high level of sophistication. This, in turn, obliges law enforcement and counter-terrorist agencies to develop the capability to provide protection to the peoples, places and institutions of North America.

In recent years, Western governments, primarily in the context of the G-7/G-8 counter-terrorism meetings, have focused significant effort toward coordinating a political response to the myriad of challenges associated with countering the newly emerging transnational and asymmetric threats. At the strategic and operational levels, however, law enforcement and military authorities have made much less progress in developing the synergistic means by which military assets and capabilities might be brought to bear on these threats.[1]

Can Canadian and American authorities meld military strategies and capabilities with those of law enforcement agencies in such a way as to generate optimal security for North American territory and populations? It is this question that frames the analysis of this paper. It begins from the assumption that sophisticated military special operations forces and their equipment might represent a useful tool for assisting civil authorities. On the surface at least, it would appear that the prudent use of expensive, high-tech, well-trained, standing military resources, in close coordination with respective policing forces, would not only increase the efficiency of joint — and in the Canadian/American context, combined — responses to the threat, but could

Lieutenant-Colonel Donald A. La Carte *is Visiting Defence Fellow at Queen's University.*

yield significant budgetary savings as well. How valid is that assumption?

CURRENT PRACTICE

It is important to observe that in the traditional sense, roles for military forces and law enforcement agencies have been essentially separate and distinct, especially in the US, where the *Posse Comitatus Act,* with some minor exceptions,[2] legislates against the use of federal troops in routine domestic matters (though National Guard units frequently fulfill such duties). Canada, on the other hand, has a longstanding tradition of employing military resources in aid of civil authorities. That said, even in Canada's case, the military has been conceived principally as a means for dealing with menaces stemming from outside its borders, with police forces being given the job of dealing with internal threats.

DND Photo JTF2 Ca

The operational deployment of Canada's counter-terrorism/special operations unit, Joint Task Force Two (JTF 2), in support of law enforcement agencies, would most likely occur under the provisions of the CF Armed Assistance Directions.

This tidy compartmentalization has been under increasing stress because of continued evolution of newly emerging asymmetrical threats. Underpinning this blurring of traditional spheres of responsibility has been the globalization of crime, coupled with the growing difficulty in sorting out both the nature and source of transnational threats. Indeed, it is less and less easy to tell what exactly is a 'crime', and what is an 'attack'. At the governmental level, amid the multiple, and sometimes overlapping, areas of jurisdiction and responsibility, such ambiguity means that it becomes difficult to even determine to whom responsibility should be given in responding to the threat.

Perpetrators of transnational crimes and initiators of terrorist attacks can and do operate outside the sovereign domain and across borders. They often have domestic links within the target country. This poses an obvious problem for law enforcement agencies, since domestic law is not always compatible with international law and, in the absence of foreign cooperation, states do not have the authority to apply their jurisdiction within the geographical confines of other states. Information sharing with our separate government departments and agencies and with each other is essential to any successful prosecution of cases involving transnational threats.

One step in the right direction, in the Canadian-American context (as in other contexts), would be more effective communication. But even in the Canada/US case, where one would expect that there should already be a great deal of such communication, appearances can be very deceiving. Witness the well-publicized recent example of Ahmed Ressam, allegedly attempting to smuggle bomb-making materials across the border between British Columbia and Washington: this act might well have been prevented by more proactive information exchange by the RCMP.[3] Failing this, the result was that American authorities were required to place police forces and border posts on elevated alert, to such an extent that for a brief period toward the end of 1999 every single vehicle passing from Canada into the US was being stopped for inspection.[4] And if Canadian and American authorities have such difficulty 'getting it right', what prospects are there elsewhere for the effective facilitation of information sharing?

There is a clear obligation, then, for Ottawa to collect and evaluate information concerning threats to sovereignty and national security — and these threats can be adjudged serious enough to warrant using military resources along with civilian ones, as is evidenced by the recent establishment, as part of the Department of National Defence, of an office of Critical Infrastructure Protection and Emergency Preparedness, announced in February 2001 for the purpose of protecting against cyber-sabotage.[5] Moreover, in the same way that transnational criminal and terrorist organizations are creating new, flexible connections, it is imperative that governments continue to demolish inter-agency barriers.

WHAT DO WE MEAN BY 'ASYMMETRIC THREAT'?

A consensus has been emerging in recent years that the threat posed by asymmetric warfare and crime has been gathering force in North America — or at least the debate over the threat has been gathering voice. Even before the 11 September attacks, this was especially the case in the US, where the threat to 'homeland security' was taken very seriously inside the government.[6] In 1998, a US Army War College conference posed the question whether America's military could find itself under successful attack at key nodes of its largely unprotected infrastructure. The answer was that it could. The same conference also noted that in thinking

about such attacks, the salient issue was not so much threat identification or even response development; rather, it was trying to figure out the "more ambiguous political question of whose job is it" to respond to the threat.[7] While many participants agreed that America's military could not afford to be distracted from its principal aim of preparing for conventional conflicts, or "fighting the nation's wars", all recognized that the great challenge of developing concepts, doctrine, and the organizational apparatus for functioning across cultural, legal and fiscal boundaries remained within the ambit of the federal bureaucracy as a whole.

The effects of globalization are certain to further reduce the geographic isolation that has until recently provided a convenient buffer from international conflict for both Canada and the US. Asymmetric dangers are expected to constitute an ever growing challenge to traditional security interests of both countries.[8] Such is the pace of events, even recent assessment which anticipated that these threats "may move into the foreground" within five to ten years[9] has been rendered anachronistic by terrorist suicide bombers and the appearance of anthrax-laced mail south of our border. But, what exactly does this imply, and what do we mean by the term 'asymmetric threat'?

Typically, the concept encompasses techniques, weapons and tactics that an adversary might employ to foil or circumvent the technological superiority of its foe — in this case, us. Essentially, an asymmetric attack seeks fundamentally to alter the so-called 'battlespace' within which conflict occurs. One recent essay at threat definition conducted for Canada's National Defence Headquarters notes that "asymmetric threat is a term used to describe attempts to circumvent or undermine an opponent's strengths while exploiting his weaknesses, using methods that differ significantly from the opponent's usual mode of operations."[10] Implicit in this form of threat, according to a briefing prepared for a US military audience, is the prospect that they represent "unconventional approaches or inexpensive means that ... confront us in ways we cannot match in kind."[11]

While asymmetry can be in the ends to be attained or in the ways and means of achieving them, attacks are likely to have a strategic impact, particularly in the moral plane. Such assaults could include the exploitation of the fears and beliefs of our population, and the undermining of political support for legitimate government or its actions. As described in the Directorate of Land Strategic Concept publication, *The Future Security Environment:*

> Ways and means include exploiting Western sensitivity to casualties, disrupting our complex economics and threatening our desire for legitimacy. These include, but are not limited to terrorism, disinformation, psychological operations, use of WMD and information system attacks. At the operational and tactical levels, opponents may interdict lines of communication, try to maximize casualties to erode our resolve, fight in complex terrain such as cities and mountains and take hostages.[12]

Perpetrators are likely to select aggressive tactics that "purposely blur boundaries between actions considered crimes and those viewed as warfare."[13] Hence the creation of the future battlespace, neither distinctly military nor uniquely in the domain of law enforcement. Asymmetric operations executed beyond the accepted norms of warfare and the law of armed conflict will present serious ethical dilemmas to Western states, constrained as these latter are in the design and implementation of responses to such operations.

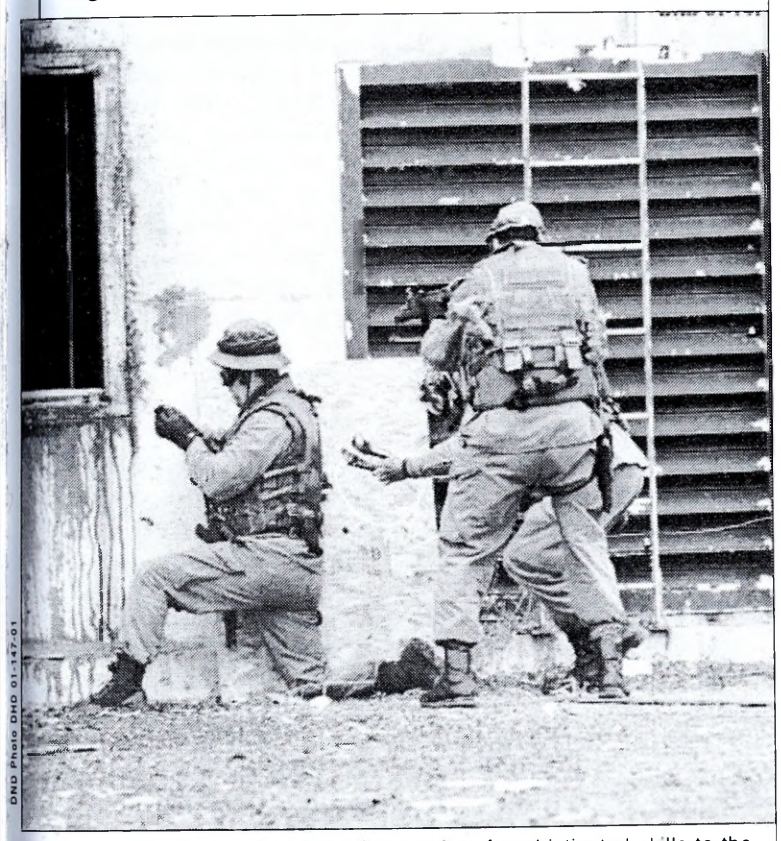
The evolution of asymmetric dangers is expected to multiply the number of potential threats to our security, along with the weapons used to carry out these threats. Less developed countries or transnational groups can purchase advanced weapons and delivery systems with relative ease in today's open arms marketplace. Globalization, it is said, will compound the challenge, congruent as it is with the "revolution in communication technology, ease of travel, [and] erosion of borders."[14] Globalization's 'downside' is that it seems to be fostering a new battlespace, one characterized by a plethora of chemical, biological and radiological menaces, along with an increase in the number of extremist groups, this latter notwithstanding that the "actual number of international terrorist incidents ... is generally in decline."[15]

DND Photo JTF2 Aa

Terrorism is, in most respects, the waging of psychological warfare. In response, we should seek to employ economy of force, a hallmark of special operations forces.

THE CHANGING NATURE OF TERRORISM

Terrorism is at the top of most lists of asymmetric threats. It is also one in which military special operations forces have played a significant role. Western experience over the past decade or so has shown that the "best way to fight terrorism is through serious, global, and transparent cooperation."[16] In recent years, the nature of the enterprise has been changing, so that today we witness fewer incidents of state-sponsored and ideological terrorism.



DND Photo DH0 01-147-01

SOF are strategic assets which bring a suite of sophisticated skills to the battlespace. These enhanced capabilities readily permit their employment across the full spectrum of operations.

Contemporary terrorist networks form amorphous, indistinct organizations and tend to operate on a linear, nonhierarchical basis. Their aims and objectives become less easily defined than previously, as it appears that today's terrorists are less interested in killing merely to attract publicity to a cause. There is a greatly reduced frequency of terrorists claiming 'credit' for their operations, just as there has been a reduction in the number of such operations.[17] But as their number has decreased, there has been an increase in the lethality of attacks, suggesting that we have entered a new phase of terrorist operations.

It is precisely from asymmetry that terrorists derive their strength. Conducting their operations outside of what we would label 'acceptable' international behavior and in accordance with unique value systems radically different from our own, some of the modern non-state combatants (including the Osama bin Laden network al Qaeda) "operate according to a 'warrior clan' ethos reminiscent of Japanese samurai or medieval crusaders, a philosophy at odds with the ethic of modern, professional armed services."[18] With random assaults propelled by what can seem the murkiest of motives, the new form of terrorism "frightens by its unpredictability", and though it retains the old terrorism's focus upon the sowing of widespread fear, the new variant can often appear "pointless since it does not lead directly to any strategic goal, and it seems exotic since it is frequently couched in the visionary rhetoric of religion."[19]

Nor is it even accurate to argue that the new terrorism has completely displaced the old; instead, the two coexist, with the earlier version making periodic reappearances. But asymmetry has altered our understanding of the threat, leading to a greater perception than heretofore of societal vulnerability. We know that we are no longer as immune as we once were. The vulnerability of public order we tend to take for granted was visibly shaken in the wake of events such as the 1993 bombing of the New York World Trade Center, the release of nerve gas in the Tokyo subway system, the truck-bomb detonation at the Oklahoma City federal building, the 1998 assaults on American embassies in Kenya and Tanzania and, most horrific of all, the use of hijacked civilian airliners used to destroy the World Trade Center and a wing of the Pentagon.

We would do well to remember that terrorism is fundamentally the waging of psychological warfare; thus, in responding to it, we should seek to employ an economy of force and economic resources. Such economy, as we will see, is a hallmark of special operations forces. The expertise of certain military resources (psychological operations staff, for example), particularly those possessed by the US, may prove advantageous to law enforcement entities charged with formulation of strategy and policy for confronting terrorists.

More and more, global terrorism has been taking on religious hues, with activists stemming from any number of ecclesiastical traditions. Recent acts of violence have been ascribed to Islamic suicide bombers, Christian militants in the US, Jewish radicals in Israel, Buddhist sects in Japan, and extremist Sikhs and Hindus in India and Canada. That religious discontent and rivalry increasingly fuel terrorist activities is evidenced by the fact that, whereas in 1980, the State Department's listing of foreign terrorist groups included hardly any religious organizations, by 1998 more than half of the thirty most dangerous groups were sectarian. And this actually understates the matter, since it leaves out the many Christian militia and other paramilitary groupings in the US; add these to the list, and the "number of religious terrorist groups would be considerable."[20] Given the multicultural basis of North American society, the trend seems portentous.

If not all religious terrorists are to be found off North American shores, neither are all terrorists. In the US especially, a home-grown variety of ultra rightists has been surfacing. According to one expert on terrorism, the "convergence of anti-government patriots and neo-nazi white supremacists is the most disturbing development in American politics."[21] Growing more volatile and visible, this home-grown collection of citizen militiamen, paramilitary neo-nazis, racialist skinheads, and white Aryan activists blended an anti-gov-

ernment ideology with supremacist mythology in proclaiming 2000 as the year of their own jihad — 'RAHOWA', or racial holy war.

CRIME AND CYBERTERRORISM

Organized crime, or what we might call with apologies to Clausewitz, the "continuation of business by criminal means", is on the rise. More decentralized, cross-cultural, and international than ever before, organized crime represents a less immediate threat than terrorism, but one that could end up undercutting the stability of legitimate government by instigating corruption and eroding public support. Recent studies also indicate that "an increase in organized crime corresponds to an increase in global drug trafficking and money laundering — two conditions which directly and indirectly threaten U.S. national security."[22] Ominously, terrorism is becoming more closely linked to organized crime. Once confined regionally, organized crime has now followed the forces of globalization and become internationalized in pace with transnational commerce. It, too, has entered the new 'battlespace', where it seeks to exploit asymmetries in legal, administrative and financial spheres.

Information warfare is another asymmetric threat increasingly encountered. Recognized as a potentially serious menace, it exploits the globally integrated, knowledge-based economies of developed countries, leaving them vulnerable to attack via their unprotected information systems.[23] This type of warfare encompasses a full spectrum of operations, ranging from "manipulation of open media to hostile psychological operations, to attacks on information infrastructure such as databases or processing centres, either through physical, electronic or processing means."[24] Cyber-terrorism can be waged at many levels, and can be focused on individual, industrial and economic espionage by states or non-state organizations. Also, it can be launched by one state against another, and can involve organized groups such as militias or even narco-terrorists, who often possess high-tech devices common to many governments. Even at the individual level there can be cause for alarm, for as Winn Schwartau points out, "in time of conflict, nothing prevents a military adversary from researching senior NATO leaders (or soldiers in the field) and threatening their families back home, turning ... computers ... into a tool that can be used by miscreant marketers, common criminals, or foreign enemies to 'get at' them."[25]

At the industrial and economic level of espionage, techniques employed by cyber-terrorists might include eavesdropping on telephone conversations, internet sniffing, password cracking, or electronic break and enter. Recent reports from the Federal Bureau of Investigation indicate that some 122 countries operate online industrial and economic espionage against the US, with a consequent loss to American businesses of approximately $300 billion a year.[26]

It is a small leap of imagination to foresee cyber-terrorists being able to develop the technological expertise to enhance their destructiveness. Terrorists will be able to extend their influence across the spectrum of conflict by means of networking, suggesting a shift of power from state to non-state actors "who can organize into sprawling multi-organizational networks more readily." Moreover, it is also evident that as our information dependency progresses, conflicts will be more likely to centre around our knowledge-based systems. In view of this, some experts see the emergence of 'netwar' as a "mode of conflict and crime at societal levels, involving measures short of traditional war in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age."[27] The challenge for Canadian and American governments becomes to formulate joint and combined responses that reach beyond mundane technological countermeasures, essentially implying a re-engineering of the entire approach to cyberterrorism.

WEAPONS OF MASS DESTRUCTION

The biological, chemical, and radiological products and technology necessary to the production of WMD are proliferating, posing a new asymmetric threat to North America. Despite control regimes, it is evident that both the means of delivery and the warheads are becoming more readily available, and the potential for development of a future WMD — a genetic

DND Photo DHD 01-147-05

SOF units, especially those designated for counter-terrorism, excel in precise and discriminating application of force.

one — can be glimpsed. WMD, with or without a long-range delivery system such as ballistic or cruise missiles, could endanger Canadian and American territory, as well as threaten troops deployed abroad. It can even be said that the mere existence of these weapons constitutes a threat in itself, even in the absence of a capability to deploy them operationally, given the significant psychological impact they possess. Although accessibility to WMD has increased, it by no means follows that the probability of terrorists actually employing WMD must be high. Such an optimistic assertion rests, in part, upon the anticipated high costs associated with the acquisition, testing and management of WMD; moreover, many experts have long considered that terrorists could accomplish their aims without relying upon WMD. This assumption would seem to be borne out by the stunning attacks in New York and Washington, but could indeed be called into question by the appearance of anthrax-tainted mail.[28]

Nevertheless, concern does and will remain about this category of weaponry. In Congress, there is a consensus for funding measures to counter the threat of chemical and biological terrorism, with a fiscal year (FY) 2000 increase of some $1.4 billion being voted for countermeasures.[29] Further appropriations are about to be announced by President Bush. American concerns have been premised on the perceived vulnerability of large urban areas in the face of more general availability of the weapons and the expertise needed to utilize them.[30] Noteworthy in this respect is that the "most devastating attacks on civilians in North America, Europe and Japan have not relied on military platforms for delivery."[31]

Although militaries have long practiced nuclear, biological and chemical defence as a byproduct of the Cold War, the initial wave of official concern was exacerbated by events in Tokyo in 1995, when the religious cult Aum Shinrikyo released a nerve agent, sarin, into the city's subway system, resulting in a dozen deaths and more than a thousand other casualties. It is important to keep things in perspective. Despite fears of copycat gas attacks occurring elsewhere, there have been none in the past six years. And, however significant the psychological impact engendered by the recent introduction of anthrax, casualties have been minimal. Indeed, biological agents remain difficult to weaponize, and the effects of attacks, with some important exceptions such as small-pox, tend to be self-limiting, with only persons directly exposed to the agent falling ill.[32] Chemical weapons pose particular problems for terrorists, not the least of which being the huge quantities of agent required to inflict mass destructions, the difficulty in dispersing the contaminant, and the unpredictable effects of their dispersal.

Notwithstanding these difficulties, however, current experiences in New Jersey, New York, Washington, Florida and elsewhere, underpin a viable concern that Canada, the US, and the other allies could be subject to future attack from biological and chemical weapons. Complacency should not be the order of the day, as a case can easily be made for a prudent insurance policy requiring ongoing intelligence and civil defence preparedness initiatives. What does follow is that we should "avoid focusing on the most horrific scenarios at the expense of preparing for the most likely ones."[33]

CANADIAN AND AMERICAN RESPONSES

In Canada, the Ressam case served to sharpen the focus on asymmetric threat policies that government agencies have been developing over the past few years. The incident disturbed the normal cordiality (if not complacency) of Canadian-American relations, and provoked a serious inquiry into whether Canadian security forces were doing their jobs. The issue grew even hotter with the discovery that not only was Ressam apparently linked to the bin Laden terrorist network, but he was also tied to the shadowy world of organized crime in Montreal. For Canadian authorities, the Ressam affair came as a wake-up call, and demonstrated how an asymmetrical, transnational threat could undermine public confidence as well as upset Canada's all-important relationship with the US.

Surprising though it might seem to some, Ottawa's response to the threats described here is fully congruent with the 'human security' agenda developed by the former foreign minister, Lloyd Axworthy. This is not to say that a Canadian response to asymmetric threat requires that agenda, merely that it is consistent with it.[34] That agenda recognizes the vulnerabilities created by the effects of globalization; viewed from this perspective, human security can be depicted as everyone's 'forward defence'. As explained by one high-ranking official in the Department of Foreign Affairs and International Trade (DFAIT), the notion of security being predicated solely on defence of the state and its territorial integrity is ceding place to a broader concept that includes a "human security dimension to foreign policy, alongside national security."[35]

Of the many aspects comprising the human security agenda, not a few relate directly to asymmetric threats. One in particular warrants highlighting: the need to address "threats from both military and non-military sources (e.g., intrastate war, state failure, human rights violations, terrorism, organized crime, drug trafficking)."[36] While human security is no panacea, it does at least make the case for contemplating public safety in a context that transcends the purely domestic framework of policy. In other words, under human security's presuppositions, the military can be argued to shoulder an important part of the burden alongside law enforcement agencies. But how might this be accomplished?

Some insight can be gleaned from the June 1999 DND document, *Shaping the Future of the Canadian Forces: A Strategy for 2020*. In harmony with the basic thrust of human security, this document recognizes a range of direct and indirect dangers to national security for which military responses "may be required", including illicit drugs, organized crime, illegal immigration, terrorism, WMD and cyber-terrorism. The document accounts for the new global battlespace and recognizes the added dimension ushered in by networks in cyberspace, though its authors tend to downplay the immediacy of the menace of cyber-terrorism.[37] Defence plan-

ners and policymakers are urged to become "innovative" and "proactive", and are enjoined to strengthen specific capabilities to combat asymmetric threat and to create counterthreat relationships with domestic and international partners.

One country in particular is singled out: future military strategy will witness strengthened "interoperability with the U.S. Armed Forces, training together ... and pursuing collaborative ways to respond to emerging asymmetric threats to continental security."[38] In the wake of the Ressam affair, it is the 'combined' or so-called 'homeland defence' aspect that stands out, for it takes a dim terrorist indeed to fail to notice that one way to strike America's heartland is by means of the continent's 'seams'.

In the US, Joint Forces Command has been mandated to define the kind of American military required in 2020, a task that obliges it also to heed the measures required to combat terrorism, including the home-grown variants. On 5 June 2000, the congressionally appointed National Commission on Terrorism released its controversial report urging government to adopt a more aggressive stance in combatting this threat on American soil. The commission was created nearly four years ago, in the aftermath of US embassy bombings in Kenya and Tanzania. In the words of its chairman, Paul Bremer, a former State Department ambassador-at-large for counter-terrorism, the "threat is changing, and it's becoming more deadly."[39]

Of significance in the commission's report, and worthy of serious consideration by Canadian authorities, was the recommendation that the US President contemplate the designation of the military as the 'lead' organization for the government's response to any "catastrophic" terrorist activities in the US.[40] Such a recommendation underscores a sense of concern that law enforcement agencies on their own may not be up to the job of combating asymmetric threats seen to involve 'vital' interests. The recommendation raised bureaucratic hob in Washington, and touched off a turf dispute involving, among others, the leadership of the Department of Defense, the CIA, and the FBI. The 11 September assaults provided the catalyst for institutional change in the form of the new Office of Homeland Security led by Governor Tom Ridge. A White House agency, the Homeland Security Council will include the Attorney General, the Secretaries of Defense, Treasury, Health and Human Services and Agriculture, as well as the Directors of the FBI and Federal Emergency Management Agency. Moreover, a decision has been taken to create a military homeland defense command.

A ROLE FOR SPECIAL OPERATIONS FORCES?

In view of the nature of asymmetric menaces, the requirement to blend military capabilities with those of law enforcement agencies, and the recently announced policy directives in Ottawa and Washington, might there be a niche here for special operations forces (SOF)? SOF are strategic assets that typically possess enhanced capabilities in training and equipment that readily permit their employment across the full spectrum of operations. Carefully selected and highly trained, SOF bring a unique suite of sophisticated skills to the battlespace, while retaining a low profile. They can be a most versatile force, particularly under conditions where wisdom might preclude the deployment of conventional military units, given political sensitivities.[41] SOF units, especially those designated for counter-terrorism, excel in the precise and discriminating application of force.

Mission focused and, by their very nature, unconventional in their thinking, Canadian and American SOF regularly evince uncommon as well as highly developed interagency linkages. That these could be useful against asymmetric adversaries in the continental context, not least because of the complexities of North American society, is evident to analysts such as John Collins, who notes that the "self-reliant, highly-motivated, superbly-trained SOF, especially those proficient in foreign languages and with cross-cultural skills, seem ideally suited for many missions ... in the twilight zone between peace and war."[42]

According to military doctrine, SOF train for the primary missions of unconventional warfare, direct action, internal defence, special reconnaissance, counter-terrorism, civil affairs, and psychological operations. As a result of this training, collateral benefits can accrue in such areas as humanitarian assistance, counter-narcotics, security assistance, and search and rescue. A 1999 study conducted by Major David Last, a political science professor at Royal Military College, examined the doctrinal aspects and listed the following possible missions for the country's SOF: counter-terrorism, counter-WMD operations, militarized international police operations (MIPO), international criminal enforcement (ICE), corporate operations, offensive and defensive information operations, peace support and stability operations (PSSO), and security and evacuation.[43] Moreover, hostage rescue, special techniques for tactical mobility, and high-tech special reconnaissance and surveillance may figure prominently in many of these missions. And, in the continental context, the spectrum of such operations will be both joint (military-civilian and multi-agency) and combined.

While SOF could probably find meaningful employment in all the operations listed above, one seems particularly suited to their talents: high-tech special reconnaissance and surveillance. Not that SOF would be used on any routine investigations, but rather in serious cases where police forces are neither equipped nor trained for a given environment. Consider the example of the 1996 Gustafson Lake incident where the RCMP lacked proper equipment and training for sustained operations in an interior hinterland. Without becoming decisively engaged, SOF surveillance patrols could readily have provided valuable assistance to law enforcement authorities in the timely collection of intelligence about the nature of the incident and activities at the site. High-tech information gathering assets, common only to military SOF units, could have contributed to a more peaceful and speedy resolution of issues.

Asymmetry demands improved human intelligence (HUMINT), and under the auspices of law enforcement, SOF could deploy detachments to supplement traditional

police assets. Working independently, SOF could confirm information gathered by other means, as well as work to deny information to those under surveillance. Small teams could deploy as close personal protection for civilian leaders. Threats posed by more destructive weapons such as WMD could require being countered by SOF direct action missions, including special reconnaissance duties and detailed technical surveys for validation of future actions. Operations against narco-terrorists and organized criminals would have a multidimensional aspect, comprising operators from military, police, legal, and other categories and institutions. Information on financial transactions and surveillance of communication nodes may become necessary to verify and locate targets.

Other more traditional but specialized military assets such as electronic warfare units, medical teams, search and rescue technicians, and communications experts could be employed as part of a broader military/civil melding of efforts or directly with SOF. The blossoming of cyber-terrorism could usher in a new SOF element, perhaps under the umbrella of psychological operations, staffed by a blended team of military, civilian and law enforcement personnel.[44]

THE LEGAL AND CONSTITUTIONAL CONTEXT

One could go on with the inventory, but for our purposes here, it is sufficient merely to illustrate the existence of valid roles in confronting asymmetric threats. Fuller capability surveys have been done, but these are in the 'classified' domain of various law enforcement and military entities. However, one important point needs to be kept in mind; while SOF formations are permanently organized and available, some nettlesome legal and constitutional matters remain, whose resolution would be essential for effective employment of SOF. In the US, not the least of these are *Posse Comitatus*[45] and the Fourth Amendment.

In Canada, the Canadian Forces operate in a supporting role under direction of the civil authority. Retaining the legal link to this authority, the Chief of the Defence Staff commands operations where potential exists for disturbance of the peace, when operational equipments are to be employed, or where critical public attention is likely.[46] Since the CF do not have a mandate to conduct direct law enforcement operations in Canada, any provision of personnel or resources is arranged under the CF assistance to provincial police forces directions (CFAPPFD). Approved by the Solicitor General and the Minister of National Defence, CF assistance remains only in a supporting role to the police force of jurisdiction, which retains full responsibility for enforcing the law. At the federal level, Canada cooperates with the US in a counter drug strategy where military surveillance assets are employed in detection and apprehension of criminals involved in illegal activity. The Solicitor General is the lead agent responsible for counter-terrorism; under the CF armed assistance directions (CFAAD), the military may provide support to resolve an incident that affects the national interest, or has the potential so to do.[47]

The operational deployment of Canada's counter-terrorism/special operations unit, Joint Task Force Two (JTF 2) or the nuclear biological chemical response team (NBCRT), in support of law enforcement agencies would most likely occur under the provisions of CFAAD. While the police would retain responsibility for the incident site, CF elements would act under military command and control.[48] In effect, the blending of military and police assets to meet a specific challenge would require the approval of the Solicitor General and the Minister of National Defence, under Cabinet supervision. Currently, Canadian defence planning recognizes that "potential for asymmetric attacks on deployed operations or on citizens, property or territory will increase the demand for flexible and unconventional contributions to the security of deployed forces, peace support missions, and Canadian interests, and also for improved intelligence."[49]

In the US, primary responsibility for combating domestic terrorism resides in the FBI, with the CIA retaining jurisdiction abroad. The *Posse Comitatus* Act of 1878 forecloses full use of federal military capabilities inside the US. The act does not apply directly to National Guard units, which remain under state control, although in certain circumstances these units have been nationalized and placed under federal control and legal constraints. The prohibitions against using regular troops or federalized National Guard forces in law enforcement are not, however, absolute. As the keeper of public order, the US President may respond to a state governor's request to call out the troops. This mechanism mainly applies to such acts of public disorder as riots.

The US National Security Act of 1947, defined by Code Title 10, refers thusly to *Posse Comitatus* restrictions:

> The Secretary of Defense shall prescribe such regulation as may be necessary to ensure that any activity (including the provision of any equipment or facility or the assignment or detail of any personnel) under this chapter does not include or permit direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law.[50]

There is an exception in Title 10 that provides for SOF to train civilian law enforcement agencies in counter- and anti-terrorism, including counter drug enforcement and security against WMD. Indeed, units of Special Operations Command have "devised such innovative tactics and techniques that many Federal agencies call on their expertise."[51] Moreover, it is recognized that the President, with congressional concurrence, may enact legislation to ease the *Posse Comitatus* restrictions in the event of extreme threats. It is possible that the emerging cyber-threats might fall into the latter category, for as Gregory Grove observes:

> If information-warfare [IW] technologies and American dependence on information infrastructures develop to a point where IW attacks may kill thousands or cause vast economic

harm, Congress may choose to pass a statutory exception regarding the protection of information infrastructures. Such an IW threat seems more credible in light of the comments of the President, a former secretary of defense and a former director of the CIA.[52]

Grove is hardly alone in his assessment of the problem. Winn Schwartau asks, "If the Pentagon deploys the SEALS, Special Forces, and Delta Forces to deter or respond to asymmetrical threats, why does Washington shrink from treating IW in the same fashion?"[53] Anticipating serious confrontation in the new battlespace, other analysts have advised the US to 'enhance its elite forces'.[54] The increased concern about transnational threats has sparked renewed debate concerning *Posse Comitatus*, with civil authorities scrambling to review and clarify their understanding of its application, so as to incorporate it into their thinking on military doctrine and operating procedures for civilian police. While this debate goes on, the American military holds to its conviction that 'soldiers cannot be policemen'.[55]

Clearly, improved systems for gathering and sharing intelligence are required in responding to asymmetric threats. This, however, touches off another legal debate, as intelligence gathering remains largely structured as it was during the Cold War. In the US, constitutional provisions, notably the Fourth Amendment, restrict the use of national intelligence for domestic law enforcement. Emerging threats are challenging the relevance of this restriction, and there are now advocacies for new legislation to "bridge the gap between the traditional use of intelligence to prosecute criminal cases, and strategic intelligence, which is used to predict, preempt, and defend against attacks on the United States and its citizens."[56] It appears time for Americans to rethink the legislative and regulatory oversights currently imposed on intelligence gathering, so that they might design a system better able to operate against threats in the new battlespace. Such a rethink will almost certainly lead to a reassessment of the merits of utilizing SOF in the gathering of HUMINT.

Reflective of this is the above-mentioned June 2000 report of the National Commission on Terrorism. Among its most controversial proposals is the one recommending that Washington "begin surveillance of every foreign student on U.S. soil since 'a small minority may exploit their student status to support terrorist activity'."[57] In view of the enormous challenge such a requirement would impose, some have been moved to restrict the surveillance to students coming from countries deemed unfriendly to the US. In all of this, the operative word in the report is 'surveillance', an activity upon which one scholar comments bluntly, "[u]nfortunately, sometimes you have to forego some human rights and civil liberties issues, if it's in the national security interest and can save lives."[58]

CONCLUSION

The comments above demonstrate how the current debate can and does take on implications for American civil liberties. In the view of civil libertarians, little about the threat of asymmetric warfare justifies the "conclusion of some officials and commentators that we must increase government power at the expense of personal freedoms."[59] That may be so, but the continued process of global integration will almost certainly exacerbate the severity of the problem caused by asymmetric threats.

With such concerns as sovereignty and homeland defence at issue, it is likely that military capabilities, both in Canada and in the US, will be irresistibly drawn into a closer, more seamless pattern of integration with law enforcement authorities. That new debates are taking place is a healthy process, one that reminds us of the need to balance our defensive requirements against the fundamentals of liberal democracy. Nevertheless, the blurring of traditional lines of responsibility, as between law enforcement and military authorities, coupled with the ambiguities surrounding the very meaning of 'criminal activity', points to a future demand for joint and combined responses. The filling of that demand is most likely to require innovative and proactive employment of SOF.

CMJ

NOTES

An earlier version of this article appeared as a chapter in *Over Here and Over There: Canada-US Defence Cooperation in an Era of Interoperability*, ed. David G. Haglund (Kingston: Queen's Quarterly Press, 2001).

1. See Carolyn W. Pumphrey, ed., *Transnational Threats: Blending Law Enforcement and Military Strategies* (Carlisle, PA: US Army War College, Strategic Studies Institute, November 2000).
2. Bonnie Baker, *The Origins of the Posse Comitatus*; available at http://www.airpower.maxwell.af.mil/air-chronicles/cc/baker1.html, 1999), pp. 3-5.
3. On 14 December 1999, Ahmed Ressam was arrested by US customs personnel on an automobile ferry crossing from Victoria to Washington. He was allegedly transporting high explosive ingredients in the trunk of his car. As of this writing, Ressam was on trial in Los Angeles, facing imprisonment of 130 years if convicted on the nine charges against him. Doug Saunders, "Security Stringent as Ressam Trial Opens," *Globe and Mail*, 13 March 2001, p. A10.
4. Bruce Wallace, "The Terror Hunt," *Maclean's*, 24 January 2000, pp. 22-26.
5. Jeff Sallot, "Guarding Canada's E-Frontier," *Globe and Mail*, 20 February 2001, p. A6. This new office is headed by an associate deputy minister, Margaret Purdy.
6. Robert Holzer, "Threats to U.S. Homeland Loom Larger," *Defense News*, 15 January 2001, pp. 1, 27.
7. Robert David Steele, "The Asymmetric Threat: Listening to the Debate," *Joint Force Quarterly*, No. 20 (Autumn/Winter 1998-99), pp. 78-79.
8. Directorate of Land Strategic Concepts, *The Future Security Environment* (Kingston, 1999), pp. v-vi. (Hereafter cited as DLSC, Security Environment.)
9. David Last, "Future of Counter-Terrorism and Special Operations Forces in Canada," a discussion paper presented to the Deputy Chief of the Defence Staff, Ottawa, May 1999, p. 1.
10. W. J. Fulton, "Threat Definition: Asymmetric Threats and Weapons of Mass Destruction" (Ottawa: Department of National Defence, April 2000), p. 2.

11. Dan Roper, "Transnational Threats — U.S. Military Strategy," briefing by US Joint Staff, J-5 Global (Chapel Hill, NC, 2 February 2000), p. 6. Also see Steven Metz and Douglas V. Johnson II, *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts*, Strategic Studies Institute Special Report (Carlisle, PA: US Army War College, January 2001).
12. DLSC, *Security Environment*.
13. Fulton, "Threat Definition," p. 2.
14. *ibid*, p. 3.
15. Department of National Defence, Directorate of Strategic Analysis, *Strategic Overview 2000* (Ottawa, September 2000), p. 113.
16. Gawdat Bahgat, "Iran and Terrorism: The Transatlantic Responses," *Studies in Conflict and Terrorism* 22 (April-June 1999), p. 149.
17. US Army War College and the Triangle Institute for Security Studies, "Transnational Threats: Blending Law Enforcement and Military Strategies" (Carlisle, PA: US Army War College, 2000), p. 1. (Hereafter cited as AWC/Triangle, "Transnational Threats.")
18. Winn Schwartau, "Looming Security Threats: Asymmetrical Adversaries," *Orbis* 44 (Spring 2000), p. 199.
19. Mark Juergensmeyer, "Understanding the New Terrorism," *Current History* 99 (April 2000), p. 160.
20. *ibid*.
21. Dennis B. Downey, "Domestic Terrorism: The Enemy Within," *Current History* 99 (April 2000), p. 169.
22. AWC/Triangle, "Transnational Threats," p. 2.
23. John Arquilla, David Ronfeldt and Michele Zanini, "Information-Age Terrorism," *Current History* 99 (April 2000), p.179. Also see Martin C. Libicki, "What Is Information Warfare?" in *Toward a Revolution in Military Affairs: Defense and Security at the Dawn of the Twenty-First Century*, ed. Thierry Gongora and Harald von Riekhoff (Westport, CT: Greenwood, 2000), pp. 37-60.
24. Last, "Future of Counter-Terrorism," p. 3.
25. Schwartau, *Looming Security Threats*, p. 200.
26. *ibid*.
27. Arquilla, Ronfeldt, and Zanini, "Information-Age Terrorism," pp. 179-80.
28. AWC/Triangle, "Transnational Threats," p. 1.
29. Jonathan B. Tucker, "Chemical and Biological Terrorism: How Real a Threat?" *Current History* 99 (April 2000), p. 147.
30. On this concern, see Oliver Thränert, "Nuclear Weapons: A Deterrent to Biological Warfare?" in *Pondering NATO's Nuclear Options: Gambits for a Post-Westphalian World*, ed. David G. Haglund (Kingston: Queen's Quarterly Press, 1999), pp. 81-105.
31. Fulton, "Threat Definition," p. 7.
32. Jonathan B. Tucker, "Chemical and Biological Terrorism: How Real a Threat?" *Current History* 99 (April 2000), pp. 147-48.
33. Henry Sokolski, "Looming Security Threats: Rethinking Bio-Chemical Dangers," *Orbis* 44 (Spring 2000), p. 219.
34. On that agenda, from the perspective of a policymaker, see Paul Heinbecker, "Human Security," *Canadian Foreign Policy* 7 (Fall 1999), pp. 19-25. For a scholarly assessment, see Fen Osler Hampson et al., *Madness in the Multitude: Human Security and World Disorder* (Toronto: Oxford University Press, forthcoming in 2001).
35. Paul Heinbecker, "Human Security: The Hard Edge," *Canadian Military Journal* 1 (Spring 2000), p. 13. At the time this article was published, Heinbecker served as Assistant Deputy Minister for Global and Security Policy; he was subsequently posted as Canada's ambassador to the UN.
36. *ibid*.
37. *Shaping the Future of the Canadian Forces: A Strategy for 2020* (Ottawa: Department of National Defence, June 2000), pp. 4-5.
38. *ibid*, p. 8.
39. Jim Geraghty, "How Secure Is Secure Enough?" Policy.com-News and Events: Daily Briefing, available at http://www.policy.com /news/dbrief/dbriefarc683.asp (5 June 2000), p. 1.
40. *ibid*, p. 2.
41. John M. Collins, "Special Operations Forces in Peacetime," *Joint Force Quarterly*, No. 21 (Spring 1999), p. 56.
42. *ibid*, p. 61.
43. Last, "Future of Counter-Terrorism," p. 4.
44. Ian Roxborough and Dana Eyre, "Which Way to the Future?" *Joint Force Quarterly*, No. 22 (Summer 1999), p. 31.
45. James G. Diehl, *The Cop and the Soldier: An Entangling Alliance? The Posse Comitatus Act and the National Security Strategy of Engagement and Enlargement*, (Carlisle, PA: US Army War College, in cooperation with the Queen's University Centre for International Relations, April 1997).
46. Douglas Bland, *The Administration of Defence Policy in Canada, 1947 to 1985* (Kingston: Ronald P. Frye, 1987), pp. 158-61.
47. B-GG-005-004/AF-023, *Civil-Military Cooperation in Peace, Emergencies, Crisis and War* (Ottawa: Department of National Defence, 1998), pp. 4/1 - 4/4.
48. *ibid*.
49. Fulton, "Threat Definition," p. 3.
50. Quoted in Baker, *Origins of Posse Comitatus*, p. 3.
51. Collins, "Special Operations Forces in Peacetime," p. 59.
52. Gregory D. Grove, *The U.S. Military and Civil Infrastructure Protection: Restrictions and Discretion under the Posse Comitatus Act*, (Stanford: Stanford University Center for International Security and Cooperation, November 1999), pp. 50-51.
53. Schwartau, "Looming Security Threats," pp. 202-3.
54. Roxborough and Eyre, Which Way to the Future?, p. 30.
55. Steele, "Asymmetric Threat," p. 80.
56. AWC/Triangle, "Transnational Threats," p. 3.
57. Quoted in Geraghty, "How Secure is Secure Enough?," p. 1.
58. Professor Yonah Alexander, director of the Inter-University Center for Terrorism Studies, quoted in Geraghty, pp. 1-2. This same reporter quotes an official of the CIA's office of public affairs as saying that "our rules and regulations are impediments to our ability to fight terrorism."
59. James X. Dempsey, "Counter-terrorism and the Constitution," *Current History* 99.

Guerrilla Matrix: Asymmetric Warfare in the Digital Economy

by Giles Trendle

this article originally appeared on netimperative.com on October 11th 2001 and was later syndicated to IT-Director.com

Small and nimble players are consistently finding innovative ways to strike big against the Goliaths. This is true whether in today's business world or the new world at war in which we live. Businesses would do well to learn the characteristics of this 'asymmetric warfare' being played out with notable achievements in today's digital economy.

As technology revolutionises and democratises the market place, conventional businesses are faced with an array of new, smaller opponents who seem to come out of nowhere with innovative ideas that threaten the old ways and undermine confidence in conventional solutions.

Shawn Fanning was an 18 year-old college dropout when he wrote the Napster file-sharing computer programme that turned the entire music industry on its head before it was bought by German media giant Bertelsmann. Napster may be neutralised, but it has spawned other file-swapping services such as Grokster, KaZaA and StreamCast which continue to threaten the profits of music companies and film studios.

Finnish student Linus Torvalds began writing open source code just for the fun of it and went on to develop the Linux operating system, today seen as a credible challenge to Microsoft as it infiltrates the mainstream market.

This David-and-Goliath-style scenario is defined in military terms as 'asymmetric warfare', whereby small players use unconventional tactics to counter the overwhelming conventional military superiority of an adversary. Asymmetric warfare can include surprise terrorist attacks such as those on September 11th; guerrillas humbling a superpower as in Vietnam; and the threat of a lone hacker paralysing the banking system or rendering the air traffic control systems inoperable.

Asymmetric warfare in the digital economy is all about resourceful freethinkers who steal a march on big business, as demonstrated by the increasing number of inventive individuals who are fixing antennas on their rooftops to create wireless-LANs (local area networks) that threaten the grand business plans of the 3G network operators.

The common theme behind the likes of Napster, Linux and the W-LAN 'guerrillas' is a mindset that relishes radical change and embraces agility of thought and action as a driver for innovation. In times of upheaval - like those generated by today's relentless technological advance - innovation lies with the people or organisations who display the versatility (and audacity) to anticipate and create the future before it arrives. In this way they spot new opportunities and outwit competitor moves.

Such pioneers often capture both the initiative and customers from the biggest and most powerful of market leaders. It is a case of innovation running rings around the traditional battle formations used by corporate commanders steeped in 20th century business strategy and doctrine.

It is clear, in both business and war, that the psychological and moral battleground has become as important in determining the outcome of a struggle as action in the main theatre of a conflict. Both Napster and Linux secured an advantage by appealing to a mindset that was not motivated primarily by money but by a sense of mission. This in turn inspires an implacable commitment to succeed. Fanning is said to have spent a 60-hour marathon session once writing code on his notebook computer for Napster.

This sort of dedication might be called 'fanatic' or, in corporate-speak, 'passionate'. The thriving band of Linux programmers are driven by the satisfaction of writing good code and winning peer respect. They are more revolutionary than mercenary, labouring for love rather than money. Microsoft, with its corporate conscripts, is confronted by a highly fanatical band of programmers who see the open source model as a compelling jihad.

Though at times divided by varying ideological standpoints on free software, the open source zealots argue that software is a resource to be shared and developed collectively so it can be used as a tool for the advancement of mankind.

Today is the era of asymmetric warfare, and asymmetric business. In a world of increasing connectivity and globalisation, there is greater opportunity for small and agile players to use the new weapon of technology - with its scope and availability - to launch innovative attacks and outflank adversaries who fail to keep ahead of the game.

'Asymmetric' players might include non-state actors, such as 'terrorists', drug cartels, or black market proliferators of weapons of mass destruction. In business it could be college-kid upstarts or entrepreneurs with new ideas. Hackers (or more correctly, crackers) can also be included on the list of asymmetric players. Whatever their mission, the small players are using technology to achieve a parity of some sorts with the entrenched leaders.

How should conventional businesses - of whatever size - respond? Executives may sit in plush conference rooms calling for 'out of the box thinking', yet most are unlikely to embrace revolutionary ideas that fly in the face of customary practice and pose a threat to their career paths and margins.

Telecom chiefs still rationalise away the importance of wireless-LANs. The Recording Industry Association of America, representing 18 of the U.S.'s biggest record companies, thought it had seen off the challenge of free downloadable music by neutralising Napster. In both cases the incumbents constructed an illusion of permanence and invulnerability.

The primary lesson in understanding how to deal with the asymmetric threat is to first accept that such a threat cannot be defeated relying on conventional methods. Just as military bombing with expensive new weaponry will not give armies the edge they need for victory over terrorism, similarly businesses cannot depend solely on conventional strategies and practices to cope with the digital world in the long run.

Microsoft seems nonplussed by the pervasive Linux threat which it cannot defeat in conventional ways: free software cannot be beaten in price (or performance); the amorphous structure of the open source community precludes any buy-out; and Linux cannot be shut down by court ruling a la Napster. Similarly, the record industry has naively equated Napster's demise with that of the much broader, more complex, and elusive online file distribution network which is still alive and well out there.

In the end, the best counter-offensive can be summed up in the expression: 'If you can't beat them, join them and beat them!' It will require identifying the pioneers in any given field, dismissing no one due to apparent lack of size, resources or experience.

It will require understanding their way of thinking. It will require the ability to 'think the unthinkable' and not rationalise away or reject ideas that are radical and revolutionary. It will require a degree of agility - both at a personal level and an organisational level - that will drive more autonomy and greater initiative. And so it will require adopting the mindset of the 'asymmetric' player in order to then create the ways and means by which to win back the advantage.

Asymmetric warfare

The idea **asymmetric warfare** fuses together many previous and more specific ideas of guerrilla warfare, espionage, atrocity, violent resistance, sabotage, non-violent resistance, and terrorism. It is a broad and inclusive term coined to recognize that two sides in a conflict may have such drastically different strengths and weaknesses that they resort to drastically different (thus 'asymmetric') tactics to achieve relative advantage - including attacks on "civilians".
Indeed, the rise of all forms of asymmetric warfare in the 20th century (including bombing civilian populations) challenged all ideas of what a "civilian" was or how or why they were to be kept immune to conflicts.
Asymmetric methods by definition do not reliably conquer or hold territory or means of production. Thus there is "no endgame", in military parlance, merely a continued escalation of attacks. Note that this criticism applies even to the side that is using conventional military tactics, if the asymmetric methods are preventing it from retaining or using territory it captures. By this definition, both the United States in the Viet Nam War and Israel in the West Bank may reasonably have been considered to have engaged in "terrorism" - to the degree their violence was for symbolic purposes.
Another argument is that a group very powerful and skilled in conventional tactics, such as a superpower, leaves no avenue of opposition other than asymmetric tactics. Either its opponents accept whatever peace process the powerful side offers, or they effectively surrender. This leads some in the peace movement to side with the conventionally less powerful side regardless of other tactics. If nothing else this discourages rewards for escalation by technology.

The end of conventional war?

Throughout the 20th century, all armies relied more and more on tactics of the guerrilla, spy, saboteur, provocateur, double agent and even terrorist. This underscored that the advantages of having no tactical unit organization were greater than the control such units provide:
"Therefore when you induce others to construct a formation while you yourself are formless, then you are concentrated while the opponent is divided... Therefore the consummation of forming an army is to arrive at formlessness. When you have no form, undercover espionage cannot find out anything intelligence cannot form a strategy." - Sun Tzu

Age of amateurs?

Global trade and mass movement of people, modern seduction and "brainwashing" techniques, religious fanaticism, the political futility of opposing undemocratic leaders or occupying powers by non-violent means, and other factors combine to suggest that the most likely future assassin is not a high-priced pro, but rather an ordinary citizen who has no prior record and whose political motive is obscure or incomprehensible. Historian Barbara Tuchman suggests that the late-19th-century anarchist assassins who killed five European (and one American) head of state from 1880 to 1901, were of this category, and although all paid with their lives, none seemed to care.
Eric Hoffer, in The True Believer, 1951, characterized the fanatic as a person incapable of self-concern, but not someone wholly destitute - there was a certain level of economic prosperity wherein the ordinary citizen had no material threat to basic survival, but also

insufficient recreation or any chance to advance socially. And that this tended to fuel mass movements.
When the first few female suicide bombers attacked Israeli targets in 2002, it sparked new fears that the methodology of brainwashing had transcended longstanding cultural boundaries, and was heralding an age of amateurs who would be deadly weapons in asymmetric warfare: unknown, uncaring, unable to be distracted or dissuaded from their mission, once they were set out on it.

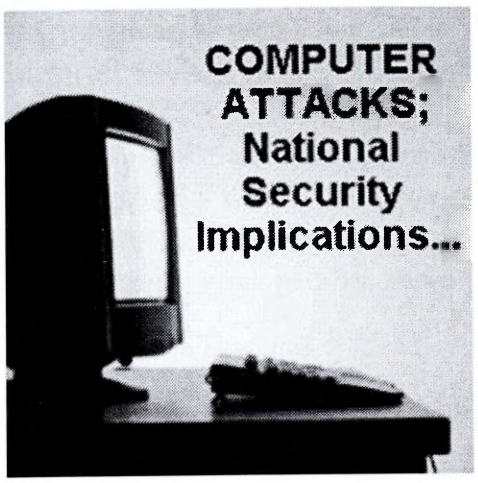
Suicide society?

Although such tactics seem wasteful, disorganized and immoral to conventional unit commanders who seek to preserve their own men and morale, there are many societies where sacrifice for the whole is respected, or even encouraged. In particular Chinese tactics and Japanese tactics have emphasized this:
"Induce them to adopt specific formations, in order to know the ground of death and life." - Sun Tzu
Like the assassins of John F. Kennedy, Martin Luther King, and Robert Kennedy in the 1960s, or the modern suicide bombers, they would likely appear from nowhere, kill their target, and be quickly caught or be already dead. Their families or loved ones may well benefit, as in the case of Palestinian suicide bombers in the West Bank during the Intifada. They may believe in some afterlife of pleasure--as the original "Hashishim" did--or simply seek to sacrifice self for a loyalty group.

Are there any civilians any more?

The sheer numbers of such people in the developing world, plus the lack of education and opportunity, and an abundance of ruthless tactical leaders who will happily employ even children as tools, suggests that the age of highly trained professional assassins, soldiers, or even "terrorists" may well be over. The new assassin or terrorist may be every frustrated individual with nothing to live for, every true believer, and in some places every grieving man.

10 July 2000



The "Love Bug," Asymmetric Warfare, and Other Computer Attacks; Future National Security Implications...

by C. L. Staten, CEO and Sr. Analyst
Emergency Response & Research Institute (ERRI)

"Only civil virtue can bring peace to an empire; only martial virtue can quell disorder in the land. The expert in using the military has three basic strategies that he applies: the best strategy is to attack the enemies reliance on acuteness of mind; the second is to attack the enemies claim that he is waging a just war; and the the last is to attack the enemies battle positions." -- Sun-Tzu, The Art of Warfare **(1)**

Has anyone noticed that the only thing that spread more rapidly than the so-called "Love Bug Virus" was the proliferation of commentary about it. In fact, the talk dominated many forums for several days after the virus was first discovered. Given this level of interest that was demonstrated and the estimated BILLIONS of dollars of damage that was been done by this virus...one has to wonder what the intelligence and defense community of the United States is doing about taking a pro-active stance to protect our vital infrastructures??

Although costly to corporate America, it would appear that we as a country, have again "dodged the bullet" of major damage to our military and intelligence C4I networks. That may be due to the fact that most of the known attacks so far have targeted commercial, business or other internet-related organizations. But, the attacks that have taken place so far beg a question that must be asked at this juncture: What is going to happen when a concerted effort is undertaken by experts to use denial of service attacks **(2)**, in concert with viruses, root-cracking, and other computer-based infrastructure attacks to attack the defense/intelligence establishment of our country and her security alliances throughout the world??

We see each of these recent sets of attacks as a potential "test of effectiveness" trial. As previously discussed by this author and a number of our other esteemed colleagues (Wilson and Fuller, Denning, Forno, Schwartau, Toffler, etc.)**(3)(4)(5)(6)** one has to wonder when we are going to take these examples of 4th Generation/Asymmetric warfare seriously enough to make them a formal and more integral part of our future defense preparedness and planning. Each wave of these attacks continues to demonstrate a new and more evolved capability on the part of our adversaries.

Given a natural evolution of these tactics and the stated intent of some our transnational enemies, We must suggest that serious consideration be given at the highest levels of the U.S. and allied governments to the possibility that these tactics may be COMBINED with the use of a series of conventional terrorist attacks -- or worse yet -- unconventional weapons (WMD's), to cause a vastly disproportionate effect on the both the economy of the USA and the overall psyche' of the world.(3) In light of these circumstances, it would appear that we may be quickly coming to a critical juncture in the way we respond to these threats and ultimately defend our country.

Stock-market watchers might suggest that some of these electronic/unconventional tactics have already had a preliminary intended effect on our economy, shown by a recent decline in world stock markets. The insurgents are spreading mistrust/a lack of confidence in the technology sector...the very place where the U.S. economy has show the greatest increases in productivity and where a majority of our advantages in international business and military superiority have been shown in recent years. The economic capabilities of many nation-states, including the United States, are increasingly becoming a "center of gravity" that will be attacked by various kinds of insurgent forces.

According to classic Clausewitzian theory, "a center of gravity is always found where the mass is concentrated most densely... Clausewitz argued that this is the place where the blows must be aimed and where the decision should be reached. He failed to develop the idea of generating many non-cooperative centers of gravity by striking at those vulnerable yet critical tendons, connections, and activities that permit a larger center of gravity to exist."**(6)**

Strategist and military thinker, Col. John R. Boyd, contradicts Clausewitz by suggesting that the tactics of the future may: "Generate many non-cooperative centers of gravity, as well as disorient or disrupt those that the adversary depends upon, in order to magnify friction, shatter cohesion, produce paralysis, and bring about his collapse; or equivalently, uncover, create, and exploit many vulnerabilities and weaknesses, hence many opportunities, to pull adversary apart and isolate remnants for mop-up or absorption."(6)

"Perpetrated by mercenaries, ideological or religious zealots-- it doesn't matter which -- corporations and business networks will undoubtedly become future targets of terrorism. More enlightened terrorists have discovered (maybe already in some countries), or will discover soon, that the path to the fear and chaos that they crave most may be more easily achieved by a wide-scale attack on infrastructure/economic targets, thus causing a general breakdown in society..."**(7)**

Particularly in those fractionalized nation-states that are already less stable or suffering the pangs of religious and political separatist movements, the targeting of economic targets may prove extremely successful in orchestrating the eventual overthrow of the established government.

The Current "Anti-Capitalist Movement" and Similarities to "Classic" Guerilla Warfare Activities

Most informed observers have not, so far, drawn any linkage between recent civil disturbances in several countries, sporadic terrorist acts, and an increasing number of various kinds of attacks on computer systems...all of which may be associated with an increasing re-emergence of what this author calls the "old left." Yet, there are many parallels that can be drawn with regard to strategies and tactics being used in recent events and those described by Mao Tse-Tung in his classic work, "Mao Tse-Tung on Guerilla Warfare."**(8)**

Griffith succinctly describes a number of Maoist tactics that may have been adapted and are being used by "anti-capitalist," Muslim extremist, FARC guerillas in Colombia, and any other number of separatists movements; "The [the guerillas] rely on imaginative leadership, distraction, surprise, and mobility to create a victorious situation before the battle is joined. The enemy is deceived and again deceived. Attacks are sudden, sharp, vicious, and of short duration. Many are harassing in nature; others are designed to dislocate the enemy's plans and to agitate and and confuse his commanders. The mind of the enemy and the will of his leaders is a target of far more importance than the bodies of his troops."**(9)**

In other words, according to Griffith, "The enemy's rear is the guerilla's front...they [the guerillas] themselves have no rear." With our increasing reliance on technology for our success, America's computer infrastructure must presently be considered one of the most essential parts of "our rear."

Clearly socialist, communist, or even anarchist in viewpoint, much of the rhetoric contained within many recent hard-core "anti-capitalist" statements would seem to advocate the future use of violence if non-violent measures and actions do not accomplish their self-determined objectives. One must wonder how long it will be before the more radical of the "anti-capitalists" decide that the use of explosives or other weapons is the next logical step in their protest of international trade.

China, Unrestricted Warfare, and Multi-Dimensional Conflict

One of the more troubling documents that this author has had occasion to read in recent times is a book by two Chinese People's Liberation Army (PLA) colonels. The book is entitled "Unrestricted War." **(10)** In it, are plans to utilize various kinds of unconventional warfare methods to defeat a superior enemy (the unnamed United States). Included would be the use of "conventional" terrorism, the use of chemical, biological, and nuclear weapons, and attacks on critical computer infrastructure targets. By combining these various unconventional tactics, "Unrestricted War"

hypothesizes that the attacker can have a advantageous disproportionate effect, even on a militarily superior enemy.

Admittedly, it is unlikely that attacks on America's computer infrastructure will cause the kind of massive numbers of dead and wounded citizens that we would normally attribute to either conventional terrorism or open warfare. While it is possible that the right kind of cyber-attack, undertaken in the right way, and attacking the right nodes of our critical systems could result in injuries or deaths, it is far more probable that these attacks will be used as a "force multiplier" and undertaken in concert with the use of other types of more conventional weapons. In fact that is exactly what Liang and Xiangsui suggest in their work described above **(11)**.

Maybe as problematic as the fact that Chinese strategists appear to be exploring plans to defeat a superpower like the United States, is the fact that the concepts outlined by the two Chinese colonels could almost immediately be undertaken by any number of "rogue states," "non-state actors," or terrorist organizations.

Conclusion

"This revolution [in Information or Asymmetric Warfare] also requires the political and military leadership to understand the purpose and consequences of war and the risks that attach to any military action. On recent evidence, none of these attributes are present to any degree, and across the world a risk-averse approach to warfare in all its forms has seeped into the corridors of power. That in turn will lead to an increasing dependence on IW (Information Warfare) as the perfect solution for fighting wars with no risk of casualties and at relatively low financial cost. But, that is to seek the very silver bullet that does not exist. As David proved to Goliath, strength can be beaten. America today looks uncomfortably like Goliath, arrogant in its power, armed to the teeth, and ignorant of its weakness." **(12)**

References:

(1) "Sun-Tzu, The Art of War," Translated by Sawyer, R. D., Published by Barnes and Noble Books/Westview Press, 1994

(2) "Series of "Real-time" EmergencyNet News Reports Concerning Denial of Service Attacks on Leading Web Sites on the Internet - 08 Feb 2000 to 16 Feb 2000", Staten. C. L. et al, EmergencyNet News, 2000. Available on the internet at: http://www.emergency.com/2000/dos2000.htm

(3)"Emerging, Devolving Threat of Terrorism," BY Fuller, F. and Wilson, GI, ENN Daily Report - 11/30/96 - Vol. 2, No. 335. Available on the Internet at: http://www.emergency.com/devlthrt.htm

(4) "Information Warfare and Security," Denning, D., Addison-Wesley, 1999. Errata. Available for purchase on the internet at: http://cseng.awl.com/bookdetail.qry?ISBN=0-201-43303-6&ptype=0

(5) "Hidden Threats And Vulnerabilities To Information Systems At The Dawn Of A New Century, Forno, R., EmergencyNet News; 11/22/98 Available on the internet at: http://www.emergency.com/techthrt.htm

(6) "War and Anti-War; Survival At the Dawn of the 21st Century," Toffler, A. and H., Published by Little Brown and Company, 1993, Pg. 141

(6) "Historical Pattern: Carl Von Clausewitz'On War'- 1832; Patterns of Conflict" Boyd, J.R., Available on the internet at: http://www.belisarius.com/default.htm

(7) "Asymmetric Warfare, the Evolution and Devolution of Terrorism; The Coming Challenge For Emergency and National Security Forces," Staten, C. L., ERRI, 04/27/98. Available on the internet at: http://www.emergency.com/asymetrc.htm

(8) "Mao Tse-Tung on Guerilla Warfare," Translated and Introduction by Brig. Gen. Samual B. Griffith, USMC, (Ret), Praeger Publishers, 1961

(9) ibid, "Mao Tse-Tung on Guerilla War," pg. 23

(10) "Unrestricted Warfare," Qiao Liang and Wang Xiangsui, Published by PLA Literature and Publishing House, 1999.

(11) ibid

(12) "The Next World War; Computers are the Weapons and the Front Line is Everywhere," Adams, J., Pg. 313, Published by Simon and Shuster, 1998

Asymmetric Warfare, the Evolution and Devolution of Terrorism;
The Coming Challenge For Emergency and National Security Forces

By: Clark L. Staten, Executive Director & Sr. Analyst
Emergency Response & Research Institute
04/27/98

"Terrorism will remain a major transnational problem, driven by continued ethnic, religious, nationalist, separatist, political, and economic motivations." (1)

The nature of global conflict is changing. It is the considered opinion of the Emergency Response & Research Institute (ERRI) that there is a general paradigm shift underway in regard to how future conflicts will unfold. This transition is one of form rather than substance. Mass violence, injuries and deaths will continue to occur, although we believe they will happen in different places and in differing ways than one might currently imagine.

With Russia's conventional forces on the verge of dissolution, the likelihood of a massive massed tank battle on the plains between Europe and Russia is almost a forgotten possibility. Similar circumstances in Saudi Arabia or Kuwait, or near of the DMZ between North and South Korea are also becoming increasingly unlikely. Although circumstances regarding another conflict with Iraq are still possible as this is written, probable prospects there would suggest that the United States (at worst) would undertake a strategic bombing campaign, rather than committing large numbers of ground troops to massed combat.

What is far more possible, however, in the coming decade, are an increasing number of "brush-fire" wars, counter-insurgency campaigns, hostage rescue operations, "drug wars," low intensity conflicts, urban combat, and "peacekeeping operations" that will require a vastly different set of tactics, equipment, training and skills than

conventional military engagements of the past. Future conflicts, at least in the near term, may not involve commitments of massive numbers of troops to fixed battle zones, but will likely involve combating small units of fanatical terrorists using Weapons of Mass Destruction (WMD) and other sophisticated tactics and technologies.(2) As Commandant of the of the Marine Corps General Charles C. Krulak, likes to say, the United States will often be fighting engagements that are more like Somalia, Haiti, and Bosnia than they are like Desert Storm. (3)

Why Is This Occurring?

Of great concern is the fact that any number of what were previously considered essentially stable countries are experiencing religious, ethnic and other internal conflicts with increasing numbers of separatist movements trying to carve up larger countries into smaller and more tightly focused ethnic areas. Some of these conflicts are ancient and have been the cause of fighting for hundreds of years. Others are more recent and the result of demographic shifts, changing political regimes, or religious/ideological shifts.

Add to these factors political and ethnic internal disintegration caused by faltering economic circumstances in several parts of SW Asia, the Far-East, Africa, South America and elsewhere and you have a combustible mix that is certain to fuel future conflicts in a number of parts of the globe for the foreseeable future.

Marine Corp Colonel Gary I. Wilson, a long-time observer and analyst of emerging trends in non-conventional warfare, also says that he believes that changes in terrorist tactics, methods and operational activities are a naturally occurring phenomena. He draws similarities between bacteria that naturally mutates in order to become resistent to antibiotics or other adverse conditions. His comparison would suggest that terrorists and their methods also mutate, or change in form, in order to find new ways to survive and better project the strengths of the terrorists against the weaknesses of opposing civilizations.

According to James Denney, ERRI Senior analyst, global societies traditionally contain a myriad of subcultures that are based on strongly held ethnic, religious, cultural and ideological beliefs. In instances where many subcultures interact, new

subcultures are generated in much the same way as a living cell generates another and another, until finally a new entity is created. Thus the structural integrity of a given society becomes increasingly complex.

Most incumbent ideologies in the postmodern era are struggling to maintain their dominant identity within their sphere of influence. Because of conflicting ideologies, presumptive religious and ethnic diversity has not materialized in many societies. For this reason, the concept of vertical ethnic and religious integration has given way to horizontal migration and factional polarization within these societies.

This is an engineered dynamic which creates a breeding ground where fanatical ethnic and religious tribalism has emerged as fractal subcultures, vying with each other for inclusion, with mutually exclusive and often conflicting agendas. This situation results in ethnic and religious migration to both geographic and political positioning within the existing society.

Through centuries of serial discrimination, imperious rule and unrelenting subculture manipulation, diversity has successfully been restricted while rulers continue to rise through the incumbent ideology or ruling system. Any perceived threat to the incumbent ideology will always be met with resistance, deflection, threat or illusional compliance, while the status quo is maintained. In some cases, a "preemptive defense" is commonly employed, whereby on one or more pretext, estranged factions are exterminated. Employing this methodology, the incumbent ideology (read government/ruling class) is insured passage from one class of rulers to the next, while those deemed unworthy or contemptible by the "powers that be" are manipulated, bypassed or ignored. This marginalization is often the motivation for violent acts.

How Is It Happening/What is Changing?

Very few countries, today, have the wherewithal to undertake a major attack on any of the major countries of the world...particularly the United States. Thus the reason

that terrorism is both evolving and devolving. (4) Most nation-states have recognized the fact that they can no longer engage in open combat nor overtly support terrorism without fear of military retaliation or even openly declared war with the United States or her allies.

Take this evolution theory one step further and you will find that as "terrorist organizations" begin to gain some measure of political legitimization and press attention, that even they will diminish their open support of sabotage and acts of violence against innocent civilians. Obviously, few rational people will vote for or openly support an organization that publicly admits it kills women and children in pursuit of its goals.

Additionally, it would appear that smaller and smaller splinter groups are breaking from the main force body. These ultra-radicals, if you will, have become the enforcers of the extreme ends of an ideology or belief and it is they who will use unconventional tactics to carry out particularly heinous acts. This devolution of terrorist organizations into smaller and more compartmentalized groups makes detection of these small cells increasing more difficult and intelligence gathering and analysis efforts even more valuable.

In addition to the concept of smaller cells of non-attributable, non-state actors, evidence would suggest that there are also cells of what we have called "virtual sapper squads that are put together just for the purpose of committing one act and then disbanded and dispersing back into the population of a friendly nation. (5) One of the first examples of this that was recognized by ERRI was the World Trade Center bombing. It is believed that this is done to further obscure the identities of the perpetrators, enable their escape and evasion and to further complicate the process of ascertaining their motives.

Concurrently such a strategy confuses the issue of tracing ties between the operatives and to nation-states, who sponsor, finance and offer refuge to these killers. International legal and moral justification of military retaliation by the victim state may also become even more difficult, if not impossible.

Threats from Multiple Simultaneous Vectors

By the advent of the 21st Century, not only is it likely that many of the conflicts facing the United States and her allies will be of an asymmetrical and devolving nature, and it is also likely that the threats will come from diverse and differing vectors. Particularly of concern is the possibility that conventional terrorism and low-intensity conflict will be accompanied or compounded by computer/infrastructure attacks that may cause damage to vital commercial, military, and government information and confront communications systems. (6) Unfortunately, it would appear that while the United States gains tremendous advantages from its advanced information and battlefield management systems, we also become increasing vulnerable to cyber-attacks from our adversaries.

In other words, we would anticipate efforts to cause widespread fear by computer-generated attacks on electrical, water, banking, government information, emergency response systems and other vital infrastructures, while simultaneously suffering terrorist tactics involving multiple conventional explosives and/or chemical/biological/nuclear devices. (7)(8) Even a country as large and sophisticated as the United States could suffer greatly at the hands of an educated, equipped, and committed group of fewer than 50 people. At the present time, such an attack could realistically be expected to cause an effect vastly disproportionate to the resources expended to undertake it.

The Battle For Hearts and Minds

In the Post-Cold-War era, our enemies, including Sadam Hussien of Iraq, Ayatollah Khomeini of Iran, Fidel Castro in Cuba, Yasar Arafat of the Palestinian Liberation Organization and any number of others have discovered that they can win the "hearts and minds" of the world's people through the selected use of real information, disinformation, manipulation of the press, propaganda, and other psychological (Psy-Ops) warfare methods. In fact, some would even go so far as to suggest that Mr. Hussien actually won the latest stand-off with the United States (early 1998), over Chemical/biological Weapons and inspections of his palaces, as he was able to manipulate public opinion in the United States and elsewhere and split the former allied Persian Gulf coalition. (9)

With assistance of diplomats from a number of Arab countries, Russia, and France, all of whom have a vested economic interest in ending United Nations sanctions against Iraq, Hussien was able to both prevent the bombing of his country and be authorized by the U.S. to sell even more petroleum, obstensively to buy food and medicine for the Iraqi people. A historical perspective might suggest, however, that such programs and funds have probably enabled Iraq to rebuild presidential palaces and maintain key weapons and military assets.

It is believed by ERRI analysts that such psy-ops and propaganda programs will continue to have an increasingly more influential impact on future conflicts, and that our military and political leadership should seriously consider expanding efforts by U.S. psychological warfare operations and units to counter these developments. (10)

Most Serious Concerns

In recent years, terrorists and insurgent movements have discovered that they can multiply fear in a civilian population by undertaking even more violent and deadly tactics. Federal Bureau of Investigation and the U.S. Department of State reviews of recent terrorist incidents would suggest that they believe that there are a fewer number of incidents, but that those that do occur are more deadly. Additionally, and all too frequently in recent years, terrorist and terrorist groups are no longer taking credit for their acts. It is believed that this anonymity may also be contributing to larger and more reprehensible atrocities.

The Impact of Weapons of Mass Destruction (WMD)

According to Richard K. Betts, some of the most important implications of Weapons of Mass Destruction (WMD) have not yet registered with the public. Betts asserts that the nature of the potential use of WMD's is changing. Rather than being weapons of deterrence, as they were during the "Cold War," they are increasingly becoming the weapons of choice of what were formally considered "second-rate" military powers or even non-state groups. (11) It is believed that these formerly impotent players on the world stage may believe that they have found a way to leverage non-conventional weapons to cause great fear and will use these weapons to attempt to intimidate legitimate governments.

Further and more fearsome, Cmdr. James Campbell, in his recent examination of the terrorist use of Chemical/Biological/Nuclear weapons, offers us a view of a "Post-Modern Terrorist," free of constraints provided by sponsoring nation-states, who have discovered that the use of WMD's affords them the ability to wield disproportionate power to cause massive numbers of casualties, even within the continental United States. (12)

At least some experts find this future use of WMD's in concurrence with recent trends in statistics involving terrorist attacks. A study of Federal Bureau of Investigation (FBI) and U.S. State Department (DoS) documents would reveal that they believe that there are a fewer number of terrorist incidents, but that they have produced a greater number of wounded and dead. In other words, non-state actors and post-modern terrorists, with their apocalyptic visions and belief that they are acting on behalf of some higher power, are likely to use WMD to maximize their kill ratios and send a larger and more fearsome message to their perceived enemies.

The Effects of Economic Terrorism

Perpetrated by mercenaries, ideological or religious zealots-- it doesn't matter which -- corporations and business networks will undoubtedly become future targets of terrorism. More enlightened terrorists have discovered (maybe already in some countries), or will discover soon, that the path to the fear and chaos that they crave most may be more easily achieved by a wide-scale attack on infrastructure/economic targets, thus causing a general breakdown in society and facilitating civil unrest and rioting. Evidence of insurgent attacks on economic targets have been clearly demonstrated in places like Corsica (banks, court houses), Greece (Bank, car dealership, and businesses), Colombia (multiple oil pipeline bombings), India (attack on multiple commercial buildings in Bombay), and Sri Lanka (bank and commercial building attacks). (13)(14)

These concepts, and the inherent threats thereto, will become even more evident and viable in future megatroplises where millions will live in what will be in reality a very fragile and easily combustible (in more than one sense of the word) environment. It is believed that these future societies of largely urbanized populations

will be even more vulnerable and susceptible to manipulation by insurgents using terror and low intensity warfare tactics.

There is even a possibility that the terrorist acts could be paid for by legal or extralegal multinational corporations that would benefit from the destruction of existing business competitors in a given city or region, or by less scrupulous business concerns that want to subvert or cause destabilization of an existing (and unfriendly) governmental system. Some evidence of these phenomena is already in evidence in Colombia, Pakistan, Burma and parts of the former Soviet Union.

An excellent example of this emerging situation might involve further study of a recent United Nations report that the GNP of the drug and crime driven "underground economy" in Pakistan is probably greater than that of the official government. Although sufficient studies are currently unavailable, this is also probably true in Colombia, and it is becoming increasingly likely that the same trend is developing in parts of the former Soviet Union, where organized crime "mafia organizations" have infiltrated or subverted legitimate business for their purposes. Needless to say, these patterns do not bode well for the future of the legitimate governments in these and other areas of the world.

Solutions and Recommendations

The prevailing thinking and overall mindset within military, diplomatic, intelligence, law enforcement, and emergency service communities may need modification in order to meet and combat these newly evolving patterns involving non-state actors and asymmetric warfare. Conceptually, the preparations, tactics, and strategies for fighting numerous "brush fire" conflicts and larger numbers of small scale but high-impact terrorist incidents, could prove a major challenge for those with an entrenched large force "Cold-War" mentality.

Those that are still mired in fighting another "Desert Storm" or want to continue to live in the comfortable past of a largely bi-polar, superpower-driven global situation may be in for a rude awakening as the nature of asymmetric conflict unfolds in the coming decade. There are few, if any, countries that can militarily challenge the United States in open combat at the present time. Some seemingly astute assessments

would suggest that China may become a future adversary with the industrial and conventional military power to eventually confront America and her allies, but they also point out that this capability is still evolving and that it may take China a minimum of three to five (3-5) years, or more, to become a major threat to the United States and overall world stability.

Instead, given a reasonably effective foreign policy, our assessment would respectfully suggest that the near term threat to Americans and our country's security may bring a confusing mix of "stateless actors," separatist and fringe "independence movements," insurgency operations, terrorist attacks, the use of Weapons of Mass Destruction (WMD), Information Warfare (IW), and other unconventional threats. The nature of our defense thinking, training, weapons, equipment, intelligence operations, and national emergency response systems must be redefined and redirected in order to meet these threats that are concurrently both devolving and evolving.

It should not be forgotten that our most important asset in our war with terrorists, and in our defense against other non-conventional threats, rests with the young men and women of our nation's national security and emergency service communities. While useful in more conventional circumstances, "Stand-off" missiles, ICBM's, Nuclear Weapons, and other theatre weapons are practically useless in our response to insurgents, revolutionaries, and terrorist threats. That responsibility will undoubtedly fall on smaller groups of highly trained, better-equipped, and highly motivated anti- and counter-terrorist operatives and agencies, who will monitor, infiltrate, close with and destroy those that would engage in this insidious type of future warfare. Our people will make the difference, if we give them the resources to accomplish the task.

Finally, it is recommended that Congressional and Presidential funding, policies, and other initiatives take all of the issues presented above into consideration in a comprehensive way. This strategy must encompass providing leadership, reallocating necessary funds to the most appropriate efforts, and bringing all of the available public and private assets to work together to study and devise strategies to confront this new and dynamic threat. All of the levels of government, academia and related businesses must find a way to better communicate, cooperate and coordinate

in an effective manner. Ultimately, we must ensure that we, as a country, are prepared to confront the asymmetric challenges of the future.

References:

1. "Global Threats And Challenges To The United States And Its Interests Abroad," by Lt. Gen. Patrick M. Hughes, USA Director, Defense Intelligence Agency, Feb. 5-6, 1997

2. The Fourth World War; Diplomacy and Espionage in the Age of Terrorism, by Marenches, C. and Adelman, D., Willam Morrow and Company, Pg. 30

3. "World Without Symmetry--Terrorism," Navy Times, 22 Sep 97

4. "Emerging, Devolving Threat of Terrorism," by Wilson, G and Fuller, F., EmergencyNet News Daily Intelligence Report, 11/30/96, Vol. 2, No. 335. On the internet at: http://www.emergency.com/devlthrt.htm

5. "THE LONG LIST OF SUSPECTS; Possible Theory of [Terrorist] Motivation," by Macko, S., EmergencyNet News Daily Report, Wednesday, July 24, 1996, Vol. 2, No. 206. On the Internet at: http://www.emergency.com/tersuspc.htm

6. "The IW Threat from Sub-State Groups: an Interdisciplinary Approach," by Rathmell, et al, Presented at 3rd International symposium on Command and Control Research and Technology, Institute for National Strategic Studies, National Defense University, June 17-20, 1997. On the Internet at: http://www.kcl.ac.uk/orgs/icsa/terrori.htm

7. "Middle East Terrorism: New Form of Warfare or Mission Impossible?" by LTC Stephen H. Gotowicki, U.S. Army, Military Review, May-June 1997, On the internet at: http://leav-www.army.mil/fmso/fmsopubs/issues/terror/terror.htm

8. "Reflections on the 1997 Commission on Critical Infrastructure Protection (PCCIP) Report," by Staten, C, ERRI Special Report, 10/23/97. On the Internet at: http://www.emergency.com/pcciprpt.htm

9. "Losing the War of Words," by George C. Wilson, Editorial, Washington Post, 30 Mar 98, Pg. 25A

10. "Manipulation And The Age Of The New Persuaders," by Thomas, T., Foreign Military Studies Office, Fort Leavenworth, KS., July, 1997, On the Internet at: http://leav-www.army.mil/fmso/fmsopubs/issues/maninfo.htm

11. "The New Threat of Mass Destruction," by Betts, R., Foreign Affairs, January/February, 1998, Pg. 27

12. Weapons of Mass Destruction - Terrorism, By Campbell, J. Interpact Press, 1997, Pg. 4-5

13. "Indian Bombings Caused By 'Foreign Extremists,' According to Police," By Staten, C., EmergencyNet News Special Report, 03/1/93. On the Internet at: http://www.emergency.com/bombay.htm

14. "Analysts Predict More Terrorist Attacks In Sri Lanka," by Jeremy Zakis, EmergencyNet News Daily Intelligence Report, Sunday, March 8, 1998 Vol. 4, No. 067. On the internet at: http://www.emergency.com/srilnk98.htm

---

This article, "The Evolution and Devolution of Terrorism; The Coming Challenge For Emergency and National Security Forces", was published in the Journal of Counterterrorism and Security International, Winter, 1999 edition, Vol. 5, No. 4, Pg. 8-11

Asymmetric warfare

Military planners are only beginning to grasp the implications of September 11 for future deterrence strategy

Richard Norton-Taylor, security editor
Wednesday October 3, 2001
The Guardian

The new buzz phrase of the moment is "asymmetric warfare": the September 11 attacks on the United States were the epitome of this. A few pilots armed with Stanley knives launch an assault on the world's only superpower, with its arsenal of nuclear weapons, cruise missiles, aircraft carriers, bombers equipped with state-of-the-art weapons and self-defence technology.

There is nothing new in asymmetric warfare. In the battle of Agincourt in 1415, English infantry armed with longbows crushed shining French knights on horseback. Excluding the shared American and Soviet cold war concept of MAD - mutually assured destruction - all warfare has been asymmetric, says Phillip Wilkinson of King's College, London.

"The smaller power applies its strengths against the weaknesses of the larger power," he says. The last leader who ignored this obvious notion was Saddam Hussein. Guerrilla fighters have applied it in South America, Cuba, and Chechnya. As have terrorists in Northern Ireland.

Britain has more experience than most, certainly more than the US. Ministry of Defence sources are making it clear that, in the new, long-term international campaign against terrorism now being planned in Whitehall, special forces will play a key role.

They point to the experience of the SAS during the communist insurgency in Malaya in the 1950s, in Oman during the 60s and 70s fighting rebels, and in Bosnia where they have seized indicted war criminals. The operations in Malaya and Oman did not only involve shooting the enemy. Part of the strategy was pychological - to turn them in a battle for "hearts and minds". This is what the US now appreciates must be one of the elements in the new, and unprecedented "war" against terrorism which will be fought on many fronts - political, diplomatic, financial, and economic.

Britain's colonial past also provided this country with experience in multifaceted unconventional warfare not shared by the US. You cannot apply a simple military response when you are challenged politically. The Americans tried in Vietnam and failed, says Wilkinson.

He is about to go to Washington at the invitation of the Pentagon - the US defence department - to discuss, among other things, the development of "logic and language" and political discourse in "complex emergencies". What exactly is meant by "war" or "victory"?

These are good questions in a world which has said goodbye (though many, perhaps most, military leaders are slow to recognise the fact) to the era of Clausewitz, the great 19th century German strategist, who was preoccupied with wars between states and the conventional enemy's "centre of gravity".

But if asymmetric warfare is not a new concept, it has taken on new, broader, dimensions. Osama bin Laden may have been the instigator of the attacks on the World Trade Centre in New York and the Pentagon. Those attacks, and the earlier suicide bomb attacks on US embassies in east Africa and the USS Cole in Aden, may have not happened without Bin Laden. He is a target, as are his band of an estimated 200 close associates and bodyguards, and his training camps in Afghanistan.

But he has spawned and inspired - if that is the right word, certainly it is the one used by counterterrorist agencies - al-Qaida (the Base), a loose network of fanatical Islamist supporters and extremists with links to jihads with origins in other Muslim countries.

Asymmetric warfare will be fought on every front, including its root causes, according to Whitehall officials who have set up a special committee in the Cabinet Office to think about its many facets. But it does have specifically military implications. W hat use is heavy metal - notably the battle tank - against terrorist groups hidden in tunnels and caves, or in urban apartments, with millions of pounds deposited in concealed bank accounts at their disposal?

What is needed, instead, are small groups of highly skilled and mobile special forces, and highly accurate weapons fired from manned or unmanned aircraft, backed up by good intelligence. What is needed, says Wilkinson, are flexible forces with a long reach.

The challenge for the military is to strike as precisely as possible at an elusive enemy. The September 11 attacks, which killed more than 6,000 people, were devastating and shocked governments around the world, but they had no "strategic effect", says a senior defence source.

The military response, therefore, was not to escalate. It would have been had the attack been by a state using military weapons. This has huge implications for deterrence theory, including nuclear weapons which are at the opposite end of the spectrum from the sophisticated, precise, and effective strategy of asymmetric warfare military planners and politicians are now talking about.

If nuclear weapons are of no use against such an enemy, there are also questions about the deterrent value and purpose of the Bush administration's missile defence project. Those who were behind the attacks on the US - an atrocity condemned by most of the "rogue" states the project is supposed to deter - do not have intercontinental missiles, are unlikely to possess them and do not need them. Trucks with conventional explosive would do.

Fears are being expressed that they will get their hands on nuclear, biological, or chemical, weapons - weapons of mass destruction. Though the ease with which terrorists could obtain such material and use them as weapons is exaggerated, this is clearly a priority for international agreements, and national security, intelligence, and civil defence agencies - all part of the arsenal of asymmetric warfare.

richard.norton-taylor@ guardian.co.uk

National Strategy Forum Revie
Winter 200

ASYMMETRIC WARFARE: OLD METHOD, NEW CONCERN

David L. Grange

"By indirection find directions out."
—Shakespeare, Hamlet

Strategists define asymmetric warfare as conflict deviating from the norm, o an indirect approach to affect a counter-balancing of force. Such warfare is not new. Combatants throughout the ages have continually sought to negate or avoid the strength of the other, while applying one's own strength against another's weakness. Asymmetric warfare is best understood as a strategy, a tactic, or a method of warfare and conflict. Because no group or state can defeat the U.S. in conventional warfare, America's adversaries and potential adversaries are turning to asymmetric strategies. We must therefore understand asymmetric warfare, and be able to respond in kind.

"When conventional tactics are altered unexpectedly according to the situation, they take on the element of surprise and increase in strategic value."
—Sun Bin, The Lost Art of War

Though there are numerous examples of asymmetry in 20th century warfare, its use was not as pronounced between adversaries as it is today. Wars were primarily fought by nation-states with balanced, conventional fighting capabilities. When asymmetric methods were used, usually in the form of maneuver or technological advantage, they had a dramatic effect.

Three prominent examples of asymmetric actions that counterbalanced established force are: the *sturmtrupp* assault tactics that broke the trench-line stalemate and three-dimensional warfare as a result of the airplane during World War I; the panzer *blitzkrieg* through France in World War II; and the *Strategic Defense Initiative* that helped end the nuclear arms race between th U.S. and the Soviet Union. The kind of asymmetric strategy and tactics seen in the Vietnam War were termed guerilla warfare. These asymmetric actions however, did not produce the dramatic, day-to-day effects on operations that we have seen since the fall of the Berlin Wall.

At the present time the U.S. has no identified conventional, war-making peer as we had prior to Desert Storm. This absence of global peer competitors makes the world more uncertain, unstable, and difficult to anticipate. As the

sole superpower, with the accompanying expectations placed on the U.S. and our extensive presence around the world, the U.S. has become a big and inviting target. The U.S. engages in humanitarian assistance, peacekeeping, and enforcement of UN or NATO sanctions, and maintains bases necessary for force projection worldwide. Our adversaries confront and confuse us with a multitude of asymmetric actions that catch us by surprise, to which we continue to respond with a *Cold War* mentality.

Since Desert Storm, our adversaries have learned not to come at us in a symmetric way since it is impossible for any country to engage the U.S. in an arms race. By using asymmetric actions, our adversaries exploit our vulnerabilities; taking advantage of the *global information environment,* they are also able to do so on the cheap.

Reality of the Operational Environment

"Whosoever desires constant success must change his conduct with the times."
—Nicolo Machiavelli, The Prince

Today we see an ambiguous world, with people, groups, and governments pursuing complex goals. The borders have blurred between governments and people, military and populace, public and private. New *fourth-generation warriors*[1], non-national and trans-national groups based on ideology, religion, tribe, culture, zealotry, and illegal economic activities, have pushed many regions of the world into anarchy.

Russia is in disarray, with increased fighting within its Muslim states in the oil-rich Caspian Sea region. The Balkans, though somewhat stabilized, have enormous corruption problems with no real peace in sight. The counter-drug war in Colombia and Mexico has intensified. Israel, the Middle East, North Korea, and Taiwan remain powder kegs.

This dangerous environment, coupled with the increased use of our military as an extension of U.S. diplomacy, has placed us in a situation where our adversaries employ asymmetric tactics to negate superior conventional strength. We Americans look at conflict through a winner's eyes-usually from a past war. Setbacks cause concern, and if our quick-fix for the conflict at hand derails, due to unintended consequences, we usually overreact and are unable to deal with reality. Our standard approach to adversary actions means that we have trouble adapting to what we actually find on the ground. Planned intervention on the cheap, with awkward constraints, is inflexible and pompous. Past high-tech, standoff warfare is largely ineffective against these fourth-generation adversaries. We continue trying to play American football on a European soccer field.

Captain Larry Seaquist notes, "While the U.S. military pushed toward high-tech, low-casualty combat, war went the opposite direction-toward brutal neighbor-on-neighbor killing, carried out by ragtag collections of citizen-warriors, some of them just children."[2]

These low-intensity conflicts have no quick-fix solutions. They have comple

cultural, religious, and historical origins where criminality, population coercion, and extremist politics abound. Asymmetric tactics, usually conducted out of necessity by our adversaries, are an economy of force and a weapon of choice.

As Liddell Hart explained, "Campaigns of this kind are more likely to continue because it is the only kind of war that fits the conditions of the modern age, while being at the same time suited to take advantage of social discontent, racial ferment, and nationalist fervors."[3]

Our diplomats, commercial investors, and military will continue to experienc the unpredictability, chaos, and asymmetric threats that are becoming the norm around the world. The greatest threat to world stability appears to be small, regional wars with which the U.S. will be forced to contend.[4] Are we ready for this type of threat?

The Threat

"It is every Muslim's duty to wage war
against U.S. and Israeli citizens
anywhere in the world."
—Osama bin Laden[5]

Americans separate war and peace; most of our enemies today do not. Osama bin Laden in Afghanistan, the "Army of Mohammed" in Yemen, and narco-guerrillas in Colombia are but a few groups that threaten America, our allies, and regional stability. The extensive, twisted links between terrorism, black marketers, drug lords, arms dealers, and zealots have created a formidable enemy.

Most of our adversaries are non-nation-state actors (terrorists, international and trans-national criminal organizations, or insurgents). They have a completely different mindset, believing they are continuously at war. Violence is a way of life. They know violence is an excellent tool against a democratic people worried about any threat to its way of life. Taking advantage of the information age, our adversaries are able to show atrocities, abuse, and destruction on our television screen daily. The values of enemies are different from ours, making it very difficult for us to understand why they don't behave the way we believe they should.

Operating in agrarian cultures, with a small toolbox of dangerous, high-tech capabilities, they maintain power with machete-wielding intimidation. Most are predators that take advantage of weak states for refuge, and the discontent of the local populace for support. If they cannot inspire support from the people, they coerce recalcitrant members. Once established, they operate in and out of these areas with impunity.

"Greater powers and resources
do not guarantee tactical superiority."
—*Sun Bin,* The Lost Art of War

These fourth-generation enemies have become very adept at using the

asymmetric tactics of information warfare. They manipulate print and radio, distort images with perception management and background film clips (or "I Roll") on global television, and disrupt the Internet. The *infosphere* has become a new battleground suited for asymmetric attack from across the globe. Serbian President Slobodan Milosevic was an expert at using the media as a weapon. Through deception, disinformation, and the "CNN factor," he excelled at this cerebral form of competition.

Saddam Hussein has convinced most of the Iraqi population, many of our Western allies, and the Arab world that the UN-U.S. sanctions are directed against the people, not his tyranny. For 10 years, through the use of asymmetric actions, he has tied up countless ships, troops, and aircraft without reinstating sanctioned compliance inspections.

The Chinese have taken serious steps in their warfighting strategy for future conflict. Not only have they steadily enhanced their conventional arsenal wit high-tech innovation, but they have learned the pronounced effect asymmetri actions have had on the U.S. and its allies over the last 10 years. Two modern-day strategists, Senior Colonel Qiuo Liang and Senior Colonel Wan Xiangsui, have laid out in detail how to conduct full-spectrum warfare again the U.S., using asymmetric strategy, in their book *Unrestricted Warfare.*[6] This warfare strategy doesn't follow any rules, counters the U.S.'s high-tech advantages, and optimizes the electro-magnetic spectrum. All dimensions of space are considered the battleground.

Adversary Actions

"Water shapes its course according to the ground over which it flows; the soldier works out his victory in relation to the foe whom he is fighting."
—*Sun Tzu,* The Art of War

Recent examples of asymmetric actions abound around the world. Riots planned by faction leaders, made up of coerced non-combatants, and manipulated by gangster police, were effective against NATO troops keepin the peace in Bosnia. Milosevic was able to move special police troops and other thugs at will throughout Kosovo, destroying life and infrastructure, while NATO's unmatched air power was incapable of stopping him.

A group of Palestinians redirected British funds earmarked for education programs to further ideals of tolerance, mutual respect, and peace, instead using the money to send children to guerrilla training schools and then put them on the streets of Israel to fight. This was a successful deception of the British government's generosity.[7]
One of the insurgent forces in Colombia, *Fuerzas Armadas Revolucionarias de Colombia* (FARC), has nationally threatened every Colombian millionair and corporate CEO unless a tax is paid for protection. This action has produced immense pressure from the upper class on government authorities in Colombia. The FARC has also leveraged the Colombian government into conceding a portion of the country to their control, separated by a recognized and accepted demilitarized zone. Colombia now has more displaced citizens (one million) than Kosovo experienced during their war.

Chechen rebels in Russia have demonstrated time after time the effectiveness of asymmetric action against conventional forces by capitalizing on local support, information warfare, terror, cutting critical supply lines, and using urban areas to render irrelevant the superiority of the Russian armored forces.

Our national expectation of a casualty-free, high-tech conflict is challenged, for example, by rogue-state impertinence, setbacks dealt by the warlords of Mogadishu, and terrorist attacks, like those on the USS Cole and our embassies in Tanzania and Kenya. We have been forced to pull back in fear, changing our operational effectiveness around the world.

What Can We Do?

"He will conquer who has learnt the artifice of deviation"
—*Sun Tzu,* The Art of War

Our response to asymmetric actions has usually been to react with defensive, hunkering-down, panic decisions; or in some cases to retaliate ineffectively with air or cruise missile attacks, occasionally injuring non-combatants or disgracing ourselves in the media. We continue to restrict ourselves to unrealistic rules of engagement, regardless of the situation. Deception, psychological operations, cyberwar, disinformation, "softwar,"[8] are all non-kinetic ingredients in the toolbox of fourth-generation warriors, that should, in turn, be used against them.

We must understand that relative strength is situational; it is based on time, speed, location, and conditions. These intangibles are harder to define and offer strength in different circumstances. The side that is weaker in resources or complex command and control systems can balance that with superior cleverness, morale, offensive attitude, security, surprise, flexibility, and organizational design that fit the task at hand. We must preempt enemy asymmetric actions by attacking the cohesion and flow of their operational cycle.

An adversary must plan, gain support, move, stage, attack, and regroup during any operation or in pursuit of a cause (Figure 1). We can cause him to fail anywhere along this process-optimally, prior to his attack phase. It's all a matter of gaining positional advantage, mentally or physically, over an opponent. Our adversaries have been very adept at gaining positional advantage with asymmetrical action against our moral and organizational domain (Figure 2). We can reverse this advantage by doing the same.

Asymmetrical targeting (deny, destroy, disrupt, dislocate, degrade) of adversary moral and organizational domains, instead of our typical, predictable, standard, conventional approach against physical strength provides a faster, effective defeat. Indirectly preventing our enemy from gaining ascendancy over the local population, denying organizations the use of safe areas, disrupting cash-flow and other supplies, negating effective use of the media, exposing corruption, disgracing the leadership, breaking power relationships, will put adversaries on the defensive and force them off balance.

This requires initiative, momentum, out-of-the-box thinking, flexibility, and winning mindset. Crimes against humanity, small wars, and probable mega-terrorist (biological, chemical, nuclear, information) disasters are threats worthy of our attention. We must turn the tide on these fourth-generation warriors using asymmetric actions with a preemptive strategy. It's a matter o being the hunter or the prey.

Notes

1. Lind, William S., Maj. John F. Schmitt, and Col. Gary I. Wilson. "Fourth-Generation Warfare: Another Look," *Marine Corps Gazette,* December 199
2. Seaquist, Larry. "Community War," *Naval Institute Proceedings,* August 2000.
3. Hart, Liddell. *Low-Intensity Operations,* 1971, p. 16.
4. Grau, Lester and Jacob Kipp. "Small Wars," *NSF Review,* Summer 2000.
5. Vince Crawley "Terror Alert," *Army Times,* Nov. 6, 2000.
6. Liang, Qiuo and Wang Xiangsui. *Unrestricted Warfare,* 1996
7. "Why are we paying for children to learn how to kill?" *News of the World,* November 5, 2000.
8. *Softwar* is a term developed by information operations strategist Chuck DeLaco to describe the hostile use of global visual media to shape another's will.

BG (Ret.) David L. Grange is Executive Vice President and Chief Operating Officer of the Robert R. McCormick Tribune Foundation. He retired from th U.S. Army in 1999 after 30 years of service, with his final position as Commanding General of the First Infantry Division. In that position, he served in Germany, Bosnia, Macedonia, and Kosovo.

FORUM
FOR APPLIED RESEARCH AND PUBLIC POLICY

Asymmetric Warfare

Like the young David with his sling-shot, hostile nations armed with cheap but effective weapons pose an increasing threat to the Goliath of U.S. military might.

BY JONATHAN B. TUCKER

Since the breakup of the Soviet Union in 1991, the United States has been the world's sole superpower. It is the only country to maintain a global naval presence, a panoply of overseas bases, and the ability to deploy military forces to distant regions. The U.S. defense budget, at over $280 billion for fiscal year 2000, is several times larger than the combined spending of the countries generally perceived as the most likely future U.S. opponents: China, Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria, and Yugoslavia.[1]

No potential adversary comes close in advanced conventional weaponry—such as cruise missiles, stealth fighter-bombers, laser-guided bombs—and supporting navigation, surveillance, target-acquisition, and communications systems. Even the Pentagon predicts that a peer competitor will not emerge until around 2010, and most analysts consider that possibility unlikely.

Given U.S. supremacy in conventional forces, few rational opponents would deliberately seek a direct military confrontation with the United States—although Iraq blundered into war by miscalculating Washington's response to the 1990 invasion of Kuwait and was soundly defeated. Instead, future adversaries who resort to military force against the United States will probably employ asymmetric, or David-and-Goliath, strategies involving innovative yet affordable weapons and tactics designed to weaken U.S. resolve and its ability to use its superior conventional military capabilities effectively.

A future opponent, for example, might employ nonconventional weapons—nuclear, chemical, biological, or radiological—or conduct terrorist attacks against military or civilian targets on American territory in a bid to deter or impede U.S. intervention in a regional conflict in the Persian Gulf, the Korean Peninsula, or the Balkans. Such an adversary could be selective in its objectives, timing the moment of an attack to maximize its strengths. Although the United States could ultimately prevail, the increased financial and human costs might undermine the political will of U.S. leaders to sustain the conflict or deter allies from providing assistance.[2]

U.S. Secretary of Defense William Cohen has warned that "a paradox of the new strategic environment is that American military superiority actually increases the threat of nuclear, biological, and chemical attack against us by creating incentives for adversaries to challenge us asymmetrically."[3]

HYPE OR THREAT?

To what extent is asymmetric warfare a new threat that poses a significant danger to the security of the United States? Three strategic assessments published by the U.S. Department of Defense have called attention to the issue.

The May 1997 Report of the Quadrennial Defense Review stated that a future adversary could "employ asymmetric methods to delay or deny U.S. access to critical facilities; disrupt our command, control, communications, and intelligence networks; or inflict higher than expected casualties in an attempt to weaken our national resolve."[4]

The National Defense Panel, a group of nongovernmental analysts commenting on the Quadrennial Defense Review, agreed that future opponents

> will seek to disable the underlying structures that enable our military operations. Forward bases and forward-deployed forces will likely be challenged and coalition partners coerced. Critical nodes that enable communications, transportation, deployment, and other means of power projection will be vulnerable.[5]

Finally, *Joint Vision 2010*, a study of warfare in the next century by the Joint Chiefs of Staff, asserted that "our most vexing future adversary may be one who can use technology to make rapid improvements in its military capabilities that provide asymmetrical counters to U.S. military strengths, including information technologies."[6]

In response to these alarming declarations, skeptics have argued that military scenarios focusing on asymmetric threats tend to overstate the vulnerabilities of the United States, and that merely identifying theoretical windows of vulnerability does not necessarily mean that real-world adversaries could climb through them. These analysts allege that the Department of Defense has exaggerated the asymmetric threat in order to justify its inflated budget in the post-Cold War era.[7]

The following analysis concludes that while the threat of asymmetric warfare on U.S. territory is of real concern, a more likely scenario is that such tactics will be used to constrain the ability of U.S. forces to intervene in regional conflicts rapidly and at relatively low cost.

THE ASYMMETRIC ARSENAL

Numerous asymmetric strategies could be used to disrupt U.S. military capabilities and bring the conflict to the U.S. homeland. For example, high-tech and low-tech countermeasures could exploit the vulnerabilities of advanced U.S. weapons and their supporting systems. Information warfare could be used to disable computer networks, paralyzing communications, transportation, power systems, and industrial enterprises. Public-relations warfare might allow opponents to exploit the international news media to weaken the resolve of U.S. decision makers. Nonconventional attacks by special forces armed with chemical and biological agents could disrupt U.S. military operations. And foreign states could sponsor terrorist attacks against civilian targets to undermine public support for foreign intervention or to deter states from joining a U.S.-led coalition.

COUNTERMEASURES

Given the Pentagon's heavy reliance on high technology, future adversaries might develop relatively simple countermeasures designed to turn sophisticated U.S. military assets into wartime liabilities. Low-tech countermeasures, such as aluminum reflectors that confuse targeting radars and heat generators that deceive infrared sensors, are cheap and easy to use. During the 1991 Gulf War, Iraq employed several deliberate countermeasures and a few inadvertent ones. Although these tactics did not have a significant impact on the outcome of the war, they did reduce the effectiveness of some high-tech weapons in the

U.S. arsenal.

For example, Iraq foiled intensive Coalition efforts to find and destroy its Scud missile launchers by deploying decoy missiles together with barrels of diesel fuel to simulate secondary explosions when hit.[8] A crude Iraqi mine put out of action the Aegis missile cruiser *U.S.S. Princeton*, one of the U.S. Navy's most advanced ships.[9] Baghdad hampered sophisticated efforts to eavesdrop on its military communications by relying on buried coaxial and fiber-optic landlines that were hard to cut or tap, rather than using radio or satellite communications.[10] And Iraq's extended-range Scud ballistic missiles were so poorly constructed that they broke up under the stress of reentry, effectively creating a swarm of "decoys" around the warhead that confused the guidance system of the Patriot antimissile defense system. As a result, few if any Patriot interceptions were successful.[11]

A more sophisticated adversary might attempt to jam transmissions from the U.S. Global Positioning Satellite system, which aids many precision-guided weapons, or to sabotage critical command, control, and communications nodes such as satellite terminals and switching stations. Knocking out a few key nodes might disable a larger network of facilities supporting U.S. military operations. Nevertheless, such tactics are essentially defensive. While effective countermeasures might delay a U.S. victory and make it more costly, they would probably not change the outcome of a conflict, given the overwhelming superiority of U.S. military forces.

INFORMATION WARFARE

The Pentagon is concerned that adversaries or terrorists might employ software commands or malicious programs to shut down or disable key military computer systems. The fact that young hackers have been able to break into U.S. Navy and National Aeronautics and Space Administration (NASA) computers suggests that determined cyber-warriors from a hostile nation or a well-financed terrorist group might inflict considerably more damage. Programmable weapon systems may also be vulnerable to attacks by self-replicating computer viruses that erase stored data. According to Defense Secretary Cohen, "We have to spend a good deal more attention to looking at ways in which our reliance upon technology can be undone by a simple interruption."[12]

The cyber-terrorist threat also extends into the civilian sector. As the most computerized country in the world, the United States relies on a vast number of networked processors and databanks for the operation of its critical infrastructure—the system of interdependent industries and institutions that provide a continual flow of goods and services essential to the nation's security and welfare.[13] Such systems include energy distribution, transportation, banking and finance, water supply systems, emergency services, telecommunications, and continuity of government. This dependence makes the United States potentially vulnerable to deliberate cyber-terrorist attacks against critical government or corporate computer networks, with the intent to create massive disruption and chaos. According to the President's Commission on Critical Infrastructure Protection, "We must learn to negotiate a new geography, where borders are irrelevant and distances meaningless, where an enemy may be able to harm the vital systems we depend on without confronting our military power."[14]

Some analysts have argued that cyber-attacks targeted at computerized systems for air-traffic control, the switching of commuter trains, or the control systems of a nuclear power plant or a chemical factory could kill large numbers of people. This threat appears to have been exaggerated because air-traffic, train, and power-plant and industrial control systems are not accessible through the Internet but have their own internal networks. For those

networked computers that are potentially vulnerable to information attacks, defenses can be enhanced by investing in greater redundancy, encryption, electronic firewalls that insulate classified computers from the outside world, tagging of data to detect outside manipulation, and compartmentalization of computer systems so that they fail gracefully rather than catastrophically.[15] The challenge is not the lack of available defenses but rather the will of government and industry to invest in them.

PUBLIC-RELATIONS WARFARE

A potentially more effective form of information warfare in the military context is an enemy's manipulation of the mass media to influence American public opinion, thereby restricting the U.S. government's ability to employ its overwhelming military superiority. During the Vietnam War, the enemy's use of asymmetric guerilla tactics and its ability to endure massive firepower while continuing to inflict American casualties gradually turned public opinion against the war and undermined the political will of policy-makers to sustain the conflict.

Since Vietnam, the U.S. public has become highly sensitive to casualties, particularly in military operations perceived as peripheral to the nation's core security interests. During the U.S. intervention in Somalia in October 1993, irregulars associated with Somali warlord Mohamed Farah Aideed killed 18 American soldiers in the streets of Mogadishu, stripped a dead soldier's body, and dragged it behind a truck in view of press cameras. These horrifying images aroused U.S. public opinion against the intervention and precipitated a rapid pullout. Given these precedents, a cunning adversary might take advantage of the "CNN factor" to weaken the resolve of U.S. policy-makers undertaking or merely contemplating a military intervention.

Iraqi President Saddam Hussein, for his part, has been able to exert substantial leverage against a vastly superior foe by exploiting the reluctance of the U.S. government to inflict civilian casualties, because of moral constraints and concerns about the negative political fallout in the Arab world. Fully aware of the American ability to strike at any target in Iraq, Saddam has situated key strategic assets such as biological-weapons plants in densely populated areas. Prior to the 1991 Persian Gulf War, he also arranged for the transportation of Iraqi citizens to potential bombing targets to serve as human shields. In this way, Saddam has repeatedly used his own civilian population as pawns in an asymmetric strategy designed to undermine the willingness of the United States to employ its overwhelming offensive capabilities.

According to one analysis, "Iraq…[has] taught the world how to put the most powerful military in history on a leash...by convincing America's leadership that political defeat will be the price of military victory.... The lessons of America's recent failure of nerve will not be lost on future opponents who lack its wealth, but possess the strength of will to fight with unconventional means."[16]

MILITARY TARGETS

With the spread of chemical and biological weapons to states that sponsor terrorism — such as Iran, Iraq, Libya, Syria, and North Korea—the Pentagon is increasingly concerned about the potential for nonconventional attacks against U.S. forces.[17] To be effective, such agents would not have to be delivered by missile or tactical fighter. Instead, they could be spread by low-tech delivery systems such as a modified agricultural sprayer mounted on a moving truck, boat, or aircraft.

During the Gulf War, U.S. military planners feared Iraq might employ its chemical and biological weapons against coalition forces deployed in Saudi Arabia, but fortunately these

attacks did not materialize.[18]

Today, the massive battlefield use of chemical or biological agents is no longer considered the most likely threat, because it could provoke a massive retaliatory strike. A more plausible scenario would involve a series of coordinated, low-level attacks by special-operations forces or terrorists, delivered by covert means against multiple targets at home and abroad. Some chemical agents such as mustard gas and VX nerve gas, and biological agents such as anthrax spores, are highly persistent and could be used to contaminate airstrips and ports in order to disrupt military operations.

Since the end of the Cold War, the Pentagon has closed several bases overseas and at home and now relies far more heavily on a small number of facilities within the continental United States that might be vulnerable to sabotage.

A fictional scenario included in a 1997 Pentagon-sponsored study envisions an asymmetric attack by a future enemy with small amounts of chemical and biological agents to impede the U.S. ability to project power to a regional theater in a timely manner.[19] In this scenario, Iraq again invades Kuwait, this time with the assistance of its erstwhile enemy Iran. Both countries recognize that if the invasion is to be successful, U.S. military intervention must be delayed, and covert chemical and biological attacks are seen as potentially effective for this purpose. Baghdad and Tehran decide to disrupt U.S. airlift and sealift operations by using a persistent chemical-warfare agent to contaminate key troop-deployment ports and airfields in the continental United States. They also release an incapacitating biological agent upwind of U.S. naval ships and other facilities on the island of Diego Garcia, the Indian Ocean base that was used in the 1991 Gulf War and in Operation Desert Fox. The attack is timed to trigger a major outbreak of incapacitating illness among American troops on the day of deployment.

This scenario is plausible in that airlift and sealift operations from U.S. bases at home and abroad are a potential Achilles' heel. Particularly vulnerable are civilian support personnel such as stevedores and data-processing specialists working at ports and control centers, since few of them have been trained or equipped with protective gear against chemical or biological attacks. At the same time, some of the assumptions underlying the scenario appear unrealistic. How likely is it that Iraq would form a military alliance with Iran—its archrival for hegemony in the Persian Gulf and former adversary in a bloody, eight-year war—or that both countries would be capable of coordinating a complex series of political, military, and terrorist attacks?

CIVILIAN TARGETS

The United States, the sole remaining superpower, has become a prominent terrorist target because of its global military presence, repeated interventions in distant conflicts, and prominent role in security alliances and peacekeeping operations. These activities have incurred the wrath of countries and groups that resent America's power and perceived arrogance, its tendency toward unilateral action, its loyal support of Israel, and the corrosive effect of American popular culture on social and religious values. Thus, terrorist outrages against U.S. targets often represent a lashing-out against America's predominant military, economic, political, and cultural influence.

Given the emergence of international terrorist operations on U.S. soil, such as the 1993 bombing of the World Trade Center in New York City, the Pentagon worries that state-sponsored terrorists might bring a future conflict to Main Street America by deliberately attacking civilian targets by asymmetric means. Rather than employing long-range ballistic missiles for strategic attacks on U.S. cities, hostile nations or state-sponsored terrorist organizations could smuggle nonconventional weapons into the United States in crates or

suitcases. Multiple simultaneous attacks against domestic targets could constrain U.S. military operations abroad by creating a major political crisis at home. Alternatively, terrorist threats might be used for political blackmail, such as compelling the United States to withdraw its forces from Saudi Arabia.

Biological or radiological attacks on U.S. citizens could have delayed effects that might not be detected for days, giving the perpetrators time to escape and the state sponsor a chance of avoiding identification. Some have argued that if terrorists were to conduct an attack in a nonattributable manner, it would be politically costly for the United States to retaliate without compelling evidence of complicity.[20]

Nevertheless, the ability of U.S. intelligence and law-enforcement agencies to track down the perpetrators of unclaimed terrorist incidents should not be underestimated. Washington was able to link the 1986 bombing of a Berlin discotheque frequented by U.S. soldiers and the 1988 bombing of Pan Am 103 to Libyan agents, suggesting that it is not easy for a state sponsor to evade responsibility.

Even so, some terrorists may not be deterrable. A few terrorist groups may believe they can carry off a biological attack without attribution; others are transnational in nature and cannot be linked to one country, such as the Islamic fundamentalists involved in the World Trade Center bombing. Such groups are only loosely associated with a state sponsor or may carry out terrorist attacks on their own initiative. Moreover, some religious fanatics may be prepared to die for their cause.

NEW DIRECTIONS

In short, the primary aim of asymmetric warfare is to constrain the ability of the United States to intervene rapidly and at relatively low cost. It is important, however, to distinguish among the various asymmetric strategies, which range from low-tech to high-tech. Only relatively developed countries with extensive technical and financial resources have the potential to mount sophisticated attacks on U.S. weapon systems and computer networks. Yet few such countries currently have hostile or aggressive intentions toward the United States that would lead them down this path. Other adversaries, such as Iraq or Yugoslavia, may desire to bloody the United States' nose, but they do not have the capability to carry out sophisticated attacks. By conflating these various actors and scenarios, the Department of Defense has tended to exaggerate the strategic significance of asymmetric warfare. It is therefore necessary to disaggregate these various threats if we are to assess them realistically.

Moreover, the Pentagon has so far made few real changes in force structure, weapon procurement, or military doctrine to address the purported vulnerabilities it has identified. To minimize the threat of asymmetric warfare to U.S. forces and weapons, the Department of Defense should consider some new policy options.

First, instead of devoting scarce resources to procuring Cold War-legacy weapon systems, the Pentagon should place greater reliance on long-range guided weapons that can hit targets from a safe distance, without the need for manned ships or aircraft to penetrate enemy defenses. The United States should also cut expenditures on a costly yet ineffective national antiballistic missile system and place greater emphasis on other types of homeland defense, such as enhanced protection of U.S. cities against terrorism with nonconventional weapons. "Star Wars" systems are impotent against the terrorist threat, which is far more likely to arrive by suitcase than by ballistic missile.

Second, if nuclear, chemical and biological weapons continue to proliferate, U.S. willingness to confront future aggressors may be sharply reduced. The Pentagon should retool its military strategy for a major ground war to minimize the number of lucrative targets vulnerable to nonconventional attack, such as dense concentrations of forces and

centralized staging areas for logistics and reinforcements. U.S. troop units and weapon platforms should be reduced in size and increased in number to permit greater mobility and dispersal across the battle zone, thereby avoiding the creation of valuable targets. U.S. armed forces should also improve their capabilities to rapidly decontaminate large aircraft and ships, and—assuming that foreign nations will allow the establishment of new bases abroad—create multiple transshipment points to limit the vulnerability of airlift and sealift operations.

Third, the United States should enhance its ability to prevent and mitigate the consequences of chemical and biological attacks. On the prevention side, the intelligence community should upgrade its technical and human resources for monitoring enemy and terrorist acquisition of relatively small quantities of chemical or biological warfare agents. To mitigate the consequences of a possible attack, the armed services should develop and deploy improved sensors to detect and identify battlefield contamination, including low-level exposures to chemical nerve agents, which have cumulative toxic effects.[21] The armed forces also need to provide protective training and equipment to key civilian defense workers. If the United States enhances and publicizes its ability to cope with the medical consequences of chemical or biological warfare, this capability would help deter such attacks.

Fourth, it is not clear that in the post-Cold War era, military intervention is always desirable or in the national interest. In the past, unilateral U.S. involvement in a regional conflict—particularly on behalf of one side in a civil war as in Vietnam, Nicaragua, and Somalia—has often proved counterproductive, eliciting widespread hostility on the part of those who resent perceived U.S. arrogance. Thus, one way to minimize the future threat of asymmetric warfare would be for the United States to employ greater restraint towards intervention in regional conflicts. Some analysts contend that by disengaging from secondary military commitments around the globe, the United States could reduce the incentive for terrorist attacks against Americans at home and abroad without adversely affecting its core security interests.[22] Obviously, an activist U.S. foreign policy requires overseas bases and operations. As the world's sole remaining superpower, the United States should be prepared to intervene when necessary to prevent genocide, to halt massive violations of human rights, or to contain regional aggression. Wherever possible, however, Washington should act as a member of a multinational coalition.

Finally, not all security threats are best addressed through military means. By strengthening nonproliferation treaties and export-control regimes designed to halt the spread of nuclear, chemical, and biological weapons, and by promoting diplomatic settlements of the festering conflicts in Yugoslavia, the Middle East, Southern Africa, and the Korean Peninsula, the United States can minimize the need for military intervention in the future. This diplomacy-centered strategy would require a much greater investment in nonmilitary instruments such as negotiation, foreign assistance, the promotion of democracy, and the effective use of the United Nations—including the full payment of back dues—backed up existentially with the big stick of U.S. military power.n

Jonathan B. Tucker is director of the CBW Nonproliferation Project at the Monterey Institute of International Studies, Monterey, CA.

1. Center for Defense Information, "The Fiscal Year 1999 Military Budget," *Defense Monitor* 27 (4) (1998), p. 2.
2. Christopher Gunther, "You Call This a Revolution?" *Foreign Service Journal* 75 (9) (September 1998), p. 22.
3. Center for Defense Information, "Military Domination or Constructive Leadership?" *Defense Monitor* 27 (3) (1998), p. 8.
4. US Department of Defense, *Report of the Quadrennial Defense Review*, "Section II: The Global Security Environment" (May 1997).
5. National Defense Panel, "Transforming Defense: National Security in the 21st Century," *Joint Force Quarterly* (Summer 1997), pp. 10-11.

6. US Department of Defense, Joint Chiefs of Staff, *Joint Vision 2010* (Washington, DC: DOD, October 1997), pp. 10-11.
7. Carl Conetta and Charles Knight, "Inventing Threats," *Bulletin of the Atomic Scientists* (March/April 1998), pp. 32-38.
8. Rick Atkinson, *Crusade: The Untold Story of the Persian Gulf War* (Boston: Houghton Mifflin, 1993), p. 175.
9. Ibid., pp. 326-329.
10. Ibid., p. 439.
11. Theodore A. Postol, "Lessons of the Gulf War Experience with Patriot," *International Security* 16 (3) (Winter 1991/1992), pp. 119-171.
12. William Cohen, "Remarks on the Quadrennial Defense Review" (Washington, DC: Center for Strategic and International Studies; May 22, 1997).
13. Federal Bureau of Investigation, National Security Division, Counterterrorism Threat Assessment and Warning Unit, *Terrorism in the United States 1996* <http://www.fbi.gov/publish/terror/terroris.pdf>, p. 19.
14. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, "Executive Summary" (October 1997), p. ix.
15. Richard Danzig, "The Next Superweapon: Panic," *New York Times* (November 15, 1998), p. A15.
16. Ralph Peters, "How Saddam Won This Round," *Newsweek* 132 (22) (November 30, 1998), p. 39.
17. Chemical warfare agents are supertoxic human-made chemicals such as mustard gas and sarin, while biological warfare agents include disease-causing germs, such as anthrax, and poisonous chemicals, such as botulinum toxin and ricin, made by living organisms.
18. "Hypothetical Biological Warfare Attack with Anthrax," in Albert J. Mauroni, *Chemical-Biological Defense: U.S. Military Policies and Decisions in the Gulf War* (Westport, CT: Praeger, 1998), pp. 216-217.
19. Booz-Allen & Hamilton, *Assessment of the Impact of Chemical and Biological Weapons on Joint Operations in 2010* (McLean, VA, October 1997); see also "Germ War Games," *Salon Magazine* (February 9, 1998) <http://www.salonmagazine.com/news/1998/02/09news.html>.
20. Danzig, "The Next Superweapon: Panic."
21. US General Accounting Office, *Chemical Weapons: DOD Does not Have a Strategy to Address Low-Level Exposures*, Report No. GAO/NSIAD-98-228 (Washington, DC: GAO, September 1998).
22. See Christopher Layne, "The Unipolar Illusion: Why New Great Powers Will Rise," *International Security* 17 (4) (Spring 1993), pp. 5-51; and Eugene Gholz, Daryl G. Press, and Harvey M. Sapolsky, "Come Home, America: The Strategy of Restraint in the Face of Temptation," *International Security* 21 (4) (Spring 1997), pp. 5-48.

Reshaping the Military for Asymmetric Warfare

The tragic and shocking attacks of Sept. 11 have raised fundamental questions about the shape and composition of future U.S. forces. An independent defense review published by the Center for Defense Information, and released just before the attacks, provides a roadmap for substantially restructuring the U.S. military to counter new threats in the first quarter of the 21st century.

The review concludes that the U.S. military can, and must, be restructured to successfully undertake fourth-generation warfare against asymmetric threats — the kind of threats posed by terrorist networks. The study places a premium on the need for addressing personnel issues and doctrine, rather than hardware. It argues for boosting the cohesion and initiative-taking of U.S. troops, and asserts that the agility of America's forces should be enhanced by creating lighter, smaller and more mobile units. In contrast to the recently-issued Quadrennial Defense Review (QDR), the report suggests reductions in legacy forces to free up resources for transformation of other forces and for the other, ever more important, components of national security.

A Different Form of Warfare

At root, the "American way of war" remains focused on a paradigm variously known as attrition, second-generation, or Industrial Age warfare. This style of war-fighting tends to be linear and slow moving, relying on masses of men and material to physically crush (albeit not necessarily through frontal assaults) or threatening to crush an opponent. Industrially, second-generation warfare emulates and relies on mass production techniques to mobilize, train and equip, and deploy military forces. . . .

Real third-generation war-fighting breaks battlefield linearity by seeking and exploiting a combination of "spaces and timing" vis-a-vis an enemy — that is, creating or at least finding weak points or gaps in enemy thinking and dispositions and taking advantage of these openings before the opponent can rectify them. The objective of this kind of warfare is to collapse the opponent's will to fight early (ideally, even before becoming decisively engaged) by introducing chaos into his intelligence/surveillance-evaluation/command-action/ reaction processes. This can be done by anticipating the actions of the opponent and preempting his intentions via unexpected thrusts and parries by highly agile, dispersed friendly forces brought together quickly for the mission and just as quickly dispersed when the action is finished. This type of warfare also may free forces from the ponderous support structure characteristic of Industrial Age warfare.

Just as second- and third-generation warfare intermingle, they are both interpenetrated by what some call fourth-generation warfare. This primarily involves land forces (although targets can be naval vessels and air assets) — irregular or guerilla warfare carried out by groups motivated by ideology, revenge, lust for power, ethnicity, religion or some other unifying bond. Such irregulars often are associated with or supported by regular military forces, but in the late 20th century this was less often the case. In fact there are countervailing trends. There are more small groups or very loosely knit organizations which employ terror by threatening to or actually attacking civilian populations and infrastructure — the so-called asymmetric style of warfare. Some receive support, safe harbor, or encouragement from nations while others seem to operate with little support. [pp. 37-38]

Strategies to Win Asymmetric Warfare

"Asymmetric" warfare . . . can be used with telling effect in major theater wars, in smaller-scale contingencies, and in terrorist attacks . .

Because of U.S. dominance in [second-generation or attrition] warfare, however, opponents instead are likely to fight "asymmetrically" — avoiding U.S. strengths and attacking its vulnerabilities. They are likely to use either third-generation maneuver warfare (with regular armed forces) or, more likely, fourth-generation irregular warfare (with irregular attacks on vulnerable military units, population, infrastructure, culture, and institutions).

Two great military strategists — an ancient one, Sun Tzu, and a 20th century one, the late John Boyd . . . explain how to fight and win such warfare. Broadly, these strategists focused on how to win by outmaneuvering an enemy mentally, so as to limit the need for actual combat. Greatly simplified, their ideas suggest that to win asymmetric war:

- *Understand that military force is not the only, or necessarily the best, means of achieving national goals — excessive or inappropriate use of force breeds resentment and plants the seeds of future conflict.*
- *Attract allies to one's own side, and subtract them from an opponent's side.*
- *Focus on two major and complementary elements: create "harmony" and cohesion on one's own side, and foster chaos and paralysis on the other side*
- *Surround the opponent with sustained ambiguity, deception, surprise, isolation, and menace; pursue multiple approaches and attacks, then switch between them and develop new thrusts faster than the opponent can cope; alternate unpredictably between the expected and unexpected, the orthodox and unorthodox, distracting moves and decisive moves, or in Sun Tzu's terminology, cheng and ch'i.*
- *Understand that success in conflict depends most upon people, then ideas, and least upon hardware.*
- *Fix fraying leadership and cohesion in the military, in part by ending constant personnel rotation among units, halting the system of premature discharging of mid-level officers, and training and empowering officers to exercise more initiative.*
- *End a fixation on complex hardware, which is not only unreliable and expensive, but also creates complex bureaucracies to build, deploy, operate, supply, and fix it — bureaucracies that are unsuited to exercising the most important components of third- and fourth-generation warfare strategy: agility, quickness, flexibility, responsiveness, creativity, initiative.*
- *Structure and equip U.S. forces so that they: are agile and flexible; provide commanders with multiple options; can switch between different thrusts quickly; continuously reshape themselves through experimentation and training; and most importantly, are well led. [pp. 72-3]*

A New Operational Focus for the Military on Smaller-Scale Contingencies

"Smaller-scale contingencies" (SSCs) include a variety of military operations of smaller scale and intensity than major theater or regional wars, such as humanitarian, peacekeeping, peace enforcement, non-combatant evacuation operations — and military action to capture a terrorist or deny him shelter. The Sept. 30, 2001, QDR has moved in the direction of giving more prominence to smaller-scale contingencies, by eliminating the strategic necessity to be prepared to fight two major regional wars. More, however, must be done to shift resources, doctrine and training to reflect the increasing demand for such operations.

The large number and variety of [SSCs], however, call for a new focus on these operations as primary missions for the military in their own right, and suggest reshaping a portion of the force away from intense force-on-force combat and towards these more complex expeditionary missions.

Some suggest that these forces should constitute a special constabulary organization structured along military lines. Such units would not have the military's heavy armament but would be more heavily armed than police. (Alternatively, others suggest enlarging regular military police units.)

The experience of units in SSC interventions in Panama, Haiti, Bosnia, Rwanda-Congo, and Kosovo suggests that creating separate quasi-military units may not be the best course. The very unpredictability of SSCs, which can turn from traditional peacekeeping to peace maintenance and even peace enforcement, argue for forces that are trained to operate across most of the spectrum of conflict. The Marine Corps' "three-block war" unit training regimen that includes scenarios for mid-intensity war-fighting, peacekeeping, and humanitarian relief support seems to be appropriate for the majority of situations that U.S. ground forces actually will face in the foreseeable future. While the Army's transformation into a medium-weight force will facilitate its participation in these missions, it will retain for the mid-term elements of heavy striking power in armored/mechanized units. [p. 66]

Directions for Transformation of Forces

- *Quicken military forces in order to refocus them on smaller-scale contingencies in which they are likely to face asymmetric or fourth-generation warfare. Improve their mobility, agility, flexibility, and strategy and decision-making cycles. [p. 41]*
- *. . . these changes envision a corresponding change in war-fighting doctrine that moves away from the ponderous and logistics-heavy formations of the 20th century to a more mobile, agile, responsive force. Such a force is made possible by incorporating lighter-weight equipment; better command, control, and communications networks; and improved intelligence, surveillance, and reconnaissance — all designed to allow U.S. commanders to get inside an opponent's observation-orientation-decision-action (OODA) cycle. [p. 117]*
- *Transform some of the active heavy armored forces into forces more suited to smaller-scale contingencies. ... Preserve a heavy capability primarily in the reserves.*
- *Focus transformation and funding on agile forces such as:*

- *light- and medium-weight Army, Marine Corps, Special Operations;*
- *littoral Navy;*
- *lift, close air support, and interdiction Air Force; and*
- defensive nuclear, biological, and chemical forces and equipment.

- *Help fund the re-orientation with moderate reductions in the forces that are already overwhelmingly dominant in force-on-force combat such as:*

  - *heavy active Army;*
  - *open-ocean Navy;*
  - *nuclear and air superiority Air Force;*
  - *and offensive nuclear forces. [p. 43]*

Overall Priorities for the Future

- *People: fix personnel problems, adequately fund military readiness and "quality of life."*
- *Doctrine and training: adequately fund training and refine doctrine for third- and fourth-generation warfare and for joint operations with other nations, civilian agencies, international bodies, and non-governmental organizations.*
- *Hardware: improve mobility with airlift, sealift, overseas facility infrastructure, and force transformation; develop equipment for interoperability with allies; prioritize development of human intelligence capabilities (and ability to process data into "understanding") over new satellite or other technical data collection and communication systems.*
- *Other national security tools: adequately fund other components of national security, including the State Department, economic aid programs, and agencies that deal with transnational issues. [p. 105]*

Implications for Units and Weapons

The report proposes a strategy of transforming some of the legacy heavy forces into more agile forces for smaller-scale contingencies. That strategy, the reduction in the heavy armored force-on-force threat, and the potential for greater allied contributions if realized could allow a refocusing of resources on transformed forces and a reduction in overall force size.

Pressure to free up funding and resources for transformed forces may be eased for a while, as military budget increases of tens of billions of dollars annually are likely in the wake of Sept. 11. Nevertheless, at some point the extra funding is likely to dry up and priorities will have to be set more tightly. Recognizing continuing resource constraints, the QDR noted, "the full promise of transformation will be realized as we divest ourselves of legacy forces and they move off the stage and resources move into new concepts, capabilities, and organizations that maximize our war-fighting effectiveness and the combat potential of America's men and women in uniform."

Reductions proposed in Reforging the Sword include:

- 3 Army divisions

- 3 aircraft carrier battle groups
- almost 4 air wings [p. 119]

The Marine Corps, with its broad mix of ground, air, and sea capabilities would keep all three active divisions and air wings.

Certain weapons are more suited — and some are less suited — to the proposed strategy. Priorities suggested are:

Continue or accelerate:

- Light Armored Vehicle
- V-22-like transport aircraft
- airlifters
- communications and other equipment for interoperability with allies
- littoral-oriented naval vessels
- low-density/high-demand aircraft and tankers

Delay, cancel or cut:

- Crusader howitzer
- Comanche scout/attack helicopter
- B-2 bomber
- CVX, DD-21, NSSN
- F-22
- Nuclear weapons [pp. 126-7]

Special Operations Capabilities

In the unlikely event that it is well known where and how a weapon of mass destruction attack against the United States is being prepared in a foreign country, U.S. forces can of course conduct pre-emptive attacks. U.S. military strategy should ensure that Special Operations and other forces have a capability for long-range raids to attack weapon development, deployment, or launch sites and command structures if necessary to prevent weapons of mass destruction (WMD) attacks. [p. 70]

Such forces would also be able to conduct operations to capture terrorists.

Intelligence

Boost the human intelligence capabilities that improve knowledge and understanding of foreign cultures and governments. [p. 43]

Apart from taking advantage of external sources of information like NGOs, the Defense Department needs to substantially improve its organic intelligence capabilities and better develop and integrate foreign area knowledge and understanding into deployed units. Intelligence capabilities for SSCs need to focus as much on understanding the society and politics of an area as on targeting hostile weapons. [pp. 66-7]

The United States is already the world leader in collection and communication of raw data and information. The area that needs attention is moving from data to "knowledge" and then to "understanding." [p.106]

National Missile Defense

As with SSCs, that there will be future terrorism attempts on U.S. soil is agreed by many observers, but when and exactly where are unpredictable. The assumption, endorsed by virtually every recent special commission or blue-ribbon panel, is that within the first quarter of the 21st century the American homeland will suffer a significant deliberate attack involving biological, chemical, nuclear, or radiological sources. Such a prediction moves fourth-generation warfare into the first rank of threats and elevates "homeland defense" to a national priority. . . .

However likely or unlikely a terrorist attack, it is not clear that the military component of national security is well equipped to do much about it. National missile defense is the foremost military option, but it has never been satisfactorily explained why an opponent would choose the expensive, technically difficult, and suicidal method of delivering a weapon of mass destruction via missile rather than via truck, boat, or plane. Some scenarios in which it would be useful to have a working missile defense can always be described, but the program becomes a matter of priorities. The strategy proposed here puts other military needs — not least of which is fully funding personnel, training, and spare parts to ensure that today's forces are fully ready — at a higher priority than a missile defense system of high cost, of unknowable reliability in actual use, and that will likely be politically costly in relations with allies and with Russia and China. [p. 69]

Increased and Improved Collaboration and Integration with Allies and Partners

The proposed strategy calls for a major new effort to boost ability and willingness to conduct military operations multinationally. This rests on an assumption that the conditions exist for allies and friends to increase their military capabilities and activities, and that an ambitious initiative to create a new mindset of collaboration could lead to realization of that potential.

A pivotal component of the strategy proposed here is to join more with partners and allies in concerted military, political, and economic action. For this to happen in the military sphere, allies will have to improve their military capabilities and be more politically ready to intervene than they were in the second half of the 20th century. (And the United States will have to alter its equipment and doctrine to allow for greater interoperability with allies.) [p. 44]

Integrate with allies and partners to collectively engage with areas of conflict, head off conflict if possible, and jointly intervene if not. Work with them to transform their militaries and to improve joint, multinational capabilities. [p. 41]

"Multinational Jointness." In addition to providing improved understanding of foreign conflict situations, there is substantial untapped potential for improved collaboration with allied or friendly forces in SSC operations. Operating more equally with foreign forces not only can reduce foreign resentment of the United States as a sole global policeman, but also could improve popular support for such operations domestically. The public is likely to look more favorably on operations with other countries where the United States is not bearing almost all of the burden (of cost, casualties, and responsibility).

The Defense Department has worked hard to make the services "joint," in terms of common — or at least compatible — communications, headquarters, equipment, and doctrine. A parallel opportunity may exist for integration of allied forces in SSCs along the lines of what the Defense Department has done for the U.S. services — expanding the concept of "jointness" to include foreign military services. If U.S. and a broad range of other nations' forces train units to be integrated into multinational command structures, a force package with a variety of types of units and nationalities could be assembled quickly for specific operations. Clearly, for this to work, much would need to be done in training, doctrine, and equipping to make allied forces more "interoperable" with U.S. forces. Decades of experience in NATO with this issue should provide a solid base to develop improved joint capability in the age of sophisticated electronics. [pp. 66-7]

Improved Collaboration and Integration with NGOs, Other Government Agencies, and International Organizations

"Civilian Jointness." The definition of "Joint and Combined Forces" may also usefully be broadened to include civilian non-governmental organizations (NGOs), such as relief agencies, and non-military Other Government Agencies (OGAs), including international organizations. These groups often have been operating in an area before intervention forces arrive, and can provide essential understanding of the situation and culture where they are located. U.S. forces have cooperated with such organizations during interventions, but these ad hoc efforts could be substantially improved with development and institutionalization of structures and procedures for cooperation and joint tasking beforehand. While experience has shown that personnel in the field will quickly establish informal structures and methods for coordinating and communicating with non-military actors, relying on this combination of luck and personal history and experience is very risky. Planners should determine definitions of relevant "mission essential tasks," which NGOs/OGAs are best organized to perform them, and how best to allocate them among the non-military actors. [p. 67]

Improved Collaboration and Integration with Civilian Agencies on Transnational Issues

Transnational problems such as international drug trafficking, illegal migration, crime, environmental conflict or damage, access to water, and health are often tied together in conflict zones. For example, drugs, crime, the environment, and economic issues are deeply intertwined in the conflict in Colombia. If U.S. forces are present in such conflict zones, it is likely they will be exposed to these issues and may have to deal with them. The approach suggested here is that procedures be improved for military units to collaborate more with the civilian agencies that focus on these issues. Current ad hoc arrangements can be made more

effective if a high-level effort is undertaken to assess how military, non-military, international (and non-government) organizations can best work together to address these complex issues. [p. 75-6]

Adjusting Forward Deployment and Increasing Military Engagement and Mobility

- *Make U.S. forces more "expeditionary." Adust forward deployment by reducing Cold War heavy, permanently-deployed forces and increasing short-term deployments, exercises, training, military-to-military contacts, and engagement with foreign militaries. [pp. 42-3]*

This paper takes the view that short-term, rotational deployments, plus increased military-to-military contacts and training can serve many of the same goals as large permanent forces in an extensive base infrastructure, and that irregular, as opposed to rote, exercises can establish effective military-to-military relationships. It holds that a more flexible and agile form of forward deployment can reduce the political and other costs of the old version.

Precipitous withdrawal is neither called for nor being called for by allies — yet. Any contemplated reductions should be coordinated with allies before actions are initiated, and usually phased withdrawals — unless other demands are made by host nations — should be the rule. Bringing selected forces back to the United States, coupled with regular combined force exercises and aperiodic deployments of military units, will allow the United States to more centrally position forces to respond to emerging contingencies without being seen as isolationist. [p. 51]