Strategy Research Project

Cyberspace: Time to Reassess, Reorganize, and Resource for Evolving Threats

by

Colonel Steven L. Hite
United States Army

United States Army War College
Class of 2012

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 15-03-2012	**2. REPORT TYPE** Strategy Research Project	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE Cyberspace: Time to Reassess, Reorganize, and Resource for Evolving Threats	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Colonel Steven L. Hite	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Colonel Joseph C. Dill Department of Command, Leadership, and Management	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army War College 122 Forbes Avenue Carlisle, PA 17013	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Approved for public release distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

A decade into the 21st Century reflects a transition from United States national security problems that exist in the physical world, to security challenges that are beginning to move across the globe in cyberspace at the speed of light. Assaults on American critical infrastructure, government and defense networks, corporate business networks, and financial networks will continue to grow as adversaries expand their cyber capabilities to achieve their goals. To effectively counter these expanding cyber threats, the United States government must reassess, reorganize, and resource its agencies and organizations to defeat adversaries in cyberspace. The U.S. is at a transition point in history as the expanding cyber domain facilitates increasing attacks against the nation.

This paper will discuss the strategic importance of organizing and addressing the growing cyber threats facing the U.S. government, Department of Defense, corporate America, allies, partners, and U.S. citizens as they increase their reliance on cyberspace. The paper concludes with strategic recommendations for increasing U.S. capability to deal with this evolving threat.

15. SUBJECT TERMS

Computer, Network, Attack, Defense, Exploitation

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	32	**19b. TELEPHONE NUMBER** *(include area code)*

USAWC STRATEGY RESEARCH PROJECT

CYBERSPACE:
TIME TO REASSESS, REORGANIZE, AND RESOURCE FOR EVOLVING THREATS

by

Colonel Steven L. Hite
United States Army

Colonel Joseph C. Dill
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.

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

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

ABSTRACT

AUTHOR: Colonel Steven L. Hite

TITLE: Cyberspace: Time to Reassess, Reorganize, and Resource for Evolving Threats

FORMAT: Strategy Research Project

DATE: 15 March 2012 WORD COUNT: 7,569 PAGES: 32

KEY TERMS: Computer, Network, Attack, Defense, Exploitation

CLASSIFICATION: Unclassified

A decade into the 21st Century reflects a transition from United States national security problems that exist in the physical world, to security challenges that are beginning to move across the globe in cyberspace at the speed of light. Assaults on American critical infrastructure, government and defense networks, corporate business networks, and financial networks will continue to grow as adversaries expand their cyber capabilities to achieve their goals. To effectively counter these expanding cyber threats, the United States government must reassess, reorganize, and resource its agencies and organizations to defeat adversaries in cyberspace. The U.S. is at a transition point in history as the expanding cyber domain facilitates increasing attacks against the nation.

This paper will discuss the strategic importance of organizing and addressing the growing cyber threats facing the U.S. government, Department of Defense, corporate America, allies, partners, and U.S. citizens as they increase their reliance on cyberspace. The paper concludes with strategic recommendations for increasing U.S. capability to deal with this evolving threat.

CYBERSPACE: TIME TO REASSESS, REORGANIZE, AND RESOURCE FOR EVOLVING THREATS

"America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration."[1] This comment made in a 2008 study commissioned for the incoming 44th President of the United States should have been a wakeup call for not only President Obama, America's elected representatives, and the entire federal government, but also state governments, corporate America and the American people themselves.

Consider for a moment how a massive cyber attack could affect the nation. At 8:17 p.m. China Standard Time (7:17 a.m. Eastern Standard Time) on a Monday, an enter key is pressed on a keyboard at a military base on Hainan Island off the coast of mainland China in the South China Sea. The keystroke routes a computer command through a network server in Mexico City. The server in Mexico City then routes the command through a computer located in an Internet café in Cuba, which automatically receives and sends a command at 7:17 a.m. to shut down one nuclear power plant, and two coal-fueled power plants supplying New York City with residential and commercial electrical power. Subways come to a halt at the beginning of rush hour in Manhattan, all traffic lights in Manhattan shut down, automated teller machines cease to function, John F. Kennedy International Airport loses power to all air traffic control radars, runway lights and flight control radios. On Wall Street, the world's largest financial district, traders arrive to a completely dark trading floor and the Federal Reserve Bank of New York at 33 Liberty Street has lost not only city power, but also power from its backup generators. Electronic money transfers in the amount of millions of dollars every minute cease to take place. Banks up and down the East Coast of the United States begin to run out of money within hours and close their doors. This illustration is an example of what is possible from a cyber attack on one major U.S. city.

From purely an economic standpoint, the potential consequences could have disastrous effects if the nation's financial networks were shut down. In the *2010 Federal Reserve Payments Study,* it was estimated that over 84 billion electronic payments worth over $40 trillion are made annually with an annual growth rate of over nine percent from 2006-2009.[2] Additionally, nefarious cyber activity is an ever growing strategic threat to the United States of America in the 21st century.

With each passing year, the United States is becoming more and more reliant on cyberspace to accomplish tasks in areas ranging from national defense, business, transportation, finance, power production, water purification and distribution, sanitation, communication, and many other critical infrastructure areas. The increased reliance on the cyber domain by American society, businesses, and the government, at all levels, is understood to be an expanding critical vulnerability that must be addressed and mitigated. The United States government, and specifically the Department of Defense (DoD), must reassess, reorganize, and resource its agencies and organizations in preparation for significant cyber threats against the nation in the future.

In June 2009, Secretary of Defense Robert Gates directed the Commander of United States Strategic Command (USSTRATCOM) to establish the United States Cyber Command (USCYBERCOM) as a sub-unified command. "USCYBERCOM is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries."[3] With the vastness of cyberspace, USCYBERCOM has subordinate service components (established between 2009 and 2010) that are responsible for conducting effective cyber operations and defending cyberspace; Army Cyber Command (ARCYBER), 24th Air Force/Air Force Cyber Command (AFCYBER), Navy Fleet Cyber Command (FLTCYBERCOM), and Marine Forces Cyber Command (MARFORCYBER).[4] Having established service component cyber commands to defend their service networks, USCYBERCOM has an increased capability to deter and defeat attacks on the overall Department of Defense networks.

The United States government must move rapidly to build Computer Network Operations (CNO) capability to defend against, exploit, and when necessary, conduct offensive actions against attacks from hackers, nation states, terrorists, and criminals. Each branch of service in the United States Armed Forces must build capabilities to conduct CNO. CNO consists of three capabilities: Computer Network Defense (CND), Computer Network Exploitation (CNE) and Computer Network Attack (CNA). This triad of capabilities, at both a national level and individual service component level, is the basis for successful civil and military operations in cyberspace. With the impending reductions in U.S. defense spending starting in 2013, senior leaders must recognize that the defense of the cyberspace domain must account for more defense spending in future defense budgets. This was recently addressed by General Raymond T. Odierno, 38th Army Chief of Staff, in a press conference on 27 January 2012 at the Pentagon on the topic of the recently released Department of Defense Strategic Guidance and its impacts on Army transition over the next six years. General Odierno specifically mentioned that the Army would increase its investment in the cyber domain.[5] The fiscal 2012 budget for DoD overall includes $2.3 billion for improvement of cyber capabilities within DoD.[6]

Background

Throughout the ages mankind has developed new military capabilities through increased understanding of the environment and evolving technology. Conflict throughout most of history was characterized by the ability of opponents with weapons to induce violence. How much "hurt" could one opponent inflict upon another? This depended on the weapon being used. Weapons were characterized by their capabilities to inflict casualties on opponents and destruction on equipment and infrastructure. Military weapons capabilities were primarily dependent upon pure physics. How much force could be put behind a projectile to propel it though a barrel towards its intended target and ultimately how much explosive force potential can be packed into the shell itself in order to fragment upon impact to kill people and break things? New technology is changing both the weapons and munitions used in conflict.

Up until the 20th century, conflict was enabled primarily through kinetic or lethal weapons applied on the ground and through the air. Conflicts were prosecuted based on the capability of opponents to induce casualties and destroy physical objects through application of physical force. In early wars, the nation with the largest tactically proficient military force generally was victorious on the battlefield. The 20th century began to change the balance of power between kinetic and non-kinetic weapons (or lethal and non-lethal weapons). Today, information has the potential to become the "bullet" of the latest “weapon systems.” Trojans, viruses, spyware, and worms are now the “munitions” used by hackers, criminals, terrorists, nation states and others as they attack the information systems of the United States through cyberspace. The strategic consequences of any type of cyber adversary attacking national level critical infrastructure such as power generation facilities, on a large scale for an extended period of time, could have extreme economic impact on the nation. Protection of the security of the country is one of the missions of the DoD. The DoD and the Department of Homeland Security work together to protect against threats to critical civilian and military computer systems and networks.[7] Planning for defensive actions and rehearsing consequence management procedures will help mitigate the effects of a large cyber attack.

Information, altered information, and a lack of information can have a significant effect on an information systems user. The ability to deny opponents information on the status of his forces or on adversary forces can tilt the balance of power in favor of the side with information dominance. Information systems can be manned by a handful of “warriors” that possess the skills to modify the behavior of an opponent without putting troops on the ground. As the capability to provide an advantage to an operative as the information environment expands, adversaries will begin to rely less on actual ground, naval, or air power in the form of troops, combat vehicles, ships and aircraft. The operative will gain a decisive advantage by using information to further a cause, close a deal, shut down power generation, or “blind” an opponent’s air defense radars. Actions against all these target types are now actionable through cyberspace without a requirement to put troops on the ground, on the seas, or in the air to reach these targets.

What exactly is cyberspace? The 1984 William Gibson science fiction novel, *Neuromancer*, described it 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.[8]

This science fiction novel definition makes cyberspace sound like some place that does not really exist, except in the mind. The United States has been painfully reminded through the 2010 Wiki Leaks release of classified information that this new domain really does exist and can be exploited by truly anyone with a computer and access to the Internet. Operational security (OPSEC) and computer security (COMPUSEC) are critical within all organizations to combat leaks of sensitive or classified information.

As we entered the 21st century, the Department of Defense in 2000 defined cyberspace in the doctrinal manual *Joint Intelligence Preparation of the Battlespace* as "the notional environment in which digitized information is communicated over computer networks."[9] It appears there is a common theme extending from science fiction that describes cyberspace as notional and non-existent. The 1982 Disney movie *TRON* contributes to this fantasy by portraying humans entering into cyberspace via an electronic teleportation device and actually fighting and defending against villains that reside inside a network.

In 2003 the administration of President Bush published “The National Strategy to Secure Cyberspace,” and describes cyberspace as the nerve center of our nation’s critical infrastructure, both public and private; “...the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructure to work.”[10] General Peter Pace, former Chairman of the Joint Chiefs of Staff, approved the following definition in December of 2006: “A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked information systems and physical infrastructures.”[11] From early definitions of cyberspace describing it as a notional, almost virtual world to a more recent description that describes it as the central hub that controls the country through a maze of computer hardware, cyberspace has become a domain that includes a multitude of physical attributes in the form of computer hardware that is very much real.

The definition of cyberspace has evolved over the years to the latest accepted version within the Department of Defense: “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.”[12] This current definition is surely not the last. As technology evolves, information systems continue to be exploited, and our understanding of the information environment expands to include the most recent understanding of cyberspace technology, so will the definition of cyberspace. Staying current with the latest cyber doctrine enhances understanding and capabilities to secure cyberspace. Looking back in time, it is important to reflect on where conflict evolved from to better understand where we are headed in the future.

Domains

Throughout time man has evolved and adapted to his environment in order to survive. First, man operated on land, physically hunting and trading to sustain his existence. The land domain was the first for man to conquer. As time passed and technology evolved, man's interest and need to travel grew. The development of boats and ships enabled him to become a seafaring hunter and trader. He had entered the maritime domain in a quest for survival and prosperity. It is interesting to reflect on the different groups that interacted in these domains throughout time.

In the beginning on the land domain, no organized nation states existed. It was likely tribal survival of the fittest prior to the rise of civilization and law and order. In the more modern land domain of just a few centuries ago, private citizens, businesses, criminals, armies and the like shared the domain. The users of the land domain in current times have stayed relatively unchanged. The maritime domain followed a similar path with virtually the same users except navies were developed to conduct operations on the high seas, although armies could be transported via this new domain. In the 20th century, man took flight into the air and extended his reach around the world. Nation states developed air forces to take advantage of the air domain, offering speed and greater range of operations, to defend their empires or attack other nations. There are several similarities that run throughout all these domains.

History has shown that man uses all domains, as he is able to in order to realize his needs, wants, and desires. All of mankind uses the land, maritime, and air domains for traveling. Each domain provides specific benefits for the user. The benefit is dependent upon the user’s needs for each of these domains. For a tourist, travel via the air domain offers fast transportation to far away vacation destinations that may not be possible to reach via the land domain. The land domain offers a physical location for all to exist, be it a home, factory, hospital or business. The maritime domain offers the most economical means to conduct global commerce. There is one domain that is still physically out of reach of all of mankind, unless enabled by a very few nation states and private companies.

Space is the fourth domain and is truly physically assessable by only a few countries, although people in every country in the world have the capability to benefit daily from space-based assets, on an ordinary day. Space-base capabilities provide advantages across the spectrum from information to economic to military, to those who have access. Of course, in time of war nations may limit availability of some space-based systems to the general public. The capabilities provided by space based assets are truly unique, enabling, and a revolution in military affairs. Around the world the common person on the street has grown to rely on space-based assets in the form of satellite navigation for cars, aircraft, and ships. Commercial aircraft and ships rely on satellite-based navigation for movement of people and goods. Satellite-based Internet access provides the only means of World Wide Web access for many countries with underdeveloped infrastructure. Weather and telecommunication satellites provide other critical capabilities that would be difficult to operate without today. Fortunately, space-based assets are simply not as vulnerable to physical attack as assets that reside in the land, maritime, and air domains due to the extreme operational altitudes.

We all are affected by actions taken in these domains. Criminals and terrorists may operate among all these domains to execute their illegal deeds. Robbery, hijacking, piracy, terrorism, commerce, transportation and military action all are enabled through these four domains. Toward the end of the 20th century, the fifth and newest domain, cyberspace, was ushered in. The 2010 National Security Strategy gave recognition to the growing importance of cyberspace when it noted, “Cyber security threats represent one of the most serious national security, public safety, and economic challenges we face as a nation.”[13] This statement is essentially the same one made in the 2008 study *Securing Cyberspace for the 44th Presidency* commissioned under the Bush administration. The creation of USCYBERCOM in 2009 and the subsequent creations of its subordinate service components was a monumental move in recognizing the increasing threat the country faces on a daily basis and taking action to create organizations whose mission it is to operate and defend within cyberspace. In order for an organization to figure out where it is going, it must first determine where it is currently. Part of this process must include environmental scanning to see who is on the cyberspace battlefield.

Cyber Adversaries

Cyberspace is a unique domain, in that it costs very little to gain access and operate within it. Adversaries need little more than a computer with Internet access to begin exploiting the cyberspace domain. Hackers do not even have to be using their own computer equipment or telecommunications connection to begin operations. This translates into the ease with which adversaries can come from all parts of societies throughout the world and become active in cyberspace.

Thirty years ago a hacker in the most basic sense brought to mind a pimply-faced school-age kid, be it high school or college, sitting at a computer at home or in a dormitory on campus. Hollywood symbolized this perfectly back in 1983 with the release of *War Games*, starring Matthew Broderick as a young high school hacker that breaks into United States government computers responsible for alerting and firing nuclear armed ballistic missiles in the defense of the nation. Although the most numerous and publicized cyber intrusions are attributed to lone computer-hacking hobbyists, such hackers pose an insignificant threat of widespread, long-duration damage to national-level infrastructures.[14]

Today nation states seeking economic or military advantage pose the greatest risk to the security of the United States. They possess the resources with which offensive cyber operations can be developed and employed against potential adversaries or even, quite frankly, neutral or friendly nation states. These threats from national governments range from propaganda and basic annoying web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption.[15] The cyberspace domain is one that requires relatively few resources to employ potentially devastating effects on targets. Nation state goals are to weaken, disrupt or destroy the U.S. through espionage for attack and technology advancement purposes, disruption of national infrastructure to attack the U.S. economy, or full-scale attack of the infrastructure when attacked by the U.S. to damage the ability of the U.S. to continue its attacks.[16] North Korea has proven that you don’t have to be a rich nation state or even possess widespread Internet access to terrorize the financial systems of another country. In April of 2011 over 30 million customers of the South

Korean Nonghyup agricultural bank were unable to access their accounts online or through ATM machines for days supposedly due to North Korean hackers who were able to download malicious code through a bank laptop and eventually infected and crashed hundreds of servers on the network.[17] Nation states with or even without extensive financial resources have great potential when it comes to developing cyber skills as long as they have well educated people. China and Russia are the most prominent nations that are thought to have a very well developed cyber attack capability. In 2007, Estonia was the victim of a huge distributed denial of service (DDoS) attack that virtually shut down the entire banking system of the country. The effect of this was a reduction in the national economy during the days of the attack, as most currency transactions take place electronically. It is widely speculated that Russia was the actor behind the cyber curtain responsible for executing the attack. These attacks on nation states in the last few years make it increasingly important for national governments to develop solutions that provide for a backup system to reduce the effects of future cyber attacks.

Criminals can be counted among the many cyberspace “actors” that routinely use the Internet to attempt to gain financially from vulnerabilities in systems. How many Americans have had their credit card information stolen, only to find out later that a criminal had made unauthorized purchases? That Dell Computer purchase on the credit card statement doesn’t look familiar? It is probably credit card fraud executed by a cyber criminal. The anonymity of cyberspace means you’ll probably never know the identity of the criminal who committed the fraud against you.

Although cyber crime is criminal activity, can it have an effect at the strategic level? Criminals are not necessarily the actors that one thinks of when reflecting on what types of cyber activities have the potential to change the strategic landscape. Arguably an attack by cyber criminals on the financial systems of the United States truly has the potential to negatively affect national and international financial markets. A cyber crime involving stealing the wealth from the United States Treasury or the United States Federal Reserve Banks could create a seismic wave of panic in the financial markets. Organized crime organizations pose a medium-level threat to the U.S. through their ability to conduct large-scale monetary theft as well as their ability to hire or develop hacker talent.[18] Nation states can use cyber criminals as a proxy to commit crimes against other nations in an effort to cover their tracks. Anonymity offers a great advantage in the cyber world to any would be wrong doers.

Terrorists are potential players in the cyber operating environment that stand to gain much from the newest domain. The world witnessed Osama Bin Laden use the Internet to post videos in order to pass his messages to the world. Terrorists use this domain to post videos of hostages and publicize their demands. The world has also witnessed the horror of hostages being beheaded on the Internet when demands have not been satisfied. Terrorist organization use of cyberspace has been limited mainly to an information medium to influence audiences worldwide. This new domain used by terrorists truly has the potential to influence strategic audiences. Although terrorist organizations have published videos on the Internet, we have yet to see a terrorist organization launch a cyber attack. Does Al-Qa'ida have the capability to launch a cyber attack? If that organization had the capability, it surely would have used it by now on the

United States. Other terrorist organizations may well have already conducted cyber attacks against targets. Due to the anonymity of cyberspace, it is difficult to determine what or if any cyber attacks from terrorist organizations have been conducted to date. Al-Qa'ida's highest priority strategic objective is to cripple the United States economically and militarily by forcing it to bury itself in debt by spending its national treasure to protect its economic sectors, facilities, and infrastructure.

The national and international corporate business worlds are potential players in cyber space crime. The temptation to be able to acquire trade and industry secrets through illegal means is too much to ignore for some profit hungry corporations. It is well known that the government of China is suspected of stealing corporate and government product designs and using them to their advantage in their industry. In November of 2011, the Associated Press published an article based upon a United States Government report stating China and Russia are using high-tech espionage to develop and build their own economies at the expense of the United States economy amounting to theft of hundreds of billions of dollars of public and private research and development in the year 2009 alone.[19] The American economy can ill afford to lose its intellectual treasure to the Chinese and the Russians so that they may grow their economies at the expense of American jobs and gross domestic product. The United States government has a choice to make. The United States can put forth the investment of national resources and protect the country and its citizens against the threats posed by corrupt governments stealing trade and industry secrets or it can put a band-aid on the wound as the American dream bleeds out through unsecure American government and corporate networks across the country and the world. If no significant changes are made, persistent cyber threats will continue to present increasing strategic risks to nation.

Threat Categories

The actions of the United States over the next decade will determine if it is on a perilous path leading to extreme strategic vulnerability or on track to mitigate the hazards associated with cyberspace. The United States government must work with the public sector to address cyber vulnerabilities that will determine if the United States remains an economic and military superpower. The country may lose its greatness and its ability to lead the free world if its leaders cannot rally the citizens and corporations of America to recognize the strategic problems the nation faces and act to fix them. Assessments of strategic vulnerability will yield actual strategic risk that the United States can expect in the future. Any identified vulnerabilities, like control systems for electrical power grids, may be targeted by an adversary and must be constantly reevaluated to determine the amount of strategic risk that is acceptable.

Strategic risks associated with cyber attacks on the United States can be broken down into two broad threat categories; attacks related to military purposes and those using cyberspace for crime and espionage.[20] These are two very broad categories that are very complex in nature. The distinction between these two threats revolves around whether a malicious action in cyberspace is comparable to the use of force, to an attack using conventional weapons.[21] The ability to use data streams over a network provides potential adversaries the ability to inflict losses on the targeted system. As much as it may seem like science fiction, data streams transported via the Internet from computers located anywhere in the world can produce both kinetic and non-kinetic effects on targets world-wide. A cyber attack that produces effects comparable to that of conventional weapons falls into the military purposes category.

The first category, attacks related to military purposes, covers more than just the military-type targets that immediately come to mind, like DoD computer networks, but also covers attacks on hydroelectric machinery or floodgates in a dam. The military doesn’t own this dam; however, the electrical power being generated at this dam powers the electric grid for a nearby military base and should be considered as an attack on the capabilities of the base. In another scenario a nation state attacks this dam with the purpose of opening floodgates in order to destroy a town or city as part of a broader military attack on the targeted country. Cyber attackers, for all practical purposes, operate behind a smoke screen that makes identification very difficult. The anonymity afforded in cyberspace has made operations in this field more desirable to less powerful nation states than on a traditional field of battle where opponents can see each other. If an opponent can be seen on the battlefield, he is vulnerable to being engaged with a weapon. Identifying the location of a cyber attacker can be as difficult as finding someone in a “house of mirrors” at a carnival. You may think you see the location of your opponent; however, the image of the person you are looking for is simply an image in a mirror being used to hide the true location of the attacker. Due to the difficulty at locating the origin of a cyber attack, responses must be carefully planned, vetted and executed to ensure the lowest collateral damage possible.

The second category, using cyberspace for crime and espionage, is the preferred modus operandi for nation states. They focus their efforts on espionage and crime, which, in cyberspace, carries very little risk.[22] The United States economy is particularly vulnerable to the effects of cyber attacks. Stolen trade secrets, technologies, and intellectual property account for staggering losses to the Gross Domestic Product of the United States. In fact, in Europe it is estimated that German losses of intellectual property via Internet economic espionage amount for approximately $20 billion and the United States losses are estimated to be anywhere from $100 billion up to $1 trillion.[23] These are staggering numbers that have the potential to go much higher as cyber attacks increase and become even more common. The United States is in an economic cyber war costing corporations their product trade secrets, innovation, American jobs, and making the country economically weaker every year with the growing theft of our intellectual property.[24]

When it comes to United States national security, all eyes are on the United States Department of Defense to provide for the defense of the nation. Is the DoD responsible for securing cyberspace in the United States or is it the responsibility of another department?

Department of Defense Strategy

Cyberspace in the year 2012 is a domain that Americans rely upon to communicate, socialize, trade, entertain, educate, plan, and conduct countless other activities. Billions of people around the globe use the Internet on Internet connected devices ranging from smart phones to tablets to desktop computers. The United States Department of Defense relies on cyberspace to function on a daily basis, just as the rest of the world so does. In fact, it is not an overstatement to say that without connectivity to DoD computer networks around the world, the Armed Forces of the United States simply cannot function anywhere near full capability. Sure, troops can conduct foot patrols and engage the enemy with their rifles when they identify their targets, but the ability to communicate and pass data, intelligence, and orders will practically cease if networks are brought down; that is until the American soldier finds a work-around to get the mission completed. The DoD employs over seven million computing devices on over 15,000 networks spread over hundreds of installation in dozens of countries around the world.[25] This size and diversity of this type of information environment can be described as a target rich environment for cyber actors from around the world.

The DoD is very concerned with three areas that are susceptible to possible adversarial action: theft or exploitation of data; disruption or denial of access or service that affects the availability of networks, information, or network-enabled resources; and destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems.[26] In preparation to combat threats from opponents in these three areas, the *Department of Defense Strategy for Operating in Cyberspace* has developed five strategic initiatives.

First, DoD will treat cyberspace as an operational domain to organize, train, and equip so that it can take full advantage of the potential capabilities.[27] This requires USCYBERCOM and its subordinate component commands to build and man the organizations required to ensure freedom of action for our forces in cyberspace. The DoD manages cyberspace risk, assures integrity and availability, and ensures the development of integrated capabilities to rapidly deliver and deploy innovative capabilities where they are needed the most.[28]

Second, DoD will protect its networks and systems through employment of new defense operating concepts.[29] Concepts drive change within the Department of Defense and must be regularly updated based upon envisioning future operating environments to enable future forces with the capabilities required to accomplish the mission. Mission accomplishment in the cyberspace mission is secured through employing the best cyber security practices, deterring and mitigating insider threats, enabling effective communications practices, preventing intrusions and developing new defense operating concepts and computing architecture to form an adaptive and dynamic defense of DoD networks and systems.[30]

Third, DoD must enable a whole-of-government cyber security strategy through partnerships with U.S. government departments and agencies and the private sector.[31] The DoD operates networks that rely upon commercial Internet Service Providers (ISP), computers, hardware, software and the like that flow into and operate within the Department of Defense. Cyber security strategy requires all players to get involved in development of integrated solutions based upon the experience and expertise of all elements. Expected participants include Department of Homeland Security (DHS), DoD, National Security Agency (NSA), ISPs, and commercial computer hardware and software developers and manufacturers. Only though a collaborative approach to cyber security, with the partnership between government and industry, will the nation benefit and become more secure in cyberspace.

Fourth, DoD must build robust relationships with U.S. allies and international partners to strengthen our collective cyber security.[32] Security can only be improved through constant, collaborative partnerships in which the latest threat information and solutions to cyber security threats can be shared to protect the security of the domain.

Finally, DoD must leverage national ingenuity through an exceptional cyber workforce and rapid technological innovation.[33] In an age of decreasing science and technology degrees being earned by Americans in universities around the country, it is not surprising that the nation is challenged to produce an adequate amount of cyber security specialists. The waning talent pool must be grown through a deliberate and prolonged campaign to lure the best and brightest students from the nation's high schools, graduate, and post-graduate institutions to lead the national and international race to secure cyberspace. The future of cyberspace rests in large part on our national leadership's ability to convince the American public that the nation is depending on them to be a part of the solution in this national security issue.

With each passing year cyberspace capabilities continue to challenge what seemed unimaginable only a few years earlier. American computer and software development companies are world leaders in innovation; however, more emphasis on collaboration with the federal government is the way ahead to secure operations in cyberspace in the future. DoD's five strategic initiatives have laid out a plan to operate effectively in cyberspace, defend national interests, and achieve national security objectives. These initiatives provide a good basis, but nothing that is revolutionary. Revolutionary change may not be required to a protect cyberspace. The United States government must make cyberspace a very high priority. High priority equates to additional funding within the national budget. As the DoD reduces the size of the armed forces starting in fiscal year 2013, it should increase spending on cyberspace. The effectiveness of current policy must be regularly assessed to ensure DoD remains on track for cyber mission success.

Future of Cyberspace

As the Internet continues to expand its network of networks, people, businesses, governments, and nations around the world become more susceptible to the threats presented in cyberspace. Nation states continue to be cautious in their cyberspace activities and focus on espionage and criminal activities because it carries almost no risk, whereas computer network attack risks starting a cyber war with the United States.[34] Espionage and criminal type activities focus on theft of information as stated before; through computer network exploitation. The State and Defense Departments say that by 2007 they had already lost about six or seven terabytes of information through exploitation of their computer networks, which is roughly about 40 million books or manuscripts.[35] The theft of information is not currently viewed as an act of war in international customary law. Legal opinions will continue to be formed as the volume of cyber attacks expand and the scope of data theft becomes simply unacceptable. The theft of American intellectual property is a very serious problem for not only the economy but also the national security of the nation. Nation states, especially China, have been highlighted in the news for years as they steal American corporate secrets that are copied and used to economic advantage of American economic competitors.

On the much darker side of cyberspace, nation states that participate in computer network attack should be ware that they are walking on perilously thin ice. In October 2011 an article was published titled “Doctrine to Establish Rules of Engagement Against Cyber Attacks” was published. The article states that new doctrine under review by the Joint Staff will publish rules of engagement that will help define conditions in which the military can conduct offensive operations against cyber threats and what specific actions can be taken.[36] Earlier, in May 2011, a *Wall Street Journal* article titled “Cyber Combat: Act of War,” was published that discussed how the Pentagon could respond to certain cyber attacks with military force. The premise behind the article is that the Pentagon has concluded that certain types of cyber attacks that produce death, damage, destruction or high-level disruption comparable to that of a conventional military attack would be a candidate for retaliation with a use of force.[37] The legalities of the use of cyberspace for offensive purposes are clearly not defined with any true international agreement as to what constitutes an act of war. This statement by the U.S. Department of Defense serves as a clear warning to any nation state or non-state actor that the U.S. reserves the right to retaliate in a conventional kinetic response. The United States government is working to establish “the laws of cyber warfare” in the absence of any international agreements or treaties. This is important so that the U.S. government is seen as a responsible nation should it be forced to defend U.S. national interests.

The future will see a world of adversaries that rely on information warfare more so than on conventional warfare. In the coming decade or two, kinetic terrorist organization attacks using bombs and bullets from groups like Al-Qa’ida will seem absolutely primitive in nature.[38] The day is coming where these types of terrorist organizations will recognize they can cause much more pain to America and other opponents in the Western world by growing their information warfare skills and attacking the services and sectors that bring great economic wealth to this country. Non-kinetic cyber attacks will inflict a lot of pain and terror into the citizens of the United States in the future without the overt violence the world has seen from terrorists in the first decade of the twenty-first century. It has been hypothesized that there are cultural and technical obstacles, such as the glorification of violence and the enormous complexities involved in understanding information infrastructures, which might prevent terrorist groups from adopting wholesale the methods of cyber terror.[39] Finally, the Director of the Federal Bureau of Investigation (FBI) stated on March 1, 2012, that in the not too distant future the FBI expects that the cyber threat will eclipse terrorism as the number one threat to the United States. If the future looks anything like the recent past, the Internet and the network of networks will continue to grow and cultivate a larger cyber threat that the nation must acknowledge and challenge before the U.S. suffers its first catastrophic cyber attack from a covert attacker. The United States must defend against and be ready for a “cyber Pearl Harbor” attack.

Conclusion

The man-made fifth domain of strategic power, cyberspace, provides a fantastic opportunity for both good and evil. The U.S. Department of Defense exists to deter aggression and when necessary, go to war to protect the nation. The way in which wars have been fought throughout history depended greatly upon the domain or domains in which they operated. Nations adapt to the current operating environments that pose the greatest risk. Cyberspace is the newest domain that man has chosen to conduct operations ranging from crime to war. Just as the United States has invested heavily in the domain of space to gain operational and strategic advantages, the nation must now invest in cyberspace to greatly expand national level capabilities to secure the nation and when necessary attack to defend national interests. This domain possesses an unimaginable amount of potential for nations that choose to invest in the possibilities. The United States Department of Defense must make a conscience decision to greatly expand the manning of cyber organizations like USCYBERCOM and its component commands. With all indications that cyber activities will continue to rapidly grow, DoD must lead change by developing new concepts to secure a changing world. The training and education of new cyber warriors must be done smartly. Cyber organizations must be truly unique hybrid organizations that include members of the armed services, federal agencies, international community, coalition members, and private commercial industry. It is only through collaboration among government and private industry organizations that the United States will be able to achieve freedom of action in cyberspace and be able to deny the same to adversaries.

The U.S. Commander-in-Chief must be presented with options in the event of a significant cyber attack on the nation. Options for responding to a cyber attack must be preplanned and ready for immediate implementation. The United States must move forward quickly to develop response policy regarding cyber attacks that range from simply annoying to threatening to catastrophic actions against the infrastructure of the nation. Policy takes time to develop and must therefore receive high priority for developing and approving. Congress has the power to make government and private industry cooperate in order to defend the nation in the cyber world. Cyber is an area that there must be a coordinated effort headed by the federal government and supported by private industry in order to prevail. The United States must act sooner rather than later to rapidly develop cyber policy to act with legal authority against all types of threats, be they nation states, criminals, terrorists, or hackers.

United States national leaders must lead the charge to recruit and grow American talent in the sciences and mathematics. The nation must provide irresistible incentives for the best and brightest high school and college students to accept the challenge of becoming the next generation of cyber warriors to defend our nation against all types of cyber threats. Offer free education and rewards for the best of the best to accept careers in the cyber realm of the United States government. Attract the best and brightest computer hardware, software and network specialists from among the U.S. population. Develop broadening experiences for government and private industry through exchange programs. These programs will facilitate communication, understanding and cooperation between government and industry for more effective national cyber defense.

Finally, the United States is the most capable nation in the world and must take the international lead role in reassessing, reorganizing, and resourcing an updated cyber strategy emphasizing cyber policy, promoting security, policing the network with international partners and growing cyber experts. With a decreasing European footprint and fewer U.S. forces deployed around the world, the United States must capitalize on growing partnerships throughout the world to increase cyber security. In the future cyber world, physical security may have little relevance or deterrent effect against catastrophic attacks on critical infrastructure or information systems. The time to reassess, reorganize, and resource is now; before a catastrophic cyber attack on American critical infrastructure or information systems paralyzes the nation.

Endnotes

[1] CSIS Commission of Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, December 2008, 11.

[2] Board of Governors of the Federal Reserve System, "*Federal Reserve Study Shows More Than Three-Quarters of Noncash Payments Are Now Electronic,*" December 8, 2010, http://www.federalreserve.gov/paymentsystems/files/fedfunds_ann.pdf (accessed January 28, 2012).

[3] *United States Strategic Command Cyber Command Factsheet,* http://www.stratcom.mil/ factsheets/cyber_command (accessed December 12, 2011).

[4] Ibid.

[5] Army Chief of Staff General Raymond T. Odierno, “Budget Impact to the Army Briefing at the Pentagon,” Washington, DC, Pentagon, January 27, 2012, http://www.defense.gov/ transcripts/transcript.aspx?transcriptid=4964, (accessed March 15, 2012).

[6] U.S. Office of Management and Budget, *Budget of the United States Government, Fiscal Year* 2012 (Washington, D.C.: U.S. Government Printing Office, 2011), 63.

[7] U.S. Department of Homeland Security, *FY 2012 Budget in Brief,* (Washington, DC: U.S. Department of Homeland Security, 2011), 12.

[8] William Gibson, *Neuromancer* (New York: Ace Books, 1984), 51, quoted in Darryl S. Shaw, *Cyberspace: What Senior Military Leaders Need to Know,* Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, April 18, 2010), 2.

[9] U.S. Joint Chiefs of Staff, *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*, Joint Publication 2-01.3 (Washington, DC: U.S. Joint Chiefs of Staff, May 24, 2000), GL-4.

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

[11] U.S. Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations (Unclassified),* (Washington, DC: Chairman of the Joint Chiefs of Staff, December 11, 2006), ix.

[12] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010 (as amended through 15 November 2011)), 86.

[13] Barrack H. Obama, *The National Security Strategy* (Washington, DC: The White House, May 2010), 27.

[14] United States Computer Emergency Readiness Team (US-CERT), Control Systems Security Program (CSSP), “Cyber Threat Source Descriptions,” http://www.us-cert.gov/control_ systems/csthreats.html (accessed March 3, 2012).

[15] Ibid.

[16] Ibid.

[17] Chico Harlan and Ellen Nakashima, “Suspected North Korean Net cyberattack on a bank raises fears for South Korea, allies,” *The Washington Post Online,* August 29, 2011, http://www.washingtonpost.com/world/ national-security/suspected-north-korean-cyber-attack-on-a-bank-raises-fears-for-s-korea-allies/2011/08/07/gIQAvWwIoJ_story.html (accessed March 14, 2012).

[18] US-CERT, CSSP, “Cyber Threat Source Descriptions,” (accessed March 14, 2012).

[19] The Associated Press, “Report accuses China, Russia of cyber-attacks,” November 3, 2011, http://www.syracuse.com/news/index.ssf/2011/11/report_accuses_china_russia_of.html (accessed February 25, 2012).

[20] James A. Lewis, *Cybersecurity: Assessing the Immediate Threat to the United States*, (Washington, DC: Center for Strategic & International Studies, May 2011), 2.

[21] Ibid.

[22] Ibid., 3.

[23] Ibid., 3-4.

[24] Mark Clayton, “The new cyber arms race,” *The Christian Science Monitor Online,* March 7, 2011, http://www.csmonitor.com/ USA/Military/2011/0307/The-new-cyber-arms-race (accessed March 3, 2012).

[25] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: July 2011), 1.

[26] Ibid., 3.

[27] Ibid., 5.

[28] Ibid.

[29] Ibid., 6.

[30] Ibid.

[31] Ibid., 8.

[32] Ibid., 9.

[33] Ibid., 10.

[34] Lewis, *Cybersecurity*, 3.

[35] Ibid.

[36] Donna Miles, “Doctrine to Establish Rules of Engagement Against Cyber Attacks,” U.S. Department of Defense, October 20, 2011, http://www.defense.gov/news/ newsarticle.aspx?id=65739 (accessed March 7, 2012).

[37] Siobhan Gorman and Julian E. Barnes, “Cyber Combat: Act of War,” *Wall Street Journal*, May 30, 2011, http://online.wsj.com/article/ SB10001424052702304563104576355623135782718.html (accessed March 14, 2012).

[38] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (New York, NY: Frank Cass, 2004), 187.

[39] Ibid.