

**AD-A279 585**



NAVAL WAR COLLEGE  
Newport, R.I.

**NETWAR:  
THE OTHER SIDE OF INFORMATION WARFARE**

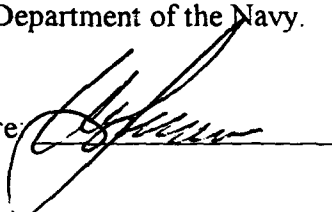
by

William M. Luoma  
LCDR USN

**DTIC  
ELECTE  
MAY 23 1994  
S F D**

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The Contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature 

This document has been approved  
for public release and sale; its  
distribution is unlimited.

8 February 1994

Paper directed by  
H. W. Clark, Jr.  
Chairman, Department of Joint Military  
Operations

**94-15266**



94 5 20 064

## REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION <b>UNCLASSIFIED</b>			1b. RESTRICTIVE MARKINGS		
2a. SECURITY CLASSIFICATION AUTHORITY			3. DISTRIBUTION AVAILABILITY OF REPORT DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.		
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE					
4. PERFORMING ORGANIZATION REPORT NUMBER(S)			5. MONITORING ORGANIZATION REPORT NUMBER(S)		
6a. NAME OF PERFORMING ORGANIZATION OPERATIONS DEPARTMENT		6b. OFFICE SYMBOL (If applicable) C		7a. NAME OF MONITORING ORGANIZATION	
6c. ADDRESS (City, State, and ZIP Code) NAVAL WAR COLLEGE NEWPORT, R.I. 02841			7b. ADDRESS (City, State, and ZIP Code)		
8a. NAME OF FUNDING/SPONSORING ORGANIZATION		8b. OFFICE SYMBOL (If applicable)		9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER	
8c. ADDRESS (City, State, and ZIP Code)		10. SOURCE OF FUNDING NUMBERS			
		PROGRAM ELEMENT NO.		PROJECT NO.	TASK NO.
				WORK UNIT ACCESSION NO.	
11. TITLE (Include Security Classification)  NETWAR: THE OTHER SIDE OF INFORMATION WARFARE" (U)					
12. PERSONAL AUTHOR(S) LCDR WILLIAM M. LUOMA, USN					
13a. TYPE OF REPORT FINAL		13b. TIME COVERED FROM TO		14. DATE OF REPORT (Year, Month, Day) 8 FEB 94	
				15. PAGE COUNT 40	
16. SUPPLEMENTARY NOTATION A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.					
17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)		
FIELD	GROUP	SUB-GROUP	INFORMATION WARFARE, COMMAND & CONTROL WARFARE; JSCP; C2W; FLEXIBLE DETERRENT OPTION; FDD; STRATEGY; CONCEPT; PRINCIPLE, LIC; OPERATIONS OTHER THAN WAR		
19. ABSTRACT (Continue on reverse if necessary and identify by block number) THE JCS' RECOGNITION OF INFORMATION WARFARE AS AN IMPORTANT AREA OF CONCERN HAS RESULTED IN THE PROMULGATION OF POLICY FOR DEVELOPMENT OF THE COMMAND AND CONTROL WARFARE (C2W) CONCEPT. HOWEVER, WHILE INTENDED TO BE EMPLOYED ACROSS THE SPECTRUM OF CONFLICT, C2W IS ORIENTED MORE TOWARD MILITARY OBJECTIVES AND LACKS 'COMPLETENESS' AS A STRATEGY WHEN VIEWED AGAINST THE PLETHORA OF FUTURE NATIONAL SECURITY THREATS. IN MANY OF THESE INSTANCES, USE OF MILITARY FORCE MAY NOT ALWAYS BE AN EFFECTIVE OR CREDIBLE EXPRESSION OF NATIONAL POWER FOR THE THEATER CINC WHEN EXECUTING HIS JOINT STRATEGIC CAPABILITIES PLAN RESPONSIBILITIES. THE NETWORK OR "NETWAR" CONCEPT COMPLEMENTS C2Q AS AN INFORMATION WARFARE STRATEGY WHICH CAN PROVIDE A VEHICLE FOR ACTION IN SCENARIOS WHERE APPLICATION OF MILITARY FORCE IS NOT APPROPRIATE AND/OR DURING OPERATIONS OTHER THAN WAR. TO BE EFFECTIVE, THE NETWAR STRATEGY REQUIRES COORDINATION OF ALL ELEMENTS OF NATIONAL POWER TO COUNTER AND NEUTRALIZE THE POWER OF NETWORK ADVERSARIES. APPLICATION OF NETWAR IN SUPPORT OF NON-MILITARY FLEXIBLE DETERRENT OPTIONS PROVIDES A FRAMEWORK FOR ANALYSIS.					
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT <input checked="" type="checkbox"/> UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS RPT <input type="checkbox"/> DTIC USERS			21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED		
22a. NAME OF RESPONSIBLE INDIVIDUAL CHAIRMAN, OPERATIONS DEPARTMENT			22b. TELEPHONE (Include Area Code) 841-3414		22c. OFFICE SYMBOL C

**Abstract of**  
**NETWAR: THE OTHER SIDE OF INFORMATION WARFARE**

The JCS' recognition of Information Warfare as an important area of concern has resulted in the promulgation of policy for development of the Command and Control Warfare (C2W) concept. However, while intended to be employed across the spectrum of conflict, C2W is oriented more toward military objectives and lacks "completeness" as a strategy when viewed against the plethora of future national security threats. In many of these instances, use of military force may not always be an effective or credible expression of national power for the theater CINC when executing his Joint Strategic Capabilities Plan responsibilities. The network or "Netwar" concept complements C2W as an Information Warfare strategy which can provide a vehicle for action in scenarios where application of military force is not appropriate and/or during operations other than war. To be effective, the Netwar strategy requires coordination of all elements of national power to counter and neutralize the power of network adversaries. Application of Netwar in support of non-military Flexible Deterrent Options provides a framework for analysis.

Accession For	
NTIS	CRA&I <input checked="" type="checkbox"/>
DTIC	TAB <input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution /	
Availability Codes	
Dist	Avail and/or Special
A-1	

## PREFACE

My purposes for writing this paper are threefold. As a Desert Storm participant, I contributed to the technological military success enjoyed by the U.N. Multinational forces and shared in the general euphoria that followed war's end, only to become disillusioned by the subsequent paralysis of U.S. foreign policy and failure of U.N. initiatives in Haiti, Bosnia, Somalia, and North Korea. It became apparent to me that there was more factors involved in the control of power than the simple application of military force. Secondly, I was interested in the emergence of Command and Control Warfare (C2W) as an Information Warfare strategy. Although C2W is meant to be applied across the spectrum of conflict, it seemed to me to lack "completeness" as a strategy when viewed against the potential national security problems of tomorrow, where there may not always be a military option. Lastly, I have long been an aficionado of science fiction and the work and vision of the "Futurists," those on the "cutting edge" of thought. As a personal computer owner and network subscriber, I am an active participant in the Third Wave and the information technology revolution. And these trends are not new; RAND analysts were working with the original cyberwar and netwar concepts as far back as 1978. It is only now in the post-Cold War era that they are receiving widespread consideration. Intrigued by the network concept and excited by the possibilities offered by C2W, I felt here lay a possible explanation for the ineffectiveness of our foreign policy and the missing piece needed to complete the Information Warfare strategy. The new JSCP provided a timely venue to examine Netwar and its applications as a strategy for Flexible Deterrent Options.

## TABLE OF CONTENTS

CHAPTER	PAGE
ABSTRACT .....	ii
PREFACE .....	iii
LIST OF TABLES .....	v
I        INTRODUCTION .....	1
The Case for Netwar .....	1
The Challenge .....	2
Basis for a New Strategy .....	3
II        THE NETWORKED WORLD .....	4
Change .....	4
Evolution of War .....	5
Impact of Technology .....	6
The Third Wave .....	7
Information as Power .....	7
War in Cyberspace .....	8
III       NETWAR .....	10
What is Netwar .....	10
War at the Speed of Thought .....	10
Cybernetic Networks .....	11
Principles of Netwar .....	12
Netwarriors .....	12
Netwarfighting Strategy .....	13
IV        CYBERWAR STRATEGY .....	15
New JSCP Direction .....	15
Role of the Theater CINCs .....	16
FDO Analysis .....	17
V        CONCLUSIONS .....	21
APPENDIX I -- FLEXIBLE DETERRENT OPTIONS .....	22
NOTES .....	28
BIBLIOGRAPHY .....	32

## LIST OF TABLES

TABLE		PAGE
I.	DIPLOMATIC FLEXIBLE DETERRENT OPTIONS (EXAMPLES) .....	23
II.	POLITICAL FLEXIBLE DETERRENT OPTIONS (EXAMPLES) .....	24
III.	ECONOMIC FLEXIBLE DETERRENT OPTIONS (EXAMPLES) .....	25
IV.	MILITARY FLEXIBLE DETERRENT OPTIONS (EXAMPLES) .....	26

# **NETWAR: THE OTHER SIDE OF INFORMATION WARFARE**

## **CHAPTER I**

### **INTRODUCTION**

**The Case for Netwar.** The Cold War hangover, the overwhelming combat success demonstrated in Desert Storm, and the explosive impact of the information technology revolution are all combining to present daunting new security challenges for a U.S. military preparing to enter the 21st Century. Traditional elements of global order are decaying and dramatic change is at hand. Formal power structures are devolving from social hierarchies linked by diplomatic convention into mutative cybernetic networks linked informally via electronic protocol. As information and knowledge replace capital and labor as the sources of wealth in post-industrial society, a new elite, the "cyberocracy"<sup>1</sup> is arising. Competition and conflict among these new information "haves" and also with "have-nots" will occur and the electronic infosphere -- "cyberspace" -- will become a new theater of operations. These growing phenomena are usually thought of and discussed in terms of "Third Wave" or "Information Warfare." However, they require clearer definition.

RAND analysts first coined the term "Cyberwar" to refer to "the conducting, and preparing to conduct, military operations according to information related principles."<sup>2</sup> This is close to the current definition for Command and Control Warfare (C2W), which is defined by JCS as "the integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions."<sup>3</sup>

However, there was another element to Cyberwar, that of network warfare or "Netwar", which C2W as it was developed did not address. For the purposes of this paper, the word "Netwar" has been adopted as an all-encompassing term for competition and conflict involving networks, and also to differentiate it from C2W. While both C2W and Netwar are Information Warfare concepts, their approaches and potential applications are different. While purporting to apply "across the operational spectrum and all levels of conflict,"<sup>4</sup> C2W almost exclusively addresses military objectives and is an offensive-minded policy geared to the application of information warfare techniques to conventional military operations on the higher-intensity side of the conflict spectrum.

In the networked world, the potential enemy is not so clearly defined. Netwar is a less-structured strategy more suitable for low-intensity conflict, or what is now being called "operations other than war." The Netwar strategy requires the coordination of all elements of national power -- diplomatic, economic and military, to counter the power of network entities and the weaknesses of networked enemies. As such, Netwar complements C2W as the other side of Information Warfare.

**The Challenge.** Conventional military forces, based on an inherent hierarchical structure, may not be an effective tool to fight an amorphous networked adversary. Under these circumstances, the traditional role of military force as a keystone in the application of national power may be neither desirable, effective nor *possible* in many scenarios. If the U.S. is to maintain its preeminent position of leadership in economic and military affairs in the post-industrial world *AND* minimize the risks inherent in an overall force draw down, then a new approach to C2W to fight the low intensity Netwar.



**Basis for a New Strategy.** The Joint Chiefs of Staff (JCS) has responded to the post-Cold War requirement for a new approach to national security strategy. This is reflected in the most recent Joint Strategic Capabilities Plan (JSCP) in the form of the Flexible Deterrent Option (FDO) concept. Although general in nature, FDO examples listed in the current JSCP encompass a wide range of options for conventional and non-conventional uses of all four elements of national power in operations other than war. Theater CINCs are charged with executing the JSCP, including the planning of theater-unique, regionally-based FDOs for employment by the National Command Authority (NCA). Accordingly, FDOs will be analyzed for suitability as the basis for the development of a "Netwarfighting" strategy for the theater CINCs.

## CHAPTER II

### THE NETWORKED WORLD

"May you live in interesting times."

Ancient Chinese curse

"Desert Storm was the end of an era and not the beginning..."

Unidentified defense analyst<sup>1</sup>

**Change.** In the last decade of the Twentieth Century, this word has come to signify uncertainty and even fear of an unknown future. This is especially true for the U.S. military in the post-Cold War era, where declining budgets, personnel reductions and a seeming lack of direction in U.S. foreign policy all lend to a general sense of unease. When confronting the Soviet threat, there was a clear cut objective which drove nearly all investment decisions, systems/technology development, and strategy and policy formulations. With the Soviet's demise and the change in emphasis from East-West confrontation to a more regional focus, radically new security challenges are not just on the horizon, but here now. This is no longer a beginning or end phase for the highly touted "New World Order," but a time of transition marked by turmoil and shaped by technology.

For global strategists and policy makers, the analytical focus has been on the possible "end state" of the world in the next 30 years and what new security problems, influenced by technology, will arise. War gamers often postulate three alternatives for the next 30 years' time frame -- a "good world" marked by peace and prosperity; a "bad world" of trade wars, nationalism, and ethnic conflict; and, an "ugly world" of despotism, genocide, and terrorism.<sup>2</sup>

Admiral Jeremiah, the Deputy Chairman of the Joint Chiefs of Staff, attempted to categorize the nature of the potential future threats to U.S. security as follows:

"...I think we are going to see a general worsening of the international conditions over the next 20 or 30 years . . . For instance, the world population will approach 10 billion people -- nearly double the current population -- by 2025. Most of that increase will come in lesser-developed countries. We expect to see fierce competition for scarce natural resources, including such things as petroleum, unpolluted water and perhaps even fresh air.

Without an international effort to control worsening social, economic and demographic conditions, by 2025 perhaps one quarter of Earth's population will be malnourished. Many governments will be chronically unable to meet their citizen's most basic needs, and the overall picture will be one of chaos in the developing world - - a picture much like what we see in Somalia today, but on a global scale.

Great potential exists for huge migrations as people flee conflict or search for better economic conditions . . . Stir into this witches' brew the proliferation of modern weapons -- including ballistic missiles and weapons of mass destruction -- and the result is a real nightmare. Trends such as these have serious implications both for international stability and America's future security."<sup>3</sup>

**Evolution of War.** Since men first began using sticks and stones for weapons, ways and means of waging war has continually evolved. Since the 16th century, the tools of war have become more technologically sophisticated and destructive until now their use is highly conditional. Deterred by nuclear force and bound by international conventions, modern military powers have become limited in their ability to engage in warfare on their own terms. Since the end of World War II, the trend has been toward low intensity, guerrilla, wars of national liberation. These were not fought between states, but between states and organizations with no readily identifiable territory, uniforms, targetable bases or command structures, but with strong communications links (*i.e.*, networks). Conflict often took place in terrain which did not favor the maneuvering of heavy, conventional forces and which served to limit the scope of any engagements. Ambush and hit and run tactics were preferred. While these conflicts mainly involved the old colonial powers fighting to keep their territorial

possessions, Vietnam and Afghanistan stand out as examples where colonial interests were not involved and the results were the same: in every case the outcome for conventional forces was a failure. Based on these trends, the outlook for, regular state-owned forces and large-scale technology and weaponry appears bleak.<sup>4</sup> The future will be based on the smart use of smart technology.

**Impact of Technology.** U.S. and coalition military capabilities displayed in the Gulf War were the manifestation of a technical military revolution of historic proportions. This revolution is said to involve three integrated developments: advances in military technology, advances in operational concepts, and new organizational techniques that take advantage of such advances. If the U.S. is leading the way in revolutionizing warfare, then it is equally true that most advances to date have occurred in the first area: military technology. As new operational concepts are developed, U.S. forces can become more lethal, smaller, more strategically flexible, better organized for conventional conflict and situations short of combat.<sup>5</sup>

One of the critical challenges will be to devise superior national defense and military operational and strategic concepts to compensate for universal access to technology.<sup>6</sup> C2W is an example of a new operational concept; FDOs are examples of new strategic concepts. These new concepts and the right force structure must be employed effectively in what is becoming a more complex and dangerous security environment.

Technology is having a similar "revolutionary" effect on the civilian world, both politically and economically, for several reasons. First, given the reduced threat in the post Cold War period, there will be great pressure to spend less and reap the rewards offered by the "peace dividend." Secondly, there is no other superpower on the horizon to challenge the U.S.. The Cold War left us a legacy of weapons technology which cannot be "disinvented,"

most notably nuclear weapons, and the problem of non-proliferation.<sup>7</sup> The media has created a "circus atmosphere" around any deployment or use of military forces. All these issues must be factored into the equation as to their influence on world power and whether the decision to use conventional force remains a viable option.

**The Third Wave.** Futurists such as Alvin and Heidi Toffler have attempted to "write the script" for the world of the future, as they perceive its development, through the use of macro-trend analysis. Their thinking is that the most basic components of the current global system are breaking down and the world is shifting from a global system based on nations to a three-tier system based on states. In the Tofflers' view, the first tier will be low technology agrarian countries seeking the bare essentials for survival and torn apart by local warlords (e.g., Somalia today). Second tier countries will have stronger internal power structures but will remain reliant on mass industrial production economies and relatively unsophisticated technology. The third tier, or "Third Wave" as it is also called, will be high technology societies based on information and knowledge and selling those services to the second tier, who will be busy exploiting the first tier. Vying for power along with the Third Wave countries will also be global networks of transnational corporations, religious extremists and other ethnic/socioeconomic groups, some regionally based and most, if not all electronically connected.<sup>8</sup> In the world of the Third Wave, networks will increasingly replace hierarchies as power structures.

**Information as Power.** New information and communications technologies are rapidly spreading worldwide. As the U.S. leads the rest of the world in the development of Third Wave, or "post-industrial" society, knowledge and information have become the strategic and transforming resources of this new society, just as capital and labor were the key

drivers of industrial society.<sup>9</sup> Agriculture is expected to yield to the information industry as the major employer in the developed world.<sup>10</sup> The shift to information and its control as the dominant source of power is seen as a natural step in man's political evolution. In the past, under aristocracy, the high-born ruled; under theocracy, the high priests ruled. In modern times, democracy and bureaucracy have enabled new kinds of people to participate in governing. The term, "cyberocracy" has been coined by RAND analysts to describe this phenomena of post-industrial, Third Wave society.<sup>11</sup> The extension of high-powered computer and telecommunications technology to the living room and the ability to network with almost anyone, anywhere will radically affect who rules, how and why. It may also affect the organization of governments and societies, the meaning of authority and democracy, nature of bureaucracies, behavior of elites and definition of progress.<sup>12</sup> As more and more people interact via electronic networks in what is termed "cyberspace,"<sup>13</sup> their thinking about "the system" and the world in which they live will invariably change. Knowledge and control of information, as the sources of wealth, will become the new "centers of gravity" for post-industrial society. However, along with the great promise of technology, there is also a dark side.

**War in Cyberspace.** Even in the "good world" scenario, not everyone will live in post-industrial society; certain regions will continue to lag behind the rest in various states of underdevelopment and chaos. There will be information "haves" and "have-nots". Competition for access to information as a commodity will increase. The ability of a nation to control information and manipulate it to meet its ends will be a large measure of success, power, and prestige, not only material wealth. Some political actors will become global information powers, but others (*i.e.*, the Third World) will fear "electronic colonization" and "informational imperialism."<sup>14</sup> Information flows through the spread of new technology and

networks will undermine traditional concepts of territorial sovereignty. Information in electronic form is difficult to control; data networks, financial data flows, electronic mail, TV and news broadcasts do not stop at national borders. Thus, recognition is spreading in governments around the world that the information technology revolution may profoundly alter the nature of political power, sovereignty and governance.<sup>15</sup> Where there is power, there is also conflict. As mankind increases human interaction via electronic means, war will migrate to the networks. Netwar will be fought in cyberspace.

## CHAPTER III

### NETWAR

"Peace, in and of itself, is not necessarily a proper objective."

RADM J. C. Wylie<sup>1</sup>

"If one could always be acquainted beforehand with the enemy's designs, one would always beat him with an inferior force."

Frederick the Great<sup>2</sup>

**What is Netwar?** Netwar is a key aspect of the informational conflict between nations and societies. This war about knowledge seeks to disrupt, deceive, deny how a target knows or thinks about itself and how it relates to the rest of the world. It can involve public opinion, propaganda, diplomacy, political and cultural subversion, promotion of opposition or dissident movements, terrorism, religious extremism, nuclear proliferation, economic sanctions, predatory trading practices and theft of electronic goods, services and technology.<sup>3</sup> Netwar allows the CINC to wage Information Warfare across the low intensity conflict spectrum. Much of this activity will take place in the electronic networks, in cyberspace. While computers are the primary weapons and networks the battleground, humans remain the ultimate targets of Netwar.

**War at the Speed of Thought.** In modern war, information is as important as firepower.<sup>4</sup> Parallel processors, fiber optic cables, high capacity satellite communications, cellular networks; these are the means both the military and civilian worlds employ to process and exchange information. Computers can process an inconceivable amount of information every second. It is believed that the only limitation to the capability of computers to support



warfare or any other endeavor is the human decision-making element: "the speed of thought."<sup>5</sup> Is this necessarily true?

The average single-path processing military computer system has a few million transistors and a like amount of memory on a chip which allows it to perform approximately 300 million computations per second. When compared to biological systems, this performance level falls somewhere equidistant between a worm and a bee. Even if computer capacity doubles every two years for the next 20 years, computers will just approach the bee's level of sophistication. In 40 years, computers will have a million times today's capacity, about one trillion connections ( $10^{12}$ ). In comparison, humans have about  $10^{11}$  neurons, each which has about  $10^4$  interconnections. This gives the human brain a complexity of  $10^{15}$ , about 1,000 trillion connections. Parallel processors may have the potential to one day overtake man in the amount of connections but in relative terms, man will remain the dominant element in high technology decision making.<sup>6</sup> His control and communications networks will be critical centers of gravity.

**Cybernetic Networks.** Webster's defines cybernetics as "the science of communication and control theory that is concerned especially with the comparative study of the automatic control systems." If one were to view a potential adversary as a biological organism, then his command and control (C2) systems would be analogous to his central nervous system. Most C2 systems, however, are constructed on a hierarchical design, with identifiable pathways and critical nodes. While they are networks, *per se*, they lack the multiple paths and redundancy of cellular network structures, in which the information exchange processes work in parallel. When control and decision making functions are integrated within a cellular network, then that network becomes cybernetic, combining the

speed of a machine with the complexity and ingenuity of a human. While invaluable to both the military and civilian worlds, it can also be dangerous.

**Principles of Netwar.** Netwar, as an Information Warfare strategy, is meant to promote the coordination of all elements of national power -- diplomatic, political, economic and military -- to achieve deterrence by identifying, analyzing and countering the activities of networked adversaries (other states) and network entities (*e.g.*, insurgencies, terrorism, ethnic factions, religious extremism, trade cartels). Many of the latter are organized like networks, even though their leadership may have a hierarchical structure. As it is related to low intensity conflict or "operations other than war," Netwar, then, can share many of the same principles: objective, unity of effort, security, restraint, perseverance, and legitimacy.<sup>7</sup>

The objective(s), as stated above, are the networks, both electronic and within the potential enemy's organizational structure. Unity of effort requires coordination by national agencies and theater combatant commanders to integrate activities into theater or country specific plans in order to achieve regional or national objectives.<sup>8</sup> Security, as in C2W, requires protection of own network(s) integrity and vulnerability. Restraint, in this instance, means the calculated use of Netwar techniques, forces, or weapons to counter an enemy's activity and possibly to deny him knowledge that he is being manipulated. Perseverance implies a long term test of wills and patience in monitoring network activities and growth. Legitimacy, the weakest of the principles in this context, may require review of existing international and bilateral treaties, as well as exploration of new legal agreements and interpretations of existing domestic laws (*e.g.*, review of intelligence oversight restrictions). The Netwar environment will be intrusive.

**Netwarriors.** Like any good government sponsored and funded program, Netwar will require a coordinating group and Command, Control, Communications, Computers, and Intelligence (C4I) systems support. Execution of the Netwar program will require a coordinated effort between many players at the strategic and theater levels.

Key to the Netwar effort will be intelligence -- information and knowledge about potential adversaries.<sup>9</sup> For the theater CINC, his Joint Intelligence Center (JIC), uniquely positioned between the strategic and tactical levels, will be the prime supporter of Netwar planning functions.<sup>10</sup> The theater JIC and national level agencies within the Intelligence Community (*e.g.*, State Department, Commerce Department, Department of Energy, Central Intelligence Agency, Defense Intelligence Agency, National Security Agency, and Federal Bureau of Investigation). They must be attuned to dynamic world changes, the shift in power/centers of gravity/conflict toward knowledge and information, the exploitation of technology and information networks, and the vulnerabilities of not only potential adversaries, but also own forces. These requirements place a premium on interagency cooperation and underscore the growing importance of both political and economic intelligence. An interagency approach is crucial to the coordination of the Netwar strategy at the strategic and operational levels.

Means to access and monitor government, commercial and international computer databases, networks, fiber optic switches, and cellular communications must be developed. Computer technologists must exploit artificial intelligence to develop expert systems using virtual reality to simulate adversary systems' network connections and processes. By establishing *a priori* models of network systems and using enabling, or introspective information, critical nodes can be determined and alternative "netwarfighting" strategies can be tested to assess their effectiveness over time.<sup>11</sup> One of the most potent means to enter a network structure is through the communications cycle. Thus, networks are extremely

vulnerable to electronic disruption, random data manipulation and computer viruses,<sup>12</sup> all of which are aspects of C2W. The technology, piggybacking on current C2W programs, exists today. All that is required is a shift of emphasis and a framework for strategy execution.

**Netwarfighting Strategy.** The 1986 Goldwater-Nichols Defense Reorganization Act greatly increased the authority and responsibility of the theater CINC's. This expanded concept has served U.S. interests well, as was most evident in the Gulf War. However, given the paradox of declining forces/assets and an expanded mission, how can the CINC effectively execute his mission? The best alternative is to develop theater warfighting strategies designed to exploit technology for its force multiplying effect both to the benefit of U.S. interests and to the detriment of potential adversaries. The theater CINC remains key to the execution of U.S. national security strategy in his theater, only he can articulate the theater perspective with a keen appreciation for allies strengths and weaknesses. An increasingly perilous, networked world will demand new and more creative strategy options for force employment. As was demonstrated in Vietnam and Afghanistan, and as is the case in Somalia and Bosnia, an enemy with a network structure can defeat a modern, hierarchical institution. Network tactics will be required to counter and defeat network foes. CINC's must plan to fight the Netwar.

## CHAPTER IV

### NETWAR STRATEGY

"To discover how much of our resources must be mobilized for war, we must first examine our own political aim and that of the enemy. We must gauge the strength and situation of the opposing state. We must gauge the character and abilities of its government and people and do the same in regard to our own. Finally, we must evaluate the political sympathies of other states and the effect the war may have on them. To assess these things in all their ramifications and diversity is plainly a colossal task. Rapid and correct appraisal of them clearly calls for the intuition of a genius; to master this complex mass by sheer methodological examination is obviously impossible. Bonaparte was quite right when he said that Newton himself would quail before the algebraic problems it could pose."

Clausewitz <sup>1</sup>

**New JSCP Direction.** JCS defines theater strategy as "the art and science of developing integrated strategic concepts and courses of action directed toward securing the objectives of national and alliance or coalition security policy and strategy by the use of force, threatened use of force, or operations not involving the use of force within a theater."<sup>2</sup> The current Joint Strategic Capabilities Plan (JSCP) reflects new thinking with regards to national strategy - employment of military forces as a element of national power is separated into two categories. For the purposes of this discussion, they will be referred to as conventional and non-conventional. Conventional use of military power is reflected in the CINCs' requirements to plan for Lesser and Major Regional Contingencies (LRC/MRC). This construct is relatively straightforward, the enemy is a known quantity, his power can be measured and means to defeat him within the constraints of US military assets can be delineated via a scientific, formulated method (*i.e.*, OPLAN or CONPLAN). His force is embodied in a hierarchical structure which can be countered via conventional means. On the other hand,

non-conventional or even *non-use* use of military force reflected in Flexible Deterrent Options (FDO) provides more of a creative challenge to both practitioners of the operational art and strategic power brokers. FDOs are deterrent measures geared to support operations other than war.

For many national security challenges of the future, there may not necessarily be a central controlling entity or identifiable hierarchy. In the networked world, information [sic] power can flow from one place to another by a multiplicity of routes, control is decentralized and can be rerouted dynamically. Decisions can be made anywhere in the network.<sup>3</sup> Complete disruption of a network's component structure may not always be possible given the amount of assets required. Short of total annihilation, the network, a cybernetic organism, cannot be destroyed. The Netwar strategy must employ a more subtle understanding of a network system's structure and interactions in order to counter its purpose and effects or to neutralize it. Within the JSCP framework, FDOs offer this opportunity to the theater CINC.

For effective coordination of FDOs at the strategic and operational levels, an interagency approach (much like the Netwar strategy) is required in the compiling, evaluating, and approval of FDOs during adaptive planning or in crisis situations. FDOs require credibility, multiple sub options and compliance with international law. Extensive regional knowledge, appreciation for allies, and firm idea of the desired end state are vital; only the theater CINC can supply these.<sup>4</sup>

**Role of the Theater CINC.** FDOs provide the NCA a broad range of options to use national power to deter or forestall the onset of a crisis. FDOs seek to pre-empt, defuse or deter a potential threat to U.S. interests, but do not put U.S. forces in jeopardy if deterrence fails.<sup>5</sup> FDOs are used to control or deter escalation and bring a crisis situation to a conclusion favorable to U.S. interests. Theater CINCs are required to plan requests for *appropriate*<sup>6</sup>

diplomatic, political and economic options that would be used in concert with (preceding, concurrent, or subsequent to) military FDO actions.<sup>7</sup> However, non-military FDOs could be used by themselves when application of military power is *not appropriate* or the risk to U.S. forces is too high. While the decision to exercise a theater FDO in this scenario rests at the strategic level, the responsibility for its execution and success ultimately rests with the CINC, *he is the one who has to live there*.

To be truly *appropriate*, FDOs must be theater-unique and, therefore, developed by the theater CINC to match the dynamics of power in his theater. In a world of networks, it is vitally important that FDOs be applied to the correct pressure points of an adversary. It may be desirable that the potential adversary *does not even know that the FDO is being applied*. Or if he is aware of its presence, then it is applied in such a manner as to give him no option but to acquiesce to U.S. interests (*e.g.*, like a choke hold in wrestling). C2W does this in conventional conflict, Netwar can do the same in non-military FDOs.

As the world becomes increasingly interconnected, the CINC must use Netwar principles to concentrate FDO planning *more and more* on national and theater networks, both electronic and cultural, if the use of non-military FDOs is to remain a viable option for his theater strategy. Otherwise, the initiative in this area will pass to the strategic level, and the CINC may find himself an agent of policy execution, and not interlocutor. Conceivably, the CINC's role could diminish to the level of being responsible for theater military affairs, only, with all diplomatic, political and economic power and decision making exercised at the strategic level.

**FDO Analysis.** Effectively articulating FDOs and orchestrating their employment are monumental tasks. The number of options and variations increase exponentially when one considers all the CINCs, their particular theaters, and our existing network of alliances and

coalition ties. The magnitude of this undertaking alluded to by the quote from Clausewitz at the beginning of this chapter will require a collaborative effort at the strategic and operational levels. Examples of FDOs, drawn from the current JSCP, are listed in Tables I-IV (lists are not all-inclusive or in priority order). For the purposes of this paper, all FDOs will be analyzed for common elements and non-military FDOs for unique areas appropriate for an overall Netwar strategic approach. Military FDOs are provided in Table IV in order to give the reader an appreciation of the wide variety of policy options available. Since they concern conventional force deployment and employment, they fall rightly under the C2W category of Information Warfare strategy vice Netwar. However, Netwar strategy can complement and enhance C2W in its employment, either supporting a military FDO or LRC/MRC.

Common to all FDOs (and to networks) is information, whether it be public affairs, propaganda, deception, psychological warfare, education, command and control. It is the common thread which runs through all four categories of options and can be viewed at the strategic, operational and tactical levels of conflict and operations other than war. Control of public opinion is critical to dominating events and can produce an astonishing "leverage" effect when managed adroitly. As a deception and propaganda tool, use of the international media's global coverage and sensationalist perspective must be a coordinated effort between the NCA, JCS and CINC, but be regarded as the CINC's tool.<sup>8</sup> However, the advent of the 500 channel, "information superhighway" will complicate this effort as more and more people will tend to tune into the channel or channels which reflect their views or relate to their tastes. Despite the "flip side" of having 500 channels of information to deal with, manipulation of the key "networks" via coordinated public affairs operations is the *sine qua non* for an effective Netwar strategy.

With regards to Diplomatic FDOs listed at Table I, potential adversaries, whether states or organizations, must be additionally analyzed according to membership in



international and regional organizations, alliances, ethnic constituencies and other cultural groups. These cross-boundary networks must be viewed as to how they support the overall power structure and where the critical nodes lie. Politically (Table II), internal networking must be discerned as to where and when to apply information or disinformation to manipulate the internal politics of an opponent to accomplish an FDO's desired goal. While Diplomatic and Political FDOs are important, it is in the Economic FDOs (Table III) where both hierarchical and network structures are potentially most vulnerable, and thus also where the greatest opportunities for Netwar lie. Economics drives the decisions and policy of both hierarchical and network power structures. Due to the vast amount of capital and number of electronic networks involved in the world's financial market, disruption for even a short period of time could have devastating effects for the system's weaker players. Freezing assets, zeroing accounts, sanctions, embargoes, influencing trade of goods and services (to include information) are all powerful tools to create leverage in any FDO, operations other than war, and LRC/MRC scenario (witness the cumulative effect of economic disruption on Iraq following the invasion of Kuwait). "Information is power and economic information is economic power."<sup>9</sup> Knowing the economic network connectivity and vulnerabilities of competitors and potential enemies is critical -- one can rest assured that they are trying to discern those of the U.S.,

In summary, an FDO must control public perceptions about its existence and purpose to be effective. It must be keyed to the adversary's networks and centers of gravity. An Economic FDO is likely to be more effective than one of the other categories if applied singularly, and even more so when combined with diplomatic/political initiatives. Military options, those of last resort, set the stage for broader, higher-intensity conflict and suggest that the enemy is more of a hierarchical power structure. The purpose of FDOs is deterrence and the avoidance of conflict in achieving U.S. national objectives, the overarching goal of

both the Netwar and the national security strategies. The defeat of Network enemies will require network tactics. The future may belong to he who can master the network form.<sup>10</sup>

## CHAPTER V

### CONCLUSIONS

Does Netwar warrant adoption as an Information Warfare strategy? Should it join C2W in the JCS lexicon? Although it could be argued that Netwar represents C2W by another name, that is not the case. While C2W is military objective oriented, Netwar seeks to apply Information Warfare through the coordination of the four elements of national power to respond to the network phenomena as a growing threat to national security. The Netwar strategy has its most merit when applied at the low intensity conflict or "operations other than war" end of the spectrum. Mostly portrayed in this paper in futuristic terms, Netwar is a relative concept today, and FDOs can provide the vehicle for its application. It would be more likely that Netwar would merge with C2W, an event which would mark the evolution of a complete Information Warfare strategy.

Until that time, however, it is useful to ponder on what lies ahead and the national security challenges which must be confronted. World demographic problems will not decrease, the post-industrial world will continue its technological development and monopoly on information and knowledge, the new centers of gravity. Networks will replace hierarchical states as the power wielders of the future. Competition and conflict will migrate to the networks. Hierarchical institutions may not be able to compete with networked adversaries, be they states or other entities. Military force, in a conventional sense, will lose its efficacy, and information may become the weapon of predators. Those not possessing the new means of wealth and power, information and knowledge, will struggle, often violently, to gain a serving of the information pie. Netwar, an Information Warfare Strategy to complement C2W, can act as a key force multiplier to the theater CINCs in executing their national security responsibilities today and tomorrow.

• • • •

APPENDIX I  
FLEXIBLE DETERRENT OPTIONS

**TABLE I**

**DIPLOMATIC FLEXIBLE DETERRENT OPTIONS  
(EXAMPLES)**

Alert and introduce Special Teams <ul style="list-style-type: none"><li>- Public diplomacy</li><li>- Mobile Training Team (MTT)</li><li>- Communications</li></ul>	Prepare to withdraw US Embassy personnel
Reduce international diplomatic ties	Reduce national embassy personnel
Increase Cultural Group Pressure	Win support of allies and friends
Initiate Non-combatant Evacuation Operations (NEO)	Pursue increased regional support
Promote democratic elections	Identify the national leader who may be able to solve the problem
Identify clearly the steps toward peaceful resolution of the crisis	Coordinate efforts to strengthen international support
Restrict activities of diplomats	Use the UN or other international venues
Alter existing meetings, programs, or schedules	Develop work with existing coalition, avoid unilateral action
Heighten informational efforts directed at: <ul style="list-style-type: none"><li>- The international community</li><li>- The people within the nation</li><li>- The opponent's allies</li><li>- The coalition</li></ul>	Show international resolve

Source: Department of Defense, Joint Strategic Capabilities Plan (JSCP)  
(Washington: U.S. Govt Print. Off., 1993), p. III-5.

**TABLE II**

**POLITICAL FLEXIBLE DETERRENT OPTIONS  
(EXAMPLES)**

Heighten public awareness of the problem and potential for conflict	Heighten informational efforts - Quickly - Honestly - Within security constraints
Gain popular support	Gain congressional support
Take measures to increase public support	Take steps to gain and maintain public confidence
Maintain open dialogue with the press	Keep selected issues as lead stories
Promote US policy objectives through public policy statements	

Source: Department of Defense, Joint Strategic Capabilities Plan (JSCP)  
(Washington: U.S. Govt Print. Off., 1993), p. III-5.

**TABLE III**

**ECONOMIC FLEXIBLE DETERRENT OPTIONS  
(EXAMPLES)**

Freeze monetary assets in the US	Encourage corporations to restrict transactions
Seize real property in the US	Reduce security assistance programs
Freeze international assets where possible	Enact trade sanctions
Cancel US-funded programs	Heighten information efforts aimed at: <ul style="list-style-type: none"><li>- financial institutions</li><li>- reducing or eliminating corporate transactions</li></ul>

Source: Department of Defense, Joint Strategic Capabilities Plan (JSCP)  
(Washington: U.S. Govt Print. Off., 1993), p. III-6.

TABLE IV

**MILITARY FLEXIBLE DETERRENT OPTIONS  
(EXAMPLES)**

Employ readily in-place assets	Move Maritime Prepositioning Squadron (MPS) to region
Upgrade alert status	Deploy surface action group (SAG) to region
Increase strategic reconnaissance	Deploy carrier battle group (CVBG) to region
Increase collection efforts	Begin moving forces to air and sea ports of embarkation
Initiate or increase show of force actions	Move Marine Expeditionary Brigade (MEB) to region
Employ electronic measures	Deploy forward-deployed amphibious ready group/Marine expeditionary unit (ARG/MEU) to region
Conduct aircraft flyovers	Activate procedures to initiate reserve callup
Increase exercise activities, schedules, and scope	Prestage or deploy contingency ready brigades
Increase military exchanges and staff visits to the area	Increase use of Special Operations Forces (SOF)
Increase naval port calls or air squadron deployments to the area	Prestage airlift
Increase Mobile Training Teams (MTT)	Prestage airlift support assets
Impose restrictions on military personnel retirements, separations, leaves and establish curfews	Prestage sealift and airlift reception assets to air and sea ports of embarkation
Institute provisions of host nation agreements	Emplace logistics infrastructure where possible
Open prepositioned stockage facilities	Open and secure sea and air lines of communication (LOCs)



TABLE IV (CONT'D)

Use naval and/or air capabilities to enforce sanctions	Increase informational efforts <ul style="list-style-type: none"><li>- PSYOP</li><li>- Measures directed at military forces of the opponent</li><li>- Mission awareness</li></ul>
Deploy tactical fighter squadrons	Move prepositioning ships into the region
Order contingency forces to initiate actions to deploy	Deploy AWACS to region

Source: Department of Defense, Joint Strategic Capabilities Plan (JSCP) (Washington: U.S. Govt Print. Off., 1993), p. III-6.

## NOTES

### Chapter I

1. David Ronfeldt, Cyberocracy, Cyberspace, and Cyberology: Political Effects of the Information Revolution, Santa Monica: RAND, 1991, p. 2.
2. John Arquilla and David Ronfeldt, Cyberwar is Coming!, Santa Monica, RAND, 1992, p. 6.
3. Joint Chiefs of Staff, Doctrine for Joint Operations, Joint Pub 3-0, Washington: September 1993, p. GL-6.
4. Joint Chiefs of Staff, Command and Control Warfare, Memorandum of Policy No. 30. Washington: March 1993, Enclosure, p. 1.

### Chapter II

1. Neff Hudson, "Future Shock." Air Force Times, October 25, 1993, p. 14.
2. Bartlett, Holman, and Somes. "Clear Strategies for a Murky World: Constructive Engagement and Selective Response," Naval War College Review, Summer 1993, p. 70.
3. David E. Jeremiah, "Pointing the Way," Defense, 1993, pp. 4-5.
4. Martin Van Creveld, "High Technology and the Transformation of War Part II," The RUSI Journal, December 1992, pp. 62-63.
5. Snider, Don M. "U.S. Military Forces in Europe: How Low Can We Go?" Survival, Winter 1992/93, p. 35.
6. Charles W. Taylor, A World 2010: A New Order of Nations, Carlisle Barracks: Strategic Studies Institute, 1992, p. 81.
7. E. R. Oxburgh, "Future Military Technology and the West," The RUSI Journal, December 1992, pp. 49-50.
8. Alvin Toffler and Heidi Toffler. War and Anti-War: Survival at the Dawn of the 21st Century, New York: Bantam Books, 1990.

9. David Ronfeldt, Cyberocracy, Cyberspace and Cyberology: Political Effects of the Information Revolution, Santa Monica: RAND, 1991, p. 3.

10. Brian Michael Murphy, The International Politics of New Information Technology, New York: St. Martin's Press, 1986, p. 261.

11. Ronfeldt, p. 2.

12. Ibid., p. 3.

13. William Gibson, as referenced by Anne W. Branscombe in, "Common Law for the Electronic Frontier," Scientific American, September 1991, p. 154.

14. Ronfeldt, p. 13.

15. Ibid.

### Chapter III

1. J. C. Wylie, Excerpts from Military Strategy: A General Theory of Power Control, Rutgers: The State University, 1967, p. 196.

2. Frederick the Great, as quoted by George Armand Furse in Information and War: Its Acquisition and Transmission, London: William Clowes & Sons, Ltd., 1895, p. 3.

3. John Arquilla and David Ronfeldt, Cyberwar is Coming!, Santa Monica, RAND, 1992, pp. 3-7.

4. Peter Grier, "The Data Weapon," Government Executive, June 1992, p. 20.

5. Hugh W. Bodnar, "The Military Technical Revolution: From Hardware to Information," Naval War College Review, Summer 1993, p. 19.

6. Gregory H. Canavan, "Changing Times Implode Defense Science Dynamics," Signal, September 1993, p. 50.

7. Joint Chiefs of Staff, Doctrine for Joint Operations, Joint Pub 3-0, Washington: September 1993, pp. V-1 - V-4.

8. Headquarters Department of the Army, FM 100-5 Operations, Washington: June 1993, p. 13-1.

9. Joint Chiefs of Staff, Doctrine for Intelligence Support to Joint Operations, Joint Test Pub 2-0, Washington: June 1991, p. IV-1.

10. Chris O. Geving, "Joint Intelligence Centers: Can They Support Operational Level Commanders?", Unpublished Research Paper, Naval War College: June 1993, p. 12.

11. Michael I. Bloom, Potential Uses of Advanced Automation Techniques in Command, Control, and Communications Countermeasures (C3CM), Alexandria: Institute for Defense Analysis, June 1990, p. 37.

12. Marshall E. Jordon, "Command and Control Warfare," Unpublished Research Paper, Montgomery: Air University, 1985, p. 30.

#### Chapter IV

1. Clausewitz, Carl von. On War. Translated and edited by Sir Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976, pp. 585-586.

2. Joint Chiefs of Staff, Doctrine for Joint Operations, Joint Pub 3-0, Washington: September 1993, p. GL-15.

3. Brian Michael Murphy, The International Politics of New Information Technology, New York: St. Martin's Press, 1986, p. 264.

4. Robert E. Ryals, "Flexible Deterrent Options: A Framework for Development, Model for Improvement," Unpublished Research Paper. Naval War College: May 1993, pp.4-8.

5. Joint Chiefs of Staff. Joint Strategic Capabilities Plan (JSCP). Washington: June 1993, p. III-4.

6. *Italics mine.*

7. *Ibid.*

8. Ron C. Plucker, "Command and Control Warfare--A New Concept for the Joint Operational Commander," Unpublished Research Paper, Naval War College, June 1993, pp. 19-20.

9. John M. Enger, quoting a French Minister of Justice in "Prospects of Global 'Information War' Poses Biggest Threat to U.S., *Los Angeles Times*, January 15, 1978, Part

VII, p.2, excerpted by David Ronfeldt in Cyberocracy, Cyberspace, and Cyberology: Political Effects of the Information Revolution, Santa Monica: RAND, 1991, p. 6.

10. John Arquilla and David Ronfeldt, Cyberwar is Coming!, Santa Monica, RAND, 1992, p. 16.

## BIBLIOGRAPHY

- Armed Forces Staff College. The Joint Staff Officer's Guide 1993. AFSC Pub 1. Washington: US Government Printing Office, 1993.
- Arquilla, John and Ronfeldt, David. Cyberwar is Coming! Santa Monica: RAND, 1992.
- Bartlett, Holman, and Simes. "Clear Strategies for a Murky World: Constructive Engagement and Selective Response." Naval War College Review, Summer 1993.
- Bloom, Michael I. Potential Uses of Advanced Automation Techniques in Command, Control, and Communications Countermeasures (C3CM). Alexandria: Institute for Defense Analysis, June 1990.
- Bodnar, John W. "The Military Technical Revolution: From Hardware to Information." Naval War College Review, Summer 1993.
- Branscombe, Anne W., "Common Law for the Electronic Frontier." Scientific American, September 1991.
- Canavan, Gregory H. "Changing Times Implode Defense Science Dynamics." Signal, September 1993.
- Clausewitz, Carl von. On War. Translated and edited by Sir Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.
- Furse, George Armand. Information in War: Its Acquisition and Transmission. London: William Clowes & Sons, Ltd., 1895.
- Geving, Chris O. "Joint Intelligence Centers: Can They Support Operational Level Commanders?" Unpublished Research Paper. Naval War College, June 1993.
- Grier, Peter. "The Data Weapon." Government Executive, June 1992.
- Hudson, Neff. "Future Shock." Air Force Times, October 25, 1993.
- Jeremiah, David E. "Pointing the Way." Defense, 1993, Vol. I.
- Joint Chiefs of Staff. Command and Control Warfare. Memorandum of Policy No. 30. Washington: March 1993.
- Joint Chiefs of Staff. Doctrine for Intelligence Support to Joint Operations. Joint Test Pub

2-0. Washington: June 1991.

Joint Chiefs of Staff. Doctrine for Joint Operations. Joint Pub 3-0. Washington: September 1993.

Joint Chiefs of Staff. Doctrine for Joint Operations in Low Intensity Conflict. Joint Pub 3-07, Initial Draft. Washington: May 1989.

Joint Chiefs of Staff. Joint Strategic Capabilities Plan (JSCP). Washington: June 1993.

Jordon, Marshall E. Command and Control Warfare. Unpublished Research Paper, Montgomery: Air University, 1985.

Lewonowski, Mark C. Information War. Montgomery: Air War College, April 1991.

Murphy, Brian Michael. The International Politics of New Information Technology. New York: St. Martin's Press, 1986.

Oxburgh, E. R. "Future Military Technology and the West." The RUSI Journal, December 1992.

Plucker, Ron C. "Command and Control Warfare-- A New Concept for the Joint Operational Commander." Unpublished Research Paper. Naval War College, June 1993.

Ronfeldt, David. Cyberocracy, Cyberspace, and Cyberology: Political Effects of the Information Revolution. Santa Monica: RAND, 1991.

Ross, Bruce M. "OPDEC and the Real-Time Media: CNN as a Force Multiplier." Unpublished Research Paper. Newport: Naval War College, June 1992.

Ryals, Robert E. "Flexible Deterrent Options: A Framework for Development, Model for Improvement." Unpublished Research Paper. Naval War College: May 1993.

Snider, Don M. "U.S. Military Forces in Europe: How Low Can We Go?" Survival, Winter 1992/93.

Sun Tzu. The Art of War. Translated by Samuel B. Griffith. London: Oxford University Press, 1963.

Taylor, Charles W. A World 2010: A New Order of Nations. Carlisle Barracks: Strategic Studies Institute, 1992.

Toffler, Alvin and Heidi. War and Anti-War: Survival at the Dawn of the 21st Century. New York: Bantam Books, 1993.

Van Creveld, Martin. "High Technology and the Transformation of War Part II." The RUSI Journal, December 1992.

Vincent, Gary A. "A New Approach to Command and Control: The Cybernetic Design." Airpower Journal, Summer 1993.

Wylie, Joseph C. Military Strategy: A General Theory of Power Control. Rutgers: The State University, 1967.





Why we see news anchorpersons only  
from the waist up.

The  
**Far Side**  
January

Saturday **22**

Sunday **23**