STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

DEFENSE OF CRITICAL INFRASTRUCTURE

BY

LIEUTENANT COLONEL LESTER H. LETTERMAN
United States Army Reserve

19990608 056

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1999

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

DTIC QUALITY INSPECTED 1

USAWC STRATEGY RESEARCH PROJECT

DEFENSE OF CRITICAL INFRASTRUCTURE

by

LTC Lester H. Letterman
U.S. Army Reserve

Robert F. Minehart, Jr.
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

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

ABSTRACT

AUTHOR: Lester H. Letterman

TITLE: DEFENSE OF CRITICAL INFRASTRUCTURE

FORMAT: Strategy Research Project

DATE: 7 April 1999

PAGES: 34

CLASSIFICATION: Unclassified

Accompanied by a new play of forces and dynamics, the age of geopolitics is giving way to the age of geoeconomics. Within our national security apparatus a strong tendency still exists to view foreign and domestic problems from a nineteenth century perspective. America's predominant leadership role, national resolve and power are being tested more frequently in a world free of the bipolar constrains of the Cold War. To obtain the desired synergistic relationship among economic, diplomatic, and military elements of power our National Security Strategy must conduct an unambiguous assessment of our interests, threats, and requirements in this emerging world order. The likely near term threats to our security will avoid America's military strengths and be directed toward the more accessible targets, our national resolve and economy. An asymmetric strike against our critical infrastructures seems the most likely means of attack. Electric power, telecommunications and transportation are among those

systems whose incapacity or destruction would have a debilitating impact on the defense and economic security of our nation. In recognition of America's dependency and vulnerability, the Department of Defense should be brought center stage in a role of Homeland Defense to protect our national infrastructures.

TABLE OF CONTENTS

ABSTRACT iii

DEFENSE OF CRITICAL INFRASTRUCTURE 1

ENDNOTES 27

BIBLIOGRAPHY 29

DEFENSE OF CRITICAL INFRASTRUCTURE

" to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."
Sun Tzu, The Art of War [1]

An analogy to Darwin's concept of evolution is appropriate for examining America's emerging strategy for security of our critical infrastructure. Like a living organism, the ability of a nation to adapt to its' environment enables it to compete successfully and ultimately determines its' survival or extinction. As a nation, we are increasingly dependent on information technologies and infrastructures to maintain a competitive economy, capable military and government, and public services. As our society grows more complex this reliance will continue and intensify.

Amid the stand off between the Cold War superpowers, the threat of nuclear war nurtured a competitive equilibrium. The playing field and game rules were understood. The potential consequences kept the game in check. In a large sense the Cold War created a period of global security and stability by subduing ethnic, religious and nationalist tensions beneath the

larger bipolar struggle between communism/authoritarian government and capitalism/democracy. Following the collapse of Eastern European communist regimes in 1989 and the dissolution of the Soviet Union in 1991, it was soon apparent how many latent conflicts were released from the domination of the Cold War. These conflicts have emerged to face the United States with a burgeoning array of significant, if tangential, threats to our national security.

TEOTWAWKI is a whimsical acronym derived from; "The end of the world as we know it." It is an idiom that aptly expresses how rapidly and completely transformation of the world is occurring. It implies a changed present, an uncertain future, and ineffectiveness in perceiving and reacting to new forces and new dynamics with yesterdays' concepts[2]. As the remaining superpower of the Cold War, the United States finds itself in a predominant leadership role. American resolve and power are being tested more frequently. Precisely because of this, America must understand and respond to threats and risks for what they are and for what they may become.

Since the end of the Second World War America's defense strategy has been one of deterrence. A strategy demanding the acme of skill according to Sun Tzu[3]. With the end of the Cold War

many reflective thinkers in the military have pronounced our arrival at a "strategic pause" in preparation for emergence of the next peer competitor. Deterrence by its very definition implies shaping the future environment requires engagement today. America may have an interlude in discerning strategic threats; however, nothing approaching an "operational pause" has occurred in America's response to many peripheral national interests. Effective competitors to America's interests do not have to be peers, regional hegemonies or even nation states.

A nation's strength is a consummation of its' national resolve to apply elements of power; economic, political or military, to achieve national goals. The relative power of nation is often viewed in terms of this empirical formula. This simplified observation does not clearly characterize the components of national resolve or the elements of power as discreet factors that can be individually targeted and defeated in detail. The United States is unchallenged militarily by a peer competitor and direct threats to the sovereignty of the United States seem unlikely. Consequently, the likely near term threats to our security will avoid America's strengths and be directed toward what I believe are the more accessible targets, national resolve and the economy.

Sun Tzu was enlightened in his view that warfare conducted by other than military means is not analogous to a war of limited objective[4]. Wars can be fought, won or lost beyond the battlefield. The Vietnam War demonstrated that tactical and operational success on the battlefield does not equate to victory[5]. More recently, the Gulf War assured the American people that we have the military strength and technology to decisively prevail in a modern military campaign and again illustrated that battlefield success does not correlate to attainment of political aims. The achievement of victory requires subjugation of the enemy's will to the desired political end[6]. Military preeminence can be rendered a moot point and military victory hollow.

America's political, military and economic elements of power are interrelated, but economic capacity is decidedly the foundation of our strength. Our strong economy provides an advantage over potential adversaries and constitutes an important element of national strength, influencing both military and political strengths as well. Our economic power is dependent on our national infrastructures. Since the beginning of strategic bombing, an attack on a nation's economy has been conducted by attacking its' underlying infrastructures. Critical national infrastructures are those systems whose incapacity or

destruction would have a debilitating impact on the defense or economic security of our nation. These critical infrastructures include electrical power systems, telecommunications, gas and oil pipelines, transportation, banking and finance, water supply and waste treatment systems, emergency services (including medical, police, and fire), and continuity of government.

It is not apparent how gradual, unrelenting and pervasive the dependence on information technology and stable infrastructure has become in dominating the commerce of our country. At a "macro" level, the reliability of our infrastructures encourages further reliance on automated systems. Business systems are designed, developed and deployed fully dependent upon our large and competent infrastructures. To realize cost savings and the efficiencies of automation, redundancy is not maintained to overcome unlikely, temporary or isolated disruption of utility services. For example at supermarket checkouts; a scanner reads barcodes on the product label, the system accesses a central database of prices, items are added to your bill and totaled, on-the-shelf inventory adjusted and reordered, and possibly payment is accepted electronically through a credit charge. If the power goes off, everything stops.

America has embraced the efficiencies of technology in automating physical processes as well. Practically every infrastructure in this country is remotely operated by computer systems called SCADAS, Supervisory Control and Data Acquisition Systems. Computer software controls everything from traffic lights to industrial processes. The processes are themselves often too complex to be effectively controlled without the help of computers. We have used SCADAS for decades and they have proven extremely effective and reliable. SCADAS are deployed where process needs to be controlled. Connected via public networks, remote sensors and control devices direct valves, switches, and pumps. More and increasingly critical processes have been relegated to the able disposition of software controlled SCADAS. Like the supermarket example, achieving operational efficiencies of process automation is a one way conversion.

The national security implication of the vulnerabilities of information technology used as the primary method of control to both physical and business processes is immense. Because of the interdependence among the infrastructures, even a minor and temporarily successful attack on a single critical system can have a devastating domino effect reaching beyond the industry directly affected. One upset domino can instigate a cascade of

successive failures of increasing magnitude potentially leading to an eventual collapse. An intermittent power failure can shut down the telecommunication system, the banks, sewage treatment plants, transportation and distribution systems. It is estimated that the repercussions of a reduction of only a few percent in efficiency or availability of services could produce second and third order effects that would exponentially weaken the entire U.S. economy[7].

Threats to critical infrastructures fall into three categories: physical, psychological and cyber. Our infrastructure is highly susceptible to sabotage. The components of our infrastructures are too vast and our society too open to thwart a physical assault. Employing guards, locks and fences is possible for only a small percentage of the overall physical structure. Power transmission towers, microwave relays, pipelines, railroads and bridges are opportune targets as they cross the farmlands, deserts and forests of our country. Remoteness is not itself an indicator of vulnerability. Bombings of the World Trade Center and the Oklahoma City Federal Building illustrate the modicum of effort that must be taken to disguise conduct of terrorist activities in a society as open as ours.

Any attack on American soil would impart a strong psychological effect. Whether a domestic bombing or a cyber attack launched from overseas, the affect on the American psyche would be similar. Separated by oceans and friendly neighbors, America has felt immune from many of the world's troubles. Continued unanswered or unanswerable attacks on our infrastructure would have a demoralizing effect on the will of the people. The loss of people's confidence in their government, military or economic foundation poses a discernable threat to national security. The public has high expectations for the reliability of our public services. The perceptual threat is tied to this expectation. It can be mitigated by shaping the public's expectations of the ability of the government to respond to an attack on our infrastructures and by acknowledging that in an attack some systems might temporarily fail.

Although potentially devastating, the current cyber threat to the United States has not been fully acknowledged. Potential threats can be foreign or domestic, internal or external, state-sponsored groups or individuals. This profile includes everything from teenage hackers, terrorists, organized crime, to sophisticated state sponsored attacks. In business, society, and warfare the capabilities and the vulnerabilities of information-based technologies have been increasingly pressed onto center

stage. As the military, economic and diplomatic elements of national power have become increasingly dependent upon information systems and information capabilities, we have begun to recognize the possibility of an adversary exploiting our dependency and the vulnerability of this new technology.

For three months during the summer of 1997, the Joint Chiefs of Staff conducted an exercise to test America's ability to withstand an organized and systematic cyber-attack. The exercise was code-named Eligible Receiver. The "bad guys" were composed of thirty-five hackers from the National Security Agency. They used only commercially available laptop computers, information and techniques downloaded from the Internet. They received no insider information and no advance intelligence data. They were allowed to attack only unclassified systems and were compelled to work within the law and the rules of the exercise. The cyber-attacks focused on three areas: the national information infrastructure, military networks, and political leadership. In each of these areas, the hackers were able to penetrate apparently well defended systems; including the electrical power grids for Detroit, Chicago, Los Angeles, St. Louis, Colorado Springs, Tampa, Oahu, and Washington D.C. The result within the game scenario was a serious degradation of the Pentagon's ability to deploy and to fight. In response to a hypothetical

international crisis in the exercise, had deployment been possible, the assessment was that with the psychological effects of the attacks it would have been unlikely that the President would have committed forces to the conflict[8].

The "off-the-shelf" attack by a handful of artificially constrained computer specialists demonstrated that we are susceptible to a strategic-level assault that is technologically feasible today. Ninety plus percent of military systems rely on Commercial off the Shelf (COTS) software and public carriers. Given that our potential adversaries have access to virtually the same information technologies that we have and that most attacks successfully exploit known security weaknesses; the likelihood of a successful attack of our military systems is almost assured. At risk are the military's mobility, logistics, command, control, communications, and intelligence systems, as well as, the infrastructure supporting our industrial base.

The issue materializing as the most likely near-term threat to national security is a cyber-attack on the infrastructures supporting both our economy and society. With information compiled from unclassified sources and briefings received by the Defense Science Board from subject matter experts within the Department of Defense (DOD) and throughout the civilian sector,

the chart below depicts the possibility of a cyber-attack against the United States is a real and growing threat[9].

IW Threat Estimate

	Validated Existence	Existence Likely but not Validated	Likely by 2005	Beyond 2005
Incompetent	W			
Hacker	W			
Disgruntled Employee	W			
Crook	W			
Organized Crime	L		W	
Political Dissident		W		
Terrorist Group		L	W	
Foreign Espionage	L			
Tactical Countermeasures		W		
Orchestrated Tactical IW			L	W
Major Strategic Disruption of U.S.				L

W = Widespread; L = Limited

The Defense Information Systems Agency (DISA) officially reported attacks to DOD networks as; 1992, 53 attacks; 1993, 115 attacks; 1994, 255 attacks; 1995, 559 attacks; 1996, more than 725 attacks; and in 1997, 575 attacks[10]. DISA believes the 500 actual reports of intrusion efforts equates to as many as 250,000 intrusion attempts. Estimates of the potential number of computer attacks are based on DISA's own Vulnerability Analysis and Assessment Program, which used DISA personnel to attempt to penetrate computer systems at various military and defense agency sites via the Internet. Since the program's inception in

1992, DISA has conducted almost 38,000 attacks on its' own computer networks. DISA successfully gained access 65 percent of the time. Of these successful attacks, only 988 or about 4 percent were detected by the targeted organizations. Of those detected, only 267 attacks or roughly 27 percent were reported[11].

The newest buzzword in the military establishment is Information Warfare. This term is used as if it identified a single definable new strategy, comprising everything from hacking to psychological operations. America's post Cold War campaigns have alerted many countries to the importance of targeting information systems as a preliminary step in any conflict: to defeat your opponent's will, to destroy command and control systems, and to attack the economic infrastructure. The National Security Agency (NSA) has acknowledged that potential adversaries are developing a body of knowledge about DOD and other U.S. systems, and methods to attack these systems. According to NSA, these methods include sophisticated computer viruses and automated attack routines that could allow adversaries to launch anonymous attacks from anywhere in the world. A single denial of service attack of a critical system at a critical point or a widespread intermittent disruption of information systems could serve to perilously degrade the nation's ability to deploy and sustain military forces. The NSA

estimate is that more than 120 countries have established computer attack capabilities. In addition, most countries are believed to be planning some degree of information warfare as part of their overall security strategy[12].

In recognition of threats to our national infrastructures, President Clinton signed Executive Order 13010 on July 15, 1996, establishing the President's Commission on Critical Infrastructure Protection (PCCIP). The Commission was chartered to formulate a comprehensive national strategy for protecting critical infrastructures. It's final report provided seventy-six proposals and recommendations and concluded that critical infrastructure be defended by whatever means necessary. The Critical Infrastructure Protection Directive (PDD-63) was released in May 1998. It was designed to strengthen the nation's defenses against the growing threat of unconventional and asymmetric attacks against our critical infrastructures.

The Department of Justice (DOJ) was assigned responsibility for facilitating and coordinating the federal government's interagency response for ensuring the successful implementation of infrastructure protection. However, the DOJ has not demonstrated that it possesses the necessary strategic vision to direct these activities in a systematic and comprehensive way.

The missions, goals and legal authorities of law enforcement are culturally different from the national security agencies. The approach of law enforcement is essentially reactive to the commission of a crime; to investigate and prosecute individuals who violate United States laws. National security is addressed collectively and proactively under a policy of deterrence.

As a measure to deter crime, America has unilaterally declared its right to pursue criminals and terrorists across national boundaries. This makes for good press, but it does not expand our jurisdiction. Extraterritorial law enforcement impinging upon sovereignty and international law is an act of war. Perpetrators of transnational crimes are generally safe from retribution beyond national boundaries because of ambiguous international law and the unwillingness of countries to bring to trial crimes committed abroad and under the laws of another country.

Applying U.S. criminal statues extraterritorially also implies applying other standards of U.S. law; compiling proof beyond a reasonable doubt and rules of evidence. Common methods of collecting national security intelligence are not compatible with the methods employed by the law enforcement community. The legal authority and means permitted for law enforcement to

engage in domestic intelligence collection differs so greatly from that of foreign intelligence collection that, in most instances, information obtained would be inadmissible in court, valueless to criminal investigators and could possibly taint the prosecution's case under domestic statues. Developing proof beyond a reasonable doubt under the concept of U.S. law will be difficult[13].

Law enforcement is generally concerned with the commission of crime as a singular act. For a state-sponsored act of terrorism or cyber-attack, arresting the perpetrators of a single "crime" will have minimal impact. Applying diplomatic, economic, or military power in many cases is a more appropriate response than a strict law enforcement response to a "crime" committed on U.S. soil. A foreign individual or group does not necessarily have to be dealt with as a criminal for violating U.S. law.

As criminal activity has become more global, law enforcement agencies have become increasingly interested in obtaining information about criminal activities outside the United States. At the same time, the national intelligence community has overlapping interests with the domestic component of the total intelligence picture. Increasingly the same groups are responsible for criminal activity both inside and outside of the

United States. The traditional boundaries that have delimited national security from law enforcement are blurred in today's international environment. Much of the thinking about national security still holds to the old-fashioned view that problems outside of the borders of the United States are national security problems, problems inside of the borders are law enforcement problems. Criminals and terrorists already exist in a world without borders. The current world situation strongly suggests that we need to reassess *posse comitatus*[14].

Where law enforcement is the most appropriate response, the Attorney General should direct investigations and prosecutions. What is missing from the current DOJ lead is a means to provide an early decision to give priority of response in an incident to law enforcement or national security. Adopting a policy to provide an early decision would require developing a national level early warning system. This warning system must be capable of assessing and categorizing incidents and indicators to correctly diagnose an event as accidental, criminal, or as part of a coordinated attack. Such a system does not exist.

With the Treaty of Westphalia in 1648 only sovereigns have been recognized as international players with the authority to make treaties or declare war. Today, a measure of power equal to

that of a sovereign state is wielded by entities other than nations. The parity of national power can be mimicked by economically and politically powerful transnational corporations or singular criminal, ideological, or religious zealots or organizations who have the political resolve and access to an increasing available arsenal of potent weapons; chemical, biological, cyber and terrorism. These new players are not bound by the conventions of nation states. Lacking geographical or political boundaries; the traditional means of leveraging reproof often can not be effectively brought to bear against these non-sovereigns. The elements of national power are broader in their employment. Contending with such international players on issues having a domestic security implication is more akin to foreign policy than it is to law enforcement and our domestic security is better treated as a national security issue rather than a law enforcement issue.

Providing for the common defense and securing domestic tranquility are the responsibility of government. During the Cold War the economic strength of the military-industrial complex brought entire industries and infrastructures into existence. The government dictated operational rules and could expect compliance. Nominally business was charged to act within the benign environment of commerce. Today, the private sector is

the economic engine of change driving the innovations and influencing the technology envelope. The political reality is that the government is without effective market leadership or the ability to exert influence over formal or informal players. The assumption of risk associated with today's non-benign business environment must be shifted from the government to the private sector either through regulation or market force.

The DOJ has not pursued a meaningful legislative agenda to adequately address business liability. The software industry especially has run unchecked and unchallenged in delivering goods that do not provide their advertised level of performance or security. Applying the same standards of product liability to the producers of software as we have to everything from baby toys to breast implants is the appropriate means of ensuring software products conform to standards. Market forces will drive the specifications for performance and help determine the criteria and boundaries for operating systems and applications suitable for home use, business use and critical processes.

The same health, welfare and safety arguments that regulate everything from automobile exhaust emissions to the expiration date of milk should be applied to industries that we rely upon for many of our basic services. Court challenges and class

action lawsuits, perhaps initially even spearheaded by DOJ, may be required to ensure adequate delivery of service. Corporate liability is limited to the failures to follow security regulations or generally accepted security precautions, of which there are too few. Lacking proof of efficacy, industry has been able to successfully fend off imposition of any mandated regulations for preventing, detecting, and reporting attacks on information systems.

For the most part the economic infrastructures of the United States are privately owned. The cultural perspective with which the public and private sectors view the acceptance of risk is very different. In matters of national security the policy of our government has been to avoid risk rather than to anticipate and attempt to manage it. The private sector has sought to manage risk rather than to avert risk. Capitalism by its very nature is not averse to risk. Higher risk is accepted for greater return. Return on investment drives the corporate decision process.

Individual corporate security measures rest on the periphery of the organized and collective approach necessary for protection of our integrated infrastructure. Corporate policies of risk management have emphasized efforts directed toward

protecting data, services and assets and for quick recovery should systems be brought down or compromised. The business risk associated with an attack on U.S. infrastructure, whether physical or cyber, is perceived as insignificant. Most companies would find it more advantageous to write off such losses as a cost of doing business rather that protect against such possibility. This fails to acknowledge the national security implications of the losses, or lessen the importance of those losses, or the need to address the vulnerabilities that produced the losses.

All of our infrastructures are regulated in some part by federal, state and local government. All of our infrastructures are influenced by market force. Regulation and market force are antagonistic. Business is not likely to endorse measures that reduce the efficiency, effectiveness or endure the financial cost of redesigning and replacing existing systems in which many of these industries have invested billions of dollars. Market forces limit the extent of self-protection to the corporate boardroom's recognition of business risks.

Redundancy, surge capacity, and the ability to rebuild and reconstitute are requirements for our infrastructure from a national security perspective. Robustness of our infrastructures

comes at a price. From a business perspective there is no bottom line return for substantial investment required in national security. Deregulation of many of our utilities means business is already working more closely on the margin; a downsized workforce, reliance on automation, just-in-time inventories, minimal excess capacity, and limited system redundancy are essential for a business to stay competitive. All of which are factors diametrical opposite to what is needed to ensure survivability and resilience of our infrastructure.

The DOJ must reconsider the validity of some of its' assumptions and cease its encryption paranoia. There are many legitimate uses for encryption. The confidence and safety provided by the business use of encryption technology far out weigh the potential loss to law enforcement and intelligence gathering. A readily available campaign slogan could be adapted from the opponents of our gun control policy "When encryption is outlawed only outlaws will have encryption." A policy mandating encryption for regulated businesses would be low cost and effective means to alleviate some of the risk of a potential cyber-attack.

What is most needed for our uncertain future is a coordinated policy bringing together the ends, ways and means required to

defend and to shape our critical infrastructure. The means seem fairly obvious, a legislative agenda to underwrite the financial burden. The appropriate vehicles for underwriting this effort could be tax incentives, government subsidization or rate regulation passing the costs back to the consumer. The ways of the policy are controversial. In a cyber-attack or for the terrorist the advantage is to the attacker, a thousand to one. In the context of asymmetric warfare, to be successful the defender must defend all of his critical systems; everywhere, at all times, against every known exploit and possible weakness. What makes the issue so complex and controversial is the expense of developing and administrating such a robust infrastructure. Business is leery of an imposed theoretical solution. It is not superficial to say the lowest common denominator to the problem has been to develop a reputable solution.

Wars are not won by defensive operations; but wars can be lost by failure to conduct defensive operations. National policy must emphasize defense of critical infrastructures as vital to our national security and treat information technology as a strategic resource. Recognizing the strategic threat associated with our dependence and the need to protect our critical infrastructure demand a policy of proactive domestic preparedness to minimize degradation of our capability and our

will to wage war. The safety of our economy, society and institutions must be guaranteed before we endeavor to pursue a policy of deterrence and engagement abroad.

America is no better prepared today than it was four years ago with the issuance of Executive Order 13310 and PDD-63. Little has transpired toward protection of our infrastructures beyond the development of a cottage industry to provide rhetoric and literature warning of the catastrophic consequences of ignoring the problem. No serious debate outside of the government is arguing a case of corporate good versus public good for a civil defense of our infrastructures. The official policy is floundering and still proffers a cum-by-ya approach between the public and private sectors to arrive at a mutually acceptable solution. Not likely! The DOJ has not aggressively provided leadership for a developing a comprehensive national policy and instead, working within its' comfort zone, has continued to address matters within the auspices of law enforcement.

America faces a serious national security issue when individuals or small groups of people possess the capability for force projection and can effectively wage war asymmetrically against the most powerful country in the world. Potentially undeterred by military superiority, all industrial democracies

are susceptible to coordinated, sophisticated attacks against infrastructure. The United States may possess superior military forces but not be capable of defending our interests. Neither oceans, deployed forces, nor coalition allies can be interposed between our critical infrastructure and potential enemies. Protecting our infrastructures has become a force protection issue.

There is still a strong tendency to view current foreign and domestic problems from a nineteenth century perspective. In the new millenium the age of geopolitics is giving way to the age of geoeconomics. The desired synergistic relationship among economic, diplomatic, and military instruments requires an unambiguous assessment of interests, threats, and requirements. Recognizing our dependency and the vulnerability of our critical infrastructures will bring them to center stage of our national security policy.

Since the end of the Cold War America's military has responded to many threats with a diverse set of non-traditional military missions: humanitarian assistance, counter-drug, counter-proliferation and peace keeping operations. Congressional interest affirmed by the Nunn/Luger/Domenici Domestic Preparedness Act recognizes the military has a role in the

preparation for countering and responding to domestic terrorism and weapons of mass destruction incidents. The current National Security Strategy incorporated Homeland Defense as a mission for the Department of Defense. These events have signaled a shifting focus of our military strategy from one of force projection to one including domestic defense[15]. It is premature to advocate the demise of maneuver warfare as the military's traditional role; however, tenants of what constitutes the mission of providing national security are broadening.

The DOD is the federal agency most likely to develop solutions to the problems of cyber-attack. DOD is consolidating responsibility for computer network defense and mandating DOD wide practices and standards for security activities such as vulnerability assessments, reporting of attacks, correction of vulnerabilities, and damage assessments. DOD's significant network structure will serve as a test bed to yield data that can be taken to corporate boardrooms or to Capitol Hill. DOD will credibly be able to articulate efficacy and cost of a cyber-security policy.

Raising the bar to protect our infrastructures from cyber-attack is not cost prohibitive. Treating infrastructure protection as a national security issue rather than a law

enforcement issue would sanction passing policy leadership to DOD. Given interagency leadership, DOD can pursue a legislative policy to enforce security measures across industries as a measure of deterrence. Laws and policies must be changed to link business risk of corporate liability with conformity to some generally accepted security policies and technologies. The essence of these private sector cyber-defense technologies and policies can be instituted from DOD's own efforts to develop and test cyber-defense solutions. Giving recognition for the defense of our infrastructure as a legitimate Homeland Defense mission will enable DOD to obtain the required funding in the programming and budgeting process.

Word Count: 5155

ENDNOTES

[1] Sun Tzu, The Art of War, trans. Samuel Griffith (New York: Oxford University Press, 1963), 76.

[2] The ideas of this paragraph are based upon remarks made by a speaker to the U.S. Army War College's, Information Warfare Class, March 1999.

[3] ibid, Sun Tzu.

[4] Ibid, Sun Tzu.

[5] Harry G. Summers, Jr., On Strategy, A Critical Analysis of the Vietnam War (New York: Dell Publishing Company,1984), 21.

[6] Carl Von Clausewitz, On War, trans. Michael Howard and Peter Paret (New Jersey: Princeton University Press, 1976), 75.

[7] Robert F. Minehart, Jr., The Information Assurance Seminar Game (Carlisle Barracks: U.S. Army War College Center for Strategic Leadership, 1998), 6-7.

[8] James Adams, "BIG PROBLEM-BAD SOLUTION: The Crisis in Critical Infrastructure and the Federal Solution," May 18, 1998, available from <http://206.132.10.154/idmarketsite/jadocs/Online.doc>; Internet; accessed January, 14 1999.

[9] Office of the Under Secretary of Defense for Acquisition and Technology, Report of the Defense Science Board Task Force on Information Warfare - Defense (IW-D), (Washington, D.C, U.S. Government Printing Office, November 1996), Appendix A.

[10] Office of the Assistance Secretary for Defense Public Affairs, "DoD News Briefing," April 23, 1998, available from < http://www.defenselink.mil/news/Apr1998/t04231998_t0423asd.html> ; Internet; accessed January 15, 1999.

[11] GAO Executive Report B-266140, "Defense Information and Financial Management Systems" available from <http://www.infowar.com/civil_de/gaosum.html-ssi>; Internet; accessed January 15, 1999.

[12] ibid, Report of the Defense Science Board Task Force on Information Warfare.

[13] Abram N. Shulsky, Silent Warfare, Understanding the World of Intelligence (New York: Brassey's Publishing, 1993), 164-165.

[14] Posse Comitatus Act, U.S.Code, vol. 10, sec. 1385 (1878). Passed in 1878, this act prohibits military participation in domestic law enforcement. National Guard units acting under command of a state governor are exempt from the provisions of the act.

[15] The White House, A National Security Strategy for a New Century, October 1998, 19-21.

BIBLIOGRAPHY

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

Clausewitz, Carl. On War. Translated by Michael Howard and Peter Paret. New Jersey: Princeton University Press, 1976.

Summers, Harry G. Jr.. On Strategy, A Critical Analysis of the Vietnam War. New York: Dell Company, 1984.

Minehart, Robert F. Jr.. The Information Assurance Seminar Game. Carlisle Barracks: U.S. Army War College Center for Strategic Leadership, 1998.

Adams, James. BIG PROBLEM-BAD SOLUTION: The Crisis in Critical Infrastructure and the Federal Solution. May 18, 1998. Available from <http://206.132.10.154/idmarketsite/jadocs/ Online.doc>. Internet. Accessed 14 January 1999.

Office of the Under Secretary of Defense for Acquisition and Technology. Report of the Defense Science Board Task Force on Information Warfare - Defense (IW-D). Washington, D.C.: U.S. Government Printing Office, November 1996.

United States Department of Defense, Office of the Assistance Secretary for Defense Public Affairs. "DoD News Briefing." April 23, 1998. Available from <http://www.defenselink.mil /news/ Apr1998/t04231998 t0423asd.html>. Internet. Accessed 15 January 1999.

General Accounting Office. "Executive Report B-266140, Defense Information and Financial Management Systems." Available from <http://www.infowar.com/civil de/gaosum.html-ssi>. Internet. Accessed 15 January 1999.

Shulsky, Abram N.. Silent Warfare, Understanding the World of Intelligence. New York: Brassey's Publishing, 1993.

Posse Comitatus Act. U.S.Code. Vol. 10, sec. 1385 (1878).

The White House. A National Security Strategy for a New Century. October 1998.