Newport, Rhode Island

Information Warfare and Its Impact on National Security (U)

By

Anita D. DeVries
LCDR USN

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

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

Signature Anita D. DeVries

13 June 1997

Paper directed by
Captain George W. Jackson
Chairman, Joint Operations Department

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	**7. Address:** NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): Information Warfare and Its Impact On National Security (U)	
9. Personal Authors: LCDR Anita D. DeVries, USN	
10.Type of Report: FINAL	**11. Date of Report:** 7 Feb 1997
12.Page Count: 19	
13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: Information, Information infrastructure, Information Warfare, U.S. Strategy, Infrastructure vulnerability, Strategic strategy, Computers, Electronic systems, Telecommunication systems.	

15.Abstract: **For years, the United States national security posture has relied heavily on secured sea lines of communication, friendly borders, unmatched human and material resources, unlimited mobilization capability, and nuclear hegemony. However, we are now an information dominate society and information warfare poses a different threat to our national security than we faced during the cold war. Acts of aggression will undoubtedly be aimed at our national information infrastructure and be launched from disgruntled nations or rogue states, by religious fanatics, terrorists, criminals, or drug cartels. Are we as a nation strategically prepared offensively and defensively to protect our national interests? This paper defines information warfare; examines its offensive and defensive components; explores potential threats, information warfare legalities and nature; and concludes that we face a tremendous challenge at the strategic level to keep our current status of being a world power to be reckoned with.**

16.Distribution / Availability of Abstract:	**Unclassified** X	**Same As Rpt**	**DTIC Users**
17.Abstract Security Classification: UNCLASSIFIED			
18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT			
19.Telephone: 841-6461		**20.Office Symbol:** C	

Abstract of

Information Warfare and Its Impact on National Security

For years, the United States national security posture has relied heavily on secured sea lines of communication, friendly borders, unmatched human and material resources, unlimited mobilization capability, and nuclear hegemony. However, we are now an information dominate society and information warfare poses a different threat to our national security than we faced during the cold war. Acts of aggression will undoubtedly be aimed at our national information infrastructure and be launched from disgruntled nations or rogue states, by religious fanatics, terrorists, criminals, or drug cartels. Are we as a nation strategically prepared offensively and defensively to protect our national interests? This paper defines information warfare; examines its offensive and defensive components; explores potential threats, information warfare legalities and nature; and concludes that we face a tremendous challenge at the strategic level to keep our current status of being a world power to be reckoned with.

Information Warfare and Its Impact on National Security

Introduction

"There's a war out there, and it's about who controls the information. It's all about the information."
COSMOS IN SNEAKERS[1]

The United States entered the 1990's facing major international changes. The changing nature of international politics is making intangible forms of power more important. National cohesion, universalistic culture, and international institutions are taking on additional significance. Power is passing from the "capital rich" to the "information rich."[2]

Today technology is shifting conflicts from traditional methods of force towards non-traditional methods, including information. Information warfare offers a wide range of technological capabilities. Information and information technologies are becoming a real weapon, one that is less burdensome economically and ecologically less dangerous. Conflict in the future will be very different from that of our past experience. The major threat to national security will probably be from entities that may not have the status of national states. If threats are other than from physical force, how will our National Security Strategy respond to the threat?

The use of information warfare could have a significant impact on the national security posture. The United States is becoming increasingly dependent on U.S. infrastructures. These infrastructures are highly interdependent because of the internetted nature of the information components and because of their reliance on the national information infrastructure. The national information infrastructure, which consists of information, information systems, telecommunications, networks, and technology, in turn is dependent on other infrastructures such as electrical power and

---

[1]A Paramount film, released in 1992.
[2]Joseph S. Nye, Jr., "Soft Power", Foreign Policy, Fall 1990, p. 164.

other forms of energy. This interconnectivity and interdependency certainly places our system in a position for possible attack.

The rapid advances in information technologies are creating new problems and vulnerabilities for the United States government. Even though technology of information systems is becoming ever more capable and sophisticated, this does not guarantee security; in fact, it may make it harder to secure the U.S. information infrastructure from attacks. Future actions may be easily accomplished through the use of information warfare against our national information infrastructure. In fact, the national information infrastructure may become the de facto "center of gravity" for future conflict. Given this, we must ensure that strong emphasis is placed on meeting emerging challenges to our national security. This paper emphasizes the potential impact information warfare poses to our national security while exploring the diverse options this technology presents to the United States.

Defining Information Warfare

Information warfare is a complex notion and has as many meanings as it has proponents, detractors, and observers. For the purpose of this paper, the following definition of information warfare will be used:

> Actions taken to preserve the integrity of one's own information systems from exploitation, corruption, or destruction while at the same time exploiting, corrupting, or destroying an adversary's information systems and in the process achieving an information advantage in the application of force. It is also actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending our information and information systems. Command and control warfare is a subset of information warfare.[3]

---

[3]"Definitions for the Discipline of Information Warfare and Strategy," School of Information Warfare and Strategy, National Defense University, Fort Lesley McNair, Washington, D.C., p. 37.

Components of Information Warfare

The definition of information warfare brings to light a critical factor: information warfare consists of both offensive and defensive components. Information warfare, whether offensive or defensive, can give the United States an advantagein any type of conflict.

Offensive Information Warfare

Offensive information warfare seeks dominance over the enemy's information, computer information systems, and control systems using a myriad of tools. Attacks can be launched against the enemy's physical computer network, its supporting infrastructure, or a product of the network. The attacks can be overt or covert and consist of either hard or soft kills. Preemptive offensive information warfare may deter a potential enemy and offer coercive leverage to resolve crises and conflicts in our favor.

Effective covert offensive information warfare could permit the U.S. to predict, with near certainty, the operations of the enemy or disable their systems. In January 1992, ABC's "Nightline" reported that a computer virus developed by the Pentagon was injected into the Iraqi military computer systems through a computer printer. According to the report, an infected chip was installed in a dot matrix printer in France which was destined for Iraq via Amman, Jordan. The infected chip was reported to have shut down portions of the Iraqi defensive radar systems. The report turned out to be a hoax. Ted Koppel and "Nightline" were the victims of mis- or dis-information given to them by U.S. News and World Report, who in turn were first duped by their sources. The story went nationwide and probably worldwide, and to this day is still remembered as fact.[4]

---

[4]Winn Schwartau, Information Warfare - Choas on the Electonic Superhighway, Thunder's Mouth Press, New York, 1994, pp. 249-251. Both "ABC Nightline" and U.S. News and World Report carried this story in February 1992. In retrospect, it appears the source of the story was an article in Infoworld on April 1, 1991, which was, in fact an April Fools joke. Schwartau's point is not that computer viruses are inapplicable in warfare, but that delivery of a computer virus in this manner is a very unlikely way to

Although this virus senario turned out to be a hoax, it illustrates the possible covert methods nations can use to achieve a hit on an adversary. Introducing viruses into information systems and mis- or dis-information to the news media are just two examples of how information warfare can manipulate a nation.

Overt offensive information warfare could seriously disable the combat capabilities of an adversary by disrupting command, control, communication, computers, and intelligence (C4I) from top to bottom. In Iraq, during Desert Storm, the central telephone exchange in Baghdad was among the first targets engaged in the war campaign. Even before the telephone exchange was attacked, anti-aircraft radars were targeted and eliminated by Army Apache helicopters.[5] We poked out their radar eyes and severed their wireless nerves; thereby eliminating the acquisition of information and the ability to communicate information. The United States has been fortunate in the fact that we have not had our borders attacked overtly since Pearl Harbor. Unfortunately, information warfare has set the stage for attacks on our information infrastructure not only overtly but convertly, too.

Theoretically, if you can functionally disrupt or destroy an opponent's information, computer information systems, or infrastructure control systems using information warfare, you may sever the head from the body of the snake by isolating the leadership from the rest of the nation or armed forces. You can possibly win a victory without physical destruction of national assets.

Defensive Information Warfare

Defensive information warfare seeks to preserve the United States' ability to protect its national information infrastructure. It ensures we continue to get "trusted" information by providing secure communication links and when required, an

---

insert such a weapon.

[5]Rick Atkinson, CRUSADE - The Untold Story of the Persian Gulf War, Houghton Mifflin Company, New York, 1993, pp. 8-33.

encryption/decryption capability. Defensive information warfare also depends on the ability to detect, correct, and/or recover from attacks. However, this is the area where the United States has not invested the necessary resources to ensure our systems are not compromised. In 1988, a software worm was released into the Internet infecting over 6,000 host computers worldwide in less than 2 hours, and in 1991, a near-total shutdown of telephone service in the Baltimore-Washington area was caused by a one-byte coding error - a "d" was replaced with a "6."[6] Federal investigators reported that computer experts had attempted to infiltrate Defense Department computers about 250,000 times in 1995.[7] A General Accounting Office (GAO) report stated that "The potential for catastrophic damage is great." The report further indicted that 162 of 500 attempts to infiltrate Pentagon Computers -- or 65% of the total -- had been successful. At a Senate hearing, Jack L. Brock, Jr., lead GAO investigator, testified that inadequate computer security could allow terrorists and enemy nations to practice "information warfare techniques" against the U.S. government.[8]

There is a blend of optimism and pessimism about the future security of our national information infrastructure. On one side, experts point out that the technology for securing our systems is improving steadily. On the other side, since security has not been historically a high priority in the design of information systems, the existence of security technology does not necessarily guarantee its proper application. Also, advances in the technology of protection may not be adequate to deal with the complex systems now being built.

With the increasing value of information as a commodity, protection of our own information infrastructure resources and denial of those same resources to an adversary

---

[6]"Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance", National Defense University, July 1996, pp. 2-18.
[7]"Computers," Facts On File World News Digest, July 18, 1996, p. 494G3.
[8]Ibid., p. 494G3.

are essential. It is important to note that most of what the U.S. can usefully do in information warfare under the current rules of engagement will be defensive, rather than offensive. While a successful defense may not win a conflict, an unsuccessful defense can make subsequent operations of any sort difficult, if not impossible. Better defenses must be engineered if we are to retain the integrity and reliability of our information systems.

Potential Threats

One of the goals cited in the February 1995 edition of the National Military Strategy of the United States is "to win the information war". Martin Libicki provides a description of various types of information warfare which can be aimed against national infrastructures and military forces in an effort to "win the information war":

- Command-and-Control warfare (C2W). Attacks on our ability to generate commands and communicate with the services and deployed forces.
- Intelligence-based warfare (IBW). Integration of sensors, emitters, and processors into reconnaissance, surveillance, target acquisition, and battlefield damage assessment systems.
- Electronic warfare (EW). Techniques that enhance, degrade, or intercept flows of electrons or information.
- Psychological warfare. Designed to affect the perception, intentions, and orientations of decision makers, commanders, and soldiers.
- "Hacker" warfare. Warriors who use their techniques to destroy, degrade, exploit, or compromise information systems.
- Economic warfare. Expressed in one of two forms: as an information blockade (which presumes that information flows are as important as supply flows) or as information imperialism (which presumes or believes that trade is war).
- Cyberwarfare. The use of information systems against the virtual personas of individuals or groups.[9]

Real forms of warfare include everything under C2W, EW, IBW, and psychological operations against commanders and forces. *Arguable* forms of warfare include psychological operations against the national will and culture, as well as techno-

---

[9]Martin C. Libicki, "What is Information Warfare?" Center for Advanced Concepts and Technology, National Defense University, August 1995, pp.7-8 and 87-89.

imperialism. Hacker warfare, information blockades, information terrorism, and semantic attacks are *potential* forms of warfare.[10] No matter what the form, they can be useful to inflict a blow on important information infrastructures.

A major new form of information warfare is the worldwide infosphere of television and broadcast news. Information warfare at the strategic level is the "battle off the battlefield" to shape the political context of the conflict.[11] Although this media created universe we live in broadcasts news that is "true", the news is just not the whole, relevant, or contextual truth. Nevertheless, this universe becomes the politically relevant universe in which the government or the armed forces are supposed to act. Somalia got into the news, and we got into Somalia despite the reality of equally disastrous starvation, disorder, and rapine right next door in Sudan. There were no reporters in Sudan, however, because the government of Sudan would not issue visas to the media. The potential for governments, militaries, parties in a civil war, or even religious fanatics to manipulate the multimedia, multisource universe of "the battle off the battlefield" for strategic information dominance should be obvious.[12]

With the desire to win the information war, information assets are now strategic assets, and should be so reflected in our national security policy. Each type of information warfare described would require its own rules of engagement, based on its methods, objectives, and technologies.

Legality of Information Warfare

Legal ramifications of information warfare raises some tough questions. For example, should we spy on the world? If an assault were made, in an electronic environment, what would our reaction be? Is a debilitating attack against General

---

[10]Ibid., p. 85.
[11]George J. Stein, "Information Warfare" Airpower Journal, Spring 1995, p. 33.
[12]John Arquilla, "The Strategic Implications of Information Dominance," Strategic Review, Summer 1994, pp. 24-30.

Electric by a foreign corporation considered worthy of national response? If a drug cartel successfully shuts down U.S. border radar systems, what is the appropriate action? How do we politically and militarily deal with remotely controlled foreign incursions into U.S. information infrastructure? When does war begin? Would the military be sent in? Should they? What actions made possible by new information systems capabilities will be legal under international law? So many questions, and yet it is evident that no one at the strategic level has the answers.

Technology has clearly outpaced existing laws governing information based intrusions. There is still much debate over the nature of an act of war in the information age, and the definition of what constitutes a computer crime. Legal aspects of information warfare must be quickly clarified due to our reliance on commercial and military information based systems. Some treaties do exist that prohibit the use of information warfare technologies that belong to the electromagnetic spectrum of weapons. However, we need stronger regulations and penalties, treaties, and rules of engagement to govern the protection of our national security in dealing with information warfare.

Historically, the United States takes pride in the fact that we are the "good guys." In being the good guys, we play by the rules. The question is, which rules? America traditionally does not start wars. However, if we were to use one or more of the information warfare methods available to garner an advantage over a foreign nation or terrorist group are we as a nation perpetrating an act of aggression? Are we setting ourselves up for another Pearl Harbor? Legally, our best course of action would be to take a defensive position.

The decision to pursue information warfare or develop information weapons is a leadership decision. It is a strategic decision in the United States because it is the Congress, representing the entire citizenry, that links means to ends. The political leaders in the United States can be expected to consider the morality of information

weapons and information warfare, no matter which group develops the weapons or engages in the warfare, and to regulate their use accordingly. Congress is very likely to conclude that the employment of information weapons at the operational level is useful and necessary, but that employment against noncombatants, or their employment at the strategic level is wrong.

The Nature of Information Warfare

Information warfare continues to evolve and U.S. society is moving rapidly to take advantage of the new opportunities presented by each technical advance in this field. U.S. allies and potential coalition partners are also looking to exploit the evolving information infrastructure and associated technologies. Conceptually, if and when potential adversaries attempt to damage these systems using information warfare techniques, information warfare inevitably takes on a strategic aspect.[13]

Targets in the United States are just as vulnerable as in-theater targets. U.S. strategy can no longer focus on conducting and supporting operations only in a region of concern. Information-based warfare techniques render geographical distance irrelevant. Strategy now requires an in-depth examination of the implications of information warfare for the U.S. and allied infrastructures that depend on the unimpeded management of information.

Within the last 2 years, electronic intruders have penetrated major U.S. telecommunications carriers and Internet service providers; many international Post, Telegraph, and Telephone organizations; and a wide variety of end user systems.[14] These intruders have included foreign intelligence agents, economic espionage agents, organized crime, drug cartels, private detectives, hackers, and insiders. The nature of

---

[13]Roger C. Molander, Andrew S. Riddle, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War", Parameters, Autumn 1996. p.85.
[14]BELLCORE, Inc., Security in Broadband Networks Briefing, John F. Kimmins, Information Infrastructure Standards Panel Meeting, March 27-28, 1996.

information warfare, exemplified by Figure 1, further complicates information protection/assurance.

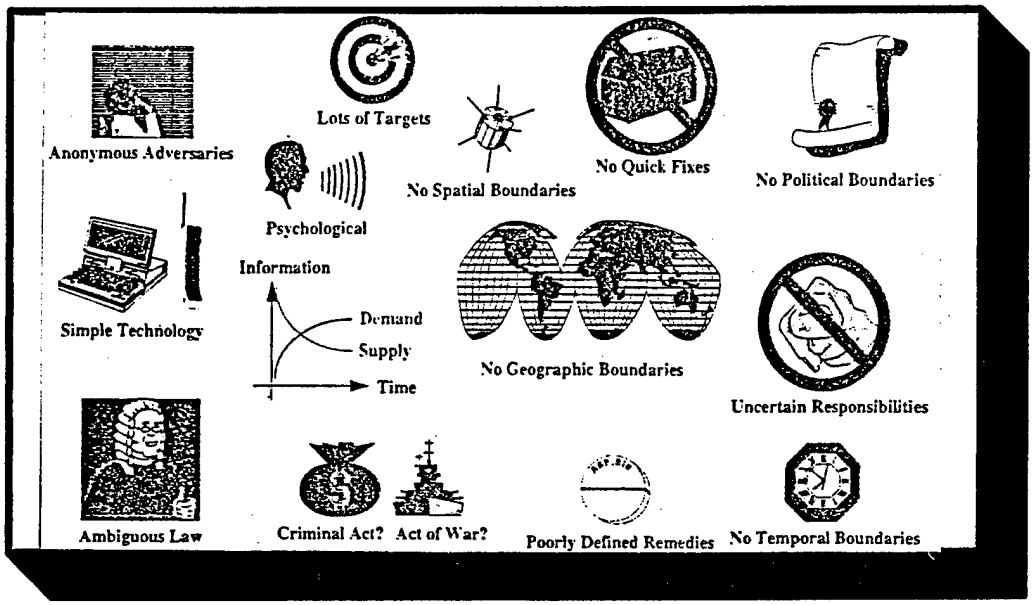

Figure 1. The Nature of Information Warfare[15]

Information warfare allows potential attackers to hide in the mesh of internetworked systems and often attackers can use previously conquered systems to launch their attacks. The lack of geographical, spatial, and political boundaries offers anonymity and invalidates established "nation state" sanctuaries.

Information warfare is also relatively cheap to wage, offering a high return on investment for resource-poor adversaries. The technology to launch attacks is relatively simple and is widely available worldwide. Information warfare systems can be cobbled together from parts available in electronics stores on the streets of any city in the world or can be ordered by mail. Technological anarchy is among us. International law is ambiguous regarding criminality in and acts of war on information infrastructures. This

---

[15]"Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance," National Defense University, July 1996, pp.1-5.

ambiguity, coupled with a lack of clear designated responsibilities for electronic defense hinders the development of remedies and limits response options. Additionally, if a possible adversary should be detected acting in a hostile or potentially hostile fashion, information warfare measures that the United States could take at the outset of such actions might require quite different rules of engagement than have been contemplated up to now.

Where Do We Stand As A Nation?

Most disconcerting is that the United States is the most information intensive society in the world and, yet, the consensus is that we are most vulnerable to attack. The United States has substantial information-based resources, including complex management systems and infrastructures involving the control of electric power, money flow, air traffic, oil and gas, and other information-dependent items. In the national security environment, these activities include transportation, logistics, pay and other monetary disbursements, manpower and personnel actions, and training. Given the increased reliance of the U.S. economy and society on such high-performance networked information infrastructures, a new set of lucrative strategic targets presents itself to potential attack from information warfare-armed opponents. The modern thief can steal more with a computer than with a gun. A terrorist may be able to do as much damage with a keyboard than with a bomb.

Winn Schwartau, warns: "...as terrorism now invades our shores, we can expect attacks upon not only airliners and water supplies, but upon the money supply, a sure way to strike terror into millions of people with a single keystroke."[16] Some social and political scientists see the possibility of an increase in terrorist activities.[17] Experience

---

[16]Winn Schwartau, Information Warfare: Chaos on the Electronic Superhighway, Thunder's Mouth Press, New York, 1994.

[17]Donn B. Parker, "The Potential Effects of Electronic Funds Transfer on National Security," Proceedings of the Fifth International Conference on Computer

has s[illegible]n that such activity is directed against our computer and communication system[illegible] which perpetrators assume, often rightly, to be at the heart of all operations.

In general, because new technologies are being designed to operate more reliably than the ones replaced, the risk that any particular mechanism may fail is being reduced. Unfortunately, the market does not work well enough to raise the security of systems at a rate fast enough to match the apparent growth in threats to systems. If a deliberate disruption occurs, its costs could be catastrophic. Since the United States is highly dependent on the reliable functioning of a single integrated technological system or small collections of such systems, we face the possibility of a "domino" collapse.

The multi-link architecture of the national and global infrastructure allows adversaries to select multiple locations and different paths for successive attempts on our systems. Not knowing what constitutes an attack, where these attacks are being initiated, or the identity of the individual, group, or nation behind the[illegible] makes pre-emptive or retaliatory attacks virtually impossible.

We have the technology to infect our adversary's information systems with viruses in "peacetime" and in war. Using such technology, however, could lead us to a ruinous counterattack. U. S. policy makers accordin[illegible]y must proceed cautiously lest they inadvertently open Pandora's Box.

How would the United States fare against a foe of the future? Martin Libicki offers that "The United States is *powerful* at antiradar and cryptographic aspects of EW, offensive intelligence-based warfare, psychological warfare against commanders and forces, and simula-warfare; it has distinct advantages in *kulturkampf* and blockading information flows. The United States is both *powerful but vulnerable* when it comes to C2W, defensive intelligence-based warfare, hackerwarfare, techno-imperialism, and Gibson-warfare. The United States is *vulnerable* to psychological warfar[illegible] against the

---

Communication, October 1980, pp.470-476.

national will, information terrorism, and semantic attack on computer networks."[18] History validates various aspects of this statement.

The current collection of laws attempts to regulate the area of information security dealing with attacks by Americans on American networks or computers, from within the borders of the United States. To the hacker, nation, or any other user outside the United States, these laws have little or no deterrent effect because they do not apply in the international community. There are currently no laws, treaties, or agreements that deal with the varied spectrum of information warfare at the international level. Also, it is important to note that laws can only be applied if the criminal is identified and caught.

Conclusion

He who wishes to snatch an advantage takes a devious and distant route and makes of it the short way.
Sun Tzu[19]

Information warfare can be used to achieve our national strategy objectives or destroy them. Information warfare involves actions taken at the national strategic level to create an information gap between what is understood regarding the political, economic, cultural, and military strengths, vulnerabilities, and interdependencies of a potential adversary and what the adversary possesses regarding friendly capabilities. It is a national strategy that employs all the tools of national power to create a competitive advantage at the national strategic level. Information warfare, in this sense, is a societal-level or nation-to-nation conflict waged, in part, through the worldwide internetted and interconnected means of information and communication.[20] Unfortunately, we lack a national definition, strategy, and policy to guide us regarding defensive and offensive information warfare concerns.

---

[18]Martin C. Libicki, "What is Information Warfare?" Center for Advanced Concepts and Technology, National Defense University, August 1995, p. 86.
[19]Sun Tzu, The Art of War, p. 102.
[20]John Arquilla and David Ronfeldt, "Cyberwar is Coming!" Comparative Strategy, April-June 1993, pp. 141-165.

national definition, strategy, and policy to guide us regarding defensive and offensive information warfare concerns.

Information warfare is real warfare; it is about using information to create such a mismatch between us and an opponent that the opponent's strategy is defeated before his forces can be deployed or his first shots fired. Information warfare attempts to target the minds of the leaders that make the key decisions of war or peace - the decisions on if, when, and how to employ the assets and capabilities embedded in their strategic structures. Thus, a lack of information hinders the overall effectiveness of a leaders decision making process. History has demonstrated the importance of information superiority and the impact on decision making when leaders lose the capability to obtain, analyze, and make sound decisions. Offensive information warfare is of strategic value but only against an adversary that is dependent on modern information architecture. Will our future adversaries meet this criteria?

As a nation, we must posture ourselves for the possibility of both offensive and defensive information warfare. We must maintain our security. It is no secret that the United States government and civilians are ill-prepared to deal with threats imposed by information warfare. The gravity of the information security issue is well recognized by Congress. If the infrastructure is directly attacked, it is not known which portions of the infrastructure will be affected, or what affect the loss of portions of the infrastructure will have on the performance of essential functional activities. The American public expects security within our borders and quick and decisive victories when confronting adversaries. Emerging information technologies and weapons give our leadership the tools to meet this expectation and achieve decisive victory. However, we must have alternative options if our security fails, for whatever reason. A policy must be established which defines what constitutes an attack on our vital national interests and the appropriate response to such an attack. It can no longer be business as usual.

Without such a policy, we cannot derive a definition or a concept upon which to base an intended national strategy.

We must develop better defenses for our national information systems. This requires a concerted effort from both the government and the private sector. Both are equally vulnerable to the current situation and both have vested interests in protecting our national infrastructure. We need an information network that is credible, available, secure, and survivable. To reach this goal, a national policy or program must be developed that can unite the multiple fragmented efforts that are on-going today.

To date, we have been lucky. Yes, there have been disruptions, compromises, and theft of information. But, as far as can be ascertained, there has been no successful systematic attempt to subvert any of our critical computing systems. Unfortunately, there is reason to believe that our luck will soon run out and that our national security will be challenged by information warfare targeted against our national information infrastructure.

Bibliography

1. Arquilla, John, "The Strategic Implications of Information Dominance," Strategic Review, Summer 1995.

2. Arquilla, John and David Ronfeldt, "Cyberwar is Coming!" Comparative Strategy, April/June 1993.

3. Atkinson, Rick, CRUSADE - The Untold Story of the Persian Gulf War, Houghton Mifflin Company, New York, 1993.

4. Baran, Nicholas, Inside the Information Superhighway, Coriolis Group Books, Scottsdale, Arizona, 1995.

5. Campen, Alan D., "Vulnerability of Info Systems Demands Immediate Action," National Defense, November 1995.

6. Campen, Alan D., "Rush to Information-Based Warfare Gambling with National Security," Signal, July 1995.

7. "Computers," Facts on File World News Digest, July 18, 1996.

8. Debban, Alan W., "Disabling Systems War-Fighting Option for the Future," Airpower Journal, Spring 1993.

9. Johnson, Craig L., "Information Warfare - Not a Paper War," Journal of Electronic Defense, vol. 17, no.8, August 1994.

10. Kraus, George F. Jr., "Information Warfare in 2015," U. S. Naval Institute Proceedings, August 1995.

11. Libicki, Martin C., "What is Information Warfare?" Center for Advanced Concepts and Technology, National Defense University, Fort Lesley McNair, Washington, DC.

12. Mahnken, Thomas G., "War in the Information Age," Joint Force Quarterly, Winter 1995-96.

13. Molander, Roger C., Andrew S. Riddle, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War," Parameters, vol. XXVI, Autumn 1996.

14. Morris, Chris, Janet Morris, and Thomas Baines, "Weapons of Mass Protection," Airpower Journal, Spring 1995.

15. National Defense University, "School of information Warfare and Strategy; A Working Dictionary," Washington: National Defense University, Academic Year 1994-95.

16. National Defense University, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, Washington: National Defense University, July 1996.

17. Nye, Joseph S., Jr., "Soft Power," Foreign Policy, Fall 1990.

18. Parker, Donn B., "The Potential Effects of Electronic Funds Transfer on National Security," Proceedings of the Fifth International Conference on Computer Communication, October 1980.

19. Ryan, Donald E. Jr., "Implications of Information-Based Warfare," Joint Force Quarterly, no.6, Autumn/Winter 1994-95.

20. Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway, Thunder's Mouth Press, New York, 1994.

21. Stein, George J., "Information Warfare" Airpower Journal, Spring 1995.

22. Szafranski, Richard, "A Theory of Information Warfare - Preparing for 2020," Airpower Journal, Spring 1995.