STRATEGY RESEARCH PROJECT

PEACETIME USE OF COMPUTER NETWORK ATTACK

BY

COLONEL DANIEL J. BUSBY
United States Army

USAWC CLASS OF 2000

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

PEACETIME USE OF COMPUTER NETWORK ATTACK

by

Colonel Daniel J. Busby
United States Army

Colonel Richard M. Meinhart
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Daniel J. Busby

TITLE: Peacetime Use of Computer Network Attack

FORMAT: Strategy Research Project

DATE: 3 April 2000 PAGES: 28 CLASSIFICATION: Unclassified

Published in May 1998, Presidential Decision Directive 63 (PDD-63), The Critical Infrastructure Protection Directive, calls for a national effort to protect America's increasingly vulnerable and interconnected information infrastructures. Such infrastructure includes telecommunications, banking and finance, energy, transportation, and essential government services. PDD-63 alerts the nation to prepare for impending cyber attacks. This paper examines the nature, scale, and likelihood of cyber attacks posited in PDD-63 and finds that the country does not face an imminent "electronic Pearl Harbor." Nonetheless, the country's information infrastructure is vulnerable to cyber attacks by a plethora of adversaries. The most dangerous threat is from state-sponsored cyber-warriors. In view of this real and growing threat, the prescriptions in PDD-63 for protecting the infrastructure are inadequate.

This paper concludes that the defensively oriented policy measures in PDD-63 are insufficient for protecting the infrastructure. These measures are not working now, and because they are entirely reactive by nature, they will not deter future attacks by state-sponsored cyber-warriors. With the potential for severe disruptions to the infrastructure so great, this paper argues that the United States must conduct open, offensive Computer Network Attacks against state-sponsored cyber-warriors during peacetime. Only then will the country be able to stop these adversaries and adequately protect its infrastructure.

TABLE OF CONTENTS

ABSTRACT III

LIST OF ILLUSTRATIONS VII

PEACETIME USE OF COMPUTER NETWORK ATTACK 1

- INFORMATION INFRASTRUCTURE: THE ISSUE 1
- WHAT IS CNA 2
- NATURE OF THE THREAT 3
- PLAUSIBILITY & SEVERITY OF THE STATE-SPONSORED THREAT 4
- ADDRESSING THE THREAT: THE NIPC 6
- INADEQUANCY OF DEFENSIVE MEASURES 7
- OFFENSIVE CNA AND DOD 8
- POLICY PROHIBITIONS ON CNA 12
- PUBLIC RESPONSES TO POTENTIAL OFFENSIVE CNA 13
- FUNDING REQUIREMENTS OF INFRASTRUCTURE SECURITY 14
- CONCLUSION 14

ENDNOTES 15

BIBLIOGRAPHY 19

LIST OF ILLUSTRATIONS

FIGURE 1 HIERARCHY OF CNA WITHIN INFORMATION OPERATIONS 3

FIGURE 2 INFORMATION OPERATIONS THREATS IN WAR AND PEACE 11

FIGURE 3 NOTIONAL INFORMATION OPERATIONS ENGAGEMENT TIME 11

PEACETIME USE OF COMPUTER NETWORK ATTACK

> Over the next quarter century, we conclude that... America will become increasingly vulnerable to hostile attack on our homeland, and our military superiority will not entirely protect us.[1]
>
> -- U.S. Commission on National Security
> in the 21st Century, August 1999

INFORMATION INFRASTRUCTURE: THE ISSUE

It is readily apparent that the United States is dependent – some say overly dependent – on information and information systems. The information explosion that has taken place in our society affects every aspect of American life, including among others, commerce, education, politics, the media, and national security. With millions of computers and innumerably Local Area Networks, telephone, and power networks, the country depends on the soundness and dependability of its information infrastructure. As the President's Commission on Critical Infrastructure Protection noted in October 1997, "our security, economy, way of life, and perhaps even survival, are now dependent on the interrelated trio of electrical energy, communications, and computers."[2] The fate of the US economy and its national security are inexorably linked to the security of its information infrastructure. Unfortunately, this infrastructure is under attack.

Former Deputy Secretary of Defense John Hamre formally declared that the country is already engaged in a cyber war involving its information infrastructure.[3] The country does not face an "electronic Pearl Harbor" in the near future; however, the facts portend the use of cyber attacks by adversaries against the country's information infrastructure. Cyber attack refers to using information-related principles to disrupt or destroy information and information systems.[4] There is a myriad of potential perpetrators of cyber attacks; however, all adversaries are not equally threatening. For example, hackers are responsible for the greatest number of intrusions, and they garner the most publicity, but they are not a grave threat to critical infrastructure. Terrorists pose a real threat to specific portions of the infrastructure, however, in general they are not well financed and do not pose a large scale threat to the infrastructure. My research has found that the most dangerous threat to the infrastructure is from state-sponsored cyber-warriors.[5] These adversaries are well financed and pose a well-coordinated, serious threat to major portions of the infrastructure.

Released in May 1998, Presidential Decision Directive 63 (PDD-63), The Critical Infrastructure Protection Directive, provides the current US policy guidance on protecting the information infrastructure from state-sponsored cyber-warriors. PDD-63 handles the threat using defensive-only measures to thwart or neutralize their attacks. The problem is defensive protection measures are not working *now*. As soon as new defensive security tools are developed, state-sponsored cyber-warriors quickly learn how to defeat them or exploit other vulnerabilities. Additionally, employees in critical industries are poorly trained on defensive security measures and fail to apply already known security fixes. Defensive measures do

not work because of mistrust between the owners of the infrastructure and the government and the lack of proper incentives for industry to cooperate. The threat of exposure, jail time, or fines will not deter state-sponsored cyber-warriors from their acts. There is scant reason to believe that any of this will change in the near future.

Because defensive measures will not work and the potential for severe disruptions to the infrastructure is so great, the US must find an offensively oriented way to deal with the growing threat from state-sponsored cyber-warriors during so called "peacetime." Unfortunately, there are no provisions in PDD-63 or its derivative National Plan for using offensively oriented countermeasures against state-sponsored cyber attacks. There are no parts of the National Infrastructure Protection Center (NIPC), including the Department of Justice (DoJ) or Federal Bureau of Investigation (FBI), that can respond directly against the source of state-sponsored cyber attacks during peacetime. Both government and industry are in denial about how to handle these adversaries.

In the remainder of this paper I will make the case that the government must disable, disarm, or destroy the state-sponsored purveyors of computer network attacks (CNA) during peacetime. I will first discuss CNA, analyze the threat from state-sponsored cyber-warriors, discuss why the defensive measures specified in PDD-63 do not and will not work to protect our critical infrastructure, and recommend who in the government should conduct offensive CNA and why. I will also discuss the legal and moral pitfalls of conducting CNA during peacetime. In the end, I will argue that the government must show its willingness and capability to conduct offensive CNA to protect the country's infrastructure.

WHAT IS CNA

CNA is an integral component of offensive Information Operations (IO). Joint Publication 3-13 specifies that offensive IO capabilities and activities include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, physical attack/destruction, special information operations (SIO), and computer network attack (CNA).[6] Conceptually, CNA is the easiest component of offensive IO to get your hands around. Unfortunately, you have to burrow through a rhetorical mountain of doctrine to find the military's plan for conducting CNA. For the Army, CNA is a component of Command & Control (C2) Attack, which is a subset of C2 Warfare, itself a subset of Information Warfare and Offensive IO. This hierarchy appears in Figure 1.[7] The aim of CNA is to deny information to an adversary by disrupting and degrading his information collection capabilities, selectively disrupting his information systems, and neutralizing or destroying his information nodes and links.[8] The focus of offensive CNA in peacetime is to destroy the adversary's capability to pursue his objectives without necessarily destroying his infrastructure in turn.

The tools of CNA are destructive and cut both ways – what infects your enemy can infect you. CNA tools include malicious code like viruses, worms (self-replicating executable code), Trojan Horses (programs that perform a desired task, but also include unexpected - and undesirable – functions), logic

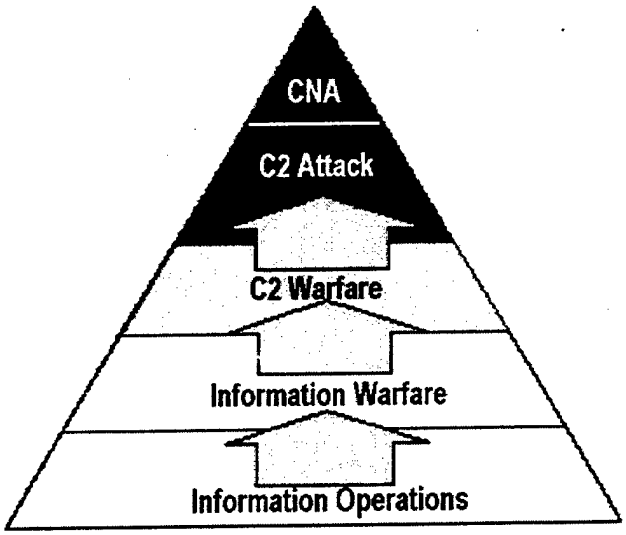

FIGURE 1 HIERARCHY OF CNA WITHIN INFORMATION OPERATIONS

bombs, Trap Doors, Machines Microbes, Electronic Jamming, and other "uninvited" software and hardware tools.[9] All of our adversaries have the same CNA tools that we have.

NATURE OF THE THREAT

The threats facing the information infrastructure come from state-sponsored cyber-warriors, terrorists, hackers, insiders, multinational corporations, foreign intelligence services, and others. Anyone with a modicum of new technology and computer skills is suddenly able to effectively target and penetrate information systems. To make attacking more convenient, there are "about 30,000 hacker-oriented sites on the Internet, bringing hacking -- and terrorism -- within the reach of even the technically challenged."[10]

The scope of the threat is persuasive, and there are clear indications that the problem is growing. It is impossible to assess with any degree of accuracy the actual number of intrusions into the nation's computer networks that have already occurred. The anecdotal statistics are alarming. Here are some examples of recent cyber threats divided into "commercial" and "security" threat categories:

Commercial Threats

- Seventy-five percent of *Fortune* 1000 companies surveyed in 1998 reported financial losses due to computer security breaches in 1997.[11]

- According to the FBI, more than 20 foreign governments are systematically vacuuming American multinational corporations of $24 billion worth of trade secrets and other intellectual assets every year.[12]

- Unknown attackers struck Yahoo, eBay, CNN, and scores of other commercial web sites with massive denial-of-service attacks in February 2000 resulting in millions of dollars in lost revenues.[13]

- Computer Economics, Inc. estimated that damage in the first two quarters of 1999 from viruses topped $7 billion.[14]

Security Threats

- Every 20 minutes someone tries to penetrate a DoD computer network.[15]

- GAO found that 65 percent of an estimated 250,000 attacks on DoD systems in 1996 were successful in attaining access. DoD detected and reported only one out of every 150 unauthorized intrusions.[16]

- During exercise Eligible Receiver in 1997, National Security Agency (NSA) "hackers" achieved "root level" access in 36 DoD networks. They simulated "turning off" sections of the U.S. power grid, "shut down" parts of the 911 network in Washington, D.C., and other cities, and gained access to systems aboard a Navy cruiser at sea.[17]

The list goes on and on; the main point is the country's vulnerability to computer attacks is growing. In the end, no one connected to a computer network is safe from an organized intrusion. However, these threats are not equally important.

There are major differences in *scale* among CNA characterized as electronic graffiti, insider vindictiveness, expensive industrial espionage, terrorist acts, etceteras. Malicious insiders, thrill seeking hackers, accident-prone users, and isolated terrorist disasters will probably not create widespread damage to the US information infrastructure. Unwittingly or not, the US has a great deal of practice handling minor interruptions to the nation's information infrastructure, because of the country's predilection to suffer natural disasters and the inevitable technological equivalents of Murphy's Law. This does not mean that these threats are benign, or that the terrorist threat is minor, only that the US can weather through these attacks. Therefore, anything less than a well orchestrated, coordinated attack should result in something less than catastrophic infrastructure failure. The well-coordinated attack is most worrisome to national security. The question is how plausible is a well-coordinated attack.

PLAUSIBILITY & SEVERITY OF THE STATE-SPONSORED THREAT

The prevailing view among government leaders is that a well-coordinated cyber attack is most likely to come from state-sponsored cyber-warriors. The goal of state-sponsored cyber-warriors in peacetime is physical and infrastructure destruction, industrial espionage, malicious hacking, fraud and theft, and/or foreign government espionage. There may also be some attempt to attain personal privacy information for some gain. In testimony before Congress, the Director of the Central Intelligence Agency said this about the threat:

> At least a dozen countries, some hostile to America, are developing programs to attack other nations' information and computer systems. China, Libya, Russia, Iraq, and Iran are among those deemed a threat.[18]

How serious a threat are these state-sponsored cyber-warriors? The Director of the NIPC testified before Congress that "the greatest potential threat to our national security is the prospect of "information warfare" by foreign militaries against our critical infrastructures."[19] The threat from state-sponsored cyber-warriors is more than theoretical. The Chinese cyber-attacked the US following the accidentally bombing of their Belgrade embassy on 7 May 1999. These attacks were "viewed by some U.S. national security officials as possible government-sponsored information warfare attacks on the United States."[20] The Chinese attitude toward CNA is the most widely publicized cyber threat, and the People's Liberation Army (PLA) is at the forefront of thinking about CNA. The PLA's political arm recently made the following announcement:

> It is essential to have an all-conquering offensive technology and to develop software and technology for Net offensives so as to be able to launch attacks and countermeasures on the Net, including information-paralyzing software, information-blocking software, and information-deception software.... [Key targets include] finance, commerce, communications, telecommunications and military affairs.[21]

Documented cases of Chinese offensive CNA during peacetime are on the rise. The Chinese government attacked "a US web site devoted to the Falun Gong meditation sect, which Chinese authorities outlawed in July 1999."[22] The attack was linked to the Internet Monitoring Bureau of China's Public Security Ministry. Like the Chinese, the Russian plans for state-sponsored cyber warfare pose a threat to the US during peacetime.

The Russians expect to conduct information warfare against foreign armed forces, civilian populations, and opposing economies. Russian doctrine advocates conducting information warfare in both peacetime and wartime and considers it an essential geo-strategic element of national power.[23] For example, according to the Center for Army Lessons Learned, the Russians will use CNA against a

> strategic command and control site..., an information strike at a national power grid..., or an information strike at the control systems of a nuclear power plant.... None are excluded from war fighting or even peace-time covert information strikes. [I]t comes as no surprise that Russia has developed viruses to affect these systems.[24]

There is also evidence that the Russians have already used CNA against the US:

> [I]n July 1999, a team of computer specialists from the Russian Academy of Sciences, an organization [linked to] Russia's top military labs, targeted computer systems at the Departments of Defense and Energy, military contractors and leading civilian universities. The Russians captured vast quantities of data [possibly including] classified naval codes and information on missile-guidance systems. DoD officials called it "a state-sponsored Russian intelligence effort to get U.S. technology."[25]

This peacetime CNA is a harbinger of future attacks against our critical information infrastructures. Does this mean that the country is facing the equivalent of an "electronic Pearl Harbor?" The answer is a qualified *no*. A recent RAND study succinctly summarizes the issue of an Electronic Pearl Harbor:

> There is no evidence that the "sky is falling in"; the country is not in imminent danger of massive disruption through infrastructure cyber attacks. That does not mean that interruptions will be free of localized catastrophic effects that compromise services and endanger national security.[26]

This is reason for cautious optimism. The infrastructure may be resilient to the perturbations of natural and man-made cyber disasters, but it is not immune from the effects of a well-coordinated attack. For instance, a well-coordinated state-sponsored CNA against the Federal Aviation Administration could cripple the nation's airline industry and could actually cause airplanes to crash. Likewise, an attack on financial institutions could disrupt the banking system and cripple the stock market, thereby destabilizing the economy. State-sponsored CNA could disrupt entire communities, states, or even the entire nation. Fortunately, there is in our society sufficient human involvement in the control processes of infrastructure information systems that the country does not face a significant widespread cyber risk in the classical sense.[27] The nation may not face an imminent "electronic Pearl Harbor," however; the specter of major disruptions to the infrastructure from state-sponsored cyber-warriors is disconcerting. Unfortunately, PDD-63 and its NIPC do not sufficiently address the threat from state-sponsored cyber-warriors.

ADDRESSING THE THREAT: THE NIPC

The main goal of PDD-63 is to put into place a structure and an organization to make sure that any disruptions of critical infrastructures are brief, infrequent, and minimally detrimental to the welfare of the US. Its essential objectives are clear and unequivocal. By the year 2000, the NIPC will have the capability to gather information on threats to the infrastructure and disseminate warnings throughout the country. By 2003, the NIPC will have the ability to protect the country's infrastructure from intentional acts of destruction or attempts of degradation. The NIPC will serve as the government's focal point for threat assessment, warning, investigation, and response for attacks against information infrastructures. This organization includes representatives from the FBI, DoJ, DoD, the Intelligence Community, other federal departments and agencies, state and local law enforcement, and private industry.

The NIPC's operations fall into three categories: protection, detection, and response. Under the category of protection, the NIPC's role is to provide information to industry and government about threats, ongoing incidents, and security vulnerabilities. Its means for providing protection is through centralized planning and information sharing. This process for protection is a partnership among the infrastructure owners, operators, and appropriate government agencies. Public and private sector cooperation is paramount, because 90 percent of the nation's information infrastructure is privately owned.

Under the category of detection, the NIPC will use the Federal Intrusion Detection Network (FIDNet) to conduct government-wide computer security monitoring, analyzing, and information sharing. FIDNet will share the results of its network monitoring throughout the country. When it becomes operational in May 2003, FIDNet will link together the FBI, DoD's Joint Task Force on Computer Network Defense (JTF-CND), NSA, and other State and federal government agencies. It will also interface with private sector systems through intermediary networks called Information Sharing and Analysis Centers.

Under the category of response, NIPC will investigate cyber intrusions to identify the attackers and issue warnings throughout the nation. The NIPC will then concentrate on prosecuting the attackers through law enforcement channels. The unifying element that permeates protection, detection, and response is the emphasis on *reacting* to intrusions ex post facto. In all that it does, the NIPC relies on defensive measures to protect the infrastructure. Unfortunately, defensive measures will not protect the infrastructure against state-sponsored cyber-warriors.

INADEQUANCY OF DEFENSIVE MEASURES

There are four reasons why defensive measures will not protect the infrastructure against state-sponsored cyber-warriors: the inherent shortcomings with security tools, the poor state of security training, the fundamental distrust between the owners of the infrastructure and the government, and a mismatch in incentives.

Computer security tools are inherently inadequate for defending against a coordinated attack from state-sponsored cyber-warriors. For one thing, as soon as new security tools are developed, these attackers quickly learn how to defeat them or exploit other vulnerabilities. In truth, all networked systems are vulnerable. Many observers have noted that America is its own worst enemy -- procuring computers open to errors and omissions.[28] In today's constantly changing technology environment, vulnerability "is largely a self-created problem: security systems are deficient in scope, resources, standardization, and implementation."[29] State-sponsored cyber-warriors can pick the time and place of their attacks, choose the weakest part of the network to attack, cause catastrophic damage in a very short time period, and move on. Unfortunately, by the time the system tools react to an attack, the damage is complete.

Training shortfalls are the second reason why defensive measures will not work against state-sponsored cyber-warriors. According to a GAO study on computer security, the US faces an increasing number and severity of computer attacks, because users and system administrators fail to apply already available defensive measures on their computer systems.[30] The owners of the nation's infrastructure simply do not enforce published security policies and procedures, install low cost firewalls, and patch known software security flaws. This is a deficiency in training, not a resource issue, and hints at an under-appreciation of the genuine threat from state-sponsored cyber-warriors.

The third shortcoming with defensive measures revolves around mistrust of government. The private sector owns the majority of the information infrastructure yet it is not cooperating with the NIPC. The reason, simply put, is that industry does not trust the government, particularly the role of the FBI in

the NIPC. The source of this mistrust revolves around legal impediments. The legal impediments to cooperation between industry and the NIPC are daunting. Industry fears the following legal liabilities may arise from cooperation:[31]

- data given to the government will not remain confidential and may be subject to Freedom of Information Act requests
- trade secrets and proprietary information given to the government will be released to competitors
- the government may classify information released by industry thus preventing industry from using it
- the government may start antitrust action against firms that share information with competitors even though the intent is to protect themselves and not collude
- firms may face certain liabilities if government gets hold of industry information

Until a proper legal framework for cooperation is developed, industry and government are not likely to trust each other.

Lastly, defensive measures will not work against state-sponsored cyber-warriors because the incentive system for the NIPC and industry to cooperate is at odds. Industry wants to be "secure enough, just in time" and not pay for more security than they need. Because investigations and adverse publicity are expensive; industry does not believe it is cost-effective for them to share information with the government. They would rather internally absorb the costs of attacks than share information with the FBI. Until these incentives are adjusted, industry will not cooperate fully with the government to combat state-sponsored cyber-warriors that attack industry systems.

The problems with security tools, security training, trust, and incentives are not insurmountable, however, they will not be resolved in the near future. In the mean time, the threat to the infrastructure from state-sponsored cyber-warriors continues. The country must move beyond the defensive measures specified in PDD-63 to protect its critical infrastructure.

OFFENSIVE CNA AND DOD

Offensive CNA will ameliorate the potential damage from state-sponsored attacks. It is true that once a computer system is damaged, it is too late for counter-offensive CNA; however, attacking the attacker may halt further attacks from occurring against other systems. As already covered, the government's plan is to respond defensively to an attack, disseminate its warnings, and await the next attack. This may help mitigate the effects of an attack *after it occurs* but it does little else, and it certainly does not *prevent* attacks. In general, deterrence does not work. The U.S. Commission on National Security/21st Century recognized that fact; it said

> taken together, the evidence suggests that threats to American security will be more diffuse, harder to anticipate, and more difficult to neutralize than ever before. Deterrence will not work as it once did; in many cases, it may not work at all.[32]

The threat of exposure, jail time, or fines will not deter state-sponsored cyber-warriors from their acts. In order to avoid strategic surprise and widespread system failures, the best computer defense is offensive CNA that stops further attacks.

DoD is well poised to conduct offensive CNA. The reasons involve more than DoD's prized organizational skills, resources, and educated labor force. DoD requires information dominance to preserve its freedom of action for power projection. Therefore, it is already developing the CNA skills it will need to fight and win on the next battlefield. More than any other agency, DoD cannot rely on defensive measures alone to provide its required freedom of action. This is particularly true in view of the fact that DoD is itself the main cyber target in asymmetric warfare. More than any other agency, DoD is functionally the proper place to turn to when state-sponsored cyber-warriors attack.

To begin with, DoD has lead-agency responsibility in PDD-63 for matters involving national security. Once an attack occurs, DoJ/FBI conduct their initial investigation. If they decide that foreign adversaries are the source of the attack, DoJ stays as the lead agency on criminal attacks and DoD takes the lead on attacks affecting national security. The decision to send a case to DoD for action must follow exhaustive investigation into the sources of the attack. This will be a cooperative effort by many organizations. Once the FBI identifies a state-sponsored cyber-warrior as the culprit, the NIPC must specifically approve the decision for offensive CNA. Given the potential political repercussions of a counter-attack against a foreign-based attacker, that may require approval from the National Command Authority. The tough challenge for the DoJ/FBI is to decide who is the genuine state-sponsored cyber-warrior and who is merely the high school hacker.

DoD is already striving to stay current in CNA technologies and methodologies. Because of its wartime requirements, DoD is investing time and money into refining its offensive CNA capabilities. It has several agencies that have wartime offensive CNA missions, including the Joint Command and Control Warfare Center, the Fleet Information Warfare Center, the Air Force Information Warfare Center, and the Army's Land Information Warfare Activity (LIWA). Based on extensive research, these are the key areas where DoD can leverage its developing wartime CNA capabilities for peacetime use:

- Target state-sponsored cyber-warriors to halt peacetime CNA campaigns against US interests
- Disable state-sponsored cyber-warriors before they can move on and attack additional systems
- Prevent escalation of CNA threats and damage to multiple infrastructures
- Conduct counter-proliferation operations to prevent the horizontal spread of disabling technologies among other state-sponsored cyber-warriors

- Obtain an accurate analysis of state-sponsored CNA capabilities and intentions
- Obtain specific knowledge about foreign security systems in order to avoiding taking down the wrong systems or inflicting unintentional damage on friendly/allied systems
- Gain practice in disabling foreign information systems for later wartime use

Another DoD advantage in conducting peacetime CNA lies in the nature of CNA activities. Fighting a cyber war is more like waging unconventional warfare than fighting conventional warfare. The US has already had an opportunity to put this type of unconventional warfare into practice. CIA Director George Tenet publicly announced in 1998 that the US was devising a computer program that could attack the infrastructure of other countries. Pundits expressed the rationale for the announcement this way: "If a country tries to destroy our infrastructure, we want to be able to do it back. It's the same approach we've taken with nuclear weapons, the prudent approach."[33] The first public application of this doctrine occurred during the Kosovo conflict. Allegedly, the US penetrated Yugoslavia's military computers and placed false radar images on Serbian anti-aircraft networks.[34]

Of all the advantages discussed above, the most salient rational for developing a peacetime offensive CNA capability, and placing it in DoD, is to understand adversary information attack capabilities and intentions. The military needs practice in accurately analyzing the threat and knowing how to disable it in wartime when the stakes are even higher. At a time when over 120 countries are working on information warfare techniques, and where the Chinese and Russians publish warfighting doctrine based on offensive peacetime information warfare, DoD needs to develop its CNA capability in peacetime. Failure to exploit these capabilities could result in compromises to national security. In responding to a recent cyber attack at the Pentagon, the Deputy Secretary of Defense stated, "I am very concerned about our ability to defend the information systems that make actual offensive operations possible."[35] By failing to conduct peacetime CNA against state-sponsored cyber-warriors, DoD allows them to live and fight again in a place and time of their choosing.

There is concern that current US doctrine does not sufficiently appreciate the scope of the threat in peacetime. Despite the mounting evidence of threats from Russia, China, and others, Army doctrine understates the peacetime threat. Figure 2 shows an extract from FM 100-6 depicting the range of expected IO threats in war and peace.[36] Notice along the "adversary" axis that state-sponsored cyber-warriors (which may include Non-state Activists and foreign militaries) are not expected to present threats against US computer networks (unauthorized access, malicious software, database corruption) during peacetime. This is in direct contravention to a mounting body of physical evidence.

A similar disregard for the threat exists at the joint level. Joint doctrine allows that offensive IO occurs across the entire spectrum of military operations. The caveat is that these actions must be permissible under the law of armed conflict, consistent with applicable domestic and international law,

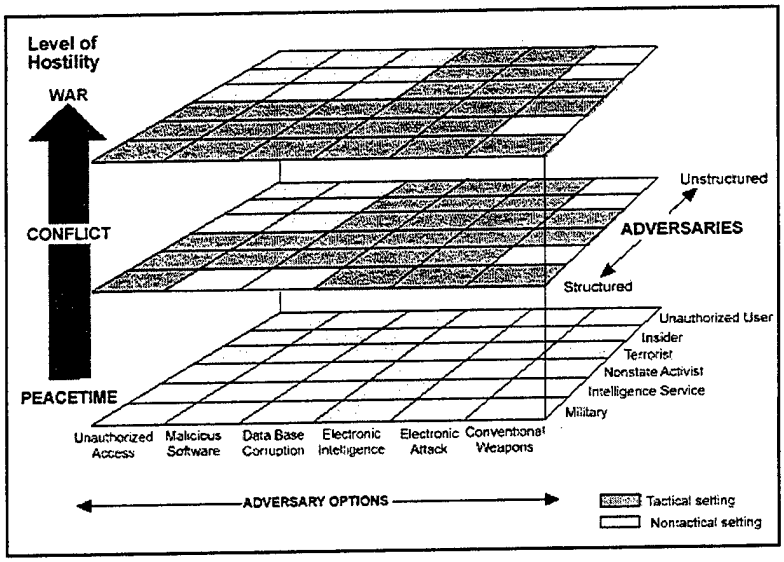

FIGURE 2 INFORMATION OPERATIONS THREATS IN WAR AND PEACE

and in accordance with applicable rules of engagement. Figure 3 shows the notational engagement times for conducting IO according to Joint Publication 3-13.[37] Notice that physical destruction of opposing computer networks and systems is not expected during peacetime. Although the doctrine concedes that CNA is a peacetime option, the idea is approached with temerity and remains protected in legalese. To ensure that ambiguity surrounds CNA, planning and execution guidance for CNA appears separately in a classified annex to the joint publication.

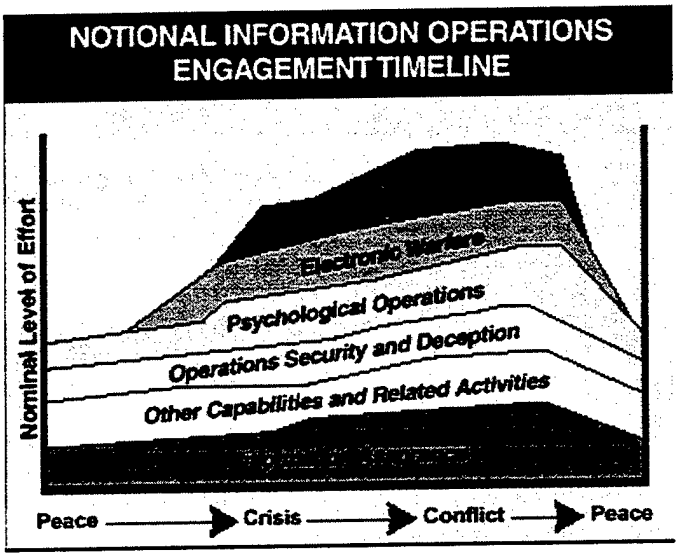

FIGURE 3 NOTIONAL INFORMATION OPERATIONS ENGAGEMENT TIME

There are no strong competitors in lieu of using DoD for peacetime offensive CNA. There are few agencies within NIPC qualified to perform CNA. The FBI has no offensive CNA capability. NSA has no targeting or offensive capabilities; it can supply CNA "know how" through the Information Operations Technology Center (IOTC) and NSA Liaison teams, however, it is not authorized to conduct offensive CNA. The CIA can do some CNA-like functions subject to presidential findings, however, its capabilities are limited. Only DoD possesses the capabilities to step beyond defensive measures and conduct offensive IO and CNA to protect the nation's infrastructure.

POLICY PROHIBITIONS ON CNA

Conducting peacetime CNA is of questionable legality under current international treaties and US law.[38] Employment of offensive CNA capabilities must be consistent with applicable international conventions and agreements, domestic law, and international law. However, international law is ambiguous in its characterizations of CNA. International law leaves it open to the US "to conduct information warfare activities, perhaps even in peacetime, without significant legal repercussions."[39] The rules that govern CNA will likely differ among peacetime, crisis, and conflict situations. International agreements and treaties do not effectively cover processes for engaging nonmilitary computer systems and other information networks during peacetime.

The domestic legal impediments to offensive CNA are not clear. There is essentially no case law and limited customary law to support CNA in peace or war. Federal, State and local laws have not kept pace with the changes in computer technology. The anonymity provided by cyberspace makes it difficult to establish appropriate jurisdictions and venues. The Computer Fraud and Abuse Act of 1986 (the Act), the most comprehensive federal statute on computer crime, is unclear on which cyber activities fall under national security protections. Unfortunately, the act has many loopholes that have allowed adversaries to escape punishment for their crimes. The "inescapable conclusion... was that the 1986 Act was at best ill equipped to combat the war [against cyber threats], and at worst [was] completely ineffective."[40] Its impact on CNA operations against state-sponsored cyber-warriors is open to interpretation.

There are other potential legal impediments to offensive CNA. If the US ties an attack to state-sponsored cyber-warriors and retaliates with CNA, the US could "probably justify its retaliation as part of its right of self-defense as set out in Article 51 of the UN Charter. However, it is not obvious that Article 51 actually provides a basis for military action against a state conducting certain information attacks."[41] Article 51 requires that an "armed attack" must have taken place in order for retaliation to be lawful. It is questionable whether CNA constitutes an armed attack. In fact, there is no clear definition in US doctrine of what action constitutes an attack against the infrastructure (should you even recognize one in progress). This complicates how we can anticipate a country's reaction to US-originated CNA.

The US could ignore Article 51, "hot pursuit", or any other international justifications and simply decide to unilaterally pursue or investigate state-sponsored cyber-warriors across international borders.

In that case, the US cannot expect international cooperation, either from transit countries or the from the source country of the attack. Such a course of action

> Seems likely to violate the sovereignty of those nations, and may be inconsistent with U.S. responsibilities under individual treaties of legal assistance. [I]t would not in itself violate international law any further. The investigation would probably be characterized as espionage.[42]

A doctrine for peacetime CNA has similarities to our past nuclear policy. The US does not disavow the first use of nuclear weapons. If the advocates of deterrence are correct, then a publicized policy of offensive CNA could work much like the "first use" nuclear policy worked against the old Soviet Union and against the Iraqi chemical threat during the Gulf War. We must demonstrate the capability to use CNA and develop a clear belief in the world of our willingness to use it during peacetime. This might serve as a deterrent and prompt Russia, China, and other nations to seek international accords and agreements to limit the use of CNA during war and peace; much like the START treaties have limited our collective nuclear capabilities. On the down side, by demonstrating our willingness to use CNA we may actually escalate the "arms race" in CNA by prompting potential adversaries to further develop their organic CNA capabilities.

PUBLIC RESPONSES TO POTENTIAL OFFENSIVE CNA

From most peoples' perspectives, there is a major difference between wartime and peacetime CNA operations. Any authorization to conduct offensive CNA in peacetime will encounter privacy concerns and will meet with fundamental distrust by the public. The very nature of CNA operations is reminiscent of Orwellian images of Big Brother interfering with the lives of the populace. The only way to mitigate these fears is to conduct *open* (re: unclassified) CNA operations against the state-sponsored cyber-warriors. Although we must protect our methodologies for conducting these counterattacks, we must allow public scrutiny of our purposes of these offensive operations. It is essential to articulate to the public the reasons for these operations and the severe consequences for inaction. The government must target state-sponsored cyber-warriors and not the purveyors of the Internet equivalent of graffiti. The huge public trust placed in the military will quickly dissipate if the country perceives that the military is after anything less than important national security threats.

Some critics of offensive CNA during peacetime may cite The Posse Comitatus Act as legal precedent for prohibiting such action. Congress passed the Posse Comitatus Act of 1878 in order to curb the military's role in law enforcement in the South. Critics suggest that this act may prevent DoD from defending or attacking non-military computer systems. It may restrict the notional authority of DoD to conduct "hot pursuit" of intruders, and the ability to obtain reports from the operators of critical elements of the civil infrastructure.[43] Congress will need to revisit the Act and ensure that the military is not engaging in unwarranted activities when conducting offensive CNA over US networks.

The trade-off we face is complicated. Infrastructure attacks are a clear and present danger to our information-dependent world. Our adversaries demonstrate the proclivity and capability to attack us. Our defensive measures are woefully inadequate to protect the myriad systems in the country. Unless we can counter-attack the attackers, we face strategic surprise and threats to our national security. The price of vigilance is to let the government become more intrusive into our increasingly computerized personnel lives. The only way to keep a check on the government is to keep it in the "open" where its actions are accountable – and out of the strictly covert world. The central issue is how much risk is the country willing to assume. Is the country willing to bear the cost of inaction?

FUNDING REQUIREMENTS OF INFRASTRUCTURE SECURITY

The cost of adequately funding infrastructure protection in all of its forms is expensive. A former Director of NSA has estimated that it could take ten years and $18.0 billion to close the information system security gap.[44] In the civilian sector, most companies only purchase "a minimal capability to detect and conquer sophisticated information attacks."[45] Between 1999 and 2002, DoD plans to spend $3.6 billion to address computer security issues.[46] Clearly, the funding for infrastructure protection is inadequate. A coherent and well-articulated strategy for protecting the nation's infrastructure is useless without the funding to support it.

CONCLUSION

The country does not face an "electronic Pearl Harbor" in the near future; however, the facts portend the use of cyber attacks by state-sponsored cyber-warriors against our country's infrastructure. This paper concludes that the defensively oriented policy measures in PDD-63 are insufficient for protecting our critical information infrastructure. Defensive measures are not working now and because they are entirely reactive by nature, they will not deter future attacks by state-sponsored cyber-warriors. Because the threat is plausible and the potential for severe disruptions is so great, the US must conduct open offensive CNA against state-sponsored cyber-warriors during peacetime.

As long as the electorate is educated on the threat posed by state-sponsored cyber-warriors, they will understand the necessity of conducting offensive CNA. In order to alleviate their inherent fears of subversive covert actions that are anathema to the principles of the country, the nation must be forthright in conducting these operations in the "open." Equally important, the country must obtain the proper legislative endorsements to ensure the international legality of such operations. Lastly, proper security is not a luxury good but is an essential component of every information age system. The country must adequately fund the security requirements of its infrastructure. Until these issues are rectified, state-sponsored cyber-warriors will continue to threaten America's critical information infrastructure and will "present the greatest challenge in preparing for the security environment of 2010-20."[47]

WORD COUNT = 5905

ENDNOTES

[1] U.S. Commission on National Security/21st Century, New World Coming: American Security in the 21st Century, available from <http://www.nssg.gov/NewWorld.nsf/ NewWorld.nsf.htm>; Internet, accessed 10 October 1999, and William J. Clinton, A National Security Strategy for a New Century (Washington, D.C.: The White House, October 1998) 3.

[2] President's Commission on Critical Infrastructure Protection. Critical Foundations: Protecting America's Infrastructures (Washington, D.C.: U.S. Government Printing Office, 13 October 1997).

[3] William Jackson, "DOD Set to Fight Hackers Both Foreign and Domestic," Government Computer News, 23 August 1999, No. 27, Vol. 18, 8.

[4] John Arquilla and David Ronfeldt , "Cyberwar Is Coming!, "Comparative Strategy, 1993, Volume 12, no. 2, pp. 141-165, available at <http://www.stl.nps.navy.mil/c4i/cyberwar.html>; Internet, accessed 7 December 1999. Cyber attacks are equivalent to cyber terrorism. Cyber terrorism "is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents. Politically motivated attacks that cause serious harm, such as severe economic hardship or sustained loss of power or water, might also be characterized as cyber terrorism." See Mark M. Pollitt, "Cyberterrorism: Fact or Fancy?," Proceedings of the 20th National Information Systems Security Conference, October 1997, available at <http://www.infowar.com/>; Internet, accessed 6 February 2000.

[5] A state-sponsored cyber-warrior is distinct from a terrorist or one who conducts state-sponsored espionage. I use the term to reflect an entity that is well organized and financed by the state. This entity conducts cyber activities that are condoned by the state and operates to further state interests. I choose the term "warrior" to differentiate these operatives from terrorists because their aims are not those of terrorists per se.

[6] CJCS, Joint Doctrine for Information Operations, Joint Publication 3-13, (Washington, D.C.: CJCS, 9 October 1998) viii.

[7] U. S. Department of the Army, Information Operations, US Army Field Manual 100-6 (Washington D.C.: Department of the Army, 27 August 1996) 2-3 – 2-4; and Ibid., GL-4-7. The terms are define as follows:

CNA are operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

C2 Attack is the synchronized execution of actions taken to accomplish established objectives that prevent effective C2 of adversarial forces by denying information to, by influencing, by degrading, or by destroying the adversary C2 system.

C2 Warfare is the integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions.

Information Warfare is Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

Information operations are continuous military operations within the Military Information Environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; IO include interacting with the GIE and exploiting or denying an adversary's information and decision capabilities.

[8] U. S. Department of the Army, 3-6.

[9] For definitions of these terms see Charles B. Everett, Moss Dewindt & Shane McDade, "The Silicon Spear an Assessment Of Information Based Warfare (IBW) and U.S. National Security," Sun Tzu Art of War in Information Warfare, available from <http:// sg.yahoo.com/Government/ Intelligence/ Information_Warfare >;Internet, accessed 10 October 1999.

[10] John Christensen, "Bracing for Guerrilla Warfare in Cyberspace," CNN Interactive, available from <http://cnn.com/TECH/specials/hackers/cyberterror/>, Internet, 6 April 1999, accessed 8 October 1999.

[11] Lou Anne DeMattei, "U.S. Vulnerability to Cyber Threat." Officer Review 39 (October 1999), 22.

[12] Tabassum Zakaria, "Economic Espionage Seen Growing Threat To US Firms," available from <http://www.infowar.com/>, Internet, 2 October 1999, accessed 6 February 2000.

[13] CNN, "FBI Follows Internet Chat Room Leads in Hacker Probe," available from <http://cnn.com/2000/TECH/computing/02/15/hacking.investigation.02/index.html>, Internet, 15 February 2000, accessed 15 February 2000.

[14] Federal Bureau of Investigation, available from <http://www.fbi.gov/nipc/nipc.htm>; Internet; accessed 8 October 1999.

[15] Katherine M. Peters, "Information Insecurity," Government Executive, April 1999, 18.

[16] DeMattei, 22.

[17] Christensen, "Bracing for Guerrilla Warfare in Cyberspace," Internet, 6 April 1999.

[18] Douglas Pasternak and Bruce B. Auster, "Terrorism at the Touch of a Keyboard," 13 July 1998; US News Online, available from <http://www.usnews.com/usnews/USNews Computer hackers as terrorists (7-13-98).htm>; Internet; accessed 8 October 1999.

[19] Michael A. Vatis, NIPC Cyber Threat Assessment October 1999, Statement for the Record of Michael A. Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation before the Senate Judiciary Committee Subcommittee on Technology and Terrorism, October 6, 1999, available at <http://www.fbi.gov/pressrm/congress/nipc10-6.htm>; Internet, accessed 12 October 1999.

[20] Bill Gertz, "China Plots Winning Role In Cyberspace," The Washington Times, 17 November 1999, p. 1.

[21] Ibid.

[22] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," Georgetown University, Nautilus Institute, available from <http://www.nautilus.org/info-policy/workshop/papers/denning.html>; Internet; accessed 4 February 2000.

[23] Timothy L. Thomas, "Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations," FMSO Special Study NO. 98-21, available from <http://call.army.mil/call/spc_sdy/98-21/diaverem.htm>, accessed 8 October 1999.

[24] Ibid.

[25] Gregory Vistica, "We're In The Middle Of A Cyberwar," Newsweek, 20 September 1999, 52.

[26] Willis H. Ware, "The Cyber-Posture of the National Information Infrastructure," Critical Technologies Institute, RAND: 1998, vii.

[27] Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," Internet, accessed 4 February 2000.

[28] Robert David Steele, "The Asymmetric Threat: Listening to the Debate," Joint Forces Quarterly, Autumn-Winter 1998-1999, Number 20: 78-79.

[29] DeMattei, 24.

[30] Government Accounting Office, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," GAO/AIMD-96-84, Government Printing Office: May 1996, Chapter 3-2. Also see DeMattei, 23.

[31] Based on a lecture from Frederick G. Tompkins, UNISYS Corporation, Managing Infrastructure Risks in the Next Millennium, lecture on February 10, 2000, USAWC, with permission.

[32] The U.S. Commission on National Security/21st Century, Internet, accessed 10 October 1999.

[33] Christensen, "Bracing for Guerrilla Warfare in Cyberspace," Internet, 6 April 1999.

[34] David A. Fulghum, "Yugoslavia Successfully Attacked by Computers," Aviation Week and Space Technology, 23 August 1999, Vol. 151, No. 8; 31.

[35] Peters, 19.

[36] U. S. Department of the Army, 1-5.

[37] CJCS, II-8.

[38] Christopher Simpson, 145 Congressional Record E 1394, Crisis in Kosovo, 24 June 1999, 106th Cong., 1st sess., Vol. 145, No. 91.

[39] Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, Information Warfare and International Law, Institute for National Strategic Studies, (Washington, D.C.: National Defense University Press, 1997) 93.

[40] Michael Bordera, "The Computer Virus War: Is The Legal System Fighting or Surrendering?," Computers & the Law Project, Fall 1997, available at <http://wings.buffalo.edu/ Complaw/ CompLawPapers/ bordera.html>; Internet, accessed on 15 December 1999.

[41] Greenberg, 83.

[42] Ibid.

[43] Electronic Privacy Information Center, "Critical Infrastructure Protection and the Endangerment of Civil Liberties: An Assessment of the President's Commission on Critical Infrastructure Protection (PCCIP)," available at <http://www.epic.org/>; Internet, accessed on 4 February 2000.

[44] Lou Anne DeMattei, "Developing A Strategic Warning Capability for Information Defense," Defense Intelligence Journal, Vol. 7, No. 2, Fall 1998, 89. By comparison, The New York Times reported in August 1999 that the White House was seeking $1.5 billion in new spending for FIDNET. DOD's Joint

Task Force on Computer Network Defense received $5.2 million in FY99 and the FY00 budget requested $3.2 million.

[45] Ibid., 88.

[46] Peters, 20.

[47] Lawrence Freedman, "America's Achilles' Heel?," Foreign Policy, 22 March 1998, No. 110, 48.

BIBLIOGRAPHY

Arquilla, John and David Ronfeldt. "Cyberwar Is Coming!" Comparative Strategy 12, no. 2 (1993): 141-165.

Boll, Kenneth. Like a Lightning Bolt – Information Warfare. Carlisle Barracks, PA: U.S. Army War College, 1 February 1999.

Bordera, Michael. "The Computer Virus War: Is The Legal System Fighting or Surrendering?" Computers & the Law Project (Fall 1997). Available at <http://wings.buffalo.edu/ Complaw/CompLawPapers/ bordera.html>. Internet. Accessed on 15 December 1999.

Cabral, Paul A. Information Warfare and Information Operations: Protecting the Global Information Environment. Carlisle Barracks, PA: U.S. Army War College, 6 March 1998.

Christensen, John. "Bracing for Guerrilla Warfare in Cyberspace." 6 April 1999. Available from <http://cnn.com/TECH/specials/hackers/cyberterror>. Internet. Accessed 8 October 1999.

CJCS. Joint Doctrine for Information Operations. Joint Publication 3-13. Washington, D.C.: CJCS, 9 October 1998.

Clinton, William J. A National Security Strategy for a New Century. Washington, D.C.: The White House, October 1998.

Coffman, David W. "Operational Art and the Human Dimension of Warfare in the 21st Century." CJCS Strategic Essay Competition, Essays 1999. Washington, D.C.: National Defense University Press, 1999.

Collin, Barry C. "The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge." Speech before the Institute for Security and Intelligence. Available from <http://oicj.acsp.uic.edu/ spearmint/public/pubs/ cjfarrago/terror02.cfm>. Internet. Accessed on 15 December 1999.

Report of the President's Commission on Critical Infrastructure Protection. Critical Foundations: Protecting America's Infrastructures. Washington, D.C.: U.S. Government Printing Office, 13 October 1997.

DeMattei, Lou Anne. "Developing A Strategic Warning Capability for Information Defense." Defense Intelligence Journal. Vol. 7, No. 2 (Fall 1998): 81-121.

DeMattei, Lou Anne. "U.S. Vulnerability to Cyber Threat." Officer Review 39 (October 1999): 22-24.

Deutch, John M. "Foreign Information Warfare Programs and Capabilities." Speech before the Senate Subcommittee on Intelligence, 25 June 1996. Office of the Director of Central Intelligence. Available at <http://www.odci.gov/cia/ public_affairs/ speeches/archives/ 1996/ dci_testimony_062596.html>. Internet. Accessed 15 December 1999.

Electronic Privacy Information Center. "Critical Infrastructure Protection and the Endangerment of Civil Liberties: An Assessment of the President's Commission on Critical Infrastructure Protection (PCCIP)." Available at <http://www.epic.org/>. Internet. Accessed on 4 February 2000.

Everett ,Charles B., Moss Dewindt and Shane McDade. "The Silicon Spear an Assessment Of Information Based Warfare (IBW) and U.S. National Security." Sun Tzu Art of War in Information

Warfare. Available from <http:// sg.yahoo.com/Government/Intelligence/Information_Warfare >. Internet. Accessed 10 October 1999.

Federal Bureau of Investigation. Available from <http://www.fbi.gov/nipc/organization.htm>. Internet. Accessed 8 October 1999.

Federal News Service. Available from <http://www.fns.gov >. Internet. Accessed 16 September 1999.

Freedman, Lawrence. "America's Achilles' Heel?" Foreign Policy. 110 (22 March 1998): 48-59.

Fulghum , David A. "Yugoslavia Successfully Attacked by Computers" Aviation Week and Space Technology. 151 (23 August 1999): 31.

Gertz, Bill. "China Plots Winning Role In Cyberspace." The Washington Times, 17 November 1999, p. 1.

Greenberg, Lawrence T., Seymour E. Goodman and Kevin J. Soo Hoo. Information Warfare and International Law. Institute for National Strategic Studies. Washington, D.C.: National Defense University Press, 1997.

Goldstein, Steve. "Pentagon Planners Gird For Cyber Assault." Philadelphia Inquirer, December 1, 1999, p. 1.

Government Accounting Office. "DoD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk." GAO/AIMD-99-107. Washington, D.C.: U.S. General Accounting Office, August 1999.

Government Accounting Office. "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks." GAO/AIMD-96-84. Washington, D.C.: U.S. General Accounting Office, May 1996.

Jackson, William. "DoD Set to Fight Hackers Both Foreign and Domestic." Government Computer News. 27 (23 August 1999): 8.

NIST Computer Security Resource Clearinghouse. "Computer Attacks: What They Are and How to Defend Against Them." Available at <http://csrc.nist.gov/ nistbul>. Internet. Accessed on 15 December 1999.

Pasternak, Douglas and Bruce B. Auster. "Terrorism at the Touch of a Keyboard." 13 July 1998. US News Online. Available from <http://www.usnews.com/usnews/USNews Computer hackers as terrorists (7-13-98).htm>. Internet. Accessed 8 October 1999.

Peters, Katherine M. "Information Insecurity." Government Executive. (April 1999):19.

President's Commission on Critical Infrastructure Protection. Critical Foundations: Protecting America's Infrastructures. Washington, D.C.: U.S. Government Printing Office, 13 October 1997.

Rasch, Mark D. Center for Information Protection Science Applications International Corporation. Available at<http://cla.org/RuhBook/chp11.htm>. Internet. Accessed on 15 December 1999.

Ross, Mitchell S. National Information Systems: the Achilles Heel of National Security. Carlisle Barracks, PA: U.S. Army War College, 3 April 1997.

Schjolberg, Stein. "The Legal Framework - Unauthorized Access to Computer Systems: Penal Legislation in 37 Countries." Available at < http://www.mossbyrett.of.no/ info/legal.html#37>. Internet. Accessed on 15 December 1999.

Simpson, Christopher. 145 Congressional Record E 1394, Crisis in Kosovo, 24 June 1999, 106th Cong., 1st sess., Vol. 145, No. 91.

Steele, Robert David. "The Asymmetric Threat: Listening to the Debate." Joint Forces Quarterly. 20 (Autumn-Winter 1998-1999): 78-79.

Stewart, Michael A. Information Operations, Information Warfare: Policy Perspectives and Implications for the Force. Carlisle Barracks, PA: U.S. Army War College, 15 April 1997.

Thomas, Timothy L. "Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations." FMSO Special Study NO. 98-21. Available from <http://call.army.mil/call/spc_sdy/98-21/diaverem.htm>. Internet. Accessed 8 October 1999.

U.S. Commission on National Security/21st Century. "New World Coming: American Security in the 21st Century." Available from <http://www.nssg.gov/NewWorld.nsf/ NewWorld.nsf.htm>. Internet. Accessed 10 October 1999.

U. S. Congress. Senate. 145 Congressional Record S6471. National Defense Authorization Act for Fiscal Year 2000. 106th Cong., 1st sess., 7 June 1998, Vol. 145, No. 79.

U. S. Department of the Army. Information Operations. U. S. Army Field Manual 100-6. Washington D.C.: Department of the Army, 27 August 1996.

Vatis, Michael A. NIPC Cyber Threat Assessment October 1999. Statement for the Record of Michael A. Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation before the Senate Judiciary Committee Subcommittee on Technology and Terrorism. October 6, 1999. Available at <http://www.fbi.gov/pressrm/congress/nipc10-6.htm>. Internet. Accessed 12 October 1999.

Vistica, Gregory. "We're In The Middle Of A Cyberwar." Newsweek, 20 September 1999, 52.

Ware, Willis H. "The Cyber-Posture of the National Information Infrastructure," Critical Technologies Institute, RAND: 1998.