Maneuver Warfare in Cyberspace

CSC 1997

Subject Area - Warfighting

EXECUTIVE SUMMARY

Title: Maneuver Warfare in Cyberspace

Author: Major P.K. Singh, Australian Army

Thesis: Information age technologies have created a new cyberspace environment in which to conduct warfare. Control of cyberspace will increasingly present a challenge for national security into the 21st Century.

Discussion: A new environment for warfare is emerging in the information age, but generally the strategic implications have not been recognized. Social and economic paradigms are radically changing with the consequences of more diverse patterns of conflict occurring among both state and non-state entities. New technology is heralding a Revolution in Military Affairs which has the potential to enhance strategic capabilities and create a cyberspace "arms race." The dynamism of the era raises vital issues such as the focus of national leadership and the validity of national security and military strategies. Russia's response to the information age highlights the potential for challenges to the existing military balance and global security. Paradoxically, the United States is increasingly vulnerable to information warfare as the information age progresses and cyberspace expands. Analysis reveals an alarming reality: there is gap between the emerging information age environment and concomitant development in doctrine, capabilities and strategies for information warfare at the strategic level.

Cyberspace has emerged as a dimension in which to attack an enemy and to break his "will" to resist, yet there is a doctrinal vacuum for this form of warfare. To help redress the situation, a conceptual framework and doctrine for warfare in cyberspace is required. Maneuver warfare theory, when combined with Warden's Five Rings model and a change to the paradigm of battlespace, is a suitable first-step way of thinking about cyber warfare. As a corollary, a three tier strategy is required prior to initiating capability development. (1) Strategic direction and guidance is required to mobilize the efforts of all government departments and agencies. (2) National security and military strategies must outline a response to the threats and opportunities of cyber warfare. (3) Definition of Department of Defense's offensive and defensive responsibilities, parameters and capabilities for strategic information warfare needs to be clearly articulated.

Overall, the paper seeks "to anticipate the changes in the character of war" and it advocates for capability development to conduct offensive and defensive maneuver in cyberspace.

# Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **1997**	2. REPORT TYPE	3. DATES COVERED **00-00-1997 to 00-00-1997**

4. TITLE AND SUBTITLE **Maneuver Warfare in Cyberspace**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Marine Corps War College,Marine Corps University,Marine Corps Combat Development Command,Quantico,VA,22134-5067**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**67**	

Recommendation: It is recommended that Department of Defense leadership promote further discussion and analytical study on the requirement to conduct strategic level offensive and defensive warfare in cyberspace.

CONTENTS

TITLE PAGE i

EXECUTIVE SUMMARY iii

LIST OF FIGURES v

ABBREVIATIONS vi

PREFACE vii

CHAPTER **Page**

1. THE STRATEGIC IMPLICATIONS OF WARFARE IN THE INFORMATION AGE 1

2. MANEUVER WARFARE IN CYBERSPACE 26

3. CONCLUSION: REALITY, THEORY AND NEXT STEPS 42

GLOSSARY - INFORMATION WARFARE & CYBERSPACE 49

BIBLIOGRAPHY 51

LIST OF FIGURES

Figure **Page**

1. Computer Transforming the Economic Environment 4

2. Toffler's Waves of Warfare 7

3. Cyberspace Vulnerabilities for National Security 22

4. Warden's Five Ring Model 30

5. Information Warfare Chart 36

6. Dimensions for Maneuver Warfare 39

7. Cyberspace Compression of Levels of War 40

ABBREVIATIONS

CONUS	Continental United States
C^{2}W	Command and Control Warfare
DoD	Department of Defense
EW	Electronic Warfare
GII	Global Information Infrastructure
GPO	Government Printing Office
INSS	Institute for National Strategic Studies
IW	Information Warfare
JROC	Joint Requirements Oversight Council
MTR	Military-Technical Revolution
NII	National Information Infrastructure
NMS	National Military Strategy
NSS	National Security Strategy
OODA	Observation-Orientation-Decision-Action
OOTW	Operations Other Than War
PDD	Presidental Decision Directive
R&D	Research and Development
RMA	Revolution in Military Affairs

PREFACE

Victory smiles upon those who anticipate the changes in
the character of war, not upon those who wait to adapt
themselves after the changes occur.
- Air Marshal Giulio Douhet

"Government and commercial computer systems are so poorly protected today that they can essentially be considered defenseless - an electronic Pearl Harbor waiting to happen."[1] With this characteristic flourish, Winn Schwartau sounded an ominous warning to a Congressional Committee hearing in 1991. This threat arose because of the emergence of the information age - a new age which will radically change the character of warfare. The impact of this age is comparable to the effect the industrial age had on war throughout the nineteenth and twentieth centuries. This paper contends that embedding information age technologies in the national and global information infrastructure created a new environment in which to conduct maneuver warfare. The new environment is called cyberspace, and it increasingly presents a challenge for national security into the 21st Century.

This paper is in three parts and written from a United States perspective. The first chapter analyzes the strategic environment for warfare in cyberspace and focuses on four key aspects which include: the new social and economic environment emerging from the information age; the contribution of the Revolution in Military Affairs (RMA) to enhance strategic capabilities and potentially start a cyberspace "arms race", which in turn raises questions on the validity of current national security and military strategies; Russia's response to the information age and the potential for challenges to the existing military

[1] Winn Schwartau, *Information Warfare - Chaos on the Electronic Superhighwa*y (New York: Thunder's Mountain Press, 1994), 13.

balance and global security; and finally, the United States' increasingly vulnerable position as the information age gathers momentum and cyberspace expands.

The second chapter explains how maneuver warfare theory might be adapted to the cyberspace environment with devastating effect. The aim is to provide a "way of thinking" about cyber warfare in a similar manner that Douhet, writing in the 1920s, envisaged the strategic implications of airpower. In short, cyberspace is a dimension to attack an enemy and to break his "will" to resist. There is a link between the first and second chapters. In essence, chapter 1 analyzes the current "reality" and exposes the gap between the emerging information age environment and concomitant development in doctrine, capabilities and strategies at the strategic level. Chapter 2 theorizes how the information age environment can be exploited as a dimension to defeat an adversary, particularly at the strategic level. The paper's conclusion brings together the reality and theory discussion from the first two chapters and suggests avenues for further investigation and analysis. Overall, the aim of the paper is to anticipate the changes in the character of war and advocate for capability development to conduct offensive and defensive maneuver in cyberspace.

CHAPTER 1

THE STRATEGIC IMPLICATIONS OF WARFARE IN THE INFORMATION AGE

> *When farming was the essence of national economies, taking land was the essence of war. As agriculture yielded to industry, war too was industrialized; nations defeated foes by destroying their productive capacity. If this pattern holds for the information age, might war follow commerce into cyberspace, pitting foes for control of this undefinable but critical ground.*[1]

The information age is having a profound effect on the world. While the future is not entirely clear, Peter Ducker says "the one thing we can be sure of is that the world that will emerge from the present rearrangement of values, beliefs, social and economic structures, of political concepts and systems, indeed, of world views, will be different from anything anyone today imagines."[2] Conceptually, the impact of the new environment has not been missed by defense planners. In an Army think-piece entitled "War in the Information Age", Army Chief of Staff General Gordon Sullivan and Colonel James Dubik reflect that the information age "will affect every aspect of human life ... and the Army is changing to accommodate this new epoch ... and positioning America's

[1] Institute for National Strategic Studies, National Defense University, *Strategic Assessment 1996: Instruments of US Power,* (Washington DC: National Defense University Press, 1996), 194.

[2] Gordon R. Sullivan & James M. Dubik, *War in the Information Age*, (Pennsylvania: Strategic Studies Institute, US Army War College, 6 June 1994) 1, citing Peter Ducker's *Post Capitalist Society.*

Army today so that it will succeed in the information age is a historic task."[3] These comments are indicative of the forward-looking approach being taken by all Services. In fact *Joint Vision 2010,* which provides the strategic template for the evolution of the US Armed Forces, speaks of "information-age technological advances" as one of the four principle concepts for core strength in the future.[4] Overall, military analysts thoroughly embrace this futuristic assessment of information age technological advances.[5]

This chapter analyzes four significant aspects of the information age pertaining to national security: the information age environment for warfare; the direction of the RMA, and the validity of current leadership's national security and military strategies; Russia's response to the information age and the potential impact on *global* security; and finally the United States' vulnerability from weaker countries or non-state groups who could use abundant cyberspace technologies for offensive action. A central theme is that while RMA proponents concentrate on comprehensive enhancements to operational and tactical capabilities with information age technology, they generally do not analyze the broader strategic implications and possibilities. A notable feature is the mismatch between the national security and military strategies and the emerging vulnerabilities of the United States in the information age.

[3] Sullivan & Dubik, 20.

[4] "Joint Vision 2010: America's Military Preparing for Tomorrow," *Joint Force Quarterly*, Summer 1996, 35.

[5] Other countries follow the United States trend. For instance in Australia, Colonel Peter Leahy, Director of Army Research and Analysis, agrees that "the information age is not yet fully upon us", and intuitively declares "information age armies will be capable of more flexibility, more versatility, faster decision making and more decisive action." Peter F. Leahy, "The Revolution in Military Affairs and the Australian Army," *The Combined Arms Journal*, Issue 2/95, (Sydney: HQ Training Command, Australian Army, 1995), 19-20.

THE EMERGING SOCIAL, POLITICAL AND ECONOMIC ENVIRONMENT FOR WARFARE

The Army defines the term "information age" in Pamphlet *525-5 Force XXI Operation*s as "a future time when social, cultural and economic patterns will reflect the decentralized non-hierarchical flow of information."[6] Images of the future generally draw upon the work of Alvin Toffler who, in 1980, described the current technological changes as the Third Wave of the three great transforming ages in history.[7] In *The Third Wave,* Toffler forecasts that the information age will bring wholesale change to society, the economy and politics, and also transform the traditional nation state system. These comprehensive changes are due to the astounding degree to which power and wealth have come to depend on knowledge. What is occurring is a deep-level change in the very nature of power. The result is that an advanced economy, with its complexities of production, financial markets, and integration of diverse systems could "not run for thirty seconds" without microprocessors and computer networks.[8]

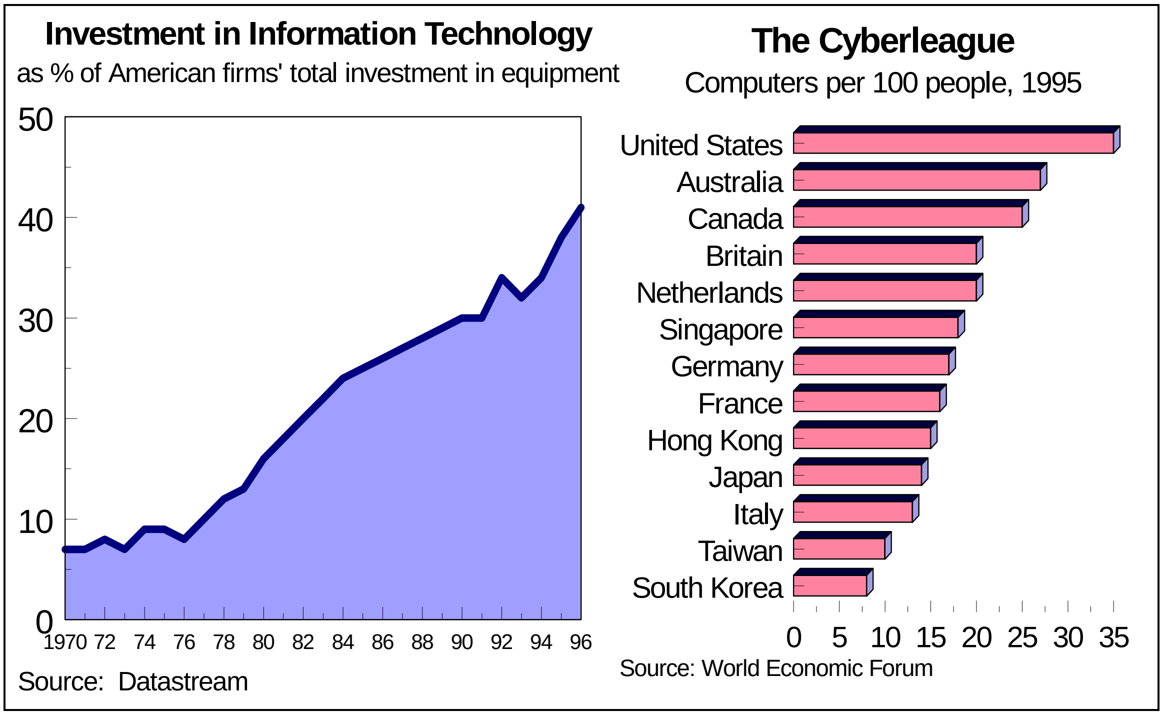
The Economist magazine recently provided evidence supporting Toffler's futuristic assessment when it surveyed the extent that the information technological

[6] US Army, Pamphlet 525-5 *Force XXI Operations*, (Fort Monroe Virginia: US Army Training and Doctrine Command, August 1994), Glossary, 1.

[7] Alvin Toffler, *The Third Wave*, (New York, Bantam Books, 1980). The agricultural revolution of 10,000 years ago was termed the First Wave, and the industrial revolution the Second Wave. The Third Wave is the "informational" age.

[8] Alvin Toffler, *Powershift*, (New York: Bantam Books, 1990), 16.

revolution will be accompanied by an economic revolution.[9] Over the past two decades, the investment in computers in America has risen 20-30% in real terms per year. Figure 1 shows the share of firms' total investment in information technology equipment has increased from 7% in 1970 to over 40% in 1996, and "... about half of all American workers now use some form of computer."[10] *The Economist* notes, however, that the real productivity gains based on this investment is yet to be realized as there is historically a lag between acquiring new technology and shifts in the economy.[11]


Investment in Information Technology

as % of American firms' total investment in equipment

Source: Datastream

The Cyberleague

Computers per 100 people, 1995

Source: World Economic Forum

***Figure 1*: Computers Transforming the Economic Environment**

[9] Pam Woodall, "The Hitchhiker's Guide to Cybernomics," *The Economist*, 28 September 1996, after 64.

[10] Woodall, 15.

[11] For instance, the introduction of the electric dynamo in the early 1880s did not yield significant productivity gains until the 1920s. Comparatively, computers are making a faster impact. Woodall, 8.

In 1992, the United States invested over $210 billion in information technology, about half the global investment, and the amount has continued to grow at about 18 percent since.[12] Nearly all economic commentators agree that the impact of information technology (semiconductors, computers, software and telecommunications) will increasingly transform the global economic environment. *The Economist* summized that there is widely divided opinion as to whether the consequences will be largely positive or negative. On the positive side, many analysts argue that the technological revolution is "an engine for growth and prosperity". Other forecasters, however, conclude that "... rapid technological change and increased international competition are fraying the job markets of the major industrialized countries. The global economy is leaving millions of disaffected workers in its train. Inequality, unemployment, and endemic poverty have become its handmaidens."[13] As the information age unbalances the economic *status quo* and states are challenged by social and political upheaval, governments will increasingly be engaged in some form of inter-state or intra-state conflict. The type of conflict wrought by information age upheaval may well be different from anything encountered in the industrial age.

Regardless of whether the outcomes of the technological revolution are positive

or

[12] Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal*, vol. 9, no. 1 (Spring 1995): 63.

[13] Woodall, 4.

negative, the overriding message is that the changing world economy calls for nothing less than a new economic paradigm. A new economic environment may have significant consequences in terms of global military power. In *The Rise and Fall of Great Powers*, Paul Kennedy's analysis of the past five centuries concludes that "the relative position of each of the states has been affected by economic and technological change, and the constant interaction between strategy and economics."[14] While cogent counter arguments to Kennedy's thesis have credibility,[15] three distinct economic indicators should be acknowledged by military strategists. First, there is a convergence in levels of income, growth, and productivity among North American, European, and Asian countries. Second, there is an evolution of global industrial networks with highly integrated and stable nodes, reinforcing the global economy.[16] Third, there is strong empirical evidence to support Toffler's argument that computerized information systems will be the foundation of economic wealth and social order. Finally, if the global economy, networks, and information systems represent strengths in the information age, then to the military mind they should also represent critical vulnerabilities -- something to be attacked or protected.

[14] Paul Kennedy, *The Rise and Fall of Great Powers*, (New York: First Vintage Books, 1989), xxi.

[15] Kennedy's thesis describes great powers moving ahead and falling behind, losing steam after trying to sustain military hegemony too long. However, Huntington effectively argues that US growth rates are not tied to the military outlays. *cf.* Samuel P. Huntington, "The US - Decline or Renewal?" *Foriegn Affairs*, vol. 67, (Winter 1988/89).

[16] James R. Golden, "Economics and National Strategy: Convergence, Global Networks, and Cooperative Competition," in *New Forces in the World Economy*, ed. B. Roberts (Cambridge, Massachusetts: The MIT Press, 1996), 19.

Turning to warfare in the information age, Toffler envisions an information age where knowledge has gone from being an adjunct to money and muscle, to being the most important ingredient of force and wealth.[17] Although the United States and other countries are riding the information age wave, other wave forms continue to exist. Two important features will emerge. First, cultural variants will arise as other countries enter the information age and adds to the complexity of the global environment.[18] Toffler believes that this phenomena of unequal growth and cultural variation will "represent the 21st century world conflict pattern."[19] Second, warfare will become an admixture, to varying degrees, of agrarian, industrial, informational age technologies and war forms. These two factors create an environment which will be characterized by complexity, unique forms of conflict, and increased global disparity between rich and poor.[20] Such an environment can be explained by Toffler's "waves of warfare" concept.

According to Toffler, a characteristic of the three great ages is the unmistakable parallel between the features of an economy and the features of warfare. The way we make war reflects the way we make wealth.[21] Each age has its own unique form of war and a true military revolution only occurs when the form of war is completely altered as a result of a civilization entering a new age. This is the essence of a military revolution. In their book *War and Anti-War,* Alvin and Heidi Toffler describe how each wave runs concurrently and sequentially (schematically shown at Figure 2). The United States

[17] Toffler, *Powershift*, 17.

[18] Such as the cultural variation between European and Japanese in Second Wave industrialism.

[19] Alvin & Heidi Toffler, *War and Anti-War,* (New York: Little Brown and Company, 1993), 256.

[20] *The Global 2000 Report to the President of the US: Entering the 21st Century*, Vol. : The Summary Report, Gerald O. Barney ed., (New York: Pergaman Press, 1980), 7.

armed forces may find themselves facing opponents fighting within any one of the three waves, or within a combination of waves. The Tofflers claim that Operations *Just Cause* and *Desert Storm* represent the first wars of the third wave.

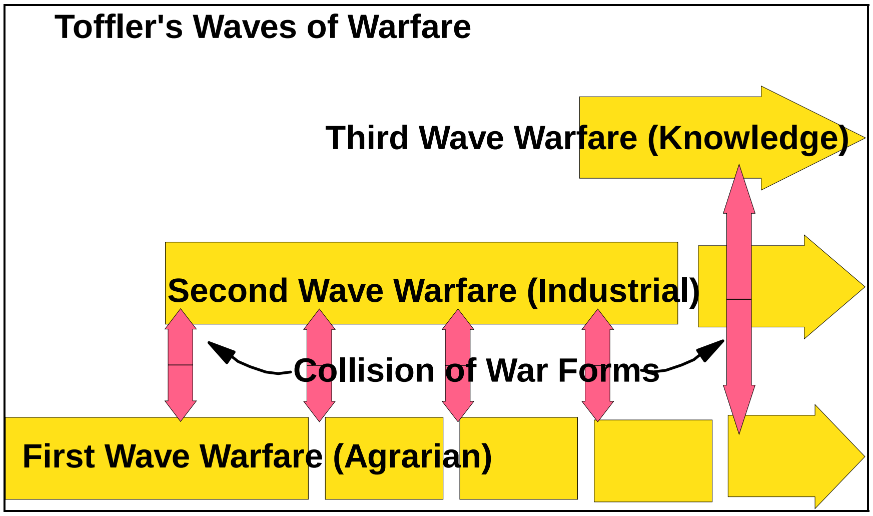

Toffler's Waves of Warfare
Third Wave Warfare (Knowledge)
Second Wave Warfare (Industrial)
Collision of War Forms
First Wave Warfare (Agrarian)

***Figure 2*: Toffler's Waves of Warfare**

In his book the *First Information War,* Alan Campen contends that in the Gulf War "knowledge came to rival weapons and tactics in importance, giving credence to the notion that an enemy might be brought to its knees principally through destruction and disruption of the means for command and control."[22] Empirical evidence supports this assertion. In Operation *Desert Storm* the electronic warfare (EW) phase lasted for 38 days, more than nine times as long as the ground operations phase. In abundance was the

[21] Toffler, *War and Anti-War,* 3.

[22] Toffler, *War and Anti-War,* 69.

latest electronic warfare equipment, airborne early-warning and control aircraft, and radar systems for reconnaissance and precision strike. Important targets were continuously and precisely attacked by EW and precision missiles throughout the entire battlespace, disrupting the command and communications system at all echelons. Control of air operations, with up to 2,000 to 3,000 sorties per day, was unprecedented. As a result, Iraqi combat effectiveness and will to fight was all but been destroyed before the beginning of the ground offensive. Linking the operational and strategic level, there were more than 3,000 computers in the war zone linked to computers in the United States, which is indicative of the increasing interface between strategic, operational and tactical levels in the information age.

Given such evidence, many analysts[23] support Toffler's claim that: "Knowledge, in short, is now the central resource of destructivity, just as it is the central source of productivity" and in the information age "a revolution is occurring that places knowledge, in various forms, at the core of military power."[24] In making this statement Toffler does

[23] Among those who agree are: Stuart E. Johhnson and Martin C. Libicki, eds., *Dominant Battlespace Knowledge: The Winning Edge* (Washington DC: National Defense University Press, 1995); Winn Schwartau, *Information Warfare - Chaos on the Electronic Superhighwa*y (New York: Thunder's Mountain Press, 1994); Edward Mann, "Desert Storm: The First Information War, *Airpower Journal*, 8, no. 4, (Winter, 1994); Owen E. Jensen, "Information Warfare: Principles of Third-Wave War", *Airpower Journal*, 8, no. 4, (Winter, 1994). Conversely, those who criticise key aspects of Toffler include: Steven Metz, "A Wake for Clausewitz: Toward a Philosophy for 21st Century Warfare," *Parameters*, (Winter, 1994-95); Richard M. Swain, review of Toffler, *War and Anti-War*, in *Military Review*, February 1994, 78; Robert J. Bunker, "The Tofflerian Paradox," *Military Review*, (May-June 1995), 99-102.

[24] Toffler, *War and Anti-War*, 69-71.

not deny that knowledge has always been important in war, but the 1990-91 Gulf War evinced new trends for warfare. Continuing the trend in computer reliance, the US Air Force contracted for the purchase of 300,000 computers in 1993.

THE RMA, NATIONAL DEFENSE STRATEGIES AND LEADERSHIP IN THE INFORMATION AGE

Widespread debate in the defense community exists on the subject of the RMA.[25] Publications, papers, and conferences abound with the concept of "third wave" warfare. Military analysts are grappling with how Toffler's concept of the impending information age might translate to change for the military. Carl Builder, a senior analyst at RAND Corporation, at a Revolution in Military Affairs Conference conducted by the Australian Defence Studies Centre over 27-28 February, 1996, identified technology as the catalyst for changing societal order with seldom foreseeable consequences at the time. "In the information age", Builder explained, "the societal implications were firstly, a diffusion of power downwards and secondly, a by passing of traditional hierarchies."[26] A recurring theme of the conference indicated:

[25] There is no precise definition for the term RMA. Earl Tilford perhaps comes closest when he defines the RMA as a "major change in the nature of warfare brought about by the innovative application of technologies with dramatic changes in military doctrine and operational concepts, fundamentally alters the character and conduct of operations." Earl H. Tilford, *The Revolution in Military Affairs: Prospects and Cautions*, Strategic Studies Institute, 23 June 1995.

[26] Keith Thomas, "A Revolution in Military Affairs," *Research and Analysis*, Newsletter no. 5, (Canberra: Directorate of Army Research and Analysis, Australian Army,March 1996), 2. Citing Carl Builder at the RMA Conference conducted by the Australian Defence Studies Centre on 27-28 February 1996.

> *... an RMA is likely to be part of a much broader social revolution brought about by new information technology. Thus, continuing challenge to existing defence paradigms, the future would seem to require a more inclusive approach, involving civil and business leaders as well as the military.*[27]

To help meet these challenges under the RMA genre, William Lind promoted the notion of a fourth generation of warfare propelled by new technology of the information age.[28] Notably, fourth generation warfare carries over a few key elements from the third generation such as mission orders, maneuver emphasis, and targeting the enemy's societal morale.

While most analysts agree that a RMA will be a bi-product of the information age, few acknowledge that the RMA "race" will in itself shape the information age. For instance, in 1906, Britain's development of the *Dreadnought* class of battleship rendered obsolete all previously constructed battleships and consequently the great powers, including Britain, were forced into an arms race. Around the world navies were revolutionized, and as such became a driving force of the industrial age. The negative consequence for Britain was that previously she was unrivaled as a sea power, but after 1906 she had a lead of just one battleship - *HMS Dreadnought*. Irrelevant naval powers such as Germany now sought to challenge British naval supremacy.[29] The RMA and the development of information age military capabilities is likely to fuel a similar "arms"

[27] Thomas, 3.

[28] William S.Lind, "The Changing Face of War," *Marine Corps Gazette*, (October 1989), .

[29] Robert K. Massie, *Dreadnought: Britain , Germany, and the Coming of the Great War,* (New York: Ballantine Books, 1991), 487. "Now charged (Admiral Jacky) Fisher's critics, at the whim of a foolish First Sea Lord, Britain had thrown it all away. By introducing a new class of ship so powerful that all previous battleships were instantly obsolete ... Germany was to be given a chance to begin a new race with Britain for naval supremacy on equal terms."

race with the same potential (*Dreadnought)* negative consequences for the United States. In this way the RMA could precipitate a change in the balance of power.

The National Defense University's, Martin Libicki wrote in 1995 that information warfare and the RMA "... has assumed almost totemic importance in the conceptual superstructure of national defense."[30] RMA concepts are providing an impetus for capability development and the allocation of defense resources. Therefore the nature of the RMA, and how it is controlled by defense policy and strategy, will be a central feature of the information age environment. National strategy should be cognizant of the RMA's potential to affect the balance of power. Andrew Marshall, a Director at the Pentagon's Office of Net Assessment, has made insightful contributions to understanding how the RMA might evolve.[31] Marshall theorized that the RMA will evolve in two stages: first, in a drive to limit casualties, stand-off platforms, stealth, precision weapons, information dominance and missile defense will emerge as the priority; while the second stage emphasizes robotics, non-lethality, psychotechnology and elaborate cyber defense.[32]

Despite the broad debate on the RMA, no consensus on information warfare's strategic or operational implications emerges.[33] Most analysts view information warfare

[30] Martin C. Libicki, *What is Information Warfare*, (Washington DC: National Defense University, October 1995), 2.

[31] Andrew W. Marshall, Senior Information Warfare Offical, Office of the Secretary of Defense / Net Assessment. Information warfare was identified as a potentially important new warfare area several years ago in OSD/NA, and has since been the subject of wide-ranging study.

[32] Andrew W. Marshall, "Some thoughts on Military Revolutions - Second Version", Memorandum for the Record, Office of the Secretary of Defense, Office of Net Assessment, (23 August, 1993).

[33] As an example of the debate see, Pat Cooper, "Information Warfare Sparks Security Affairs Revolution," *Defense News*, vol. 10, no. 23, June 12-18, 1995, 1.

as an adjunct to conventional strikes - a force multiplier - rather than a stand alone method of warfare.[34] Discussion of the strategic implications of information warfare among the military and the defense community has been limited to a few writers, but none propose a comprehensive framework for the strategic use of such warfare.[35] At issue is the extent to which a revolution can be initiated or shaped by deliberate policy decisions.[36] Certainly making an RMA happen and controlling its development are themes that Admiral William Owens stressed when vice chairman of the Joint Chiefs of Staff. Through the Joint Requirements Oversight Council (JROC), Admiral Owens declared that: "If we decide to accelerate the process by emphasizing those systems and weapons that drive the revolution in military art, we can reach ours years - perhaps decades - before any other nation."[37]

Similarly, Marshall advises that the United States should accelerate the RMA pace in order to deter a peer competitor from making similar investments -- essentially to price the competitor out of the market by creating an insurmountable technology gap. To achieve this end, Steven Metz and James Kevit assert in "Strategy and the Revolution in

[34] Of this genre include: George Stein, 30-55; Edward Mann, "Desert Storm: The First Information War?", *Airpower Journal*, vol. 8, no. 4, (Winter 1994), 4-14; and Owen Jensen, "Information Warfare: Principles of Third Wave War," *Airpower Journal*, vol. 8, no. 4, (Winter 1994), 35-44.

[35] Steven Metz and James Kevit, "Strategy and the Revolution in Military Affairs: From Theory to Policy," (27 June 1995), in *Joint Electronic Library*, CD-ROM, September 1996, 14.

[36] Thinking about an RMA as a predictive problem misses the point. Instead an RMA should be thought of as something to make happen: "It is easier to design the future than it is to predict it." Paul Bracken and Raoul Alcala, *Whither the RMA: Two Perspectives on Tomorrow's Army*, (Pennsylvania: Strategic Studies Institute, US Army War College, 22 July 1994).

[37] William A. Owens, "The Emerging System of Systems," *Military Review*, (May - June 1995), 19.

Military Affairs: From Theory to Policy," that "in order to master the RMA rather than be dragged along by it, Americans must debate its theoretical underpinning, strategic implications, core assumptions and normative choices."[38] Unfortunately to date there has been little debate on these national level strategic issues in the United States.[39]

There is, however, concern that the United States will not only need to be prepared to fight an information age war, but also first (agrarian) and second (industrial) wave adversaries. This concern is sometimes called the "bandwidth problem". In *Technology and War,* Martin van Creveld describes a future predominantly influenced by terrorism and insurgency and warns that a technology dependent military force might be unbalanced because "... technology and war operate on a logic which is not only different but actually opposed; the very concept of 'technological superiority' is somewhat misleading when applied to the context of war."[40] For instance, the technical sophistication of the United States in the Vietnam War could not overcome the agrarian age North Vietnamese and Viet Cong.

Admiral Owens' paper entitled "JROC: Harnessing the Revolution in Military Affairs" in *Joint Forces Quarterly*,[41] almost exclusively focuses on capability

[38] Metz and Kevit, iii.

[39] By contrast, the subject of an RMA has attracted a good deal of attention among defense analysts and within the Department of Defense. As a consequence a series of task forces have been formed to assess the potential for innovation in key areas of warfare such as missile defense and precision strike. Significant resources are being allocated to new ways to bring the information age onto the battlefield. The Army's *Force XXI* concept, the Marine Corps' *Sea Dragon* and the recent *Report of the Defense Board Task Force on Tactics and Technology for 21st Century Military Superiority,* Office of the Secretary of Defense (October 1996).

[40] Martin van Creveld, *Technology and War - From 2000 BC to Present,* (New York: The Free Press, 1989), 319.

[41] William A. Owens, "JROC: Harnessing the Revolution in Military Affairs," *Joint Forces Quarterly,* (Winter 1993-1994), 55-57.

development at the operational level. Such focus is typical across DoD and negatively impacts on national security and military strategies. For instance, *A National Security Strategy of Engagement and Enlargement* (NSS), February 1996, states: "The new era presents a different set of threats to our security," and goes on to list proliferation of weapons of mass destruction, terrorism, narcotics trafficking, organized crime, environmental and natural resource issues as new challenges to US security strategy.[42] The glaring omission in the NSS is the threat to the national information systems.Also, the section in the NSS outlining the requirement for a strong defense capability does not include the concept of protecting national information systems as a task for the military or any other agency.[43]

The *National Military Strategy* (NMS) is derived form the NSS and consequently fails acknowledge the strategic implications of the information age. The NMS also omits recognition of any threat to national information systems from a military aggressor. The limitations are readily apparent when the NMS states:

> *The strategic landscape is characterized by four principle dangers which our military must address: regional instability; the proliferation of weapons of mass destruction; transnational dangers such as drug trafficking and terrorism; and the dangers to democracy and reform in the former Soviet Union, Eastern Europe and elsewhere.*[44]

To "Win the Information War" the NMS remains steadfastly focused on the operational and tactical levels and the scope for information warfare is limited to *Desert Storm* type

[42] *A National Security Strategy of Engagement and Enlargement,* (Washington DC: US GPO, February 1996), 12-13. Hereafter cited as NSS.

[43] NSS, 13.

[44] *National Military Strategy of the United States of America,* (Washington DC: US GPO, 1995), i. Hereafter NMS.

scenarios.[45] The evidence indicates that the NSS and NMS missed the strategic implications of the emerging information age.

Unfortunately, *Joint Vision 2010* also does not address what the NSS and NMS missed on the question of information warfare at the strategic level. Although *Joint Vision 2010* describes the information era "of accelerating technological change" as one to be harnessed for "dominant battlespace awareness," dominant maneuver, precision engagement, full-dimensional protection, and focused logistics. For the military, the parameters for information warfare are confined to a regional conflict scenario and the spectrum of operational and tactical capabilities. Only in passing does *Joint Vision 2010* reflect that: "In addition, increased strategic level programs will be required in this critical area (of defensive information warfare)."[46]

Enthusiasm for embracing the information age at the operational level contrasts inertia at the strategic level. From a national perspective only a few initiatives are underway. Presidential Decision Directive (PDD) 29 of 1994, created a Security Policy Board to address a variety of security issues to include information systems security and risk management. However, a July 1995 report commissioned for the Joint Staff entitled "Information Warfare" indicated that "there is no national policy on information warfare ... (which) is a source of concern for many, particularly in the DoD."[47] Below the

[45] NMS, 15.

[46] "Joint Vision 2010: America's Military Preparing for Tomorrow," *Joint Force Quarterly*, (Summer 1996), 41.

[47] Science Applications International Corporation Report, *Information Warfare - Legal, Regulatory, Policy and Organizational Considerations for Assurance,* A Research Report for the Chief, Information Warfare Division (J6K), Command, Control, Communications and Computer Systems Directorate, Joint Staff, The Pentagon, Washington DC, 4 July 1995, 2-51.

executive advisory level, there is no overarching authority to take the lead for information warfare policy, strategy, or defense.

The absence of a leading authority in Government is surprising given President Clinton's and Vice President Gore's awareness of the economic and social implications of the information age is evinced by their firm platform to "use information technology to improve American's quality of life and reinvigorate the economy;"[48] and their vision for expanding the Global Information Infrastructure (GII) to build an inter-connected and interdependent global community.[49] Presidential leadership, however, views threats to the National Information Infrastructure (NII) and GII only in the context of criminal behavior, a matter for security managers. The issue of the NII and GII becoming a military target, a matter for the National Command Authority and Defense, has not been formally acknowledged. Vice President Al Gore's document, entitled *Global Information Infrastructure: Agenda for Cooperation* provides evidence of a misguided assumption of a GII and NII free from military manipulation. The following extract reveals how Gore merely equates "security challenges" solely within the context of criminal behavior:

> *A network as vast and complex as the GII will pose difficult security challenges for all nations. The same modern technology that makes communication faster and easier also makes communication systems vulnerable to ever greater security risks. These risks are not new - most are well-known to security managers.*[50]

[48] Al Gore, *Creating a Government that Works Better and Costs Less: Reengineering Through Information Technology*, (Washington DC: US GPO, September 1993), 2. Vice president Gore is spearheading administration efforts under the Information Infrastructure Task Force (IITF).

[49] Al Gore, *Global Information Infrastructure: Agenda for Cooperation*, (Washington DC: US GPO, January 1995).

[50] Al Gore, *Global Information Infratsructure: Agenda for Coorperatio*n, 23.

When it comes to addressing information age issues, leadership should accept its responsibility for creative innovation and protection of national information interests.

Absence of progress on the issue of strategic information warfare is alarming in the light of some warnings. In 1991, Winn Schwartau submitted testimony to a Congressional Committee that "inadequate security planning on the part of both the government and the private sector"[51] could result in an electronic Pearl Harbor. A range of government sponsored reports support Schwartau's assessment. The National Research Council reported in *Growing Vulnerability of the Public Switched Networks: Implications for National Security*, that "because of powerful trends in the evolution of the nation's telecommunications and information networks, they are becoming more vulnerable to serious interruptions of service."[52] Other examples of the growing

[51] Schwartau, 13.

[52] The National Research Council Report, US Department of Commerce, *Growing Vulnerability of the Public Switched Networks: Implications for National Security*, (Washington DC: National Academy Press, 1989), 1.

vulnerability of information systems abound in Government reports and papers.[53] Overall, Metz and Kevit believe that a strategic vacuum exists and the vulnerabilities to the NII continue to become more pronounced. At the end of their article, both analysts postulate: "If the United States is to lead and master the revolution rather than be its eventual victim, this (strategic) vacuum must be filled."[54]

THE CHANGING GLOBAL ENVIRONMENT:
RUSSIA'S RESPONSE TO THE INFORMATION AGE

Russia's perspective on the impact of the information age will be a major factor in shaping the global strategic information warfare environment. There is the potential for Russia to bypass the United States' expensive R&D investment and develop its so-called "sixth generation" of cyberspace warfare technology. Despite Russia's struggling economy, there is the long-term potential for reasserting military power through cyberspace. Russia could make advances in cyberspace in a similar manner that the Soviet Union harnessed nuclear technology for war despite its struggling post-war economy.

[53] Reports of the same genre include: Office of the Manager, National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications, An Awareness Document*, Arlington, Virginia: 5 December 1994; and Naval War College, *Symposium Report: Evolving the National Information Infratsructure (NII); A Symposium for Government and Industry*, (Naval War College, 9 January 1995).

[54] Metz , 41.

Mary FitzGerald, an adjunct professor at the United States' Air Command and Staff College and research fellow with the Hudson Institute's National Security Studies Group, recently analyzed Russia's perspective on the impact of information technology. FitzGerald states that the Russians believe that a military-technical revolution (MTR) is emerging where "... precision-guided, non-nuclear, deep-strike weapons, and the systems used to integrate them, are revolutionizing all aspects of military art and force structure - and elevating combat capabilities by a million-fold."[55] The strategic impact is equally dramatic as Admiral V.S. Pirumov says in *Two Aspects of Parity and Defense Sufficiency*, "... that a war's main objective is shifting away from seizure of the opponent's territory and moving towards neutralizing his political or military-economic potential - eliminating a competitor - and ensuring the victor's supremacy in the political arena or in raw materials and sales markets."[56] Clearly the Russians envision a radical change to their concept of warfare.

In *Military Review,* Lieutenant Commander Randall Bowdish describes how the Russians foresee impending sixth generation of information warfare technology as a potential for cyber warfare to inflict decisive military and political defeat on an enemy at

[55] Mary C, FitzGerald, "The Russian Military's Strategy For 'Sixth Generation' Warfare," *Orbis*, (Summer 1994), 457.

[56] Mary C. FitzGerald, "Russian Views on Information Warfare," *Army*, (May 1994), 58.

low cost and without occupying enemy territory.[57] FitzGerald also states that Russia's sixth generation warfare is intended to change the laws of combat and the principles of military science. In past wars the emphasis was on the battle on the earth's surface, with the vertical coordinate (primarily air) playing a supporting role. In future wars the "... main vector of combat will be the vertical or aerospace coordinate, with operations on the ground playing a supporting role."[58] The changing emphasis in "vectors" has not been acknowledged in the United States in key publications such as *Joint Vision 2010*.

Russian analysts realize the potential to use sixth generation cyberspace weapons at the outset of war with devastating effect. The impact on national strategy and campaign planning is apparent, as Defense Minister P. Grachev described in 1993: "If war begins, it will be with an air-space offensive operation by both sides. Strikes on main facilities and troops will be made from space and from the air."[59] Electronic-fires makes these strategies possible. Timothy Thomas, in a *Parameters* article "Deterring Information Warfare: A New Strategic Challenge", argues that Russia is cognizant of this first-strike potential and is at the forefront of theoretical attempts to prepare against the possibly of strategic information assault. In speech given at the Russian-US conference

[57] Randall G. Bowdish, "The Revolution in Military Affairs: The Sixth Generation," *Military Review*, (November-December, 1995), 26. General Major V. Shipchenko, as head of the Scientific Research Department of the General Staff Academy, describes how warfare has evolved through at least five generations. The first generation involved infantry and cavalry without firearms. The second generation saw the development of gunpowder and smooth-bore weapons. Rifled small arms and tube artillery were introduced in the third generation. The fourth witnessed automatic weapons, tanks, aircraft, radio equipment and powerful means of transporting weapons. Nuclear weapons brought the fifth generation of warfare.

[58] Mary C, FitzGerald, *Orbis*, 458.

[59] Mary C, FitzGerald, *Orbis*, 458. From an interview with Defense Minister Pavel Grachev, "General Grachev on the Army and on the Soldier," *Argumenty i fakty*, (February 1993), 1-2.

on "Evolving Post-Cold war National Security Issues", V.I. Tsymbaluch indicates the strategic implication of a first strike cyberspace maneuver:

> *From a military point of view, the use of information warfare means against Russia or its armed forces will categorically not be considered a non-military phase of conflict, whether there are casualties or not ... considering the possible catastrophic consequences of the use of strategic information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces, ... Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself.*[60]

Accordingly, Russia is determined not to lag behind other nations in ushering in the "sixth generation" of warfare. Russia's doctrine demands the fielding of world-class advanced capabilities for both local and large-scale wars. On 2 November, 1993, President Yeltsin and the Security Council approved Russia's first official military doctrine: "Basic Provisions of the Military Doctrine of the Russian Federation." The new doctrine emphasized a priority for "appropriations for the most promising scientific and technological defense developments ... (including) highly efficient C^3I, strategic warning, EW, and precision non-nuclear weapons systems, as well as systems for their information support."[61] The Russian military elite argue that advanced C^3I and EW systems must

[60] Timothy Thomas, "Deterring Information Warfare: A New Strategic Challenge," *Parameters*, vol XXVI, (Winter 1996-97), 82. Citing V.I. Tsymbal, "Kontseptsiya *Informatsionnoy voyny*" (Concept of Information Warfare), speech given at the Russian-US conference on "Evolving Post-Cold war National Security Issues," (Moscow 12-14 September 1995), 7.

[61] Mary C, Fitzgerald, *Orbis*, 473. Citing "Basic Provions of the Military Doctrine of the Russian Federation", *Voennaya mysl*, (November 1993).

govern allocation of scarce defense resources. The new strategy is contrary to Gorbachev's 1987 (Soviet) "defensive doctrine". Henceforth, the new doctrine asserts that Russia's armed forces will prepare for "... both defensive and offensive operations with a massive use of existing and future weapons irrespective of how war starts and is conducted."[62] Russian analysts Yevgeniy Korotchenko and Nikolay Plotnikov conclude:

> *We are now seeing a tendency toward a shift in the center of gravity away from traditional methods of force and the means of combat toward non-traditional methods, including information. Their impact is imperceptible and appears gradually. ... Thus today information and information technologies are becoming a real weapon. A weapon not just in a metaphoric sense but in a direct sense as well.*[63]

Some commentators believe that Russia's economic climate precludes the acquisition of high-technology capabilities. However, Sergei Modestov argues in "The Possibilities for Mutual Deterrence: A Russian View," that information warfare technologies represent a relatively inexpensive strategic capability. Russia's could redress its inferiority in conventional and nuclear weapons, with information warfare weapons. Therefore capabilities for command and control, communications, intelligence and warning, electronic warfare, and special mathematical programming actions (computer viruses) is crucial to Russia's acquisition program. In short, information warfare capabilities represent a viable means to restore Russia's strategic reach and lethality and

[62] Mary C, Fitzgerald, *Orbis*, 474.

[63] Timothy Thomas, 81.

thereby provide a mechanism for deterrence.[64] Is it possible that despite a struggling economy, Russian determination and forethought could produce a first-rate strategic information warfare capability? If so, the impact on the current superpower imbalance could be profound.

A DIGITAL PEARL HARBOR:
THE CYBERSPACE VULNERABILITY OF THE UNITED STATES

Russia has clearly signalled an intention to develop both offensive and defensive information warfare capabilities. Russia's information warfare strategy should cause the United States to examine the extent that it is vulnerable to attacks through cyberspace. The United States with its high technology and economic capability has a rich array of information targets for an adversary can exploit. An adversary's targets include: telecommunications, space based sensors, communications and relay systems; automated aids to financial, banking and commercial transactions; supporting power productions and distribution systems; cultural systems of all kinds; and the whole gamut of media hardware and software that shapes public perceptions. In "A Theory of Information Warfare: Preparing for 2020", Richard Szafranski contends that "strategic information systems in states with high technomic capability oftentimes are mirrored by operational-level ones of equal complexity. All are vulnerable to attack."[65]

[64] Sergei Modestov, "The Possibilities for Mutual Deterrence: A Russian View," *Parameters*, vol. 26, no. 4, (Winter 1996-97), 97.

[65] Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal*, (Spring 1995), 62. 'Technomic' is a term used to describe a society that is reliant on the fusion of technological and economy power.

A recent RAND report for the Pentagon entitled *Strategic Information Warfare: A New Face of War,*[66] describes seven defining features of strategic information warfare for the United States. Features include low entry cost, blurred "traditional" boundaries, expanded role for perception management, a new strategic intelligence challenge, formidable tactical warning and attack assessment problems, difficulty of building and sustaining coalitions and vulnerability of the US homeland. A brief outline of this environment is shown at Figure 3. Clearly, the United States in the leading the information age has exposed numerous opportunities for a potential aggressor.

Features	**Warfare Issues**
Low entry cost.	Unlike traditional weapons and technologies, development of information-based techniques does not require sizable financial resources or state sponsorship. Information systems expertise and access to important networks may be the only prerequisites.
Blurred traditional boundaries.	Traditional distinctions - public versus private interests, warlike versus criminal behaviour - and geographic boundaries, such as those between nations as historically defined, are complicated by the growing interaction within the information infrastructure.
Expanded role for management perception.	New information-based techniques may substantially increase the power of deception and of image-manipulation activities, dramatically complicating government efforts to build political support for security related activities. In short, government propaganda can be undermined.
A new strategic intelligence challenge.	Poorly understood strategic IW vulnerabilities and targets diminish the effectiveness of classical intelligence collection and analysis methods. A new field of analysis focused on strategic IW may have to be developed.
Formidable tactical warning and attack assessment problems.	There is currently no adequate tactical warning system for distinguishing between strategic IW attacks and other kinds of cyberspace activities, including espionage or accidents.
Difficulty of building and sustaining coalitions.	Reliance on coalitions is likely to increase the vulnerbilities of security postures of all the partners to strategic IW attacks, giving opponents a disproportinate strategic advantage.
Vulnerability of the US homeland. Source: RAND	Information based techniques render geographical distance irrelevant; targets in the continental United States are just as vulnerable as the in-theater targets. Given the increased reliance of the US economy and society on a high-performance networked information infratsructure, a new set of lucrative strategic targets.

Figure 3: Cyberspace Vulnerabilities for National Security

[66] *Roger C. Molander, Andrew S. Riddle, Peter A. Wilson, Strategic Information Warfare: A New Face of War,* (Santa Monica: RAND, 1996).

Conceptually, potential adversaries could attempt to damage, destroy, or manipulate these systems using a range of information warfare techniques. The lack of redundancy in systems is of particular concern as the information age progresses. The information age is witnessing the embedding into the NII substantial information-based resources, including complex management systems and infrastructure involving the control of electric power, money flow, air traffic, oil and gas and other information dependent items. As the information age gains momentum, redundant "industrial age" systems are falling into disrepair, being dismantled, or simply forgotten. Redundancy for information age systems age are generally other computrized information systems. If primary computer systems are vulnerable, then redundancy systems of the same genre are as well. The reliance on information systems and the lack of non-information system infrastructure has led to the creation of critical vulnerabilities.

National policy-making for information warfare has not been able to keep pace with rapidly changing information technologies, systems and vulnerabilities. Policy and guidance is made after the fact and specific issues falling into the realm of information warfare are addressed in policy documents as the need arises. Consequently there is no national policy on information warfare[67] From a federal government perspective, PDD 29 created the Security Policy Board, which addresses a variety of security issues to include information systems security and risk management. Yet it is a policy advisory body and

[67] Science Applications International Corporation Report, *Information Warfare - Legal, Regulatory, Policy and Organizational Considerations for Assurance,* A Research Report for the Chief,

has no responsibility or authority to coordinate interagency agreements, resolve agreements, define strategies, or designate capabilities.

A research report prepared for the Joint Staff entitled *Information Warfare - Legal, Regulatory, Policy and Organizational Considerations for Assurance,* provides a comprehensive overview of the complexities for strategic information warfare. A complexity concerns information warfare attacks on civil information systems without any intent of disabling the military information infrastructure. It is highly likely that non-military targets linked to the NII may be the ultimate targets of information warfare actions. These attacks may be aimed at disabling economic activities, safe traffic control, power distribution, and in other ways that undermine national security. The question arises as to whether these wider defense issues are outside the purview of the Department of Defense. While there is no legislation defining responsibilities for responding to an attack against information infrastructure, the Secretary of Defense certainly has an obligation to fulfill his responsibilities to defend the United States from acts of war.

Attacks on the United States' NII should be expected. While an attack on the NII might not directly affect the capability of military hardware or war fighting capability, such an attack could invisibly (or visibly) weaken the United States without a shot being fired and without direct identification of the adversary. For example, during *Desert Storm,* the Allied forces concentrated fire power on the Iraqi NII. These attacks left Iraq blind to attack, crippled the Iraqi economy, and demoralized the nation. While Allied

Information Warfare Division (J6K), Command, Control, Communications and Computer Systems forces primarily used precision munitions to destroy the NII, similar attacks can be accomplished against the United States through electronic means.[68] On the one hand, the United States leads the world into the information age and is the first to benefit. On the other hand, information technology may become an Achilles heel for national security.

In the absence of policy direction, it is problematic for the military to adapt doctrine, force structure, and enhance capabilities to meet the new cyberspace environment. If the short-coming is policy, rather than technological capability, then the question is *what do we want our military forces of the future to do?* In terms of strategically exploiting or protecting the vulnerabilities of national information systems, the issue is unresolved. The risk is that the Government might be not be seeing bigger picture or the strategic security challenges of the information age. As Metz and Kevit opine "American leaders, in other words, must decide not only what the United States can do with a more effective military force, but what it should do."[69] Therefore the military should develop a framework and doctrine for war in cyberspace for all levels of war. As William Perry, former Secretary of Defense, alluded "We live in an age that is driven by information. Technological breakthroughs ...are changing the face of war and how we prepare for war."[70] Chapter 2 will discuss the development of a conceptual framework and doctrine for war in cyberspace at the strategic level.

Direcetorate, Joint Staff, 4 July 1995, 2-51.

[68] *Information Warfare - Legal, Regulatory, Policy and Organizational Considerations for Assurance,* 2-66.

[69] Metz, 41.

[70] Molander, 1.

CHAPTER 2

MANEUVER WARFARE IN CYBERSPACE

Warfare has indeed shifted from being a duel of strike systems to being a duel of information systems.
- Mary FitzGerald, 1994

The ubiquity of global communications has created cyberspace avenues that radiate into and out of first world countries such as the United States. Cyberspace, particularly the cyberspace networks for national and global information infrastructures, is increasingly integral to the functioning of all vital national systems These new networks have created the cyberspace battlefield. Conducting information warfare across cyberspace will not lessen the brutality of war, it simply adds a new dimension for that brutality to be played out. In short, cyberspace is a viable dimension in which to coerce an enemy and to break his will to resist. Although at this stage the concept of the cyberspace dimension transcends our traditional understanding of battlespace. Not all agree with this vision of cyberwar. Some argue that it is morally unacceptable for a military force to undertake information warfare activities during peace-time. Certainly this paradigm may have influenced the Joint Chiefs of Staff when they circumscribed the military's legitimate role in information warfare to the narrower dimensions of command

and control warfare (C^2W). Although the Air Force contends that DoD's concept of C^2W is focused at the operational level and ignores the strategic level of armed conflict.[71]

This chapter argues that warfare in cyberspace should be embraced as "an act of force, (where) there is no logical limit to the application of that force."[72] This vision of using force in cyberspace requires a conceptual framework and doctrine to become reality.[73] Unfortunately there is no official information warfare doctrine.[74] To help close this doctrinal hiatus, this chapter intends to illustrate how maneuver warfare theory might be adapted to the cyberspace environment with devastating effect. It also reinforces the previous chapter's argument that cyberspace represents a threat to national security.

***SOFT KILLING* THE ENEMY IN CYBERSPACE**

In a 1992 RAND paper entitled *Cyberwar is Coming!*, John Arquilla and David Ronfeldt identified the need for the development of new doctrine to coincide with the emergence of the cyberspace dimension. The report focused on warfare in the battlefield environment and in particular *Force XXI Operations*.[75] The call for a new doctrine,

[71] Alan D. Campen, "Assessments Necessary in Coming to Terms with Information War," *Signal*, (June 1996), 47. Referring to an Air Force document entitled "Cornorstones of IW".

[72] Carl von Clausewitz, *On War*, ed. and trans. Micheal Howard and Peter Paret, (New Jersey: Princeton University Press, 1984), 77.

[73] After doctrine, organisational setup and equipment acquisition can occur, and together these activities will eventually produce a viable strategic capability for maneuver in cyberspace.

[74] Stein 37. In 1995 Stein wrote that C^2W doctrine remains incomplete. A joint publication is currently being prepared for Information Warfare, but at this stage the author has not seen the draft. It therefore remains to be seen if the new joint publication addresses the issue of strategic information warfare and accordingly assigns responsibilities and tasks.

[75] John Arquilla and David Ronfeldt, *Cyberwar is Coming!*, (Santa Monica: RAND P-7791, 1992), 7.

however, should also be applied to the strategic level of war. New doctrine should evolve as an extension to existing maneuver warfare theories.

Maneuver warfare theory has evolved through the writings of theorists such as Sun Tzu, Clausewitz, Liddell Hart, J.F.C. Fuller, and more recently William Lind. Maneuver theory is "... a way of fighting smart, of out-thinking your opponent that you may not be able to over power with brute strength ... being consistently faster through however many OODA (Observation-Orientation-Decision-Action) loops it takes until the enemy loses cohesion - until he can no longer fight as an effective, organized force."[76] Maneuver warfare theory does not provide absolute maxims for the successful conduct of war or to provide a formula for victory. Instead, maneuver warfare is the process of, as defense consultant Edward Luttwak writes, "seeking to destroy the enemy's physical substance, the goal is to incapacitate by *systematic* disruption."[77] Lind theorizes that maneuver warfare is "a thought process which seeks to pit strength against weakness to break the enemy's will."[78] The aim of warfare is not necessarily to kill the enemy, in fact, the "acme of skill" is to subdue an adversary without killing.[79] In a philosophical sense, it appears that cyberspace is fertile ground to apply force, out-wit the enemy, and use coercion without necessarily killing. The most effective way to think about applying force, is to understand cyberspace through its connectivity with strategic systems and subsystems.

[76] William S. Lind, *Maneuver Warfare Handbook*, (London: Westview Press Inc, 1985), 2-6.

[77] Richard D. Hooker, ed., *Manuever Warfare: An Anthology*, (Novato CA: Presido Press, 1993), 21.

[78] Hooker , 185.

In the *Airpower Journal* article "The Enemy as a System," Colonel John Warden opined "As strategists and operational artists, we must rid ourselves of the idea that the central feature of war is the clash of military forces [and] if we are going to think strategically, we think of the enemy as a system composed of numerous subsystems."[80] Thinking of the enemy as a system is the basis to understanding how cyberspace might be exploited for warfare. Warden's simplistic Five Ring model was developed in order to create a conceptual framework of an enemy system for use in planning a strategic air offensive. The model is not mechanistic, but merely offers a platform to understand how to go about attacking a strategic center of gravity and thereby destroy an enemy's will and capacity for war. In this context: "Strategic war is war to force the enemy state or organization to do what you want it to do. In the extreme, it may even be a war to destroy the state or organization. It is, however, the *whole system* that is our target, not its military forces."[81] For instance, an attack on a strategic center of gravity with "electronic fires" through cyberspace might be conducted in conjunction with other attacks on the operational level center of gravity with traditional warfare methods.

Warden's Five-Ring model can be used for planning a strategic offensive or defensive information warfare campaign at the strategic level (Figure 4). An important caveat is the limitation of planning cyberspace maneuver in unsuitable environments. While the effects of information warfare could be devastating in information technology reliant countries such as the United States, Australia and Britain; conversely the effects

[79] Sun Tzu, *The Art of War*, trans. by Samuel B. Griffith, (New York: Oxford University Press, 1971), 77.

[80] John A. Warden III, "The Enemy as a System," *Airpower Journal*, (Spring 1995), 42.

could be negligible against agrarian countires like Vietnam or newly industrialising countries like China. In this regard Warden's model has been criticized as being too mechanistic and leads planners into over-estimating the strategic effects on an adversary's war capacity and will.[82] Nevertheless, the model can be used as a framework for understanding the direct and indirect consequences for the use of force, in conventional or information warfare, to attack a strategic center of gravity.

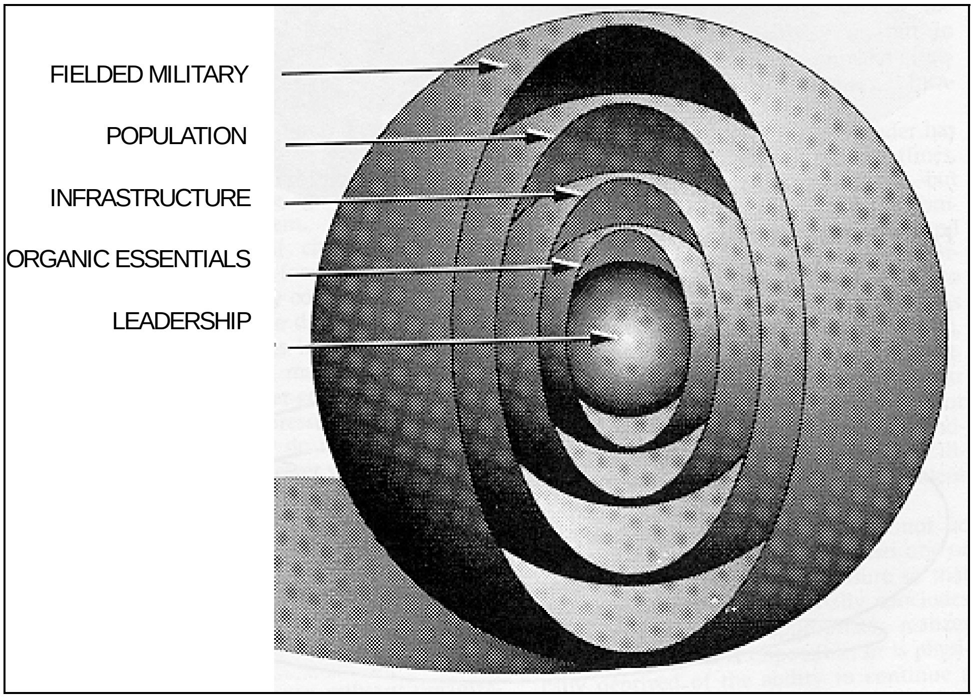


Figure 4: **Warden's Five Ring Model**

The national command element, or leadership ring, is the most important element because it is responsible for effective operation and coordination of other systems to

[81] Warden, 47.

achieve national goals. Information warfare attacks on the outer rings and subsystems can manipulate, distract, overload and even overwhelm the ladership's stability. Information warfare can also be used to create an impression that the national command element is out of control. A myriad of attacks through cyberspace might result in *command paralysis*.

The second ring represents the organic essentials of the state. Essential industries and services form the productive capacity of a state for self-sustainment and growth. Precise attacks on these systems would significantly impair the military capacity of an adversary. In *Strategic Assessment 1996: Instruments of US Power*, the Institute for National Strategic Studies reports "the hot button issue of information warfare is an attack on the nation's commercial computer systems - telecommunications, power, banking, safety systems."[83] The second ring's reliance on information technology is increasing due to the expanding GII and therefore assummes greater importance as a critical vulnerability.

The third most critical ring is the infrastructure. It includes such assets as the transportation and communications systems. Penetration of information age technologies

[82] Stein, 38. Stein argues that the doctrine as presented in Air Force Manual (AFM) 1-1, *Basic Aerospace Doctrine of the United States Air Force*, could be used as a template to start thinking about information warfare.

[83] INSS, *Strategic Assessment 1996: Instruments of US Power*, 195.

in these subsystems has been profound and their impact continues to grow. A notable trend is the dismantling of redundancy mechanisms to keep vital national systems operating when the computerized system fails. Economic analyst Joseph Schumpeter forecast how industrial age redundancy mechanisms will continue to disappear in his "gales of creative destruction" thesis. Schumpeter explained that new systems and technology not only replace the old, they destroy them and this is a characteristic of American capitalism.[84] Therefore in destroying or weakening a computerized subsystem, the potential exists to completely deny a nation of a particular range of capabilities. For instance, an attack through cyberspace could neutralize both the computerized air traffic control subsystem and its computerized back-up. The entire air transportation industry in the United States would grind to a halt because a manual back-up system to control the airspace no longer exists.

The fourth ring is the population, the very basis for the moral cause of a nation in a conflict. Early theorists such as Giulio Douhet thought that wars could be won by inflicting such casualties on the civilian population that morale would break with subsequent capitulation. Although, in the Second World War there was no catastrophic collapse of morale in Britain or Germany leading to capitulation, the Japanese leadership did capitulate because of effective nuclear and fire-storm bombing. Attacks across

[84] Woodall, 8. In the 1930s, Schumpeter explained economic growth primarily in terms of technological innovation. Capitalism moves in long waves of 50 yearsor so and technological revolutions caues "gales of creative destruction" in which old industries are swept away by new ones."

cyberspace might not cause national morale to collapse, but attacking vital subsystems could weaken morale and thereby divert the attention of national leadership and degrade wartime productivity. For example, corruption or destruction of the United States' social security subsystem, or manipulation of the tax, or personal financial records could cause individual stress for tens of millions. An aggressor could by-pass information barriers in other countries and directly address a nation's citizens. The Internet is one such cyberspace network for disseminating information. With the impending proliferation of satellites, there is also relatively low cost access to global broadcasts and news. The potential to spread misinformation and propaganda will increase dramatically.

The last ring is the fielded military of the state. Military systems are designed for operational useare difficult to penetrate. Generally these systems are independent from public systems and therefore less vulnerable to attack. An aggressor could, however, attack computer systems governing logistics and maintenance through their links to civilian contractors' and suppliers' networks. Attacks through cyberspace could disrupt the military's deep-maintenance, manpower mobilization, logistics preparations, and even morale -- by focusing attacks on the families of servicemen who are engaged in operations.

The central thrust of Warden's Five-Ring model is that "it is imperative to remember that all actions are aimed against the mind of the enemy command or against the enemy system as a whole."[85] Maneuver in cyberspace presents the warfighter with the

[85] Warden, 51.

opportunity to use the concept of parallel attack rather than simply engage in serial attack. Serial attack is the old fashioned ebb and flow of battle. It is a linear concept where two adversaries engage in a series of attacks and counter attacks. In parallel attack, the point of attack is against multiple targets and the effects are non-linear. Parallel warfare might include simultaneous attacks at the strategic and operational level, maneuvering offensive capabilities across the land, sea, air, and cyberspace. Such attacks could be coordinated against the enemy's "five rings" of power with devastating effect. Maneuver in cyberspace increases the potential and opportunities to employ parallel blows and unexpected actions to shatter the enemy's cohesion and create a turbulent and deteriorating situation with which enemy leadership cannot cope. Maneuver warfare in cyberspace at the strategic level offers a means to achieve such an outcome.

If this is the case, then information warfare attacks should not be viewed as equating to a few hackers trying to penetrate an enemy system. This perception of information warfare would be akin to a single bomber attacking the enemy's capital. Instead, information warfare attacks should be conducted with massive force, if necessary by tens of thousands of hackers, something equivalent to a "thousand bomber" raid. Such attacks might be conducted for months or years to destroy the enemy's strategic center of gravity.

While the thrust of Warden's Five-Ring model lends itself to warfare at the higher end of the spectrum of conflict, it is also appropriate for the lower end of the spectrum. Martin van Creveld, in *Transformation of War*, contends that future war will not be a relatively simple high-tech conventional war, but rather extremely complex low-intensity conflict. Van Creveld states that war will turn to the complex environment because "computers have come to dominate the relatively simpler environments of mid- to high intensity conflict."[86] Aggressors without access to traditional weapons might increasingly use cyberspace as a way to achieve objectives. Cyberspace cam be used by terrorists, criminals and other non-state insurgents to undermine government authority, create mayhem, gain notoriety, or cause damage and casualties. Information warfare could very quickly emerge as a feature of low intensity warfare. In certain circumstances information warfare should be included as a category of OOTW.[87]

TECHNIQUES AND WEAPONS FOR CYBER WAR

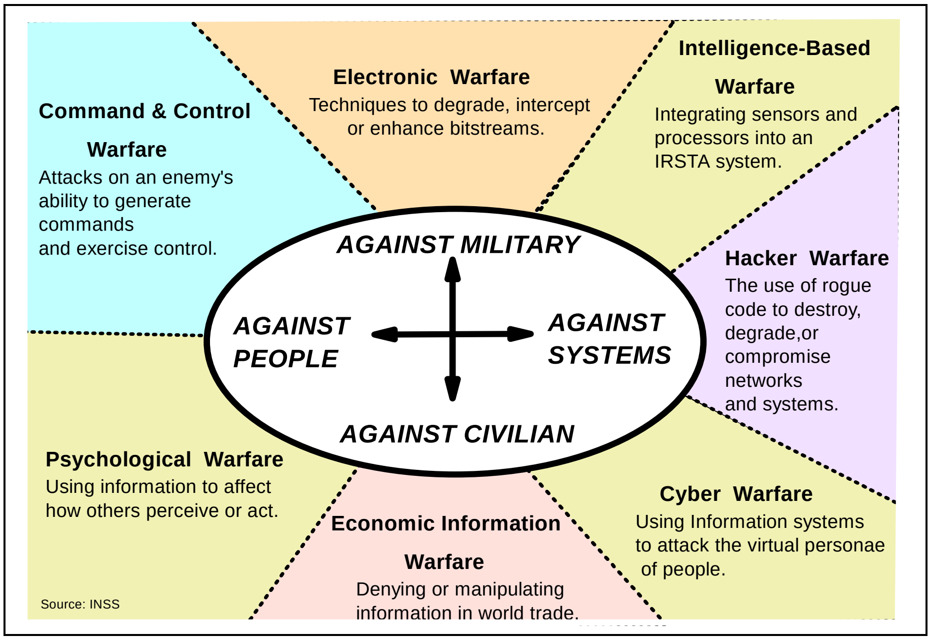
If the United States could manipulate an adversary's (either state or non-state) computer systems, it might achieve an advantage similar to neutralizing an enemy's command, key war-time industries, transportation, communications, and ultimately national resolve. However, since potential adversaries range from cyberspace deficient to cyberspace dependent, the value of targeting information systems varies greatly. The circumstances of the conflict will influence how the systems are attacked. For instance, force could be used in either a gradual way; a tap here and there to gently coerce a nation; or if required, harder hits could be employed to bludgeon a nation into submission.

[86] Thomas X. Hammes, "The Evolution of War: The Fourth Generation," *Marine Corps Gazette*, (September 1994), 37.

[87] Report of the Senior Working Group on Military Operations Other Than War (OOTW), May 1994, Advanced Research Projects Agency did not include information warfare or cyberspace manipulation in the spectrum of OOTW, whereas the criteria used for assessing the characteristicss of OOTW are pertinent to aggressive activities by states using the cyberspace dimension. Is a paradigm shift for OOTW required as a result of the information age?

Different environments and varying desired outcomes require a range of techniques and weapons to be available to the cyberspace warrior.

The Institute for National Strategic Studies (INSS) has the most refined conceptual overview of the techniques and targets available to assist planning a campaign in cyberspace.[88] A schematic overview of the techniques for information warfare is at Figure 5. In planning the cyber campaign, consideration will be given to which technique, or combination of techniques, are appropriate for the desired outcome. Both weapons (such as computer viruses) and techniques (such as economic information warfare) will be the tools of trade for the cyberwarrior.


Electronic Warfare
Techniques to degrade, intercept or enhance bitstreams.
Intelligence-Based Warfare
Integrating sensors and processors into an IRSTA system.
Command & Control Warfare
Attacks on an enemy's ability to generate commands and exercise control.
AGAINST MILITARY
AGAINST PEOPLE
AGAINST SYSTEMS
AGAINST CIVILIAN
Hacker Warfare
The use of rogue code to destroy, degrade,or compromise networks and systems.
Psychological Warfare
Using information to affect how others perceive or act.
Cyber Warfare
Using Information systems to attack the virtual personae of people.
Economic Information Warfare
Denying or manipulating information in world trade.

Source: INSS

***Figure 5*: Information Warfare Chart**

[88] Also see Martin C. Libicki, *What is Information Warfare*; and INNS Report, 94; and *Information Warfare - Legal, Regulatory, Policy and Organizational Considerations for Assurance*, 2-63 to 2-68.

A comprehensive overview of the weapons to manipulate cyberspace is provided by Peter Denning in *Computers Under Attack: Intruders, Worms and Viruses*.[89] It is not the intention of this paper to elaborate on the extensive technical aspects, suffice it to say that there are two attack modes; inside or outside paths. The inside path of attack includes inserting bad hardware or software components at the source. This mode requires the cooperation or unintentional compliance of insiders. Outside paths refer to unauthorized access over external routes, such as phone or Internet networks. This mode of attack could manipulate or steal individual files, or manipulate the files that make the system run. *Intruders, worms,* and *viruses* represent some of the weapons used in a duel across cyberspace.

Arquilla and Ronfeldt in their article "Cyberwar is Coming" theorize that "the information revolution will cause shifts, both in how societies may come into conflict and how their armed forces may wage war." They made a distinction between "netwar" for "societal-level ideational conflict" waged in part through "internetted" modes of communication and "cyberwar" for military conflict.[90] Their concept of "netwar", when combined with Warden's model of national power, offers insights into how cyberspace might be used for maneuver warfare. Arquilla and Ronfeldt explain that:

[89] Peter Denning, *Computers Under Attack: Intruders, Worms and Viruses*, (New York: ACM Press, 1990).

[90] Arquilla and Ronfeldt, "Cyberwar is Coming," *Comparative Strateg*y, vol. 12, (November 1993), 141-165.

> *Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population knows or thinks it knows about the world around it. A netwar may focus on public or elite opinion, or both. It may involve public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception or interference with local media, infiltration of computer networks and databases, and efforts to promote dissent or opposition movements across computer networks. Thus designing a strategy for netwar may mean grouping together from a new perspective a number of measures that have been used before but were viewed separately ... In other words, netwar represents a new entry on the spectrum of conflict that spans economic, political and social, as well as military forms of "war".*[91]

Importantly in this context, reference is made to warfare in cyberspace as a new and distinct form of economic, political, social, and military mode of warfare.

A feature of maneuver warfare in cyberspace is the potential for strategic first-strike. Andrew Krepinevich, as head of the Defense Budget Project, predicted that "just as we think about initial strikes on airfields and transportation to achieve air superiority, we'll now think about electronic strikes designed to foul up an enemy's ability to communicate, to coordinate, to move information and organize operations. The conflict may actually start with imbedding things like computer viruses in the other side's information system. We will be at war for days before the other side realizes it."[92] This first strike environment for information warfare is reminiscent of the nuclear first strike potential and strategic dilemmas of the Cold War.

By applying the principles of maneuver warfare an aggressor could manipulate national assets and power; conduct a information warfare campaign at the strategic level

[91] Arquilla and Ronfeldt "Cyberwar is Coming," *Comparative Strateg*y, 141-165.

in conjunction conventional operations; and gain an initial advantage by employing first-strike against a range of vital systems. However, to recognize the potential for warfare in cyberspace, the military needs to redefine its understanding of battlespace and its paradigm for the strategic, operational, and tactical levels of war.

REDEFINING BATTLESPACE FOR CYBER MANEUVER

A new paradigm for battlespace is required in order to adapt the concept of maneuver warfare in cyberspace. Until recently, the definition of battlespace has proven adequate for maneuver warfare in the three dimensional physical battlespace. The Army's Field Manual 100-5, *Operations*, defines battlespace as "a physical volume that expands or contracts in relation to the ability to acquire and engage the enemy."[93] The definition ignores the electromagnetic spectrum. A more inclusive definition is provided in Army Pamphlet (DA Pam) 525-5, *Force XXI Operations* for battlespace where "components of this (battle)space are determined by the maximum capabilities of friendly and enemy forces to acquire and dominate each other by fires and maneuver and in the electromagnetic spectrum."[94] Naval doctrine embraces this broader definition of battlespace in Naval Doctrine Command's publication *Naval Warfare*.[95]

[92] Dan Cordtz, "War in the 21st Century: The Digitized Battlefield," *Financial World,* (29 August, 1995), 48.

[93] US Army, Field Manual (FM) 100-5, *Operations*, Washington DC: Headquarters Department of the Army, June 1993**)**, 6-12.

[94] US Army Pamphlet 525-5, *Force XXI Operations* (Fort Monroe, VA: US Army Training and Doctrine Command, 1 August 1994), Glossary -1.

[95] Naval Doctrine Command, NDP-1, *Naval Warfare* (Washington: GPO, 1994), 72.

In the information age there will be a merging of the physical and non-physical elements of battlespace and cyberspace will become a distinct dimension for warfare in its own right. Previously, cyberspace was considered as an adjunct to the traditional dimensions of land, sea, air and space. Figure 6 shows how this new concept might be envisaged (noting that the diagram is not a proportional representation).

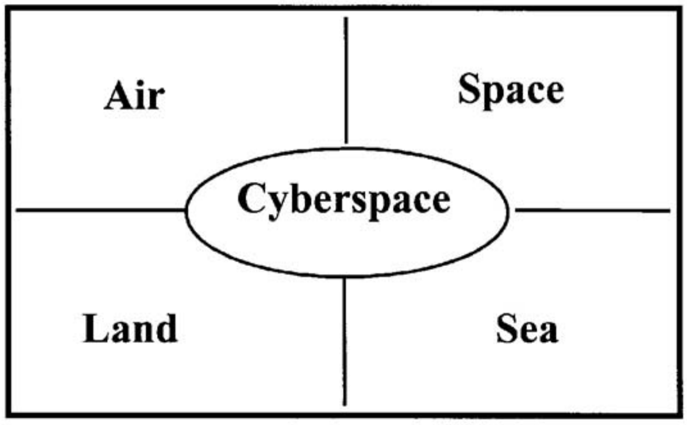


Figure 6: **Five Dimensions for Maneuver Warfare**

In cyberspace the maximum capability for maneuvering force is not defined by physical mass. The effect of the cyberspace dimension is to increase, almost without limit, the proportions of the modern battlespace. Cyberspace changed the environment for warfare because it profoundly reduces the distance between the forward area of operations and continental bases. For instance, the United States' preparation for deployment of combat units and logistic support from CONUS can be interdicted by an enemy maneuvering through cyberspace. In cyberspace, there is no longer a differentiation between forward deployed areas, intermediate areas, and CONUS. Strategic information warfare is likely to transcend a unified command's (CinC) geographic boundaries, hence confusing the national command and control structure.

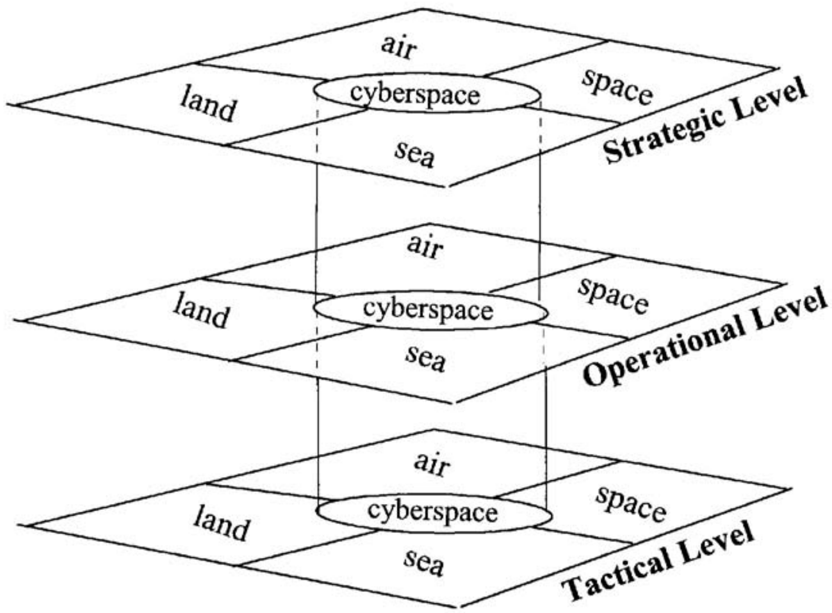


***Figure 7*: Cyberspace Compression of Levels of War**

Disabling enemy systems by targeting key nodes, or frustrating vital subsystems by using soft kill techniques, might be frustrated by the difficulty of identifying exactly how information systems are connected. There is a considerable difference between destroying an individual target and destroying a system. At this stage much of the cyberspace dimension is invisible. It is also rapidly changing. Like terrain, cyberspace should be mapped. Dynamics such as cyberspace highways, systems, subsystems, gates, barriers, node points, choke points all need to be mapped. Such maps provide the vital intelligence for campaign planning. An aggressor, for instance, could manipulate certain companies in a stock market, say London, which could cause considerable angst in the United States. Having the cyberspace maps showing the connectivity between systems, and understanding the nature of causality in cyberspace, will be the key to gaining dominance in this dimension.

In conclusion, warfare in cyberspace should be viewed as a means to destroy the enemy's center of gravity with massive force. The opportunity has arisen because the information age has created critical strategic vulnerabilities. War will increasingly be a struggle between information systems and forces dominating cyberspace have a distinct advantage in imposing their will on an adversary. However, the concept of maneuver warfare in cyberspace is not one of singularity because conflict will still encompass all forms of war. The real power of exerting force on an adversary through cyberspace is its combined effect with the application of force in the conventional dimensions of land, sea, and air. Changing our way of thinking about cyber warfare will be the first step to developing doctrine, strategy, and capability. Foremost in changing our military paradigms will be a redefinition and new understanding of battlespace in the information age.

CHAPTER 3

CONCLUSION: REALITY, THEORY AND NEXT STEPS

> *In the information age, enemies can violate the comforting national security sanctuary of time and distance instantly, anonymously and with impunity. Fundamental personal, economic and national security ride on what the United States does - or does not do - to prevail in conflict in this era.*[96]
>
> \- Alan Campen, 1996

This paper revealed the "double-edged" nature of cyberspace for countries increasingly reliant on information age technologies to support their economy and underpin their computer dependent society. For instance, while information technology is rapidly becoming the mainstay of economic and military power for the United States, it also exposes an Achilles heel for national security. In essence, the paper explored the nexus between reality and theory. It found that military paradigms, strategies, and capabilities need adjustment if the United States is to prepare for warfare in the information age, particulary at the strategic level. This paper will conclude by summarizing its main findings and suggesting areas for further discussion and analysis.

[96] Campen, 47.

On Reality

Chapter 1 explored the strategic implications of the emerging information age. Overall, analysis reveals a slowly but dramatically changing environment which demands a shift in national security and military strategies. The reality is:

- The information age is will yield multi-dimensional changes to the economy, society, and warfare over the longer term. National centers of gravity and critical cyberspace vulnerabilities will emerge as a new technological and economic environment takes shape. Concomitant adjustment of strategic defense priorities are required.
- RMA theorists have appropriately anticipated opportunities to enhance operational and battlefield capabilities through cyberspace. However, the broader strategic security implications are underestimated. Opportunities for war on a grand scale in cyberspace have largely been ignored. A new vision of strategic warfare across the cyberspace dimension is required as a precursor to development of appropriate strategic capabilities. Underestimation of the impending strategic environment is also reflected in national security and military strategies.
- Analysis of Russia's response to the information age illustrates how the new environment is a global concern. The fundamental changes in strategy and capability development indicate that Russia is planning to exploit grand scale information age opportunities. If successful, Russia could gradually challenge

the United States' sole position as a military superpower. China and other nations might adopt similar policies to Russia.

- The "bandwidth" problem for warfare across the agrarian, industrial and informational spectrum should be addressed in the *National Military Strategy* and *Joint Vision 2010*.
- Economic, social, and political disorder might be created as a result of the dynamics of the information age. Such an environment will witness the military increasingly engaged in unfamiliar forms of OOTW. At a minimum, military doctrine for OOTW should identify the military's role if cyberspace is used for low level conflict by state and non-state aggressors.
- The increasing vulnerability of national information systems creates a conundrum for national security. The issue has not been addressed in the published national security and military strategies or by establishing a lead authority to control and coordinate interagency policies and strategies. There will be no real progress in strategic information warfare until these issues are addressed.

On Theory

Doctrine for strategic warfare in cyberspace is nonexistent, (although Joint C^2W doctrine for the operational and tactical level has been published)[97]. The strategy on how to defend the United States' information infrastructure is in a state of flux.[98] The two

[97] See Glossary.

[98] INSS, 196.

conditions are linked; for there can be no cogent strategy for defense without first establishing a doctrine. Chapter 2 discussed how the military could develop a conceptual framework and doctrine for fighting in cyberspace. Chapter 2 theorized:

- The first step is to accept warfare in cyberspace in a Clausewitzian Trinitarian sense. All *War* involves a fusion of forces - rational (leadership), irrational (people) and non-rational (military) forces. There should be neither legal, moral, nor logical impediments to the military engaging and preparing for warfare in cyberspace.
- Second, the physical and non-physical characteristics of cyberspace make maneuver warfare theory an appropriate model for planning a cyberbattle or campaign. One of the major difficulties will be target selection not only to kill or soft-kill an enemy, but to achieve the desired outcome of breaking the enemy's will. Adaptation of Warden's five ring model and *Basic Aerospace Doctrine of the United States Air Force,* when combined with maneuver theory, and a new pardigm for battlespace, represent an appropriate starting point for learning how to systematically attack the enemy as a system through cyberspace. Over time, and with experience, the doctrine for information warfare will evolve in its own right.
- Third, understanding the weaponry and techniques to be used across cyberspace is essential. The military must develop an expertise in cyberspace weaponry in the same professional manner that other weapon systems are

employed. Progress being made by the Institute for National Strategic Studies for developing techniques for information warfare should be encouraged.

- Fourth, critical to maneuver is an understanding of the terrain or battlespace. Maneuver warfare in cyberspace is set to challenge our traditional understanding of battlespace and the paradigm for levels of war. Increased connectivity at all levels of war, and the ability of actions in cyberspace to instantaneously cut across vast distances, requires a rethinking of command and control doctrine .

On Next Steps

Finally, this paper proposes a three tier strategy for preparing an offensive and defensive capability to allow maneuver warfare in cyberspace. Broadly, the three tiers are first, establish top leadership to promote and coordinate change; second, develop and articulate national security and military strategies for strategic information warfare and define the requirements for offensive and defensive capabilities; and third, define the role and responsibilities for the military and other agencies in the information warfare environment.

The decision to pursue information warfare or develop information weapons is a national leadership decision. Strategic analysts widely agree that an immediate and vital first step is the assignment of a focal point in the federal government leadership to coordinate the United States' response to the strategic information warfare threat. The focal point should be at the highest level, even Cabinet level, since only in this forum can necessary interdepartmental and interagency coordination be undertaken. Capability funding is paramount, so Congress will be a vital component in all aspects of strategic information warfare development.[99] The overarching office should also have the responsibility for the close coordination with industry, since the United States' information infrastructure is being developed almost exclusively by the commercial sector. Once established, this high-level leadership should immediately take responsibility for initiating and managing comprehensive implementation of national-level strategic information offensive and defensive capabilities.

The NSS needs to address the appropriate level of preparedness for strategic information warfare. This requires an ongoing risk assessment to determine the degree of threat and vulnerability. A RAND report asserts that without an immediate risk assessment there is no sound basis for presidential decision-making on strategic information warfare matters.[100] Comprehensive strategies need to be formulated as a response to the threats and vulnerabilities. Strategies will also need to be in place to ensure that investment in and employment of offensive strategic warfare capabilities is controlled. This might require a specialized and permanent organization with both analytical and executive functions.

The United States military has a dilemma because it has not embraced the information warfare concept at the strategic level of war. Rather than face the broader complexities of information warfare, the DoD has accepted a narrower role for itself. The dilemma is whether Defense should accept an expanded role for strategic information warfare or continue with a narrower (operational) role. Traditionally the task

[99] Szafranski, 64.

of war-fighting has always been the responsibility of the uniformed services, in particular the unified commands. Two key questions arise. Should defensive strategic information warfare be assigned as a civil defense issue or a military issue? Moreover, should the capability for offensive strategic information warfare be a State Department function or reside with the Department of Defense? In January 1995, the Secretary of Defense created the Information Warfare Executive Board to facilitate "the development and achievement of national information warfare goals."[101] Perhaps this might be a step towards Defense assuming a broader role for strategic information warfare, both in its offensive and defensive forms.

Finale

Information warfare doctrine, strategy and capabilities need to be developed if the opportunities and threats created by the cyberspace environment are to be controlled. Above all, investigating new ways of using cyberspace as a means to impose our will on an adversary must be ingrained in military thinking for all levels of war-- strategic, operational and tactical. The desired outcome is to anticipate changes in the character of war and gain an unassailable lead in preparedness for information warfare. This course of action would evoke the very essence of Sun Tzu's axiom:

> *He who excels at resolving difficulties does so before they arise.*
> *He who excels in conquering his enemies triumphs before threats materialize.*[102]

[100] *Molander,* 8.

[101] *Molander,* 2.

[102] Sun Tzu, 77. (Tu Mu's interpretation)[103]Schwartau, 327.

GLOSSARY -
INFORMATION WARFARE & CYBERSPACE

Information warfare and cyberspaceare interdependent concepts. Joint Publication 3-13.1, *Joint Doctrine for Command and Control Warfare (C^2W)* defines information warfare as:

> *Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based prcesses, information systems, and computer-based networks.*

Information warfare is sometimes erroneously referred to as command and control warfare (C^2W). Doctrinally C^2W is undertaken at the operational level ad aims to use "operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), 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 form such actions." In theory, information warfare actually is a much larger set of activities aimed at the mind and will of the enemy.

Cyberspace, as described by Winn Schwartau in *Information Warfare - Chaos of the Information Superhighway,* is the network through which computers are linked. Cyberspace can be a network of just two computers or, at the other end of the scale, the entire global network of computers and pathways. The global network can be thought of as " divided into groups of local or regional cyberspace - hundreds and millions of smaller cyberspaces all over the world."[103] In Schwartau's concept of cyberspace, there are no national or regional boundaries to inhibit anyone from communicating across the network. Schwartau states that cyberspace has two constituents:

> *1. Personal, corporate, or organizational ("small-c") cyberspaces. The doors to these cyberspaces are the electronic borders by which we can specify the location of an individual cyberspace. The doors of these cyberspaces open up onto the information highways.*
> *2. The information highways and communications systems, including the National Information Infrastructure. These are the threads that, tied together, make ("big-C") Cyberspace.*[104]

Cyberspace, in brief, is that physical and non-physical dimension across which computers process and transmit information. The world's communications network of wires, fibers, microwave and satellite transmissions are the superhighways connecting cyberspace. Various forms of information warfare can be undertaken using the cyberspace dimension. "Information" is the message, while cyberspace is the dimension in which the message is lodged, retained, transmitted or manipulated.

[104] Schwartau, 329.

BIBLIOGRAPHY

I. Government Policy Documents

Gore, Al. *Global Information Infrastructure: Agenda for Cooperation*. Washington DC: US GPO, January 1995.

Gore, Al. *Creating a Government that Works Better and Costs Less: Reengineering Through Information Technology*. Washington DC: US GPO, September 1993.

A National Security Strategy of Engagement and Enlargement. Washington DC: US GPO, February 1996.

National Military Strategy of the United States of America. Washington DC: US GPO, 1995.

II. Government and Departmental Sponsored Reports

The RAND Corporation. National Defense Research Center. Report to Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence). *Strategic Information Warfare: A New Face of War.* Santa Monica: RAND, 1996.

Defense Science Board 1996 Summer Study Task Force. *Tactics and Technology for 21st Century Military Superiority.* vol. 1, Final Report, Office of the Secretary of Defense, Pentagon, Washington DC, October 1996.

Science Applications International Corporation. *Information Warfare - Legal, Regulatory, Policy and Organizational Considerations for Assurance.* A Research Report for the Chief, Information Warfare Division (J6K), Command, Control, Communications and Computer Systems Direcetorate, Joint Staff, 4 July 1995,

Advance Research Projects Agency. *Report of the Senior Working Group on Military Operations Other Than War (OOTW).* May 1994.

US Department of Commerce. *The Global 2000 Report to the President of the US: Entering the 21st Century*. Vol. : The Summary Report, Gerald O. Barney ed., New York: Pergaman Press, 1980.

The National Research Council. US Department of Commerce. *Growing Vulnerability of the Public Switched Networks: Implications for National Security*. Washington DC: National Academy Press, 1989.

Office of the Manager, National Communications System. *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications, An Awareness Document*. Arlington, Virginia, 5 December 1994.

Institute for National Strategic Studies. *Strategic Assessment 1996: Instruments of US Power*. Washington DC: National Defense University Press, 1996.

III. Military Publications

Department of Defense. "Joint Vision 2010: America's Military Preparing for Tomorrow," *Joint Force Quarterly*, Summer 1996.

Department of Defense. Joint Publication 3-13.1, *Joint Doctrine for Command and Control (C2W*). 7 February 1996. Joint Electronic Library CD-ROM, September 1996.

Department of Defense. Naval Doctrine Command, NDP-1, *Naval Warfar*e. Washington DC: GPO, 1994.

Department of Defense. US Army, Pamphlet 525-5, *Force XXI Operations*. Fort Monroe, Virginia: US Army Training and Doctrine Command, 1 August 1994.

Department of Defense. US Army, Field Manual (FM) 100-5, *Operations*. Washington DC: Headquarters Department of the Army, June 1993**.**

Department of Defense. US Air Force, Air Force Manual (AFM) 1-1, *Basic Aerospace Doctrine of the United States Air Force*.

IV. Books

Arquilla, John and David Ronfeldt. *Cyberwar is Coming!* Santa Monica: RAND P-7791, 1992.

Bracken, Paul and Raoul Alcala. *Whither the RMA: Two Perspectives on Tomorrow's Army*. Pennsylvania: Strategic Studies Institute, US Army War College, 22 July 1994.

Clausewitz, Carl von. *On War*. ed.and trans. Micheal Howard and Peter Paret. New Jersey: Princeton University Press, 1984.

Creveld, Martin van. *Technology and War - From 2000 BC to Present*. New York: The Free Press, 1989.

Creveld, Martin van. *Technology and War*. New York: The Free Press, 1991.

Denning, Peter, ed. *Computers Under Attack: Intruders, Worms, and Viruses*. NASA Ames Research Center. New York: Addison-Wesley, 1990.

Hooker, Richard D., ed. *Manuever Warfare: An Anthology*. Novato CA: Presido Press, 1993.

Johhnson, Stuart E.and Martin C. Libicki, eds. *Dominant Battlespace Knowledge: The Winning Edge.* Washington DC: National Defense University Press, 1995.

Kennedy, Paul. *The Rise and Fall of Great Powers*. New York: First Vintage Books, 1989.

Libicki, Martin C. *What is Information Warfare*. Washington DC: National Defense University, October 1995.

Lind, William S. *Maneuver Warfare Handbook*. London: Westview Press Inc., 1985.

Massie, Robert K. *Dreadnought:Britain,Germany, and the Coming of the Great War*. New York: Ballantine Books, 1991.

Rinaldi, Steven M. *Beyond the Industrial Web: Economic Synergies and Targeting Methodolgies.* Maxwell, Alabama: School of Advanced Airpower Studies, April 1995.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighwa*y. New York: Thunder's Mountain Press, 1995.

Sullivan, Gordon R. and James M. Dubik *War in the Information Age*. Pennsylvania: Strategic Studies Institute, US Army War College, 6 June 1994.

Sun Tzu. *The Art of War*. Trans. by Samuel B. Griffith. New York: Oxford University Press, 1971.

Toffler, Alvin and Heidi Toffler. *War and Anti-War*. Boston: Little Brown, 1993.

Toffler, Alvin. *Powershift: Knowledeg, Wealth, and Violence at the Edge of the 21st Century*. New York: Bantam, 1990.

Toffler, Alvin. *The Third Wave*. New York: Bantam Books, 1980.

V. Journal and Periodical Articles

Arquillia, John and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy*, 12, Spring 1993.

Bowdish, Randall "The Revolution in Military Affairs: The Sixth Generation." *Military Review*, 75, November-December 1995.

Bunker, Robert J. "Advanced Battlespace and Cybermaneuver Concepts: Implications for Force XXI." *Parameters US Army College Quarterl*y, Vol. XXVI, no. 3, Autumn 1996.

Bunker, Robert J. "The Transition to the Fourth Epoch." *Marine Corps Gazette*, September 1994.

Bunker, Robert J. "The Tofflerian Paradox." *Military Review*, May-June 1995.

Cohn, Eliot, "What to Do about National Defense." *Commentary*, 98, 5 November 1994.

Campen, Alan D. "Assessments Necessary in Coming to Terms with Information War." *Signal*, June 1996.

Fitzgerald, Mary C. "Russia's New Military Doctrine." *Naval War College Review*, 46, Spring 1993.

Fitzgerald, Mary C. "The Russian Military Strategy for 'Sixth Generation' Warfare.' *Orbis*, 38, Summer 1994.

Fitzgerald, Mary C. The Russian Image of Future War", *Comparative Strategy*, 13 April-June 1994.

Golden, James R. "Economics and National Strategy: Convergence, Global Networks, and Cooperative Competition," in *New Forces in the World Economy*, ed. B. Roberts, Cambridge, Massachusetts: The MIT Press, 1996.

Hammes, Thomas X. "The Evolution of War: The Fourth Generation." *Marine Corps Gazette*, September 1994.

Harknett, Richard J. "Information Warfare and Deterence." *Parameters US Army College Quarterl*y, Vol. XXVI, no. 3, Autumn 1996.

Huntington, Samuel P. "The US - Decline or Renewal?" *Foriegn Affairs*, vol. 67, Winter 1988/89.

Jensen, Owen E. "Information Warfare: Principles of Third-Wave War." *Airpower Journal*, 8, no. 4, Winter, 1994.

Leahy, Peter F. "The Revolution in Military Affairs and the Australian Army." *The Combined Arms Journal*, Issue 2/95, Sydney: HQ Training Command, Australian Army, 1995.

Libicki, Martin C. "What is Information Warfare?" *Strategic Forum*, no. 28, Washington National Defense University, Institute for National Strategic Studies, May 1995.

Mann, Edward. "Desert Storm: The First Information War." *Airpower Journal*, 8, no. 4, Winter, 1994.

Metz, Steven. "A Wake for Clausewitz: Toward a Philosophy for 21st Century Warfare." *Parameters*, Winter, 1994-95.

Metz, Steven and James Kevit, "Strategy and the Revolution in Military Affairs: From Theory to Policy." (27 June 1995), in *Joint Electronic Library*, CD-ROM, September 1996.

Modestov, Sergei. "The Possibilities for Mutual Deterrence: A Russian View." *Parameters*, vol. 26, no. 4, Winter 1996-97.

Molander, Roger C., Andrew S, Riddile and Peter A. Wilson, "Strategic Information Warfare: A New Face of War." *Parameters US Army College Quarterl*y, Vol. XXVI, no. 3 Autumn 1996.

Owens, William A. "The Emerging System of Systems." *Military Review*, May - June 1995.

Owens, William A. "JROC: Harnessing the Revolution in Military Affairs." *Joint Forces Quarterly*, Winter 1993-1994.

Stein, George J. "Information Warfare." *Airpower Journal*, vol. IX, no.1, Spring 1995.

Swain, Richard M. Review of Toffler, *War and Anti-War*, in *Military Review*, February 1994.

Szafranski, Richard.   "A Theory of Information Warfare: Preparing for 2020." *Airpower Journal*, vol. IX, no.1, Spring 1995.

Thomas, Keith. "A Revolution in Military Affairs." *Research and Analysis*, Newsletter no. 5, Canberra: Directorate of Army Research and Analysis, Australian Army,March 1996.

Thomas, Timothy. "Deterring Information Warfare: A New Strategic Challenge." *Parameters*, vol XXVI, Winter 1996-97.

Tilford, Earl H. *The Revolution in Military Affairs: Prospects and Cautions*, Strategic Studies Institute, 23 June 1995.

Warden, John A. "The Enemy as a System", *Airpower Journal*, vol. IX, no.1, Spring 1995.

VI. Newspaper and Magazine Articles

Cooper, Patrick. "Information Warfare Sparks Security Affairs Revolution." *Defense News*, 12-18 June 1995.

Cordtz, Dan.   "War in the 21st Century: The Digitized Battlefield." *Financial World,* 29 August 1995.

Woodall, Pam. "The Hitchhiker's Guide to Cybernomics," *The Economist*, 28 September 1996.