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.

STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS: COMPUTER NETWORK ATTACK IN THE 21ST CENTURY

BY

20020604 228

LIEUTENANT COLONEL JENNIE M. WILLIAMSON
United States Army

DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2002

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

USAWC STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS: COMPUTER NETWORK ATTACK IN THE 21st CENTURY

by

Lieutenant Colonel (P) Jennie M. Williamson
United States Army

Colonel David Lopez
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.

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

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

ABSTRACT

AUTHOR: LTC Jennie M. Williamson

TITLE: Information Operations: Computer Network Attack in the 21st Century

FORMAT: Strategy Research Project

DATE: 09 April 2002 PAGES: 27 CLASSIFICATION: Unclassified

U.S. Information systems and critical infrastructures are vulnerable to attacks. The Department of Defense must establish directives to defend the U.S. information systems and critical infrastructures. The United States must devise measures to protect its citizens, critical infrastructures, and computer systems. The 21st century is more dynamic, with potential threats capable of launching cyber warfare via multiple means, targeting key United States' centers of gravity. Therefore, the United States must design a comprehensive computer network attack policy to deter potential adversaries. This study addresses current information operations policy, DOD roles and responsibilities, Computer Network Attack Concept and Strategy. Lastly, this report outlines the ends, ways and means of a computer network attack policy, designed to protect and sustain national security. The study highlights the current US information operations policy as it relates to computer network attack. Further, the study describes why the US must protect its information systems and critical infrastructures against potential attacks.

TABLE OF CONTENTS

ABSTRACT iii

INFORMATION OPERATIONS: COMPUTER NETWORK ATTACK IN THE 21ST CENTURY 1

CURRENT INFORMATION OPERATIONS POLICY 2

DEPARTMENT OF DEFENSE ROLES AND RESPONSIBILITIES 6

COMPUTER NETWORK ATTACK CONCEPT AND STRATEGY 7

ENDS (STRATEGIC OBJECTIVES) 10

WAYS (COURSE OF ACTION) 12

MEANS (RESOURCES) 13

CONCLUSION 14

ENDNOTES 17

BIBLIOGRAPHY 21

INFORMATION OPERATIONS: COMPUTER NETWORK ATTACK IN THE 21ST CENTURY

> Protecting critical information resources will become "one of the defining challenges of national security in the years to come", says Deputy Secretary of Defense John Hamre. Noting that the Pentagon is charged with protecting 28,000 different computer systems, he warns that securing the virtual world from cyber threats is as much a process of management approach and attention as it is of technology.[1]
>
> —John Hamre
> Deputy Defense Secretary

This study addresses current information operations policy, describes Department of Defense (DOD) roles and responsibilities, and recommends a Computer Network Attack Strategy. Lastly, this study outlines the ends, ways, and means on which to frame a computer network attack policy designed to protect and sustain our national security.

In the 21st century, protecting DOD critical information systems and critical infrastructures will be one of the greatest challenges for the United States. Today, more than ever, U.S. information systems are vulnerable to hostile attacks, even though "Information superiority is essential to our capability to meet the challenges of the 21st Century".[2] The United States has led the world into the information age; in doing so it has become critically dependent on its technologies to conduct national and international commerce, governmental functions, and military operations. Protection of the United States information and communications infrastructure has become a vital national interest.[3]

Information Operations are those actions taken to affect an adversary's information systems while defending one's own information and information systems.[4] Computer Network Attack (CNA), an element of information operations, refers to operations launched to disrupt, deny, degrade, or destroy information resident in computers and computer networks. Critical infrastructures are those physical and cyber-based systems essential to the minimal operations of the economy and government.[5] Critical infrastructure includes: information systems, computer networks, energy, banking and finance, transportation, water, and emergency services. The rapid development of technology and its interconnectivity have made it increasingly easier to attack critical U.S. infrastructures with physical or computer based attacks.[6] These infrastructures are driven by information technology and are the foundation for the United States dominance in global markets. Further, these critical assets are vital to our strategic national interests. They must be protected from potential adversaries and terrorists. The United States must devise measures to defend and protect its information systems and if

necessary, to neutralize an opponent's information capabilities. Many potential adversaries and terrorists are envious of the strong U.S. economy, values, and way of life. They would do anything to attack America's critical infrastructures and information systems.

The United States is one of the most technologically advanced countries in the world. In America, every major business office and most households have a personal computer. These computer systems are inextricably linked to secure and nonsecure computer networks. Furthermore, the Internet serves millions of interconnected subscribers globally who make billions of transactions daily. The Internet waveform is growing by nanoseconds, opening the US information systems and critical infrastructures to attack. The Internet is used as a primary means by which people, businesses and foreign and domestic governments conduct their daily operations. Critical infrastructures are essential to our country's economic success in the global market and our pursuit of happiness. Moreover, these infrastructures are key to the United States achieving its National Security Strategy through economic, social, and military means.

During the Cold War the United States deadliest threat was a nuclear attack from the Soviet Union. In the 21st century, the United States faces the even greater challenge of protecting its critical information systems and critical infrastructures. Today, the threat comes from terrorists using asymmetric tactics. The US is the world's super power and leads the way in information technology and information dominance. Accordingly, the US is more vulnerable to terrorist attacks. Many potential actors could gain unauthorized access to our information systems via covert or overt means.

DOD must update its computer network attack policy. Currently, the United States has only two policies that address information operations: Presidential Decision Directive (PDD) 63 and the National Security Strategy for a Global Age. These key National Security Strategy documents list information operations as a critical infrastructure, but do not address computer network attack. Today, information is key to the United States sustaining and maintaining information dominance. The Department of Defense must develop clearly defined policies that address protective measures for computer network attack.

CURRENT INFORMATION OPERATIONS POLICY

Presently, the US has only two policies that incorporate information operations: Presidential Decision Directive (PDD) 63 and the National Security Strategy for a Global Age of 2000. In May 1998, Presidential Decision Directive (PDD) 63 recognized that addressing computer- based risks to our nation's critical infrastructures requires a new approach that involves coordination and cooperation across federal agencies and among public and private-

sector entities and other nations. The Clinton administration implemented PDD 63 as the linchpin for safeguarding America's critical infrastructures. PDD 63 created several new entities for developing and implementing a strategy for critical infrastructure protection. Additionally, PDD 63 tasked every department and other federal agencies with developing critical infrastructure protection plans and establishing related links with private industry sectors.[7]

Currently, the US has no specific standing operating policy that governs computer network attack. A computer network attack policy would increase America's readiness. This policy would also cover our critical infrastructures that function over this waveform. Protecting our critical infrastructures in the 21st century requires that we develop a greater understanding of their vulnerabilities and act decisively to reduce them.[8] In July 1996, President Clinton, established the Commission on Critical Infrastructure Protection. However, there has been little progress in formulating a standard policy in this area.

Current DOD information systems policy is outdated and does not sufficiently address the 21st century requirements. The time has come for DOD to reassess its computer information system policies. Many current DOD policies were developed when computers were physically and electronically isolated; these policies did not anticipate today's "networked" environment.[9] Today, DOD systems are digitally interconnected globally to millions of other computer information systems. Further, DOD must establish standards, rules, and training that make users aware of the vulnerabilities of our information systems. DOD must design security measures that render critical infrastructures impervious to outside attacks in order to safeguard the US computer networks. Currently, there is no standardized training that covers computer network attack programs.

In December 2000, the Clinton Administration, published a 67-page National Security Strategy document that addresses some elements of strategy for engagement relating to information operations. However, this strategy document does not address computer network attack and the relevance of computers to our national security strategy. This document refers to information operations only through mentioning critical infrastructures and by suggesting responses to threats and crises via command control communications intelligence surveillance reconnaissance (C4ISR). This document does not mention computer network attack, a sub-element of information operations that is a critical resource to achieving the US national objectives.

The Clinton administration nonetheless recognized the vulnerability of America's computer information systems and critical infrastructure. In December 2000, President Clinton released

his National Security Strategy for a Global Age which outlined key strategic policy. This document cites critical infrastructure protection and thereby highlights information operations:

- Adapting our alliances
- Encouraging the reorientation of other states,
- including former adversaries
- Encouraging democratization, open markets, free trade, and sustainable development
- Preventing conflict
- Countering potential regional aggressors
- Confronting new threats
- Critical Infrastructure Protection
- Steering international peace and stability operations.[10]

Critical infrastructure protection is essential to the continued development of the U.S. information technology and is directly linked to the economy and national security. Critical infrastructures including; telecommunications, energy, finance, transportation, water, and emergency services--, form a bedrock upon which the success of all our endeavors -- economic, social, and military --depend.[11] All these critical areas can be targeted by terrorists; successful attack could cause catastrophic damage to American citizens at home and abroad. Although the Clinton strategy cites information operations as a critical information infrastructure, it does not address computer network attack. U.S. infrastructures are highly interconnected, both physically and through their reliance upon information technology and the national information infrastructure.[12] Since such interrelationships cut across critical components of the national infrastructure, the system is very vulnerable. The public telephone network relies on the power grid, the power grid on transportation, and all the sectors on telecommunications and the financial structure. Most of today's cybernetic networks are actually combinations of networks, interconnected and interdependent. Interactions among these subsystems are critical to overall network performance; indeed they are the essence of network performance.[13]

Since the Cold War, the United States has been the global leader in the information age of technology. Information systems and computer networks have emerged as a major catalyst for the development of the U.S. infrastructure and the global economy. With this new information age, average Americans have been more and more reliant upon information technology. This new age has altered the way Americans views technology. It has also dramatically increased US vulnerability to computer network attacks.

The September 11, 2001 attacks on the World Trade Center and the Pentagon dramatically revealed U.S. inability to protect its critical infrastructures. "Waiting for disaster is a dangerous strategy. Now is the time to act to protect our future".[14] The United States has

known for decades the vulnerabilities of its critical infrastructures and information systems. But prior to the September 11, 2001 terrorist attack, the US had done little to emplace measures to protect its critical infrastructures. These attacks tragically demonstrated vulnerabilities in the U.S. infrastructure. They also revealed that our enemies are capable of even more unimaginable attacks. These terrorist attacks on our nation proved that our critical infrastructures and defense information systems are not immune to enemy targeting. Furthermore, these attacks proved to the US that terrorist groups are capable and motivated to attack our homeland and destroy both military and civilian targets. The US must now place the highest priority on safeguarding its information systems and critical infrastructures. The US cannot afford to have its critical infrastructures and information systems attacked. Such attacks will be very costly and damaging to our economy. But the loss of one American life to a terrorist is one too many.

Since the September 11, 2001 terrorists attacks, U.S. leadership has made protection of our critical infrastructures a top priority by establishing a Homeland Defense Office and adapting other security measures to protect its citizens, information systems, and critical infrastructures. According to the Government Computer News of October 9, 2001, President Bush established a new office for cyber security and counterterrorism, a part of Homeland Defense. This new office was charged with designing a plan to protect the US and its critical infrastructures from attacks. On Sept. 11, America's commercial airspace had been weaponized and turned viciously against its financial and defense establishments in an infrastructure attack. This senseless attack killed thousands and led to grave physical and financial losses.[15] Further, this attack changed the way the average American views terrorism. President Bush responded with his Executive Order on Critical Infrastructure Protection in the Information Age. It is now the policy of the United States to protect against disruption of operation of information systems for critical infrastructure in order to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, causing the least damage possible.[16]

On September 30, 2001, the Bush Administration (DOD) published its Quadrennial Defense Review Report (QDR). The following enduring national interests were highlighted:

- Ensuring U.S. security and freedom of action, including:
- U.S. sovereignty, territorial integrity, and freedom
- Safety of U.S. citizens at home and abroad
- Protection of critical U.S. infrastructure
- Honoring international commitments, including:
- Security and well being of allies and friends
- Precluding hostile domination of critical areas, particularly

- Europe Northeast Asia, the East Asian littoral, and the Middle East and Southwest Asia
- Peace and stability in the Western Hemisphere
- Contributing to economic well-being, including:
- Vitality and productivity of the global economy.
- Security of international sea, air, and space, and information lines of communication
- Access to key markets and strategic resources.[17]

After the September 11 attack, the Bush administration made protecting America infrastructure a top priority. Yet, the most recent QDR failed to adequately address Information operations and failed to address computer network attack in the document.

DEPARTMENT OF DEFENSE ROLES AND RESPONSIBILITIES

The Department of Defense must remain engaged in protecting America's information systems and critical infrastructures. DOD must take an aggressive role in establishing policy, strategy, and operational control of U.S. information systems. DOD must accomplish the following actions to improve its efforts to protect and secure the U.S. information systems: Increase the resources devoted to computer security, update the policies that govern computer security, and increase security training for system network administrators.[18] The Department of Defense information operations policy is insufficient; it does not cover all of the key parameters. It omits cyber attack strategy, both offensive and defensive; terrorist attacks, both externally and internally, on Information systems; and information warfare. Computer network capabilities can be used to deter attacks. By revalidating the current computer network attack policy, the United States would reduce the enemies' chance of infiltrating our secure information systems.

DOD has a vast and complex information infrastructure: currently it has over 2.1 million computers, 10,000 local networks, and 100 long distance networks.[19] DOD critically depends on information technology. It uses computers to help design weapons, identify and track enemy targets, pay soldiers, mobilize reservists, and manage supplies. These figures do not account for the two million plus computer users that regularly do business with the DOD. Indeed DOD's very warfighting capability is dependent on computer-based telecommunications networks and information systems.[20] Without doubt, DOD, information systems and critical infrastructures are vital to our national security. Therefore, DOD must set and enforce policy and guidelines to protect its computer systems.

Within DOD, the October 2000 Unified Command Plan (UCP) designated the United States Commander in Chief of Space Command (USCINCSPACE) as the military lead for defending DOD Computer Networks. Space Command is responsible for developing DOD's

concept of operations and implementation plans for computer network attack. Additionally, Space Command is responsible for determining DOD capabilities, and successful employment of computer attacks in support of the United States national security objectives. Computer network attack will provide the warfighter a more lethal tool on the battlefield. According to Air Force General Myers, commander-in-chief U.S. Space Command and Air Force Space Command, DOD is moving forward to make computer network attacks part of the military arsenal.[21]

DOD computer network systems are the nucleus of the US information systems. Hence they are more susceptible to being attacked than any other network. There is mounting evidence that attacks on DOD computer systems pose a serious threat to national security.[22] The enemy can access many of the defense systems via global Internet connections. Terrorists or other adversaries can launch attacks on the defense information systems and degrade the U.S. readiness, even its capability to deploy and sustain military forces. DOD must take precautionary measures to prevent and defend its computer information systems.

Today, computer technology is growing at an alarming rate, which only increases the requirement for a current defense computer network attack policy. Our 21st century enemies do not fight by established rules of armed combat. Terrorist attacks are now bolder and more daring. According to the Defense Information Systems Agency (DISA), in recent years the number of computer attacks on DOD systems has doubled.[23] This problem alone makes US information networks more vulnerable to attack. DOD can reduce this vulnerability by establishing a seamless information systems security program.

COMPUTER NETWORK ATTACK CONCEPT AND STRATEGY

Currently, there are four dimensions of warfare: land, sea, air and space. These four dimensions have evolved throughout centuries of armed conflict. They have become standard planning factors for war campaigns. The time has come to include Computer Networks as the fifth dimension in the art of war. This new dimension changes the current methodology of warfighting. Comprehending what is new requires an understanding of what has changed.

In the past, nation-states conducted military operations in the traditional four dimensions to reach the enemy's strategic centers of gravity. Nations gauge progress toward achieving their war aims by measuring the number of enemy killed, amounts of supplies destroyed, extent of the enemy infrastructure rendered unusable, transportation disrupted, and so forth. The ultimate goal of attrition warfare is to destroy the enemy's will to make war by destroying its physical war-making capabilities.[24]

Previously, weapons technologies were designed to physically destroy the enemies' forces in one or more of the four dimensions. Military planners factored in time, space and resources in their planning cycle. However, these constraints are no longer essential. Given this new Computer Networks dimension, the race to gain numerical advantage over an enemy arms stockpile is no longer warranted. The Information Age affords the strategist new opportunities and new strategy options for a planned end state. Today, CNA alters the strategic planner's methodology due to its scope and depth of effectiveness. This unique cyber tool could allow a nation-state to impose its will upon another without physically damaging one building. This fifth dimension in the art of war changes the concept of strategic planning, because computers are not conventional warfighting tools.

Computer network attack can be used to facilitate strategic, operational, and tactical ends. Further, because physical destruction seldom results from CNA, decision-makers find it a particularly attractive option in situations short of armed conflict.[25] Information technology has changed the focus of national security due to Internet access and its capabilities. The US must now develop a strategy that includes: protecting military targets and safeguarding other national centers of gravity, such as: information systems, finance centers, airlines, and energy plants. .

For many years, great military minds such as Carl Von Clausewitz provided the principles on the art of war. Clausewitz reasoned that commitment to war emerges from the confluence of three centers of national powers: the people, the military, and the government.[26] Clausewitz believed that when these national powers are unified in pursuit of one common goal within an act of war, this combination produces a national will to fight. He also believed if an enemy disrupted the balance between the people, the military, and the government, the nation would subsequently lose its national will to fight. He reasoned that such a defeat then revealed that nation's more vulnerable power centers, causing it either to yield or face destruction of its leadership and people.[27] Computer Network Attack does not conform to the traditional applications of the use of force, because it is not defined as a force or conventional weapon. CNA is not clearly defined within the umbrella of *jus ad bellum,* that body of international law governing the resort to force as an instrument of national policy.[28] International law governing the use of force must be changed to depict new force norms concerning a computer network attack. War theory now consists of two major principles-discrimination and proportionality. For centuries, these principles undergirted standard rules of warfare. Discrimination simply recognizes the difference in treatment accorded the warrior and the innocent bystander. Combatants and their weapons are legal targets for the application of force; they assume the risk of their status, since they are present upon the battlefield by their own will. For the purpose

of this analysis, discrimination as well recognizes noncombatants' immunity from deliberate and direct attack against their person or possessions. Proportionality refers to the level and extent of force used by combatants in the discharge of their duties. The principle of proportionally balances positive consequences (military advantage) against harmful ones (collateral damage and incidental injury).[29] Computer Network Attack can be directed in an entirely different and more effective manner. It can be a weapon of mass disruption that crosses into unchartered territory from a conventional military standpoint. CNA has primary and secondary implementations based upon its target and overall objective. CNA could invoke higher order effects upon an aggressor nation, which could have ramifications on the civil population, critical infrastructures, and military posture. A computer network attack can be launched anonymously, travel at the speed of the Internet, and affect both civilian and military targets.

A computer network attack alters the conventional wartime paradigm. It can affect economic, social, mental, and physical well-being, either directly or indirectly. Its potential scope grows almost daily; it is capable of targeting everything from individual persons, objects, or entire societies.[30] CNA is a different force multiplier because it effects people indirectly and does not create physical damage like other kinetic military weapons. A computer network attack offers analogous asymmetrical benefits. In the first place, the attack will not merit a response involving the use of force. At a minimum, the legality of such a response will be debatable. Thus, because of the potentially grave impact of CNA on a state's infrastructure, it can offer a high gain, low risk option.[31] Military and civilian organizations, business, educational and financial institutions are driven by the power of technology. So they are targets of opportunity for a computer network attack. Michael Schmitt, a George C. Marshall International Fellow provides hypothetical examples on how Computer Network Attacks could target a state's civilian infrastructure in the following manner:

- Trains are misrouted and crash after the computer systems controlling them are maliciously manipulated.
- An information blockade is mounted to limit the flow of electronic information into or out of a target state.
- Banking computer systems are broken into and their databases corrupted.
- An automated municipal traffic control system is compromised, thereby causing massive traffic jams and frustrating responses by emergency fire, medical, and law enforcement vehicles.
- Intrusion into the controlling water distribution system allows the intruder to rapidly open and close valves. This creates a hammer effect that eventually causes widespread pipe ruptures.
- A logic bomb set to activate upon initiation of mass casualty operations is imbedded in a municipal emergency response computer system.[32]

These computer network attacks could cripple a city's internal functions and invoke fear throughout the populace.

The unique nature of computer network attack has implications for practitioners and policymakers. First, its potential nature may result in aggressor nations using CNA widely to accomplish a number of goals in the political and economic arenas. Such use will bring into question which policies should govern the use of CNA, wartime rules of engagement or civil law. As a political or economic tool, a computer network attack may aim to stress the population at large, which in turn will put pressure on the policymakers of the attacked state. In this way, CNA could take on the nature of economic sanctions, which could potentially cause widespread suffering of innocents as a means to achieve political influence.[33] Technologically advanced nations with critical infrastructures are vulnerable to computer network attacks that could disrupt the daily lives of civilians and immobilize military capabilities.

The United States is a world leader in high technology exports, including satellites, cellular phones, computers, information security, and commercial aircraft.[34] In order to maintain this information dominance, the United States must have a comprehensive computer attack strategy. The main points of a U.S. computer network attack strategy should serve the interests of the United States and it allies. This strategy should highlight deterrence and right of first use. The military application of such a policy has to consider: who, what, and how to attack, accounting for short- and long-term ramifications. A CNA policy must address the possible threats to civilian populations, as well as the political, and military communities. To successfully execute a computer network attack on a nation, the United States will transcend to the next level of warfare, cyberspace.

A computer network attack strategy in the 21st century could parallel the nuclear deterrence strategy of the last half of the 20th century. A U.S. computer network attack could render a targeted nation helpless without a great risk of loss of life to its armed forces. This warfare technically does not have physical boundaries. Strategic planning must be thorough and have a clearly defined end state.

ENDS (STRATEGIC OBJECTIVES)

Major General Richard A. Chilcoat provides the ends-ways-means framework that systematize strategic analysis:

> "Strategic Art entails the orchestration of all the instruments of national power to yield specific, well-defined end states. Desired end states and strategic outcomes derive from the national interests and are variously defined in terms of physical security, economic well-being and the promotion of values. Strategy as, broadly defined, is therefore: the skillful formulation, coordination, and

application of ends (objectives) ways (courses of action), and means (supporting resources) to promote and defend our national interests".[35]

The ends for which the United States should establish a computer network attack strategy are as follows:

- "Deny the efforts of hostile intruders to disrupt, destroy, or defeat United States information systems".[36]
- Protect and sustain U.S. position as the world's information dominance leader.
- Combine military and private information sectors to ensure long-term success in creating new hardware and software computer technology that protects information assurance.
- Share Computer Network Attack technology will promote peace and not support aggressor nations.

The United States is the world's super power. The Information Age has provided the United States with a distinct advantage within this spectrum. The United States is the world's information dominant leader and must sustain this posture. The Army safeguards and develops emerging information technologies in support of national security. A Computer Network Attack strategy is required to ensure the nation's world leadership into the 22nd century. Joint Vision 2020 and Army Vision 2010 guide the transformation of our forces. The overall goal of the Army's transformation efforts is to create a force capable of full spectrum dominance as the land component member of the Joint team. Both vision documents recognize the need for information dominance--the ability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Computer network operations, consisting of computer network defense and computer network attack supported by space control activities, provides the foundation from which the Army's goal of information dominance can be achieved.[37] The Army must be prepared to conduct a computer network attack to preclude future aggression.

U.S. computer attack strategy must also bring together public and private sectors to incorporate and sustain a sound policy. This new concept will help circumvent loopholes within current and future information systems whether military or civilian. DOD is charged with defending the nation and should play a leading role in the discussions on how to defend in the information dimension of warfare. DOD cannot complete this mission alone, because computer network attacks affect more than military targets.[38] Effective defensive operations will require the efforts of other government agencies and private sector companies. A computer network attack strategy governs wartime operations and must include the private sector due to the proliferation of computers throughout America. Information Assurance must be given priority and deemed a center of gravity to effectively institute an all-encompassing policy. Lieutenant

General Joseph K. Kellogg Jr., the Joint Staff Director for Command, Control, Communications and Computers (C4), declares: "The result is an unquestioned need for information assurance. Our war fighters must have complete confidence in the accuracy, authenticity and integrity of their information to achieve information superiority, a fundamental enabler for achieving Joint Vision 2020".[39]

WAYS (COURSE OF ACTION)

The United States must formulate a computer attack strategy that ensures national defense measures are met and private citizens rights are protected. This strategy should outline overarching reasons why the U.S. military power, information assurance, and economic success ride on a waveform called the Internet. The American people should be made aware of the threat and possible implications of an attack on their way of life.

Courses of actions the Department of Defense should take are as follows:

- Give information assurance priority for protection to the strategic center of gravity and, within it, specifically to telecommunications switches, electric power distribution mechanisms, gas and oil pipeline distribution mechanisms, interbank transfer mechanisms, and transportation dispatch systems. Within the defense mechanism center of gravity, communications networks, logistics and personnel databases, and transportation management systems must also be protected.[40]
- Unify a government and private sector response to protect the confidentiality, integrity, availability, and reliability of United States information and information systems against the strategic information threat.[41]
- Redefine the Defense Information Support Agency mission to include identifying critical Information Technologies, developing joint doctrine, prioritizing acquisition, ensuring interoperability between services, and protecting DOD critical information infrastructure. Technology, used correctly, begets doctrine; doctrine begets organization.[42] DOD can only achieve a sound and secure Computer Network Attack strategy through Joint Interoperability. To the extent that tomorrow's military power is defined by expertise at information rather than the application of force, military superiority may flow to those organized from the former task rather than the latter one.[43]
- Selective defense should focus on government and private sector information and information systems that are deemed critical to national security.
- Lead a vigorous public debate. The Information Age presents security risks that are economic and political, and not solely military in nature. These threats must be made known to the American people as a first step in building public support for national security priorities that are becoming more complicated daily. Government agencies and the commercial sector must find common ground to underwrite a national commitment to information assurance.[44]
- Establish a National Information Assurance Council (NIAC) to make national security policy recommendations to the president aimed at bringing about our national security vision of information assurance.[45]
- Expand the United States National Security Emergency Response Preparedness planning to include physical protection for key network switching and control systems

that manage areas within our strategic centers of gravity designated for priority protection.[46]

- Establish an Information Assurance Center, patterned after the Center for Disease Control, and answerable to NIAC to perform surveillance, research, prevention and control, and infrastructure functions within the information assurance mission.[47]
- Encourage the President and Congress to support the National Security Telecommunications Advisory Council (NSTAC) efforts to establish a Security Center of Excellence and expand the NSTAC concept by creating as similar committees in areas designated for priority.[48]
- Direct Chairman of the Joint Chiefs of Staff to promulgate a national military strategy that addresses the computer network attack, and that assures the flow of information, and that sustains information dominance in wartime.
- Educate the media on the importance of information assurance and the critical role they play in public awareness.

MEANS (RESOURCES)

- Create agencies within NATO and the United Nations to handle international information assurance issues, policies, standards, and responses to violations of said policy. Provide assistance and manpower to garner acceptance by all member nations.
- Appoint a cabinet-level Secretary of National Information to advise the President and give guidance and direction to Federal agencies and coordinate closely with the private sector. The Secretary will develop, integrate and monitor compliance with our national information infrastructures.[49]
- Publish a written National Computer Network Attack Strategy, advocated by the Secretary of National Information, to formalize our CNA vision and objectives and coordinate its implementation within the interagency process and the private sector. This strategy must provide a coordinated national strategy, unifying concerns and efforts of both government and private sectors. It must seek to identify unintended effects of new Information Technologies, take advantage of unexpected opportunities, and keep pace with emerging technologies.[50]
- The President must establish the Department of Information and move the Critical Infrastructures Assurance Office from the Department of Commerce to the Department of Information. The National Infrastructure Assurance Office, which is currently under the Federal Bureau of Investigation, should be under the operational control of the Department of Information.
- Allocate two billion dollars on Research and Development of the Computer Network Attack Program (CNAP) and a new National Defense Strategy; the CNAP will generate CNA strategy and policy documents, as well a joint certification of all hardware and software associated with the implementation phase.
- Provide the USACINCSPACE and NIAC leverage to adequately manage this program with the Secretary of National Information oversight.
- Legislate a set of Information Age War Powers as the basis for federal intervention in assuring the continued operation of the national information infrastructure in responding to threats to the national security.[51]
- Foster cooperation and adherence to this strategy among all users of information services within the United States as well as within the international community.[52]

CONCLUSION

To prevent future terrorist attacks, DOD must update its computer network attack policy and make computer network attacks a critical asset of the military arsenal. Our enemies are now using asymmetric approaches like open terrorism, information operations, and weapons of mass disruption. The US must devise measures to counter these attacks.

The United States is at the dawn of a new century. There is no other country in the world that can match the US information technology. In the 21st century, the US has become dependent on its technologies to make critical decisions to fight and win our nations wars. Moreover, the US depends upon technology to conduct national and international commerce and trade, and to direct military operations. The United States, more than any other country, is vulnerable to attack. The United States must continue to develop and implement policy and strategy to defend its information systems and critical infrastructures. Terrorists are no longer using conventional means but rather asymmetric tactics to attack our information systems and critical infrastructures. In the past, intelligence provided information on the enemy's capability and potential terrorist attacks. Today, the terrorist can attack the US information systems and critical infrastructures via covert or overt means without warning. These attacks can be achieved through infiltration of our computer networks. The United States must sustain its information dominance and ensure democracy and peace are shared by its allies.

A Computer Network Attack strategy will provide a sound foundation through the next century. Information and information systems are catalysts for the U.S. success is on the battlefield, in the boardroom, and financial markets. The Information Age has dramatically changed the quality of life of Americans and created a new and lasting dependence upon its services. More importantly, information age technologies are permanently imbedded into the political, military, and economic aspects of our critical infrastructures. America's information transformation calls for a new National Defense Strategy that includes Computer Network Attack as a new center of gravity. We can no longer deter rouge nations with our enormous Army, fleets, squadrons or arsenal. The United States must lead the world into the next century with a National Defense Policy that takes advantage of all the capabilities of information technology.

In December 1996, former Senator Sam Nunn, upon receiving the Marshall Award from the Association of United States Army, offered an insightful statement about the Information Age and America's requirement to have sound policies in place:

> "Fortunately, so far this country has not had any serious breakdowns in our information infrastructure. Americans have not had to endure any unexpected, prolonged, and widespread interruption of power. We have not had any

> grounding of our air traffic control system; and we have not had any loss of banking or financial services. We must not, however, wait for an electronic Pearl Harbor to spur us into rethinking these vulnerabilities and challenges. There is no question that the Information Age will greatly benefit our citizens ...but we must make certain that in our rush to connect, we must also formulate a national policy that promotes the security of our information infrastructure".[53]

Senator Nunn words are very prophetic in the wake of September 11, 2001. Terrorism landed on America's shore and has changed our worldview. Destruction of the World Trade Center and the Pentagon attack prove that horrific acts of violence can be inflicted upon a super power and affect its economy, military, government, transportation system, and civilian populace. These terrorist attacks were a devastating physical assault on America's symbols of wealth, power and freedom. Unlike conventional attacks that are limited to a small geographic area or location, a cyberattack has the potential to disrupt an entire state or region or -even the whole nation.[54]

Without doubt, the September 11, 2001 attack on our nation affected all Americans. Protecting and preventing America from further physical or cyber attack requires a collaborative effort from all Americans. We must formulate a Computer Network Attack Strategy to prevent future terrorist attacks in cyberspace. U.S. must retool its National Security Strategy to adequately protect our critical infrastructures. We must develop over-arching support to make computer network attack a valuable instrument in the 21st century. U.S. leaders must aggressively implement policy to protect our information systems and critical infrastructures. Further, policy makers must understand the threat that America faces in the Information Age and devise necessary measures to secure the nation against future attacks. U.S. information systems and critical infrastructures will remain vulnerable to terrorists and adversary attacks. Terrorist groups are continuing to enhance their information technology and use the Internet to formulate attack plans against the US and its allies. Our reliance on information technology has made us vulnerable to both foreign and domestic attacks of this type that were inconceivable in the past. We must now proactively develop this fifth dimension of war. DOD must formulate new directives that take advantage of cutting edge technology and facilitates quick adaptation into military defense to ensure, that our national security remains intact.

WORD COUNT = 6,265

ENDNOTES

[1] John Hamre, "Information Assurance and The New Security Epoch," USIA Electronic Journal, November 1998; available from http://usinfo.state.gov/journals/itps/1198/ijpe/pj48hamr.htm;Internet; accessed 9 October 2001.

[2] Ibid.

[3] U.S. President's Commission on Critical Infrastructure Protection, Critical Foundation: Protecting America's Infrastructures, U.S. (Washington: President Commission on Critical Infrastructure, October 1997, A-8.

[4] U.S. Joint Chiefs of Staff, Joint Pub 3-13: Joint Doctrine for Information Operations, (Washington: U.S. Government Printing Office, 9 October 1998), I-9.

[5] William J. Clinton, Presidential Decision Directive/NSC-63 (Washington: The White House, May 1998), 2.

[6] Bob Bennett, "Bennett Introduces Bill To Protect Critical Infrastructure Through Information Sharing," 24 September 2001; http://www.senate.gov/~bennett/bennett_introduces_bill_to_pro.html; Internet; accessed 26 November 2001.

[7] General Accounting Office, Critical Infrastructure Protection, Comprehensive Strategy Can Draw on Year 2000 Experiences, (Washington: United States General Accounting Office, October 1999), 5

[8] U.S. President's Commission on Critical infrastructure Protection, 6.

[9] General Accounting Office, Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (Washington: U.S. General Accounting Office, May 1996), 5

[10] William J. Clinton, A National Security Strategy For A Global Age (Washington: The White House, December 2000), 67.

[11] Ibid., 24.

[12] Ibid.

[13] Michael N. Schmitt,"Computer Network Attack and The Use of Force in International Law: Thoughts on a Normative Framework," 8 July 2001: available from http://www.usafa.af.mil/iita/assets/images/FNLSCHM.doc; Internet accessed 10 December 2001.

[14] U.S. President's Commission on Critical infrastructure Protection, 6.

[15] Bennett, 1.

[16] George W. Bush, "Executive Order on Critical Infrastructure Protection," October 16, 2001, available from http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html; Internet accessed 26 November 2001.

[17] Department of Defense, Quadrennial Defense Review Report (Washington: U.S. General Accounting Office, 30 September 2001), 2.

[18] General Accounting Office, 5.

[19] Schmitt, 1.

[20] Ibid, 10.

[21] Paul Stone, "Space Command Plans for Computer Network Attack Mission," Armed Forces News 10 January 2000; available from http://www.af.mil/news/Jan2000/n20000110_000031.html; Internet; accessed 27 September 2001.

[22] General Accounting Office, 4.

[23] Ibid, 2.

[24] Kevin J. Kennedy, Bruce M. Lawlor, and Arne J. Nelson, Grand Strategy for Information Age National Security: Information Assurance for the Twenty-first Century (Alabama: Air University Press, August 1997), 25.

[25] Schmitt, 3.

[26] Edward J. Villacres, and Christopher Bassford, "Reclaiming the Clausewitzian Trinity," Parameters 25 (Autumn 1995): 9-20.

[27] Carl von Clausewitz. On War, Edited and translated by Michael Howard and Peter Paret, (Princeton, NJ4: Princeton University Press, 1976), 90.

[28] Schmitt, 1.

[29] William J. Bayles, "The Ethics of Computer Network Attack," Spring 2001; available from http://carlisle-www.army.mil/usawc/Parameters/01spring/bayles; Internet; accessed 1 October 2001.

[30] Schmitt, 11.

[31] Ibid, 6.

[32] Ibid, 3.

[33] Bayles, 5.

[34] Clinton, 33.

[35] Richard A. Chilcoat, "Strategic Art: The New Discipline for the 21St Century Leaders," in USAWC, Selected Readings: Course 1 Strategic Leadership, Volume 1 (Carlisle Barracks: U.S. Army War College, 1998), 95.

[36] Clinton, 42.

[37] Richard V. Geraci, "The Critical Battlespace: Computer Network Operations," Army, 51 December 2001, page 44.

[38] Kennedy, 52.

[39] Geraci. Quote taken from "Joint Vision 2010 Speech," by Joseph K. Kellogg, Jr.

[40] Kennedy, 52.

[41] Ibid.

[42] Martin C. Libicki, The Mesh and the Net. (Washington: National Defense University, March 1994), 50.

[43] David S. Alberts, The Unintended Consequences of Information Age Technologies. (Washington: National Defense University, 1996), 11.

[44] Kennedy, 52.

[45] Ibid.

[46] Ibid.

[47] Ibid.

[48] Ibid.

[49] Roger C. Molander, Andrew S. Riddle, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War," Parameters 29 (August 1996): 90.

[50] U.S. Joints Chief of Staff, National Military Strategy of the United States of America, Shape, Respond, Prepare Now: A Military Strategy for a New Era, (Washington: U.S. Joint Chiefs of Staff 1997), 11.

[51] U.S. 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: U.S. Government Printing Office, November 1996), 81.

[52] Peter T. Farrell, "A National Security Strategy For Information Assurance," (Carlisle, Barracks, U.S. Army War College, April 1997), 21.

[53] Nunn Sam, "Marshall Medal Winner Outlines National Security Challenges," Army 32 (December 1996): 42-43.

[54] Jon Kyl, "Challenges in Cybercrime: The National Infrastructure Protection Center," 22 May 2001, available from http://kyl.senate.gov/0501sub/open.htm; Internet; accessed 26 November 2001.

BIBLIOGRAPHY

Alberts, David S. "The Unintended Consequences of Information Age Technologies." Washington: National Defense University, 1996.

Bayles, William J. "The Ethics of Computer Network Attack." Spring 2001. available from http://Carlisle-www.army.mil/usawc/Pararmeters/01spring/bayles. Internet Accessed October 1, 2001.

Bennett, Bob, "Bennett Introduces Bill To Protect Critical Infrastructure Through Information Sharing," 24 September 2001; available from http://www.senate.gov/~bennett/bennett_introduces_bill_to_pro.html. Internet. Accessed 26 November 2001.

Chilcoat, Richard A., Strategic Art: The New Discipline for the 21st Century Leaders. USAWC, Selected Readings: Course 1 Strategic Leadership Volume 1 USAWC 1998.

Clausewitz, Carl von, On War. edited and translated by Michael Howard and Peter Paret Princeton, NJ: Princeton University Press, 1976.

Clinton, William J., A National Security Strategy For A Global Age. Washington, D.C.: The White House, December 2000.

_____. Presidential Decision Directive/NSC-63 Washington, D.C.: The White House, May 1998.

Department of Defense, Quadrennial Defense Review Report Washington, D.C. U.S. General Accounting Office, 30 September 2001.

Farrell, Peter T. A National Security Strategic for Information Assurance. Strategy Research Project Carlisle Barracks: U.S. Army War College, April 1997.

U.S. General Accounting Office. "Comprehensive Strategy Can Draw on Year 2000 Experiences." In Critical Infrastructure Protection. Washington, D.C.: U.S. General Accounting Office, October 1999.

_____. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Washington, D.C.: U.S. General Accounting Office, May 1996.

Geraci, Richard V., "The Critical Battlespace: Computer Network Operations, Army, December 2001.

Hamre, John, "Information Assurance and The New Security Epoch." USIA Electronic Journal, Vol.3, No.4, November 1998; available from <http://usinfo.state.gov/journals/itps/1198/ijpe/pj48hamr.htm>. Internet. Accessed 9 October 2001.

Kennedy, Kevin J., Bruce M. Lawlor, and Arne J. Nelson. Grand Strategy For Information Age National Security: Information Assurance For the 21st Century. Harvard University: John F. Kennedy School of Government, 1996.

Kyl, Jon, "Challenges in Cybercrime: The National Infrastructure Protection Center." May 22, 2001, available from < http://kyl.senate.gov/0501sub/open.htm >. Internet. Accessed November 26, 2001.

Libicki, Martin C. "The Mesh and the Net." Washington, D. C., National Defense University, March 1994.

Marsh, Robert, T., President's Commission on Critical Infrastructure Protection, Critical Foundation: Protecting America's Infrastructures, United States Government Printing Office, October 1997.

Molander, Roger C., Andrew S. Riddle, and Peter A. Wilson, "Strategic Information Warfare; A New Face of War." Parameters 29 August 1996.

Nunn, Sam, "Marshall Medal Winner Outlines National Security Challenges." Army December 1996.

Schmitt, Michael N., "Computer Network Attack and The Use of Force in International Law: Thoughts on a Normative Framework." 8 July 2001; available from <http://www.usafa.af.mil/iita/assets/images/FNLSCHM.doc>. Internet. Accessed 10 December 2001.

Stone, Paul, "Space Command Plans for Computer Network Attack Mission." Armed Forces News 10 January 2000: available from <http://www.af.mil/news/Jan2000/n20000110_000031.html>. Internet. Accessed 27 September 2001.

Joints Chief of Staff, National Military Strategy of the United States of America, Shape, Respond, Prepare Now: A Military Strategy for a New Era, Washington, D.C. 1997.

_____. Joint Pub 3-13: Joint Doctrine for Information Operations, Washington, D.C.: U.S. Government Printing Office, 9 October 1998.

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.: US Government Printing Office, November 1996.

Villacres, Edward J., and Christopher Bassford, "Reclaiming the Clausewitzian Trinity." Parameters 25, Autumn 1995.