Strategy Research Project

CYBERSPACE: WHAT SENIOR MILITARY LEADERS NEED TO KNOW

BY

COLONEL DARRYL S. SHAW
United States Army

USAWC CLASS OF 2010

U.S. Army War College, Carlisle Barracks, PA 17013-5050

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
30 MAR 2010		

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyberspace: What Senior Military Leaders Need to Know	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Darryl Shaw	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College ,122 Forbes Ave.,Carlisle,PA,17013-5220	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
see attached

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**28**	

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

PROPERTY OF U.S. ARMY

USAWC STRATEGY RESEARCH PROJECT

CYBERSPACE: WHAT SENIOR MILITARY LEADERS NEED TO KNOW

by

Colonel Darryl S. Shaw
United States Army

Professor David J. Smith
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

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

ABSTRACT

AUTHOR: Colonel Darryl S. Shaw

TITLE: Cyberspace: What Senior Military Leaders Need to Know

FORMAT: Strategy Research Project

DATE: 18 March 2010 WORD COUNT: 5,480 PAGES: 28

KEY TERMS: China, Russia, Cyber Attack, Department of Defense

CLASSIFICATION: Unclassified

In the last century, the United States was protected from a direct physical attack by its adversaries due to its geographic isolation. However, today any adversary with sufficient capability can exploit vulnerabilities in the United States' critical network infrastructures using cyber warfare and leverage physical attacks to significantly impact the lives of its citizens and erode their confidence in its ability to protect their way of life. Currently, the United States is the most technologically advanced country with the greatest dependency on computer based systems and networks making it also the most vulnerable nation state in the globally connected world. This strategic research paper presents information senior military leaders need to know about cyberspace to prevent or minimize the effects of any future cyber attacks by a nation state or non-state actor against the United States' critical network infrastructures.

CYBERSPACE: WHAT SENIOR MILITARY LEADERS NEED TO KNOW

> Our technological advantage is a key to America's military dominance. But our defense and military networks are under constant attack. Al Qaeda and other terrorist groups have spoken of their desire to unleash a cyber attack on our country -- attacks that are harder to detect and harder to defend against. Indeed, in today's world, acts of terror could come not only from a few extremists in suicide vests but from a few key strokes on the computer -- a weapon of mass disruption.[1]
>
> —Barack Obama
> 44th President of the United States

Cyberspace has emerged as a national security concern for the United States and the Department of Defense because it is vital to our way of life and will influence future military operations. Much has been written about the issues of cyberspace, but many questions still remain among senior military leaders. They clearly realize that the Department of Defense must retain freedom of access to cyberspace to conduct military operations to protect the American people and advance the interests of the United States.

The Department of Defense considers cyberspace a global domain and just as vital as the air, land, sea and space domains. As such, the Department of Defense recognizes the benefits of keeping cyberspace safe, secure, and available for use. Maintaining access to the cyberspace domain is a vital interest of the United States. Therefore, senior military leaders must understand cyberspace and that the growing threats to it are one of the most serious national security challenges of the 21st century for the United States and its allies.

This strategic research paper addresses what senior military leaders need to know about cyberspace based upon conversations with members of the 2010 United

States Army War College class. It defines cyberspace, describes the threats, discusses the United States policy and strategy for cyberspace, and describes the roles and responsibilities for the Department of Defense.

Definition of Cyberspace

The term cyberspace was first used in 1982 by an American-Canadian writer, William Ford Gibson, in his short story "Burning Chrome." This fictional work portrayed two computer users who used hardware and software to successfully break into the computer system of a notorious criminal containing financial information for organized crime. The term gained further recognition when William Gibson used it in his 1984 novel, *Neuromancer,* telling the story of a computer user that was hired to conduct an intrusion into a computer system. In *Neuromancer,* Gibson defined cyberspace as:

> A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data.[2]

Since 1984, there have various attempts by numerous entities to more adequately define cyberspace. Some of those definitions are listed below in Table 1. Despite their differences, there are similarities within each definition. Such as: the role(s) of electronics, telecommunications infrastructures and information systems.[3] The definitions contained in Table 1 indicate cyberspace is more than computers and the information contained on them. However, they do not mention the unique characteristics of the cyberspace domain in comparison to the land, sea, air, and space domains.

Source	Definition
Google	The electronic medium of a computer networks, in which online communications takes place...a metaphor for the non-physical terrain created by computer systems…the impression of space and community formed by computers, computer networks and their users…the place where a telephone conversation appears to occur…the place between the phones.
Oxford English Dictionary (1997)	The notional environment within which electronic communications occur.
Walter Sharp, *Cyberspace and the Use of Force (1999)*	The environment created by the confluence of cooperative networks of computers, information systems and telecommunications infrastructures commonly referred to as the Internet and the World Wide Web.
Gregory Rattray, *Strategic Warfare in Cyberspace (2001)*	A physical domain resulting from the creation of information systems and networks that enable electronic interactions to take place…Cyberspace is a man-made environment for the creation, transmittal, and use of information in a variety of formats…Cyberspace consists of electronically powered hardware, networks, operating systems and transmission standards.
National Military Strategy for Cyberspace Operations (2006)	A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked systems and physical infrastructures.
National Security Presidential Directive 54 (2008)	The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.
Deputy Secretary of Defense Gordon England (2008)	A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Table 1: Definitions of Cyberspace[4]

For the purpose of this paper, cyberspace will be defined as:

A man-made global domain within the information environment whose distinctive characteristic is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information using interdependent and interconnected information technology infrastructures including the Internet, telecommunications networks, computers systems, and embedded processor and controllers.

To fully recognize cyberspace as a domain, senior leaders must understand the following distinctive characteristics that makes it different from the air, land, sea and space domains:

- The cost of entry for access to cyberspace is very low. All that is required is a communications device and a network connection.
- Users have the ability to conceal their identity and location which makes it extremely difficult to attribute any hostile actions to a particular user or nation state.
- Nation states or non-state actors can coordinate and conduct a cyber attack across the globe almost instantaneously.
- Cyberspace is always expanding and its boundaries continue to grow with new technologies and every new computer or Internet-capable cell phone.
- Cyberspace does not have the commonly recognized physical dimensions of height, depth and length.

Key Components of Cyberspace

There are four key components of cyberspace which make it unique and are important to addressing many of the questions associated with it. Cyberspace has a systems component, a content and application component, a people and social component, and an overarching governance component.[5] Figure 1 depicts those components in relation to each other.

The systems component consists of the technical aspects, infrastructure and architecture of cyberspace. This component includes the hardware and software applications that users rely on to store, transmit, and manipulate information in

cyberspace. Globally, a significant portion of today's economy is associated with manufacturing microprocessors, personal computers, routers, servers and operating systems for this component. There is also a sizeable portion of the economy devoted to operating and maintaining the globally interconnected communications backbone infrastructure – telecommunication firms, Internet service providers, cellular phone companies, and other public networks – for civil and military communications. For added security, many nation states, militaries, governments and private organizations use these same technologies to create closed private networks with a restricted number of connection points to public communications networks.

<table>
<tr><td colspan="3">GOVERNANCE
<u>COMPONENT</u>
Overlays all aspects of cyberspace</td></tr>
<tr><td><u>SYSTEMS COMPONENT</u>
Technical foundation, infrastructure and architecture</td><td>CONTENT/APPLICATION
<u>COMPONENT</u>
Information base and mechanisms for accessing and processing information</td><td>PEOPLE/SOCIAL
<u>COMPONENT</u>
Communications and interactions between people and information</td></tr>
</table>

Figure 1: Components of Cyberspace[6]

The content and application component refers to the information that is contained in cyberspace and the tools used to access and process that information. The content and application component relies upon the systems component and provides the applications for users to manage and share information. Some of the most commonly used applications today are email, search engines, instant messaging, electronic commerce, blogs, social networking sites, Internet telephony, news, mapping and peer-to-peer file sharing. The content and application component of cyberspace is very

dynamic because new applications continue to emerge allowing users to interact with each other and their information on a more flexible and responsive basis.[7]

The people and social component refers to the communications and interactions between people in cyberspace and the information they share. The previous two components of cyberspace enabled the growth of the people and social component by facilitating the creation of communities in cyberspace to access and share information among users. Presently, there are numerous communities meeting users' needs that are flourishing such as: dating sites, online news, health-care, religion, political, and technological. These sites allow members worldwide to interact socially and share information on a regular basis.

Unfortunately, there are some online communities with negative implications for national security. Terrorist have created communities in cyberspace to recruit new members, coordinate actions and spread their message. Also, criminals have created communities in cyberspace to commit crime and to track their business ventures.

The final governance component affects all the previous components of cyberspace. It affects the technological specifications (systems component), the standardization for data formatting and exchange (content and application component), and the legal frameworks of countries for users of cyberspace (people and social component). The mechanisms for governance of the Internet are extremely complex and require expenditure of considerable resources in various forums to achieve objectives. If governance is measured against the criteria of being open, democratic, transparent, dynamic, adaptable, accountable, efficient, and effective, then governance of the Internet has generally performed well.[8]

However, in the future, the United States may need to change its position on Internet governance. Preliminary views on this subject are being debated at Internet Governance Forums and a recent white paper stated:

> Internet Governance is an isolating and abstract term that suggests a nexus with an official government entity. The term also implies a role for the U.S. Congress in Internet decision-making. It is a misnomer because there is no true governance of the Internet; only a series of agreements between distributed and loosely connected group of organizations and influencers.[9]

One of the most remarkable aspects of cyberspace is its evolution and exponential growth. Cyberspace began in 1970's when computers were interconnected and email systems were created to share information between government research centers and academia. In the 1990s Web sites for information sharing became popular and in the early 2000s search engines and e-commerce flourished. Experts estimate that during the past 33 years, user population of the Internet increased from approximately 1 million users in 1992 to 1.2 billion users in 2007. It is further predicted that the Internet will have over 2 billion users by the end of this year. Additionally, the first cell phone appeared in 1973 and 37 years later there are more than 3.3 billion cell phones worldwide.[10]

This constant acceleration in the evolution of cyberspace will have an impact on the economy and society worldwide. Therefore, policy makers and senior leaders must understand the basic components of cyberspace and the threats to cyberspace to establish a policy and strategy for the United States and the Department of Defense.

Threats to Cyberspace

The availability of unclassified details concerning attacks in cyberspace is limited, but there are numerous reports on a variety of cyber attacks against the computers and

networks utilized by governmental agencies and large corporations. These reports serve as evidence that within the United States privately owned networks, networks operated by governmental agencies, and unclassified military and intelligence agency networks are experiencing virtually constant cyber intrusions and attacks.

In 2002, United States computer security authorities detected a series of cyber intrusions into unclassified United States military, government, and government contractor Web sites and computer systems. These intrusions are attributed to elements in China and targeted the United States Army Information Systems Engineering Command, the Naval Ocean Systems Center, the Missile Defense Agency, and Sandia National Laboratories. It is estimated the individuals or organizations in China downloaded 10 to 20 terabytes of data, an amount comparable to the entire print collection of the Library of Congress. In addition to seeking to acquire important information about military and government activities, the operation conducted reconnaissance of the U.S. command and control system, gaining information that could be used for future targeting. [11]

As shown in Figure 2, in 2007 the United States Strategic Command estimated five million computers within the Department of Defense experienced 43,880 incidents of malicious activity from various sources—a 31 percent increase over the previous year.[12] In one instance, the unclassified email system in the Office of the Secretary of Defense was penetrated and an estimated 1,500 computers were taken off line in response.[13]

Also in 2007, cyber attacks were conducted against the Departments of Homeland Security and Commerce, National Aeronautics and Space Administration

(NASA) and the National Defense University by unknown foreign entities.[14] The Department of Homeland Security suffered unauthorized intrusions in several of it's divisions, including the Transportation Security Agency.[15] The Department of Commerce took their Bureau of Industry and Security off-line for several months in response to cyber attacks. [16]

NASA was forced to impose strict email restrictions before several shuttle launches because some of their designs for new launches were compromised. [17] Recently, the Executive Office of the President of the United States revealed they also experienced cyber attacks on their networks.[18]

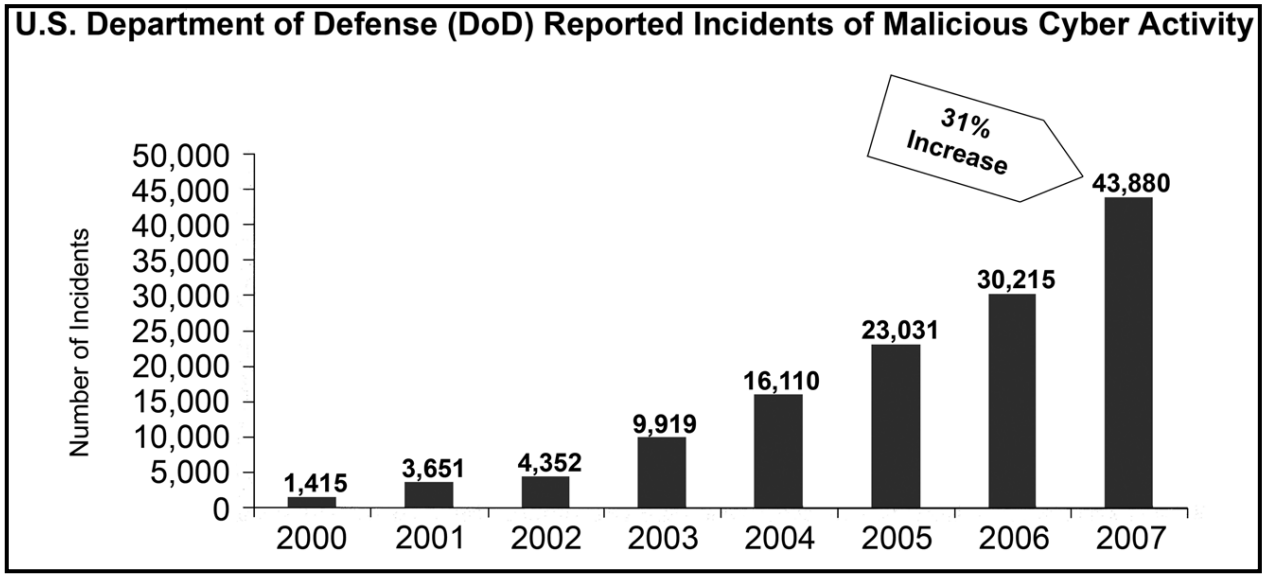

Figure 2: Incidents of Malicious Cyber Activity

In 2008, the Department of Defense suffered a severe cyber attack that may have originated in Russia and caused concern amongst senior military commanders and raised potential implications for the United States national security. The attack involved an intrusive piece of malicious software, commonly called malware, designed to target military networks. The malware was able to spread to any flash drive plugged

into an infected computer and prompted the Department of Defense to ban the use of all flash drives department-wide. These restrictions have made information sharing in the military more difficult and reflect the severity of the cyber threat.

The Department of Defense has not released the full details about the amount of damage inflicted by the attack, but they have said it affected the classified and unclassified networks of the United States Central Command in Tampa, Florida and in Iraq and Afghanistan.[19] However, the attack underscores the danger and significance of warfare in cyberspace which could be used to undermine the United States' military superiority.

The 2009 Annual Threat Assessment of the Intelligence Community estimated cyber-related business losses to be 42 billion dollars for the United States, 140 billion dollars globally, and possibly 1 trillion dollars in intellectual property worldwide.[20] Several of the Department of Defense's largest defense contractors, such as Raytheon, Lockheed Martin, Boeing and Northrop Grumman were victims of cyber attacks on their unclassified networks designed to acquire critical information on systems they were designing for the military.[21]

Types of Cyber Attacks

Various forms of cyber attacks occur on the Internet, ranging from virus infections to denial of access to cyberspace. These attacks can be divided into three categories: simple unstructured (simple), advanced structured (advanced), and complex coordinated (complex). To determine the category of an attack, it is important to examine a nation state or non-state actor resources, capabilities, resources, structures and motivations. Table 2 summarizes the characteristics of each category. A complex attack has not occurred against the United States, but there is concern that the

escalating nature of previous cyber attacks could serve as the preparation for well coordinated complex attack against our critical network infrastructures. The likelihood of any attack being successful depends on the nature of the attack, the nature of the system being attacked and the counter measures that are used to prevent an attack from succeeding.

Simple cyber attacks can be carried out by anyone with basic computer skills and basic analytical capabilities. The attacker does not need any special resources and can download hacker tools from a website, pick a target and launch an attack. Simple cyber attacks are common and they tend to attack known vulnerabilities. For example, Web defacements and denial of service attacks are a good example of this type of attack.

Advanced cyber attacks are a more sophisticated than simple attacks. At this threat level, the attacker has the ability to write programs or modify programs for their specific intent. The attacker also has an in-depth knowledge of networks, operating systems and the functionality of common firewalls and intrusion detection systems. To conduct an advanced cyber attack, nation states or non-state actors would have to recruit or hire someone with an education in computer science or a great deal of experience working with computer systems.

Advanced attacks also require more time to analyze target networks and systems to identify vulnerabilities and plan the actual attack. This may require the attackers to rehears their attack in a lab prior to implementation. Typically, an advanced cyber attack is launched against a single organization or a number of organizations with similar technology.

	SIMPLE	ADVANCED	COMPLEX
TARGET SCOPE	Single system or net	Multiple systems or nets	Multiple networks
TARGET ANALYSIS	None	Elementary	Detailed
EFFECTS CONTROL	Unfocused	Focused	Scalable
RESOURCES REQUIRED	One or more computer-literate people	One or more sophisticated programmers; simple test-bed	Several expert programmers, analysts, and planners; sophisticated test-bed
STRUCTURES REQUIRED	None	None	Synchronized teams
POTENTIAL USE	Harassment	Tactical attacks	Strategic attacks

Table 2: Cyber Threats[22]

Advanced cyber attacks can identify new vulnerabilities, but are limited in their ability to fully exploit them due to constraints in knowledge and available resources. They usually include new viruses and zero-day attacks (exploitation of a vulnerability as soon as it is discovered) applications and operating systems.[23] An example of an advanced cyber attack was the Nimda computer virus which caused billions of damage worldwide.[24] The Nimda virus was released on September 18, 2001 and became the Internet's fastest spreading worm within 22 minutes. Nimda affected user workstations running Windows 95, 98, Me, NT, 2000, or XP and servers running Windows NT and 2000. Nimda was effective because it used a variety of methods to spread such as: email, open network shares, and compromised websites.[25]

Complex cyber attacks are much more difficult to conduct than simple and advanced cyber attacks and they pose the greatest danger to United States national security and the Department of Defense. Complex cyber attacks require a team or teams of individuals with expertise in multiple technical areas such as: networks,

operating systems, programming languages, infrastructure topologies and control systems, intelligence gathering and analysis and planning. Thus, it would take a significant amount of time for non-state actors to acquire this depth of knowledge and capability compared to a nation state. Additionally, the complexity of such an attack would require a dedicated test bed and a significant amount of planning and coordination.

Complex cyber attacks can also identify vulnerabilities, but they have the depth of knowledge and resources to fully exploit the vulnerabilities across multiple networks systems and organizations. An example of a complex cyber attack would be an attack conducted against mutable critical network infrastructures in the United States to hinder military deployments.

Adversaries may also prepare for conducting a cyber attack using social engineering or by gaining physical access to system resources. By using social engineering, an adversary deceives personnel to disclose confidential information such as user names and passwords, access points, identification badges, and hours of operation as the first step to attacking a network. Traditional approaches that an adversary uses are official sounding phones calls, an intruder posing as an employee or system administrator, or even an official visitor using an organization's phone to seek technical information.[26] The knowledge that is gained can be utilized by a nation state or non-state actor to conduct a simple, advanced, or complex cyber attack.

Additionally, adversaries may also attempt to gain physical access to networks resources in preparation for an attack. By gaining physical access to the equipment or transmission mediums, an adversary could modify the hardware or software and

emplace monitoring devices to gather information to support a cyber attack. Having physical access to facilities and equipment provides an advantage to gaining unfettered access to a network and nation states and non-state actors will employ social engineering to gain access to the United States' networks. Therefore, preventing physical intrusions is vital for the Department of Defense.

United States Policy and Strategy

As the threats in cyberspace have grown in sophistication over time, the United States has attempted to address national security issues posed by them. The dual-challenge the United States continues to face is maintaining an environment that promotes efficiency, innovation, economic prosperity and free trade while also promoting safety, civil liberties and privacy rights.[27] The first steps towards a comprehensive policy to protect the United States' critical network infrastructures from a cyber attack were taken during President Clinton's second administration. In May 1998, President Clinton signed Presidential Decision Directive (PDD)/National Security Council 63 (PDD 63), "Critical Infrastructure Protection." PPD 63 assigned oversight to federal agencies for the protection of the nation's critical network infrastructures from a cyber attack.[28]

The PDD initiated a range of actions designed to improve security programs, establish a partnership between the government and the private sector, and improve the nation's ability to detect and respond to serious cyber attacks. Although PDD 63 has been superseded it continues to serve as the foundation for most of the current United States infrastructure protection policy.

President Bush signed Executive Order 13231, "Critical Infrastructure Protection in the Information Age" on October 16, 2001. The Executive Order served as a

continuous effort to protect the networks for critical infrastructure, including emergency preparedness communications and the physical assets that support them. The Executive Order also assigned responsibility to the Secretary of Defense and the Director of Central Intelligence to oversee, develop and ensure implementation of policies and standards for the security of information systems that support operations under their control.[29]

Policy and oversight structure for protecting critical infrastructure from a cyber attack established by Executive Order 13231 changed in 2002 when the Homeland Security Act was signed into law by President Bush. The Homeland Security Act established the Department of Homeland Defense and assigned it broad responsibility for protecting critical infrastructures from acts of terror and natural disasters. However, it did not give the Department of Homeland Security responsibility for protecting the critical infrastructures from basic faults, such as the Northeast blackout of 2003.[30] During the blackout, most computer-based networks that were designed to detect unauthorized border crossings, port landings, or access to many vulnerable sites failed.

In February 2003, the Department of Homeland Security (DHS) published a National Security Strategy to Secure Cyberspace. In this strategy, President Bush states:

> In the past few years, threats in cyberspace have risen dramatically. The policy of the United States is to protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States.[31]

The purpose of this document was to coordinate and focus the efforts of the United States to secure its critical private and public infrastructures for agriculture, food, water, public health, emergency services, government, defense industrial base,

information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping against a cyber attack by a adversary. The role of the Department of Homeland Security is emphasized and the National Security Strategy to Secure Cyberspace identifies the private sector as best equipped and structured to respond to cyber threats. Unfortunately, the strategy only addressed security challenges, did not demand results, and failed to require the industry segments to secure themselves by recommending tough laws and regulations.

The Homeland Security Presidential Directive 7, “Critical Infrastructure Identification, Prioritization and Protection” was signed in December 2003 and established the United States Government policy for protecting critical infrastructures from terrorist attacks. The Department of Defense was assigned responsibility for protecting infrastructures related to the defense industrial base. The Department of Homeland Security was given responsibility for protection of most other national level infrastructures including some that are critical to the Department of Defense.

In 2006, the National Infrastructure Protection Plan was signed by multiple agency heads to include the Department of Defense in an effort to improve the protection of critical infrastructures and key resources from a terrorist attack and natural disaster. But, it does not address how to prevent, deter, neutralize, or mitigate the effects of a deliberate cyber attack by a nation state or non state actors. This is one area where the United States has to improve its policy and develop a national security strategy that embraces the domestic and international aspects of cyberspace.

President Obama has identified the importance of cyberspace and realizes the United States must take a leadership role and signal to the world that it is serious about

addressing cyber threats. In a speech on May 29, 2009, President Obama identified five key actions the United States will undertake to strengthen its cyber security posture; (1) Develop a develop a new comprehensive strategy to secure America's information and communications networks; (2) Work with all the key players -- including state and local governments and the private sector -- to ensure an organized and unified response to future cyber incidents; (3) Strengthen the public/private partnerships that are critical to cyber security; (4) Invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet future challenges in cyberspace; and (5) Begin a national campaign to promote cyber security awareness to build a digital workforce for the 21st century.[32]

To achieve this vision, the United States must adopt a policy and strategy that addresses the full range of threat and vulnerability reduction, international engagement, incident response, resiliency and recovery policies and activities they relate to cyber attacks on critical network infrastructures.[33] A key component of the strategy must be deterrence by implementing a cyber offensive capability, cyber defensive capability, and an intelligence capability to gather data and information about a cyber threat or adversary.

The offensive capability is necessary and provides the United States with the ability to defend its critical network infrastructures by attacking an adversary's cyber capabilities and infrastructure. The defensive capability allows the United States to apply its resources to protect its critical network infrastructures from a potential cyber attack and to minimize or mitigate the damage if a cyber attack is successful. Finally, the intelligence capability allows the United States to collect and analyze the information

necessary to conduct offensive and defensive cyber operations against a nation state or non state actors thereby serving as a cyber deterrent.

A solid cyber deterrence strategy will contribute to other national security activities by assuring allies and dissuading adversaries while maintaining a readiness posture to defeat adversaries in the event of actual war. Cyber deterrence depends on the ability of the United States to project an image of resolve, willpower, and capability to convince a potential adversary to refrain from any activity that threatens the United States and allied interests.[34]

Offensive and defensive cyber capabilities are only a portion of the deterrence strategy for the United States. The United States can maximize deterrence by applying all the instruments of power – diplomatic, information, military and economic – to respond to a cyber attack and increase the strategic pressures and risk to a nation-state or non state actor that conducts such an attack against the United States or its adversaries.

For instance, in response to a cyber attack, the most effective response may be political and economic to isolate the attacker from the global community, mobilize the international community to condemn the attack or to impose economic sanctions. Likewise, the United States may elect to conduct military strikes in retaliation for a devastating cyber attack against its critical infrastructures. The type of response from the United States to a cyber attack depends upon the identity of the attacker and the nature of the potential attacks. But, the United States must always have the capability and flexibility to tailor its response to a cyber attack by employing the instruments of power in whatever combination desired.

The Department of Defense Roles and Responsibilities

The mission of the Department of Defense is to protect the American people and advance the interests of the United States. In the recently released Quadrennial Defense Review (QDR), the Department of Defense identified the ability to operate effectively in cyberspace as one of the key areas where it must rebalance its policy, doctrine and capabilities.[35] Protecting and defending access to cyberspace is critical because according to Deputy Defense Secretary William J. Lynn III, the Department of Defense currently operates approximately 15,000 computer networks across 4,000 military installations in 88 countries and spends billions of dollars annually to administer, monitor and defend those networks.[36] Clearly, in the 21st century, armed forces cannot conduct high-tempo, effective operations without assured access to cyberspace.

To provide assured access to cyberspace, the Defense Department of Defense identified four critical steps in the QDR to strengthen its capabilities in cyberspace. The first step was to centralize command of cyberspace operations with the creation of the United States Cyber Command (USCYBERCOM) as a sub-unified command under the United States Strategic Command. USCYBERCOM is designed to lead, integrate and coordinate the defense, protection and operation of the Department of Defense networks. Additionally, USCYBERCOM will be prepared to conduct full spectrum military operations in cyberspace when directed by the National Command Authority.[37]

The second step is for the Department of Defense to develop a comprehensive approach to their operations in cyberspace by improving operational planning and relationships with interagencies, industry, and international partners. The goal is to improve confidence in cyberspace operations by enhancing the effectiveness of all efforts to protect the critical network infrastructures of the Department of Defense.

Next, the Department of Defense must enhance partnerships with other agencies and governments. Due to the interconnectivity of networks in cyberspace, the Department of Defense networks rely heavily on commercial infrastructure. Thus, the Department of Defense must collaborate with other Federal Departments and agencies and the international community to ensure access to cyberspace and to enhance its ability to operate effectively in cyberspace. This may require the Department of Defense to share information, support law enforcement activities, provide support to the civil authorities and improve cooperation with the Department of Homeland Defense.

The final step for the Department of Defense is to develop greater expertise and awareness amongst all personnel about the threats and vulnerabilities in cyberspace. All personnel that use the Department of Defense networks must be educated, trained and empowered to counter cyber threats and reduce vulnerabilities at the lowest level possible. It is imperative for users and system administrators to gain a sense of ownership of the networks that facilitate their ability to work and to be held accountable for ensuring network security by implementing best practices.[38] Additionally, the Department of Defense must train their personnel to operate in cyberspace under conditions when their networks may be contested or under an attack by an adversary.

Conclusion

Continuous attacks on information networks which seek to compromise, steal, change or completely destroy information, especially by nation states, leave the United States vulnerable to the loss of its military technological advantage.[39] Thus, it is imperative that senior military leaders recognize the importance of cyberspace as a man-made domain similar to the commonly known warfighting domains - air, land, sea, and space. However, there are several distinct characteristics that makes cyberspace

unique and different in how the Department of Defense defines and protects the United States vital interests in cyber space.

To date, there have been numerous attacks the threats to against various entities within the United States. These occurrences clearly illustrate the United States, the Department of Defense, and the Defense Industrial base are under constant probes and attacks in the cyberspace domain. The attacks can be classified as simple or advanced depending upon the nature of the attacks and their intended purpose, but there is a possibility they are creating the conditions for a nation state or non-state actor to conduct a well coordinated complex attack against the United States.

Based upon the threats and the types of attacks a nation state of non-state actor may chose to initiate, it is evident that policies, processes and procedures are needed to mitigate cyber related threats. Several presidential administrations, to include President Obama, have recognized the importance of cyberspace as a vital interest to the National Security of the United States. As the nature of the threats have evolved in sophistication, each administration attempted to address and mitigate the risks in cyberspace. During his first year in office, President Obama directed a 60-day review to assess the United States policies and structures for cyber security which will hopefully result in a comprehensive policy and strategy to protect the United States interests in cyberspace.

Finally, the Department of Defense has the fundamental responsibility to ensure it has access to cyberspace to conduct military operations to protect the American people and advance the interests of the United States. Like the air, land, sea, and

space domains, the cyberspace domain must be protected to ensure the United States remains a beneficiary of all it has to offer.

Endnotes

[1] Barack Obama, *Remarks By The President On Securing Our Nation's Cyber Infrastructure*, (May 29, 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (accessed 25 March 2010).

[2] William Gibson, *Neuromancer* (New York: Ace Books, 1984), 51.

[3] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security* (Washington, DC: National Defense University Press, 2009), 24.

[4] Ibid., 27.

[5] Edward Skoudis and Elihu Zimet, "A Graphical Introduction to the Structural Elements of Cyberspace," in *Cyberpower and National Security* (Washington, DC: National Defense University Press, 2009), 91.

[6] Ibid., 92.

[7] Ibid., 110.

[8] Harold Kwalwasser, "Internet Governance," in *Cyberpower and National Security,* (Washington, DC: National Defense University Press, 2009), 520.

[9] Stuart H. Star, "Towards a Preliminary Theory of Cyberpower," in *Cyberpower and National Security,* (Washington, DC: National Defense University Press, 2009), 67.

[10] Ibid., 52.

[11] U.S. Congress, *US-China Economic and Security Review Commission, USCC 2008 Annual Report to Congress* (Washington, DC: U.S Government Printing Office, March 2008), 162.

[12] Ibid., 163.

[13] Sharon Gaudin, "Hack Attack Forces Pentagon to Take Computers Offline," *Information Week,* June 22, 2007, http://www.informationweek.com/news/security/showArticle.jhtml?articleID=200000073 (accessed 27 January 2010).

[14] James R. Langevin, Michael T. McCaul and Harry Raduege, *Securing CyberSpace for the 44th Presidency* (Washington, DC: Center for Strategic and International Studies, December 2008), 12.

[15] Ibid, 13.

[16] Ibid, 13.

[17] Ibid, 13.

[18] Ibid, 13.

[19] Julian E. Barnes, “Cyber-Attack on Defense Department Computers Raises Concerns,” *Los Angeles Times,* November 28, 2008, http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28 (accessed January 13, 2010).

[20] Dennis C. Blair, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Washington, DC: Office of the Director of National Intelligence, February 12, 2009), 39, http://www.dni.gov/testimonies/20090212_testimony.pdf (accessed, January 31, 2010).

[21] Andy Greenberg, “Cyber Spies Target Silent Victims,” *Forbes.Com,* September 11, 2007*,* http://www.forbes.com/2007/09/11/cyberspies-raytheon-lockheed-tech-cx_ag_0911 cyberspies.html (accessed January 25, 2010).

[22] Irving Lachow, “Cyber Terrorism: Menace or Myth?,” in *Cyberpower and National Security,* (Washington, DC: National Defense University Press, 2009), 444.

[23] Ibid., 447.

[24] Ibid., 444.

[25] CERT, “CERT Advisor CA-2001-26 Nimda Worm,” September 18, 2001, http://www.cert.org/ advisories/CA-2001-26.html (accessed January 13, 2010).

[26] Andew M. Colarik, *Cyber Terrorism: Political and Economic Implications* (Hershey, PA: Idea Group Publishing, 2006), 95.

[27] Executive Office of the President, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: Executive Office of the President, 2009), http://www.whitehouse.gov/assets/documents/Cyberspace_ Policy_Review_final.pdf (accessed December 20, 2009).

[28] Richard K. Kilroy, Jr., “Relooking the Cyber-terrorism Threat and Military Support to the National Cyber-warfare Response,” in *The Proteus Futures Digest* (Carlisle Barracks, PA: U.S. Army War College, 2007), 201.

[29] William D. O’Neil, Cyberspace and Infrastructure,” in *Cyberpower and National Security,* (Washington, DC: National Defense University Press, 2009), 131.

[30] Ibid., 132.

[31] George W. Bush*, The National Strategy to Secure Cyberspace* (Washington: DC: the White House, February 2003), iii.

[32] Barrack Obama, "Remarks by the President on Securing our Nation's Cyber Infrastructure**,"** May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (Accessed November 20, 2009).

[33] Executive Office of the President, iii.

[34] Richard L. Kulger, "Deterrence of Cyber Attacks," in *Cyberpower and National Security,* (Washington, DC: National Defense University Press, 2009), 326.

[35] U.S. Department of Defense, *Quadrennial Defense Report*, (Washington, DC: U.S. Department of Defense, February 2010), iii.

[36] Gerry J. Gilomore, "Lynn Lists Aerospace, Cyber-Age Challenges", *Defense.gov*, January 21, 2010, http://www.defense.gov/news/newsarticle.aspx?id=57664 (accessed February 1, 2010).

[37] U.S. Department of Defense, 38.

[38] U.S. Department of Defense, 38.

[39] James R. Langevin, Michael T. McCaul and Harry Raduege, *Securing CyberSpace for the 44th Presidency* (Washington, DC: Center for Strategic and International Studies, December 2008), 11.